



ПРОГРАММНЫЙ КОМПЛЕКС

INFOWATCH ARMA СТЕНА

Межсетевой экран нового поколения
для промышленных и корпоративных сетей

**Руководство по настройке «ARMA Стена» с использованием
интерфейса командной строки (CLI)**

Версия 2 ред. от 09.02.2026

Листов 776

СОДЕРЖАНИЕ

Термины и сокращения	12
Аннотация.....	16
1 Подготовка к работе.....	17
1.1 Установка	17
1.1.1 Установка ПО ARMA Стена в ПАК	17
1.1.2 Настройка интерфейсов	23
1.1.3 Настройка часового пояса.....	26
1.1.4 Ручная настройка даты и времени.....	27
1.2 Способы управления.....	28
1.2.1 Последовательная консоль	28
1.2.2 SSH подключение	30
1.2.3 Веб-интерфейс	32
1.3 Управление лицензией.....	35
1.3.1 Активация системы ARMA Стена	35
1.3.2 Информация о текущей лицензии.....	42
2 Интерфейс командной строки	43
2.1 Эксплуатационный режим.....	46
2.2 Конфигурационный режим	47
3 Интерфейсы.....	53
3.1 Физический интерфейс.....	53
3.1.1 Конфигурирование.....	53
3.1.2 Расширенные настройки	59
3.1.3 VLAN 802.1Q.....	68
3.1.4 SPAN.....	73
3.2 Сетевой мост	73
3.2.1 Основные настройки.....	74
3.2.2 Настройка DHCP(v6).....	80
3.2.3 Делегирование префиксов DHCPv6 (PD)	81
3.2.4 Настройка параметров сетевого моста	82
3.2.5 STP	83
3.2.6 VLAN.....	84
3.3 Агрегированный интерфейс	92

3.3.1	Конфигурирование.....	92
3.3.2	VLAN	106
3.3.3	SPAN	114
3.3.4	Мониторинг и эксплуатация	115
3.3.5	Примеры настройки агрегированного канала.....	119
3.4	Туннелирование	122
3.4.1	Общие команды настройки	123
3.4.2	GRE	124
3.4.3	ERSPAN	126
3.5	PPPoE.....	128
3.5.1	Настройка PPPoE-соединения.....	128
3.5.2	Команды настройки PPPoE	129
3.6	Интерфейс Loopback	132
3.6.1	Настройка loopback-интерфейса	132
3.6.2	Дополнительные настройки loopback-интерфейса	133
3.6.3	SPAN	134
3.6.4	Мониторинг loopback-интерфейса.....	134
3.7	Интерфейс Dummy	135
3.7.1	Настройка dummy-интерфейса	136
3.7.2	Дополнительные настройки dummy-интерфейса	136
3.7.3	SPAN	137
3.7.4	Мониторинг dummy-интерфейса	138
3.8	WireGuard.....	139
3.8.1	Настройка интерфейса WireGuard	139
3.8.2	Дополнительные настройки интерфейса WireGuard.....	142
3.8.3	SPAN	146
3.8.4	Настройка WireGuard в режиме «сеть - сеть»	147
3.9	VXLAN	149
3.9.1	Общие параметры	150
3.9.2	Режимы туннеля	153
3.9.3	Single VXLAN Device (SVD).....	154
3.9.4	Параметры маршрутизации IPv4	154
3.9.5	Параметры маршрутизации IPv6	157

3.9.6	SPAN	159
3.9.7	Пример настройки VXLAN	160
4	Системные настройки	162
4.1	DNS	162
4.1.1	Системный DNS.....	162
4.1.2	Динамический DNS.....	164
4.1.3	Перенаправляющий DNS	170
4.2	Шлюз по умолчанию	175
4.3	Системный Прокси	176
4.4	Служба NTP.....	177
4.4.1	Дополнительные настройки NTP.....	178
4.5	Планировщик задач Cron.....	178
4.6	Мониторинг аппаратной платформы	179
4.6.1	Мониторинг блока питания	179
4.6.2	Мониторинг аппаратной платформы.....	181
4.7	Мониторинг процессов.....	182
4.8	Управление питанием.....	185
4.9	Zabbix.....	186
5	Управление системой.....	189
5.1	Управление конфигурацией.....	189
5.1.1	Настройки архива конфигурации.....	190
5.1.2	Сравнение конфигураций.....	190
5.1.3	Восстановление конфигурации	192
5.1.4	Удаление конфигурации	192
5.1.5	Экспорт конфигурации.....	193
5.1.6	Импорт конфигурации	197
5.2	Обновление системы	200
5.3	Сброс настроек	206
5.4	Аварийный режим.....	208
5.4.1	Автоматический переход в аварийный режим	209
5.4.2	Переход в аварийный режим по команде оператора	209
5.4.3	Информация о причинах перехода в аварийный режим.....	211
5.4.4	Отключение аварийного режима	212

5.4.5	Дополнительные параметры	212
5.4.6	Загрузка в аварийном режиме при неисправности интерфейса	213
5.5	Контроль целостности	215
5.5.1	Список контролируемых объектов КЦ	216
5.5.2	Регистрация событий КЦ	220
5.5.3	Пересчёт эталонных значений КЦ	222
5.5.4	Диагностика и восстановление службы контроля целостности при загрузке	222
6	Управление доступом	224
6.1	Аутентификация	224
6.2	Локальные учётные записи	224
6.2.1	Просмотр локальных учётных записей	224
6.2.2	Добавление пользовательских учётных записей	236
6.2.3	Политика паролей учётных записей	238
6.2.4	Временная блокировка учётных записей	239
6.2.5	Назначение прав доступа пользовательским учётным записям	241
6.2.6	Тайм-аут пользовательской сессии	254
6.2.7	Блокировка пользователя	254
6.2.8	Управление пользовательскими сессиями	256
6.3	Аутентификация RADIUS	258
6.3.1	Добавление внешнего Radius-сервера	259
6.3.2	Дополнительные команды настройки Radius-сервера	260
6.4	Multifactor Radius Adapter	261
6.4.1	Multifactor Radius Adapter - Windows	261
6.4.2	Multifactor Radius Adapter - Linux	282
7	Маршрутизация	290
7.1	Маршрутизация	290
7.1.1	Настройка статического маршрута	290
7.1.2	Настройка интерфейсного маршрута	290
7.1.3	Настройка тупикового маршрута	291
7.1.4	Настройка статической записи ARP	292
7.2	Отказоустойчивая маршрутизация	292
7.2.1	Добавление маршрута	292

7.2.2	Проверка доступности маршрута.....	293
7.2.3	Пример настройки отказоустойчивой маршрутизации	294
7.3	Протоколы маршрутизации	295
7.3.1	RIP	295
7.3.2	OSPFv2	301
7.3.3	OSPFv3	315
7.3.4	BGPv4	319
7.4	ECMP.....	331
7.5	Политики фильтрации маршрутов.....	334
7.5.1	Политика списка доступа	334
7.5.2	Политика списка префиксов.....	337
7.5.3	Политика маршрутной карты	340
8	VRF.....	346
8.1	Конфигурация	346
8.2	Обслуживание VRF	348
8.3	Пример конфигурирования VRF	350
9	Отказоустойчивость.....	353
9.1	VRRP.....	353
9.1.1	Глобальные настройки	358
9.1.2	Настройка Gratuitous ARP.....	359
9.1.3	Команды настройки группы VRRP.....	360
9.1.4	Динамическая корректировка стоимости маршрута.....	367
9.1.5	Группа синхронизации VRRP	368
9.2	Синхронизация конфигурации	371
9.2.1	Команды настройки синхронизации конфигурации	376
9.2.2	Точечная синхронизация конфигурации.....	378
9.2.3	Настройка синхронизации конфигурации в отказоустойчивом кластере	379
9.2.4	Особенности настройки устройств кластера	381
9.3	Пример настройки отказоустойчивого кластера.....	383
9.4	Пример настройки динамической корректировки стоимости маршрута ..	385
10	Балансировка нагрузки	392
10.1	Балансировка нагрузки на WAN-интерфейсах.....	392

10.1.1	Основные настройки	392
10.1.2	Проверка состояния интерфейсов	393
10.1.3	Правила балансировки	396
10.1.4	Пример настройки	402
10.2	Обратный прокси-сервер	403
10.2.1	Основные настройки обратного прокси-сервера	403
10.2.2	Пример настройки обратного прокси-сервера	413
11	VPN.....	416
11.1	OpenConnect.....	416
11.1.1	Подключение через VPN-клиент.....	416
11.2	OpenVPN.....	421
11.2.1	Site-to-Site.....	421
11.2.2	Сервер - Клиент	428
11.3	IPsec	440
11.3.1	IKE	442
11.3.2	ESP.....	447
11.3.3	GRE over IPSEC.....	450
11.3.4	IPSEC Site-to-Site (Policy Based)	455
12	Межсетевой экран	464
12.1	Межсетевой экран	464
12.1.1	Глобальные настройки	467
12.1.2	Группы.....	469
12.1.3	Стандартная политика на основе системных наборов правил	476
12.1.4	Политика на основе зон	505
12.1.5	Мониторинг срабатывания правил	508
12.1.6	Журнал межсетевого экрана	510
12.2	NAT.....	513
12.2.1	Правила NAT	513
12.2.2	Примеры создания правил NAT.....	517
13	COB (IDS/IPS).....	519
13.1	Включение IDS/IPS	519
13.1.1	Примеры настройки включения COB.....	523
13.2	Правила Suricata	526

13.2.1	Создание правила Suricata.....	528
13.2.2	Создание правила IDS/IPS для фильтрации L7 по протоколу	530
13.2.3	Редактирование правил Suricata.....	532
13.2.4	Выключение правил Suricata	534
13.2.5	Удаление правила Suricata.....	536
13.2.6	Обновление правил Suricata.....	537
13.3	Команды настройки Suricata	539
13.4	Контроль протоколов.....	556
13.4.1	ADS.....	557
13.4.2	Alpha Link	563
13.4.3	AoE	564
13.4.4	DNP3.....	565
13.4.5	ENIP/CIP	569
13.4.6	EtherCAT.....	572
13.4.7	Fanuc FOCAS	580
13.4.8	GOOSE.....	583
13.4.9	IEC 60870-5-104.....	588
13.4.10	KRUG.....	589
13.4.11	MMS.....	590
13.4.12	Modbus TCP.....	593
13.4.13	OPC DA (только L3/IP Layer).....	595
13.4.14	OPC UA.....	596
13.4.15	S7comm.....	598
13.4.16	S7comm Plus	602
13.4.17	UMAS.....	604
13.5	Просмотр журнала событий IDS/IPS	607
13.6	Настройка интерфейса для анализа зеркального трафика (SPAN) в COB 607	
14	Контроль приложений и доменов	609
14.1	Контроль приложений.....	609
14.2	Контроль доменов	617
15	Сервисы	620
15.1	DHCP.....	620

15.1.1	DHCP-сервер	620
15.1.2	DHCP-ретранслятор	620
15.2	Отслеживание соединений	623
15.2.1	Основные настройки	623
15.2.2	Мониторинг состояния	625
15.3	Учёт сетевого трафика	626
15.3.1	NetFlow	626
15.3.2	sFlow	631
15.4	Приоритизация трафика	632
15.4.1	Общие принципы работы	632
15.4.2	Создание политики обработки трафика	636
15.4.3	Применение политики	654
15.4.4	Примеры настройки политик	655
15.5	SNMP	657
15.5.1	SNMPv2c	658
15.5.2	SNMPv3	659
15.5.3	MIB-файлы	662
15.6	Stunnel	662
15.6.1	Общие настройки stunnel	663
15.6.2	Настройка серверного режима	664
15.6.3	Настройка клиентского режима	666
15.7	LLDP	669
15.7.1	Общие настройки LLDP	670
15.8	Interface State Sender	671
15.8.1	Общие настройки ISS	672
16	Прокси-сервер	675
16.1	Основные настройки прокси-сервера	675
16.2	URL-фильтрация	684
16.2.1	Настройки глобальных URL-фильтров	686
16.2.2	Настройка групп пользователей для URL-фильтрации	691
16.3	Кэширующий прокси-сервер	694
16.3.1	Настройка прокси-сервера	696
16.3.2	Обновление чёрного списка	696

16.3.3	Настройка ПК «Client»	696
16.3.4	Настройка политик блокировки	697
16.4	Прозрачный режим прокси-сервер.....	697
16.4.1	Настройка NAT для перенаправления HTTPS и HTTP трафика на прокси-сервер:.....	698
16.4.2	Настройка NAT для маскировки адресов локальной сети:.....	699
16.4.3	Настройка системного DNS-сервера:	699
16.4.4	Сгенерировать сертификат УЦ:.....	700
16.4.5	Настройки прокси-сервера:	701
16.4.6	Настройка ПК «Client»:.....	702
16.4.7	Проверка:.....	703
16.5	Технология единого входа	703
16.5.1	Аутентификация по протоколу Kerberos	704
16.5.2	Аутентификация пользователей по протоколу NTLMv2	706
16.5.3	Аутентификация пользователей LDAP	708
16.5.4	Настройки подмены сертификата TLS-Bump	710
16.6	Группы пользователей.....	712
16.7	Параметры ICAP-клиента.....	713
16.8	Прокси-сервер ActiveSync.....	713
17	Dr.Web	716
17.1	Лицензирование Dr.Web	716
17.2	Принципы работы Dr.Web	717
17.3	Включение Dr.Web.....	721
17.4	Конфигурация Dr.Web ICAPD	721
17.4.1	Общие настройки	722
17.4.2	Настройки блокировок	726
17.4.3	Белый список	729
17.4.4	Чёрный список	730
17.4.5	Список реклам.....	731
17.5	Правила проверки трафика Dr.Web ICAPD	732
17.5.1	Набор правил по умолчанию	733
17.5.2	Формат правил	734
17.5.3	Примеры правил проверки трафика и блокировки доступа	743

17.6	Обновление Dr.Web	743
17.6.1	Обновление Dr.Web через сеть Интернет.....	744
17.6.2	Ручное обновление Dr.Web без доступа к сети Интернет.....	747
17.6.3	Параметры конфигурации компонента обновления Dr.Web.....	748
17.7	Журналирование Dr.Web.....	749
18	Логирирование.....	752
18.1	Настройки глобального журнала.....	752
18.2	Просмотр глобального журнала.....	752
18.3	Экспорт журнала	759
18.3.1	Экспорт журнала в файл.....	759
18.3.2	Экспорт на удалённый сервер по протоколу Syslog (RFC3164).....	763
18.3.3	Экспорт в ARMA Management Console	771
18.3.4	Экспорт в терминал пользователя.....	776

ТЕРМИНЫ И СОКРАЩЕНИЯ

В настоящем руководстве использованы определения, представленные в таблице (см. [Таблица «Термины и сокращения»](#)).

Таблица «Термины и сокращения»

Термины и сокращения	Значение
ИБ	Информационная безопасность
МЭ	Межсетевой экран
ОЗУ	Оперативное запоминающее устройство
ОС	Операционная система
ПО	Программное обеспечение
СОВ	Система обнаружения вторжений
ЦП	Центральный процессор
ABR	Area Border Router – маршрутизатор, соединяющий одну или несколько областей OSPF, не являющихся магистральными, с магистральной областью
AD	Active Directory – службы каталогов, позволяющие использовать групповые политики для обеспечения единообразия настройки пользовательской рабочей среды
AFI	Address Family Identifier – идентификатор семейства адресов
ARMA Стена	InfoWatch ARMA Стена
ASN	Autonomous System Number – уникальный номер, позволяющий автономным системам обмениваться данными маршрутизации с другими подключёнными системами
BGP	Border Gateway Protocol – протокол граничного шлюза, используемый для построения динамической маршрутизации
CA	Certification Authority – центр сертификации
CIDR	Classless Inter-Domain Routing – бесклассовая междоменная маршрутизация
DBD	Database Descriptor – дескриптор базы данных
DHCP	Dynamic Host Configuration Protocol, протокол динамической настройки узла
FTP	File Transfer Protocol – протокол передачи файлов по сети

Термины и сокращения	Значение
HMAC	Hash-based Message Authentication Code, код проверки подлинности сообщений, использующий хеш-функции – механизм проверки целостности информации
HTTP	HyperText Transfer Protocol, протокол передачи гипертекста – протокол прикладного уровня передачи данных
HTTPS	HyperText Transfer Protocol Secure – расширение протокола HTTP для поддержки шифрования в целях повышения безопасности
IGP	Interior Gateway Protocol – тип протокола, используемый для обмена информацией о маршрутизации между маршрутизаторами в автономной системе
IP	Internet Protocol, межсетевой протокол – маршрутизируемый протокол сетевого уровня стека TCP/IP
LAN	Local Area Network – локальная вычислительная сеть
LDP	Label Distribution Protocol – протокол распределения меток
LSA	Link State Advertisement – пакеты, которыми обмениваются маршрутизаторы. В них содержится информация о состоянии маршрутизаторов и состоянии канала между ними
MD5	Message Digest 5 – 128-битный алгоритм хеширования, применяемый для проверки целостности информации и хранения хеш-суммы пароля
NAT	Network Address Translation, преобразование сетевых адресов – технология преобразования IP-адресов
NBMA	A non-broadcast multiple access network – сеть множественного доступа без широковещательной передачи
NSSA	Not So Stubby Area – не настолько тупиковая область, используется в классификации областей для маршрутизаторов OSPF
NTLMv2	NT LAN Manager – протокол сетевой аутентификации, встроенный в ОС Microsoft Windows
NTP	Network Time Protocol, протокол сетевого времени – сетевой протокол для синхронизации внутренних часов компьютера с использованием сетей с переменной латентностью
OSPF	Open Shortest Path First – протокол динамической маршрутизации, основанный на технологии отслеживания состояния канала

Термины и сокращения	Значение
PPPoE	Point-to-point protocol over Ethernet – сетевой протокол канального уровня передачи кадров PPP через Ethernet
QoS	Quality of Service, качество обслуживания – способность сети обеспечить необходимый сервис заданному трафику в определённых технологических рамках
Realm	Совокупность пользователей и серверов приложений, о которых имеет информацию Центр распределения ключей
RFC	Request for Comments, рабочее предложение – документ из серии пронумерованных информационных документов Интернета
SNMP	Simple Network Management Protocol, простой протокол сетевого управления – стандартный интернет-протокол для управления устройствами в IP-сетях на основе архитектур TCP/UDP
SPF	Shortest Path First – алгоритм для обнаружения Loop-Free путей в сети
SSH	Secure Shell, безопасная оболочка – сетевой протокол прикладного уровня, позволяющий производить удалённое управление операционной системой и туннелирование TCP-соединений
SSL	Secure Sockets Layer, уровень защищённых сокетов – криптографический протокол
STP	Spanning Tree Protocol, протокол основного дерева – канальный протокол, предназначенный для устранения петель в топологии сети Ethernet
SYN cookie	Техника противодействия SYN-флуд-атаке
TCP	Transmission Control Protocol, протокол управления передачей – один из основных протоколов передачи данных интернета
TLS	Transport layer security – протокол защиты транспортного уровня
USB	Universal Serial Bus – универсальная последовательная шина
UUCP	Unix-to-unix copy – команда копирования файлов между двумя компьютерами под управлением операционной системы UNIX, использующая одноимённый протокол
VLAN	Virtual Local Area Network – виртуальная локальная компьютерная сеть
VPN	Virtual Private Network, виртуальная частная сеть – обобщённое название технологий, позволяющих обеспечить одно или несколько сетевых соединений поверх другой сети

Термины и сокращения	Значение
VRRP	Virtual Router Redundancy Protocol, протокол резервирования виртуального маршрутизатора – сетевой протокол, предназначенный для увеличения доступности маршрутизаторов, выполняющих роль шлюза по умолчанию
WAN	Wide Area Network – глобальная вычислительная сеть
WireGuard	Коммуникационный протокол и бесплатное ПО с открытым исходным кодом, предназначенным для реализации зашифрованных виртуальных частных сетей

АННОТАЦИЯ

Настоящее руководство по настройке **ARMA Стена** в CLI предназначено для технических специалистов и пользователей, выполняющих конфигурирование и мониторинг работы **InfoWatch ARMA Стена v.4.8**.

Руководство по настройке **ARMA Стена** в CLI описывает принципы работы с **ARMA Стена**, доступные функции, их подробное описание, настройку и использование.

Пользователю **ARMA Стена** необходимо изучить настоящее руководство перед эксплуатацией.

1 ПОДГОТОВКА К РАБОТЕ

1.1 Установка

В настоящем разделе представлено описание установки и первоначальной настройки системы **ARMA Стена**.

1.1.1 Установка ПО ARMA Стена в ПАК

Для установки **ARMA Стена** в программно-аппаратный комплекс (ПАК) используется ISO-образ, который представляет собой файл, содержащий все необходимые данные для установки операционной системы в режиме реального времени. Установка **ARMA Стена** производится с USB-накопителя.

Для записи установочного образа «**ARMA Стена**» на USB-накопитель необходимо использовать специализированное программное обеспечение для записи образов на внешние накопители, такое как «Rufus» (<https://rufus-usb.ru.uptodown.com/windows>). Запись образа производится в соответствии с инструкцией по использованию данного программного обеспечения.

Для установки **ARMA Стена** необходимо выполнить следующие шаги:

1. Загрузить **ARMA Стена** в режиме «live».
2. Выполнить установку образа.

Примечание:

Для инсталляции системы необходимо использовать устройство хранения данных с минимальным объёмом 16 Гбайт. Носители с меньшим объёмом памяти не отображаются в перечне доступных дисков при выборе целевого носителя для установки.

Примечание:

После установки системы **ARMA Стена** весь транзитный трафик будет блокироваться.

1.1.1.1 Загрузка в режиме «live»

Для загрузки **ARMA Стена** в режиме «live» необходимо выполнить следующие действия:

1. Подключить подготовленный USB-накопитель с установочным образом в один из доступных USB-портов на аппаратной платформе. Аппаратная платформа во время подключения установочного USB-накопителя должна быть выключена.
2. Включить аппаратную платформу.
3. Выбрать в течение 10 секунд с помощью **клавиш клавиатуры со стрелками вверх и вниз**, в открывшемся меню варианты загрузки (см. [Рисунок – Варианты загрузки ОС](#)):

- «**Live system (amd64-ngfwos)**» – стандартная загрузка, выполняется по умолчанию;
- «**Live system (amd64-ngfwos fail-safe mode)**» – загрузка в безопасном режиме (Initramfs).

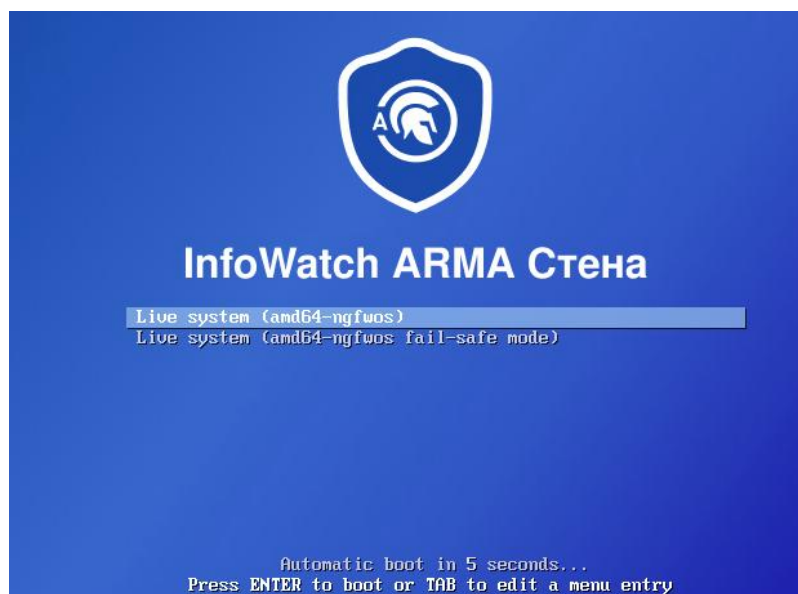


Рисунок – Варианты загрузки ОС

4. Нажать **клавишу «ENTER»** для подтверждения выбранного способа и начала загрузки.

Примечание:

Загрузка **ARMA Стена** в режиме «**live**» по умолчанию автоматически выполняется при следующих условиях:

- в случае бездействия пользователя в меню загрузки в течение 10 секунд;
- в случае неподтверждённого выбора способа загрузки и последующего бездействия пользователя в течение 5 минут.

5. При появлении приглашения на вход в консольном интерфейсе, указать следующие учётные данные, нажимая **клавишу «ENTER»** после каждого ввода:

- «**ngfwos login:**» – «admin»;
- «**Password:**» – «admin».

Примечание:

Пароль пользователя не отображается при наборе.

После успешной аутентификации будет отображён интерфейс командной строки в эксплуатационном режиме (см. [Рисунок – Интерфейс командной строки](#)).

```
admin@ngfwos:~$
```

Рисунок – Интерфейс командной строки

1.1.1.2 Установка образа

В качестве примера приведено описание установки образа **ARMA Стена** на один жёсткий диск, без деления на несколько разделов. Вводимые команды могут отличаться для каждой конкретной ситуации.

Для запуска процесса установки образа **ARMA Стена** необходимо выполнить следующие действия:

1. Ввести команду **«install image»**:

```
admin@ngfwos:~$ install image
```

и нажать **клавишу «ENTER»**.

В процессе установки системой будут выводиться запросы, в некоторых случаях содержащие предлагаемый ответ по умолчанию, заключённый в скобки.

При необходимости отмены выполнения команды, следует нажать комбинацию **клавиш «CTRL» + «C»**.

2. Подтвердить запуск процесса установки **ARMA Стена**. Ввести **«y»** и нажать **клавишу «ENTER»**:

```
This command will install NGFWOS to your permanent storage.  
Would you like to continue? [y/N]
```

3. Ввести имя образа и нажать **клавишу «ENTER»**:

```
What would you like to name this image? (Default: номер_релизной_версии_ПО)
```

4. Ввести новый пароль для УЗ «admin» и нажать **клавишу «ENTER»**:

```
Please enter a password for the "admin" user:
```

5. Ввести повторно пароль для УЗ «admin» и нажать **клавишу «ENTER»**:

```
Please confirm password for the "admin" user:
```

6. Если требуется создать API-ключ для доступа к веб-интерфейсу системы, следует ввести **«Y»** и нажать **«ENTER»**:

```
Would you like to set API key? [Y/n]
```

6.1. Ввести дополнительный новый пароль, который будет использоваться в качестве API-ключа для УЗ «admin», и нажать **клавишу «ENTER»**:

```
Please enter API key for the "admin" user:
```

6.2. Повторно ввести дополнительный пароль для УЗ «admin» и нажать **клавишу «ENTER»**:

Please confirm API key for the "admin" user:

Примечание:

В системе **ARMA Стена** пароли хранятся в зашифрованном виде.

7. Нажать **клавишу «ENTER»** на следующий запрос:

What console should be used by default? (K: KVM, S: Serial)? (Default: K)

8. Ввести имя раздела для установки и нажать **клавишу «ENTER»**:

Which one should be used for installation? (Default: /dev/sda)

Примечание:

В случае, если все накопительные устройства, доступные в системе, имеют объём памяти менее 16 Гбайт, процесс установки будет прекращен, и будет выведено следующее сообщение: *«No suitable disk was found. There must be at least one disk of 16 GB or greater size. Exiting from NGFWOS installation»*.

Примечание:

В случае, если в ПАК установлено два диска, система предложит настроить конфигурацию RAID-1. Для отказа от настройки RAID-1 необходимо ввести «n» и нажать **клавишу «ENTER»**:

Probing disks
2 disk(s) found
Would you like to configure RAID-1 mirroring? [Y/n]

При подтверждении конфигурации RAID-1 система выведет запрос на добавление перечисленных дисков в массив. Для объединения дисков в RAID-1 необходимо ввести «Y» и нажать **клавишу «ENTER»**:

The following disks were found:
/dev/sda (469.0 GB)
/dev/sda (469.0 GB)
Would you like to configure RAID-1 mirroring on them? [Y/n]

Примечание:

В случае выполнения установки с USB-накопителя, система определит его как второй жёсткий диск и предложит настроить конфигурацию RAID-1. Для корректного продолжения установки следует отказаться

от настройки RAID. Для этого необходимо ввести «**n**» и подтвердить действие нажатием **клавиши «ENTER»**.

Примечание:

При повторной установке системы **ARMA Стена**, если на устройстве ранее был сконфигурирован RAID-массив, установка должна выполняться исключительно на существующий RAID-массив. Попытка установки программного обеспечения на отдельный физический диск без использования ранее настроенного RAID-массива приведёт к невозможности последующей активации системы.

9. Ввести «**y**» и нажать **клавишу «ENTER»** для подтверждения удаления всех данных с устройства:

Installation will delete all data on the drive. Continue? [y/N]

Примечание:

Все данные на диске будут безвозвратно удалены.

10. Нажать **клавишу «ENTER»** на следующий запрос:

Would you like to use all the free space on the drive? [Y/n]

11. Программа предложит выбрать следующие доступные конфигурационные файлы для загрузки:

Creating partition table...
The following config files are available for boot:
1: Default live boot config
2: DHCP client on eth0, SSH
3: DHCP client on eth0, SSH, 192.168.1.1 on eth1, IPS minimal
Which file would you like as boot config? (Default: 2)

Система **ARMA Стена** автоматически устанавливает определённый набор настроек в зависимости от выбранного конфигурационного файла:

- **1 конфигурационный файл** – загружается базовая конфигурация с заводскими параметрами.
- **2 конфигурационный файл** (*используется по умолчанию*) – загружается базовая конфигурация с заводскими параметрами, дополненная следующими настройками:
 - включение доступа к системе по протоколу **SSH** на порту 22;

- настройка сетевого интерфейса **eth0** в режиме DHCP-клиента для автоматического получения IPv4-адреса.
- **3 конфигурационный файл** – загружается базовая конфигурация с заводскими параметрами, дополненная следующими компонентами:
 - включение доступа к системе по протоколу **SSH** на порту 22;
 - настройка сетевого интерфейса **eth0** в режиме DHCP-клиента для автоматического получения IPv4-адреса;
 - назначение статического IPv4-адреса **192.168.1.1/24** на сетевой интерфейс **eth1**;
 - активация встроенного DHCP-сервера на интерфейсе **eth1** с диапазоном выдаваемых адресов **192.168.1.100** до **192.168.1.254** (маска подсети – **/24**);
 - включение правил **Suricata** в режиме захвата трафика **IPS** на интерфейсе **eth0** со следующими параметрами:
 - набор правил:
/config/files/configuration/suricata/rule-files/.rules*;
 - политика обработки пакетов, захваченных в середине потока (midstream-policy): *ignore*;
 - количество потоков обработки трафика через netmap: *auto*;
 - отключение проверки контрольных сумм:
checksum-checks «no».

Примечание:

Для корректной работы **конфигурационного файла 3** устройство должно иметь как минимум два активных физических сетевых интерфейса. Отсутствие второго интерфейса приведёт к переходу системы в **аварийный режим** после перезагрузки.

Ввести номер конфигурационного файла и нажать **клавишу «ENTER»**.

12. После завершения процесса установки образа, системой будет выведено сообщение о необходимости выполнить перезагрузку **ARMA Стена**. Извлечь USB-носитель с установочным образом и в командной строке ввести команду **«reboot»**:

```
The image installed successfully; please reboot now.  
admin@ngfwos:~$ reboot
```

Подтвердить перезагрузку системы, введя **«y»** и нажав **клавишу «ENTER»**:

Are you sure you want to reboot this system? [y/N] y

После перезагрузки **ARMA Стена** будет отображено приглашение авторизации в локальном консольном интерфейсе:

Welcome to NGFWOS – ngfwos tty1

ngfwos login:

Для входа в локальный консольный интерфейс необходимо указать учётные данные, нажимая **клавишу «ENTER»** после каждого ввода:

- **«ngfwos login:»** – «admin»;
- **«Password:»** – пароль, заданный на этапе установки образа **ARMA Стена** (пункт 4).

При первоначальной загрузке необходимо произвести активацию лицензии **ARMA Стена**. Процесс активации лицензии подробно описан в разделе [«Управление лицензией»](#) настоящего руководства.

Настройка системы производится в режиме конфигурирования. Подробное описание работы в режиме конфигурирования представлено в разделе [«Конфигурационный режим»](#) настоящего руководства.

1.1.2 Настройка интерфейсов

Примечание:

По умолчанию в системе ARMA Стена разрешён весь входящий и исходящий трафик. Транзитный трафик по умолчанию блокируется.

Рекомендуется установить строгую политику фильтрации трафика путём явного запрета всего входящего и исходящего трафика на уровне межсетевого экрана (см. раздел [«Межсетевой экран»](#)).

Просмотреть конфигурацию сетевых интерфейсов возможно с помощью команды **«show interfaces»**:

- результат выполнения команды «show interfaces» в эксплуатационном режиме:

```
admin@ngfwos:~$ show interfaces
```

Codes: S - State, L - Link, u - Up, D - Down, A - Admin Down

Interface	IP Address	MAC	VRF	MTU	S/L
eth0	192.168.10.35/24	00:45:56:bd:0d:ec	default	1500	u/u
eth1	-	00:45:56:bd:7a:57	default	1500	u/u
lo	127.0.0.1/8 ::1/128	00:00:00:00:00:00	default	65536	u/u

- результат выполнения команды «show interfaces» в конфигурационном режиме:

```
admin@ngfwos:~$ configure
[edit]
admin@ngfwos# show interfaces
Must specify config path
ethernet eth0 {
    address dhcp
    hw-id 00:45:56:bd:0d:ec
}
ethernet eth1 {
    hw-id 00:45:56:bd:7a:57
}
loopback lo {
}
[edit]
admin@ngfwos#
```

Физическим интерфейсам по умолчанию назначается имя «**ethN**», где «**N**» – идентификатор, присвоенный интерфейсу системой.

Для назначения статического IP-адреса на сетевой интерфейс необходимо ввести следующую команду в конфигурационном режиме:

```
# Перейти в конфигурационный режим командой configure | conf:
admin@ngfwos:~$ configure

# Назначить статический IP-адрес интерфейсу ethN:
admin@ngfwos# set interfaces ethernet <ethN> address <адрес>

# Применить настройки к текущей конфигурации:
admin@ngfwos# commit

# Сохранить новую конфигурацию:
admin@ngfwos# save

# Выйти из конфигурационного режима:
admin@ngfwos# exit
exit
admin@ngfwos:~$
```

где:

- **<ethN>** – имя интерфейса, например eth0;
- **<адрес>** – IP-адрес в формате x.x.x.x/x (IPv4) или h:h:h:h:h:h:h/x (IPv6).

Для настройки получения IP-адреса по протоколу «DHCP» необходимо ввести следующую команду в конфигурационном режиме:

```
admin@ngfwos# set interfaces ethernet ethN address dhcp
admin@ngfwos# commit
admin@ngfwos# save
```

На одном сетевом интерфейсе допускается настройка нескольких IP-адресов. Для этого необходимо последовательно выполнить команду «set interfaces ethernet <ethN> address <адрес>» для каждого требуемого адреса.

Для добавления текстового описания к интерфейсу используется команда:

```
admin@ngfwos# set interfaces ethernet ethN description <описание>
admin@ngfwos# commit
admin@ngfwos# save
```

где **<описание>** – краткое текстовое описание. Допускается использование символов кириллического и латинского алфавитов. Описание не должно начинаться с последовательности «//». Запрещено использование символов «"», «'» и перенос строки. Максимальная длина значения – «127» символов. При наличии пробелов значение поля должно быть заключено в двойные кавычки.

Полный перечень параметров и синтаксис команд для настройки сетевых интерфейсов приведён в разделе «[Интерфейсы](#)» настоящего руководства.

Примечание:

Некорректная конфигурация сетевых интерфейсов может привести к потере сетевого доступа к устройству ARMA Стена.

1.1.3 Настройка часового пояса

Настройка часового пояса обязательна, поскольку все временные метки в глобальном журнале формируются с учётом указанной временной зоны. Отсутствие корректной конфигурации затрудняет сопоставление логов между различными системами.

Команда установки часового пояса в системе **ARMA Стена**:

```
# Перейти в конфигурационный режим:
admin@ngfwos:~$ configure
[edit]

# Установить необходимый часовой пояс:
admin@ngfwos# set system time-zone <timezone>

# Применить настройки к текущей конфигурации:
admin@ngfwos# commit

# Сохранить новую конфигурацию:
admin@ngfwos# save

# Выйти из конфигурационного режима:
admin@ngfwos# exit
exit
admin@ngfwos:~$
```

где **<timezone>** - значение часового пояса. Задаётся в формате **Region/Location**, соответствующем географическому положению устройства. Пример: «*set system time-zone Europe/Moscow*» - устанавливает московский часовой пояс (UTC+3).

Примечание:

По умолчанию используется UTC.

Список значений часовых поясов России:

- **Europe/Kaliningrad** – Калининградское время (UTC+2);

- **Europe/Moscow** – Московское время (UTC+3);
- **Europe/Volgograd** – Волгоградское время (UTC+3);
- **Europe/Kirov** – Время Кирова (UTC+3);
- **Europe/Volgograd** – Волгоградское время (UTC+3);
- **Europe/Simferopol** – Крым (Симферополь) – (UTC+3);
- **Europe/Astrakhan** – Астраханское время (UTC+4);
- **Europe/Ulyanovsk** – Ульяновское время (UTC+4);
- **Europe/Samara** – Самарское время (UTC+4);
- **Europe/Saratov** – Саратовское время (UTC+4);
- **Asia/Yekaterinburg** – Екатеринбургское время (UTC+5);
- **Asia/Omsk** – Омское время (UTC+6);
- **Asia/Novosibirsk** – Новосибирское время (UTC+7);
- **Asia/Barnaul** – Барнаульское время (UTC+7);
- **Asia/Tomsk** – Томское время (UTC+7);
- **Asia/Novokuznetsk** – Новокузнецкое время (UTC+7);
- **Asia/Krasnoyarsk** – Красноярское время (UTC+7);
- **Asia/Irkutsk** – Иркутское время (UTC+8);
- **Asia/Chita** – Забайкальский край (Чита) (UTC+9);
- **Asia/Yakutsk** – Якутское время (UTC+9);
- **Asia/Vladivostok** – Владивостокское время (UTC+10);
- **Asia/Magadan** – Магаданское время (UTC+11);
- **Asia/Sakhalin** – Сахалин (UTC+11);
- **Asia/Srednekolymsk** – Среднеколымское время (UTC+11);
- **Asia/Kamchatka** – Камчатское время (UTC+12);
- **Asia/Anadyr** – Анадырское время (UTC+12).

Для получения списка поддерживаемых временных зон использовать автодополнение командной строки после ввода «**set system time-zone**» + **TAB**. Учёт перехода на летнее время выполняется автоматически на основе календарных правил для выбранной зоны.

1.1.4 Ручная настройка даты и времени

Для ручной установки текущих даты и времени в эксплуатационном режиме следует выполнить команду:

```
admin@ngfwos:~$ set date <time_and_date>
```

где **<time_and_date>** – значение даты и времени, подлежащее установке. Поддерживаются следующие форматы:

- **<MMDDhhmm>** - где **<MM>** – месяц (01-12), **<DD>** – день месяца (01-31), **<hh>** – часы (00-23), **<mm>** – минуты (00-59);
- **<MMDDhhmmYY>** – дополнительно указывается двузначный год (например, «25» для 2025 года);
- **<MMDDhhmmCCYY>** – дополнительно указывается полный год, где «CC» обозначает век, а «YY» – год в столетии (например, «2025»);
- **<MMDDhhmmYY.ss>** – дополнительно указываются секунды «ss» (00-59).

Для обеспечения точности и согласованности временных параметров в распределённых системах рекомендуется осуществлять синхронизацию времени с использованием протокола **NTP (Network Time Protocol)**. Дополнительная информация о настройке и конфигурации **NTP** представлена в разделе «[Служба NTP](#)».

Для отображения текущих значений даты и времени в эксплуатационном режиме используется команда:

```
admin@ngfwos:~$ show date
```

1.2 Способы управления

Управление и настройка системы **ARMA Стена** осуществляется следующими способами:

- **Локальный доступ** – реализуется через стандартную или последовательную консоль (RS-232). Данный метод предоставляет доступ только к командному интерпретатору (CLI).
- **Удалённый доступ** – по протоколу SSH с использованием SSH-клиента (например PuTTY). Обеспечивает доступ к командному интерфейсу CLI.
- **Доступ через ПО ARMA MC** – часть конфигурационных операций может быть выполнена с использованием программного обеспечения **ARMA Management Console (MC)**, которая предоставляет доступ к веб-интерфейсу системы **ARMA Стена**.

1.2.1 Последовательная консоль

При подключении через консольный порт (RS-232) используются следующие параметры:

- скорость: 115200 бит/с;

- без контроля чётности (No parity);
- 8 бит данных (8 data bits);
- 1 стоповый бит (1 stop bits).

Примечание:

При использовании USB-переходников, в которых, как правило, применяется программная эмуляция последовательного порта без аппаратного управления потоком, рекомендуется устанавливать скорость передачи данных на уровне **9600 бит/с**.

Команды конфигурации последовательной консоли:

1. Определить устройство, используемое в качестве последовательной консоли:

```
admin@ngfwos:~$ conf
[edit]
admin@ngfwos# set system console device <устройство>
admin@ngfwos# commit
admin@ngfwos# save
```

Поддерживаемые типы устройств:

- **ttySN** – последовательный порт (например, ttyS0);
- **ttyUSBX** – USB-адаптер последовательного порта (например, ttyUSB0);
- **hvc0** – консоль Xen (виртуальная машина).

2. Установить скорость передачи данных:

```
admin@ngfwos:~$ conf
[edit]
admin@ngfwos# set system console device <устройство> speed <скорость>
admin@ngfwos# commit
admin@ngfwos# save
```

Допустимые значения скорости:

- **1200**;
- **2400**;
- **4800**;
- **9600**;
- **19200**;
- **38400** - по умолчанию для Xen-консоли;

- **57600**;
- **115200** - по умолчанию для последовательного порта.

1.2.2 SSH подключение

Сервер SSH обеспечивает безопасный удалённый доступ к управлению функциями локального консольного интерфейса **ARMA Стена**.

Для осуществления удалённого подключения рекомендуется использовать любой SSH-клиент, поддерживающий аутентификацию с использованием пароля.

Для включения SSH необходимо выполнить следующую команду в конфигурационном режиме:

```
admin@ngfwos:~$ conf
[edit]
admin@ngfwos# set service ssh port 22
admin@ngfwos# commit
admin@ngfwos# save
```

где «**22**» – назначаемый порт. Возможно указать значение порта в диапазоне от «1» до «65535».

Для указания IP-адреса, прослушиваемого сервисом «SSH», необходимо ввести команду:

```
admin@ngfwos:~$ conf
[edit]
admin@ngfwos# set service ssh listen-address 192.168.2.11
admin@ngfwos# commit
admin@ngfwos# save
```

где «**192.168.2.11**» – IP-адрес прослушивания сервисом «SSH», приведён в качестве примера. Возможно указать IP-адрес в формате IPv4 или IPv6.

Для указания алгоритма шифрования необходимо выполнить команду:

```
admin@ngfwos:~$ conf
[edit]
admin@ngfwos# set service ssh ciphers aes128-ctr
admin@ngfwos# commit
admin@ngfwos# save
```

где «**aes128-ctr**» – алгоритм шифрования, приведён в качестве примера.

Поддерживаются следующие алгоритмы шифрования:

- **3des-cbc**;
- **aes128-cbc**;

- **aes128-ctr;**
- **aes128-gcm@openssh.com;**
- **aes192-cbc;**
- **aes192-ctr;**
- **aes256-cbc;**
- **aes256-ctr;**
- **aes256-gcm@openssh.com;**
- **chacha20-poly1305@openssh.com;**
- **rijndael-cbc@lysator.liu.se.**

Примечание:

Всем пользовательским учётные записи, кроме «**admin**», закрыт доступ по протоколам SCP и SFTP. Доступ **УЗ** «**admin**» к домашним каталогам других пользователей запрещён.

Для указания разрешённого алгоритма подписи открытого ключа необходимо выполнить команду:

```
admin@ngfwos:~$ conf
[edit]
admin@ngfwos# set service ssh pubkey-accepted-algorithm <algorithm>
admin@ngfwos# commit
admin@ngfwos# save
```

где **<algorithm>** – имя разрешённого алгоритма подписи.

Поддерживаются следующие алгоритмы:

- **ecdsa-sha2-nistp256;**
- **ecdsa-sha2-nistp256-cert-v01@openssh.com;**
- **ecdsa-sha2-nistp384;**
- **ecdsa-sha2-nistp384-cert-v01@openssh.com;**
- **ecdsa-sha2-nistp521;**
- **ecdsa-sha2-nistp521-cert-v01@openssh.com;**
- **rsa-sha2-256;**
- **rsa-sha2-256-cert-v01@openssh.com;**
- **rsa-sha2-512;**
- **rsa-sha2-512-cert-v01@openssh.com;**

- **sk-ecdsa-sha2-nistp256-cert-v01@openssh.com;**
- **sk-ecdsa-sha2-nistp256@openssh.com;**
- **sk-ssh-ed25519-cert-v01@openssh.com;**
- **sk-ssh-ed25519@openssh.com;**
- **ssh-dss;**
- **ssh-dss-cert-v01@openssh.com;**
- **ssh-ed25519;**
- **ssh-ed25519-cert-v01@openssh.com;**
- **ssh-rsa;**
- **ssh-rsa-cert-v01@openssh.com;**
- **webauthn-sk-ecdsa-sha2-nistp256@openssh.com.**

Для перезапуска службы SSH необходимо в эксплуатационном режиме ввести следующую команду:

```
admin@ngfwos:~$ restart ssh
```

1.2.3 Веб-интерфейс

ARMA Стена поставляется с базовым интерфейсом командной строки (CLI), обеспечивающим полный доступ к настройкам системы. Для удобства настройки и контроля работы системы **ARMA Стена** предусмотрена интеграция с ПО **ARMA Management Console** начиная с версии **1.8**, которая предоставляет доступ к графическому интерфейсу пользователя (GUI) системы **ARMA Стена**.

Для обеспечения взаимодействия между **ARMA MC** и устройством **ARMA Стена** требуется выполнить активацию системы (см. [Управление лицензией](#)) и установить API-ключ для HTTP-запросов.

Для создания и установки API-ключа необходимо ввести следующую команду в конфигурационном режиме:

```
admin@ngfwos# set service https api keys user <УЗ> key <key>
```

где:

- **<УЗ>** - имя локальной учётной записи в системе **ARMA Стена**;
- **<key>** - пользовательский пароль (API-ключ) для локальной учётной записи **<УЗ>**. Данные параметры будут использоваться для взаимодействия с **MC**.

Примечание:

При использовании API-ключа, ассоциированного с учётной записью, имеющей ограниченные привилегии в системе **ARMA Стена** (см. раздел «[Временная блокировка учётных записей](#)» настоящего руководства), уровень доступа к функциональным возможностям веб-интерфейса **ARMA Стена** в составе **ARMA MC** определяется набором разрешений, назначенных данной учётной записи.

Если учётная запись не обладает достаточными правами для доступа к определённому разделу или операции в веб-интерфейсе **ARMA Стена**, то поведение системы будет зависеть от версии **ARMA MC**:

в **ARMA MC** версии **2.0 и выше** – в левом нижнем углу интерфейса отображается уведомление о запрете доступа;

в **ARMA MC** версии **1.8 и ниже** – при попытке выполнить операцию, требующую недостающих прав, возвращается сообщение об ошибке: «Request failed with status code 500».

Доступ к веб-интерфейсу **ARMA Стена** через **ARMA MC** **запрещён** для учётных записей, которым не назначен класс доступа или которые принадлежат к классу, не включающему разрешённые команды. В таких случаях система блокирует подключение и отображает соответствующее сообщение о недостатке прав.

Примечание:

Рекомендуется использовать API-ключ, привязанный к учётной записи из класса «**NGFW_Administrators**». Задать API-ключ для учётной записи можно с помощью выполнения команды «set service https api keys user <user> <API-key>». По умолчанию задание API-ключей доступно только пользователям с правами «**NGFW_Administrators**» и «**NGFW_Super_Administrators**».

Применить настройки командой **commit**:

```
admin@ngfwos# commit
```

```
WARNING: No certificate specified, using build-in self-signed  
certificates. Do not use them in a production environment!
```

```
[ service https ]
```

```
WARNING: No certificate specified, using build-in self-signed  
certificates. Do not use them in a production environment!
```

Сохранить конфигурацию командой **save**:

```
admin@ngfwos# save
```

Для подключения **ARMA Стена** к **МС** необходимо выполнить следующие шаги:

1. Авторизоваться в веб-интерфейсе **МС**.
2. Выбрать раздел меню «**Администрирование**», затем – подраздел «**Источники**» (см. [Рисунок – Источники](#)).

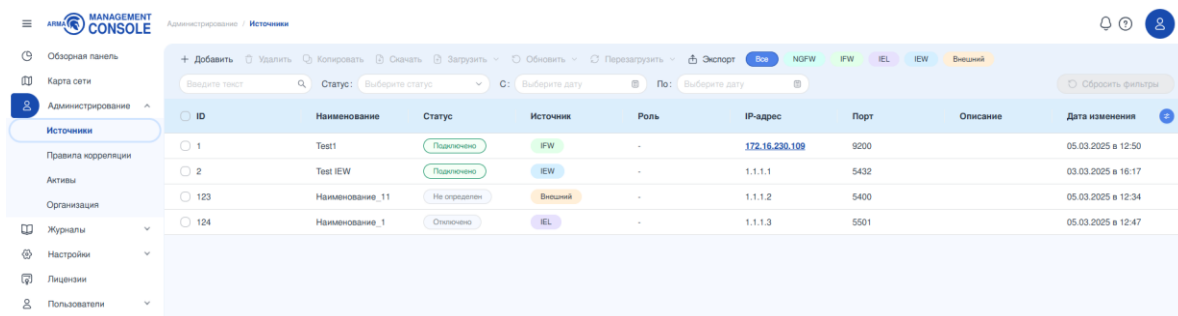


Рисунок – Источники

3. В панели инструментов нажать кнопку «+ **Добавить**».
4. В открывшейся карточке «**Добавление источника**» выбрать тип источника «**NGFW**» и указать значения следующих параметров (см. [Рисунок – Добавление нового источника событий «NGFW»](#)):

- «**Наименование**» – отображаемое в **МС** имя устройства. Параметр может содержать только латинские и кириллические буквы, пробел, спецсимволы («.», «_», «-») и не может превышать 128 символов;
- «**IP-адрес**» – IP-адрес подключаемой **ARMA Стена**;
- «**Логин пользователя**» – ввести имя учётной записи (<УЗ>), используемой для создания API-ключа в системе **ARMA Стена**;
- «**API-Ключ**» – ввести пароль (<key>), указанный при создании API-ключа для учётной записи (<УЗ>) в **ARMA Стена**;
- «**Порт**» – значение порта входящих логов. Указываются порты в диапазоне от «**1500**» до «**65535**». Значение должно быть уникальным, не заданным ранее в источниках **МС**.

При необходимости заполнить поле «**Описание**» дополнительной информацией об устройстве. Поле может содержать не более 250 символов.

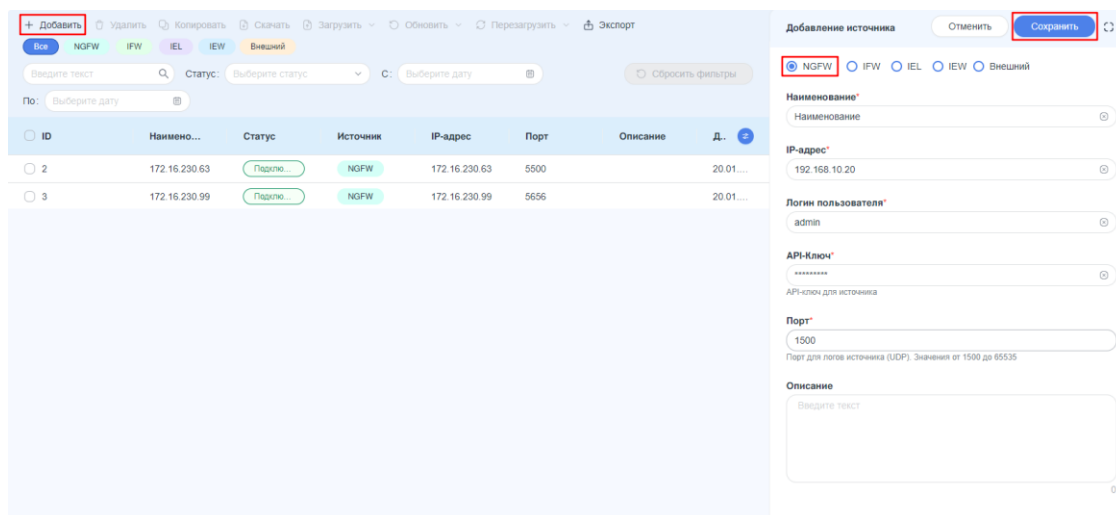


Рисунок – Добавление нового источника событий «NGFW»

После сохранения настроек в столбе «**Статус**» таблицы «**Источники**» отобразится значение «**Подключено**». При указании неверных учётных данных **ARMA MC** отобразит статус «**Не авторизован**». Статус «**Ошибка**» отображается, если произошла ошибка, которая может быть связана с аппаратным или программным обеспечением источника «NGFW», а также при использовании данных несуществующей локальной учётной записи в **ARMA Стена**.

1.3 Управление лицензией

В настоящем разделе представлено описание лицензирования продукта, предусматривающего механизм управления лицензией, который позволяет:

- активировать новую лицензию:
 - автоматическим способом;
 - ручным способом.
- просматривать информацию о действующей лицензии.

Примечание:

Управление лицензией доступно только пользователям, у которых имеются права на использование команды **license**. (см. [Назначение прав доступа пользовательским учётным записям](#)).

1.3.1 Активация системы ARMA Стена

Активация – это процедура введения в действие лицензии, дающей право на использование полнофункциональной версии системы **ARMA Стена** в течение срока действия лицензии.

При первоначальной загрузке системы **ARMA Стена** необходимо произвести активацию лицензии. Активация лицензии осуществляется двумя сценариями:

- автоматическая активация через интернет;

- ручная активация без подключения к сети Интернет.

Примечание:

Лицензионный ключ предоставляется согласно условиям в договоре поставки.

В системе **ARMA Стена** в неактивированном состоянии пользователю доступны только следующие действия: настроить сеть, настроить сервис SSH, настроить системный DNS, создать ключи HTTP API и активировать лицензию.

Перечень команд, доступных в системе с неактивированной лицензией (см. [Таблица «Команды, разрешённые при неактивированной лицензии»](#)).

Таблица «Команды, разрешённые при неактивированной лицензии»

Режим работы	Команда	Краткое описание
Эксплуатационный	configure	Войти в конфигурационный режим
Эксплуатационный	license	Лицензирование продукта NGFW
Эксплуатационный	install	Установить новую систему
Эксплуатационный	show	Показать системную информацию
Эксплуатационный	ping	Отправить запрос эха ICMP
Эксплуатационный	reboot	Перезагрузить систему
Эксплуатационный	poweroff	Выключить систему
Эксплуатационный	traceroute	Отслеживание сетевого пути к узлу
Эксплуатационный	telnet	Telnet к узлу
Эксплуатационный	third-party	Управление внешними компонентами
Эксплуатационный	exit	Выход из системы
Конфигурационный	comment	Добавьте комментарий к этому элементу конфигурации
Конфигурационный	commit	Зафиксировать текущий набор изменений
Конфигурационный	commit-check	Проверка синтаксической и логической корректности введенных команд без их применения
Конфигурационный	commit-confirm	Зафиксировать текущий набор изменений с обязательным «подтверждением»
Конфигурационный	save	Сохранить активную конфигурацию в файл config.boot
Конфигурационный	confirm	Подтвердить набор изменений

Режим работы	Команда	Краткое описание
Конфигурационный	compare	Сравнение изменений конфигурации
Конфигурационный	copy	Копирование элемента конфигурации
Конфигурационный	discard	Отменить незафиксированные изменения
Конфигурационный	edit	Редактирование вложенного элемента
Конфигурационный	run	Выполнение команд эксплуатационного режима
Конфигурационный	exit	Выход из конфигурационного режима
Конфигурационный	set service https api keys user	Команда установки ключа для http-запросов
Конфигурационный	delete service https api keys user	Команда удаления ключа для http-запросов
Конфигурационный	set interfaces ethernet	Команда настройки сетевых интерфейсов
Конфигурационный	delete interfaces ethernet	Команда удаления настроек сетевых интерфейсов
Конфигурационный	set service ssh	Команда настройки сервиса ssh
Конфигурационный	delete service ssh	Команда удаления настроек сервиса ssh
Конфигурационный	set system name- server	Команда настройки системного DNS
Конфигурационный	delete system name- server	Команда удаления настроек системного DNS
Конфигурационный	set protocols static route	Команда настройки шлюза по умолчанию для IPv4
Конфигурационный	delete protocols static route	Команда удаления настроек шлюза по умолчанию для IPv4

Режим работы	Команда	Краткое описание
Конфигурационный	set protocols static route6	Команда настройки шлюза по умолчанию для IPv6
Конфигурационный	delete protocols static route6	Команда удаления настроек шлюза по умолчанию для IPv6
Конфигурационный	show	Показать конфигурацию

В случае удаления файла лицензии из активированной системы, **ARMA Стена** заблокирует выполнение команд, которые не входят в перечень разрешённых при неактивированном состоянии (см. [Таблица «Команды разрешенные при неактивированной лицензии»](#)). При этом настройки системы останутся неизменными, и она продолжит функционировать, однако возможность внесения изменений будет недоступна. При попытке выполнить неразрешённую команду, будет выведено сообщение об ошибке следующего содержания: **«Invalid command: [введенная команда]»**.

Для возобновления доступа пользователю потребуется повторно активировать систему или восстановить файл лицензии в каталоге **«/config/»** из сохранённой копии, если таковая имеется.

При замене оборудования повторное приобретение лицензии не требуется.

1.3.1.1 Автоматическая активация лицензии

Для автоматической активации лицензии необходимо выполнить следующие действия:

1. Настроить сетевой интерфейс для подключения к сети Интернет (см. [Настройка интерфейсов](#)).
2. В эксплуатационном режиме ввести команду:

```
admin@ngfwos:~$ license activate <serial>
```

где **<serial>** - уникальный лицензионный ключ в допустимом формате.

Примечание:

При наличии активной лицензии система выведет предупреждение о том, что успешная активация новой лицензии приведёт к перезаписи текущей: **«Successful activation of a new license will overwrite your current license, are you sure you want to proceed ? [Y/n]»**. Для

подтверждения замены необходимо ввести «**y**» и нажать **клавишу «Enter»**. Для отмены операции, ввести «**n**».

- При успешной активации лицензии отобразится сообщение:

Activation response: license activated, Status: ok
License activation is complete.

В случае ввода недопустимого или некорректного лицензионного ключа система вернёт ошибку:

activation response: bad serial number format , status: error

- Для завершения процесса активации и применения лицензии требуется повторная аутентификация в системе. При появлении запроса:

You are able to edit configuration of the system right now. Operational-mode commands will be available after relogin
Do you want to relogin right now ? [Y/n]

ввести «**y**» для подтверждения выхода и повторного входа или «**n**» – для отмены.

Если выход из системы и повторная аутентификация не выполнены, функциональные возможности эксплуатационного режима остаются ограниченными в соответствии с состоянием до активации лицензии. Команды конфигурационного режима доступны в полном объёме без необходимости выхода из системы.

- По завершении повторного входа активируется полный функционал системы.

1.3.1.2 Ручная активация лицензии

Для ручной активации лицензии необходимо выполнить следующие действия (см. [Рисунок – Ручная активация лицензии](#)):



Рисунок – Ручная активация лицензии

- В эксплуатационном режиме ввести команду:

```
admin@ngfwos:~$ license get-token <serial>
```

где **<serial>** - лицензионный ключ.

- Система сгенерирует токен и выведет его в консоль:

```
=====BEGIN=====
rXoj/XXXXksAqF6KOKsQ7tt9Rgv9LTjzlliGZ6wc
slQAAAAbMjAyNS0wMS0yMlXXXXo0NjowMy44NDY0NTTha
=====END=====
```

- Полученный токен необходимо передать в техподдержку ООО «**ИнфоВотч АРМА**».
- Специалист **InfoWatch** предоставит файл лицензии в формате **bin**, который необходимо загрузить в систему **ARMA Стена** в каталог «**/config/**».

Для выполнения данной операции возможно использовать программное обеспечение, поддерживающее передачу файлов по протоколам SFTP или SCP (например, WinSCP для операционной системы Windows), либо воспользоваться командой «scp» через интерфейс командной строки. Возможны также альтернативные способы передачи данных.

Пример использования команды «scp»:

```
C:\Users\test> scp c:\Users\test\Desktop\license.bin
admin@172.16.20.76:/config>
```

Команда выполнит копирование файл лицензии «license.bin» в каталог «**/config/**» на системе **ARMA Стена**, доступной по IP-адресу 172.16.20.76.

- После генерации токена система выводит уведомление о необходимости размещения файла лицензии в каталоге «**/config/**» и переходит в режим ожидания:

```
Please place received 'license.bin' file in /config/license.bin
Please press enter when the license files is placed.
```

Нажатие **клавиши «Enter»** инициирует проверку наличия файла «**/config/license.bin**»:

- При обнаружении файла лицензии система начинает процесс активации.
- При отсутствии файла выводится сообщение:

```
Did not found file. Please place license file to /config/license.bin and
press Enter.
```

Повторное нажатие **клавиши «Enter»** приводит к повторной проверке наличия файла.

Для выхода из режима ожидания и возврата в командную строку необходимо нажать сочетание **клавиш «Ctrl+C»**.

6. После размещения файла **license.bin** в каталоге **/config/** необходимо выполнить активацию лицензии командой:

```
admin@ngfwos:~$ license activate-offline
```

7. Для завершения процесса активации и применения лицензии требуется повторная аутентификация в системе. При появлении запроса:

```
You are able to edit configuration of the system right now. Operational-mode  
commands will be available after relogin  
Do you want to relogin right now ? [Y/n]
```

ввести **«y»** для подтверждения выхода и повторного входа или **«n»** – для отмены.

Если выход из системы и повторная аутентификация не выполнены, функциональные возможности эксплуатационного режима остаются ограниченными в соответствии с состоянием до активации лицензии. Команды конфигурационного режима доступны в полном объёме без необходимости выхода из системы.

8. По завершении повторного входа активируется полный функционал системы.

1.3.1.3 Повторная активация лицензии

Повторная активация **ARMA Стена** может потребоваться в следующих случаях:

- После обновления программного обеспечения **«ARMA Стена»** (с версии 4.6 и ниже).
- При истечении срока действия текущей лицензии.
- При замене аппаратной платформы или проблемах лицензионного файла.

Процесс повторной активации лицензии **ARMA Стена** в **автоматическом режиме** полностью аналогичен процессу первичной автоматической активации (см. [Автоматическая активация лицензии](#)).

Для повторной **ручной активации лицензии** необходимо выполнить следующие действия:

1. В эксплуатационном режиме ввести команду для удаления старого файла лицензии:

```
admin@ngfwos:~$ delete file /config/license.bin
```

После нажатия **клавиши «Enter»** система запросит подтверждение для удаления файла:

```
Do you want to erase the running:///config/license.bin file? (Y/N):
```

Необходимо ввести «**y**» для подтверждения удаления файла лицензии или «**n**» – для отмены. После ввода «**y**» и удаления файла система выдаст подтверждение вида:

```
File erased
```

2. Выполнить все действия, начиная с генерации нового токена (пункт 1 предыдущего раздела):

```
admin@ngfwos:~$ license get-token <serial>
```

Все остальные этапы повторной активации полностью идентичны процедуре первичной ручной активации (см. [Ручная активация лицензии](#)).

1.3.2 Информация о текущей лицензии

Для просмотра статуса лицензии необходимо в эксплуатационном режиме ввести команду «**show version**»:

```
admin@ngfwos:~$ show version
```

```
Version:          NGFWOS 4.5
```

```
Built by:         IW ARMA CICD
```

```
Built on:         Mon 24 Jan 2025 08:30 UTC
```

```
Build UUID:       xx64xx7e-0a33-xxxx-axxd-f2ea8fcxxx8b
```

```
Build commit ID:  xxc33ed1xxxxxx-dirty
```

```
Architecture:     x86_64
```

```
Boot via:         installed image
```

```
System type:      KVM guest
```

```
Hardware vendor:  QEMU
```

```
Hardware model:   Standard PC (Q35 + ICH9, 2009)
```

```
Hardware S/N:     
```

```
Hardware UUID:    xxx30bcb-xxxx-xxxx-xxxx-xxxx1d5d3dcf
```

```
license start:    2025-01-24T16:09:02.858887Z
```

```
license end:      2025-02-24T16:09:02.861340Z
```

Для ознакомления с пользовательским лицензионным соглашением необходимо ввести команду «**show license**» в эксплуатационном режиме.

2 ИНТЕРФЕЙС КОМАНДНОЙ СТРОКИ

Доступ к интерфейсу командной строки системы **ARMA Стена** возможно получить при подключении к устройству:

- через стандартную консоль, с использованием подключения по HDMI или VGA с подключением клавиатуры;
- через последовательную консоль (RS-232) (см. раздел «[Последовательная консоль](#)»);
- по защищённому сетевому каналу с использованием протокола SSH (см. раздел «[SSH подключение](#)»).

Работа с интерфейсом командной строки

Интерфейс командной строки (CLI) предоставляет возможность получения справочной информации по всем поддерживаемым командам путём ввода символа «?».

Для автоматического дополнения вводимых команд и параметров применяется клавиша **Tab**. При частичном вводе команды и нажатии **Tab** система предлагает возможные варианты завершения. Например, при наборе в командной строке значения «sh» и последующем нажатии клавиши **TAB**, система предложит подходящий вариант – команду «show». Повторное нажатие клавиши **TAB** отобразит список всех доступных дополнительных команд и параметров, связанных с текущим контекстом выполнения команды «show»:

```
admin@ngfwos:~$ s[pressTAB]
set      show      suricata
```

```
admin@ngfwos:~$ show [tab]
```

Possible completions:

app-control	Show available categories and applications for application control
arp	Show Address Resolution Protocol (ARP) information
babel	Show Babel routing protocol information
bfd	Show Bidirectional Forwarding Detection (BFD)
bgp	BGP information
bridge	Show bridging information
configuration	Show available saved configurations
conntrack	Show conntrack tables entries
conntrack-sync	Show connection tracking synchronization information
console-server	Show Console-Server information
container	Show containers
date	Show system time and date
dhcp	Show DHCP (Dynamic Host Configuration Protocol) information
...	

Прокрутка содержимого в терминале осуществляется с помощью следующих сочетаний клавиш:

- **Shift+PageUp** – прокрутка вверх;
- **Shift+PageDown** – прокрутка вниз.

Если объем вывода команды превышает размер терминального буфера, данные отображаются постранично. В этом случае появляется приглашение «:», указывающее на режим постраничного просмотра. В данном режиме доступны следующие действия:

- Для прекращения вывода данных используется клавиша «q».
- Для перехода к следующей странице используется клавиша «SPACE».
- Для перехода к предыдущей странице используется клавиша «b».
- Для перемещения выводимой на экран информации на одну строку вниз используется клавиша «ENTER».
- Для перемещения выводимой информации на одну строку вверх и на одну строку вниз используются клавиши «↑» и «↓» соответственно.
- Для перемещения выводимой информации влево и вправо используются клавиши «←» и «→» соответственно, если вывод данных в строке содержит

количество символов, превышающее буфер отображаемой на экране информации по горизонтали.

В **ARMA Стена** используются два режима работы:

- **«эксплуатационный режим»** – предназначен для мониторинга состояния системы, диагностики и выполнения операций с файлами;
- **«конфигурационный режим»** – используется для внесения и фиксации изменений в конфигурацию системы.

После успешной аутентификации пользователь автоматически попадает в **эксплуатационный режим**. Переход в **конфигурационный режим** осуществляется командой **«configure»**:

```
admin@ngfwos:~$ configure
[edit]
admin@ngfwos#
```

Для возврата в **эксплуатационный режим** из конфигурационного используется команда **«exit»**. Если в конфигурацию были внесены изменения, перед выходом требуется либо подтвердить их с помощью команды **«commit»**, либо отменить с помощью **«discard»** (или **«exit discard»**).

```
admin@ngfwos# exit
exit
admin@ngfwos:~$
```

Выполнение команды **«exit»** в эксплуатационном режиме приводит к завершению сеанса текущей учётной записи.

Действующую в данный момент конфигурацию возможно сохранить в файл при помощи команды **«save»** в конфигурационном режиме. По умолчанию, конфигурация сохраняется в файл **«config.boot»** расположенном в каталоге **«/config/»**. При инициализации системы происходит автоматическая загрузка конфигурации из файла **«/config/config.boot»**. В связи с этим, после завершения настройки всех требуемых сервисов, необходимо выполнить сохранение текущей конфигурации в указанный файл для обеспечения корректной загрузки параметров при следующем запуске устройства. Рекомендуется выполнять регулярное сохранение конфигурации после внесения любых изменений в настройки системы.

Формат приглашения командной строки содержит следующую информацию:

- имя учётной записи пользователя под которой выполнен вход в систему;
- имя узла системы, на который выполнен вход;
- текущий режим интерфейса командной строки;

- текущий уровень иерархии конфигурации (только в конфигурационном режиме).

В [таблице «Запрос на ввод команд»](#) приведены некоторые примеры запросов на ввод команд и их значения.

Таблица «Запрос на ввод команд»

Вид запроса	Описание запроса
admin@ngfwos:~\$	Пользователь: <i>admin</i> Имя узла: <i>ngfwos</i> Режим работы: <i>эксплуатационный режим</i>
[edit] admin@ngfwos#	Пользователь: <i>admin</i> Имя узла: <i>ngfwos</i> Режим работы: <i>конфигурационный режим</i> Уровень в иерархии конфигурации: <i>[edit] (верхний уровень)</i>

2.1 Эксплуатационный режим

Эксплуатационный режим предоставляет возможность управлять питанием устройства, получать информацию о текущем состоянии операционной системы и ее сервисов, а также выполнять диагностические команды, такие как traceroute или ping.

Основные команды эксплуатационного режима представлены в [таблице «Команды эксплуатационного режима»](#).

Таблица «Команды эксплуатационного режима»

Команда	Краткое описание
add	Добавить объект в службу
clear	Очистить информацию о системе
clone	Клонировать объект
configure	Войти в конфигурационный режим
connect	Установить соединение
copy	Копировать объект
delete	Удалить объект
disconnect	Разорвать соединение
exit	Выход из системы
force	Принудительное выполнение операции

Команда	Краткое описание
format	Форматировать устройство
generate	Сгенерировать объект/ключ
import	Импортировать объект
install	Установить новую систему
monitor	Мониторинг системной информации
mtr	Проследить путь Traceroute и ping к цели
ping	Отправка эхо-запроса ICMP
poweroff	Выключить систему
reboot	Перезагрузить систему
release	Освободить указанную переменную
rename	Переименовать объект
renew	Обновить указанную переменную
reset	Сброс службы
restart	Перезапустить отдельную службу
set	Добавить значение параметра конфигурации
show	Показать информацию о системе
suricata	Работает с правилами suricata
telnet	Telnet к узлу
traceroute	Трассировка сетевого пути к узлу
update	Обновление данных для службы
wake-on-lan	Отправка пакета Wake-On-LAN (WOL)

2.2 Конфигурационный режим

Конфигурационный режим предназначен для внесения и фиксации изменений конфигурации, а также сохранения конфигурационных файлов.

Переход в конфигурационный режим осуществляется из эксплуатационного режима командой:

```
admin@ngfwos:~$ configure
[edit]
admin@ngfwos#
```

Подтверждением входа в конфигурационный режим является изменение приглашения: символ «\$» заменяется на «#», а также отображается текущий уровень иерархии (например, **[edit]**).

Примечание:

Примеры команд данного руководства с приглашением **admin@ngfwos:~\$** следует выполнять в эксплуатационном режиме. Если в начале команды нет приглашения, а идёт сразу команда, например «set interfaces ethernet eth1 address 192.168.22.1/24», то данные команды выполняются в конфигурационном режиме.

Основные команды конфигурационного режима:

1. **«set»** – добавление или изменение параметра конфигурации.

```
[edit]  
admin@ngfwos# set interfaces ethernet eth1 disable
```

2. **«delete»** – удаление параметров конфигурации. При этом также удаляются все подуровни ниже текущего уровня, указанного в команде. При удалении записи элемент также примет значение по умолчанию, если таковое существует. Например, удалить IP-адрес для интерфейса «eth1».

```
[edit]  
admin@ngfwos# delete interfaces ethernet eth1 address
```

3. **«edit»** – переход на указанный уровень иерархии конфигурации для упрощения ввода последующих команд. Все команды, выполняемые в режиме конфигурации, связаны с определённым уровнем иерархической структуры, который задаётся администратором при вводе команд. В режиме конфигурации можно вносить изменения в настройки операционной системы с самого верхнего уровня иерархической структуры, однако в таком случае цепочка команд при ручном вводе будет достаточно длинной. Изменение уровня иерархической структуры позволяет сократить длину используемых команд и упростить настройку конфигурации операционной системы.

Например:

```
[edit]  
admin@ngfwos# edit interfaces ethernet eth1  
[edit interfaces ethernet eth1]  
admin@ngfwos# set address 192.168.22.1/24  
admin@ngfwos# set description "LAN"
```

Пример выше демонстрирует работу команды **«edit»**. После ввода команды «edit interfaces ethernet eth1» система переходит на уровень иерархической

структуры конфигурации, связанный с цепочкой команд «interfaces ethernet eth1». Все команды, будут выполняться в отношении данного уровня.

Для возвращения на самый верхний уровень иерархической структуры используются команды: «**top**» или «**exit**».

Для перемещения на один уровень иерархической структуры вверх используется команда «**up**».

4. «**commit**» – применение внесённых изменений. После применения изменений «рабочая» конфигурация становится «активной».

Допускается добавление комментария:

```
commit comment <message>.
```

Примечание:

Изменения, внесённые в конфигурацию, не применяются до выполнения команды «**commit**».

5. «**commit-confirm**» – команда, предназначенная для временного применения внесённых изменений в конфигурацию системы с автоматическим откатом к предыдущей сохранённой конфигурации в случае отсутствия подтверждения в течение заданного интервала времени. По истечении указанного времени система автоматически перезагружается с использованием предыдущей рабочей конфигурации.

Для запуска процедуры требуется подтверждение выполнения команды. На запрос системы необходимо ввести «**y**»:

```
admin@ngfwos# commit-confirm
```

```
You should save previous commits before commit-confirm !
```

```
commit-confirm will automatically reboot in 10 minutes unless changes  
are confirmed.
```

```
Proceed ? [Y/n] y
```

```
Initialized commit-confirm; 10 minutes to confirm before reboot
```

По умолчанию продолжительность интервала составляет **10 минут**. Допускается явное указание иного значения интервала в минутах, например: «**commit-confirm 25**».

Для подтверждения корректности внесённых изменений и отмены запланированной перезагрузки используется команда «**confirm**»:

```
admin@ngfwos# confirm
```

```
Reboot timer stopped
```

После выполнения команды **confirm** изменения фиксируются в текущей конфигурации, а таймер автоматической перезагрузки останавливается.

6. **«commit-check»** – выполняет проверку синтаксической и логической корректности введённых команд без их фактического применения к конфигурации системы.

В случае успешной проверки система выведет соответствующее сообщение:

```
admin@ngfwos# commit-check
```

```
Configuration check success
```

```
[edit]
```

```
admin@ngfwos#
```

Примечание:

При выходе из конфигурационного режима без предварительного выполнения команды **«commit»** настройки не будут применены.

7. **«save»** – сохранить активную конфигурацию в файл config.boot:

```
[edit]
```

```
save
```

При попытке перезагрузки или выключения системы без сохранения изменений выводится предупреждение:

```
Warning: there are unsaved configuration changes!
```

```
Run 'save' command if you do not want to lose those changes after  
reboot/shutdown.
```

8. **«exit»** – выход из текущего уровня иерархии или из конфигурационного режима.

```
[edit interfaces ethernet eth1]
```

```
admin@ngfwos# exit
```

```
[edit]
```

```
admin@ngfwos# exit
```

```
exit
```

```
admin@ngfwos:~$
```

Примечание:

Команда «**exit**» не применится для выхода из конфигурационного режима в случае наличия в конфигурации незафиксированных изменений.

```
[edit]
admin@ngfwos# exit
Cannot exit: configuration modified.
Use 'exit discard' to discard the changes and exit.
```

В случае выхода из конфигурационного режима без сохранения внесённых настроек системы выведет предупреждение и перейдёт в эксплуатационный режим:

```
[edit]
admin@ngfwos# exit
Warning: configuration changes have not been saved.
exit
admin@ngfwos:~$
```

9. «**exit discard**» – принудительный выход из конфигурационного режима с отменой всех незафиксированных изменений.
10. «**run**» – выполнение команд эксплуатационного режима без выхода из конфигурационного режима.

```
[edit]
admin@ngfwos# run show system commit
```

11. «**show**» – отображение текущей рабочей конфигурации с маркировкой изменений:
 - «+» – добавленные строки;
 - «>» – изменённые строки;
 - «-» – удалённые строки.

```
[edit]
admin@ngfwos# show
```

Для команды возможно указать дополнительные параметры вывода информации о конфигурации системы **ARMA Стена**:

- **show | commands** – вывод конфигурации в виде последовательности команд «**set**».

Примечание:

Для вывода информации обо всех выполненных командах «**set**» используется команда «**run show configuration commands**» в конфигурационном режиме или «**show configuration commands**» в эксплуатационном режиме.

- **show | json** - вывод конфигурации в формате JSON.
- **show | strip-private** - скрывает конфиденциальных данных при выводе конфигурацию системы. При использовании данной команды происходит фильтрация выходных данных команды **show**, в результате чего удаляются или скрываются конфиденциальные данные, такие как пароли, ключи шифрования и другая чувствительная информация. Это может быть полезно, например, при необходимости предоставить техническую поддержку или сообществу доступ к логам или конфигурации устройства для устранения неполадок, при этом сохраняя конфиденциальность данных.
- **show | count** - отображение количества строк в конфигурации.
- **show | match <pattern>** - вывод только строк, соответствующих заданному шаблону <pattern>.
- **show | no-match <pattern>** - вывод только строк, не соответствующих шаблону <pattern>.
- **show | more** - постраничный вывод.
- **show | no-more** - отключение постраничного вывода.

3 ИНТЕРФЕЙСЫ

Примечание:

Перед удалением сетевых интерфейсов требуется обязательно исключить их из состава всех сервисов и служб, в которых они используются. К таким службам могут относиться маршрутизация, NAT, МЭ, балансировка нагрузки, VPN-туннели, COB и др. Невыполнение данного шага может привести к нарушению сетевой связности, сбоям в работе сервисов или ошибкам в конфигурации. Рекомендуется проверить все зависимости перед выполнением операции удаления интерфейса.

3.1 Физический интерфейс

Физические интерфейсы Ethernet получают имена в формате «**ethN**», где «**N**» – идентификатор, присвоенный интерфейсу.

3.1.1 Конфигурирование

1. Назначение IP-адреса и префикса сети интерфейсу Ethernet:

```
set interfaces ethernet ethN address <ip-адрес>
```

где:

- «**ethN**» – имя интерфейса;
- **<ip-адрес>** – IP-адрес в формате CIDR (<x.x.x.x/x> – для IPv4; <h:h:h:h:h:h:h/x> – для IPv6). Возможно назначение нескольких IP-адресов на интерфейс. Каждый указанный IP-адрес не заменяет назначенный ранее.

2. Назначить получение адреса и префикса от сервера DHCP:

```
set interfaces ethernet ethN address <dhcp | dhcpv6>
```

Для освобождения текущего IP-адреса, полученного клиентом DHCP от сервера, в эксплуатационном режиме следует выполнить команду:

```
admin@ngfwos:~$ release <dhcp | dhcpv6> interface <имя_интерфейса>
```

Устройство отправляет серверу DHCP сообщение RELEASE, уведомляя о прекращении использования выделенного адреса. В результате сетевой интерфейс теряет присвоенный IPv4-адрес. Это может привести к потере сетевой связности, если на интерфейсе не настроен статический IP-адрес.

Для принудительного обновления или запроса нового IP-адреса у DHCP-сервера в эксплуатационном режиме используется команда:

```
admin@ngfwos:~$ renew <dhcp | dhcpv6> interface <имя_интерфейса>
```

После выполнения команды клиент инициирует процесс получения нового адреса или обновления текущей аренды в соответствии с протоколом DHCP.

3. Добавить текстовое описание интерфейса Ethernet:

```
set interfaces ethernet ethN description <описание>
```

где **<описание>** – краткое текстовое описание. Допускается использование символов кириллического и латинского алфавитов. Описание не должно начинаться с последовательности «//». Запрещено использование символов «"», «'» и перенос строки. Максимальная длина значения – «127» символов. При наличии пробелов значение поля должно быть заключено в двойные кавычки.

4. Вывести информации о настроенных интерфейсах Ethernet:

- команда в эксплуатационном режиме:

```
admin@ngfwos:~$ show interfaces
```

Пример:

```
admin@ngfwos# run show interfaces
Codes: S - State, L - Link, u - Up, D - Down, A - Admin Down
Interface      IP Address      MAC              VRF      MTU
S/L    Description
-----
eth0          172.16.100.10/24  00:50:23:bd:1b:e9  default  1500
u/u      WAN
eth1          192.168.67.1/24   00:50:25:bd:11:3b  default  1500
u/u      LAN
           192.168.68.1/24
lo          127.0.0.1/8       00:00:00:00:00:00  default  65536
u/u
           ::1/128
[edit]
```

- команда в конфигурационном режиме:

```
admin@ngfwos# show interfaces
```

Пример:

```
admin@ngfwos# show interfaces
Must specify config path
ethernet eth0 {
    address dhcp
    description WAN
    hw-id 00:50:23:bd:1b:e9
}
ethernet eth1 {
    address 192.168.67.1/24
    address 192.168.67.2/24
    description LAN
    hw-id 00:50:25:bd:11:3b
}
loopback lo {
}
```

5. Отключение интерфейса Ethernet с сохранением настройки:

```
set interfaces ethernet ethN disable
```

Интерфейс будет переведён в состояние административного отключения (A/D).

6. Отключение генерации управления потоком Ethernet (кадров паузы):

```
set interfaces ethernet ethN disable-flow-control
```

Передающая станция, будь то компьютер или сетевой коммутатор, может передавать данные с более высокой скоростью, чем принимающая станция способна обработать. Чтобы избежать перегрузки, принимающая сторона может использовать механизм управления потоком. Этот механизм уведомляет отправителя о необходимости приостановить передачу данных до тех пор, пока принимающая станция не будет готова их принять.

7. Отключение обнаружения изменений физического состояния канала связи:

```
set interfaces ethernet ethN disable-link-detect
```

С помощью данной команды возможно настроить сетевой интерфейс таким образом, чтобы он не обнаруживал изменений физического состояния канала связи, например, при отсоединении кабеля. По умолчанию установлен параметр, который фиксирует такие изменения.

7. Установка MAC-адреса интерфейса Ethernet:

```
set interfaces ethernet ethN mac <xx:xx:xx:xx:xx:xx>
```

где **<xx:xx:xx:xx:xx:xx>** - MAC-адрес для интерфейса Ethernet. По умолчанию используется MAC-адрес первого интерфейса, добавленного в интерфейс Ethernet.

Примечание:

Для предотвращения ошибок при изменении HWID сетевой карты (на виртуальной машине они генерируются случайным образом при запуске, а на физическом оборудовании могут меняться, например, при замене сетевого оборудования или при установке **ARMA Стена** на другое оборудование) необходимо выполнить следующие действия:

1. Удалить старый HWID с помощью команды **«delete interfaces ethernet ethN hw-id»**.
2. Отключить автоматическое назначение MAC-адреса сетевой карте с помощью команды **«set interfaces ethernet ethN hw-id-auto-pinning false»**.
3. Назначить новый HWID с помощью команды **«set interfaces ethernet ethN hw-id <h:h:h:h:h:h>»**.

8. Установка значения MTU для интерфейса Ethernet:

```
set interfaces ethernet ethN mtu <mtu>
```

где **<mtu>** - значение MTU для интерфейса Ethernet. Возможно указать значение в диапазоне от «68» до «9190».

9. Установка режима дуплекса для интерфейса Ethernet:

```
set interfaces ethernet ethN duplex <auto | full | half>
```

где **<auto | full | half>** - режим дуплекса интерфейса. Возможно указать следующие режимы:

- **auto** - маршрутизатор автоматически согласует режим дуплекса с интерфейсом на другом конце канала. Установлен по умолчанию;
- **full** - полнодуплексный режим;
- **half** - полудуплексный режим.

Команда используется для установки характеристик режима дуплекса для интерфейса Ethernet. Если режим дуплекса устанавливается явно, то также потребуется явно указать значение параметра «interfaces ethernet ethN speed».

Примечание:

Не всё оборудование поддерживает возможность явного указания режима дуплекса (или определённые режимы работы). Если используется оборудование, не поддерживающее такую установку (или определённые

режимы работы), при фиксации изменений будет отображено сообщение об ошибке.

10. Установка скорости интерфейса Ethernet:

```
set interfaces ethernet ethN speed <скорость>
```

где **<скорость>** - устанавливаемая скорость интерфейса Ethernet. Возможно указать следующие значения:

- **auto** - скорость интерфейса будет автоматически согласована маршрутизатором с интерфейсом на другом конце подключения. Установлен по умолчанию;
- **10** - 10 Мбит/с;
- **100** - 100 Мбит/с;
- **1000** - 1 Гбит/с;
- **2500** - 2,5Гбит/с;
- **5000** - 5 Гбит/с;
- **10000** - 10 Гбит/с;
- **25000** - 25 Гбит/с;
- **40000** - 40 Гбит/с;
- **50000** - 50 Гбит/с;
- **100000** - 100 Гбит/с.

Команда используется для установки скорости интерфейса Ethernet. Если режим дуплекса устанавливается явно, то также потребуется явно указать значение параметра «interfaces ethernet ethN duplex».

Примечание:

Программно-аппаратные комплексы **K10000** на базе сервера «Тринити Е8» с сетевым адаптером «LR-LINK LREC9804BF-4SFP+ 10G PCIe3.0 Intel XL710», поддерживают подключение только со скоростями **1 Гбит/с** и **10 Гбит/с**. Кроме того, встроенные сетевые карты на материнской плате **несовместимы** с оборудованием, работающим на скорости **100 Мбит/с и ниже**.

Примечание:

Оборудование может не поддерживать возможность явной установки скорости передачи (или определённые режимы работы). Если используется оборудование, не поддерживающее такую установку (или определённые режимы работы), при фиксации изменений будет отображено сообщение об ошибке.

11. Проверка пропускной способности интерфейса в реальном времени:

```
admin@ngfwos:~$ monitor bandwidth interface ethN
```

12. Включить различные типы аппаратной разгрузки (offload) на интерфейсе Ethernet:

```
set interfaces ethernet ethN offload <gro | gso | lro | rps | sg | tso>
```

где **<gro | gso | lro | rps | sg | tso>** - тип аппаратной разгрузки на указанном интерфейсе Ethernet. Возможно указать следующие значения:

- **lro** - данный метод направлен на увеличение пропускной способности сетевых подключений с высокой пропускной способностью путём снижения нагрузки на центральный процессор. Он реализуется путём объединения нескольких входящих пакетов из одного потока в единый буфер перед их передачей в верхний уровень сетевого стека, что позволяет сократить количество обрабатываемых пакетов.

Примечание:

Известно, что в некоторых случаях LRO может изменять заголовки пакетов передаваемого трафика, что нарушает принцип сквозной передачи данных в компьютерных сетях. LRO также может разгружать только сегменты TCP, инкапсулированные в пакеты IPv4. В связи с этими ограничениями рекомендуется по возможности использовать технологию GRO.

- **gso** - реализует обобщённый LRO в программном обеспечении, которое не ограничено протоколами TCP/IPv4 и не имеет проблем, связанных с LRO.
- **gro** - является дополнением к GSO. В идеале любой кадр, собранный с помощью GRO, должен быть сегментирован для создания идентичной последовательности кадров с помощью GSO, а любая последовательность кадров, сегментированная с помощью GSO, должна быть способна собраться обратно в оригинал с помощью GRO. Единственным исключением из этого является IPv4 ID в случае, если для данного IP-заголовка установлен бит DF.
- **rps** - представляет собой логическую программную реализацию RSS. В отличие от RSS, который выбирает очередь и, следовательно, процессор для запуска обработчика аппаратных прерываний, RPS сам решает, какой процессор будет обрабатывать протокол, минуя обработчик прерываний. Это достигается путём помещения пакета в очередь ожидания нужного процессора и его пробуждения для

обработки. RPS обладает рядом преимуществ перед RSS: её можно использовать с любым сетевым адаптером; легко добавлять программные фильтры для хеширования по новым протоколам; не увеличивает частоту прерываний аппаратных устройств, хотя и вводит межпроцессорные прерывания (IPI).

- **tso** - позволяет адаптерам принимать большой объём данных, превышающий размер MTU. Механизм TSO разбивает данные на отдельные пакеты и автоматически вставляет заданные пользователем заголовки L2/L3/L4 в каждый пакет. Благодаря TSO процессор не перегружается при работе с большим объёмом данных.
- **sg** - технология, которая позволяет передавать данные не через один большой буфер, а через несколько маленьких, что увеличивает производительность при обработке больших запросов на ввод-вывод.

Примечание:

Для использования TSO/LRO с адаптерами VMXNET3 необходимо включить аппаратную разгрузку типа SG.

Примечание:

Сетевой адаптер Intel серии **X710** в системе **ARMA Стена** не поддерживает режим «**offload**».

3.1.2 Расширенные настройки

1. Установка значения TCP MSS:

```
set interfaces ethernet ethN ip adjust-mss <mss | clamp-mss-to-pmtu>
```

где:

- **<mss>** - значение MSS. Возможно указать значение в диапазоне от «536» до «65535».
- **<clamp-mss-to-pmtu>** - автоматически устанавливать MSS в нужное значение.

Поскольку обнаружение PMTU в сети Интернет работает нестабильно, иногда возникает необходимость ограничить значение TCP MSS. Это поле находится в опциях TCP в части SYN-пакета. Установив значение MSS, система сообщает удалённой стороне, что не следует отправлять пакеты размером больше этого значения.

2. Установка тайм-аута записи в ARP-кэш для интерфейса Ethernet:

```
set interfaces ethernet ethN ip arp-cache-timeout <1-86400>
```

где **<1-86400>** - значение тайм-аута записи в ARP-кэш в секундах. Возможно указать значение в диапазоне от «1» до «86400». По умолчанию используется значение «30».

3. Отключить фильтрацию ARP на интерфейсе Ethernet:

```
set interfaces ethernet ethN ip disable-arp-filter
```

Если параметр не установлен (по умолчанию), это позволяет иметь несколько сетевых интерфейсов в одной подсети и отвечать на ARP для каждого интерфейса в зависимости от того, будет ли ядро направлять пакет с IP-адресом ARP через этот интерфейс. Для этого необходимо использовать маршрутизацию на основе источника.

4. Отключить переадресацию IP на интерфейсе Ethernet:

```
set interfaces ethernet ethN ip disable-forwarding
```

Если параметр установлен, интерфейс переходит в режим хоста, и переадресация IPv6 на этом интерфейсе отключается.

5. Включить направленную широковещательную пересылку на интерфейсе Ethernet:

```
set interfaces ethernet ethN ip enable-directed-broadcast
```

В случае активации данной опции, входящие пакеты направленной широковещательной рассылки IP будут перенаправляться через указанный интерфейс. В случае если данный параметр не задан (по умолчанию), входящие пакеты направленной широковещательной рассылки IP не будут передаваться.

6. Включить приём ARP пакетов на интерфейсе Ethernet:

```
set interfaces ethernet ethN ip enable-arp-accept
```

Определяет поведение для ARP-пакетов, IP-записи которых ещё не присутствуют в ARP-таблице. Если эта настройка включена, то создаются новые записи в ARP-таблице. Как ответы, так и запросы типа Gratuitous ARP будут вызывать обновление ARP-таблицы, если эта настройка включена. Если в ARP-таблице уже содержится IP-адрес кадра Gratuitous ARP, то ARP-таблица будет обновлена независимо от того, включена или выключена эта настройка.

7. Включить анонсирование ARP пакетов на интерфейсе Ethernet:

```
set interfaces ethernet ethN ip enable-arp-announce
```

Если параметр не задан, используется любой локальный адрес, который настроен на любом интерфейсе. Если параметр установлен, рекомендуется избегать использования локальных адресов, которые не входят в подсеть цели

для данного интерфейса. Этот режим полезен, когда целевые узлы, доступные через данный интерфейс, требуют, чтобы IP-адрес источника в ARP-запросах был частью их логической сети, настроенной на принимающем интерфейсе. При генерации запроса система проверяет все подсети, включающие целевой IP-адрес, и сохраняем адрес источника, если он принадлежит такой подсети. Если подходящей подсети не найдено, система выбирает адрес источника в соответствии с правилами для уровня 2.

8. Включить игнорирование ARP пакетов на интерфейсе Ethernet:

```
set interfaces ethernet ethN ip enable-arp-ignore
```

Данный параметр определяет режимы отправки ответов на ARP-запросы, которые разрешают локальные целевые IP-адреса. Если параметр включён, ответ будет отправлен только в том случае, если целевой IP-адрес является локальным адресом, настроенным на входящем интерфейсе. Если параметр отключён (по умолчанию), ответ будет получен для любого локального целевого IP-адреса, настроенного на любом интерфейсе.

9. Включить политику проверки источника по обратному пути, как указано в RFC 3704:

```
set interfaces ethernet ethN ip source-validation <strict | loose | disable>
```

где **<strict | loose | disable>** - режим проверки источника. Возможно указать следующие значения:

- **strict** - каждый входящий пакет проверяется по FIB, и принимается только если пришёл через оптимальный (наилучший) обратный путь, определённый в таблице маршрутизации. Все пакеты, не удовлетворяющие этому условию, автоматически отбрасываются.
- **loose** - адрес источника каждого входящего пакета также проверяется по FIB, и если адрес источника не достижим ни через один интерфейс, проверка пакета будет неудачной.
- **disable** - нет проверки источника.

В настоящее время в RFC 3704 рекомендуется включать strict режим для предотвращения подмены IP адресов в результате DDos атак. При использовании асимметричной или другой сложной маршрутизации рекомендуется использовать loose режим.

10. Включить получение IPv6-адреса с помощью автоконфигурации без статического изменения (SLAAC):

```
set interfaces ethernet ethN ipv6 address autoconf
```

В соответствии с RFC 4862, хосты IPv6 могут автоматически настраиваться при подключении к сети IPv6 с использованием протокола Neighbor Discovery Protocol (NDP) через сообщения ICMPv6 об обнаружении маршрутизатора. При первом подключении к сети хост отправляет многоадресный запрос link-local router solicitation для получения параметров конфигурации. Маршрутизаторы отвечают на этот запрос пакетом router advertisement, содержащим параметры конфигурации уровня Интернета.

Примечание:

Данный метод автоматически отключает пересылку трафика IPv6 на сетевом интерфейсе.

11. Включить префикс EUI-64 на основе MAC адреса для IPv6 адреса интерфейса Ethernet:

```
set interfaces ethernet ethN ipv6 address eui64 <prefix>
```

где **<prefix>** - сеть IPv6 в формате <h:h:h:h:h:h/h/64>.

12. Удалить локальный адрес IPv6 по умолчанию для интерфейса Ethernet:

```
set interfaces ethernet ethN ipv6 address no-default-link-local
```

13. Отключить IP переадресацию на интерфейсе Ethernet:

```
set interfaces ethernet ethN ipv6 disable-forwarding
```

В случае установки, интерфейс будет переведён в режим хоста, а переадресация IPv6 на данном интерфейсе будет отключена.

14. Установить значения TCP MSS:

```
set interfaces ethernet ethN ipv6 adjust-mss <mss | clamp-mss-to-pmtu>
```

где:

- **<mss>** - значение MSS. Возможно указать значение в диапазоне от «536» до «65535».
- **<clamp-mss-to-pmtu>** - автоматически устанавливать MSS в нужное значение.

15. Принимать обнаружение дублирующего адреса:

```
set interfaces ethernet ethN ipv6 accept-dad <0-2>
```

где **<0-2>** - режим приёма DAD. Возможно указать следующие значения:

- **0** - отключить DAD;
- **1** - включить DAD (по умолчанию);

- **2** - включить DAD и отключить работу IPv6, если обнаружен дублированный MAC-адрес link-local.

16. Установить количество сообщений NS для отправки при выполнении DAD:

```
set interfaces ethernet ethN ipv6 dup-addr-detect-transmits <n>
```

где **<n>** - количество NS-сообщений. В случае установки значения «0», функция обнаружения дубликатов адресов (DAD) будет отключена. По умолчанию используется значение «1».

17. Разместить интерфейс Ethernet в указанном экземпляре VRF:

```
set interfaces ethernet ethN vrf <vrf>
```

где **<vrf>** - имя экземпляра VRF.

18. Включить прокси ARP частного VLAN на интерфейсе Ethernet:

```
set interfaces ethernet ethN ip proxy-arp-pvlan
```

Разрешить ответы ARP-прокси с того же интерфейса, с которого был получен ARP-запрос или запрос на предложение. Это необходимо для поддержки функций Ethernet-коммутаторов, описанных в RFC 3069, где отдельные порты не могут напрямую связываться друг с другом, но могут связываться с вышестоящим маршрутизатором. Как указано в RFC 3069, этого можно достичь путём включения прокси-ARP.

Необязательно использовать вместе с `proxy_arp`.

19. Включить прокси ARP на интерфейсе Ethernet:

```
set interfaces ethernet ethN ip enable-proxy-arp
```

Прокси ARP позволяет интерфейсу Ethernet отвечать своим MAC-адресом на ARP-запросы IP-адресов назначения в подсетях, подключённых к другим интерфейсам системы. Последующие пакеты, отправленные на эти IP-адреса назначения, пересылаются системой соответствующим образом.

3.1.2.1 Пример настройки Proxy ARP

В качестве примера настройки Proxy ARP будет использоваться схема стенда, представленная на рисунке (см. [Рисунок – Схема стенда для настройки Proxy ARP](#)).

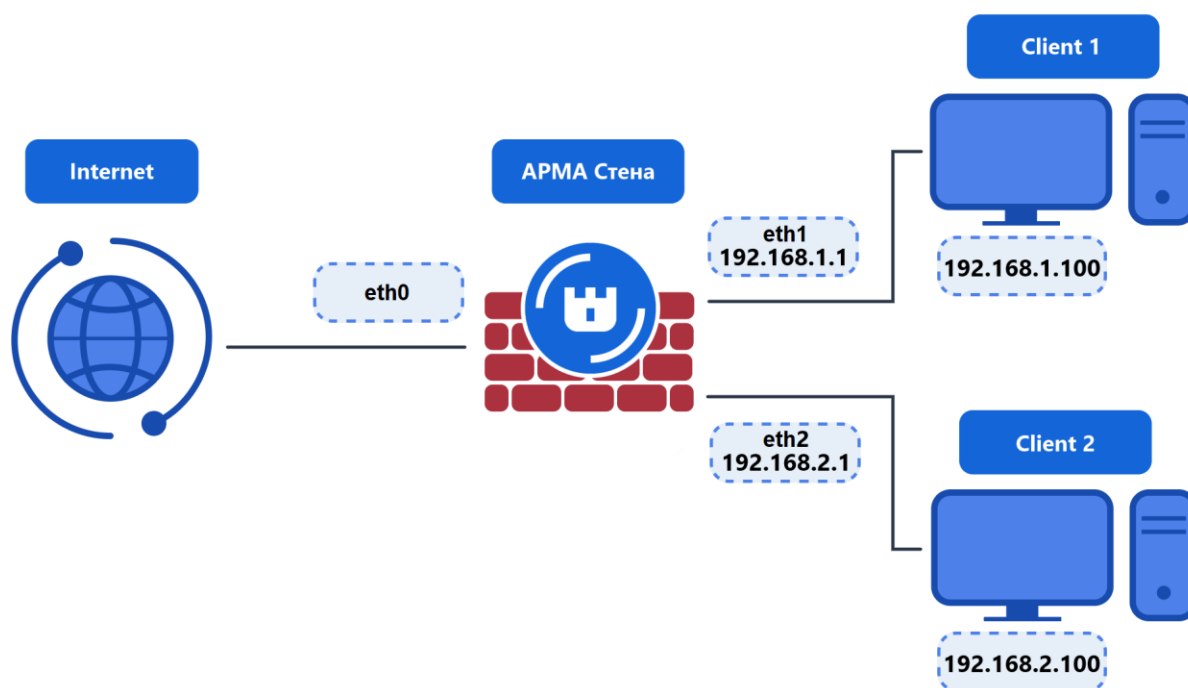


Рисунок – Схема стенда для настройки Proxy ARP

Для настройки Proxy ARP необходимо выполнить следующие действия:

1. На **ARMA Стена** ввести следующие команды:

```

set interfaces ethernet eth1 address 192.168.1.1/24
set interfaces ethernet eth2 address 192.168.2.1/24
set interfaces ethernet eth1 ip enable-proxy-arp
set interfaces ethernet eth2 ip enable-proxy-arp
commit
save
  
```

2. Для обеспечения беспрепятственного прохождения пакетов необходимо создать разрешающее правило МЭ (см. [Создание правил МЭ](#) настоящего руководства).
3. На ПК **Client 1** и ПК **Client 2** в свойствах сетевого подключения необходимо указать маску «**255.255.0.0**» (см. [Рисунок – ПК Client 1. Свойства сетевого подключения](#)).

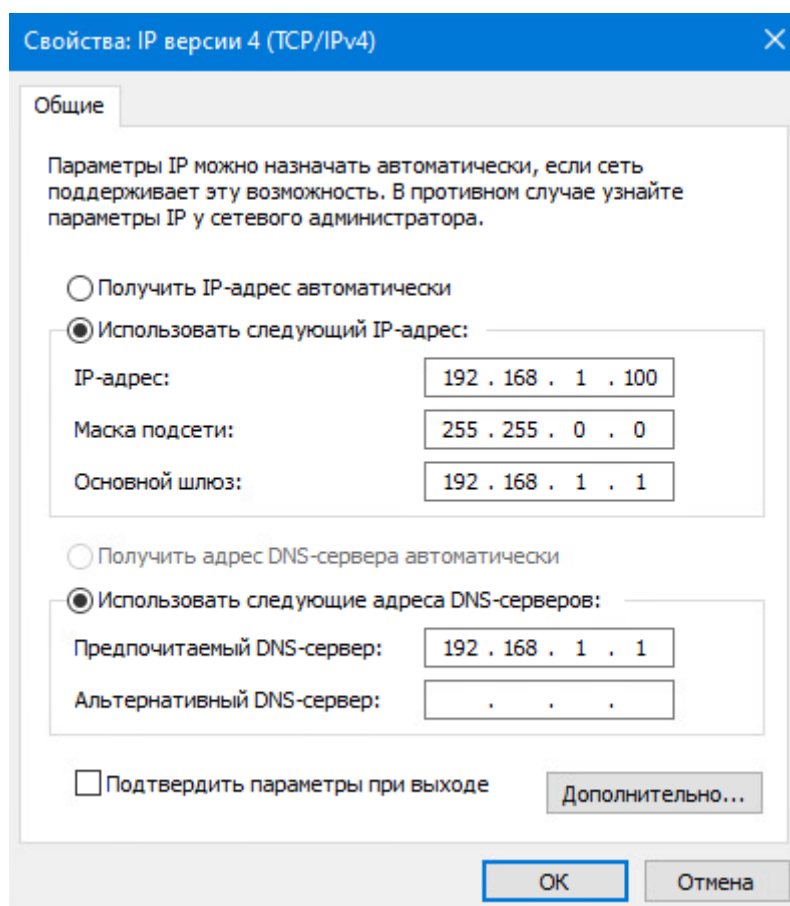


Рисунок – ПК Client 1. Свойства сетевого подключения

Для проверки работы Proxu ARP необходимо на ПК **Client 1** инициировать пинг IP-адреса ПК **Client 2**. Успешный результат выполнения команды будет свидетельствовать о корректной настройке **ARMA Стена** (см. [Рисунок – ПК Client 1. Результат выполнения команды «ping»](#)).

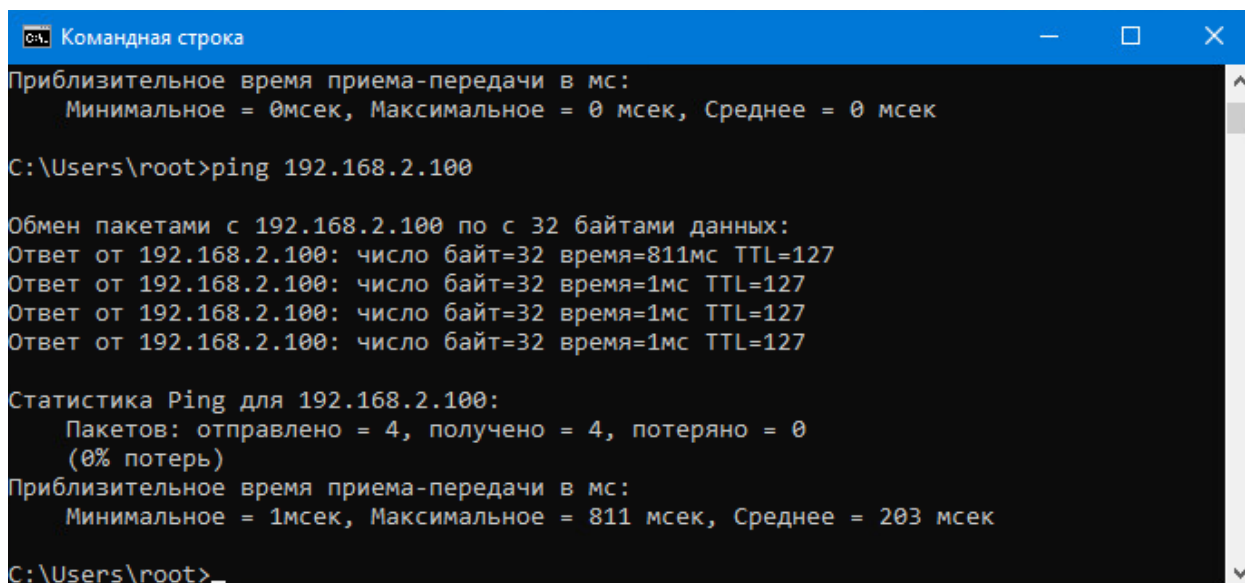


Рисунок – ПК Client 1. Результат выполнения команды «ping»

3.1.2.2 Настройки получения адреса по DHCP(v6)

1. Установить идентификатор, используемый клиентом для идентификации себя DHCP сервером:

```
set interfaces ethernet ethN dhcp-options client-id <description>
```

где **<description>** - значение идентификатора.

В случае предоставления идентификатора пользователь обязан использовать один и тот же идентификатор во всех последующих сообщениях.

2. Изменить системное имя устройства, передаваемое DHCP серверу:

```
set interfaces ethernet ethN dhcp-options host-name <hostname>
```

где **<hostname>** - новое системное имя хоста, передаваемое DHCP серверу.

Вместо передачи реального системного имени хоста на DHCP-сервер будет передано заданное значение в качестве имени хоста.

3. Определить тип клиента поставщика для DHCP-сервера:

```
set interfaces ethernet ethN dhcp-options vendor-class-id <vendor-id>
```

где **<vendor-id>** - значение опций DHCP.

Опция «vendor-class-id» используется для запроса у сервера определённого класса опций поставщика.

4. Запросить у DHCP-сервера только адрес, не запрашивая шлюз по умолчанию:

```
set interfaces ethernet ethN dhcp-options no-default-route
```

5. Установить значение расстояния для шлюза по умолчанию, отправляемого сервером DHCP:

```
set interfaces ethernet ethN dhcp-options default-route-distance <distance>
```

где **<distance>** - значение расстояния для шлюза по умолчанию. Возможно указать значение в диапазоне от «1» до «255». По умолчанию используется значение «210».

6. Отклонить аренду DHCP с заданного адреса или диапазона:

```
set interfaces ethernet ethN dhcp-options reject <address>
```

где **<address>** - IP-адрес, возможно указать несколько раз в формате <x.x.x.x> и/или <x.x.x.x/x>.

7. Задать уникальный идентификатор DHCP (DUID) для интерфейса Ethernet:

```
set interfaces ethernet ethN dhcpv6-options duid <h[:h]...>
```

где **<h[[:h]]...>** - значение уникального идентификатора DHCP.

Уникальный идентификатор DHCP (DUID) используется системой для получения IP-адреса от сервера DHCPv6. Он состоит из двухбайтового поля типа DUID и поля идентификатора переменной длины до 128 байт. Фактическая длина DUID зависит от типа. Сервер сравнивает DUID с данными в своей базе и предоставляет системе необходимую информацию, такую как адрес, время аренды, DNS-серверы и другие параметры.

8. Не отправлять сообщение об освобождении при выходе:

```
set interfaces ethernet ethN dhcpv6-options no-release
```

Данный параметр означает, что при использовании протокола DHCP для получения IPv6-адресов адрес не будет освобождаться автоматически. Это может быть полезно, если необходимо сохранить полученный адрес после отключения интерфейса или перезагрузки. В таком случае адрес возможно будет использовать многократно при последующих операциях подключения.

9. Получить только параметры конфигурации без запроса IPv6-адреса:

```
set interfaces ethernet ethN dhcpv6-options parameters-only
```

Данная опция указывает клиенту DHCPv6 (dhcp6c) обмениваться с сервером исключительно информационными параметрами конфигурации, такими как список адресов DNS-серверов. Использование параметра уместно в случаях, когда клиенту не требуются параметры с состоянием – например, IPv6-адреса или делегированные префиксы.

10. Включить функцию Rapid Commit для быстрого получения IPv6-адреса:

```
set interfaces ethernet ethN dhcpv6-options rapid-commit
```

11. Запросить временный IPv6-адрес:

```
set interfaces ethernet ethN dhcpv6-options temporary
```

Запрашивается только временный адрес, и не создаёт партнёрство IANA (Identity Association for Non-temporary Addresses).

3.1.2.3 Делегирование префиксов DHCPv6 (PD)

1. Задать размер делегируемого префикса для экземпляра делегирования префикса на интерфейсе Ethernet:

```
set interfaces ethernet ethN dhcpv6-options pd <id> length <length>
```

где:

- **<id>** - номер экземпляра делегированного префикса. Значение должно быть больше или равно нулю.
 - **<length>** - значение размера делегируемого префикса. Возможно указать значение в диапазоне от «32» до «64». По умолчанию используется значение «64».
2. Указать адрес интерфейса **<address>**, используемый локально на интерфейсе **<delegatee>**, на который был делегирован префикс:

```
set interfaces ethernet ethN dhcpv6-options pd <id> interface <delegatee> address <address>
```

где:

- **<delegatee>** - сетевой интерфейс.
- **<address>** - значение, используемое для формирования адреса интерфейса IPv6. Значение должно быть больше нуля.

Интерфейс будет объединён с делегированным префиксом и идентификатором **sla-id** для формирования полного адреса интерфейса. По умолчанию используется расширенный уникальный идентификатор интерфейса (EUI-64).

3. Указать значение идентификатора агрегатора уровня сайта SLA **<sla-id>** на интерфейсе **<delegatee>**:

```
set interfaces ethernet ethN dhcpv6-options pd <id> interface <delegatee> sla-id <id>
```

где **<id>** - значение идентификатора агрегатора уровня сайта. Идентификатор должен быть положительным десятичным числом и соответствовать максимально допустимой длине идентификаторов SLA.

3.1.3 VLAN 802.1Q

VLAN – это технология, позволяющая строить виртуальные сети с независимой от физических устройств топологией.

IEEE 802.1Q – открытый стандарт, который описывает процедуру тегирования трафика для передачи информации о принадлежности к VLAN по сетям стандарта IEEE 802.3 Ethernet.

В **ARMA Стена** интерфейсы 802.1q представлены как виртуальные интерфейсы.

3.1.3.1 Команды настройки VLAN-интерфейса

1. Команда создания VLAN-интерфейса:

```
set interfaces ethernet <interface> vif <vlan-id>
```

где:

- **<interface>** – имя физического интерфейса, например «eth1»;
- **<vlan-id>** – идентификатор VLAN. Возможно указание значения в диапазоне от «0» до «4094».

На одном физическом интерфейсе возможно создать несколько VLAN-интерфейсов.

Примечание:

Нельзя создавать виртуальные интерфейсы для физического интерфейса, который участвует в сетевом мосте с поддержкой VLAN.

2. Команда назначения адреса VLAN-интерфейсу:

```
set interfaces ethernet <interface> vif <vlan-id> address <address | dhcp | dhcpv6>
```

где:

- **<interface>** – имя физического интерфейса;
- **<vlan-id>** – идентификатор VLAN;
- **<address | dhcp | dhcpv6>** – IP-адрес VLAN-интерфейса. Возможно указать IP-адрес в формате: IPv4 – «x.x.x.x/x» или «dhcp», IPv6 – «h:h:h:h:h:h/h/x» или «dhcpv6».

Примеры назначения IP-адреса для VLAN-интерфейса «eth0.5»:

```
set interfaces ethernet eth0 vif 5 address 192.168.20.1/24
set interfaces ethernet eth0 vif 5 address 2001:db8::1/64
set interfaces ethernet eth0 vif 5 address dhcp
set interfaces ethernet eth0 vif 5 address dhcpv6
```

3. Команда создания описания для VLAN-интерфейса:

```
set interfaces ethernet <interface> vif <vlan-id> description <description>
```

где **<description>** – краткое текстовое описание. Допускается использование символов кириллического и латинского алфавитов. Описание не должно начинаться с последовательности «//». Запрещено использование символов «"», «'» и перенос строки. Максимальная длина значения – «127» символов. При наличии пробелов значение поля должно быть заключено в двойные кавычки.

Примеры описания для VLAN-интерфейса «eth0.5»:

```
set interfaces ethernet eth0 vif 5 description 'Интерфейс VLAN0.5'
set interfaces ethernet eth0 vif 5 description Интерфейс_VLAN0.5
```

4. Команда отключения VLAN-интерфейса:

```
set interfaces ethernet <interface> vif <vlan-id> disable
```

После отключения интерфейс будет переведён в состояние административного отключения.

Примечание:

При необходимости удаления VLAN-интерфейса, на который выполняется зеркалирование трафика, требуется предварительно выключить зеркалирование на данный VLAN-интерфейс (см. [SPAN](#)).

В противном случае при создании нового VLAN-интерфейса на физическом интерфейсе, использовавшемся для зеркалирования трафика на удалённый VLAN-интерфейс, возникнет ошибка.

5. Команда отключения контроля состояния физического канала связи:

```
set interfaces ethernet <interface> vif <vlan-id> disable-link-detect
```

По умолчанию VLAN-интерфейсы настроены на обнаружение изменения физического состояния канала, например, при отсоединении кабеля.

6. Команда установки пользовательского MAC-адреса для VLAN-интерфейса:

```
set interfaces ethernet <interface> vif <vlan-id> mac <xx:xx:xx:xx:xx:xx>
```

где **<xx:xx:xx:xx:xx:xx>** - пользовательский MAC-адрес.

7. Команда установки размера MTU для VLAN-интерфейса:

```
set interfaces ethernet <interface> vif <vlan-id> mtu <mtu>
```

где **<mtu>** – значение MTU. Возможно указание значения в диапазоне от «1280» до «9190».

Примечание:

Значение MTU должно быть меньшим или равным значению MTU родительского интерфейса.

8. Команда установки тайм-аута записи ARP-кэша для VLAN-интерфейса:

```
set interfaces ethernet <interface> vif <vlan-id> ip arp-cache-timeout <time>
```

где **<time>** – время тайм-аута в секундах. Возможно указание значения в диапазоне от «1» до «86400». По умолчанию используется значение «30».

9. Команда отключения фильтрации ARP-запросов на VLAN-интерфейсе:

```
set interfaces ethernet <interface> vif <vlan-id> ip disable-arp-filter
```

Если параметр установлен, то программа отвечает на ARP-запросы адресами других интерфейсов.

По умолчанию параметр не установлен, что позволяет иметь несколько сетевых интерфейсов в одной подсети и отвечать на ARP-запросы для каждого интерфейса в зависимости от того, будет ли программа маршрутизировать ARP-пакет через этот интерфейс. Для работы функции необходимо использовать маршрутизацию на основе источника.

10. Команды настройки поведения хоста в зависимости от интерфейса:

```
set interfaces ethernet <interface> vif <vlan-id> ip disable-forwarding
```

Если параметр установлен, интерфейс переключится в режим хоста и IP-переадресация на интерфейсе будет отключена.

11. Команда включения приёма ARP-пакетов на VLAN-интерфейсе:

```
set interfaces ethernet <interface> vif <vlan-id> ip enable-arp-accept
```

Определяет поведение для ARP-пакетов, IP-записи которых нет в ARP-таблице. Если параметр включён, то создаются новые записи в ARP-таблице.

Ответы и запросы типа «gratuitous arp» обновляют ARP-таблицы, если параметр включён.

Если ARP-таблица содержит IP-адрес кадра «gratuitous arp», то ARP-таблица обновится независимо от того, включён или выключен этот параметр.

12. Команда включения анонсирования ARP-пакетов на VLAN-интерфейсе:

```
set interfaces ethernet <interface> vif <vlan-id> ip enable-arp-announce
```

13. Команда установки режима отправки ответов на ARP-запросы, разрешённые локальными целевыми IP-адресами:

```
set interfaces ethernet <interface> vif <vlan-id> ip enable-arp-ignore
```

Если целевой IP-адрес является локальным адресом, настроенным на входящем интерфейсе, ответ на ARP-запрос будет отправлен.

Если параметр отключён, то ответ будет отправлен для любого локального целевого IP-адреса, настроенного на любом интерфейсе. Применяется по умолчанию.

14. Команда включения ARP-прокси на VLAN-интерфейсе:

```
set interfaces ethernet <interface> vif <vlan-id> ip enable-proxy-arp
```

ARP-прокси позволяет интерфейсу отвечать собственным MAC-адресом на ARP-запросы для IP-адресов назначения в подсетях, подключённых к другим интерфейсам в системе.

15. Команда включения разрешения возвращать ARP-прокси-ответы на тот же интерфейс, с которого был получен ARP-запрос:

```
set interfaces ethernet <interface> vif <vlan-id> ip proxy-arp-pvlan
```

16. Команда включения политики проверки источника по обратному пути на VLAN-интерфейсе:

```
set interfaces ethernet <interface> vif <vlan-id> ip source-validation <strict | loose | disable>
```

где:

- **<strict>** – входящий пакет проверяется по FIB, и если интерфейс не является наилучшим обратным путём, то проверка пакета завершится неудачей. По умолчанию неудачные пакеты отбрасываются;
- **<loose>** – адрес источника входящего пакета проверяется по FIB, и если адрес источника не достижим ни через один интерфейс, проверка пакета завершится неудачей;
- **<disable>** – нет проверки источника.

Рекомендуется включать строгий режим для предотвращения подмены IP-адресов в результате DDoS-атак. При использовании асимметричной или другой сложной маршрутизации рекомендуется использовать свободный режим.

17. Команда включения механизма получения IPv6-адреса с помощью протокола «Neighbor Discovery Protocol» через ICMPv6-сообщения об обнаружении маршрутизатора на VLAN-интерфейсе:

```
set interfaces ethernet <interface> vif <vlan-id> ipv6 address autoconf
```

Примечание:

Данный режим автоматически отключает пересылку IPv6-трафика на указанном интерфейсе.

18. Команда удаления локального IPv6-адреса по умолчанию для VLAN-интерфейса:

```
set interfaces ethernet <interface> vif <vlan-id> ipv6 address no-default-link-local
```

19. Команда изменения системного имени устройства, передаваемого DHCP-серверу:

```
set interfaces ethernet <interface> vif <vlan-id> dhcp-options host-name  
<hostname>
```

где **<hostname>** – новое имя хоста, отправляемое взамен реального имени хоста системы на DHCP-сервер.

3.1.4 SPAN

Функция зеркалирования интерфейсов в **ARMA Стена** позволяет копировать входящий и исходящий трафик интерфейса на другой интерфейс. Функция используется для анализа трафика и должна поддерживаться принимающим устройством, например, коммутатором.

Для настройки зеркалирования интерфейса для входящего трафика необходимо ввести команду:

```
set interfaces ethernet eth1 mirror ingress eth3
```

Входящий трафик на интерфейсе «eth1» копируется на интерфейс «eth3». Интерфейсы приведены в качестве примера.

Для настройки зеркалирования интерфейса для исходящего трафика необходимо ввести команду:

```
set interfaces ethernet eth1 mirror egress eth3
```

Исходящий трафик на интерфейсе «eth1» копируется на интерфейс «eth3». Интерфейсы приведены в качестве примера.

Примечание:

Невозможно назначить сетевой мост для зеркалирования трафика сетевого интерфейса, если данный интерфейс является участником этого сетевого моста.

Примечание:

Зеркалирование трафика на субинтерфейс VLAN сетевого интерфейса не может быть реализовано даже при применении промежуточных этапов перенаправления трафика.

3.2 Сетевой мост

Сетевой мост – это сетевое устройство, предназначенное для объединения сегментов сети передачи данных в единую сеть. Он функционирует на канальном уровне модели OSI, обеспечивая прозрачное прохождение протоколов через него.

Примечание:

В системе **ARMA Стена** функциональность протокола STP по умолчанию выключена.

Для создания сетевого моста необходимо выполнить следующие действия:

1. Для включения функции «STP» следует ввести команду:

```
set interfaces bridge br0 stp
```

где **«br0»** – имя сетевого интерфейса.

2. Для добавления интерфейсов-участников моста «br0» следует ввести следующие команды:

```
set interfaces bridge br0 member interface eth0  
set interfaces bridge br0 member interface eth1
```

3. Для назначения MAC-адреса для моста «br0» следует ввести команду:

```
set interfaces bridge br0 mac 00:11:11:00:22:22
```

где **«00:11:11:00:22:22»** – MAC-адрес.

3.2.1 Основные настройки

1. Команда создания сетевого моста:

```
set interfaces bridge <brN>
```

где **<brN>** – имя сетевого моста. Оно должно иметь вид «brN», где N представляет собой уникальный идентификатор сетевого моста. Возможно указать идентификатор в диапазоне от «0» до «999999999999».

2. Команда добавления сетевого интерфейса в состав сетевого моста:

```
set interfaces bridge <brN> member interface <member>
```

где **<member>** – имя сетевого интерфейса. На сетевом интерфейсе не должно быть настроек конфигурации IP-адреса перед добавлением его в сетевой мост. Поддерживаемые типы сетевых интерфейсов: Ethernet, Bond/Link Aggregation, L2TPv3, OpenVPN, VXLAN, WLAN/WIFI - Wireless LAN, Tunnel, GENEVE.

Примечание:

Один и тот же сетевой интерфейс может быть участником только одного сетевого моста.

Примечание:

Нельзя назначить сетевой интерфейс на сетевой мост, если данный интерфейс настроен на зеркалирование трафика на этот сетевой мост.

Примечание:

При изменении участников сетевого моста с включённой поддержкой VLAN не допускается указывать интерфейсы, которые имеют дочерние VLAN.

3. Установить приоритет для сетевого интерфейса, который входит в состав сетевого моста:

```
set interfaces bridge <brN> member interface <member> priority <priority>
```

где **<priority>** – значение приоритета для интерфейса, входящего в состав сетевого моста. Возможно указать значение в диапазоне от «1» до «63».

4. Установить стоимость для сетевого интерфейса, который входит в состав сетевого моста:

```
set interfaces bridge <brN> member interface <member> cost <cost>
```

где **<cost>** – стоимость пути для интерфейса, входящего в состав сетевого моста. Более быстрый интерфейс должен иметь меньшую стоимость. Возможно указать значение в диапазоне от «1» до «65535». Значение по умолчанию для стоимости пути рассчитывается исходя из пропускной способности канала (см. [Таблица «Соответствия пропускной способности и назначаемой по умолчанию стоимости пути»](#)).

Каждый интерфейс в мосту может иметь различную скорость передачи данных, и это значение учитывается при выборе канала связи.

Таблица «Соответствия пропускной способности и назначаемой по умолчанию стоимости пути»

Пропускная способность канала	Стоимость пути протокола STP для интерфейса
4 Mbit/s	250
10 Mbit/s	100
16 Mbit/s	62
100 Mbit/s	19
1 Gbit/s	4
2 Gbit/s	3
10 Gbit/s	2

5. Команда назначения адреса для сетевого моста:

```
set interfaces bridge <brN> address <address | dhcp | dhcpv6>
```

где **<address | dhcp | dhcpv6>** – адрес сетевого моста. Возможно указать: IPv4-адрес - **<x.x.x.x/x>**, IPv6-адрес - **<h:h:h:h:h:h:h/x>**, dhcp или dhcpv6.

6. Команда добавления описания для сетевого моста:

```
set interfaces bridge <brN> description <description>
```

где **<description>** – мнемоническое имя или описание для сетевого моста.

7. Команда отключения сетевого моста с сохранением настройки:

```
set interfaces bridge <brN> disable
```

Интерфейс будет переведён в состояние административно отключённого режима (A/D).

8. Команда отключения генерации управления потоком Ethernet:

```
set interfaces bridge <brN> disable-flow-control
```

9. Команда настройки сетевого интерфейса таким образом, чтобы он не обнаруживал изменений физического состояния канала связи, например, при отсоединении кабеля:

```
set interfaces bridge <brN> disable-link-detect
```

По умолчанию сетевые интерфейсы настроены на обнаружение изменения физического состояния канала.

10. Команда назначения MAC-адреса для сетевого моста:

```
set interfaces bridge <brN> mac <xx:xx:xx:xx:xx:xx>
```

где **<xx:xx:xx:xx:xx:xx>** – пользовательский MAC-адрес сетевого моста.

11. Команда для установки размера MTU для сетевого моста:

```
set interfaces bridge <brN> mtu <mtu>
```

где **<mtu>** – размер MTU в байтах. Возможно указать значение в диапазоне от «1280» до «16000». По умолчанию используется значение «1500».

12. Команда для установки значения TCP MSS для сетевого моста:

```
set interfaces bridge <brN> ip|ipv6 adjust-mss <mss | clamp-mss-to-pmtu>
```

где **<mss | clamp-mss-to-pmtu>** – значение TCP MSS. Возможно указать значение в диапазоне от «536» до «65535» или **<clamp-mss-to-pmtu>** – для автоматической установки правильного значения MSS.

В связи с тем, что обнаружение PMTU в сети интернет не всегда работает корректно, иногда требуется установить значение TCP MSS в соответствии с

определёнными параметрами. Это значение указывается в поле «MSS» в части параметров TCP пакета SYN. Установив значение MSS, система сообщает удалённой стороне, что не принимает пакеты размером больше этого значения. Значение MSS возможно рассчитать по формуле: $MSS = MTU - 20$ (заголовок IP) – 20 (заголовок TCP), где «MTU» – максимальный размер кадра. В результате получается значение «1452» байта для MTU 1492 байта.

13. Команда установки тайм-аута записи в ARP-кэш для сетевого моста:

```
set interfaces bridge <brN> ip arp-cache-timeout <1-86400>
```

где **<1-86400>** – тайм-аут записи в ARP-кэш в секундах. Возможно указать значение в диапазоне от «1» до «86400». По умолчанию используется значение «30».

14. Команда отключения фильтрации ARP на сетевом мосту:

```
set interfaces bridge <brN> ip disable-arp-filter
```

Если этот параметр активирован, то ядро может отвечать на запросы ARP, используя адреса с других интерфейсов. По умолчанию этот параметр деактивирован. Это позволяет иметь несколько сетевых интерфейсов в одной подсети, и ответ на ARP-запросы каждого интерфейса зависит от того, будет ли ядро маршрутизировать пакет с ARP-адресом через этот интерфейс. Для работы этой функции необходимо использовать маршрутизацию на основе источника.

15. Команда настройки поведения хоста/маршрутизатора для сетевого моста:

```
set interfaces bridge <brN> ip|ipv6 disable-forwarding
```

Интерфейс будет переведён в режим хоста, при этом переадресация IPv6 в данном интерфейсе будет отключена.

16. Команда установки различных режимов широковещательной переадресации IP-пакетов для сетевого моста:

```
set interfaces bridge <brN> ip enable-directed-broadcast
```

В случае активации данного параметра, пакеты направленной широковещательной рассылки IP, поступающие на указанный интерфейс, будут пересылаться. Если параметр не активирован (по умолчанию), пакеты направленной широковещательной рассылки IP не будут пересылаться.

17. Команда включения приёма ARP пакетов на сетевом мосту:

```
set interfaces bridge <brN> ip enable-arp-accept
```

Определяет поведение для ARP-пакетов, IP-адреса которых ещё не присутствуют в ARP-таблице. Если данная настройка включена, то создаются

новые записи в ARP-таблице. Как ответы, так и запросы типа gratuitous ARP будут вызывать обновление ARP-таблицы, если данная настройка включена. Если в ARP-таблице уже содержится IP-адрес кадра gratuitous ARP, то ARP-таблица будет обновлена независимо от того, включена или выключена данная настройка.

18. Команда включения анонсирования ARP пакетов на сетевом мосту:

```
set interfaces bridge <brN> ip enable-arp-announce
```

В случае настройки рекомендуется избегать использования локальных адресов, не принадлежащих целевой подсети для данного интерфейса. Этот режим полезен, когда целевые хосты, доступные через данный интерфейс, требуют, чтобы IP-адрес источника в ARP-запросах был частью их логической сети, настроенной на принимающем интерфейсе. При формировании запроса система проверяет все свои подсети, включающие целевой IP-адрес, и сохраняет исходный адрес, если он принадлежит такой подсети. В противном случае система выбирает адрес источника в соответствии с правилами для второго уровня.

19. Команда включения игнорирования ARP пакетов на сетевом мосту:

```
set interfaces bridge <brN> ip enable-arp-ignore
```

Данный параметр определяет режимы отправки ответов на полученные ARP-запросы, разрешающие локальные целевые IP-адреса. В случае, если параметр включён, ответ будет отправлен только в том случае, если целевой IP-адрес является локальным и настроен на входящем интерфейсе. Если параметр отключён (по умолчанию), ответ будет получен для любого локального целевого IP-адреса, настроенного на любом интерфейсе.

20. Команда включения прокси ARP на сетевом мосту:

```
set interfaces bridge <brN> ip enable-proxy-arp
```

Прокси ARP позволяет сетевому мосту отвечать собственным MAC-адресом на запросы ARP для IP-адресов назначения, находящихся в подсетях, подключённых к другим интерфейсам системы. Последующие пакеты, отправленные на эти IP-адреса назначения, перенаправляются системой соответствующим образом.

21. Команда включения прокси ARP частного VLAN на сетевом мосту:

```
set interfaces bridge <brN> ip proxy-arp-pvlan
```

22. Команда включения политики проверки источника по обратному пути:

```
set interfaces bridge <brN> ip source-validation <strict | loose | disable>
```

где **<strict | loose>** - режим проверки источника по обратному пути. Возможно указать следующие значения:

<strict> (строгий режим) - каждый входящий пакет проверяется по FIB, и если интерфейс не является наилучшим обратным путём, то проверка пакета будет неудачной. По умолчанию неудачные пакеты отбрасываются;

<loose> (свободный режим) - адрес источника каждого входящего пакета также проверяется по FIB, и если адрес источника не достижим ни через один интерфейс, проверка пакета будет неудачной;

<disable> - нет проверки источника.

В настоящее время в RFC 3704 рекомендуется использовать строгий режим для предотвращения подмены IP-адресов в результате DDoS-атак. При использовании асимметричной или другой сложной маршрутизации рекомендуется использовать свободный режим.

23. Команда включения механизма получения IPv6-адреса на сетевом мосту:

```
set interfaces bridge <brN> ipv6 address autoconf
```

Примечание:

Данный метод автоматически отключает пересылку трафика IPv6 на сетевом мосту.

24. Команда назначения уникального 64-битного IPv6-адреса на основе MAC адреса:

```
set interfaces bridge <brN> ipv6 address eui64 <prefix>
```

где **<prefix>** - IPv6-адрес в формате <h:h:h:h:h:h:h/64>.

25. Команда отключения назначения локального IPv6-адреса по умолчанию для сетевого моста:

```
set interfaces bridge <brN> ipv6 address no-default-link-local
```

26. Команда настройки функции Duplicate Address Detection (DAD) для сетевого моста:

```
set interfaces bridge <brN> ipv6 accept-dad <0-2>
```

где **<0-2>** - режим работы DAD. Возможно указать следующие значения: «0» - отключить DAD, «1» - включить DAD, «2» - включить DAD и отключить работу IPv6, если обнаружен дублированный MAC-адрес link-local. По умолчанию используется режим «1».

27. Команда настройки сообщений NS для отправки при выполнении DAD:

```
set interfaces bridge <brN> ipv6 dup-addr-detect-transmits <n>
```

где **<n>** - количество сообщений NS для отправки при выполнении DAD. Возможно указать следующие значения: «0» - отключение обнаружения дубликатов адресов (DAD), «1-n». По умолчанию используется значение «1».

28. Команда размещения сетевого моста в VRF:

```
set interfaces bridge <brN> vrf <vrf>
```

где **<vrf>** - имя VRF.

3.2.2 Настройка DHCP(v6)

1. Команда определения идентификатора для DHCP-сервера:

```
set interfaces bridge <brN> dhcp-options client-id <description>
```

Определяет идентификатор, который будет использоваться системой для идентификации себя на DHCP-сервере. В случае предоставления пользователем идентификатора, он должен использовать его во всех последующих сообщениях. Сервер, в свою очередь, должен использовать этот идентификатор для идентификации пользователя.

2. Команда для изменения системного имени системы (hostname), передаваемое DHCP-серверу:

```
set interfaces bridge <brN> dhcp-options host-name <hostname>
```

где **<hostname>** - новое имя системы.

3. Команда запроса определённого класса параметров поставщика DHCP-сервера:

```
set interfaces bridge <brN> dhcp-options vendor-class-id <vendor-id>
```

Опцию «vendor-class-id» возможно использовать для запроса у сервера определённого класса опций поставщика.

4. Команда запроса только адреса у DHCP-сервера:

```
set interfaces bridge <brN> dhcp-options no-default-route
```

При активации параметра «no-default-route» у DHCP сервера запрашивается только адрес, но не запрашивается шлюз по умолчанию.

5. Команда для установки значения расстояния по умолчанию для шлюза, отправляемого DHCP-сервером:

```
set interfaces bridge <brN> dhcp-options default-route-distance <distance>
```

где **<distance>** - расстояние для маршрута по умолчанию от DHCP-сервера. Возможно указать значение в диапазоне от «1» до «255».

6. Отклонять запросы DHCP с заданного адреса или диапазона адресов:

```
set interfaces bridge <brN> dhcp-options reject <address>
```

где **<address>** - адрес (<x.x.x.x>) и/или диапазон адресов (<x.x.x.x/x>).

7. Задать уникальный идентификатор DHCP (DUID) для сетевого моста:

```
set interfaces bridge <brN> dhcpv6-options duid <duid>
```

где **<duid>** - уникальный идентификатор DHCP в формате h[[:h]...].

Уникальный идентификатор DHCP (DUID) используется клиентом для получения IP-адреса от сервера DHCPv6. Он состоит из двухбайтового поля типа DUID и поля идентификатора переменной длины до 128 байт. Фактическая длина DUID зависит от типа. Сервер сравнивает DUID с базой данных и предоставляет клиенту необходимые данные (адрес, время аренды, DNS-серверы и т. д.).

8. Отключить отправку сообщения об освобождении адреса:

```
set interfaces bridge <brN> dhcpv6-options no-release
```

Предотвращает отправку сообщения об освобождении при выходе клиента, чтобы сохранить назначенный адрес или префикс.

9. Включить обмен с серверами только информационными настройками:

```
set interfaces bridge <brN> dhcpv6-options parameters-only
```

Параметр «parameters-only» в опции определяет, что DHCPv6 должен обмениваться с серверами только информационными настройками. Примером таких параметров является список адресов DNS-серверов. Этот параметр полезен в случае, когда системе не требуются параметры с сохранением состояния, такие как IPv6-адреса или префиксы.

10. Включить получение настроек для VLAN-интерфейса от DHCPv6-сервера:

```
set interfaces bridge <brN> dhcpv6-options rapid-commit
```

11. Запросить только временный адрес и не создавать партнёрство IANA:

```
set interfaces bridge <brN> dhcpv6-options temporary
```

3.2.3 Делегирование префиксов DHCPv6 (PD)

1. Задать размер делегируемого префикса <length> для экземпляра делегирования префикса <id> на сетевом мосту:

```
set interfaces bridge <brN> dhcpv6-options pd <id> length <length>
```

где:

- **<id>** - экземпляр префиксного делегирования. Значение должно быть больше или равное «0»;
- **<length>** - длина делегированного префикса. Возможно указать значение в диапазоне от «32» до «64». По умолчанию используется значение «64».

Некоторые провайдеры по умолчанию предоставляют префикс /64. Чтобы запросить префикс другого размера, необходимо использовать опцию для запроса большего делегирования для данного экземпляра делегирования префикса <id>. Значение этой опции должно находиться в диапазоне от 32 до 64. Таким образом, можно запросить делегирование префикса от /32 (если это позволяет провайдер) до /64.

2. Определить адрес интерфейса <address>, используемый локально на интерфейсе <delegatee>, на который был делегирован префикс:

```
set interfaces bridge <brN> dhcpv6-options pd <id> interface <delegatee> address <address>
```

3. Задать значение идентификатора агрегатора уровня сайта SLA <sla-id> на интерфейсе <delegatee>:

```
set interfaces bridge <brN> dhcpv6-options pd <id> interface <delegatee> sla-id <sla-id>
```

где **<sla-id>** - значение идентификатора агрегатора уровня сайта (SLA). Идентификатор должен представлять собой десятичное число больше 0 и соответствовать требованиям к длине идентификаторов SLA.

Пример: если идентификатор (ID) равен 1 и клиенту предоставлен IPv6-префикс 2001:db8:ffff::/48, DHCPv6 объединит эти два значения в один IPv6-префикс, 2001:db8:ffff:1::/64, и настроит этот префикс на указанном интерфейсе.

3.2.4 Настройка параметров сетевого моста

1. Определить временной интервал, по истечении которого MAC-адрес сетевого моста будет считаться неактуальным:

```
set interfaces bridge <brN> aging <time>
```

где **<time>** - интервал времени хранения, в секундах, по истечении которого MAC-адрес удаляется из таблицы пересылки. Возможно указать значение в диапазоне от «10» до «1000000». По умолчанию используется значение «300».

При значении «0» функция MAC-адресного обучения отключается (всегда используется широковещательная передача).

2. Определить временной промежуток ожидания сетевого моста пакета «hello» от корня связующего дерева:

```
set interfaces bridge <brN> max-age <time>
```

где **<time>** - интервал времени, в секундах, в течение которого сетевой мост ожидает получения пакета «hello» перед перевычислением топологии связующего дерева. Возможно указать значение в диапазоне от «6» до «40». По умолчанию используется значение «20».

3. Включить IGMP/MLD querier:

```
set interfaces bridge <brN> igmp querier
```

4. Включить IGMP/MLD snooping:

```
set interfaces bridge <brN> igmp snooping
```

3.2.5 STP

STP (Spanning Tree Protocol) – это сетевой протокол, который формирует логическую топологию без циклов для сетей Ethernet. Основная задача STP – предотвращение мостовых циклов и связанного с ними широковещательного излучения. Связующее дерево также позволяет включать в схему сети резервные каналы, обеспечивающие бесперебойную работу в случае сбоя активного канала.

Команды настройки STP:

1. Включить протокол STP на сетевом мосту:

```
set interfaces bridge <brN> stp
```

2. Установить время задержки пересылки для протокола STP:

```
set interfaces bridge <brN> forwarding-delay <delay>
```

где **<delay>** - значение времени задержки пересылки в секундах. Возможно указать значение в диапазоне от «2» до «30». По умолчанию используется значение «15».

Время задержки пересылки – это время, в течение которого устройство находится в состоянии прослушивания и обучения перед переходом в состояние пересылки. Это время необходимо для того, чтобы новое устройство, подключённое к загруженной сети, могло проанализировать трафик перед началом работы.

3. Установить интервал отправки hello-пакетов для протокола STP:

```
set interfaces bridge <brN> hello-time <interval>
```

где **<interval>** - значение интервала времени в секундах. Возможно указать значение в диапазоне от «1» до «10». По умолчанию используется значение «2».

Корневой мост и назначенные мосты периодически отправляют приветственный пакет, который используется для передачи информации о топологии по всей мостовой локальной сети.

3.2.6 VLAN

В системе **ARMA Стена** интерфейсы 802.1q представлены в виде виртуальных интерфейсов, которые подчиняются физическому интерфейсу. Для обозначения таких интерфейсов используется термин «**vif**».

Примечание:

Не рекомендуется использовать параметр `vif 1` для мостов, поддерживающих VLAN, поскольку такие мосты предполагают, что все немаркированные пакеты принадлежат участнику VLAN 1 по умолчанию, а идентификатор VLAN родительского интерфейса моста всегда равен 1.

Для активации сетевого моста с поддержкой VLAN, необходимо активировать соответствующий параметр, который позволит использовать настройки VLAN для данного моста:

```
set interfaces bridge <brN> enable-vlan
```

Примечание:

В случае если интерфейсы, участвующие в сетевом мосту, имеют дочерние VLAN-интерфейсы, то функция поддержки VLAN на этом мосту будет недоступна.

Установить тип интерфейса моста:

```
set interfaces bridge <brN> protocol <802.1ad|802.1q>
```

где **<802.1ad|802.1q>** - тип интерфейса моста. Возможно указать следующие значения: «802.1q» или «802.1ad». По умолчанию используется значение «802.1q».

3.2.6.1 Основные настройки

1. Создать новый VLAN-интерфейс на сетевом мосту <brN>, используя номер VLAN, указанный через <vlan-id>:

```
set interfaces bridge <brN> vif <vlan-id>
```


где **<vlan-id>** - номер VLAN. Возможно указать значение в диапазоне от «0» до «4094». На одном физическом интерфейсе возможно создать несколько VLAN-интерфейсов.

Примечание:

На интерфейсах vif принимаются только пакеты с метками 802.1Q.

2. Установить адрес для VLAN-интерфейса:

```
set interfaces bridge <brN> vif <vlan-id> address <address | dhcp | dhcpv6>
```

где **<address | dhcp | dhcpv6>** – адрес сетевого моста. Возможно указать: IPv4-адрес - <x.x.x.x/x>, IPv6-адрес - <h:h:h:h:h:h:h/x>, dhcp или dhcpv6.

3. Задать описание для VLAN-интерфейса:

```
set interfaces bridge <brN> description <description>
```

где **<description>** – мнемоническое имя или описание для VLAN-интерфейса.

4. Команда отключения VLAN-интерфейса с сохранением настройки:

```
set interfaces bridge <brN> vif <vlan-id> disable
```

Интерфейс будет переведён в состояние административно отключённого режима (A/D).

5. Команда настройки VLAN-интерфейса таким образом, чтобы он не обнаруживал изменений физического состояния канала связи, например, при отсоединении кабеля:

```
set interfaces bridge <brN> vif <vlan-id> disable-link-detect
```

По умолчанию VLAN-интерфейс настроен на обнаружение изменения физического состояния канала.

6. Команда назначения MAC-адреса для VLAN-интерфейса:

```
set interfaces bridge <brN> vif <vlan-id> mac <xx:xx:xx:xx:xx:xx>
```

где **<xx:xx:xx:xx:xx:xx>** – пользовательский MAC-адрес VLAN-интерфейса.

7. Команда для установки размера MTU для VLAN-интерфейса:

```
set interfaces bridge <brN> vif <vlan-id> mtu <mtu>
```

где **<mtu>** – размер MTU в байтах. Возможно указать значение в диапазоне от «68» до «16000».

8. Команда для установки значения TCP MSS для VLAN-интерфейса:

```
set interfaces bridge <brN> vif <vlan-id> ip|ipv6 adjust-mss <mss | clamp-mss-to-pmtu>
```

где **<mss | clamp-mss-to-pmtu>** – значение TCP MSS. Возможно указать значение в диапазоне от «536» до «65535» или **<clamp-mss-to-pmtu>** - для автоматической установки правильного значения MSS.

9. Команда установки тайм-аут записи в ARP-кэш для VLAN-интерфейса:

```
set interfaces bridge <brN> vif <vlan-id> ip arp-cache-timeout <1-86400>
```

где **<1-86400>** – тайм-аут записи в ARP-кэш в секундах. Возможно указать значение в диапазоне от «1» до «86400». По умолчанию используется значение «30».

10. Команда отключения фильтрации ARP на VLAN-интерфейсе:

```
set interfaces bridge <brN> vif <vlan-id> ip disable-arp-filter
```

Если этот параметр активирован, то ядро может отвечать на запросы ARP, используя адреса с других интерфейсов. По умолчанию этот параметр деактивирован. Это позволяет иметь несколько сетевых интерфейсов в одной подсети, и ответ на ARP-адреса каждого интерфейса зависит от того, будет ли ядро маршрутизировать пакет с ARP-адресом через этот интерфейс. Для работы этой функции необходимо использовать маршрутизацию на основе источника.

11. Команда настройки поведения хоста/маршрутизатора для VLAN-интерфейса:

```
set interfaces bridge <brN> vif <vlan-id> ip disable-forwarding
```

Интерфейс будет переведён в режим хоста, при этом переадресация IPv6 в данном интерфейсе будет отключена.

12. Команда установки различных режимов широковещательной переадресации IP-пакетов для VLAN-интерфейса:

```
set interfaces bridge <brN> vif <vlan-id> ip enable-directed-broadcast
```

В случае активации данного параметра, пакеты направленной широковещательной рассылки IP, поступающие на указанный интерфейс, будут пересылаться. Если параметр не активирован (по умолчанию), пакеты направленной широковещательной рассылки IP не будут пересылаться.

13. Команда включения приёма ARP пакетов на VLAN-интерфейсе:

```
set interfaces bridge <brN> vif <vlan-id> ip enable-arp-accept
```

Определяет поведение для ARP-пакетов, IP-адреса которых ещё не присутствуют в ARP-таблице. Если данная настройка включена, то создаются

новые записи в ARP-таблице. Как ответы, так и запросы типа gratuitous ARP будут вызывать обновление ARP-таблицы, если данная настройка включена. Если в ARP-таблице уже содержится IP-адрес кадра gratuitous ARP, то ARP-таблица будет обновлена независимо от того, включена или выключена данная настройка.

14. Команда включения анонсирования ARP пакетов на VLAN-интерфейсе:

```
set interfaces bridge <brN> vif <vlan-id> ip enable-arp-announce
```

В случае настройки рекомендуется избегать использования локальных адресов, не принадлежащих целевой подсети для данного интерфейса. Этот режим полезен, когда целевые хосты, доступные через данный интерфейс, требуют, чтобы IP-адрес источника в ARP-запросах был частью их логической сети, настроенной на принимающем интерфейсе. При формировании запроса система проверяет все свои подсети, включающие целевой IP-адрес, и сохраняет исходный адрес, если он принадлежит такой подсети. В противном случае система выбирает адрес источника в соответствии с правилами для второго уровня.

15. Команда включения игнорирования ARP пакетов на VLAN-интерфейсе:

```
set interfaces bridge <brN> vif <vlan-id> ip enable-arp-ignore
```

Данный параметр определяет режимы отправки ответов на полученные ARP-запросы, разрешающие локальные целевые IP-адреса. В случае, если параметр включён, ответ будет отправлен только в том случае, если целевой IP-адрес является локальным и настроен на входящем интерфейсе. Если параметр отключён (по умолчанию), ответ будет получен для любого локального целевого IP-адреса, настроенного на любом интерфейсе.

16. Команда включения прокси ARP на VLAN-интерфейсе:

```
set interfaces bridge <brN> vif <vlan-id> ip enable-proxy-arp
```

Прокси ARP позволяет VLAN-интерфейсу отвечать собственным MAC-адресом на запросы ARP для IP-адресов назначения, находящихся в подсетях, подключённых к другим интерфейсам системы. Последующие пакеты, отправленные на эти IP-адреса назначения, перенаправляются системой соответствующим образом.

17. Команда включения прокси ARP частного VLAN на VLAN-интерфейсе:

```
set interfaces bridge <brN> vif <vlan-id> ip proxy-arp-pvlan
```

Прокси-сервер ARP отвечает на запросы того же интерфейса, от которого был получен запрос ARP. Это сделано для поддержки функций коммутатора (ethernet), таких как RFC 3069, где отдельным портам запрещено

взаимодействовать друг с другом, но разрешено взаимодействовать с вышестоящим маршрутизатором. Как описано в RFC 3069, возможно разрешить этим хостам взаимодействовать через вышестоящий маршрутизатор с помощью прокси ARP.

18. Команда включения политики проверки источника по обратному пути:

```
set interfaces bridge <brN> vif <vlan-id> ip source-validation <strict | loose | disable>
```

где **<strict | loose>** - режим проверки источника по обратному пути. Возможно указать следующие значения:

<strict> (строгий режим) - каждый входящий пакет проверяется по FIB, и если интерфейс не является наилучшим обратным путём, то проверка пакета будет неудачной. По умолчанию неудачные пакеты отбрасываются;

<loose> (свободный режим) - адрес источника каждого входящего пакета также проверяется по FIB, и если адрес источника не достижим ни через один интерфейс, проверка пакета будет неудачной;

<disable> - нет проверки источника.

В настоящее время в RFC 3704 рекомендуется использовать строгий режим для предотвращения подмены IP-адресов в результате DDoS-атак. При использовании асимметричной или другой сложной маршрутизации рекомендуется использовать свободный режим.

19. Команда включения механизма получения IPv6-адреса на VLAN-интерфейсе:

```
set interfaces bridge <brN> vif <vlan-id> ipv6 address autoconf
```

Примечание:

Данный метод автоматически отключает пересылку трафика IPv6 на VLAN-интерфейсе.

20. Команда назначения уникального 64-битного IPv6-адреса на основе MAC адреса:

```
set interfaces bridge <brN> vif <vlan-id> ipv6 address eui64 <prefix>
```

где **<prefix>** - IPv6-адрес в формате <h:h:h:h:h:h:h/64>.

21. Команда отключения назначения локального IPv6-адреса по умолчанию для VLAN-интерфейса:

```
set interfaces bridge <brN> vif <vlan-id> ipv6 address no-default-link-local
```

22. Команда отключения IP переадресации на VLAN-интерфейсе:

```
set interfaces bridge <brN> vif <vlan-id> ipv6 disable-forwarding
```

Интерфейс будет переведён в режим хоста, а переадресация IPv6 на данном интерфейсе будет отключена.

23. Команда настройки функции Duplicate Address Detection (DAD) для VLAN-интерфейса:

```
set interfaces bridge <brN> vif <vlan-id> ipv6 accept-dad <0-2>
```

где **<0-2>** - режим работы DAD. Возможно указать следующие значения: «0» - отключить DAD, «1» - включить DAD, «2» - включить DAD и отключить работу IPv6, если обнаружен дублированный MAC-адрес link-local. По умолчанию используется режим «1».

24. Команда настройки сообщений NS для отправки при выполнении DAD:

```
set interfaces bridge <brN> vif <vlan-id> ipv6 dup-addr-detect-transmits <n>
```

где **<n>** - количество сообщений NS для отправки при выполнении DAD. Возможно указать следующие значения: «0» - отключение обнаружения дубликатов адресов (DAD), «1-n». По умолчанию используется значение «1».

25. Команда размещения VLAN-интерфейса в VRF:

```
set interfaces bridge <brN> vif <vlan-id> vrf <vrf>
```

где **<vrf>** - имя VRF.

26. Установить собственный флаг идентификатора VLAN для интерфейса:

```
set interfaces bridge <brN> member interface <member> native-vlan <id>
```

где:

- **<id>** - номер VLAN. Возможно указать значение в диапазоне от «0» до «4094»;
- **<member>** - имя интерфейса.

При поступлении пакета данных без тега VLAN на порт, пакет данных будет вынужден получить тег с определённым идентификатором VLAN. При выходе флага идентификатора VLAN из порта, тег идентификатора VLAN будет удалён.

27. Передавать определённые идентификаторы VLAN через интерфейс участника моста:

```
set interfaces bridge <brN> member interface <member> allowed-vlan <id>
```

Это может быть отдельный идентификатор VLAN (<id>) или диапазон идентификаторов VLAN, разделённых дефисом (<idN>-<idM>).

3.2.6.2 Настройка DHCP(v6)

1. Команда определения идентификатора для DHCP-сервера:

```
set interfaces bridge <brN> vif <vlan-id> dhcp-options client-id <description>
```

Определяет идентификатор, который будет использоваться системой для идентификации себя на DHCP-сервере. В случае предоставления пользователем идентификатора, он должен использовать его во всех последующих сообщениях. Сервер, в свою очередь, должен использовать этот идентификатор для идентификации пользователя.

2. Команда для изменения системного имени системы (hostname), передаваемое DHCP-серверу:

```
set interfaces bridge <brN> vif <vlan-id> dhcp-options host-name <hostname>
```

где **<hostname>** - новое имя системы.

3. Команда запроса определённого класса параметров поставщика DHCP-сервера:

```
set interfaces bridge <brN> vif <vlan-id> dhcp-options vendor-class-id <vendor-id>
```

Опцию «vendor-class-id» возможно использовать для запроса у сервера определённого класса опций поставщика.

4. Команда запроса только адреса у DHCP-сервера:

```
set interfaces bridge <brN> vif <vlan-id> dhcp-options no-default-route
```

При активации параметра «no-default-route» у DHCP сервера запрашивается только адрес, но не запрашивается шлюз по умолчанию.

5. Команда для установки значения расстояния по умолчанию для шлюза, отправляемого DHCP-сервером:

```
set interfaces bridge <brN> vif <vlan-id> dhcp-options default-route-distance <distance>
```

где **<distance>** - расстояние для маршрута по умолчанию от DHCP-сервера. Возможно указать значение в диапазоне от «1» до «255».

6. Отклонять запросы DHCP с заданного адреса или диапазона адресов:

```
set interfaces bridge <brN> vif <vlan-id> dhcp-options reject <address>
```

где **<address>** - адрес (<x.x.x.x>) и/или диапазон адресов (<x.x.x.x/x>).

7. Задать уникальный идентификатор DHCP (DUID) для сетевого моста:

```
set interfaces bridge <brN> vif <vlan-id> dhcpv6-options duid <duid>
```

где **<duid>** - уникальный идентификатор DHCP в формате h[[:h]...].

Уникальный идентификатор DHCP (DUID) используется клиентом для получения IP-адреса от сервера DHCPv6. Он состоит из двухбайтового поля типа DUID и поля идентификатора переменной длины до 128 байт. Фактическая длина DUID зависит от типа. Сервер сравнивает DUID с базой данных и предоставляет клиенту необходимые данные (адрес, время аренды, DNS-серверы и т. д.).

8. Отключить отправку сообщения об освобождении адреса:

```
set interfaces bridge <brN> vif <vlan-id> dhcpv6-options no-release
```

Предотвращает отправку сообщения об освобождении при выходе клиента, чтобы сохранить назначенный адрес или префикс.

9. Включить обмен с серверами только информационными настройками:

```
set interfaces bridge <brN> vif <vlan-id> dhcpv6-options parameters-only
```

Параметр «parameters-only» в опции определяет, что DHCPv6 должен обмениваться с серверами только информационными настройками. Примером таких параметров является список адресов DNS-серверов. Этот параметр полезен в случае, когда системе не требуются параметры с сохранением состояния, такие как IPv6-адреса или префиксы.

10. Включить получение настроек для VLAN-интерфейса от DHCPv6-сервера:

```
set interfaces bridge <brN> vif <vlan-id> dhcpv6-options rapid-commit
```

11. Запросить только временный адрес и не создавать партнёрство IANA:

```
set interfaces bridge <brN> vif <vlan-id> dhcpv6-options temporary
```

3.2.6.3 Делегирование префиксов DHCPv6 (PD)

1. Задать размер делегируемого префикса <length> для экземпляра делегирования префикса <id> на сетевом мосту:

```
set interfaces bridge <brN> vif <vlan-id> dhcpv6-options pd <id> length <length>
```

где:

- **<id>** - экземпляр префиксного делегирования. Значение должно быть больше или равное «0»;
- **<length>** - длина делегированного префикса. Возможно указать значение в диапазоне от «32» до «64». По умолчанию используется значение «64».

Некоторые провайдеры по умолчанию предоставляют префикс /64. Чтобы запросить префикс другого размера, необходимо использовать опцию для запроса большего делегирования для данного экземпляра делегирования префикса <id>. Значение этой опции должно находиться в диапазоне от 32 до 64. Таким образом, можно запросить делегирование префикса от /32 (если это позволяет провайдер) до /64.

2. Определить адрес интерфейса <address>, используемый локально на интерфейсе <delegatee>, на который был делегирован префикс:

```
set interfaces bridge <brN> vif <vlan-id> dhcpv6-options pd <id> interface  
<delegatee> address <address>
```

Адрес интерфейса будет объединён с делегированным префиксом и идентификатором SLA для формирования полного адреса интерфейса. По умолчанию используется адрес EUI-64 интерфейса.

3. Задать значение идентификатора агрегатора уровня сайта SLA <sla-id> на интерфейсе <delegatee>:

```
set interfaces bridge <brN> vif <vlan-id> dhcpv6-options pd <id> interface  
<delegatee> sla-id <id>
```

где **<sla-id>** - значение идентификатора агрегатора уровня сайта (SLA). Идентификатор должен представлять собой десятичное число больше 0 и соответствовать требованиям к длине идентификаторов SLA.

Пример: если идентификатор (ID) равен 1 и клиенту предоставлен IPv6-префикс 2001:db8:ffff::/48, DHCPv6 объединит эти два значения в один IPv6-префикс, 2001:db8:ffff:1::/64, и настроит этот префикс на указанном интерфейсе.

3.3 Агрегированный интерфейс

Механизм агрегирования каналов (Link Aggregation Control Protocol - LACP) объединяет несколько физических интерфейсов в один логический (агрегированный) интерфейс. Поведение связанных интерфейсов зависит от выбранного режима работы. В общем случае режимы обеспечивают либо горячее резервирование, либо балансировку нагрузки. Также может осуществляться мониторинг состояния канала.

Создание агрегированного интерфейса возможно только из неконфигурированных интерфейсов.

3.3.1 Конфигурирование

3.3.1.1 Основные настройки интерфейса

1. Создание агрегированного интерфейса и назначение ему IP-адрес:


```
set interfaces bonding <bond1> address <address | dhcp | dhcpv6>
```

где:

- **<bond1>** – идентификатор интерфейса агрегированных каналов, приведён в качестве примера. Имя агрегированного интерфейса должно соответствовать формату «bondN», где N - числовой идентификатор;
- **<address | dhcp | dhcpv6>** – IP-адрес для интерфейса агрегированных каналов. IP-адрес возможно указать несколько раз как IPv4 и/или IPv6 адрес в формате <x.x.x.x/x> и/или <h:h:h:h:h:h:h/x>. Возможно получение адреса по протоколу DHCP и/или DHCPv6.

2. Установка описание для интерфейса агрегированных каналов:

```
set interfaces bonding <bondN> description <description>
```

где **<description>** - описание группы агрегирования.

3. Отключение интерфейса агрегированных каналов с сохранением настроек:

```
set interfaces bonding <bondN> disable
```

Интерфейс будет переведён в состояние административного отключения (A/D).

4. Добавить сетевой интерфейс в состав интерфейса агрегированных каналов:

```
set interfaces bonding <bondN> member interface <member>
```

где **<member>** - сетевой интерфейс.

Примечание:

В случае, если на добавляемом интерфейсе установлен параметр **hw_id_auto_pinning**, то при применении настроек возникает ошибка **«Cannot add interface «ethN» to bond, it has a «hw_id_auto_pinning» assigned!»**. Для устранения этой ошибки необходимо удалить ветку **hw_id_auto_pinning** на данном интерфейсе, используя команду *«delete interfaces ethernet ethN hw_id_auto_pinning»*.

Если на добавляемом интерфейсе ранее был удалён параметр **hw_id**, то при применении настроек возникает ошибка **«Cannot add interface «ethN» to bond, it has a «» assigned!»**. Для исправления этой ошибки необходимо добавить в интерфейс ethN удалённый параметр **hw_id**, используя команду *«set interfaces ethernet ethN hw_id <xx:xx:xx:xx:xx:xx>»*.

5. Отключение генерации управления потоком Ethernet (кадров паузы):

```
set interfaces bonding <bondN> disable-flow-control
```

Передающая станция, будь то компьютер или сетевой коммутатор, может передавать данные с более высокой скоростью, чем принимающая станция способна обработать. Чтобы избежать перегрузки, принимающая сторона может использовать механизм управления потоком. Этот механизм уведомляет отправителя о необходимости приостановить передачу данных до тех пор, пока принимающая станция не будет готова их принять.

6. Отключение обнаружения изменений физического состояния канала связи:

```
set interfaces bonding <bondN> disable-link-detect
```

С помощью данной команды возможно настроить сетевой интерфейс таким образом, чтобы он не обнаруживал изменений физического состояния канала связи, например, при отсоединении кабеля. По умолчанию установлен параметр, который фиксирует такие изменения.

7. Установка MAC-адреса интерфейса агрегированных каналов:

```
set interfaces bonding <bondN> mac <xx:xx:xx:xx:xx:xx>
```

где **<xx:xx:xx:xx:xx:xx>** - MAC-адрес для интерфейса агрегированных каналов. По умолчанию используется MAC-адрес первого интерфейса, добавленного в интерфейс агрегированных каналов.

8. Установка значения MTU для интерфейса агрегированных каналов:

```
set interfaces bonding <bondN> mtu <mtu>
```

где **<mtu>** - значение MTU для интерфейса агрегированных каналов. Возможно указать значение в диапазоне от «68» до «9190».

9. Установка значения TCP MSS:

```
set interfaces bonding <bondN> ip adjust-mss <mss | clamp-mss-to-pmtu>
```

где:

- **<mss>** - значение MSS. Возможно указать значение в диапазоне от «536» до «65535».
- **<clamp-mss-to-pmtu>** - автоматически устанавливать MSS в нужное значение.

Поскольку обнаружение PMTU в сети Интернет работает нестабильно, иногда возникает необходимость ограничить значение TCP MSS. Это поле находится в опциях TCP в части SYN-пакета. Установив значение MSS, система сообщает удалённой стороне, что не следует отправлять пакеты размером больше этого значения.

10. Установка тайм-аута записи в ARP-кэш для интерфейса агрегированных каналов:

```
set interfaces bonding <bondN> ip arp-cache-timeout <1-86400>
```

где **<1-86400>** - значение тайм-аута записи в ARP-кэш в секундах. Возможно указать значение в диапазоне от «1» до «86400». По умолчанию используется значение «30».

11. Отключить фильтрацию ARP на интерфейсе агрегированных каналов:

```
set interfaces bonding <bondN> ip disable-arp-filter
```

Если параметр не установлен (по умолчанию), это позволяет иметь несколько сетевых интерфейсов в одной подсети и отвечать на ARP для каждого интерфейса в зависимости от того, будет ли ядро направлять пакет с IP-адресом ARP через этот интерфейс. Для этого необходимо использовать маршрутизацию на основе источника.

12. Отключить переадресацию IP на интерфейсе агрегированных каналов:

```
set interfaces bonding <bondN> ip disable-forwarding
```

Если параметр установлен, интерфейс переходит в режим хоста, и переадресация IPv6 на этом интерфейсе отключается.

13. Включить направленную широковещательную пересылку на интерфейсе агрегированных каналов:

```
set interfaces bonding <bondN> ip enable-directed-broadcast
```

В случае активации данной опции, входящие пакеты направленной широковещательной рассылки IP будут перенаправляться через указанный интерфейс. В случае если данный параметр не задан (по умолчанию), входящие пакеты направленной широковещательной рассылки IP не будут передаваться.

14. Включить приём ARP пакетов на интерфейсе агрегированных каналов:

```
set interfaces bonding <bondN> ip enable-arp-accept
```

Определяет поведение для ARP-пакетов, IP-записи которых ещё не присутствуют в ARP-таблице. Если эта настройка включена, то создаются новые записи в ARP-таблице. Как ответы, так и запросы типа Gratuitous ARP будут вызывать обновление ARP-таблицы, если эта настройка включена. Если в ARP-таблице уже содержится IP-адрес кадра Gratuitous ARP, то ARP-таблица будет обновлена независимо от того, включена или выключена эта настройка.

15. Включить анонсирование ARP пакетов на интерфейсе агрегированных каналов:

```
set interfaces bonding <bondN> ip enable-arp-announce
```

Если параметр не задан, используется любой локальный адрес, который настроен на любом интерфейсе. Если параметр установлен, рекомендуется избегать использования локальных адресов, которые не входят в подсеть цели для данного интерфейса. Этот режим полезен, когда целевые узлы, доступные через данный интерфейс, требуют, чтобы IP-адрес источника в ARP-запросах был частью их логической сети, настроенной на принимающем интерфейсе. При генерации запроса система проверяет все подсети, включающие целевой IP-адрес, и сохраняем адрес источника, если он принадлежит такой подсети. Если подходящей подсети не найдено, система выбирает адрес источника в соответствии с правилами для уровня 2.

16. Включить игнорирование ARP пакетов на интерфейсе агрегированных каналов:

```
set interfaces bonding <bondN> ip enable-arp-ignore
```

Данный параметр определяет режимы отправки ответов на ARP-запросы, которые разрешают локальные целевые IP-адреса. Если параметр включён, ответ будет отправлен только в том случае, если целевой IP-адрес является локальным адресом, настроенным на входящем интерфейсе. Если параметр отключён (по умолчанию), ответ будет получен для любого локального целевого IP-адреса, настроенного на любом интерфейсе.

17. Включить прокси ARP на интерфейсе агрегированных каналов:

```
set interfaces bonding <bondN> ip enable-proxy-arp
```

Прокси ARP позволяет интерфейсу Ethernet отвечать своим MAC-адресом на ARP-запросы IP-адресов назначения в подсетях, подключённых к другим интерфейсам системы. Последующие пакеты, отправленные на эти IP-адреса назначения, пересылаются системой соответствующим образом.

18. Включить прокси ARP частного VLAN на интерфейсе агрегированных каналов:

```
set interfaces bonding <bondN> ip proxy-arp-pvlan
```

Разрешить ответы ARP-прокси с того же интерфейса, с которого был получен ARP-запрос или запрос на предложение. Это необходимо для поддержки функций Ethernet-коммутаторов, описанных в RFC 3069, где отдельные порты не могут напрямую связываться друг с другом, но могут связываться с вышестоящим маршрутизатором. Как указано в RFC 3069, этого можно достичь путём включения прокси-ARP.

Необязательно использовать вместе с `proxy_arp`.

19. Включить политику проверки источника по обратному пути, как указано в RFC 3704:

```
set interfaces bonding <bondN> ip source-validation <strict | loose | disable>
```

где **<strict | loose | disable>** - режим проверки источника. Возможно указать следующие значения:

- **strict** - каждый входящий пакет проверяется по FIB, и если интерфейс не является наилучшим обратным путём, то проверка пакета будет неудачной. По умолчанию неудачные пакеты отбрасываются.
- **loose** - адрес источника каждого входящего пакета также проверяется по FIB, и если адрес источника не достижим ни через один интерфейс, проверка пакета будет неудачной.
- **disable** - нет проверки источника.

В настоящее время в RFC 3704 рекомендуется включать strict режим для предотвращения подмены IP-адресов в результате DDos атак. При использовании асимметричной или другой сложной маршрутизации рекомендуется использовать loose режим.

20. Включить получение IPv6-адреса с помощью автоконфигурации без статического изменения (SLAAC):

```
set interfaces bonding <bondN> ipv6 address autoconf
```

В соответствии с RFC 4862, хосты IPv6 могут автоматически настраиваться при подключении к сети IPv6 с использованием протокола Neighbor Discovery Protocol (NDP) через сообщения ICMPv6 об обнаружении маршрутизатора. При первом подключении к сети хост отправляет многоадресный запрос link-local router solicitation для получения параметров конфигурации. Маршрутизаторы отвечают на этот запрос пакетом router advertisement, содержащим параметры конфигурации уровня Интернета.

Примечание:

Данный метод автоматически отключает пересылку трафика IPv6 на сетевом интерфейсе.

21. Включить префикс EUI-64 на основе MAC адреса для IPv6 адреса интерфейса агрегированных каналов:

```
set interfaces bonding <bondN> ipv6 address eui64 <prefix>
```

где **<prefix>** - сеть IPv6 в формате <h:h:h:h:h:h:h/64>.

22. Удалить локальный адрес IPv6 по умолчанию для интерфейса агрегированных каналов:

```
set interfaces bonding <bondN> ipv6 address no-default-link-local
```

23. Отключить IP переадресацию на интерфейсе агрегированных каналов:

```
set interfaces bonding <bondN> ipv6 disable-forwarding
```

В случае установки, интерфейс будет переведён в режим хоста, а переадресация IPv6 на данном интерфейсе будет отключена.

24. Установить значения TCP MSS:

```
set interfaces bonding <bondN> ipv6 adjust-mss <mss | clamp-mss-to-pmtu>
```

где:

- **<mss>** - значение MSS. Возможно указать значение в диапазоне от «536» до «65535».
- **<clamp-mss-to-pmtu>** - автоматически устанавливать MSS в нужное значение.

25. Принимать обнаружение дублирующегося адреса:

```
set interfaces bonding <bondN> ipv6 accept-dad <0-2>
```

где **<0-2>** - режим приёма DAD. Возможно указать следующие значения:

- **0** - отключить DAD;
- **1** - включить DAD (по умолчанию);
- **2** - включить DAD и отключить работу IPv6, если обнаружен дублированный MAC-адрес link-local.

26. Установить количество сообщений NS для отправки при выполнении DAD:

```
set interfaces bonding <bondN> ipv6 dup-addr-detect-transmits <n>
```

где **<n>** - количество NS-сообщений. В случае установки значения «0», функция обнаружения дубликатов адресов (DAD) будет отключена. По умолчанию используется значение «1».

27. Разместить интерфейс агрегированных каналов в указанном экземпляре VRF:

```
set interfaces bonding <bondN> vrf <vrf>
```

где **<vrf>** - имя экземпляра VRF.

3.3.1.2 Настройки получения адреса по DHCP(v6)

1. Установить идентификатор, используемый клиентом для идентификации себя DHCP сервером:

```
set interfaces bonding <bondN> dhcp-options client-id <description>
```

где **<description>** - значение идентификатора.

В случае предоставления идентификатора пользователь обязан использовать один и тот же идентификатор во всех последующих сообщениях.

2. Изменить системное имя устройства, передаваемое DHCP серверу:

```
set interfaces bonding <bondN> dhcp-options host-name <hostname>
```

где **<hostname>** - новое системное имя хоста, передаваемое DHCP серверу.

Вместо передачи реального системного имени хоста на DHCP-сервер будет передано заданное значение в качестве имени хоста.

3. Определить тип клиента поставщика для DHCP-сервера:

```
set interfaces bonding <bondN> dhcp-options vendor-class-id <vendor-id>
```

где **<vendor-id>** - значение опций DHCP.

Опция «vendor-class-id» используется для запроса у сервера определённого класса опций поставщика.

4. Запросить у DHCP-сервера только адрес, не запрашивая шлюз по умолчанию:

```
set interfaces bonding <bondN> dhcp-options no-default-route
```

5. Установить значение расстояния для шлюза по умолчанию, отправляемого сервером DHCP:

```
set interfaces bonding <bondN> dhcp-options default-route-distance <distance>
```

где **<distance>** - значение расстояния для шлюза по умолчанию. Возможно указать значение в диапазоне от «1» до «255». По умолчанию используется значение «210».

6. Отклонить аренду DHCP с заданного адреса или диапазона:

```
set interfaces bonding <bondN> dhcp-options reject <address>
```

где **<address>** - IP-адрес, возможно указать несколько раз в формате <x.x.x.x> и/или <x.x.x.x/x>.

7. Задать уникальный идентификатор DHCP (DUID) для интерфейса агрегированных каналов:

```
set interfaces bonding <bondN> dhcpv6-options duid <h[[:h]...]>
```

где **<h[[:h]...]>** - значение уникального идентификатора DHCP.

Уникальный идентификатор DHCP (DUID) используется системой для получения IP-адреса от сервера DHCPv6. Он состоит из двухбайтового поля типа DUID и поля идентификатора переменной длины до 128 байт. Фактическая длина DUID зависит от типа. Сервер сравнивает DUID с данными в своей базе и

предоставляет системе необходимую информацию, такую как адрес, время аренды, DNS-серверы и другие параметры.

8. Не отправлять сообщение об освобождении при выходе:

```
set interfaces bonding <bondN> dhcpv6-options no-release
```

Данный параметр означает, что при использовании протокола DHCP для получения IPv6-адресов адрес не будет освобождаться автоматически. Это может быть полезно, если необходимо сохранить полученный адрес после отключения интерфейса или перезагрузки. В таком случае адрес возможно будет использовать многократного при последующих операциях подключения.

9. Получить только параметры конфигурации, без указания адреса:

```
set interfaces bonding <bondN> dhcpv6-options parameters-only
```

Данный параметр указывает на то, что DHCPv6 обменивается с серверами только информационными параметрами конфигурации. Примером таких параметров является список адресов DNS-серверов. Это утверждение может быть полезно, если клиенту не требуются параметры конфигурации с состоянием, такие как IPv6-адреса или префиксы.

10. Включить функцию Rapid Commit для быстрого получения IPv6-адреса:

```
set interfaces bonding <bondN> dhcpv6-options rapid-commit
```

11. Запросить временный IPv6-адрес:

```
set interfaces bonding <bondN> dhcpv6-options temporary
```

Запрашивается только временный адрес, и не создаёт партнёрство IANA (Identity Association for Non-temporary Addresses).

3.3.1.3 Делегирование префиксов DHCPv6 (PD)

1. Задать размер делегируемого префикса для экземпляра делегирования префикса на интерфейсе агрегированных каналов:

```
set interfaces bonding <bondN> dhcpv6-options pd <id> length <length>
```

где:

- **<id>** - номер экземпляра делегированного префикса. Значение должно быть больше или равно нулю.
- **<length>** - значение размера делегируемого префикса. Возможно указать значение в диапазоне от «32» до «64». По умолчанию используется значение «64».

2. Указать адрес интерфейса <address>, используемый локально на интерфейсе <delegatee>, на который был делегирован префикс:

```
set interfaces bonding <bondN> dhcpv6-options pd <id> interface <delegatee>  
address <address>
```

где:

- **<delegatee>** - сетевой интерфейс.
- **<address>** - значение, используемое для формирования адреса интерфейса IPv6. Значение должно быть больше нуля.

Интерфейс будет объединён с делегированным префиксом и идентификатором sla-id для формирования полного адреса интерфейса. По умолчанию используется расширенный уникальный идентификатор интерфейса (EUI-64).

3. Указать значение идентификатора агрегатора уровня сайта SLA <sla-id> на интерфейсе <delegatee>:

```
set interfaces bonding <bondN> dhcpv6-options pd <id> interface <delegatee>  
sla-id <id>
```

где **<id>** - значение идентификатора агрегатора уровня сайта. Идентификатор должен быть положительным десятичным числом и соответствовать максимально допустимой длине идентификаторов SLA.

3.3.1.4 Настройка параметров для агрегированного интерфейса

1. Определить режим работы агрегированного интерфейса:

```
set interfaces bonding <bondN> mode <802.3ad | active-backup | broadcast |  
round-robin | transmit-load-balance | adaptive-load-balance | xor-hash>
```

Возможно указать следующие режимы работы агрегированного интерфейса:

- **802.3ad** (по умолчанию) – это стандарт IEEE, также называемый LACP (Link Aggregation Control Protocol). Он включает автоматическую настройку агрегации, поэтому требуется минимальная настройка коммутатора. Режим, при котором создаются агрегированные группы сетевых карт с одинаковой скоростью и дуплексом. При таком объединении передача задействует все каналы в активной агрегации, согласно стандарту IEEE 802.3ad. Выбор ведомого устройства для исходящего трафика производится в соответствии с хэш-политикой передачи, которая может быть изменена по сравнению со стандартной простой XOR-политикой с помощью опции hash-policy. Обеспечивает как увеличение пропускной способности, так и отказоустойчивость.

Примечание:

Для использования режима 802.3ad необходимо, чтобы сетевой коммутатор поддерживал эту функцию.

- **active-backup** - в данном режиме только один сетевой интерфейс из агрегированных будет активным. Остальные интерфейсы станут активными только в случае отказа текущего активного интерфейса. При такой политике MAC-адрес агрегированного интерфейса отображается только на активном интерфейсе, что позволяет избегать конфликтов с коммутатором. Режим обеспечивает отказоустойчивость, но не предназначен для балансировки нагрузки на подчинённых интерфейсах.
- **broadcast** - широковещательный режим, пакеты отправляются через все подчинённые интерфейсы одновременно. Режим обеспечивает значительную отказоустойчивость.
- **round-robin** - пакеты отправляются последовательно, начиная с первого доступного интерфейса и заканчивая последним. При выходе одного из интерфейсов из строя, оставшиеся продолжают работать. Режим применяется для балансировки нагрузки и отказоустойчивости.
- **transmit-load-balance** - использование адаптивной балансировки нагрузки при передаче в качестве режима агрегирования. Этот режим является типом агрегирования каналов, не требующим никакой специальной поддержки коммутатором. Исходящий трафик распределяется в соответствии с текущей загрузкой (рассчитанной относительно скорости) на каждом интерфейсе Ethernet в интерфейсе агрегирования. Входящий трафик принимается текущим интерфейсом Ethernet. Если происходит сбой принимающего интерфейса Ethernet, происходит переход MAC-адреса сбойного интерфейса на другой интерфейс Ethernet.
- **adaptive-load-balance** - использование адаптивной балансировки нагрузки в качестве режима агрегирования. В этом режиме для трафика IPv4 производятся как адаптивная балансировка нагрузки при передаче, так и балансировка нагрузки при приёме, и не требуется специальной поддержки коммутатора. Балансировка нагрузки на приём достигается с помощью согласования по протоколу ARP. Драйвер бондинга перехватывает ARP-ответы, отправленные локальной системой, и переписывает аппаратный адрес источника уникальным аппаратным адресом одного из ведомых в бондинге. Это позволяет разным пирам использовать разные аппаратные адреса для сервера. Трафик, получаемый от соединений, созданных сервером,

также балансируется. Когда локальная система отправляет ARP-запрос, драйвер связывания копирует и сохраняет IP-информацию об аналоге из ARP-пакета. Когда ARP-ответ приходит от равного интерфейса, драйвер бондинга извлекает его аппаратный адрес и инициирует ARP-ответ этому равному интерфейсу, назначая его одним из ведомых в бондинге. Проблемным результатом использования ARP-переговоров для балансировки является то, что каждый раз при передаче ARP-запроса используется аппаратный адрес связи. Таким образом, равные участники узнают аппаратный адрес связи, и балансировка принимаемого трафика сводится к текущему ведомому. Это решается путём отправки обновлений (ARP-ответов) всем равным с их индивидуально назначенным аппаратным адресом, чтобы трафик перераспределился. Приёмный трафик также перераспределяется при добавлении нового ведомого в соединение и при повторной активации неактивного ведомого. Нагрузка на приём распределяется последовательно (по кругу) между группой самых высокоскоростных ведомых в связке. При восстановлении соединения или добавлении нового ведомого в связку, принимаемый трафик перераспределяется между всеми активными ведомыми в связке путём инициирования ARP-ответов с выбранным MAC-адресом каждому из клиентов. Параметр `updelay` должен быть установлен в значение, равное или большее, чем задержка пересылки коммутатора, чтобы ARP-ответы, отправленные клиентам, не были заблокированы коммутатором.

- **xor-hash** - использование политики «исключающего ИЛИ» в качестве режима агрегирования. Передача распределяется между сетевыми интерфейсами используя формулу: [(«MAC-адрес источника» XOR «MAC-адрес назначения») по модулю «slave count»]. Альтернативные политики передачи могут быть выбраны с помощью опции `hash-policy`. Этот режим обеспечивает балансировку нагрузки и отказоустойчивость.

2. Определить минимальное количество сетевых интерфейсов, входящих в состав агрегированного интерфейса:

```
set interfaces bonding <bondN> min-links <0-16>
```

где **<0-16>** - количество интерфейсов-участников. Возможно указать значение в диапазоне от «0» до «16». По умолчанию установлено значение «0», что означает отключение данного параметра. В этом случае агрегация будет функционировать до тех пор, пока есть активный агрегатор, независимо от их общего количества.

Примечание:

Данный параметр оказывает влияние только на режим **802.3ad**.

Поскольку агрегатор не может работать без хотя бы одного доступного канала, установка этого параметра на 0 или 1 будет иметь одинаковый эффект.

3. Определить скорость передачи LPDU пакетов между участками внутри агрегированного интерфейса:

```
set interfaces bonding <bondN> lacp-rate <slow | fast>
```

где **<slow | fast>** - скорость передачи LPDU. Возможно указать следующие значения:

- **slow** - запрашивать партнёра о передаче LACPDU каждые 30 секунд. Значение используется по умолчанию.
- **fast** - запрашивать партнёра о передаче LACPDU с периодичностью в одну секунду.

Примечание:

Данный параметр оказывает влияние только на режим **802.3ad**.

4. Указать системный MAC-адрес 802.3ad, который будет использоваться для обменов LACPDU:

```
set interfaces bonding <bondN> system-mac <mac address>
```

где **<mac address>** - MAC-адрес в формате <h:h:h:h:h:h>.

5. Установить метод хеширования, определяющий принцип балансировки трафика в режимах агрегирования xor-hash, 802.3ad и transmit-load-balance:

```
set interfaces bonding <bondN> hash-policy <policy>
```

где **<policy>** - метод хеширования. Возможно указать следующие значения:

- **layer2** - хеш на основе протокола 2 уровня. Для генерации хеша используются MAC-адреса отправителя и получателя. Весь трафик между определённой парой узлов всегда идёт по определённому каналу. Значение используется по умолчанию.
- **layer2+3** - хеш на основе протоколов 2 и 3 уровней. Используется комбинацию MAC и IP-адресов для генерации хеша. Благодаря этому обеспечивается более равномерная балансировка трафика, особенно в случае, когда большая его часть передаётся через промежуточные маршрутизаторы.

- **layer3+4** - хеш на основе протоколов 3 и 4 уровней. Канал для отправки пакета определяется по совокупности IP-адресов и номеров портов источника и назначения. Благодаря этому трафик определённого узла может распределяться между несколькими каналами, хотя пакеты одного и того же TCP-соединения или UDP-потока всегда передаются по одному и тому же каналу. Алгоритм не полностью совместим с IEEE 802.3ad.
 - **encap2+3** - хеш на основе протоколов 2 и 3 уровней с разбором инкапсуляции. Используется механизм, аналогичный layer2+3 с возможностью анализа инкапсулированных заголовков.
 - **encap3+4** - хеш на основе протоколов 3 и 4 уровней с разбором инкапсуляции. Используется механизм, аналогичный layer3+4 с возможностью анализа инкапсулированных заголовков.
6. Определить основной интерфейс среди всех интерфейсов, входящих в состав агрегированного интерфейса:

```
set interfaces bonding <bondN> primary <interface>
```

где **<interface>** - идентификатор основного интерфейса в интерфейсе агрегированных каналов.

Указанный интерфейс будет использоваться в качестве основного до тех пор, пока он доступен. В случае выхода основного интерфейса из строя будут использоваться альтернативные интерфейсы. Это может быть полезно, если один интерфейс обладает более высокой пропускной способностью по сравнению с другими. Опция **primary** доступна только в режимах **active-backup**, **transmit-load-balance** и **adaptive-load-balance**.

7. Установить интервал ARP мониторинга для агрегированного интерфейса:

```
set interfaces bonding <bondN> arp-monitor interval <time>
```

где **<time>** - значение частоты мониторинга ARP-каналов в миллисекундах. Возможно указать значение в диапазоне от «0» до «4294967295». По умолчанию установлено значение «0» - мониторинг ARP отключён.

ARP-монитор периодически проверяет ведомые устройства, чтобы определить, отправляли ли они или получали трафик в последнее время (точный критерий зависит от режима связывания и состояния ведомого устройства). Регулярный трафик генерируется с помощью ARP-зондов, отправленных на адреса, указанные в опции arp-monitor target. Если ARP-мониторинг используется в режиме, совместимом с эфирным каналом (режимы round-robin и xor-hash), коммутатор должен быть настроен в режиме, равномерно распределяющем пакеты по всем каналам. Если коммутатор настроен на распределение пакетов

в режиме XOR, все ответы от ARP-целей будут приниматься по одному каналу, что может привести к сбою в работе других членов команды.

8. Определить IP-адреса, которые будут использоваться в качестве пиров для ARP мониторинга, при значении параметра `arp-monitor interval` больше 0:

```
set interfaces bonding <bondN> arp-monitor target <address>
```

где **<address>** - IP-адрес в формате `<x.x.x.x>`. Возможно указать несколько целевых IP-адресов. Для запуска ARP-мониторинга необходимо указать хотя бы один IP-адрес. Максимальное количество IP-адресов, которое допускается задать, составляет «16».

3.3.2 VLAN

IEEE 802.1q, также известный как Dot1q, представляет собой сетевой стандарт, который поддерживает виртуальные локальные сети VLAN в сетях Ethernet, соответствующих стандарту IEEE 802.3. Стандарт определяет систему маркировки кадров Ethernet и процедуры, которые должны использоваться сетевыми устройствами при работе с такими кадрами. Стандарт также включает положения о схеме приоритизации качества обслуживания, известной как IEEE 802.1p, и определяет протокол регистрации общих атрибутов.

В системе **ARMA Стена** интерфейсы 802.1q представлены как виртуальные интерфейсы, подчинённые физическому интерфейсу. Для обозначения такого интерфейса используется термин «**vif**».

3.3.2.1 Основные настройки

1. Создать новый интерфейс VLAN на агрегированном интерфейсе:

```
set interfaces bonding <bondN> vif <vlan-id>
```

где **<vlan-id>** - идентификатор VLAN для виртуального интерфейса, используемый с системой тегов VLAN стандарта 802.1Q. Возможно указать значение в диапазоне от «0» до «4094».

Следует отметить, что на виртуальном интерфейсе агрегированных каналов будут обрабатываться только сетевые пакеты, имеющие теги стандарта 802.1Q. Для одного интерфейса агрегированных каналов возможно определить несколько виртуальных интерфейсов. Для этого необходимо создать соответствующее количество узлов конфигурации `vif`.

2. Назначить IP-адрес для интерфейса VLAN агрегированных каналов:

```
set interfaces bonding <bondN> vif <vlan-id> address <address | dhcp | dhcpv6>
```

где **<address | dhcp | dhcpv6>** - IP-адрес для данного виртуального интерфейса агрегированных каналов. Возможно указать следующие значения: `<x.x.x.x/x>`,

dhcp - для IPv4; <h:h:h:h:h:h:h/x>, dhcpv6 - для IPv6. IP-адрес может быть указан несколько раз как IPv4 и/или IPv6-адрес.

3. Задать текстовое описание виртуального интерфейса агрегированных каналов:

```
set interfaces bonding <bondN> vif <vlan-id> description <description>
```

где **<description>** - мнемоническое имя или описание виртуального интерфейса.

4. Отключить виртуальный интерфейс агрегированных каналов с сохранением текущих настроек:

```
set interfaces bonding <bondN> vif <vlan-id> disable
```

После отключения интерфейс будет переведён в режим административного отключения (A/D).

5. Отключить обнаружение изменений физического состояния канала связи, например, при отсоединении кабеля:

```
set interfaces bonding <bondN> vif <vlan-id> disable-link-detect
```

6. Задать MAC-адрес для виртуального интерфейса агрегированных каналов:

```
set interfaces bonding <bondN> vif <vlan-id> mac <xx:xx:xx:xx:xx:xx>
```

где **<xx:xx:xx:xx:xx:xx>** - MAC-адрес.

7. Установить значение MTU для виртуального интерфейса агрегированных каналов:

```
set interfaces bonding <bondN> vif <vlan-id> mtu <mtu>
```

где **<mtu>** - значения MTU для виртуального интерфейса. Возможно указать значение в диапазоне от «68» до «9190».

8. Установить значения TCP MSS для виртуального интерфейса агрегированных каналов:

```
set interfaces bonding <bondN> vif <vlan-id> ip adjust-mss <mss | clamp-mss-to-pmtu>
```

где:

- **<mss>** - значение MSS. Возможно указать значение в диапазоне от «536» до «65535».
- **<clamp-mss-to-pmtu>** - автоматически устанавливать MSS в нужное значение.

9. Установка тайм-аута записи в ARP-кэш для виртуального интерфейса агрегированных каналов:

```
set interfaces bonding <bondN> vif <vlan-id> ip arp-cache-timeout <1-86400>
```

где **<1-86400>** - значение тайм-аута записи в ARP-кэш в секундах. Возможно указать значение в диапазоне от «1» до «86400». По умолчанию используется значение «30».

10. Отключить фильтрацию ARP на виртуальном интерфейсе агрегированных каналов:

```
set interfaces bonding <bondN> vif <vlan-id> ip disable-arp-filter
```

Если параметр не установлен (по умолчанию), это позволяет иметь несколько сетевых интерфейсов в одной подсети и отвечать на ARP для каждого интерфейса в зависимости от того, будет ли ядро направлять пакет с IP-адресом ARP через этот интерфейс. Для этого необходимо использовать маршрутизацию на основе источника.

11. Отключить переадресацию IP на виртуальном интерфейсе агрегированных каналов:

```
set interfaces bonding <bondN> vif <vlan-id> ip disable-forwarding
```

Если параметр установлен, интерфейс переходит в режим хоста, и переадресация IPv6 на этом интерфейсе отключается.

12. Включить направленную широковещательную пересылку на виртуальном интерфейсе агрегированных каналов:

```
set interfaces bonding <bondN> vif <vlan-id> ip enable-directed-broadcast
```

В случае активации данной опции, входящие пакеты направленной широковещательной рассылки IP будут перенаправляться через указанный интерфейс. В случае если данный параметр не задан (по умолчанию), входящие пакеты направленной широковещательной рассылки IP не будут передаваться.

13. Включить приём ARP пакетов на виртуальном интерфейсе агрегированных каналов:

```
set interfaces bonding <bondN> vif <vlan-id> ip enable-arp-accept
```

Определяет поведение для ARP-пакетов, IP-записи которых ещё не присутствуют в ARP-таблице. Если эта настройка включена, то создаются новые записи в ARP-таблице. Как ответы, так и запросы типа Gratuitous ARP будут вызывать обновление ARP-таблицы, если эта настройка включена. Если в ARP-

таблице уже содержится IP-адрес кадра Gratuitous ARP, то ARP-таблица будет обновлена независимо от того, включена или выключена эта настройка.

14. Включить анонсирование ARP пакетов на виртуальном интерфейсе агрегированных каналов:

```
set interfaces bonding <bondN> vif <vlan-id> ip enable-arp-announce
```

Если параметр не задан, используется любой локальный адрес, который настроен на любом интерфейсе. Если параметр установлен, рекомендуется избегать использования локальных адресов, которые не входят в подсеть цели для данного интерфейса. Этот режим полезен, когда целевые узлы, доступные через данный интерфейс, требуют, чтобы IP-адрес источника в ARP-запросах был частью их логической сети, настроенной на принимающем интерфейсе. При генерации запроса система проверяет все подсети, включающие целевой IP-адрес, и сохраняет адрес источника, если он принадлежит такой подсети. Если подходящей подсети не найдено, система выбирает адрес источника в соответствии с правилами для уровня 2.

15. Включить игнорирование ARP пакетов на виртуальном интерфейсе агрегированных каналов:

```
set interfaces bonding <bondN> vif <vlan-id> ip enable-arp-ignore
```

Данный параметр определяет режимы отправки ответов на ARP-запросы, которые разрешают локальные целевые IP-адреса. Если параметр включён, ответ будет отправлен только в том случае, если целевой IP-адрес является локальным адресом, настроенным на входящем интерфейсе. Если параметр отключён (по умолчанию), ответ будет получен для любого локального целевого IP-адреса, настроенного на любом интерфейсе.

16. Включить прокси ARP на виртуальном интерфейсе агрегированных каналов:

```
set interfaces bonding <bondN> vif <vlan-id> ip enable-proxy-arp
```

Прокси ARP позволяет интерфейсу Ethernet отвечать своим MAC-адресом на ARP-запросы IP-адресов назначения в подсетях, подключённых к другим интерфейсам системы. Последующие пакеты, отправленные на эти IP-адреса назначения, пересылаются системой соответствующим образом.

17. Включить прокси ARP частного VLAN на виртуальном интерфейсе агрегированных каналов:

```
set interfaces bonding <bondN> vif <vlan-id> ip proxy-arp-pvlan
```

Разрешить ответы ARP-прокси с того же интерфейса, с которого был получен ARP-запрос или запрос на предложение. Это необходимо для поддержки функций Ethernet-коммутаторов, описанных в RFC 3069, где отдельные порты не

могут напрямую связываться друг с другом, но могут связываться с вышестоящим маршрутизатором. Как указано в RFC 3069, этого можно достичь путём включения прокси ARP.

Необязательно использовать вместе с прокси ARP.

18. Включить политику проверки источника по обратному пути, как указано в RFC 3704:

```
set interfaces bonding <bondN> vif <vlan-id> ip source-validation <strict | loose | disable>
```

где **<strict | loose | disable>** - режим проверки источника. Возможно указать следующие значения:

- **strict** - каждый входящий пакет проверяется по FIB, и если интерфейс не является наилучшим обратным путём, то проверка пакета будет неудачной. По умолчанию неудачные пакеты отбрасываются.
- **loose** - адрес источника каждого входящего пакета также проверяется по FIB, и если адрес источника не достижим ни через один интерфейс, проверка пакета будет неудачной.
- **disable** - нет проверки источника.

В настоящее время в RFC 3704 рекомендуется включать strict режим для предотвращения подмены IP адресов в результате DDos атак. При использовании асимметричной или другой сложной маршрутизации рекомендуется использовать loose режим.

19. Включить получение IPv6-адреса с помощью автоконфигурации без статического изменения (SLAAC):

```
set interfaces bonding <bondN> vif <vlan-id> ipv6 address autoconf
```

В соответствии с RFC 4862, хосты IPv6 могут автоматически настраиваться при подключении к сети IPv6 с использованием протокола Neighbor Discovery Protocol (NDP) через сообщения ICMPv6 об обнаружении маршрутизатора. При первом подключении к сети хост отправляет многоадресный запрос link-local router solicitation для получения параметров конфигурации. Маршрутизаторы отвечают на этот запрос пакетом router advertisement, содержащим параметры конфигурации уровня Интернета.

Примечание:

Данный метод автоматически отключает пересылку трафика IPv6 на сетевом интерфейсе.

20. Включить префикс EUI-64 на основе MAC адреса для IPv6 адреса виртуального интерфейса агрегированных каналов:

```
set interfaces bonding <bondN> vif <vlan-id> ipv6 address eui64 <prefix>
```

где **<prefix>** - сеть IPv6 в формате <h:h:h:h:h:h:h/64>.

21. Удалить локальный адрес IPv6 по умолчанию для виртуального интерфейса агрегированных каналов:

```
set interfaces bonding <bondN> vif <vlan-id> ipv6 address no-default-link-local
```

22. Отключить IP переадресацию на виртуальном интерфейсе агрегированных каналов:

```
set interfaces bonding <bondN> vif <vlan-id> ipv6 disable-forwarding
```

В случае установки, интерфейс будет переведён в режим хоста, а переадресация IPv6 на данном интерфейсе будет отключена.

23. Установить значения TCP MSS:

```
set interfaces bonding <bondN> vif <vlan-id> ipv6 adjust-mss <mss | clamp-mss-to-pmtu>
```

где:

- **<mss>** - значение MSS. Возможно указать значение в диапазоне от «536» до «65535».
- **<clamp-mss-to-pmtu>** - автоматически устанавливать MSS в нужное значение.

24. Принимать обнаружение дублирующегося адреса:

```
set interfaces bonding <bondN> vif <vlan-id> ipv6 accept-dad <0-2>
```

где **<0-2>** - режим приёма DAD. Возможно указать следующие значения:

- **0** - отключить DAD;
- **1** - включить DAD (по умолчанию);
- **2** - включить DAD и отключить работу IPv6, если обнаружен дублированный MAC-адрес link-local.

25. Установить количество сообщений NS для отправки при выполнении DAD:

```
set interfaces bonding <bondN> vif <vlan-id> ipv6 dup-addr-detect-transmits <n>
```

где **<n>** - количество NS-сообщений. В случае установки значения «0», функция обнаружения дубликатов адресов (DAD) будет отключена. По умолчанию используется значение «1».

26. Разместить виртуальный интерфейс агрегированных каналов в указанном экземпляре VRF:

```
set interfaces bonding <bondN> vif <vlan-id> vrf <vrf>
```

где **<vrf>** - имя экземпляра VRF.

3.3.2.2 Настройки получения адреса по DHCP(v6)

1. Установить идентификатор, используемый клиентом для идентификации себя DHCP сервером:

```
set interfaces bonding <bondN> vif <vlan-id> dhcp-options client-id <description>
```

где **<description>** - значение идентификатора.

В случае предоставления идентификатора пользователь обязан использовать один и тот же идентификатор во всех последующих сообщениях.

2. Изменить системное имя устройства, передаваемое DHCP серверу:

```
set interfaces bonding <bondN> vif <vlan-id> dhcp-options host-name <hostname>
```

где **<hostname>** - новое системное имя хоста, передаваемое DHCP серверу.

Вместо передачи реального системного имени хоста на DHCP-сервер будет передано заданное значение в качестве имени хоста.

3. Определить тип клиента поставщика для DHCP-сервера:

```
set interfaces bonding <bondN> vif <vlan-id> dhcp-options vendor-class-id <vendor-id>
```

где **<vendor-id>** - значение опций DHCP.

Опция «vendor-class-id» используется для запроса у сервера определённого класса опций поставщика.

4. Запросить у DHCP-сервера только адрес, не запрашивая шлюз по умолчанию:

```
set interfaces bonding <bondN> vif <vlan-id> dhcp-options no-default-route
```

5. Установить значение расстояния для шлюза по умолчанию, отправляемого сервером DHCP:

```
set interfaces bonding <bondN> vif <vlan-id> dhcp-options default-route-distance <distance>
```

где **<distance>** - значение расстояния для шлюза по умолчанию. Возможно указать значение в диапазоне от «1» до «255». По умолчанию используется значение «210».

6. Отклонить аренду DHCP с заданного адреса или диапазона:

```
set interfaces bonding <bondN> vif <vlan-id> dhcp-options reject <address>
```

где **<address>** - IP-адрес, возможно указать несколько раз в формате <x.x.x.x> и/или <x.x.x.x/x>.

7. Задать уникальный идентификатор DHCP (DUID) для интерфейса агрегированных каналов:

```
set interfaces bonding <bondN> vif <vlan-id> dhcpv6-options duid <duid>
```

где **<duid>** - значение уникального идентификатора DHCP.

Уникальный идентификатор DHCP (DUID) используется системой для получения IP-адреса от сервера DHCPv6. Он состоит из двухбайтового поля типа DUID и поля идентификатора переменной длины до 128 байт. Фактическая длина DUID зависит от типа. Сервер сравнивает DUID с данными в своей базе и предоставляет системе необходимую информацию, такую как адрес, время аренды, DNS-серверы и другие параметры.

8. Не отправлять сообщение об освобождении при выходе:

```
set interfaces bonding <bondN> vif <vlan-id> dhcpv6-options no-release
```

Данный параметр означает, что при использовании протокола DHCP для получения IPv6-адресов адрес не будет освобождаться автоматически. Это может быть полезно, если необходимо сохранить полученный адрес после отключения интерфейса или перезагрузки. В таком случае адрес возможно будет использовать многократно при последующих операциях подключения.

9. Получить только параметры конфигурации, без указания адреса:

```
set interfaces bonding <bondN> vif <vlan-id> dhcpv6-options parameters-only
```

Данный параметр указывает на то, что dhcpv6с обменивается с серверами только информационными параметрами конфигурации. Примером таких параметров является список адресов DNS-серверов. Это утверждение может быть полезно, если клиенту не требуются параметры конфигурации с состоянием, такие как IPv6-адреса или префиксы.

10. Включить функцию Rapid Commit для быстрого получения IPv6-адреса:

```
set interfaces bonding <bondN> vif <vlan-id> dhcpv6-options rapid-commi
```

11. Запросить временный IPv6-адрес:

```
set interfaces bonding <bondN> vif <vlan-id> dhcpv6-options temporary
```

Запрашивается только временный адрес, и не создаёт партнёрство IANA (Identity Association for Non-temporary Addresses).

3.3.2.3 Делегирование префиксов DHCPv6 (PD)

1. Задать размер делегируемого префикса для экземпляра делегирования префикса на виртуальном интерфейсе агрегированных каналов:

```
set interfaces bonding <bondN> vif <vlan-id> dhcpv6-options pd <id> length <length>
```

где:

- **<id>** - номер экземпляра делегированного префикса. Значение должно быть больше или равно нулю.
- **<length>** - значение размера делегируемого префикса. Возможно указать значение в диапазоне от «32» до «64». По умолчанию используется значение «64».

2. Указать адрес интерфейса <address>, используемый локально на интерфейсе <delegatee>, на который был делегирован префикс:

```
set interfaces bonding <bondN> vif <vlan-id> dhcpv6-options pd <id> interface <delegatee> address <address>
```

где:

- **<delegatee>** - сетевой интерфейс.
- **<address>** - значение, используемое для формирования адреса интерфейса IPv6. Значение должно быть больше нуля.

Интерфейс будет объединён с делегированным префиксом и идентификатором sla-id для формирования полного адреса интерфейса. По умолчанию используется расширенный уникальный идентификатор интерфейса (EUI-64).

3. Указать значение идентификатора агрегатора уровня сайта SLA <sla-id> на интерфейсе <delegatee>:

```
set interfaces bonding <bondN> vif <vlan-id> dhcpv6-options pd <id> interface <delegatee> sla-id <id>
```

где **<id>** - значение идентификатора агрегатора уровня сайта. Идентификатор должен быть положительным десятичным числом и соответствовать максимально допустимой длине идентификаторов SLA.

3.3.3 SPAN

Функция зеркалирования интерфейсов в **ARMA Стена** позволяет копировать входящий и исходящий трафик интерфейса на другой интерфейс. Функция

используется для анализа трафика и должна поддерживаться принимающим устройством, например, коммутатором.

Для настройки зеркалирования интерфейсов в системе **ARMA Стена** используется опция «mirror». При этом необходимо указать зеркальный порт как для входящего, так и для исходящего трафика.

Для настройки зеркалирования интерфейса для входящего трафика необходимо ввести команду:

```
set interfaces bonding <bondN> mirror ingress <inbound-interface>
```

где **<inbound-interface>** - имя интерфейса, на который будет дублироваться весь входящий трафик. Интерфейс должен быть определён в системе.

Для настройки зеркалирования интерфейса для исходящего трафика необходимо ввести команду:

```
set interfaces bonding <bondN> mirror egress <outbound-interface>
```

где **<outbound-interface>** - имя интерфейса, на который будет дублироваться весь исходящий трафик. Интерфейс должен быть определён в системе.

3.3.4 Мониторинг и эксплуатация

1. Команда вывода информации об агрегированных интерфейсах:

```
admin@ngfwos:~$ show interfaces bonding
```

Пример работы команды show interfaces bonding (см. [Рисунок – Информация об агрегированных интерфейсах](#)):

```
admin@ngfwos:$ show interfaces bonding
Codes: S - State, L - Link, u - Up, D - Down, A - Admin Down
Interface      IP Address      S/L  Description
-----
bond0          -               u/u  my-sw1 int 23 and 24
bond0.10       192.168.0.1/24  u/u  office-net
bond0.100      10.10.10.1/24   u/u  management-net
```

Рисунок – Информация об агрегированных интерфейсах

2. Команда для отображения подробной информации об агрегированных интерфейсах:

```
admin@ngfwos:~$ show interfaces bonding detail
```

Пример работы команды show interfaces bonding detail (см. [Рисунок – Подробная информация об агрегированных интерфейсах](#)):

```
admin@ngfwos:~$ show interfaces bonding detail
bond1: <BROADCAST,MULTICAST,MASTER,UP,LOWER_UP> mtu 9190 qdisc noqueue state UP group default qlen 1000
link/ether 00:50:56:bd:76:f3 brd ff:ff:ff:ff:ff:ff
inet 172.16.230.201/24 brd 172.16.230.255 scope global bond1
    valid_lft forever preferred_lft forever
inet6 fe80::250:56ff:febd:76f3/64 scope link
    valid_lft forever preferred_lft forever

RX:   bytes  packets  errors  dropped  overrun    mcast
      10942316  150193    0       652      0         571
TX:   bytes  packets  errors  dropped  carrier    collisions
      318708    2567      0        0        0          0
bond1.1@bond1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9190 qdisc noqueue state UP group default qlen 1000
link/ether 00:50:56:bd:76:f3 brd ff:ff:ff:ff:ff:ff
inet 172.16.230.201/24 brd 172.16.230.255 scope link
    valid_lft forever preferred_lft forever

RX:   bytes  packets  errors  dropped  overrun    mcast
      0        0         0        0        0          0
TX:   bytes  packets  errors  dropped  carrier    collisions
      966      9         0        0        0          0
admin@ngfwos:~$
```

Рисунок – Подробная информация об агрегированных интерфейсах

3. Команда вывода информации об указанном агрегированном интерфейсе:

```
admin@ngfwos:~$ show interfaces bonding <bondN>
```

Пример работы команды `show interfaces bonding <bondN>` (см. [Рисунок – Информация об агрегированном интерфейсе bond1](#)):

```
admin@ngfwos:~$ show interfaces bonding bond1
bond1: <BROADCAST,MULTICAST,MASTER,UP,LOWER_UP> mtu 9190 qdisc noqueue state UP group default qlen 1000
link/ether 00:50:56:bd:76:f3 brd ff:ff:ff:ff:ff:ff
inet 172.16.230.201/24 brd 172.16.230.255 scope global bond1
    valid_lft forever preferred_lft forever
inet6 fe80::250:56ff:febd:76f3/64 scope link
    valid_lft forever preferred_lft forever

RX:   bytes  packets  errors  dropped  overrun    mcast
      10942316  150193    0       652      0         571
TX:   bytes  packets  errors  dropped  carrier    collisions
      308788    2487      0        0        0          0
admin@ngfwos:~$
```

Рисунок – Информация об агрегированном интерфейсе bond1

4. Команда вывода подробной информации об указанном агрегированном интерфейсе:

```
admin@ngfwos:~$ show interfaces bonding <bondN> detail
```

Пример работы команды `show interfaces bonding <bondN> detail` (см. [Рисунок – Подробная информация об агрегированном интерфейсе bond1](#)):


```
admin@ngfwos:~$ show interfaces bonding bond1 detail
Ethernet Channel Bonding Driver: v6.6.54-amd64-vyos

Bonding Mode: IEEE 802.3ad Dynamic link aggregation
Transmit Hash Policy: layer2 (0)
MII Status: up
MII Polling Interval (ms): 100
Up Delay (ms): 0
Down Delay (ms): 0
Peer Notification Delay (ms): 0

802.3ad info
LACP active: on
LACP rate: slow
Min links: 0
Aggregator selection policy (ad_select): stable
System priority: 65535
System MAC address: 00:50:56:bd:76:f3
Active Aggregator Info:
    Aggregator ID: 1
    Number of ports: 1
    Actor Key: 15
    Partner Key: 1
    Partner Mac Address: 00:00:00:00:00:00

Slave Interface: eth1
MII Status: up
Speed: 10000 Mbps
Duplex: full
Link Failure Count: 0
Permanent HW addr: 00:50:56:bd:76:f3
Slave queue ID: 0
Aggregator ID: 1
Actor Churn State: none
Partner Churn State: churned
Actor Churned Count: 0
Partner Churned Count: 1
details actor lacp pdu:
    system priority: 65535
    system mac address: 00:50:56:bd:76:f3
    port key: 15
    port priority: 255
    port number: 1
    port state: 77
details partner lacp pdu:
    system priority: 65535
    system mac address: 00:00:00:00:00:00
    oper key: 1
    port priority: 255
    port number: 1
    port state: 1

Slave Interface: eth2
MII Status: up
Speed: 10000 Mbps
Duplex: full
Link Failure Count: 0
Permanent HW addr: 00:50:56:bd:0b:21
Slave queue ID: 0
Aggregator ID: 2
Actor Churn State: churned
Partner Churn State: churned
Actor Churned Count: 1
Partner Churned Count: 1
details actor lacp pdu:
    system priority: 65535
    system mac address: 00:50:56:bd:76:f3
    port key: 15
    port priority: 255
    port number: 2
    port state: 69
details partner lacp pdu:
    system priority: 65535
    system mac address: 00:00:00:00:00:00
    oper key: 1
    port priority: 255
    port number: 1
    port state: 1
admin@ngfwos:~$
```

Рисунок – Подробная информация об агрегированном интерфейсе bond1

5. Команда вывода информации об агрегированных интерфейсах, использующих протокол LACP:

```
admin@ngfwos:~$ show interfaces bonding lACP detail
```

Пример работы команды `show interfaces bonding lACP detail` (см. [Рисунок – Информация об агрегированных интерфейсах, использующих протокол LACP](#)):

```
admin@ngfwos:~$ show interfaces bonding lACP detail
Interface      Members      Mode      Rate      System-MAC      Hash
-----
bond1          eth1,eth2    active    slow      00:50:56:bd:76:f3  layer2
admin@ngfwos:~$
```

Рисунок – Информация об агрегированных интерфейсах, использующих протокол LACP

5. Команда вывода информации об указанном агрегированном интерфейсе, использующем протокол LACP:

```
admin@ngfwos:~$ show interfaces bonding <bondN> lACP detail
```

6. Команда вывода информации о LACP-соседях в указанном агрегированном интерфейсе, использующем протокол LACP:

```
admin@ngfwos:~$ show interfaces bonding <bondN> lACP neighbors
```

Пример работы команды `show interfaces bonding <bondN> lACP neighbors` (см. [Рисунок – Информация о LACP-соседях в указанном агрегированном интерфейсе](#)):

```
admin@ngfwos:~$ show interfaces bonding bond1 lACP neighbors
Interface      Member      Local ID      Remote ID
-----
bond1          eth1        00:50:56:bd:76:f3  00:00:00:00:00:00
bond1          eth2        00:50:56:bd:76:f3  00:00:00:00:00:00
admin@ngfwos:~$
```

Рисунок – Информация о LACP-соседях в указанном агрегированном интерфейсе

7. Команда вывода информации о ведомых (slave) интерфейсах в указанном агрегированном интерфейсе:

```
admin@ngfwos:~$ show interfaces bonding <bondN> slaves
```

Пример работы команды `show interfaces bonding <bondN> slaves` (см. [Рисунок – Информация о ведомых \(slave\) интерфейсах в указанном агрегированном интерфейсе](#)):

```
admin@ngfwos:~$ show interfaces bonding bond1 slaves
Interface      RX: bytes  packets  TX: bytes  packets
bond1
  eth2          0           0        31124      251
  eth1          0           0        31124      251

admin@ngfwos:~$
```

Рисунок – Информация о ведомых (slave) интерфейсах в указанном агрегированном интерфейсе

- Команда вывода полной информации об указанном виртуальном интерфейсе агрегированного интерфейса:

```
admin@ngfwos:~$ show interfaces bonding <bondN> vif <id>
```

- Команда вывода краткой информации об указанном виртуальном интерфейсе агрегированного интерфейса:

```
admin@ngfwos:~$ show interfaces bonding <bondN> vif <id> brief
```

3.3.5 Примеры настройки агрегированного канала

Пример настройки агрегированного канала между двумя устройствами ARMA Стена

Для демонстрации конфигурации агрегированного канала используется тестовая схема, представленная на рисунке (см. [Рисунок – Агрегированный канал](#)). Агрегированный канал функционирует в режиме 802.3ad.

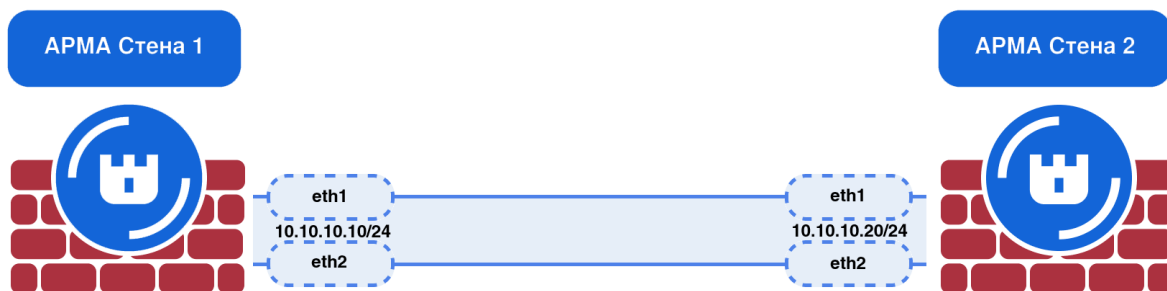


Рисунок – Агрегированный канал

Конфигурация **ARMA Стена 1**:

```
set interfaces bonding bond0
set interfaces bonding bond0 address 10.10.10.10/24
set interfaces bonding bond0 member interface eth1
set interfaces bonding bond0 member interface eth2
```

Проверка конфигурации:

```
show interfaces bonding bond0
address 10.10.10.10/24
member {
    interface eth1
    interface eth2
}
```

Конфигурация **ARMA Стена 2**:

```
set interfaces bonding bond0
set interfaces bonding bond0 address 10.10.10.20/24
set interfaces bonding bond0 member interface eth1
set interfaces bonding bond0 member interface eth2
```

Проверка конфигурации:

```
show interfaces bonding bond0
address 10.10.10.20/24
member {
    interface eth1
    interface eth2
}
```

Проверка соединения и балансировки трафика

Для проверки работоспособности агрегированного канала на **ARMA Стена 1** выполняется команда ping адреса интерфейса **ARMA Стена 2**:

```
admin@ngfwos:~$ ping 10.10.10.20
PING 10.10.10.20 (10.10.10.20) 56(84) bytes of data.
64 bytes from 10.10.10.20: icmp_seq=1 ttl=64 time=0.593 ms
64 bytes from 10.10.10.20: icmp_seq=2 ttl=64 time=0.426 ms
64 bytes from 10.10.10.20: icmp_seq=3 ttl=64 time=0.407 ms
```

На **ARMA Стена 2** производится анализ счётчиков трафика на физических интерфейсах:

```
admin@ngfwos:~$ clear interfaces ethernet counters # Сбросить счётчик
Ethernet-интерфейсов
admin@ngfwos:~$ show interfaces ethernet eth1
admin@ngfwos:~$ show interfaces ethernet eth2
```

Анализ вывода команд показывает, что значение параметра *packets* для интерфейсов *eth1* и *eth2* изменяется приблизительно одинаково, что подтверждает равномерное распределение трафика между каналами и корректную работу **LACP**.

Пример настройки агрегированного канала между устройством ARMA Стена и коммутатором Arista

Данная конфигурация реализует агрегацию каналов между устройством **ARMA Стена** и управляемым коммутатором **Arista** (см. [Рисунок – Агрегированный канал между различными устройствами](#)).

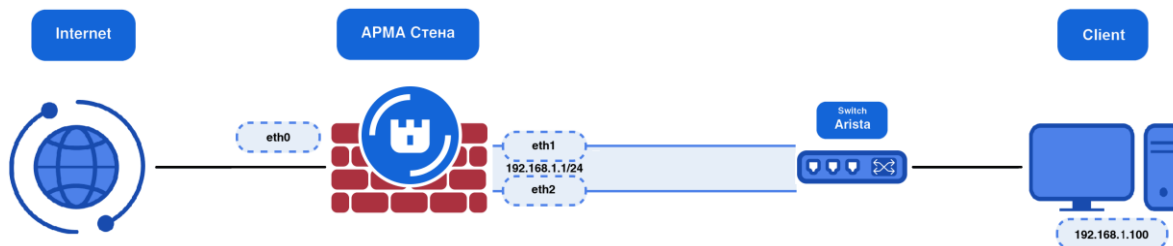


Рисунок – Агрегированный канал между различными устройствами

Конфигурация ARMA Стена:

```
set interfaces bonding bond1 address '192.168.1.1/24'
set interfaces bonding bond1 member interface 'eth1'
set interfaces bonding bond1 member interface 'eth2'
set interfaces ethernet eth0 address 'dhcp'
set nat source rule 10 outbound-interface name 'eth0'
set nat source rule 10 translation address 'masquerade'
```

Конфигурация коммутатора Arista:

```
interface Ethernet1
  channel-group 1 mode active
interface Ethernet2
  channel-group 1 mode active
```

Конфигурация клиентского устройства:

На клиентском устройстве необходимо задать следующие параметры сети (см. [Рисунок – Конфигурация IP-адреса](#)):

- IP-адрес 192.168.1.100/24;
- маску подсети – 255.255.255.0;
- шлюз по умолчанию – 192.168.1.1;
- адрес DNS-сервера.

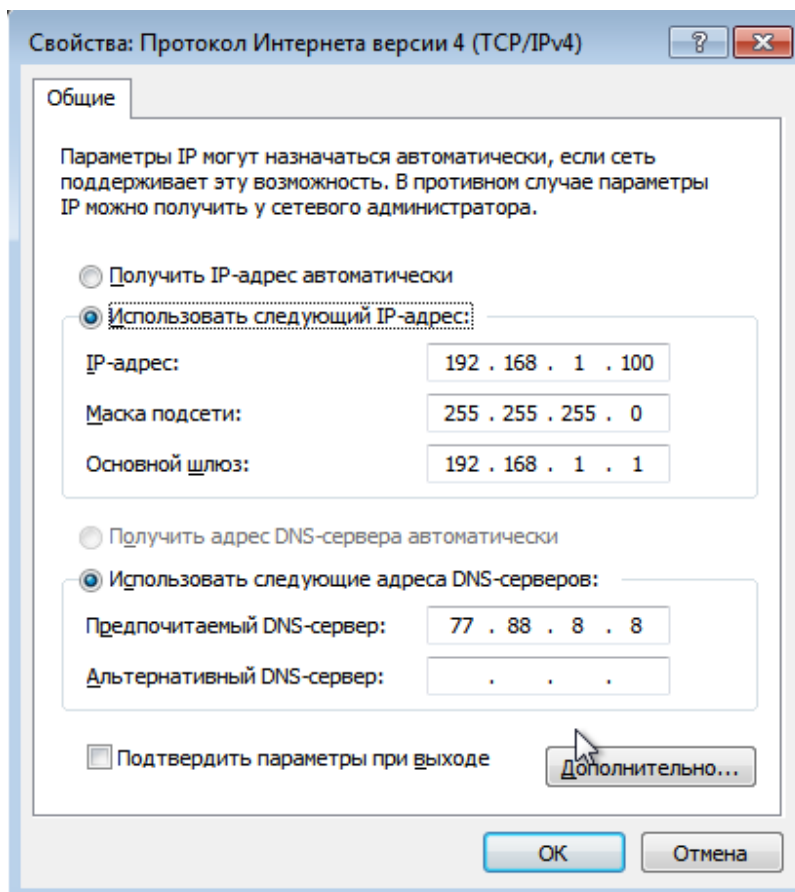


Рисунок – Конфигурация IP-адреса

Проверка функционирования:

Через веб-браузер на хосте клиента выполняется загрузка внешних веб-страниц. Успешное открытие ресурсов подтверждает наличие сетевого соединения и работоспособность **NAT**. Нагрузка на физические интерфейсы *eth1* и *eth2* устройства **ARMA Стена** распределяется согласно политике балансировки **LACP**, что может быть верифицировано путём мониторинга счётчиков интерфейсов на стороне как **ARMA Стена**, так и коммутатора **Arista**.

3.4 Туннелирование

Туннелирование сетевых пакетов – это механизм для инкапсуляции пакетов одного сетевого протокола в пакеты другого протокола. Пакеты инкапсулируемого протокола вкладываются в пакеты транспортного протокола. Инкапсулированный пакет перенаправляется в сеть назначения, затем извлекается вложенный пакет, который перенаправляется получателю.

В **ARMA Стена** поддерживаются следующие протоколы туннелирования: **ERSPAN**, **GRE**, **GRETap**, **IPIP**, **IP6IP6**, **6in4 (SIT)**. Все эти протоколы сгруппированы в «**interfaces tunnel**».

3.4.1 Общие команды настройки

1. Установка первичного или вторичного IP-адреса для туннельного интерфейса:

```
set interfaces tunnel <tunN> address <address>
```

где:

- **<tunN>** - имя туннельного интерфейса;
- **<address>** - интерфейсный IP-адрес. Возможно указать адрес несколько раз. Значение указывается в формате: **<x.x.x.x/x>** - для IPv4, **<h:h:h:h:h:h:h/x>** - для IPv6.

2. Указание краткого текстового описания для туннельного интерфейса:

```
set interfaces tunnel <tunN> description <description>
```

где **<description>** - текстовое описание туннельного интерфейса.

3. Отключение туннельного интерфейса с сохранением текущей настройки:

```
set interfaces tunnel <tunN> disable
```

4. Отключение механизма временной остановки передачи данных (Ethernet flow control):

```
set interfaces tunnel <tunN> disable-flow-control
```

5. Отключение механизма контроля физического состояния канала связи:

```
set interfaces tunnel <tunN> disable-link-detect
```

По умолчанию механизм отслеживает изменения состояния физического канала, например, при отсоединении кабеля.

6. Установка размера MTU для туннельного интерфейса:

```
set interfaces tunnel <tunN> mtu <mtu>
```

где **<mtu>** - размер MTU. Возможно указать значения в диапазоне от «68» до «16000».

7. Поместить интерфейс в данный экземпляр VRF:

```
set interfaces tunnel <tunN> vrf <vrf>
```

где **<vrf>** - имя vrf.

8. Установка используемого типа инкапсуляции пакетов:

```
set interfaces tunnel <tunN> encapsulation <tun>
```

где **<tun>** - тип инкапсуляции. Возможно указать следующие значения:

- **erspan** - анализатор инкапсулированных удалённых коммутируемых портов;
- **gre** - generic Routing Encapsulation (сетевой уровень);
- **gretap** - generic Routing Encapsulation (канальный уровень);
- **ip6erspan** - инкапсулированный анализатор удалённых коммутируемых портов через IPv6;
- **ip6gre** - GRE поверх IPv6 (сетевой уровень);
- **ip6gretap** - GRE поверх IPv6 (канальный уровень);
- **ip6ip6** - IPv6 в инкапсуляции IPv6;
- **ipip** - IPv4 в инкапсуляции IPv4;
- **ipip6** - IPv4 в инкапсуляции IPv6;
- **sit** - simple Internet Transition (IPv6 в IPv4).

9. Указание IP-адреса удалённого оконечного узла туннеля:

```
set interfaces tunnel <tunN> remote <address>
```

где **<address>** - IP-адрес оконечного узла туннеля на удалённом маршрутизаторе. Значение указывается в формате: **<x.x.x.x/x>** - для IPv4, **<h:h:h:h:h:h/x>** - для IPv6.

10. Указание IP-адрес источника, используемый для инициирования соединения:

```
set interfaces tunnel <tunN> source-address <address>
```

где **<address>** - IP-адрес источника. Значение указывается в формате: **<x.x.x.x>** - для IPv4, **<h:h:h:h:h:h>** - для IPv6.

11. Указание интерфейса, используемого для установления соединения:

```
set interfaces tunnel <tunN> source-interface <interface>
```

где **<interface>** - интерфейс, используемый для установления соединения.

3.4.2 GRE

Протокол **GRE** представляет собой универсальный механизм инкапсуляции пакетов различных сетевых протоколов для их передачи другим протоколом. Исходный пакет, также называемый «пассажирским», может относиться к любому сетевому протоколу. В качестве транспортного протокола может использоваться один из маршрутизируемых IP-протоколов. Пакет пассажирского протокола сначала инкапсулируется в пакет **GRE**, создавая «туннель» **GRE**. Затем пакет **GRE** инкапсулируется в пакет транспортного протокола («носителя»), который затем

направляется в сеть назначения. После этого исходный пакет извлекается и доставляется адресату.

Туннели **GRE** не имеют средств контроля состояния, то есть протокол не предоставляет возможности автоматического отслеживания доступности конечных узлов. Однако существует возможность отслеживания состояния другого конечного узла путём отправки специальных сообщений, подтверждающих активность. Конечное устройство считается неактивным, если оно перестаёт отвечать на такие сообщения.

GRE не обеспечивает безопасность данных. Существует возможность настройки ключа на каждом из конечных узлов туннеля, который позволяет конечным точкам аутентифицировать друг друга. Однако следует учитывать, что ключ передаётся в открытом виде в каждом пакете. В случае необходимости обеспечения безопасности передаваемых данных, **GRE** может использоваться совместно с **IPSec**.

В качестве примера настройки туннеля **GRE**, используется схема стенда, представленная на рисунке (см. [Рисунок – Схема стенда для настройки туннеля GRE](#)).

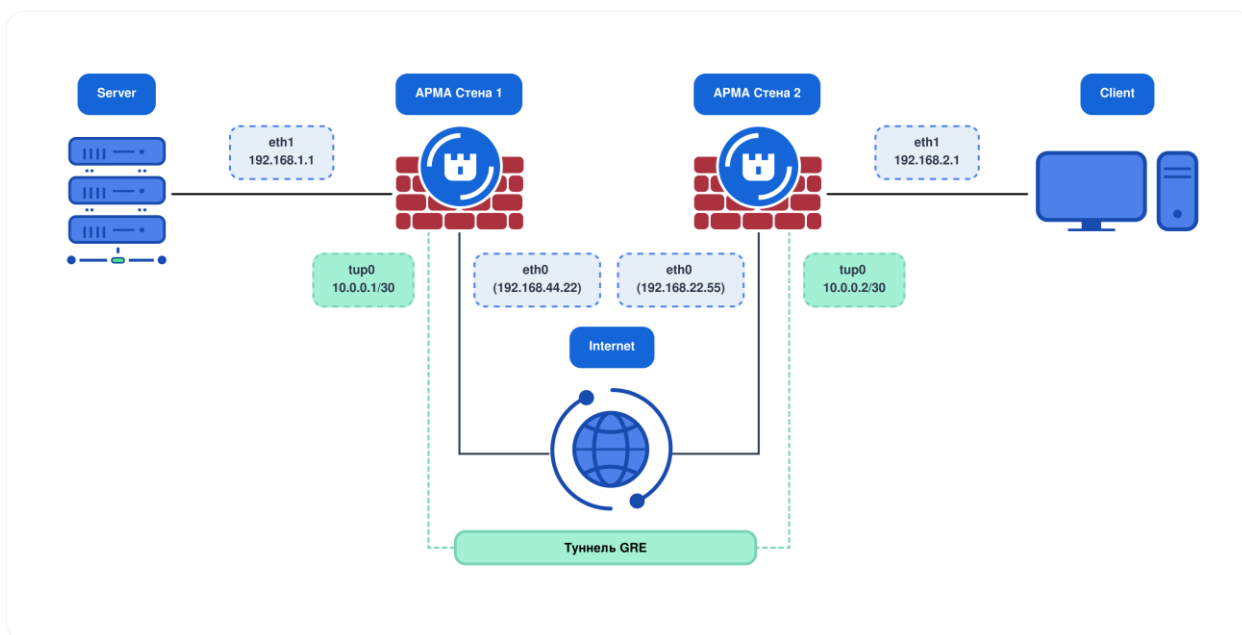


Рисунок – Схема стенда для настройки туннеля GRE

Используемые IP-адреса приведены в качестве примера.

Для настройки туннеля GRE необходимо выполнить следующие шаги:

1. Настроить конфигурацию туннеля GRE на **ARMA Стена1**, введя команды:

```
set interfaces tunnel tun0 address '10.0.0.1/30'
set interfaces tunnel tun0 encapsulation 'gre'
set interfaces tunnel tun0 remote '192.168.22.55'
set interfaces tunnel tun0 source-address '192.168.44.22'
```

2. Настроить конфигурацию туннеля GRE на **ARMA Стена2**, введя команды:

```
set interfaces tunnel tun0 address '10.0.0.2/30'  
set interfaces tunnel tun0 encapsulation 'gre'  
set interfaces tunnel tun0 remote '192.168.44.22'  
set interfaces tunnel tun0 source-address '192.168.22.55'
```

3. Настроить маршрут на каждой **ARMA Стена**:

```
set protocols static route 192.168.2.0/24 interface tun0 #ARMA Стена1  
  
set protocols static route 192.168.1.0/24 interface tun0 #ARMA Стена2
```

4. Проверить работу туннеля GRE.

Для проверки работы необходимо с ПК «Client» выполнить команду «ping» ПК «Server». При правильной настройке, команда выполнится успешно.

Настройка туннельных протоколов **GRETAP, IPIP, IPIP6, IP6IP6, 6in4 (SIT)** осуществляется по аналогии с настройкой протокола **GRE**.

3.4.3 ERSPAN

ERSPAN (Encapsulated Remote Switched Port Analyzer) – технология, которая используется для зеркалирования трафика в L3 сетях на основе механизма GRE инкапсуляции.

В качестве примера настройки туннеля ERSPAN, используется схема стенда, представленная на рисунке (см. [Рисунок – Схема стенда для настройки туннеля GRE](#)).

Для настройки туннеля ERSPAN необходимо выполнить следующие шаги:

1. Настроить конфигурацию туннеля ERSPAN на **ARMA Стена2**, введя команды:

```
set interfaces tunnel tun50 encapsulation erspan  
set interfaces tunnel tun50 parameters erspan direction ingress  
set interfaces tunnel tun50 parameters erspan version 2  
set interfaces tunnel tun50 parameters ip key 1  
set interfaces tunnel tun50 remote 192.168.44.22  
set interfaces tunnel tun50 source-address 192.168.22.55  
set interfaces tunnel tun50 source-interface eth0  
  
# Указать источник зеркалирования трафика - с «eth1» в туннель «tun50»:  
set interfaces ethernet eth1 mirror ingress tun50
```

Просмотр настроек:

```
admin@ngfwos# show interfaces tunnel tun50
encapsulation erspan
parameters {
    erspan {
        direction ingress
        version 2
    }
    ip {
        key 1
    }
}
remote 192.168.44.22
source-address 192.168.22.55
source-interface eth0
[edit]
admin@ngfwos#
```

2. Настроить конфигурацию туннеля ERSPAN на **ARMA Стена1**, введя команды:

```
set interfaces tunnel tun50 encapsulation erspan
set interfaces tunnel tun50 parameters erspan direction egress
set interfaces tunnel tun50 parameters erspan version 2
set interfaces tunnel tun50 parameters ip key 1
set interfaces tunnel tun50 remote 192.168.22.55
set interfaces tunnel tun50 source-address 192.168.44.22
set interfaces tunnel tun50 source-interface eth0

# Указать интерфейс, к которому подключен анализатор трафика:
set interfaces tunnel tun50 mirror ingress eth1
```

Просмотр настроек:

```
admin@ngfwos# show interfaces tunnel tun50
encapsulation erspan
parameters {
    erspan {
        direction ingress
        version 2
    }
    ip {
        key 1
    }
}
remote 192.168.22.55
source-address 192.168.44.22
source-interface eth0
[edit]
admin@ngfwos#
```

Трафик с интерфейса «eth1» устройства **ARMA Стена2** будет зеркалироваться и передаваться через туннель tun50 на удалённое устройство **ARMA Стена1**, где он будет доступен для анализа на интерфейсе «eth1».

3.5 PPPoE

PPPoE обеспечивает механизм аутентификации пользователей, управления сеансами и маршрутизации данных через сеть Ethernet. PPPoE может использоваться в различных промышленных и специализированных сетях.

3.5.1 Настройка PPPoE-соединения

В качестве примера приведены настройки PPPoE-соединения между провайдером и **ARMA Стена**.

Параметры для настройки PPPoE:

- сетевое оборудование провайдера подключено к интерфейсу «eth0» устройства **ARMA Стена**;
- для связи с провайдером не требуется настройка VLAN для сетевого интерфейса;
- для настройки используются учётные данные PPPoE от DSL провайдера: user – «userID», password – «secret»;
- максимальный размер MTU, который используется в DSL, составляет «1492» байта.

Примечание:

Маршрут по умолчанию автоматически прописывается после включения интерфейса.

Для настройки протокола PPPoE необходимо ввести следующие команды:

```
set interfaces pppoe pppoe0 mtu 1492
set interfaces pppoe pppoe0 authentication username userID
set interfaces pppoe pppoe0 authentication password secret
set interfaces pppoe pppoe0 source-interface eth0
```

где **«pppoe0»** – имя PPPoE-интерфейса.

Следует провести настройку межсетевого экрана для работы на интерфейсе «PPPoE». Для этого необходимо назначить политики межсетевого экрана для всех направлений трафика на интерфейсе «pppoe0».

Отдельные провайдеры требуют построения PPPoE-соединения через VLAN-интерфейс. В **ARMA Стена** существует возможность создать PPPoE-сессию через VLAN-интерфейс.

Пример настройки построения PPPoE-соединения через VLAN-интерфейс «eth0.7»:

```
set interfaces pppoe pppoe0 authentication username userID
set interfaces pppoe pppoe0 authentication password secret
set interfaces pppoe pppoe0 source-interface eth0.7
```

3.5.2 Команды настройки PPPoE

3.5.2.1 Основные команды

1. Команда добавления описания для PPPoE-интерфейса:

```
set interfaces pppoe <pppoeN> description <description>
```

где:

- **<pppoeN>** – имя pppoe-интерфейса, например «pppoe0»;
- **<description>** – описание интерфейса.

2. Команда отключения PPPoE-интерфейса:

```
set interfaces pppoe <pppoeN> disable
```

После отключения интерфейс будет переведён в состояние административного отключения.

3. Команда настройки MTU для PPPoE-интерфейса:

```
set interfaces pppoe <pppoeN> mtu <mtu>
```

где **<mtu>** – значение MTU. Возможно указание значения в диапазоне от «1280» до «9190».

4. Команда размещения PPPoE-интерфейса в заданном экземпляре VRF:

```
set interfaces pppoe <pppoeN> vrf <vrf>
```

где **<vrf>** – имя VRF.

5. Команда определения интерфейса для привязки к нему PPPoE-соединения:

```
set interfaces pppoe <pppoeN> source-interface <source-interface>
```

где **<source-interface>** – имя интерфейса.

3.5.2.2 Команды настройки параметров PPPoE

1. Команда выбора определённого сервера доступа для PPPoE-соединения:

```
set interfaces pppoe <pppoeN> access-concentrator <name>
```

где **<name>** – имя сервера доступа.

2. Команда установки имени пользователя для аутентификации PPPoE-соединения на удалённом сервере:

```
set interfaces pppoe <pppoeN> authentication username <username>
```

где **<username>** – имя пользователя.

3. Команда установки пароля пользователя для аутентификации PPPoE-соединения на удалённом сервере:

```
set interfaces pppoe <pppoeN> authentication password <password>
```

где **<password>** – пароль пользователя.

4. Команда активации режима «соединение по запросу»:

```
set interfaces pppoe <pppoeN> connect-on-demand
```

5. Команда запроса адреса у сервера PPPoE без установки маршрутов по умолчанию:

```
set interfaces pppoe <pppoeN> no-default-route
```

6. Команда установки расстояния для шлюза по умолчанию, отправляемого сервером PPPoE:

```
set interfaces pppoe <pppoeN> default-route-distance <distance>
```

где **<distance>** – значение дистанции. Возможно указание значения в диапазоне от «1» до «255».

7. Команда установки значения MRU:

```
set interfaces pppoe <pppoeN> mru <mru>
```

где **<mru>** – значение MRU. Возможно указание значения в диапазоне от «128» до «16384». По умолчанию используется значение «1492».

При использовании протокола IPv6 размер MRU должен составлять не менее «1280» байт.

8. Команда установки интервала ожидания для PPPoE-интерфейса:

```
set interfaces pppoe <pppoeN> idle-timeout <time>
```

где **<time>** – время ожидания. Возможно указание значения в диапазоне от «0» до «86400».

Если параметр не задан или равен «0», то соединение по запросу будет всегда оставаться включённым.

9. Команда установки времени задержки повторного набора номера для использования в постоянных PPPoE-сессиях:

```
set interfaces pppoe <pppoeN> holdoff <time>
```

где **<time>** – время задержки в секундах. Возможно указание значения в диапазоне от «0» до «86400». По умолчанию используется значение «30».

10. Команда установки адреса локального устройства для сеанса PPPoE:

```
set interfaces pppoe <pppoeN> local-address <x.x.x.x>
```

где **<x.x.x.x>** – IP-адрес локального устройства.

Если адрес локального устройства не задан, то он будет согласован в процессе инициализации PPPoE-сессии.

11. Команда отключения использования внешних DNS-серверов:

```
set interfaces pppoe <pppoeN> no-peer-dns
```

12. Команда установки адреса удалённого устройства для сеанса PPPoE:

```
set interfaces pppoe <pppoeN> remote-address <x.x.x.x>
```

где **<x.x.x.x>** – IP-адрес удалённого устройства.

Если адрес удалённого устройства не задан, то он будет согласован в процессе инициализации PPPoE-сессии.

13. Команда установки сервиса, по которому локальный интерфейс PPPoE будет выбирать серверы доступа для подключения:

```
set interfaces pppoe <pppoeN> service-name <name>
```

где **<name>** – имя сервиса.

3.5.2.3 Команды мониторинга PPPoE

1. Команда вывода подробной информации об интерфейсе PPPoE:

```
admin@ngfwos:~$ show interfaces pppoe <pppoeN>
```

где **<pppoeN>** – имя PPPoE-интерфейса.

2. Команда вывода информации об очередях для интерфейса PPPoE:

```
admin@ngfwos:~$ show interfaces pppoe <pppoeN> queue
```

3. Команда отключения интерфейса PPPoE:

```
admin@ngfwos:~$ disconnect interface <pppoeN>
```

4. Команда включения интерфейса PPPoE:

```
admin@ngfwos:~$ connect interface <pppoeN>
```

3.6 Интерфейс Loopback

Loopback-интерфейс в системе **ARMA Стена** представляет собой виртуальное сетевое устройство, реализованное полностью в программном обеспечении. Данный интерфейс обеспечивает внутреннюю маршрутизацию сетевого трафика без его выхода за пределы системы.

Loopback-интерфейс всегда находится в активном состоянии (up), что позволяет использовать его для управляющего трафика, а также в качестве источника или назначения для протоколов IGP, таких как BGP. Это обеспечивает независимость внутренних BGP-соединений от состояния физических интерфейсов и позволяет выбирать несколько маршрутов к цели.

Для создания дополнительных виртуальных интерфейсов рекомендуется использовать интерфейс **Dummy**, поскольку он является более предпочтительным решением для подобных задач.

Примечание:

В системе **ARMA Стена** существует только один loopback-интерфейс, который обозначается как «**lo**». Если требуется наличие нескольких интерфейсов, то следует использовать интерфейс «**Dummy**».

3.6.1 Настройка loopback-интерфейса

1. Назначить loopback-интерфейсу IP-адрес и префикс сети:


```
set interfaces loopback lo address <address>
```

где:

- **<address>** – IPv4-адрес или IPv6-адрес для интерфейса в формате <x.x.x.x/x> и <h:h:h:h:h:h:h/x> соответственно. Возможно указать несколько адресов для интерфейса.

В протоколе IPv4 для loopback-интерфейса зарезервирован адресный диапазон «127.0.0.1 – 127.255.255.255». В протоколе IPv6 для loopback-интерфейса определён единственный адрес «::1». Адресами по умолчанию для loopback являются **127.0.0.1/8** для IPv4 и **::1/128** для IPv6.

2. Установить описание для loopback-интерфейса:

```
set interfaces loopback lo description <description>
```

где:

- **<description>** – описание интерфейса.

3.6.2 Дополнительные настройки loopback-интерфейса

1. Включить политику проверки источника по обратному пути, как указано в RFC 3704:

```
set interfaces loopback lo ip source-validation <strict | loose | disable>
```

где **<strict | loose | disable>** - режим проверки источника. Возможно указать следующие значения:

- **strict** - каждый входящий пакет проверяется по FIB, и принимается только если пришёл через оптимальный (наилучший) обратный путь, определённый в таблице маршрутизации. Все пакеты, не удовлетворяющие этому условию, автоматически отбрасываются.
- **loose** - адрес источника каждого входящего пакета также проверяется по FIB, и если адрес источника не достижим ни через один интерфейс, проверка пакета будет неудачной.
- **disable** - нет проверки источника.

В настоящее время в RFC 3704 рекомендуется включать «strict» режим для предотвращения подмены IP адресов в результате DDos атак. При использовании асимметричной или другой сложной маршрутизации рекомендуется использовать «loose» режим.

2. Перенаправить входящий трафик с loopback-интерфейса на другой интерфейс:

```
set interfaces loopback lo redirect <интерфейс>
```

где **<интерфейс>** - имя интерфейса, на который будет перенаправляться весь входящий трафик. Интерфейс должен быть определён в системе.

3.6.3 SPAN

Функция зеркалирования интерфейсов в **ARMA Стена** позволяет копировать входящий и исходящий трафик интерфейса на другой интерфейс. Функция используется для анализа трафика и должна поддерживаться принимающим устройством, например, коммутатором.

Для настройки зеркалирования loopback-интерфейса для входящего трафика необходимо ввести команду:

```
set interfaces loopback lo mirror ingress eth1
```

Входящий трафик на интерфейсе «lo» копируется на интерфейс «eth1». Интерфейсы приведены в качестве примера.

Для настройки зеркалирования loopback-интерфейса для исходящего трафика необходимо ввести команду:

```
set interfaces loopback lo mirror egress eth1
```

Исходящий трафик на интерфейсе «lo» копируется на интерфейс «eth1». Интерфейсы приведены в качестве примера.

3.6.4 Мониторинг loopback-интерфейса

1. Вывести информацию о loopback-интерфейсе:

```
admin@ngfwos:~$ show interfaces loopback

Codes: S - State, L - Link, u - Up, D - Down, A - Admin Down
Interface      IP Address      S/L
Description
-----
-----
lo             127.0.0.1/8     u/u
               ::1/128
admin@ngfwos:~$
```

2. Вывести подробную информацию о loopback-интерфейсе:

```
admin@ngfwos:~$ show interfaces loopback lo

lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group
default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 fe80::200:ff:fe00:0/64 scope link
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever

RX:      bytes  packets  errors  dropped  overrun      mcast
      133810617    618831        0         0          0          0
TX:      bytes  packets  errors  dropped  carrier  collisions
      133810617    618831        0         0          0          0

admin@ngfwos:~$
```

3.7 Интерфейс Dummy

Интерфейс **Dummy** выполняет функции, аналогичные интерфейсу **Loopback**. Однако в отличие от интерфейса **Loopback**, который может быть только один, интерфейс **Dummy** может быть несколько.

Примечание:

Dummy-интерфейсы всегда остаются в состоянии активен (UP) аналогично **Loopback**-интерфейсу.

На системах с несколькими резервными каналами связи и маршрутами рекомендуется использовать выделенный адрес для управления и динамических протоколов маршрутизации. Однако назначение этого адреса физическому каналу связи является рискованным: если этот канал выйдет из строя, адрес станет недоступным. Общее решение заключается в том, чтобы назначить управляющий адрес на **loopback**-интерфейс (виртуальный интерфейс обратной петли) или **dummy**-интерфейс (фиктивный интерфейс) и анонсировать этот адрес через все физические каналы, чтобы он был доступен через любой из них. Поскольку в системах на базе Linux может быть только один **loopback**-интерфейс, предпочтительнее использовать **dummy**-интерфейс для этой цели, поскольку их можно добавлять, удалять и отключать независимо друг от друга.

Интерфейс **Dummy** получают имена в формате «**dumN**», где «N» – идентификатор, присвоенный интерфейсу.

3.7.1 Настройка dummy-интерфейса

1. Назначить dummy-интерфейсу IP-адрес и префикс сети:

```
set interfaces dummy dumN address <address>
```

где:

- **<address>** – IPv4-адрес или IPv6-адрес для интерфейса в формате `<x.x.x.x/x>` и `<h:h:h:h:h:h:h/x>` соответственно. Возможно указать несколько адресов для интерфейса.

2. Установить описание для dummy-интерфейса:

```
set interfaces dummy dumN description <description>
```

где:

- **<description>** – описание интерфейса.

3. Установить значение MTU для dummy-интерфейса:

```
set interfaces dummy dumN mtu <mtu>
```

где:

- **<mtu>** – значение MTU для dummy-интерфейса. Возможно указать значение в диапазоне от «68» до «16000». По умолчанию используется значение «1500».

4. Отключить dummy-интерфейс:

```
set interfaces dummy dumN disable
```

После отключения интерфейс будет переведён в состояние административного отключения (A/D).

3.7.2 Дополнительные настройки dummy-интерфейса

1. Включить политику проверки источника по обратному пути, как указано в RFC 3704:

```
set interfaces dummy dumN ip source-validation <strict | loose | disable>
```

где **<strict | loose | disable>** - режим проверки источника. Возможно указать следующие значения:

- **strict** - каждый входящий пакет проверяется по FIB, и принимается только если пришёл через оптимальный (наилучший) обратный путь, определённый в таблице маршрутизации. Все пакеты, не удовлетворяющие этому условию, автоматически отбрасываются.

- **loose** - адрес источника каждого входящего пакета также проверяется по FIB, и если адрес источника не достижим ни через один интерфейс, проверка пакета будет неудачной.
- **disable** - нет проверки источника.

В настоящее время в RFC 3704 рекомендуется включать «strict» режим для предотвращения подмены IP адресов в результате DDos атак. При использовании асимметричной или другой сложной маршрутизации рекомендуется использовать «loose» режим.

2. Отключить IP-форвардинг (пересылку пакетов) для dummy-интерфейса:

```
set interfaces dummy dumN ip|ipv6 disable-forwarding
```

3. Настроить IPv6-адрес на dummy-интерфейсе, используя механизм EUI-64 для автоматической генерации уникального идентификатора интерфейса:

```
set interfaces dummy dumN ipv6 address eui64 <prefix>
```

где **<prefix>** - префикс IPv6 в формате <h:h:h:h:h:h:h/64>.

4. Отключить автоматическое назначение link-local IPv6-адреса на dummy-интерфейсе:

```
set interfaces dummy dumN ipv6 address no-default-link-local
```

5. Перенаправить входящий трафик с dummy-интерфейса на другой интерфейс:

```
set interfaces dummy dumN redirect <интерфейс>
```

где **<интерфейс>** - имя интерфейса, на который будет перенаправляться весь входящий трафик. Интерфейс должен быть определён в системе.

5. Разместить dummy-интерфейс в определённом экземпляре VRF:

```
set interfaces dummy dumN vrf <vrf>
```

где **<vrf>** - имя VRF.

3.7.3 SPAN

Функция зеркалирования интерфейсов в **ARMA Стена** позволяет копировать входящий и исходящий трафик интерфейса на другой интерфейс. Функция используется для анализа трафика и должна поддерживаться принимающим устройством, например, коммутатором.

Для настройки зеркалирования dummy-интерфейса для входящего трафика необходимо ввести команду:

```
set interfaces dummy dumN mirror ingress eth1
```

Входящий трафик на интерфейсе «dumN» копируется на интерфейс «eth1». Интерфейсы приведены в качестве примера.

Для настройки зеркалирования dummy-интерфейса для исходящего трафика необходимо ввести команду:

```
set interfaces dummy dumN mirror egress eth1
```

Исходящий трафик на интерфейсе «dumN» копируется на интерфейс «eth1». Интерфейсы приведены в качестве примера.

3.7.4 Мониторинг dummy-интерфейса

1. Вывести информацию о dummy-интерфейсах:

```
admin@ngfwos:~$ show interfaces dummy
```

Codes: S - State, L - Link, u - Up, D - Down, A - Admin Down

Interface	IP Address	S/L
Description		
-----	-----	---
dumN	x.x.x.x/x	u/u

```
admin@ngfwos:~$
```

2. Вывести подробную информацию о dummy-интерфейсе:

```
admin@ngfwos:~$ show interfaces dummy dumN
```

dum1: <BROADCAST,NOARP,UP,LOWER_UP> mtu 16000 qdisc noqueue state UNKNOWN group default qlen 1000

link/ether 4a:7b:19:48:fd:1e brd ff:ff:ff:ff:ff:ff

inet x.x.x.x/x brd x.x.x.x scope global dum1

valid_lft forever preferred_lft forever

inet6 fe80::487b:19ff:fe48:fd1e/64 scope link

valid_lft forever preferred_lft forever

RX:	bytes	packets	errors	dropped	overrun	mcast
	0	0	0	0	0	0
TX:	bytes	packets	errors	dropped	carrier	collisions
	0	0	0	0	0	0

```
admin@ngfwos:~$
```

3.8 WireGuard

WireGuard – это крайне простой, быстрый и современный VPN, который использует передовые методы криптографии.

В системе **ARMA Стена WireGuard** функционирует путём добавления сетевого интерфейса, подобно ethN, который именуется как «**wgN**», где «**N**» – идентификатор, присвоенный интерфейсу (wg0, wg1, wg2, и т.д.).

3.8.1 Настройка интерфейса WireGuard

1. Указать IP-адрес для интерфейса:

```
set interfaces wireguard <wgN> address <address>
```

где:

- **<wgN>** - имя интерфейса WireGuard;
- **<address>** - IP-адрес. Значение указывается в формате: **<x.x.x.x/x>** - для IPv4, **<h:h:h:h:h:h:h/x>** - для IPv6.

2. Добавить текстовое описание для интерфейса:

```
set interfaces wireguard <wgN> description <description>
```

где **<description>** - текстовое описание интерфейса.

3. Генерация ключей (приватного и публичного) для использования в WireGuard:

```
admin@ngfwos:~$ generate pki wireguard key-pair
```

Пример генерации приватного и публичного ключа:

```
admin@ngfwos:~$ generate pki wireguard key-pair
Private key: iP/CtjqjXCU2DZl6ne/Suz2XXSaKtKDJYXUWuxBVWg=
Public key: mnLBjPePCpki3wZ6gXXXfmZ9g/4ATKPKoTQdRMOq/Hw=

admin@ngfwos:~$
```

4. Установить приватный ключ для интерфейса WireGuard:

```
set interfaces wireguard <wgN> private-key <private-key>
```

где **<private-key>** - приватный ключ в кодировке Base64.

5. Генерация ключей (приватного и публичного) для использования в WireGuard и установка приватного ключа на интерфейс WireGuard:

```
admin@ngfwos:~$ generate pki wireguard key-pair install interface <wgN>
```

Данная команда выполняет функции двух предшествующих. Она осуществляет генерацию ключей и сохраняет закрытый ключ в соответствующей секции конфигурационного файла.

6. Установить порт, который будет использоваться интерфейсом WireGuard для прослушивания входящих подключений:

```
set interfaces wireguard <wgN> port <1-65535>
```

где **<1-65535>** - номер порта. Возможно указать значение в диапазоне от «1» до «65535».

7. Создать блок настроек удалённого узла (пир) в интерфейсе Wireguard:

```
set interfaces wireguard <wgN> peer <name>
```

где **<name>** - имя пира, с которым будет установлен защищённый туннель.

- 7.1. Установить IP-адрес пира:

```
set interfaces wireguard <wgN> peer <name> address <address>
```

где **<address>** - IP-адрес в формате <x.x.x.x> для IPv4 или <h:h:h:h:h:h:h> для IPv6.

- 7.2. Указать сеть, которой разрешено проходить через пир:

```
set interfaces wireguard <wgN> peer <name> allowed-ips <address>
```

где **<address>** - сети в формате <x.x.x.x/x> или <h:h:h:h:h:h:h/x>. Возможно определить и маршрутизировать несколько сетей.

Примечание:

Возможно установить один и тот же параметр «allowed_ips» для нескольких пиров WireGuard.

- 7.3. Добавить текстовое описание для пира:

```
set interfaces wireguard <wgN> peer <name> description <description>
```

- 7.4. Отключение пира с сохранением текущих настроек:

```
set interfaces wireguard <wgN> peer <name> disable
```

- 7.5. Установить интервал отправки сообщений проверки соединения:

```
set interfaces wireguard <wgN> peer <name> persistent-keepalive <1-65535>
```

где **<1-65535>** - значение интервала в секундах. Возможно указать значение в диапазоне от «1» до «65535».

7.6. Установить номер порта, используемого для соединения с пиром:

```
set interfaces wireguard <wgN> peer <name> port <1-65535>
```

где **<1-65535>** - номер порта, по которому локальное устройство будет доступно для построения туннеля через интерфейс WireGuard. Возможно указать значение в диапазоне от «1» до «65535».

7.7. Указать открытый ключ пира в кодировке base64:

```
set interfaces wireguard <wgN> peer <name> public-key <public-key>
```

где **<public-key>** - открытый ключ.

7.8. Установить предварительно согласованный ключ в кодировке base64 для пира:

```
set interfaces wireguard <wgN> peer <name> preshared-key <preshared-key>
```

где **<preshared-key>** - предварительно согласованный ключ.

Параметр обеспечивает дополнительный уровень защиты для VPN-соединения посредством применения предварительно согласованного ключа для шифрования данных. Это означает, что сетевой трафик между узлами будет дополнительно защищён с использованием указанного ключа, что значительно усложняет возможность перехвата и дешифровки данных для потенциальных злоумышленников.

8. Указать размера MTU для интерфейса:

```
set interfaces wireguard <wgN> mtu <mtu>
```

где **<mtu>** - размер MTU. Возможно указать значения в диапазоне от «68» до «16000».

9. Включает режим, при котором для каждого пира создаётся отдельный поток обработки на указанном интерфейсе:

```
set interfaces wireguard <wgN> per-client-thread
```

Примечание:

Опция per-client-thread является факультативной. Она позволяет каждому клиентскому соединению обрабатываться в отдельном потоке, что улучшает параллельную обработку и повышает общую производительность системы, особенно на многопроцессорных архитектурах с поддержкой многопоточности. Сегментация обработки запросов на уровне клиентских потоков может сократить время отклика системы за счёт уменьшения конкуренции за ресурсы

центрального процессора между различными клиентскими соединениями.

10. Установить метку (firewall mark), которая будет присвоена всем пакетам, отправляемых через интерфейс:

```
set interfaces wireguard <wgN> fwmark <number>
```

где **<number>** - 32-битное значение, устанавливаемое для всех исходящих пакетов. По умолчанию используется значение «0» - отключено.

11. Отключение интерфейса с сохранением текущих настроек:

```
set interfaces wireguard <wgN> disable
```

3.8.2 Дополнительные настройки интерфейса WireGuard

1. Установка значения TCP MSS:

```
set interfaces wireguard <wgN> ip adjust-mss <mss | clamp-mss-to-pmtu>
```

где:

- **<mss>** - значение MSS. Возможно указать значение в диапазоне от «536» до «65535».
- **<clamp-mss-to-pmtu>** - автоматически устанавливать MSS в нужное значение.

Поскольку обнаружение PMTU в сети Интернет работает нестабильно, иногда возникает необходимость ограничить значение TCP MSS. Это поле находится в опциях TCP в части SYN-пакета. Установив значение MSS, система сообщает удалённой стороне, что не следует отправлять пакеты размером больше этого значения.

2. Установка тайм-аута записи в ARP-кэш для интерфейса:

```
set interfaces wireguard <wgN> ip arp-cache-timeout <1-86400>
```

где **<1-86400>** - значение тайм-аута записи в ARP-кэш в секундах. Возможно указать значение в диапазоне от «1» до «86400». По умолчанию используется значение «30».

3. Отключить фильтрацию ARP на интерфейсе:

```
set interfaces wireguard <wgN> ip disable-arp-filter
```

Если параметр не установлен (по умолчанию), это позволяет иметь несколько сетевых интерфейсов в одной подсети и отвечать на ARP для каждого интерфейса в зависимости от того, будет ли ядро направлять пакет с IP-адресом

ARP через этот интерфейс. Для этого необходимо использовать маршрутизацию на основе источника.

4. Отключить переадресацию IP на интерфейсе:

```
set interfaces wireguard <wgN> ip disable-forwarding
```

Если параметр установлен, интерфейс переходит в режим хоста, и переадресация IPv6 на этом интерфейсе отключается.

5. Включить направленную широковещательную пересылку на интерфейсе:

```
set interfaces wireguard <wgN> ip enable-directed-broadcast
```

В случае активации данной опции, входящие пакеты направленной широковещательной рассылки IP будут перенаправляться через указанный интерфейс. В случае если данный параметр не задан (по умолчанию), входящие пакеты направленной широковещательной рассылки IP не будут передаваться.

6. Включить приём ARP пакетов на интерфейсе:

```
set interfaces wireguard <wgN> ip enable-arp-accept
```

Определяет поведение для ARP-пакетов, IP-записи которых ещё не присутствуют в ARP-таблице. Если эта настройка включена, то создаются новые записи в ARP-таблице. Как ответы, так и запросы типа Gratuitous ARP будут вызывать обновление ARP-таблицы, если эта настройка включена. Если в ARP-таблице уже содержится IP-адрес кадра Gratuitous ARP, то ARP-таблица будет обновлена независимо от того, включена или выключена эта настройка.

7. Включить анонсирование ARP пакетов на интерфейсе:

```
set interfaces wireguard <wgN> ip enable-arp-announce
```

Если параметр не задан, используется любой локальный адрес, который настроен на любом интерфейсе. Если параметр установлен, рекомендуется избегать использования локальных адресов, которые не входят в подсеть цели для данного интерфейса. Этот режим полезен, когда целевые узлы, доступные через данный интерфейс, требуют, чтобы IP-адрес источника в ARP-запросах был частью их логической сети, настроенной на принимающем интерфейсе. При генерации запроса система проверяет все подсети, включающие целевой IP-адрес, и сохраняет адрес источника, если он принадлежит такой подсети. Если подходящей подсети не найдено, система выбирает адрес источника в соответствии с правилами для уровня 2.

8. Включить игнорирование ARP пакетов на интерфейсе:

```
set interfaces wireguard <wgN> ip enable-arp-ignore
```

Данный параметр определяет режимы отправки ответов на ARP-запросы, которые разрешают локальные целевые IP-адреса. Если параметр включён, ответ будет отправлен только в том случае, если целевой IP-адрес является локальным адресом, настроенным на входящем интерфейсе. Если параметр отключён (по умолчанию), ответ будет получен для любого локального целевого IP-адреса, настроенного на любом интерфейсе.

9. Включить прокси ARP на интерфейсе:

```
set interfaces wireguard <wgN> ip enable-proxy-arp
```

Прокси ARP позволяет интерфейсу отвечать своим MAC-адресом на ARP-запросы IP-адресов назначения в подсетях, подключённых к другим интерфейсам системы. Последующие пакеты, отправленные на эти IP-адреса назначения, пересылаются системой соответствующим образом.

10. Включить прокси ARP частного VLAN на интерфейсе:

```
set interfaces wireguard <wgN> ip proxy-arp-pvlan
```

Разрешить ответы ARP-прокси с того же интерфейса, с которого был получен ARP-запрос или запрос на предложение. Это необходимо для поддержки функций Ethernet-коммутаторов, описанных в RFC 3069, где отдельные порты не могут напрямую связываться друг с другом, но могут связываться с вышестоящим маршрутизатором. Как указано в RFC 3069, этого можно достичь путём включения прокси-ARP.

Необязательно использовать вместе с `proxy_arp`.

11. Включить политику проверки источника по обратному пути, как указано в RFC 3704:

```
set interfaces wireguard <wgN> ip|ipv6 source-validation <strict | loose | disable>
```

где **<strict | loose | disable>** - режим проверки источника. Возможно указать следующие значения:

- **strict** - каждый входящий пакет проверяется по FIB, и принимается только если пришёл через оптимальный (наилучший) обратный путь, определённый в таблице маршрутизации. Все пакеты, не удовлетворяющие этому условию, автоматически отбрасываются.
- **loose** - адрес источника каждого входящего пакета также проверяется по FIB, и если адрес источника не достижим ни через один интерфейс, проверка пакета будет неудачной.
- **disable** - нет проверки источника.

В настоящее время в RFC 3704 рекомендуется включать strict режим для предотвращения подмены IP адресов в результате DDos атак. При использовании асимметричной или другой сложной маршрутизации рекомендуется использовать loose режим.

12. Включить получение IPv6-адреса с помощью автоконфигурации без статического изменения (SLAAC):

```
set interfaces wireguard <wgN> ipv6 address autoconf
```

В соответствии с RFC 4862, хосты IPv6 могут автоматически настраиваться при подключении к сети IPv6 с использованием протокола Neighbor Discovery Protocol (NDP) через сообщения ICMPv6 об обнаружении маршрутизатора. При первом подключении к сети хост отправляет многоадресный запрос link-local router solicitation для получения параметров конфигурации. Маршрутизаторы отвечают на этот запрос пакетом router advertisement, содержащим параметры конфигурации уровня Интернета.

Примечание:

Данный метод автоматически отключает пересылку трафика IPv6 на сетевом интерфейсе.

13. Включить префикс EUI-64 на основе MAC адреса для IPv6 адреса интерфейса:

```
set interfaces wireguard <wgN> ipv6 address eui64 <prefix>
```

где **<prefix>** - сеть IPv6 в формате <h:h:h:h:h:h:h/64>.

14. Удалить локальный адрес IPv6 по умолчанию для интерфейса:

```
set interfaces wireguard <wgN> ipv6 address no-default-link-local
```

15. Отключить IP переадресацию на интерфейсе:

```
set interfaces wireguard <wgN> ipv6 disable-forwarding
```

В случае установки, интерфейс будет переведён в режим хоста, а переадресация IPv6 на данном интерфейсе будет отключена.

16. Установить значения TCP MSS:

```
set interfaces wireguard <wgN> ipv6 adjust-mss <mss | clamp-mss-to-pmtu>
```

где:

- **<mss>** - значение MSS. Возможно указать значение в диапазоне от «536» до «65535».
- **<clamp-mss-to-pmtu>** - автоматически устанавливать MSS в нужное значение.

17. Принимать обнаружение дублирующегося адреса:

```
set interfaces wireguard <wgN> ipv6 accept-dad <0-2>
```

где **<0-2>** - режим приёма DAD. Возможно указать следующие значения:

- **0** - отключить DAD;
- **1** - включить DAD (по умолчанию);
- **2** - включить DAD и отключить работу IPv6, если обнаружен дублированный MAC-адрес link-local.

18. Установить количество сообщений NS для отправки при выполнении DAD:

```
set interfaces wireguard <wgN> ipv6 dup-addr-detect-transmits <n>
```

где **<n>** - количество NS-сообщений. В случае установки значения «0», функция обнаружения дубликатов адресов (DAD) будет отключена. По умолчанию используется значение «1».

19. Настроить времена достижимости для IPv6-адресов на интерфейсе WireGuard:

```
set interfaces wireguard <wgN> ipv6 base-reachable-time <1-86400>
```

где **<1-86400>** - время в секундах, в течение которого соседний узел считается достижимым после последнего успешного обмена сообщениями. Возможно указать значение в диапазоне от «1» до «86400». По умолчанию используется значение «30». Это значение используется для расчёта времени жизни записей в таблице соседей.

20. Разместить интерфейс в указанном экземпляре VRF:

```
set interfaces wireguard <wgN> vrf <vrf>
```

где **<vrf>** - имя экземпляра VRF.

3.8.3 SPAN

Функция зеркалирования интерфейсов в **ARMA Стена** позволяет копировать входящий и исходящий трафик интерфейса на другой интерфейс. Функция используется для анализа трафика и должна поддерживаться принимающим устройством, например, коммутатором.

Для настройки зеркалирования интерфейса WireGuard для входящего трафика необходимо ввести команду:

```
set interfaces wireguard <wgN> mirror ingress eth1
```

Входящий трафик на интерфейсе «wgN» копируется на интерфейс «eth1». Интерфейсы приведены в качестве примера.

Для настройки зеркалирования интерфейса WireGuard для исходящего трафика необходимо ввести команду:

```
set interfaces wireguard <wgN> mirror egress eth1
```

Исходящий трафик на интерфейсе «wgN» копируется на интерфейс «eth1». Интерфейсы приведены в качестве примера.

3.8.4 Настройка WireGuard в режиме «сеть - сеть»

В качестве примера настройки WireGuard в режиме «**сеть - сеть**» будет использоваться схема стенда, представленная на рисунке (см. [Рисунок – Схема стенда для настройки VPN в режиме «сеть - сеть»](#)).

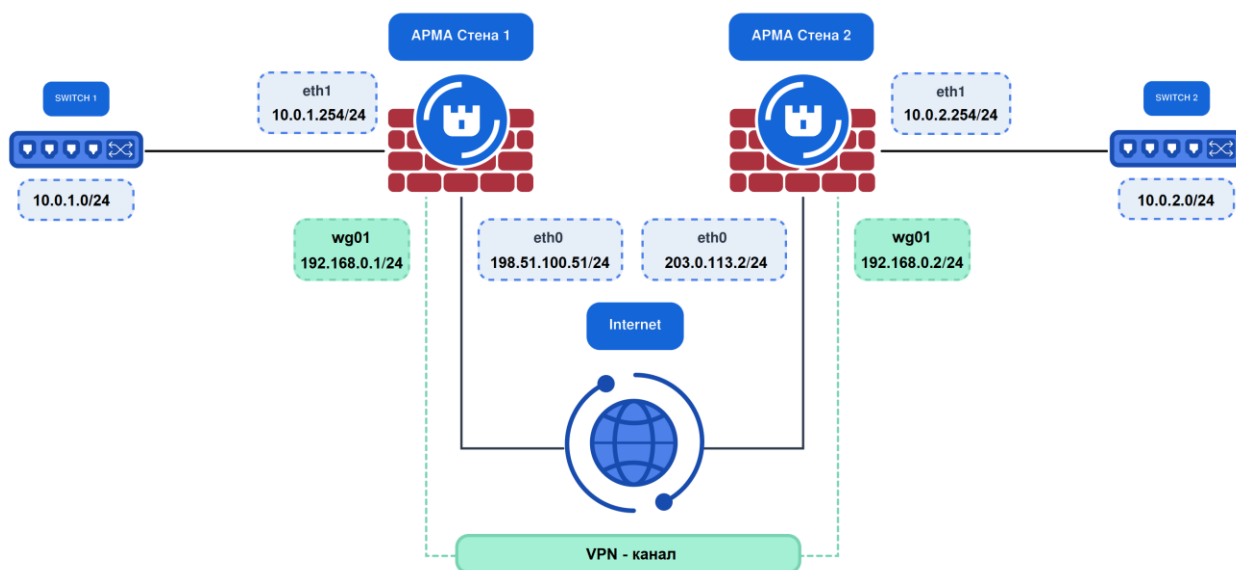


Рисунок – Схема стенда для настройки VPN в режиме «сеть - сеть»

3.8.4.1 Генерация ключей

Для генерации ключей на обоих **АРМА Стена** необходимо в режиме эксплуатации ввести следующую команду:

```
admin@ngfwos:~$ generate pki wireguard key-pair
```

Автоматически будет выведено содержимое закрытого и открытого ключей – «**Private key**» и «**Public key**» соответственно.

3.8.4.2 Настройка АРМА Стена 1

3.8.4.2.1 Настройка туннеля

Для конфигурирования туннельного интерфейса **АРМА Стена 1** необходимо ввести следующие команды:

```
set interfaces wireguard wg01 address 192.168.0.1/24
set interfaces wireguard wg01 description 'VPN-to-Client'
set interfaces wireguard wg01 peer Client address 203.0.113.2
set interfaces wireguard wg01 peer Client allowed-ips 10.0.2.0/24
set interfaces wireguard wg01 peer Client port 51820
set interfaces wireguard wg01 peer Client public-key 'ExAmPLekeyCl'
set interfaces wireguard wg01 port 51820
set interfaces wireguard wg01 private-key 'ExAmPLePrivatekeyS'
```

где:

- «**192.168.0.1/24**» – локальный IP-адрес;
- «**VPN-to-Client**» – описание интерфейса «wg01»;
- «**10.0.2.0/24**» – удалённая сеть;
- «**192.168.0.0/24**» – туннельная сеть;
- «**203.0.113.2**» – IP-адрес интерфейса **ARMA Стена 2** с доступом к сети Интернет;
- «**51820**» – порт;
- «**ExAmPLekeyCl**» – содержимое открытого ключа **ARMA Стена 2**;
- «**ExAmPLePrivatekeyS**» – содержимое закрытого ключа **ARMA Стена 1**.

Зафиксировать изменения с помощью ввода команд «**commit**» и «**save**».

3.8.4.2.2 Настройка статического маршрута

Для настройки статического маршрута на **ARMA Стена 1** необходимо ввести следующую команду:

```
set protocols static route 10.0.2.0/24 interface wg01
```

где «**10.0.2.0/24**» – удалённая сеть.

Зафиксировать изменения с помощью ввода команд «**commit**» и «**save**».

3.8.4.3 Настройка ARMA Стена 2

3.8.4.3.1 Настройка туннеля

Для конфигурирования туннельного интерфейса **ARMA Стена 2** необходимо ввести следующие команды:


```
set interfaces wireguard wg01 address 192.168.0.2/24
set interfaces wireguard wg01 description 'VPN-to-Server'
set interfaces wireguard wg01 peer Server address 198.51.100.51
set interfaces wireguard wg01 peer Server allowed-ips 10.0.1.0/24
set interfaces wireguard wg01 peer Server port 51820
set interfaces wireguard wg01 peer Server public-key "ExAmPLekeyS"
set interfaces wireguard wg01 port 51820
set interfaces wireguard wg01 private-key 'ExAmPLePrivatekeyCI'
```

где:

- «**192.168.0.2/24**» – локальный IP-адрес;
- «**VPN-to-Server**» – описание интерфейса «wg01»;
- «**10.0.1.0/24**» – удалённая сеть;
- «**192.168.0.0/24**» – туннельная сеть;
- «**198.51.100.51**» – IP-адрес интерфейса **ARMA Стена 1** с доступом к сети Интернет;
- «**51820**» – порт;
- «**ExAmPLekeyS**» – содержимое открытого ключа **ARMA Стена 1**;
- «**ExAmPLePrivatekeyCI**» – содержимое закрытого ключа **ARMA Стена 2**.

Зафиксировать изменения с помощью ввода команд «**commit**» и «**save**».

3.8.4.3.2 Настройка статического маршрута

Для настройки статического маршрута на **ARMA Стена 2** необходимо ввести следующую команду:

```
set protocols static route 10.0.1.0/24 interface wg01
```

где «**10.0.1.0/24**» – удалённая сеть.

Зафиксировать изменения с помощью ввода команд «**commit**» и «**save**».

3.9 VXLAN

VXLAN (Virtual Extensible LAN) – технология сетевой виртуализации, предназначенная для преодоления ограничений масштабируемости при развёртывании крупных облачных инфраструктур. **VXLAN** реализует инкапсуляцию Ethernet-кадров уровня 2 модели OSI в UDP-дейтаграммы уровня 4. Стандартный UDP-порт, выделенный IANA для VXLAN, – **4789**.

Туннелирование осуществляется между конечными точками **VXLAN** (VTEP – VXLAN Tunnel Endpoints), которые могут быть реализованы как на физических, так и на

виртуальных коммутационных портах и отвечают за инкапсуляцию и декапсуляцию трафика.

Для корректной работы **VXLAN** необходимо:

- открыть UDP-порт 4789 на межсетевом экране;
- установить значение MTU не менее 1554 байт на всех интерфейсах, участвующих в передаче VXLAN-трафика.

3.9.1 Общие параметры

1. Назначение IP-адресов интерфейсу:

```
set interfaces vxlan <vxlanN> address <address>
```

где:

- **<vxlanN>** – имя VXLAN-интерфейса, где «N» – числовой идентификатор, задаваемый пользователем;
- **<address>** – IP-адрес интерфейса. Допускается многократное указание адресов в форматах: IPv4 – <x.x.x.x/x>, IPv6 – <h:h:h:h:h:h:h/x>.

2. Указание описания интерфейса:

```
set interfaces vxlan <vxlanN> description <description>
```

где **<description>** – текстовое описание vxlan интерфейса.

3. Отключение интерфейса:

```
set interfaces vxlan <vxlanN> disable
```

Команда переводит интерфейс в административно выключенное состояние (A/D). Конфигурация сохраняется.

4. Назначение пользовательского MAC-адреса:

```
set interfaces vxlan <vxlanN> mac <xx:xx:xx:xx:xx:xx>
```

где **<xx:xx:xx:xx:xx:xx>** – пользовательский MAC-адрес.

5. Установка значения MTU для интерфейса:

```
set interfaces vxlan <vxlanN> mtu <mtu>
```

где **<mtu>** – размер максимальной передаваемой единицы (MTU) в байтах. Возможно указать значения в диапазоне от «1200» до «16000». По умолчанию используется значение «1500».

6. Задание идентификатора VXLAN-сегмента (VNI):

```
set interfaces vxlan <vxlanN> vni <number>
```

где **<number>** - 24-битное значение, уникально определяющие сегмент. Возможно указать значения в диапазоне от «0» до «16777214».

Позволяет одновременно использовать до 16 миллионов VXLAN-сегментов в пределах одного административного домена.

7. Указание UDP-порта удалённой VTEP:

```
set interfaces vxlan <vxlanN> port <port>
```

где **<port>** - номер UDP-порта. Возможно указать значения в диапазоне от «1» до «65535». Значение по умолчанию - «4789».

8. Указание исходного IP-адреса транспортной сети:

```
set interfaces vxlan <vxlanN> source-address <address>
```

где **<address>** - IP-адрес в формате IPv4 (x.x.x.x) или IPv6 (h:h:h:h:h:h:h:h). Обязателен при развёртывании VXLAN через L2VPN/EVPN.

9. Включение поддержки VXLAN-GPE:

```
set interfaces vxlan <vxlanN> gpe
```

При включении данной опции VXLAN-трафик инкапсулируется с использованием формата VXLAN-GPE (RFC 9184), что позволяет транспортировать не только Ethernet-кадры, но и другие типы сетевых пакетов (например, IPv4, IPv6, MPLS) через VXLAN-туннель.

Примечание:

Функция доступна только при включённом внешнем (external) режиме.

10. Включение внешнего (external) режима:

```
set interfaces vxlan <vxlanN> parameters external
```

В данном режиме управление инкапсуляцией и маршрутизацией VXLAN-трафика передаётся внешнему агенту (например, контроллеру или пользовательскому dataplane).

11. Включение подавления ARP/NDP-запросов:

```
set interfaces vxlan <vxlanN> parameters neighbor-suppress
```

При активации устройство не пересылает ARP- (IPv4) или NDP- (IPv6) запросы, если запрашиваемый MAC-адрес уже присутствует в локальной FDB. Вместо этого устройство само генерирует и отправляет ответ от имени целевого узла.

12. Отключение динамического обучения FDB:

```
set interfaces vxlan <vxlanN> parameters nolearning
```

Запрещает автоматическое добавление MAC-адресов в таблицу FDB на основе входящего трафика. Все записи должны быть заданы статически или предоставлены внешним контроллером (например, через EVPN).

13. Включение фильтрации по VNI:

```
set interfaces vxlan <vxlanN> parameters vni-filter
```

При активации принимаются только те VXLAN-пакеты, у которых VNI присутствует в предварительно настроенной таблице разрешённых идентификаторов. Остальные пакеты отбрасываются.

Примечание:

При отсутствии настроенной таблицы разрешённых VNI интерфейс может не принимать трафик. Необходимо обеспечить наличие механизма управления VNI (например, EVPN).

14. Настройка бита DF в IP-заголовке транспортного пакета:

```
set interfaces vxlan <vxlanN> parameters ip df <mode>
```

где **<mode>** – режим обработки бита Don't Fragment. Возможно указать следующие значения:

- **set** – всегда устанавливать бит DF в 1. Инкапсулированные пакеты не могут быть фрагментированы промежуточными маршрутизаторами. Если MTU недостаточно, пакет будет отброшен, и отправителю может быть возвращено сообщение ICMP «Fragmentation Needed».
- **unset** – всегда сбрасывать бит DF в 0 (значение по умолчанию). Разрешает фрагментацию инкапсулированных пакетов на транспортном уровне при необходимости.
- **inherit** – копировать значение бита DF из исходного (внутреннего) IP-заголовка инкапсулируемого пакета. Поведение фрагментации наследуется от оригинального трафика.

15. Установка значения поля TOS:

```
set interfaces vxlan <vxlanN> parameters ip tos <value>
```

где **<value>** – целое число в диапазоне от «0» до «99», представляющее значение TOS.

16. Установка значения TTL:

```
set interfaces vxlan <vxlanN> parameters ip ttl <value>
```

где **<value>** - значение Time to Live:

- **0** - включает режим наследования: значение TTL копируется из исходного (внутреннего) IP-заголовка инкапсулируемого пакета;
- **Значение в диапазоне от «1» до «255»** - устанавливает фиксированное значение TTL для всех исходящих инкапсулированных пакетов, независимо от содержимого внутреннего трафика.

По умолчанию используется значение «16».

17. Установка Flow Label для IPv6:

```
set interfaces vxlan <vxlanN> parameters ipv6 flowlabel <value>
```

где **<value>** – значение поля Flow Label. Возможно указать следующие значения:

- **inherit** – копировать значение Flow Label из исходного (внутреннего) IPv6-заголовка;
- **0x0–0xFFFFF** – задать фиксированное шестнадцатеричное значение в диапазоне от «0x0» до «0xFFFFF». Это значение будет использоваться во всех исходящих инкапсулированных IPv6-пакетах, независимо от содержимого внутреннего трафика.

18. Перенаправление трафика на другой интерфейс:

```
set interfaces vxlan <vxlanN> redirect <interface-name>
```

где **<interface-name>** - имя существующего сетевого интерфейса назначения, на который будет перенаправлен трафик.

Используется для передачи трафика внешним анализаторам или пользовательским dataplane-приложениям без обработки в стандартном сетевом стеке.

19. Привязка интерфейса к VRF:

```
set interfaces vxlan <vxlanN> vrf <vrf-name>
```

где **<vrf-name>** - имя существующего VRF-экземпляра в системе.

3.9.2 Режимы туннеля

VXLAN поддерживает два режима установления туннелей: **multicast** и **unicast**.

Multicast-режим

Активируется при указании multicast-группы:

```
set interfaces vxlan <vxlanN> group <multicast-address>
```

где **<multicast-address>** - IPv4 (x.x.x.x) или IPv6 (h:h:h:h:h:h:h:h) multicast-адрес.

Дополнительно требуется указать интерфейс источника:

```
set interfaces vxlan <vxlanN> source-interface <interface>
```

где **<interface>** - имя физического или логического интерфейса, через который передаётся VXLAN-трафик. Параметр обязателен в multicast-режиме.

Unicast-режим

Активируется при указании адреса удалённой VTEP:

```
set interfaces vxlan <vxlanN> remote <address>
```

где **<address>** - IPv4 (x.x.x.x) или IPv6 (h:h:h:h:h:h:h:h) адрес удалённой стороны.

3.9.3 Single VXLAN Device (SVD)

FRRouting (FRR) поддерживает метод настройки VLAN–VNI-ассоциаций через единый контейнерный VXLAN-интерфейс – Single VXLAN Device (SVD). Это позволяет назначать несколько VLAN–VNI-сопоставлений одному интерфейсу, устраняя необходимость создания отдельного VXLAN-интерфейса на каждый VNI и повышая масштабируемость.

Конфигурация:

```
set interfaces vxlan <vxlanN> vlan-to-vni <vlan-id> vni <vni-id>
```

где:

- **<vlan-id>** - идентификатор VLAN в диапазоне от «0» до «4094» или диапазон в формате <start-end> (например, 100-200);
- **<vni-id>** - идентификатор VLAN в диапазоне от «0» до «16777214» или диапазон в формате <start-end> (например, 10100-10200).

3.9.4 Параметры маршрутизации IPv4

1. Корректировка MSS:

```
set interfaces vxlan <vxlanN> ip adjust-mss <mss | clamp-mss-to-pmtu>
```

где:

- **<mss>** - фиксированное значение MSS в диапазоне от «536» до «65535».

- **<clamp-mss-to-pmtu>** - автоматически вычисляет и устанавливает MSS на основе Path MTU (PMTU) для каждого соединения. $MSS = PMTU - 40$ (20 байт IP + 20 байт TCP).

2. Тайм-аут ARP-кэша:

```
set interfaces vxlan <vxlanN> ip arp-cache-timeout <timeout>
```

где **<timeout>** - значение тайм-аута записи в ARP-кэш в секундах. Возможно указать значение в диапазоне от «1» до «86400». По умолчанию используется значение «30».

3. Отключение ARP-фильтрации:

```
set interfaces vxlan <vxlanN> ip disable-arp-filter
```

Разрешает ответ на ARP-запросы любым интерфейсом, на котором настроен запрашиваемый IP-адрес.

4. Отключение IP-маршрутизации:

```
set interfaces vxlan <vxlanN> ip disable-forwarding
```

Переводит интерфейс в режим хоста.

5. Разрешение направленной широковещательной пересылки:

```
set interfaces vxlan <vxlanN> ip enable-directed-broadcast
```

При активации данной опции пакеты, адресованные широковещательному адресу подсети, связанной с интерфейсом, будут рассылаться всем хостам в этой подсети.

6. Автоматическое создание записей ARP по GARP:

```
set interfaces vxlan <vxlanN> ip enable-arp-accept
```

Разрешает автоматическое создание новых записей в ARP-таблице интерфейса vxlan при получении gratuitous ARP-пакетов (GARP). Эта функция ускоряет обновление ARP-кэша при динамических изменениях в сети.

7. Ограниченный выбор исходного адреса в ARP-запросах:

```
set interfaces vxlan <vxlanN> ip enable-arp-announce
```

Если параметр не задан, используется любой локальный адрес, который настроен на любом интерфейсе. Если параметр установлен, рекомендуется избегать использования локальных адресов, которые не входят в подсеть цели для данного интерфейса. Этот режим полезен, когда целевые узлы, доступные через данный интерфейс, требуют, чтобы IP-адрес источника в ARP-запросах

был частью их логической сети, настроенной на принимающем интерфейсе. При генерации запроса система проверяет все подсети, включающие целевой IP-адрес, и сохраняем адрес источника, если он принадлежит такой подсети. Если подходящей подсети не найдено, система выбирает адрес источника в соответствии с правилами для уровня 2.

8. Игнорирование ARP-запросов для чужих адресов:

```
set interfaces vxlan <vxlanN> ip enable-arp-ignore
```

Ограничивает ответы на входящие ARP-запросы только в том случае, если запрашиваемый IP-адрес назначен непосредственно на интерфейс, через который получен ARP-запрос. При активации данной опции система игнорирует ARP-запросы, направленные на локальные IP-адреса, назначенные на других интерфейсах. Если параметр отключён (по умолчанию), ответ будет получен для любого локального целевого IP-адреса, настроенного на любом интерфейсе.

9. Включение Proxy ARP:

```
set interfaces vxlan <vxlanN> ip enable-proxy-arp
```

При активации система будет отвечать на ARP-запросы, направленные на IP-адреса, не назначенные локально на этом интерфейсе, но доступные через маршрутизацию на другие интерфейсы или подсети. В ответе указывается MAC-адрес интерфейса vxlan, что позволяет отправителю направлять трафик на этот MAC, после чего система пересылает пакеты по назначению.

10. Включение Private VLAN Proxy ARP:

```
set interfaces vxlan <vxlanN> ip proxy-arp-pvlan
```

Эта функция позволяет системе отвечать на ARP-запросы отправителю на тот же интерфейс, с которого был получен запрос, даже если запрашиваемый IP-адрес принадлежит другому хосту в той же подсети. Это необходимо для поддержки сценариев изоляции портов (port isolation), при которых хосты в одном L2-сегменте не могут напрямую обмениваться трафиком, но могут взаимодействовать через центральный маршрутизатор (например, шлюз).

Необязательно использовать вместе с proxy_arp.

11. Проверка источника по обратному пути (RPF):

```
set interfaces vxlan <vxlanN> ip source-validation <strict | loose | disable>
```

где **<strict | loose | disable>** - режим проверки источника. Возможно указать следующие значения:

- **strict** - каждый входящий пакет проверяется по FIB, и принимается только если пришёл через оптимальный (наилучший) обратный путь, определённый в таблице маршрутизации. Все пакеты, не удовлетворяющие этому условию, автоматически отбрасываются.
- **loose** - адрес источника каждого входящего пакета также проверяется по FIB, и если адрес источника не достижим ни через один интерфейс, проверка пакета будет неудачной.
- **disable** - нет проверки источника. Все пакеты принимаются независимо от маршрутизации.

Рекомендуется *strict* для защиты от IP-spoofing.

3.9.5 Параметры маршрутизации IPv6

1. Настройка DAD:

```
set interfaces vxlan <vxlanN> ipv6 accept-dad <mode>
```

где **<mode>** – режим приёма DAD. Возможно указать следующие значения:

- **0** – DAD отключён. Адреса (включая link-local) активируются немедленно без проверки дублирования.
- **1** – DAD включён (по умолчанию). Система отправляет Neighbor Solicitation (NS) для проверки уникальности адреса. Если получен ответ – адрес не активируется.
- **2** – DAD включён с дополнительной проверкой MAC-адреса. Если обнаружен дубликат link-local-адреса, сгенерированного на основе MAC-адреса интерфейса, IPv6 на интерфейсе полностью отключается.

DAD – обязательная процедура в IPv6 (RFC 4862), предназначенная для проверки уникальности адреса в пределах локального канального сегмента до его активации.

2. Включение поддержки Stateless Address Autoconfiguration (SLAAC):

```
set interfaces vxlan <vxlanN> ipv6 address autoconf
```

При активации интерфейс автоматически конфигурирует свои IPv6-адреса на основе Router Advertisement (RA) сообщений, получаемых от локальных IPv6-маршрутизаторов через протокол Neighbor Discovery Protocol (NDP).

Примечание:

Данный метод отключает IPv6-маршрутизацию (forwarding) на интерфейсе vxlan, переводя его в режим хоста. Согласно требованию RFC 4862 – устройства, использующие SLAAC, не должны одновременно быть маршрутизаторами.

3. Получить IPv6-адрес на VXLAN-интерфейс с использованием метода EUI-64 (RFC 4291):

```
set interfaces vxlan <vxlanN> ipv6 address eui64 <prefix>
```

где **<prefix>** - сеть IPv6 в формате <h:h:h:h:h:h:h/64>.

4. Отключение link-local-адреса:

```
set interfaces vxlan <vxlanN> ipv6 address no-default-link-local
```

По умолчанию ядро системы присваивает link-local-адрес каждому IPv6-включённому интерфейсу; данная команда отключает это поведение.

5. Корректировка MSS для IPv6:

```
set interfaces vxlan <vxlanN> ipv6 adjust-mss <mss | clamp-mss-to-pmtu>
```

где:

- **<mss>** - фиксированное значение MSS в диапазоне от «536» до «65535».
- **<clamp-mss-to-pmtu>** - автоматически вычисляет и устанавливает MSS на основе Path MTU (PMTU) для каждого соединения. $MSS = PMTU - 40$ (20 байт IP + 20 байт TCP).

6. Базовое время достижимости соседей:

```
set interfaces vxlan <vxlanN> ipv6 base-reachable-time <seconds>
```

где **<seconds>** - значение в диапазоне от «1» до «86400» секунд (1 секунда – 24 часа). Значение по умолчанию - «30». Это значение определяет, как долго система считает, что MAC-адрес соседа (полученный через NDP) остаётся действительным, прежде чем потребуются повторная проверка его доступности.

7. Отключение IPv6-маршрутизации:

```
set interfaces vxlan <vxlanN> ipv6 disable-forwarding
```

После выполнения команды интерфейс переходит в режим хоста (host mode): система будет обрабатывать только пакеты, адресованные локально (на назначенные IPv6-адреса), и не будет пересылать через этот интерфейс трафик между другими узлами.

8. Количество DAD-запросов:

```
set interfaces vxlan <vxlanN> ipv6 dup-addr-detect-transmits <n>
```

где **<n>** - целое число:

- **0** - отключает DAD полностью; адрес активируется немедленно без проверки;
- **1-n** - количество NS-пакетов, отправляемых с интервалом ~1 секунда.

По умолчанию используется значение «1».

9. Проверка источника IPv6 (RPF):

```
set interfaces vxlan <vxlanN> ipv6 source-validation <strict | loose | disable>
```

где **<strict | loose | disable>** - режим проверки источника. Возможно указать следующие значения:

- **strict** - каждый входящий пакет проверяется по FIB, и принимается только если пришёл через оптимальный (наилучший) обратный путь, определённый в таблице маршрутизации. Все пакеты, не удовлетворяющие этому условию, автоматически отбрасываются.
- **loose** - адрес источника каждого входящего пакета также проверяется по FIB, и если адрес источника не достижим ни через один интерфейс, проверка пакета будет неудачной.
- **disable** - нет проверки источника. Все пакеты принимаются независимо от маршрутизации.

В настоящее время в RFC 3704 рекомендуется включать strict режим для предотвращения подмены IP адресов в результате DDos атак. При использовании асимметричной или другой сложной маршрутизации рекомендуется использовать loose режим.

3.9.6 SPAN

Функция зеркалирования интерфейсов в **ARMA Стена** позволяет копировать входящий и исходящий трафик интерфейса на другой интерфейс. Функция используется для анализа трафика и должна поддерживаться принимающим устройством, например, коммутатором.

Для настройки зеркалирования интерфейсов в системе **ARMA Стена** используется опция «mirror». При этом необходимо указать зеркальный порт как для входящего, так и для исходящего трафика.

Для настройки зеркалирования интерфейса для входящего трафика необходимо ввести команду:

```
set interfaces vxlan <vxlanN> mirror ingress <inbound-interface>
```

где **<inbound-interface>** - имя интерфейса, на который будет дублироваться весь входящий трафик. Интерфейс должен быть определён в системе.

Для настройки зеркалирования интерфейса для исходящего трафика необходимо ввести команду:

```
set interfaces vxlan <vxlanN> mirror egress <outbound-interface>
```

где **<outbound-interface>** - имя интерфейса, на который будет дублироваться весь исходящий трафик. Интерфейс должен быть определён в системе.

3.9.7 Пример настройки VXLAN

Для демонстрации настройки VXLAN-туннеля используется тестовая топология, представленная на рисунке (см. [Рисунок – VXLAN](#)).

В примере реализована базовая конфигурация точечного (unicast) VXLAN-туннеля между двумя узлами **ARMA Стена**, обеспечивающего прозрачное L2-соединение между двумя географически разнесёнными сегментами локальной сети.

Такой подход позволяет расширить VLAN через IP-инфраструктуру (overlay-сеть) без изменения конфигурации конечных хостов. Подобные схемы широко применяются при объединении дата-центров, подключении удалённых филиалов или создании изолированных tenant-сетей в мультиарендных средах.

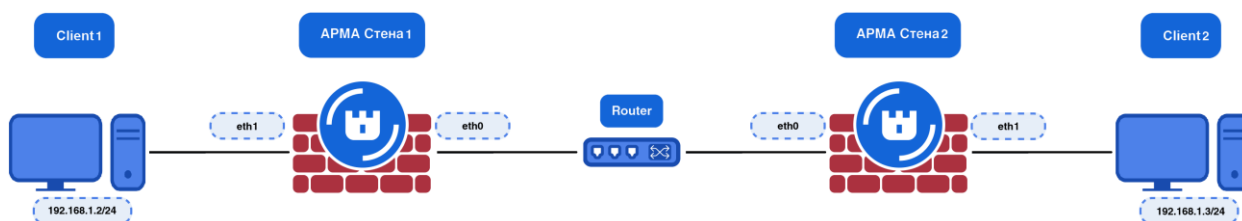


Рисунок – VXLAN

Конфигурация узлов

ARMA Стена 1:

```
set interfaces ethernet eth0 address '100.96.0.2/30'
set protocols static route 0.0.0.0/0 next-hop 100.96.0.1
set interfaces vxlan vxlan1 remote '100.96.1.2'
set interfaces vxlan vxlan1 vni '300'
set interfaces bridge br0 member interface eth1
set interfaces bridge br0 member interface vxlan1
```

ARMA Стена 2:

```
set interfaces ethernet eth0 address '100.96.1.2/30'
set protocols static route 0.0.0.0/0 next-hop 100.96.1.1
set interfaces vxlan vxlan1 remote '100.96.0.2'
set interfaces vxlan vxlan1 vni '300'
set interfaces bridge br0 member interface eth1
set interfaces bridge br0 member interface vxlan1
```

Интерфейсы **eth0** используются как транспортные (underlay) для передачи инкапсулированного VXLAN-трафика. Параметр «**remote**» задаёт IP-адрес удалённой VTEP, что активирует unicast-режим. Общий **VNI** (300) обеспечивает принадлежность обоих узлов к одному overlay-сегменту. L2-мост **br0** объединяет локальный клиентский интерфейс (eth1) и VXLAN-интерфейс (vxlan1), создавая единый broadcast-домен.

Проверка соединения

Для проверки работоспособности туннеля выполняется ICMP-запрос между конечными хостами Client1 (192.168.1.2) и Client2 (192.168.1.3).

Выполнить ICMP запрос на Client1 – «**ping 192.168.1.3**».

Соединение считается установленным, если ICMP-запросы успешно проходят между хостами. Успешная проверка подтверждает корректность настройки VXLAN-туннеля, включая инкапсуляцию/декапсуляцию трафика, сопоставление VNI и работу L2-моста на обоих узлах.

4 СИСТЕМНЫЕ НАСТРОЙКИ

4.1 DNS

Система доменных имён (DNS) представляет собой распределённую базу данных, которая устанавливает соответствие между понятными для человека доменными именами и числовыми IP-адресами. Эти соответствия фиксируются в ресурсных записях, которые хранятся на серверах имён, расположенных по всему интернету. Устройство, которому требуется получить доступ к узлу через интернет, отправляет запрос DNS на сервер имён. Сервер имён считывает свои ресурсные записи и возвращает ответ с IP-адресом указанного имени.

Система **ARMA Стена** предоставляет три основные функции, связанные с DNS:

1. системный DNS;
2. динамический DNS;
3. перенаправляющий DNS.

4.1.1 Системный DNS

В системном DNS задаётся список серверов имён, используемых системой **ARMA Стена** для преобразования доменных имён в IP-адреса.

Примечание:

На текущий момент маршрутизация DNS-запросов через VRF не поддерживается. Все DNS-запросы выполняются в контексте глобальной таблицы маршрутизации.

Для добавления DNS-сервера используется команда:

```
set system name-server <address>
```

где **<address>** – IP-адрес DNS-сервера в формате <x.x.x.x> для IPv4 и <h:h:h:h:h:h:h> для IPv6, либо имя сетевого интерфейса, на котором активирован DHCP-клиент.

Поддерживается указание нескольких DNS-серверов. Каждый сервер настраивается отдельной командой «set system name-server».

Просмотр списка DNS-серверов:

- в конфигурационном режиме:

```
admin@ngfwos# show system name-server
```

```
name-server 9.9.9.9
```

```
name-server 8.8.8.8
```

```
[edit]
```

```
admin@ngfwos#
```

- в эксплуатационном режиме:

```
admin@ngfwos:~$ show configuration | match name-server
```

```
configure-command "delete system name-server"
```

```
configure-command "set system name-server"
```

```
configure-command "copy system name-server"
```

```
configure-command "delete system name-server"
```

```
configure-command "rename system name-server"
```

```
configure-command "set system name-server"
```

```
configure-command "show system name-server"
```

```
name-server 9.9.9.9
```

```
name-server 8.8.8.8
```

```
admin@ngfwos:~$
```

Домены для разрешения неквалифицированных имён

Для разрешения неквалифицированных (неполных) имён система использует список доменов поиска. При выполнении запроса к хосту без указания доменной части система последовательно дополняет запрашиваемое имя каждым из доменов из данного списка до тех пор, пока не будет получено корректное разрешение.

Добавление домена в список поиска осуществляется командой:

```
set system domain-search <domain>
```

где **<domain>** – доменное имя, используемое для дополнения неполных имён при разрешении DNS-запросов. Установлены следующие ограничения:

- максимальное количество доменов в списке - 6;
- максимальная длина полного доменного имени - 253 символа;
- максимальное количество меток (элементов, разделённых точками) - 127;
- длина отдельной метки - не более 63 символов;
- метка не может начинаться или заканчиваться дефисом;

- разрешённые символы: латинские буквы (a–z), цифры (0–9), дефисы (-) и точки (.) в качестве разделителей меток.

Пример конфигурации доменов поиска:

Настройка системы на попытку завершения домена в следующем порядке: infowatch.io (первый), infowatch.net (второй) и infowatch.network (последний):

```
set system domain-search infowatch.io
set system domain-search infowatch.net
set system domain-search infowatch.network
```

Просмотр списка доменов поиска:

- в конфигурационном режиме:

```
admin@ngfwos# show system domain-search

domain-search infowatch.io
[edit]
admin@ngfwos#
```

- в эксплуатационном режиме:

```
admin@ngfwos:~$ show configuration | match domain-search

domain-search infowatch.io
        configure-command "delete system domain-search"
        configure-command "set system domain-search"
admin@ngfwos:~$
```

4.1.2 Динамический DNS

Динамический DNS (DDNS) – технология, позволяющая информации на DNS-сервере обновляться в реальном времени и, по желанию, в автоматическом режиме. Она применяется для назначения постоянного доменного имени устройству (компьютеру, сетевому накопителю) с динамическим и статическим IP-адресом.

Система **ARMA Стена** имеет возможность обновлять удалённую запись DNS при получении нового IP-адреса интерфейса. Для этого в состав системы входит клиент **ddclient**.

Клиент ddclient использует два способа обновления DNS-записей. Первый способ, в соответствии с RFC 2136, предполагает отправку обновлений непосредственно демону DNS. Второй способ предполагает использование стороннего сервиса, такого как DynDNS.com или другой аналогичный сайт. Этот способ использует HTTP-

запросы для передачи нового IP-адреса. В системе **ARMA Стена** возможно настроить оба этих способа.

4.1.2.1 Команды настройки DDNS в соответствии с RFC 2136

1. Создать новую конфигурацию DDNS, которая будет обновлять IP-адрес, назначенный указанному интерфейсу:

```
set service dns dynamic name <service-name> address interface <interface>
```

где:

<service-name> – имя службы DDNS;

<interface> – имя сетевого интерфейса.

2. Указать описание для настраиваемой службы DDNS:

```
set service dns dynamic name <service-name> description <text>
```

где **<text>** - краткое описание <service-name> службы DDNS.

3. Указать файл, содержащий ключ аутентификации TSIG для обновления RFC2136, совместно используемый с удалённым DNS сервером:

```
set service dns dynamic name <service-name> key <filename>
```

где **<filename>** - имя файла, расположенного в директории «**/config/auth**».

4. Указать адрес DNS-сервера, используемый при обновлении данного динамического назначения:

```
set service dns dynamic name <service-name> server <server>
```

где **<server>** - адрес DNS-сервера в формате: <x.x.x.x> - для IPv4; <h:h:h:h:h:h:h> - для IPv6; <hostname> - полное доменное имя удалённого сервера.

5. Указать обновляемую зону DNS:

```
set service dns dynamic name <service-name> zone <zone>
```

где **<zone>** - имя зоны DNS.

6. Указать DNS запись, которая должна быть обновлена:

```
set service dns dynamic name <service-name> host-name <record>
```

где **<record>** - имя хоста для регистрации в службе DDNS.

7. Указать значение TTL для указанной записи ресурса:

```
set service dns dynamic name <service-name> ttl <ttl>
```

где **<ttl>** - значение TTL в секундах. Возможно указать значение в диапазоне от «0» до «2147483647». По умолчанию используется значение «600».

8. Указать интервал обновления DDNS:

```
set service dns dynamic interval <60-3600>
```

где **<60-3600>** - интервал обновления в секундах. Возможно указать значение в диапазоне от «60» до «3600». По умолчанию используется значение «300».

4.1.2.1.1 Пример настройки DDNS

Необходимо зарегистрировать DNS-запись «example.arma.ru» на DNS-сервере «ns1.arma.ru». Для аутентификации используется файл «my.key», который находится в директории «**/config/auth/my.key**». Значение TTL должно быть установлено равным 300 секундам.

Для данной настройки необходимо ввести следующие команды:

```
set service dns dynamic name test-DNS address interface eth0
set service dns dynamic name test-DNS description 'RFC 2136 dynamic dns service'
set service dns dynamic name test-DNS key /config/auth/my.key
set service dns dynamic name test-DNS server ns1.arma.ru
set service dns dynamic name test-DNS zone arma.ru
set service dns dynamic name test-DNS host-name example.arma.ru
set service dns dynamic name test-DNS protocol nsupdate
set service dns dynamic name test-DNS ttl 300
commit
save
```

Для просмотра настроек необходимо в конфигурационном режиме ввести команду «show service dns dynamic»:

```
admin@ngfwos# show service dns dynamic
name test-DNS {
    address {
        interface eth0
    }
    description "RFC 2136 dynamic dns service"
    host-name example.arma.ru
    key /config/auth/my.key
    protocol nsupdate
    server ns1.arma.ru
    ttl 300
    zone arma.ru
}
[edit]
admin@ngfwos#
```

Вид записи в конфигурации ddclient:

```
# ddclient configuration for interface "eth0":
#
# Web service dynamic DNS configuration for test-DNS: [nsupdate, example.arma.ru]
use=if, \
if=eth0, \
protocol=nsupdate, \
server=ns1.arma.ru, \
zone=arma.ru, \
password='/config/auth/my.key', \
ttl=300 \
example.arma.ru
```

4.1.2.2 Команды настройки DDNS на основе HTTP

Примечание:

В **ARMA Стена** возможно использовать любые сервисы, основанные на протоколах, поддерживаемых **ddclient**. Для этого необходимо указать логин, пароль, одно или несколько имён хостов, протокол и сервер.

На одном интерфейсе возможно использовать несколько сервисов.

1. Создать новую конфигурацию DDNS, которая будет обновлять IP-адрес, назначенный указанному интерфейсу:

```
set service dns dynamic name <service-name> address interface <interface>
```

где:

<service-name> – имя службы DDNS;

<interface> – имя сетевого интерфейса.

2. Указать описание для настраиваемой службы DDNS:

```
set service dns dynamic name <service-name> description <text>
```

где **<text>** - краткое описание <service-name> службы DDNS.

3. Указать динамическое DNS-имя хоста, связанное с поставщиком DDNS:

```
set service dns dynamic name <service-name> host-name <hostname>
```

где **<hostname>** - имя хоста для регистрации в службе DDNS.

4. Указать имя пользователя, используемое при аутентификации запроса на обновление:

```
set service dns dynamic name <service-name> username <username>
```

где **<username>** - имя пользователя.

5. Указать пароль, используемый при аутентификации запроса на обновление:

```
set service dns dynamic name <service-name> password <password>
```

6. Указать протокол ddclient, используемый для связи с провайдером:

```
set service dns dynamic name <service-name> protocol <protocol>
```

где **<protocol>** - имя протокола. Возможно указать следующие значения:

- 1984;
- changeip;
- cloudflare;
- digitalocean;
- dinahosting;
- dnsexit2;
- dnsmadeeasy;
- domeneshop;
- dondominio;
- dslreports1;
- duckdns;
- dyndns1;
- dyndns2;

- easydns;
- enom;
- freedns;
- freemyip;
- gandi;
- godaddy;
- googledomains;
- hetzner;
- infomaniak;
- keysystems;
- mythicdyn;
- namecheap;
- nfsn;
- njalla;
- noip;
- nsupdate;
- ovh;
- regfishde;
- sitelutions;
- woima;
- Yandex;
- zoneedit1.

7. Указать сервер, на который отправляются запросы на обновление:

```
set service dns dynamic name <service-name> server <server>
```

где **<server>** - адрес удалённого динамического DNS-сервер в формате <x.x.x.x>, <h:h:h:h:h:h:h> или <hostname>.

8. Разрешить явный IPv6-адрес для интерфейса:

```
set service dns dynamic name <service-name> ip-version ipv6
```

4.1.2.2.1 Пример настройки DDNS

Использовать deSEC (dedyn.io) в качестве предпочтительного поставщика услуг:

```
set service dns dynamic name dedyn description 'deSEC dynamic dns service'  
set service dns dynamic name dedyn username myusername  
set service dns dynamic name dedyn password mypassword  
set service dns dynamic name dedyn host-name myhostname.dedyn.io  
set service dns dynamic name dedyn protocol dyndns2  
set service dns dynamic name dedyn server update.dedyn.io  
set service dns dynamic name dedyn address interface eth0
```

4.1.2.3 Настройки для работы с NAT

По умолчанию ddclient обновляет динамическую DNS-запись, используя IP-адрес, непосредственно подключённый к интерфейсу. Если устройство находится за NAT, то запись будет обновлена и будет указывать на внутренний IP-адрес.

Для того чтобы ddclient определял внешние IP-адреса, необходимо выполнить следующие настройки:

1. Указать удалённый URL-адрес для получения IP-адреса системы:

```
set service dns dynamic name <service-name> address web <url>
```

где **<url>** - удалённый URL-адрес. ddclient загрузит <url> и попытается извлечь системный IP-адрес из полученного ответа.

2. Указать шаблон для пропуска ответов HTTP(S) для извлечения внешнего IP-адреса:

```
set service dns dynamic name <service-name> address web skip <pattern>
```

где **<pattern>** - шаблон для пропуска ответов HTTP(S). Клиент ddclient будет игнорировать все адреса, расположенные перед строкой, указанной в поле <pattern>.

4.1.3 Перенаправляющий DNS

Перенаправляющий DNS-сервер выполняет функцию пересылки полученных рекурсивных запросов вышестоящему кэширующему серверу в виде рекурсивных запросов. Это позволяет снизить нагрузку на кэширующий DNS-сервер.

Перенаправляющий DNS-сервер обладает следующими характеристиками:

- Способность обрабатывать рекурсивные запросы без выполнения рекурсии.
- Предоставление локального кэша в ближайшем сетевом расположении.
- Увеличение гибкости в определении локального доменного пространства.

В системе **ARMA Стена** перенаправляющий DNS-сервер может работать без вышестоящего DNS-сервера. Он может выступать как в качестве полноценного

рекурсивного DNS-сервера, так и пересылать запросы на настраиваемые вышестоящего DNS-серверы.

4.1.3.1 Команды настройки перенаправляющего DNS

1. Перенаправлять входящие DNS-запросы на DNS-серверы, настроенные в системе:

```
set service dns forwarding system
```

2. Указать интерфейс, на который DHCP-клиенты направляют DNS-запросы:

```
set service dns forwarding dhcp <interface>
```

где **<interface>** - имя сетевого интерфейса.

3. Указать адрес и порт DNS-сервера, на который будут передаваться все DNS-запросы:

```
set service dns forwarding name-server <address> [port <port>]
```

где:

- **<address>** - адрес DNS-сервера в формате <x.x.x.x> для IPv4 и <h:h:h:h:h:h:h> для IPv6;
- **<port>** - номер порта DNS-сервера. Возможно указать значение в диапазоне от «1» до «65535». По умолчанию используется «53» порт.

Поддерживается возможность указать несколько адресов для использования различных DNS серверов.

4. Перенаправлять полученные запросы для определённого домена <domain-name> на заданный DNS-сервер <address>:

```
set service dns forwarding domain <domain-name> name-server <address>
```

Возможно указание нескольких серверов имён. Эта функция может быть использована для разделения конфигурации DNS-горизонта.

Примечание:

Это также применимо к зонам с обратным поиском (18.172.in-addr.arpa).

5. Добавить NTA для домена <domain-name>:

```
set service dns forwarding domain <domain-name> addnta
```

Этот параметр необходимо установить в случае, если домен не поддерживает DNSSEC.

6. Установить «recursion desired» бит для запросов к вышестоящему DNS-серверу:

```
set service dns forwarding domain <domain-name> recursion-desired
```

7. Указать адрес сети, в которой узлам разрешено использовать перенаправляющий DNS-сервер:

```
set service dns forwarding allow-from <network>
```

где **<network>** - адрес сети в формате <x.x.x.x/x> для IPv4 и <h:h:h:h:h:h/h> для IPv6.

Сеть «0.0.0.0/0» или «::/0» позволит всем сетям IPv4 и IPv6 обращаться к этому серверу. Однако, как правило, это нежелательно, поскольку открытые DNS-ретрансляторы могут быть использованы для проведения DDoS-атак.

8. Указать уровень обработки DNSSEC:

```
set service dns forwarding dnssec <off | process-no-validate | process | log-fail | validate>
```

где **<off | process-no-validate | process | log-fail | validate>** - уровень обработки. Перенаправляющий DNS-сервер имеет 5 различных уровней обработки DNSSEC (в порядке от наименьшего к наибольшему уровню обработки):

- **«off»** - в этом режиме обработка DNSSEC не выполняется. Перенаправляющий DNS-сервер не будет устанавливать бит DNSSEC OK (DO) в исходящих запросах и будет игнорировать биты DO и AD в запросах;
- **«process-no-validate»** - в этом режиме перенаправляющий DNS сервер будет устанавливать DO-бит в исходящих запросах и предоставлять RR-наборы, связанные с DNSSEC RRsets (NSEC, RRSIG), клиентам, которые их запрашивают (с помощью DO-бита в запросе), за исключением зон, предоставляемых с помощью настройки зон для авторизации. В этом режиме он не будет выполнять никаких проверок, даже по запросу клиента. *Используется по умолчанию;*
- **«process»** - поведение перенаправляющего DNS-сервера будет аналогично поведению в режиме «process-no-validate». Однако перенаправляющий DNS сервер попытается проверить данные, если в запросе установлен хотя бы один из битов DO или AD. В этом случае он установит бит AD в ответе, когда данные будут успешно проверены, или отправит «SERVFAIL», когда проверка окажется ложной;
- **«log-fail»** - в этом режиме перенаправляющий DNS сервер будет пытаться проверить все данные, получаемые с доверенных серверов, независимо от запросов клиента по DNSSEC, и записывать результат

проверки в журнал. Этот режим можно использовать для определения дополнительной нагрузки и количества возможных фиктивных ответов перед включением полномасштабной проверки. Ответы на запросы клиента такие же, как и в «process».

- **«validate»** - максимальный режим обработки DNSSEC. В этом режиме все запросы будут проверены и в случае обнаружения нелегитимных данных будет отправлен ответ «SERVFAIL», независимо от запроса клиента.

Примечание:

Инструмент Dig для Unix/Linux при выполнении запроса устанавливает AD-бит, что может привести к неожиданным результатам запроса при тестировании. В таком случае рекомендуется использовать опцию +noad в командной строке dig.

Примечание:

CD бит корректно выполняется для «process» и «validate». Для «log-fail» сбои также будут регистрироваться.

9. Отключить поиск по имени узла в файле «/etc/hosts» для перенаправляющего DNS-сервера:

```
set service dns forwarding ignore-hosts-file
```

DHCP-сервер системы **ARMA Стена** использует этот файл для добавления резолверов к назначенным адресам.

10. Указать максимальное количество записей кэша DNS:

```
set service dns forwarding cache-size <0-2147483647>
```

где **<0-2147483647>** - значение максимального количества записей кэша DNS. Возможно указать значение в диапазоне от «0» до «2147483647». По умолчанию используется значение «10000».

11. Установить максимальное время кэширования отрицательных записей:

```
set service dns forwarding negative-ttl <0-7200>
```

где **<0-7200>** - значение времени для кэширования записей NXDOMAIN в секундах. Возможно указать значение в диапазоне от «0» до «7200». По умолчанию используется значение «3600».

Запрос, на который нет подтверждённого ответа, кэшируется, чтобы впоследствии быстро исключить DNS запись, не создавая большой нагрузки на удалённый сервер.

12. Установить время, в течение которого необходимо ожидать ответа удалённого сервера, прежде чем прервать работу и выдать ответ «SERVFAIL»:

```
set service dns forwarding timeout <10-60000>
```

где **<10-60000>** - значение времени ожидания ответа от удалённого сервера в миллисекундах. Возможно указать значение в диапазоне от «10» до «60000». По умолчанию используется значение «1500».

13. Указать локальные IPv4 или IPv6 адреса, к которым будет привязан перенаправляющий DNS-сервер:

```
set service dns forwarding listen-address <address>
```

где **<address>** - локальный адрес в формате <x.x.x.x> для IPv4 и <h:h:h:h:h:h:h> для IPv6. Эти адреса перенаправляющий DNS-сервер будет использовать для прослушивания входящих соединений.

14. Указать локальные IPv4 или IPv6 адреса, используемые в качестве адреса источника для отправки запросов:

```
set service dns forwarding source-address <address>
```

где **<address>** - локальный адрес в формате <x.x.x.x> для IPv4 и <h:h:h:h:h:h:h> для IPv6. С этого адреса перенаправляющий DNS-сервер будет отправлять перенаправленные на него исходящие DNS запросы.

15. Включить параметр, который делает перенаправляющий DNS-сервер неизвестным для зон: «10.in-addr.arpa», «168.192.in-addr.arpa», «16-31.172.in-addr.arpa», что позволяет использовать вышестоящие DNS-серверы для обратного поиска этих зон:

```
set service dns forwarding no-serve-rfc1918
```

4.1.3.2 Команды мониторинга и эксплуатация

1. Показать статистику работы перенаправляющего DNS-сервера:

```
admin@ngfwos:~$ show dns forwarding statistics
```

2. Сброс кэша переадресации DNS:

```
admin@ngfwos:~$ reset dns forwarding <all | domain <domain-name> >
```

Возможно очистить кэш для всех записей или только для записей, связанных с определённым доменом.

3. Перезапустить процесс перенаправляющего DNS-сервера:

```
admin@ngfwos:~$ restart dns forwarding
```

При этом происходит очистка локального кэша переадресации DNS.

4.1.3.3 Пример настройки

Пример настройки разделённого DNS (split DNS) для домена example.com.

Для настройки разделённого DNS будут использоваться следующие параметры:

1. Все DNS-запросы для домена «example.com» будут перенаправляться на DNS-сервер по адресу «192.0.2.254» и «2001:db8:cafe::1».
2. Все остальные DNS-запросы будут перенаправлены на другой набор DNS-серверов по адресам «192.0.2.1», «192.0.2.2», «2001:db8::1:ffff» и «2001:db8::2:ffff».
3. Перенаправляющий DNS-сервер будет прослушивать запросы только по адресам внутреннего интерфейса eth1 – «192.168.1.254» для IPv4 и «2001:db8::ffff» для IPv6.
4. Перенаправляющий DNS-сервер будет принимать запросы на поиск только из внутренних подсетей – «192.168.1.0/24» и «2001:db8::/64».
5. Перенаправляющий DNS-сервер будет передавать обратные запросы на поиск для зон «10.in-addr.arpa», «168.192.in-addr.arpa», «16-31.172.in-addr.arpa» на вышестоящий сервер.

Список команд для настройки:

```
set service dns forwarding domain example.com name-server 192.0.2.254
set service dns forwarding domain example.com name-server 2001:db8:cafe::1
set service dns forwarding name-server 192.0.2.1
set service dns forwarding name-server 192.0.2.2
set service dns forwarding name-server 2001:db8::1:ffff
set service dns forwarding name-server 2001:db8::2:ffff
set service dns forwarding listen-address 192.168.1.254
set service dns forwarding listen-address 2001:db8::ffff
set service dns forwarding allow-from 192.168.1.0/24
set service dns forwarding allow-from 2001:db8::/64
set service dns forwarding no-serve-rfc1918
```

4.2 Шлюз по умолчанию

Команда для настройки статического маршрута по умолчанию:

```
set protocols static route 0.0.0.0/0 next-hop <address>
```

где **<address>** - адрес маршрутизатора следующего узла в формате <x.x.x.x>.

Для удаления статического маршрута по умолчанию необходимо ввести команду:

```
delete protocols static route 0.0.0.0/0
```

Для просмотра записей в таблице маршрутизации для маршрута по умолчанию необходимо ввести команду:

```
admin@ngfwos:~$ show ip route 0.0.0.0
```

```
Known via "static", distance 210, metric 0, tag 210, best
```

```
Last update 08:13:46 ago
```

```
* 192.168.200.1, via eth3, weight 1
```

```
* 192.168.200.1, via eth4, weight 1
```

4.3 Системный Прокси

В некоторых IT-средах для подключения к сети Интернет необходимо использовать прокси-сервер.

Для настройки прокси-сервера в системе предусмотрены следующие команды в конфигурационном режиме:

1. Указать адрес прокси-сервера, который будет использоваться для всех исходящих соединений, инициированных системой **ARMA Стена**, включая HTTP, HTTPS и FTP (включая анонимный FTP):

```
set system proxy url <url>
```

где **<url>** - url-адрес прокси-сервера. Адрес должен начинаться с «**Ошибка! Недопустимый объект гиперссылки.**» или с «**Ошибка! Недопустимый объект гиперссылки.**».

2. Определить порт прокси-сервера:

```
set system proxy port <port>
```

где **<port>** - порт подключения к прокси. Возможно указать значение в диапазоне от «1» до «65535». Используется в случае, если прокси-сервер работает не на стандартном порту «80».

3. Установить имя пользователя для аутентификации на прокси-сервере:

```
set system proxy username <username>
```

где **<username>** - имя пользователя для аутентификации на прокси-сервере. Допускается использование латинских букв (a–z, A–Z), цифр (0–9) и специальных символов, за исключением символов «"» и «'». Имя пользователя не должно начинаться с последовательности «//» или пробела, и иметь длину не более 128 символов.

4. Установить пароль для аутентификации на прокси-сервере:

```
set system proxy password <password>
```

где **<password>** - допускается использование латинских букв (a–z, A–Z), цифр (0–9) и специальных символов, за исключением символов «"» и «'». Пароль не должен начинаться с последовательности «//» или пробела, и иметь длину не более 128 символов.

4.4 Служба NTP

Служба NTP позволяет устанавливать и поддерживать системное время, синхронизированное с серверами точного времени.

В **ARMA Стена** используется протокол NTPv4, соответствующий международному стандарту «RFC-5905». Обмен с серверами информацией о временных метках выполняется по протоколу UDP через порт «123».

ARMA Стена использует следующие адреса NTP-серверов первого уровня:

- «ntp1.vniiftri.ru»;
- «ntp2.vniiftri.ru»;
- «ntp3.vniiftri.ru»;
- «ntp4.vniiftri.ru»;
- «ntp1.niiftri.irkutsk.ru»;
- «ntp2.niiftri.irkutsk.ru»;
- «vniiftri.khv.ru»;
- «vniiftri2.khv.ru»;
- «ntp.sstf.nsk.ru».

Для добавления NTP-сервера необходимо ввести следующую команду:

```
set service ntp server <address>
```

где **<address>** – адрес NTP-сервера, указываемый в формате **IPv4/IPv6-адреса** или **FQDN**.

Для удаления NTP-сервера необходимо ввести следующую команду:

```
delete service ntp server <address>
```

Для просмотра списка используемых NTP-серверов необходимо в режиме конфигурирования ввести следующую команду:

```
show service ntp
```

Для перезапуска службы NTP необходимо в эксплуатационном режиме ввести следующую команду:

```
admin@ngfwos:~$ restart ntp
```

4.4.1 Дополнительные настройки NTP

Для включения или отключения какого-либо дополнительного параметра сервера NTP, следует ввести соответствующую команду:

```
set service ntp server <address> <attribute>  
delete service ntp server <address> <attribute>
```

где **<attribute>** – дополнительный параметр NTP.

Возможна настройка следующих дополнительных параметров сервера NTP:

- **«noselect»** – назначение сервера NTP как неиспользуемого;
- **«nts»** – включение защиты сетевого времени NTS для сервера NTP;
- **«pool»** – указание адреса, являющегося пулом серверов NTP;
- **«prefer»** – назначение сервера NTP как предпочтительного.

4.5 Планировщик задач Cron

Планировщик задач **Cron** позволяет выполнять различные задачи согласно заданному расписанию.

Для установки времени запуска задачи необходимо ввести следующую команду:

```
set system task-scheduler task <task> crontab-spec <spec>
```

где:

- **<task>** – имя задачи;
- **<spec>** – время запуска задачи.

Для настройки параметра **<spec>** используется стандартный синтаксис сервиса **Cron** в виде пяти атрибутов **«* * * * *»**, воспринимаемых как:

- **«минуты»** – возможно использование значений в диапазоне от **«0»** до **«59»**;
- **«часы»** – возможно использование значений в диапазоне от **«0»** до **«23»**;
- **«число»** – возможно использование значений в диапазоне от **«1»** до **«31»**;
- **«месяц»** – возможно использование значений в диапазоне от **«1»** до **«12»**;
- **«дни недели»** – возможно использование значений в диапазоне от **«0»** до **«7»**. Значения от **«1»** до **«6»** принимаются как дни недели с «понедельника» до «субботы» соответственно. Значения **«0»** или **«7»** принимаются как «воскресенье».

Поля могут содержать одно или несколько значений, разделенных запятыми, или диапазон значений, разделённых дефисом. Существует возможность указать шаг, используя символ «/». Например, при указании атрибутов следующим образом: «*** /2 * * ***» – задача будет выполняться каждые два часа.

В качестве примера приведена команда для настройки выполнения задачи «Task1» ежедневно в 07:00 и 18:00:

```
set system task-scheduler task Task1 crontab-spec '00 07,18 * * *'
```

Для настройки интервала запуска задачи возможно применение параметра «**interval**»:

```
set system task-scheduler task <task> interval <interval>
```

где **<interval>** – интервал времени, в течение которого задача должна быть выполнена. Задаётся в виде числа с одним из следующих суффиксов: «**m**» – минуты, «**h**» – часы, «**d**» – дни. В случае ввода значения без суффикса, интервал воспринимается в минутах.

Для указания скрипта, запускаемого по расписанию, необходимо ввести следующую команду с параметром «**executable path**»:

```
set system task-scheduler task <task> executable path <path>
```

где **<path>** – путь к скрипту.

Для установки параметров скрипта необходимо ввести следующую команду:

```
set system task-scheduler task <task> executable arguments <args>
```

где **<args>** – параметр скрипта.

Создание и редактирование скриптов возможно выполнять с помощью какого-либо текстового редактора, например «**nano**».

4.6 Мониторинг аппаратной платформы

4.6.1 Мониторинг блока питания

Для проверки состояния блоков питания в программно-аппаратных комплексах серии **K1000** и **K10000** необходимо выполнить следующую команду в эксплуатационном режиме (см. [Рисунок – Мониторинг блоков питания](#)):

```
admin@ngfwos:~$ show health psu
```

```
admin@ngfwos:~$ show health psu
Parameter      PSU1      Sensor    PSU2      Sensor
Presence       Present   ok        Present   ok
Input voltage   229 volts ok        229 volts ok
Input Power     65 watts  ok        65 watts  ok
Temperature     29 degrees C ok        38 degrees C ok
admin@ngfwos:~$
```

Рисунок – Мониторинг блоков питания

В столбце «**Sensor**» значение «**ok**» свидетельствует о нормальном функционировании датчика. В случае если состояние датчика не может быть определено, в данном столбце отображается «**ns**» или «**N/A**».

В случае отсутствия блока питания в строке «**Presence**» будет отображаться значение «**Missing**» (см. [Рисунок – Блок питания отсутствует](#)):

```
admin@ngfwos:~$ show health psu
Parameter      PSU1      Sensor    PSU2      Sensor
Presence       Missing   ok        Present   ok
Input voltage   N/A       N/A       228 volts ok
Input Power     N/A       N/A       110 watts ok
Temperature     N/A       N/A       36 degrees C ok
admin@ngfwos:~$
```

Рисунок – Блок питания отсутствует

Примечание:

Для осуществления мониторинга блоков питания необходимо активировать в BIOS поддержку **BMC** (Baseboard Management Controller) (см. [Рисунок – Включение BMC](#)).

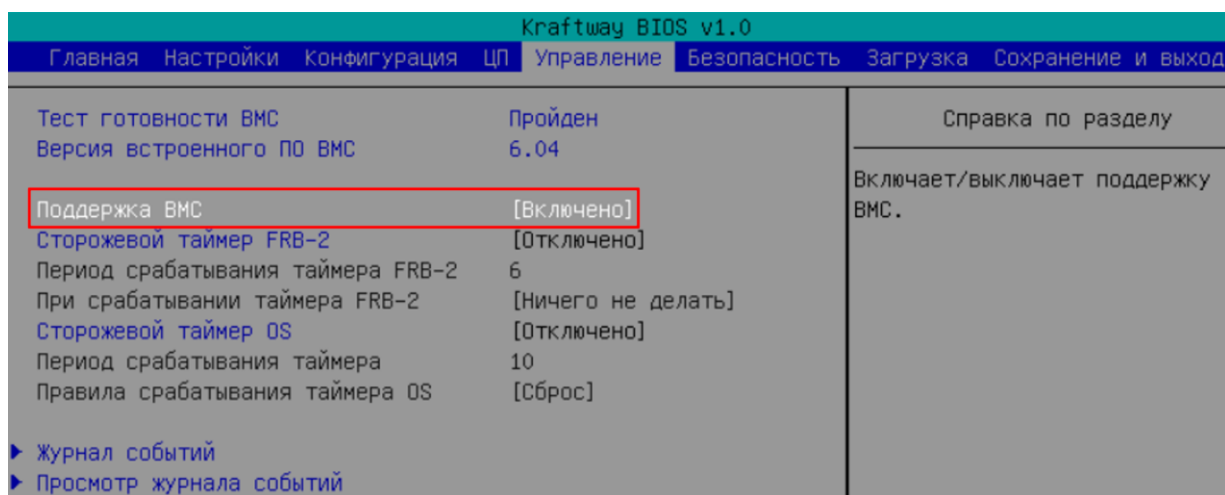


Рисунок – Включение BMC

Если оборудование не поддерживает технологию **BMC** или эта функция отключена в BIOS, то при выполнении команды «**show health psu**» будет выведено сообщение об отсутствии поддержки IPMI на устройстве «*Device doesn't support IPMI for getting PSU info*».

4.6.2 Мониторинг аппаратной платформы

В системе **ARMA Стена** возможен мониторинг текущего состояния компонентов устройства, включая систему питания и охлаждения. Это позволяет предотвратить возможные аварийные ситуации, связанные с оборудованием.

Для просмотра состояния аппаратной платформы системы необходимо ввести следующую команду в эксплуатационном режиме (см. [Рисунок – Мониторинг аппаратной платформы](#)):

```
admin@ngfwos:~$ show health all
```

```
admin@ngfwos:~$ show health all

Power Supplies:
Parameter      Value      Sensor
PSU1 Presence   Present    ok
PSU1 Input Voltage 229 volts  ok
PSU1 Input Power  25 watts   ok
PSU1 Temperature  35 degrees C ok
PSU2 Presence   Present    ok
PSU2 Input Voltage 233 volts  ok
PSU2 Input Power  25 watts   ok
PSU2 Temperature  41 degrees C ok

Fans:
Parameter      Value      Sensor
Fan 1 Speed    6080 RPM   ok
Fan 2 Speed    5840 RPM   ok
Fan 3 Speed    6320 RPM   ok
Fan 4 Speed    6400 RPM   ok
Fan 5 Speed    6240 RPM   ok

Voltages:
Parameter      Value      Sensor
+0.6V VTT      0.61 volts ok
+1.05V Combined 1.07 volts ok
+1.05V PCH      1.05 volts ok
+1.2V VDDQ      1.22 volts ok
+12V Rail       11.97 volts ok
+3.3V Dual      3.33 volts ok
+3.3V PCH       3.33 volts ok
+5V Dual        5.00 volts ok
Battery voltage 3.08 volts ok
DDR4 VPP        1.26 volts ok
VCC Input       1.83 volts ok
VCC KRHV SB     1.32 volts ok

Temperatures:
Parameter      Value      Sensor
CPU Temperature 31 degrees C ok
System Temp 1   21.50 degrees C ok
System Temp 2   21.50 degrees C ok
admin@ngfwos:~$
```

Рисунок – Мониторинг аппаратной платформы

Примечание:

Для осуществления мониторинга аппаратной платформы необходимо активировать в BIOS поддержку **ВМС**.

4.7 Мониторинг процессов

Для получения информации о текущих процессах, выполняемых на устройстве **ARMA Стена**, в эксплуатационном режиме необходимо выполнить следующую команду:

```
admin@ngfwos:~$ show system processes [text]
```

Команда предоставляет данные о состоянии запущенных процессов в системе в табличном виде (см. [Рисунок – Базовая информация о процессах](#)). Таблица содержит следующие поля:

- **PID** - уникальный числовой идентификатор процесса, присваиваемый ядром операционной системы при его запуске;
- **USER** - имя пользователя, от имени которого выполняется процесс. Для системных процессов указано значение root;
- **PR** - приоритет планирования процесса (значение динамического приоритета), определяемое на основе параметра NICE и внутренней логики планировщика;
- **NI** - статический параметр корректировки приоритета процесса; допустимые значения находятся в диапазоне от «-20» до «19». Процессы с меньшим значением nice получают больше CPU-времени;
- **STAT** - состояние процесса согласно классификации ядра Linux:
 - **R** - процесс выполняется в текущий момент;
 - **S** - процесс находится в состоянии ожидания (прерываемый сон);
 - **D** - процесс заблокирован в непрерывающем режиме (например, ожидание операций ввода-вывода);
 - **Z** - завершённый процесс (zombie или defunct), не получивший сигнала от родительского процесса;
 - **T** - процесс приостановлен (остановлен сигналом);
 - **W** - процесс находится в состоянии swap;
 - **<** - процесс имеет повышенный приоритет (запущен с приоритетом real-time);
 - **N** - процесс выполняется с пониженным приоритетом;

- **L** - процесс имеет страницы памяти, заблокированные в RAM (обычно указывает на использование real-time планирования);
- **I** - поток ядра в режиме бездействия (idle), не имеющий активного выполнения.
- **C** - индикатор загрузки процессора;
- **%CPU** - доля использования центрального процессора данным процессом за последний интервал измерения;
- **%MEM** - процент использования оперативной памяти относительно общего объёма RAM;
- **VSZ** - объём виртуальной памяти, занимаемой процессом (в килобайтах);
- **RSS** - объём резидентной памяти (физической памяти, используемой процессом без учёта свопа), в килобайтах;
- **TTY** - терминал, связанный с процессом. Для фоновых и системных процессов значение - «?»;
- **TIME** - суммарное время CPU, затраченное на выполнение процесса, отображается в формате ЧЧ:ММ:СС;
- **COMMAND** - имя исполняемого файла или команды, запустившей процесс. Для потоков ядра указано название в квадратных скобках (например, [kthreadd]).

```
admin@ngfwos:~$ show system processes
1 root    19  0 Ss    0 0.1 0.1 168332 12408 ?    00:02:17 /sbin/init noautologin
2 root    19  0 S      0 0.0 0.0 0 0 ?    00:00:00 [kthreadd]
3 root    19  0 S      0 0.0 0.0 0 0 ?    00:00:00 [pool_workqueue_release]
4 root    39 -20 I<    0 0.0 0.0 0 0 ?    00:00:00 [kworker/R-rcu_g]
5 root    39 -20 I<    0 0.0 0.0 0 0 ?    00:00:00 [kworker/R-rcu_p]
6 root    39 -20 I<    0 0.0 0.0 0 0 ?    00:00:00 [kworker/R-slub_]
7 root    39 -20 I<    0 0.0 0.0 0 0 ?    00:00:00 [kworker/R-netns]
9 root    39 -20 I<    0 0.0 0.0 0 0 ?    00:00:00 [kworker/0:0H-events_highpri]
11 root   19  0 I      0 0.0 0.0 0 0 ?    00:00:00 [kworker/u8:0-ext4-rsv-conversion]
12 root   39 -20 I<    0 0.0 0.0 0 0 ?    00:00:00 [kworker/R-mm_pe]
13 root   19  0 I      0 0.0 0.0 0 0 ?    00:00:00 [rcu_tasks_kthread]
14 root   19  0 I      0 0.0 0.0 0 0 ?    00:00:00 [rcu_tasks_trace_kthread]
15 root   19  0 S      0 0.0 0.0 0 0 ?    00:00:07 [ksoftirqd/0]
16 root   19  0 I      0 0.0 0.0 0 0 ?    00:00:59 [rcu_preempt]
17 root   139 - S      0 0.0 0.0 0 0 ?    00:00:01 [migration/0]
18 root   90 - S      0 0.0 0.0 0 0 ?    00:00:00 [idle_inject/0]
19 root   19  0 S      0 0.0 0.0 0 0 ?    00:00:00 [cpuhp/0]
20 root   19  0 S      0 0.0 0.0 0 0 ?    00:00:00 [cpuhp/1]
21 root   90 - S      0 0.0 0.0 0 0 ?    00:00:00 [idle_inject/1]
22 root   139 - S      0 0.0 0.0 0 0 ?    00:00:01 [migration/1]
23 root   19  0 S      0 0.0 0.0 0 0 ?    00:00:07 [ksoftirqd/1]
25 root   39 -20 I<    0 0.0 0.0 0 0 ?    00:00:00 [kworker/1:0H-events_highpri]
26 root   19  0 S      0 0.0 0.0 0 0 ?    00:00:00 [cpuhp/2]
27 root   90 - S      0 0.0 0.0 0 0 ?    00:00:00 [idle_inject/2]
28 root   139 - S      0 0.0 0.0 0 0 ?    00:00:01 [migration/2]
29 root   19  0 S      0 0.0 0.0 0 0 ?    00:00:07 [ksoftirqd/2]
31 root   39 -20 I<    0 0.0 0.0 0 0 ?    00:00:00 [kworker/2:0H-events_highpri]
32 root   19  0 S      0 0.0 0.0 0 0 ?    00:00:00 [cpuhp/3]
```

Рисунок – Базовая информация о процессах

Возможно использование дополнительных опций вывода [text] для детализации информации:

- **extensive** – формирует подробной информации о текущем состоянии процессов (см. [Рисунок – Детализированный вывод информации](#)).

```
admin@ngfwos:~$ show system processes extensive
top - 10:47:34 up 1 day, 4:26, 2 users, load average: 0.21, 0.20, 0.18
Tasks: 198 total, 1 running, 195 sleeping, 2 stopped, 0 zombie
%Cpu(s): 16.7 us, 16.7 sy, 0.0 ni, 66.7 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st
MiB Mem : 11690.6 total, 5247.6 free, 4148.4 used, 2702.8 buff/cache
MiB Swap: 0.0 total, 0.0 free, 0.0 used, 7542.2 avail Mem

  PID USER      PR  NI   VIRT   RES   SHR  S  %CPU  %MEM    TIME+  COMMAND
    1 root        20   0 168332 12408  9080  S   0.0   0.1   2:17.79 systemd
    2 root        20   0      0      0      0  S   0.0   0.0   0:00.07 kthreadd
    3 root        20   0      0      0      0  S   0.0   0.0   0:00.00 pool_wo+
    4 root         0 -20      0      0      0  I   0.0   0.0   0:00.00 kworker+
    5 root         0 -20      0      0      0  I   0.0   0.0   0:00.00 kworker+
    6 root         0 -20      0      0      0  I   0.0   0.0   0:00.00 kworker+
    7 root         0 -20      0      0      0  I   0.0   0.0   0:00.00 kworker+
    9 root         0 -20      0      0      0  I   0.0   0.0   0:00.00 kworker+
   11 root        20   0      0      0      0  I   0.0   0.0   0:00.00 kworker+
   12 root         0 -20      0      0      0  I   0.0   0.0   0:00.00 kworker+
   13 root        20   0      0      0      0  I   0.0   0.0   0:00.00 rcu_tas+
   14 root        20   0      0      0      0  I   0.0   0.0   0:00.00 rcu_tas+
   15 root        20   0      0      0      0  S   0.0   0.0   0:07.70 ksoftir+
   16 root        20   0      0      0      0  I   0.0   0.0   0:59.75 rcu_pre+
   17 root        rt    0      0      0      0  S   0.0   0.0   0:01.41 migrati+
   18 root       -51   0      0      0      0  S   0.0   0.0   0:00.00 idle_in+
   19 root        20   0      0      0      0  S   0.0   0.0   0:00.00 cpuhp/0
   20 root        20   0      0      0      0  S   0.0   0.0   0:00.00 cpuhp/1
```

Рисунок – Детализированный вывод информации

- **json** – выводит древовидную структуру процессов в формате JSON, предназначенном для программной обработки и интеграции с внешними системами (см. [Рисунок – Мониторинг процессов в формате JSON](#)).

```
admin@ngfwos:~$ show system processes json
[{"PID": "1", "USER": "root", "PRI": "19", "NICE": "0", "STAT": "Ss", "C": "0", "%CPU": "0.1", "%MEM": "0.1", "VSZ": "168332", "RSS": "12408", "TTY": "?", "TIME": "00:02:17", "COMMAND": "/sbin/init noautologin"}, {"PID": "2", "USER": "root", "PRI": "19", "NICE": "0", "STAT": "S", "C": "0", "%CPU": "0.0", "%MEM": "0.0", "VSZ": "0", "RSS": "0", "TTY": "?", "TIME": "00:00:00", "COMMAND": "[kthreadd]"}, {"PID": "3", "USER": "root", "PRI": "19", "NICE": "0", "STAT": "S", "C": "0", "%CPU": "0.0", "%MEM": "0.0", "VSZ": "0", "RSS": "0", "TTY": "?", "TIME": "00:00:00", "COMMAND": "[pool_workqueue_release]"}, {"PID": "4", "USER": "root", "PRI": "39", "NICE": "-20", "STAT": "I<", "C": "0", "%CPU": "0.0", "%MEM": "0.0", "VSZ": "0", "RSS": "0", "TTY": "?", "TIME": "00:00:00", "COMMAND": "[kworker/R-rcu_g]"}, {"PID": "5", "USER": "root", "PRI": "39", "NICE": "-20", "STAT": "I<", "C": "0", "%CPU": "0.0", "%MEM": "0.0", "VSZ": "0", "RSS": "0", "TTY": "?", "TIME": "00:00:00", "COMMAND": "[kworker/R-rcu_u_p]"}, {"PID": "6", "USER": "root", "PRI": "39", "NICE": "-20", "STAT": "I<", "C": "0", "%CPU": "0.0", "%MEM": "0.0", "VSZ": "0", "RSS": "0", "TTY": "?", "TIME": "00:00:00", "COMMAND": "[kworker/R-slub_]"}, {"PID": "7", "USER": "root", "PRI": "39", "NICE": "-20", "STAT": "I<", "C": "0", "%CPU": "0.0", "%MEM": "0.0", "VSZ": "0", "RSS": "0", "TTY": "?", "TIME": "00:00:00", "COMMAND": "[kworker/R-netns]"}, {"PID": "9", "USER": "root", "PRI": "39", "NICE": "-20", "STAT": "I<", "C": "0", "%CPU": "0.0", "%MEM": "0.0", "VSZ": "0", "RSS": "0", "TTY": "?", "TIME": "00:00:00", "COMMAND": "[kworker/0:0H-events_highpri]"}, {"PID": "11", "USER": "root", "PRI": "19", "NICE": "0", "STAT": "I", "C": "0", "%CPU": "0.0", "%MEM": "0.0", "VSZ": "0", "RSS": "0", "TTY": "?", "TIME": "00:00:00", "COMMAND": "[kworker/u8:0-ext4-rsv-conversion]"}, {"PID": "12", "USER": "root", "PRI": "39", "NICE": "-20", "STAT": "I<", "C": "0", "%CPU": "0.0", "%MEM": "0.0", "VSZ": "0", "RSS": "0", "TTY": "?", "TIME": "00:00:00", "COMMAND": "[kworker/R-netns]"}, {"PID": "13", "USER": "root", "PRI": "19", "NICE": "0", "STAT": "I", "C": "0", "%CPU": "0.0", "%MEM": "0.0", "VSZ": "0", "RSS": "0", "TTY": "?", "TIME": "00:00:00", "COMMAND": "[kworker/R-netns]"}, {"PID": "14", "USER": "root", "PRI": "19", "NICE": "0", "STAT": "I", "C": "0", "%CPU": "0.0", "%MEM": "0.0", "VSZ": "0", "RSS": "0", "TTY": "?", "TIME": "00:00:00", "COMMAND": "[kworker/R-netns]"}, {"PID": "15", "USER": "root", "PRI": "19", "NICE": "0", "STAT": "I", "C": "0", "%CPU": "0.0", "%MEM": "0.0", "VSZ": "0", "RSS": "0", "TTY": "?", "TIME": "00:00:00", "COMMAND": "[kworker/R-netns]"}, {"PID": "16", "USER": "root", "PRI": "19", "NICE": "0", "STAT": "I", "C": "0", "%CPU": "0.0", "%MEM": "0.0", "VSZ": "0", "RSS": "0", "TTY": "?", "TIME": "00:00:00", "COMMAND": "[kworker/R-netns]"}, {"PID": "17", "USER": "root", "PRI": "19", "NICE": "0", "STAT": "I", "C": "0", "%CPU": "0.0", "%MEM": "0.0", "VSZ": "0", "RSS": "0", "TTY": "?", "TIME": "00:00:00", "COMMAND": "[kworker/R-netns]"}, {"PID": "18", "USER": "root", "PRI": "19", "NICE": "0", "STAT": "I", "C": "0", "%CPU": "0.0", "%MEM": "0.0", "VSZ": "0", "RSS": "0", "TTY": "?", "TIME": "00:00:00", "COMMAND": "[kworker/R-netns]"}, {"PID": "19", "USER": "root", "PRI": "19", "NICE": "0", "STAT": "I", "C": "0", "%CPU": "0.0", "%MEM": "0.0", "VSZ": "0", "RSS": "0", "TTY": "?", "TIME": "00:00:00", "COMMAND": "[kworker/R-netns]"}, {"PID": "20", "USER": "root", "PRI": "19", "NICE": "0", "STAT": "I", "C": "0", "%CPU": "0.0", "%MEM": "0.0", "VSZ": "0", "RSS": "0", "TTY": "?", "TIME": "00:00:00", "COMMAND": "[kworker/R-netns]"}]
```

Рисунок – Мониторинг процессов в формате JSON

- **summary** – отображает сводные данные о загрузке системы, включая время непрерывной работы (uptime) и среднюю нагрузку за последние 1, 5 и 15 минут, выраженную в процентах от максимально допустимого значения. (см. [Рисунок – Сводная информация о загрузке системы](#)).

```
admin@ngfwos:~$ show system processes summary
Uptime: 1d 4h 27m 47s

Load averages:
1 minute: 3.5%
5 minutes: 4.5%
15 minutes: 4.5%
```

Рисунок – Сводная информация о загрузке системы

- **tree** – представляет процессы в виде иерархического дерева, отражающего родительско-дочерние связи между ними (см. [Рисунок – Иерархическое представление процессов в виде дерева](#)).

```
admin@ngfwos:~$ show system processes tree
PID    PGID    SID TTY      TIME CMD
2       0       0 ?        00:00:00 kthread
3       0       0 ?        00:00:00 pool_workqueue_release
4       0       0 ?        00:00:00 kworker/R-rcu_g
5       0       0 ?        00:00:00 kworker/R-rcu_p
6       0       0 ?        00:00:00 kworker/R-slub_
7       0       0 ?        00:00:00 kworker/R-netns
9       0       0 ?        00:00:00 kworker/0:0H-events_highpri
11      0       0 ?        00:00:00 kworker/u8:0-ext4-rsv-conversion
12      0       0 ?        00:00:00 kworker/R-mm_pe
13      0       0 ?        00:00:00 rcu_tasks_kthread
14      0       0 ?        00:00:00 rcu_tasks_trace_kthread
15      0       0 ?        00:00:07 ksoftirqd/0
16      0       0 ?        00:00:59 rcu_preempt
17      0       0 ?        00:00:01 migration/0
18      0       0 ?        00:00:00 idle_inject/0
19      0       0 ?        00:00:00 cpuhp/0
```

Рисунок – Иерархическое представление процессов в виде дерева

4.8 Управление питанием

Время непрерывной работы системы и средняя нагрузка

Для просмотра времени непрерывной работы **ARMA Стена** и средней нагрузки за последние 1, 5 и 15 минут, выраженную в процентах от максимально допустимого значения, необходимо в эксплуатационном режиме ввести команду:

```
admin@ngfwos:~$ show system uptime
Uptime: 1d 4h 27m 47s

Load averages:
1 minute: 3.5%
5 minutes: 4.5%
15 minutes: 4.5%
```

Перезагрузка устройства

Для перезагрузки **ARMA Стена** необходимо в эксплуатационном режиме ввести команду «**reboot**», а затем ввести «**y**» и нажать клавишу «**ENTER**» на запрос «**Are you sure you want to reboot this system? [y/N]**».

```
admin@ngfwos:~$ reboot
Are you sure you want to reboot this system? [y/N] y
```

Выключение устройства

Для выключения **ARMA Стена** необходимо в эксплуатационном режиме ввести команду «**poweroff**», а затем ввести «**y**» и нажать **клавишу «ENTER»** на запрос «**Are you sure you want to poweroff this system? [y/N]**».

```
admin@ngfwos:~$ poweroff
Are you sure you want to poweroff this system? [y/N] y
```

4.9 Zabbix

Zabbix предназначен для мониторинга состояния IT-инфраструктуры, включая серверы, сетевые устройства и приложения. Система позволяет собирать метрики, анализировать данные и оповещать об инцидентах. В системе **ARMA Стена** интегрирован zabbix-агент версии **7.0.10** для обеспечения взаимодействия и передачи данных о состоянии системы.

Команды настройки zabbix-агента:

1. Установить имя хоста, используемое Zabbix-агентом для идентификации устройства в интерфейсе Zabbix-сервера:

```
set service monitoring zabbix-agent host-name <name>
```

где **<name>** – имя хоста Zabbix-агента.

2. Установить IP-адрес или DNS-имя Zabbix-сервера, который будет подключаться к Zabbix-агенту в пассивном режиме работы:

```
set service monitoring zabbix-agent server <server>
```

где **<server>** – адрес Zabbix-сервера в формате <x.x.x.x>, <h:h:h:h:h:h:h> или <hostname>.

3. Установить порт подключения к Zabbix-агенту в пассивном режиме, через который Zabbix-сервер опрашивает клиентов:

```
set service monitoring zabbix-agent port <1-65535>
```

где **<1-65535>** – номер порта. Возможно указать значение в диапазоне от «1» до «65535». По умолчанию используется порт «10050».

4. Установить IP-адрес или DNS-имя Zabbix-сервера, который будет подключаться к Zabbix-агенту в активном режиме работы:

```
set service monitoring zabbix-agent server-active <server> port <1-65535>
```


где:

- **<server>** – адрес Zabbix-сервера в формате **<x.x.x.x>**, **<h:h:h:h:h:h:h:h>** или **<hostname>**;
- **<1-65535>** – номер порта, который будет использоваться для подключения к Zabbix-серверу в активном режиме. Возможно указать значение в диапазоне от «1» до «65535».

5. Определить на каких IP-адресах агент должен прослушивать входящие соединения:

```
set service monitoring zabbix-agent listen-address <address>
```

где **<address>** – IP-адрес в формате **<x.x.x.x>** и/или **<h:h:h:h:h:h:h:h>**. Возможно указать как один, так и несколько IP-адресов. По умолчанию используется значение «0.0.0.0» – агент прослушивает все интерфейсы.

6. Установить максимальное время ожидания ответа при обмене информацией с Zabbix-сервером:

```
set service monitoring zabbix-agent timeout <1-30>
```

где **<1-30>** – целочисленное значение времени ожидания в секундах. Возможно указать значение в диапазоне от «1» до «30». По умолчанию используется значение «3».

7. Определить максимальный размер данных в буфере памяти:

```
set service monitoring zabbix-agent limits buffer-size <2-65535>
```

где **<2-65535>** – размер буфера. Возможно указать значение в диапазоне от «2» до «65535». По умолчанию используется значение «1000». Агент отправит все собранные данные на Zabbix-сервер, если буфер будет заполнен.

8. Определить частоту отправки значений из буфера на Zabbix-сервер:

```
set service monitoring zabbix-agent limits buffer-flush-interval <1-3600>
```

где **<1-3600>** – значение частоты отправки данных из буфера. Возможно указать значение в диапазоне от «1» до «3600». По умолчанию используется значение «5». Агент отправит все собранные данные на Zabbix-сервер раньше установленного времени, если буфер будет заполнен.

9. Определить путь к директории, содержащей отдельные конфигурационные файлы для Zabbix-agent:

```
set service monitoring zabbix-agent directory <text>
```

где **<text>** – путь к директории.

10. Включить логирование выполняемых команд через Zabbix-agent:

```
set service monitoring zabbix-agent log remote-commands
```

11. Настройки уровня логирования Zabbix-agent:

```
set service monitoring zabbix-agent log debug-level <level>
```

где **<level>** – уровень детализации журнала. Возможно указать следующие значения:

- **basic** – базовый уровень логирования. Включает только самую важную информацию о работе Zabbix-agent.
- **critical** – логируются только критически важные события, которые могут привести к сбою работы Zabbix-agent.
- **error** – логируются ошибки, возникающие в процессе работы Zabbix-agent. Это более детальный уровень по сравнению с «critical».
- **warning** – логируются предупреждения, которые указывают на потенциальные проблемы, но не являются критическими. Используется по умолчанию.
- **debug** – логируется отладочная информация, включая технические детали работы Zabbix-agent.
- **extended-debug** – расширенный уровень отладочной информации. Включает максимально подробные данные о работе Zabbix-agent.

12. Установить максимальный размер файла журнала:

```
set service monitoring zabbix-agent log size <0-1024>
```

где **<0-1024>** – максимальный размер файла журнала в мегабайтах. Возможно указать значение в диапазоне от «1» до «1024». По умолчанию используется значение «0» – ротация файла отключена. Если предельный размер файла журнала достигнут и ротация файлов по какой-либо причине не удалась, существующий файл журнала затирается и начинается заново.

5 УПРАВЛЕНИЕ СИСТЕМОЙ

5.1 Управление конфигурацией

ARMA Стена использует единый конфигурационный файл для всей системы – «`/config/config.boot`», который содержит полную конфигурацию устройства. Данный подход обеспечивает удобство создания шаблонов, резервного копирования и тиражирования настроек между устройствами. Поддерживается возможность сохранения конфигурации на удалённый сервер для архивации или резервного копирования.

В системе **ARMA Стена** реализовано три типа конфигурации:

1. **Активная конфигурация** – конфигурация системы, которая в данный момент загружена и используется. Любое изменение конфигурации должно быть зафиксировано, чтобы оно стало принадлежать активной конфигурации.
2. **Рабочая конфигурация** – конфигурация, которая в данный момент изменяется в конфигурационном режиме. Изменения, внесённые в рабочую конфигурацию, не влияют на работу системы до выполнения команды «`commit`». После фиксации рабочая конфигурация становится активной конфигурацией.
3. **Сохранённая конфигурация** – конфигурация, которая была сохранена в файл («`/config/config.boot`») с помощью команды «`save`». Сохранённая конфигурация используется при последующей загрузке системы. Допускается хранение нескольких версий конфигурации.

Для просмотра параметров активной конфигурации используется команда:

```
admin@ngfwos:~$ show configuration
```

Просмотр осуществляется постранично. Навигация при просмотре выведенной информации, осуществляется с помощью клавиш клавиатуры со стрелками вверх и вниз. Для завершения просмотра параметров конфигурации следует нажать **клавишу «q»**.

Примечание:

При увеличении размера конфигурационного файла процесс применения новых настроек может замедлиться, а также может увеличиться время загрузки системы, поскольку для обработки объёмного конфигурационного файла при загрузке может потребоваться больше времени.

5.1.1 Настройки архива конфигурации

Для задания максимального количества хранимых локальных версий конфигурации необходимо ввести следующую команду:

```
set system config-management commit-revisions <N>
```

где **<N>** – целочисленное значение максимально возможного количества хранящихся активных конфигураций. Возможно указание значения в диапазоне от «1» до «65535». По умолчанию используется значение «100».

При достижении указанного лимита самая старая версия конфигурации автоматически удаляется для освобождения места под новую.

Для отображения списка всех доступных локальных резервных копий конфигурации (см. [Рисунок – Список резервных копий конфигурации](#)) необходимо в эксплуатационном режиме ввести следующую команду:

```
admin@ngfwos:~$ show system commit
```

```
admin@ngfwos:~$ show system commit
0  2024-08-27 09:17:30 by admin via cli
1  2024-08-26 15:51:01 by admin via cli
2  2024-08-26 15:40:33 by admin via cli
3  2024-08-24 15:32:41 by admin via cli
4  2024-08-24 15:30:51 by admin via cli
5  2024-08-24 15:20:27 by admin via cli
6  2024-08-21 13:02:42 by admin via cli
7  2024-08-21 13:00:51 by admin via cli
8  2024-08-21 12:28:22 by admin via cli
9  2024-08-21 12:27:49 by admin via cli
10 2024-08-21 12:27:47 by root via init
```

Рисунок – Список резервных копий конфигурации

5.1.2 Сравнение конфигураций

Для выполнения сравнения различных версий конфигурации следует использовать команду «**compare**».

Возможны следующие варианты сравнения конфигураций:

1. Для сравнения версии активной конфигурации **<N>** с версией **<M>** необходимо ввести следующую команду:

```
compare <N> <M> [commands]
```

где **<N>** и **<M>** – номера версий активной конфигурации.

Выведенный список будет содержать информацию о добавленных и удалённых параметрах версии активной конфигурации **<N>** относительно версии **<M>** в виде строк, отмеченных знаками «+» и «-» соответственно.

Дополнительный параметр «**commands**» выводит различие конфигураций в виде команд.

2. Для сравнения рабочей и активной конфигурации необходимо ввести следующую команду:

```
compare
```

3. Для сравнения рабочей и активной конфигурации и вывода списка команд «set», выполненных в рабочей конфигурации, необходимо ввести следующую команду:

```
compare commands
```

4. Для сравнения рабочей конфигурации с сохранённой необходимо ввести следующую команду:

```
compare saved
```

5. Для сравнения рабочей конфигурации с выбранной версией **<N>** активной конфигурации необходимо ввести следующую команду:

```
compare <N> [commands]
```

где **<N>** – номер версии активной конфигурации.

6. В эксплуатационном режиме для сравнения рабочей и активной конфигурации необходимо ввести следующую команду:

```
~$ show system commit diff <N>
```

Примечание:

Для текущего пользователя команда **«compare»** позволяет просматривать изменения только в тех разделах конфигурации, которые были указаны в его пользовательском классе в параметре **«configure-command show [раздел_конфигурации]»**. Если изменения, внесённые с помощью команд **«set»** или **«delete»**, не затрагивают разрешённые для отображения разделы, то на экране появится сообщение **«No changes between working and active configurations»** или, в случае использования команды **«compare commands»**, пустая строка.

Если у пользовательского класса указана общая команда **«configure-command show»**, то будут показаны все изменения во всех разделах конфигурации без каких-либо ограничений.

Если команда **«show»** не задана ни для конкретных разделов, ни в общем виде, то также появится сообщение **«No changes between working and active configurations»** (или пустая строка для команды **«compare commands»**), даже если были внесены изменения в конфигурацию.

5.1.3 Восстановление конфигурации

Для выполнения восстановления конфигурации к какой-либо версии активной конфигурации необходимо использовать команду **«rollback»**.

В процессе восстановления автоматически будет создана сохранённая конфигурация, аналогичная выбранной версии активной конфигурации, и выполнена перезагрузка **ARMA Стена**, для подтверждения которой необходимо ввести **«y»** и нажать **клавишу «ENTER»**:

```
rollback <N>
Proceed with reboot? [Y/n] y
```

Примечание:

Не рекомендуется восстанавливать конфигурацию с пометкой **«init»**, так как это может привести к некорректной работе системы (см. [Рисунок – Список резервных версий конфигурации](#)).

```
admin@ngfwos# rollback
Possible completions:
<N> Rollback to revision N (requires reboot)
      (use rollback-soft for a non-disruptive rollback)

Revisions:
 0  2025-03-05 16:03:04 admin by cli
 1  2025-03-05 10:35:02 admin by cli
 2  2025-03-05 10:15:30 admin by cli
 3  2025-03-05 10:10:03 admin by cli
 4  2025-03-05 07:34:58 admin by cli
 5  2025-03-05 07:34:29 admin by cli
 6  2025-03-05 07:30:31 admin by cli
 7  2025-03-04 16:07:46 admin by cli
 8  2025-03-04 15:12:38 admin by cli
 9  2025-03-04 15:09:03 admin by cli
10  2025-03-04 15:07:48 admin by cli
11  2025-03-04 11:18:32 admin by cli
12  2025-03-04 11:17:33 admin by cli
13  2025-03-04 10:19:52 root  by ngfwos-boot-config-loader
14  2025-03-04 10:00:02 admin by cli
15  2025-03-04 09:59:19 root  by ngfwos-boot-config-loader
16  2025-03-04 09:59:11 root  by init
```

Рисунок – Список резервных версий конфигурации

5.1.4 Удаление конфигурации

Для удаления локального архива конфигурации необходимо ввести следующую команду в эксплуатационном режиме:

```
admin@ngfwos:~$ delete commit <N>
```

где **<N>** - номер архива конфигурации в локальном хранилище.

После успешного удаления система выведет соответствующее уведомление:

```
Successfully deleted revision <N>.  
admin@ngfwos:~$
```

Система предоставляет возможность одновременного удаления нескольких конфигурационных архивов. Для этого в эксплуатационном режиме необходимо ввести следующую команду:

```
admin@ngfwos:~$ delete commit <N1,N2,...,Nn>
```

где **<N1,N2,...,Nn>** - номера архивов конфигурации в локальном хранилище, указанные через запятую без пробелов.

После успешного удаления система выведет соответствующее уведомление:

```
Successfully deleted revision <N1, N2, ..., Nn>.  
admin@ngfwos:~$
```

Примечание:

Удалять конфигурацию с меткой **«init»** запрещено.

5.1.5 Экспорт конфигурации

Система **ARMA Стена** поддерживает два основных способа экспорта конфигурации: **ручной экспорт**, инициируемый администратором, и **автоматический экспорт**, выполняемый после каждой успешной фиксации конфигурации (команда **«commit»**).

5.1.5.1 Ручной экспорт конфигурации

Ручной экспорт предназначен для сохранения текущей активной конфигурации (**«config.boot»**) либо в виде файла на локальной файловой системе устройства, либо в виде архива при передаче на удалённый сервер.

Локальное сохранение

Конфигурация сохраняется в файл на локальной файловой системе устройства с использованием следующей команды в конфигурационном режиме:

```
save <track>/<file>
```

где:

- **<track>** – путь к директории для сохранения;
- **<file>** – имя файла конфигурации.

Если путь не указан, файл сохраняется в домашний каталог пользователя, от имени которого выполнена команда (например, для пользователя «admin» это будет каталог **«/home/admin/»**).

Примечание:

При выполнении команды от учётной записи, отличной от «**admin**», сохранение конфигурации возможно только в домашний каталог данной учётной записи или в директорию «**/tmp/**». Попытка указать иной путь приводит к отказу в выполнении операции.

Только учётная запись «**admin**» обладает правами на сохранение файла в системные каталоги, отличные от домашнего каталога пользователя и директории **/tmp/**.

Пример сохранения конфигурации под именем «**test.boot**» в локальный каталог «**/config/**»:

```
[edit]
admin@ngfwos# save /config/test.boot
```

Экспорт на удалённый сервер

Поддерживается передача архива конфигурации на удалённый сервер по протоколам **TFTP, FTP, SCP, SFTP**.

Примечание:

Экспорт архива конфигурации на удалённый сервер доступен только для встроенной учётной записи «**admin**».

Архив конфигурации содержит следующие файлы:

- основной файл конфигурации («**config.boot**»);
- полное содержимое каталога «**/config/files/**» (сертификаты, скрипты и прочие дополнительные файлы);
- полное содержимое каталога «**/config/scripts/**».

Структура архива:

```
config.boot - основной файл конфигурации
/files/ — копия содержимого каталога /config/files/
├─ suricata_db
└─ configuration
    ├─ — app-control
    ├─ — service
    ├─ — suricata
    └─ — third-party
/scripts/ — копия содержимого каталога /config/scripts/
└─ commit
    └─ — pre-hooks.d
```

Для экспорта используется следующая команда в конфигурационном режиме:

```
save <URL>
```

где **<URL>** - URI удалённого ресурса. Поддерживаются следующие URL:

- **scp://<user>:<passwd>@<host>:<file>;**
- **sftp://<user>:<passwd>@<host>:<file>;**
- **ftp://<user>:<passwd>@<host>:<file>;**
- **tftp://<host>:<file>.**

Параметры URI:

- **<user>** – имя пользователя на удалённом сервере;
- **<passwd>** – пароль пользователя;
- **<host>** – сетевой адрес удалённого сервера (IP-адрес или доменное имя);
- **<file>** – полный путь и имя файла на удалённом сервере.

Пример экспорта конфигурационного архива под именем «ngfw1.config» на TFTP-сервер: «tftp://192.168.0.100»:

```
save tftp://192.168.0.100/ngfw1.config
```

Экспорт зашифрованного архива

Для повышения уровня защиты конфигурационных данных поддерживается экспорт в виде зашифрованного архива.

Примечание:

Экспорт зашифрованного архива конфигурации на удалённый сервер доступен исключительно для встроенной учётной записи «**admin**».

Команда для инициализации зашифрованного экспорта:

```
save <track>/<file> | <URL> <symbol>
```

где:

- **<track>/<file>** – локальный путь и имя файла;
- **<URL>** – URI удалённого сервера (при экспорте по сети);
- **<symbol>** – произвольный символ (например, «р»), указывающий на необходимость шифрования. Символ не влияет на содержимое, но обязателен для активации режима шифрования. В качестве символа не допускается использование специальных символов: «'», «"», «`».

При локальном сохранении конфигурации с включённым шифрованием создаётся архив, аналогичный тому, который формируется при экспорте на удалённый сервер. В этом случае сохраняется не только основной файл конфигурации («config.boot»), но и полное содержимое каталогов «/config/files/» и «/config/scripts/».

Пример команды:

```
save /config/backup.ngfw.7z p
```

```
save scp://admin:pass@192.168.10.50 /backups/ngfw p
```

После выполнения команды система запросит ввод пароля для шифрования архива:

Please provide password to encrypt archive with configuration:

Необходимо ввести пароль и подтвердить его нажатием клавиши **«Enter»**. Восстановление данных без пароля невозможно.

5.1.5.2 Автоматический экспорт конфигурации

После каждой успешной операции «commit» система **ARMA Стена** может автоматически создавать и передавать резервную копию конфигурации на удалённый ресурс.

Имя экспортируемого архива формируется по шаблону: **«config.boot-hostname.ГГГГММДД_ЧЧММСС»**.

Поддерживается экспорт на удалённые серверы по следующим протоколам: **TFTP**, **FTP**, **SCP**, **SFTP**, а также в репозиторий **Git**. Экспорт может быть настроен как в открытом виде, так и с шифрованием архива.

Архив конфигурации содержит:

- основной файл конфигурации (**config.boot**);
- полное содержимое каталога **/config/files/**.

Автоматический экспорт в открытом виде

Для настройки автоматического экспорта без шифрования используются следующие команды в конфигурационном режиме:

```
set system config-management commit-archive location <URI>  
set system config-management commit-archive source-address <address>
```

где:

- **<URI>** – URI удалённого ресурса;

- **<addres>** – IP-адрес интерфейса системы **ARMA Стена**, используемый как источник при передаче.

Поддерживаются следующие форматы URI:

- `http://<user>:<passwd>@<host>:/<dir>`
- `https://<user>:<passwd>@<host>:/<dir>`
- `ftp://<user>:<passwd>@<host>/<dir>`
- `sftp://<user>:<passwd>@<host>/<dir>`
- `scp://<user>:<passwd>@<host>/<dir>`
- `tftp://<host>/<dir>`
- `git+https://<user>:<passwd>@<host>/<path>`

Параметры:

- **<user>** – имя пользователя для аутентификации на удалённом сервере;
- **<passwd>** – пароль пользователя;
- **<host>** – сетевой адрес удалённого сервера (IP-адрес или доменное имя);
- **<dir>** – каталог на удалённом сервере для сохранения файла;
- **<path>** – путь к Git-репозиторию.

Автоматический экспорт в зашифрованном виде

Для обеспечения конфиденциальности конфигурационных данных при автоматическом экспорте поддерживается шифрование архива.

Для включения шифрования необходимо добавить параметр **password**:

```
set system config-management commit-archive location <URI>
set system config-management commit-archive source-address <addres>
set system config-management commit-archive password <password>
```

где **<password>** – пароль, используемый для шифрования архива конфигурации.

5.1.6 Импорт конфигурации

Система **ARMA Стена** поддерживает два метода импорта конфигурации:

- **Полная замена (load)** – замещение текущей конфигурации загружаемой.
- **Объединение (merge)** – интеграция параметров из внешнего файла конфигурации в текущую конфигурацию без удаления существующих настроек.

Полная замена конфигурации (load)

Примечание:

Возможен импорт как файла конфигурации, так и архива конфигурации. При импорте архива конфигурации директории «/config/files/» и «/config/scripts»/ **ARMA Стена** будут переименованы в «/config/files.bk» и «/config/scripts.bk», после чего директории из архива будут распакованы в соответствующий каталог. При выполнении команд «commit» и «save», переименованные каталоги будут безвозвратно удалены. Если сохранение конфигурации не будет выполнено (например, выполнением команды «exit discard») или **ARMA Стена** будет перезагружена до сохранения конфигурации, то система восстановит старый файл конфигурации и каталоги.

1. Для импорта новой конфигурации с заменой текущей необходимо ввести следующую команду:

```
load <source>
```

где **<source>** – путь или URI к файлу конфигурации.

Примечание:

Если выполняется импорт из зашифрованного архива конфигурации, система запросит пароль от архива.

Поддерживаются следующие источники:

- **<file>** – локальный файл в файловой системе устройства;
- **scp://<user>:<passwd>@<host>:<file>** – файл на удалённом сервере по протоколу SCP;
- **sftp://<user>:<passwd>@<host>/<file>** – файл по протоколу SFTP;
- **ftp://<user>:<passwd>@<host>/<file>** – файл по протоколу FTP;
- **http://<host>/<file>** – файл по протоколу HTTP;
- **https://<host>/<file>** – файл по протоколу HTTPS;
- **tftp://<host>/<file>** – файл по протоколу TFTP.

Параметры URI:

- **<user>** – имя пользователя на удалённом сервере;
- **<passwd>** – пароль пользователя;
- **<host>** – сетевой адрес удалённого сервера (IP-адрес или доменное имя);

- **<file>** – путь и имя файла конфигурации на удалённой или локальной системе.

2. Установка пароля администратора.

Во время импорта файла конфигурации система запросит установку нового пароля для учётной записи **admin**:

```
Do you want set admin password for new configuration? [Y/n]
```

При выборе «**Y**» система последовательно запросит ввод и подтверждение нового пароля:

```
Please enter a password for the "admin" user:  
Please confirm password for the "admin" user:
```

При отказе от установки пароля (выбор «**n**») будет применён пароль по умолчанию: «*admin*».

3. Подтверждение загрузки конфигурации.

После успешной загрузки появится сообщение:

```
Loading configuration from '/home/admin/backup.config.boot'  
Load complete. Use 'commit' to make changes effective.  
[edit]
```

Для фиксации изменений требуется выполнить команды:

```
admin@ngfwos# commit  
[edit]  
admin@ngfwos# save
```

В качестве примера приведены команды для выполнения:

- импорта конфигурационного файла «ngfw1.config.boot» из локальной директории «/config/»:

```
load /config/ngfw1.config.boot
```

- импорта конфигурационного файла «050424.config.boot» с FTP-сервера «ftp://46.24.16.27»:

```
load ftp://ngfw:Fgw43!dweP@46.24.16.27/050424.config.boot
```

Объединение конфигурации (merge)

Команда **merge** добавляет параметры из указанного файла конфигурации в текущую конфигурацию без удаления существующих настроек. Если в

загружаемом файле содержатся параметры, уже присутствующие в текущей конфигурации, они будут перезаписаны.

Формат команды в конфигурационном режиме для объединения конфигураций:

```
admin@ngfwos# merge <source>

Merge complete. Use 'commit' to make changes effective.
[edit]
admin@ngfwos# commit
[edit]
admin@ngfwos# save
```

Поддерживаются следующие источники:

- **<file>** - локальный файл в файловой системе устройства;
- **scp://<user>:<passwd>@<host>:<file>** - файл на удалённом сервере по протоколу SCP;
- **sftp://<user>:<passwd>@<host>/<file>** - файл по протоколу SFTP;
- **ftp://<user>:<passwd>@<host>/<file>** - файл по протоколу FTP;
- **http://<host>/<file>** - файл по протоколу HTTP;
- **https://<host>/<file>** - файл по протоколу HTTPS;
- **tftp://<host>/<file>** - файл по протоколу TFTP.

Примечание:

Файл конфигурации, используемый в команде «**merge**», обязательно должен содержать корневой раздел «**interfaces**», даже если он пустой. Отсутствие данного раздела приведёт к ошибке выполнения команды, и операция объединения будет отменена.

5.2 Обновление системы

Обновление программного обеспечения системы **ARMA Стена** поставляется в виде файла образа в формате «**ISO**».

Файл обновления может быть получен одним из следующих способов:

- загрузка файла с удалённого сервера компании «**InfoWatch ARMA**»;
- использование USB-накопителя, предоставленного компанией «**InfoWatch ARMA**».

Примечание:

Для выполнения процедуры обновления требуется наличие свободного места на диске объёмом не менее **16 Гбайт**, плюс объём, занимаемый каталогом «**/config/**».

Для получения информации о состоянии файлового хранилища в эксплуатационном режиме необходимо выполнить команду (см. [Рисунок – Информация об файловом хранилище](#)):

```
admin@ngfwos:~$ show system storage
```

```
admin@ngfwos:~$ show system storage
Filesystem      Size  Used Avail Use% Mounted on
udev            7.5G     0  7.5G   0% /dev
tmpfs           1.5G   2.9M   1.5G   1% /run
/dev/sda3       234G   759M   221G   1% /usr/lib/live/mount/persistence
/dev/loop0      531M   531M     0 100% /usr/lib/live/mount/rootfs/4.4.2.squashfs
tmpfs           7.5G     0  7.5G   0% /usr/lib/live/mount/overlay
overlay         234G   759M   221G   1% /
tmpfs           7.5G     0  7.5G   0% /dev/shm
tmpfs           5.0M     0   5.0M   0% /run/lock
efivarfs        192K    66K   122K  36% /sys/firmware/efi/efivars
tmpfs           7.5G   4.0K   7.5G   1% /tmp
tmpfs           7.5G  256K   7.5G   1% /var/tmp
none            7.5G     0  7.5G   0% /etc/cni/net.d
none            7.5G    68K   7.5G   1% /opt/vyatta/config
tmpfs           1.5G     0   1.5G   0% /run/user/1002
admin@ngfwos:~$
```

Рисунок – Информация об файловом хранилище

Примечание:

Перед началом процедуры обновления рекомендуется выполнить резервное копирование конфигурации системы **ARMA Стена**. Инструкция по созданию резервной копии приведена в разделе «[Экспорт конфигурации](#)» настоящего руководства.

Примечание:

В случае, если в системе настроена аутентификация по протоколу **Kerberos**, перед выполнением обновления необходимо скопировать файл «***.keytab**» из каталога «**/home/admin/**» (каталог указан по умолчанию и может отличаться от фактически используемого пользователем) в каталог «**/config/**».

В случае необходимости сохранения критически важных данных, таких как внешние сертификаты, пользовательские правила СОВ или пользовательские скрипты, которые расположены за пределами директории «**/config/**», требуется осуществить их предварительное копирование в указанную директорию перед выполнением обновления.

После завершения обновления системы следует вернуть перенесённые файлы обратно в их первоначальные директории.

Примечание:

При выполнении обновления программного обеспечения системы **ARMA Стена** с версии **4.5** до версии **4.8** текущая лицензия становится недействительной. В этом случае требуется повторная активация системы с использованием нового лицензионного ключа. Подробнее о шагах повторной активации см. «[Повторная активация лицензии](#)».

Рекомендуется заблаговременно обратиться в службу технической поддержки ООО «ИнфоВотч АРМА» для получения нового ключа активации.

Примечание:

При обновлении системы **ARMA Стена** в отказоустойчивый кластер с настроенной синхронизацией конфигурации, необходимо соблюдать следующий порядок действий:

1. Выполнить обновление программного обеспечения на резервном узле **ARMA Стена**.
2. После успешного завершения обновления резервного узла выполнить обновление основного (мастер) узла **ARMA Стена**.

Отключение узла, не подвергающегося обновлению, в процессе обновления второго узла не требуется.

В течение всего процесса обновления не рекомендуется вносить изменения в конфигурационные файлы на обоих узлах кластера во избежание конфликтов конфигураций или некорректного применения настроек.

Примечание:

После завершения процедуры обновления создаётся новый экземпляр глобального журнала событий. Записи событий, сформированные до обновления, сохраняются и остаются доступны в предыдущей версии системы.

Процедура установки обновления:

1. Выполнить аутентификацию в системе **ARMA Стена** с использованием встроенной учётной записи **admin** или иной учётной записи, обладающей привилегиями на выполнение команды «**add**» в эксплуатационном режиме (см. раздел «[Временная блокировка учётных записей](#)»).

2. Скопировать полученный ISO-образ обновления в локальную директорию файловой системы **ARMA Стена**.

Для выполнения данной операции возможно использовать программное обеспечение, поддерживающее передачу файлов по протоколам SFTP или SCP (например, WinSCP для операционной системы Windows), либо воспользоваться командой «scp» через интерфейс командной строки. Возможны также альтернативные способы передачи данных.

3. В эксплуатационном режиме выполнить команду установки образа:

```
admin@ngfwos:~$ add system image </config/ngfw.iso>
```

где:

- **</config/ngfw.iso>** – путь к загруженному файлу (указан в качестве примера).

4. После успешной проверки контрольной суммы ISO-образа установщиком ввести имя сборки и подтвердить выбор нажатием **клавиши «ENTER»**:

```
Validating image checksums  
What would you like to name this image? (Default: номер_релизной_версии_ПО)
```

5. Подтвердить назначение нового образа в качестве загружаемого по умолчанию, введя **«y»** и нажав **клавишу «ENTER»**:

```
Would you like to set the new image as the default one for boot? [Y/n]
```

6. Подтвердить копирование текущей активной конфигурации в новый образ, введя **«y»** и нажав **клавишу «ENTER»**:

```
An active configuration was found. Would you like to copy it to the new image? [Y/n]
```

7. Подтвердить копирование SSH-ключей текущей конфигурации, введя **«y»** и нажав **клавишу «ENTER»**:

```
Copying configuration directory  
Would you like to copy SSH host keys? [Y/n]
```

Примечание:

В случае отсутствия свободного места на диске установка будет отменена.

8. После успешного завершения процедуры обновления выполнить перезагрузку системы:

```
Copying SSH host keys
Copying system image files
Cleaning up
Unmounting target filesystems
Removing temporary files
```

```
# Команда перезагрузки системы:
admin@ngfwos:~$ reboot
```

```
# Ввести «у» для подтверждения перезагрузки системы:
Are you sure you want to reboot this system? [y/N] y
```

9. После перезагрузки системы необходимо перейти в конфигурационный режим и выполнить сохранение активной конфигурации:

```
admin@ngfwos:~$ configure
[edit]
admin@ngfwos# save
[edit]
admin@ngfwos# exit
exit
```

Примечание:

В случае, если сохранение конфигурации не было выполнено, после повторной перезагрузки система перейдёт в аварийный режим работы. Для выхода из аварийного режима необходимо повторить шаги из п.9 и выполнить команду «**emergency exit**».

10. Для корректной инициализации службы контроля целостности необходимо произвести повторную перезагрузку системы.

```
admin@ngfwos:~$ reboot
Are you sure you want to reboot this system? [y/N] y
```

Примечание:

В случае недоступности системы **ARMA Стена** по сети после перезагрузки требуется инициировать повторную перезагрузку устройства через локальный интерфейс CLI. Данное действие обеспечит восстановление сетевого доступа к системе.

Переназначение загрузочного образа

Изменение образа, используемого по умолчанию, возможно двумя способами:

- через командный интерфейс (CLI);

- через меню загрузчика GRUB.

Использование CLI:

1. В эксплуатационном режиме выполнить команду

```
admin@ngfwos:~$ set system image default-boot
```

2. В выведенном списке доступных образов выбрать требуемый, ввести соответствующий номер строки и нажать **клавишу «ENTER»**:

```
The following images are available:
  1: 4.8 (running) (default boot)
  2: 4.7
Select an image to set as default:
```

3. Перезагрузить систему:

```
Select the default boot image: 2
The image "4.7" is now default boot image

admin@ngfwos:~$ reboot
```

Использование меню GRUB:

При перезагрузке системы в течение 5 секунд после старта отображается меню **GRUB**, позволяющее выбрать требуемый образ вручную (см. [Рисунок – Выбор образа для загрузки](#)).



Рисунок – Выбор образа для загрузки

Удаление архивного образа

Для освобождения дискового пространства допускается удаление неиспользуемых образов.

1. В эксплуатационном режиме ввести команду:

```
admin@ngfwos:~$ delete system image
```

2. В выведенном списке выбрать образ, подлежащий удалению, ввести соответствующий номер строки (например, **2**) и нажать **клавишу «ENTER»**:

```
The following image(s) can be deleted:
```

```
1: 4.8 (running) (default boot)
2: 4.7
```

Select an image to delete: 2

Примечание:

Удаление образа, назначенного по умолчанию, невозможно. Перед удалением требуется переназначить загрузочный образ по умолчанию на другой.

3. Подтвердить удаление, введя **«y»** и нажав **клавишу «ENTER»**:

```
Do you really want to delete the image 4.7? [y/N] y
```

4. По завершении операции выводится сообщение: **«The image "4.7" was successfully deleted»**.

Информация о версиях образов

Для отображения информации о текущей версии программного обеспечения необходимо выполнить команду **«show version»**.

Для просмотра списка сохранённых образов используется команда эксплуатационного режима:

```
admin@ngfwos:~$ show system image
Name                               Default boot   Running
-----
4.8                               Yes            Yes
4.7
admin@ngfwos:~$
```

5.3 Сброс настроек

В системе **ARMA Стена** предусмотрена возможность сброса текущей конфигурации до заводских настроек.

Для выполнения сброса необходимо последовательно выполнить следующие действия:

1. Загрузка конфигурации по умолчанию.

В конфигурационном режиме необходимо выполнить команду:

```
admin@ngfwos# load /opt/ngfwos/etc/config.boot.default
```

2. Установка пароля администратора.

Система запросит установку нового пароля для учётной записи **«admin»**:

```
Do you want set admin password for new configuration? [Y/n]
```

При выборе **«Y»** система последовательно запросит ввод и подтверждение нового пароля:

```
Please enter a password for the "admin" user:
Please confirm password for the "admin" user:
```

При отказе от установки пароля (выбор **«n»**) будет применён пароль по умолчанию: **«admin»**.

3. Подтверждение загрузки конфигурации.

После успешной загрузки появится сообщение:

```
Loading configuration from '/opt/ngfwos/etc/config.boot.default'
Load complete. Use 'commit' to make changes effective.
[edit]
```

Для фиксации изменений требуется выполнить команду:

```
admin@ngfwos# commit
```

При выполнении сброса через SSH-соединение после команды «commit» соединение будет разорвано. Это обусловлено отсутствием в конфигурации по умолчанию настроек сетевых интерфейсов и параметров SSH-доступа.

Дальнейшее взаимодействие с системой возможно только через локальную консоль. Необходимо войти в систему под учётной записью «admin», используя пароль, заданный на этапе сброса, либо пароль по умолчанию (admin), если установка пароля была отклонена.

Примечание:

Для отмены сброса вместо команды **«commit»** следует выполнить **«exit discard»**.

4. Сохранение конфигурации.

После входа в локальную консоль следует перейти в режим конфигурирования и выполнить сохранение конфигурации:

```
admin@ngfwos:~$ configure
[edit]
admin@ngfwos# save
```

Без выполнения данной команды после перезагрузки система восстановит предыдущую (сохранённую) конфигурацию, и сброс не будет зафиксирован.

5. Перезагрузка устройства.

Для окончательного применения заводских настроек необходимо перезагрузить устройство:

```
admin@ngfwos# run reboot
Are you sure you want to reboot this system (ngfwos)? [y/N] y
```

После перезагрузки система **ARMA Стена** будет работать с конфигурацией по умолчанию.

5.4 Аварийный режим

В системе **ARMA Стена** предусмотрено два механизма активации аварийного режима:

1. автоматический переход в аварийный режим;
2. переход в аварийный режим по команде оператора.

Примечание:

При переходе системы **ARMA Стена** в аварийный режим весь сетевой трафик, проходящий через устройство, блокируется до устранения причин, вызвавших сбой. Управление системой в данном состоянии осуществляется исключительно через локальную консоль.

Примечание:

При возникновении критических ошибок ядра системы **ARMA Стена** (*kernel panic*), система выведет уведомление «**Rebooting in 60 seconds**» и автоматически перезагрузится через 60 секунд для восстановления работоспособности.

В случае невозможности восстановления работоспособности после перезагрузки рекомендуется обратиться в службу технической поддержки **ООО «ИнфоВотч АРМА»**.

5.4.1 Автоматический переход в аварийный режим

Автоматический переход в аварийный режим инициируется по следующим причинам:

1. Нарушение целостности конфигурационного файла системы.

Функция контроля целостности обеспечивает мониторинг состояния конфигурационных файлов, и в случае обнаружения нарушения целостности система автоматически переходит в аварийный режим работы.

Для восстановления конфигурационного файла рекомендуется использовать процедуру восстановления конфигурации из архивных локальных копий (см. раздел «[Восстановление конфигурации](#)»).

В случае невозможности восстановления файла конфигурации, существует возможность выполнить сброс настроек системы до заводских параметров (см. раздел «[Сброс настроек](#)»). При выполнении команды сброса система выводит предупреждение о предстоящем отключении аварийного режима. После подтверждения система восстанавливает сетевые интерфейсы, отключает аварийный режим и загружает конфигурацию по умолчанию.

2. Наличие менее 5% свободного места на диске.

В случае возникновения ситуации, когда система не сможет вести журнал событий из-за недостатка свободного места на диске, она автоматически перейдёт в аварийный режим для обеспечения безопасности и контроля сетевого трафика.

При объёме свободного места менее 10 % система каждые 60 секунд выводит предупреждение: «*Free space on disk is low, please clear logs*».

Для освобождения места на диске рекомендуется очистить глобальный журнал событий (см. раздел «[Настройки глобального журнала](#)»).

5.4.2 Переход в аварийный режим по команде оператора

Для активации аварийного режима вручную необходимо выполнить следующие действия:

1. Ввести в эксплуатационном режиме команду:

```
admin@ngfwos:~$ emergency enter
```

2. Ввести «y» для подтверждения перехода в аварийный режим:

```
Emergency mode will block all network traffic and you will need to manually exit it.  
Continue? [y/N]
```

Примечание:

В случае выполнения команды перехода в аварийный режим через удалённое подключение по протоколу SSH, связь с системой **ARMA Стена** будет прервана после подтверждения. Дальнейшее управление возможно только через локальную консоль.

3. Система выведет уведомление о блокировке всего сетевого трафика:

```
Entering emergency state
```

```
All network traffic was stopped
```

```
admin@ngfwos:~$
```

После перезагрузки системы выведет предупреждение о работе в аварийном режиме (см. [Рисунок – Аварийный режим работы](#)).

```
[ OK ] Finished systemd-user-sess...ervice - Permit User Sessions.
[ OK ] Started getty@tty1.service - Getty on tty1.
[ OK ] Reached target getty.target - Login Prompts.

Welcome to NGFWOS - ngfwos tty1

ngfwos login: [ 61.620447] ngfwos-router[1160]: System is emergency state caus
ed by 1 reason(s)
[ 61.620729] ngfwos-router[1160]: See logs & '/config/emergency_state' for mor
e details
[ 61.620884] ngfwos-router[1160]: You can rollback to older config or load def
ault
[ 61.621042] ngfwos-router[1160]: You can exit emergency state with op-command
'emergency exit'

Hint: Num Lock on

ngfwos login: admin
Password:
Welcome to NGFWOS!

      NGFWOS 4.5.1

admin@ngfwos:~$
```

Рисунок – Аварийный режим работы

Примечание:

При выполнении команды «**emergency enter**» в активированном аварийном режиме, система выведет сообщение «**Already in emergency state**», информирующее о том, что она уже находится в этом режиме.

При функционировании системы в режиме аварийной работы возникновение сообщения «**System is emergency state**» указывает на повторное нарушение целостности контролируемых объектов.

5.4.3 Информация о причинах перехода в аварийный режим

Для получения сведений о текущем состоянии системы в эксплуатационном режиме используется команда:

```
admin@ngfwos:~$ emergency state

#Пример вывода информации:
System is in emergency state caused by 3 reason(s)
See logs & '/config/emergency_state' for more details
You can rollback to older config or load default
You can view reasons with op-command 'emergency state reasons'
You can exit emergency state with op-command 'emergency exit'

admin@ngfwos:~$
```

Данный вывод указывает, что система находится в аварийном режиме, содержит количество зафиксированных причин перехода, а также рекомендации по диагностике и восстановлению.

Для получения детализированного перечня причин перехода в аварийный режим, включая временные метки и описания событий, используется команда:

```
admin@ngfwos:~$ emergency state reasons

#Пример вывода информации:
[Reason #1]
[Datetime]: 18.11.2025 08:27:15
[Reason]:
/config/config.boot integrity violation
=====
[Reason #2]
[Datetime]: 18.11.2025 08:28:25
[Reason]:
/config/config.boot integrity violation
=====
[Reason #3]
[Datetime]: 18.11.2025 08:29:28
[Reason]:
/config/config.boot integrity violation
=====

admin@ngfwos:~$
```

Дополнительно информация о причинах перехода в аварийный режим сохраняется в файле «**/config/emergency_state**». Данный файл может использоваться для последующего анализа или передачи в службу технической поддержки.

5.4.4 Отключение аварийного режима

Примечание:

Для отключения аварийного режима система **ARMA Стена** должна иметь активную лицензию. Подробнее об активации системы **ARMA Стена** в разделе [«Управление лицензией»](#).

Независимо от способа перехода в аварийный режим (автоматический или ручной), для выхода из него необходимо выполнить команду отключения аварийного режима. Для этого необходимо выполнить следующие действия:

1. Устранить причину активации аварийного режима.
2. Ввести команду для выхода из аварийного режима:

```
admin@ngfwos:~$ emergency exit
```

3. Подтвердить перезагрузку системы, введя «у»:

```
WARNING!!! ALL SYSTEM INTEGRITY WILL RECALCULATED!!!  
To exit from emergency mode you will need to reboot. Reboot now? [y/N]
```

Примечание:

В случае подтверждения перезагрузки и отключения аварийного режима система произведёт пересчёт контрольных сумм для всех отслеживаемых файлов.

4. Если причина неполадки устранена, система будет загружаться в штатном режиме.

5.4.5 Дополнительные параметры

В системе **ARMA Стена** предусмотрена возможность деактивации механизма блокировки сетевых интерфейсов при переходе в режим аварийной работы. Данная функциональность необходима в случаях ограниченной физической доступности управляющего оборудования или при критичных требованиях к обеспечению непрерывности сетевого трафика.

Примечание:

В целях обеспечения безопасности и соответствия требованиям ФСТЭК России рекомендуется не отключать механизм блокировки сетевых интерфейсов при переходе системы в аварийный режим работы.

Примечание:

Право на деактивацию функции блокировки сетевых интерфейсов в случае перевода системы в аварийный режим предоставлено исключительно встроенной учётной записи «**admin**».

Для выключения блокировки сетевых интерфейсов в аварийном режиме необходимо ввести следующие команды в конфигурационном режиме:

```
admin@ngfwos# set system option emergency remove-nics no
```

```
# Применить настройку:
```

```
admin@ngfwos# commit
```

```
WARNING! You are disabling the automated removal of nics after entering emergency state.
```

```
FSTEC of Russia strongly recommends to have this option enabled. You are acting at your own risk!
```

```
# Сохранить изменения:
```

```
admin@ngfwos# save
```

При установленном параметре «**remove-nics**» в значение «**yes**» будут блокироваться все сетевые интерфейсы устройства при переходе в аварийный режим работы. В данном режиме управление системой осуществляется исключительно посредством локальной консоли. **Значение используется по умолчанию.**

В случае установки параметра «**remove-nics**» в значение «**no**», система продолжит функционировать без блокировки сетевых интерфейсов, при этом будут выводиться предупреждающие сообщения о работе в аварийном режиме.

5.4.6 Загрузка в аварийном режиме при неисправности интерфейса

В случае отказа физического интерфейса, система **ARMA Стена** после перезагрузки автоматически переходит в аварийный режим работы (см. [Рисунок – Загрузка системы в аварийном режиме при неисправном физическом интерфейсе](#)). Возврат к штатному режиму функционирования посредством команды «emergency exit» невозможен, так как в конфигурационном файле сохраняются данные о неисправном интерфейсе. При последующих загрузках система выполняет проверку конфигурации, и при отсутствии вышедшего из строя физического интерфейса повторно активирует аварийный режим.

```
[ OK ] Finished systemd-user-sess...ervice - Permit User Sessions.
[ OK ] Started getty@tty1.service - Getty on tty1.
[ OK ] Reached target getty.target - Login Prompts.
[ 54.217759] ngfwos-router[1610]: This application is in emergency state cause
d by: error loading config /opt/vyatta/etc/config/config.boot
[ 54.475184] ngfwos-router[2498]: WARNING:root:Adding new reason of emergency
state. See /config/emergency_state
[ 54.506694] ngfwos-router[1610]: This system now is in emergency state. Pleas
e rollback to older config or load default
[ 54.507410] ngfwos-router[1610]: You can exit emergency state with op-command
'emergency exit'
[ 55.131259] ngfwos-config[1158]: Configuration error

Welcome to NGFWOS - ngfwos tty1
ngfwos login: _
```

Рисунок – Загрузка системы в аварийном режиме при неисправном физическом интерфейсе

Для восстановления штатного режима работы системы необходимо выполнить следующую последовательность действий:

1. сохранить текущую конфигурацию с помощью команды **«save»** в конфигурационном режиме;
2. деактивировать аварийный режим с использованием команды **«emergency exit»**.

Перейди в конфигурационный режим:

```
admin@ngfwos:~$ configure
```

WARNING: There was a config error on boot: saving the configuration now could overwrite data.

You may want to check and reload the boot config

Сохранить конфигурацию:

```
admin@ngfwos# save
```

Выйди из конфигурационного режима:

```
admin@ngfwos# exit
```

Выйти из аварийного режима работы системы:

```
admin@ngfwos:~$ emergency exit
```

Подтвердить выход из аварийного режима работы системы, ввести «y» и нажать клавишу «Enter»:

WARNING!!! ALL SYSTEM INTEGRITY WILL RECALCULATED!!!

To exit from emergency mode you will need to reboot. Reboot now? [y/N] y

После выполнения указанных действий система перезагрузится и возобновит работу в штатном режиме. Информация о вышедшем из строя физическом

интерфейсе будет удалена из конфигурационного файла, что исключит повторный переход в аварийный режим.

5.5 Контроль целостности

Контроль целостности (**КЦ**) представляет собой механизм, предназначенный для обнаружения и предотвращения несанкционированных изменений или повреждений файлов, способных нарушить безопасность и работоспособность системы **ARMA Стена**.

Автоматическая проверка **КЦ** выполняется в следующие моменты:

- при загрузке системы;
- ежечасно в момент времени **xx:00:00**;
- при выполнении команд: «**commit**», «**save**», «**reboot**», «**poweroff**».

Если требуется изменить время автоматической проверки **КЦ** – например, чтобы она выполнялась не в 00 минут каждого часа, а в другую минуту в пределах часа, – допускается указать желаемую минуту с помощью следующей команды в конфигурационном режиме:

```
set system integrity-control period <0-59>
```

где **<0-59>** – целочисленное значение минуты в пределах часа, в которую планируется запускать проверку. Возможно указать значение в диапазоне от «0» до «59». По умолчанию проверка контроля целостности запускается в 0-ю минуту каждого часа (например, 09:00, 10:00, 11:00 и т.д.).

Пример:

Команда «set system integrity-control period 10» устанавливает время запуска автоматической проверки КЦ на XX:10 (например, 09:10, 10:10, 11:10 и т.д.).

Ручной запуск проверки целостности осуществляется командой:

```
admin@ngfwos:~$ integrity-control run <path/to/file | all>
```

где:

- **<path/to/file>** - абсолютный путь к конкретному контролируемому файлу. При нажатии клавиши **Tab** система предоставляет автодополнение со списком всех объектов, находящихся под контролем **КЦ**;
- **<all>** - инициирует проверку целостности всех контролируемых объектов.

При успешном завершении проверки система выводит сообщение: «*Integrity is ok*».

Все события, связанные с функционированием механизма контроля целостности, включая действия администратора, регистрируются в глобальном журнале. Для просмотра этих событий применяется фильтр «**arma-endpoint**»:

```
admin@ngfwos:~$ show logging arma-endpoint
```

Настройка уровня логирования событий **КЦ** выполняется в конфигурационном режиме командой:

```
set system integrity-control log level <level>
```

где **<level>** – уровень детализации журналирования событий **КЦ**. Доступны следующие значения:

- **fatal** – фатальные ошибки;
- **error** – ошибки;
- **warning** – предупреждения;
- **info** – информационные сообщения (уровень по умолчанию);
- **debug** – отладочная информация;
- **trace** – максимально подробное трассировочное журналирование.

Примечание:

Изменение уровня логирования вступает в силу только после перезапуска службы контроля целостности, что возможно исключительно после перезагрузки всего устройства.

При задании уровня логирования записываются только события строго указанного уровня, без включения событий более высоких (более приоритетных) уровней.

Примечание:

Команды конфигурирования службы **КЦ** («set system integrity-control») и команда ручного пересчёта эталонных значений («integrity-control update») по умолчанию доступны только встроенной УЗ «**admin**».

5.5.1 Список контролируемых объектов КЦ

Для отображения списка объектов, подлежащих контролю целостности, используется команда:

```
admin@ngfwos:~$ show system integrity-control [notify | emergency | json]
```

Дополнительные параметры позволяют фильтровать вывод:

- **notify** - отображает объекты, при нарушении целостности которых система генерирует уведомление;

- **emergency** - отображает объекты, при нарушении целостности которых система переходит в аварийный режим;
- **json** - отображает полный список объектов в формате JSON.

Список объектов, контролируемых по умолчанию, приведён в [таблице «Список контролируемых объектов по умолчанию»](#).

Таблица «Список контролируемых объектов по умолчанию»

Действие	Объект
emergency	/config/config.boot
emergency	/opt/ngfwos/etc/config.boot.default
emergency	/opt/ngfwos/etc/config.boot.ssh_dhcp
emergency	/opt/ngfwos/etc/config.boot.ssh_dhcp_static_ips
notify	/boot/initrd.img
notify	/boot/initrd.img-6.6.54-amd64-ngfwos
notify	/boot/vmlinuz
notify	/boot/vmlinuz-6.6.54-amd64-ngfwos
notify	/etc/containers/containers.conf
notify	/etc/containers/registries.conf
notify	/etc/containers/storage.conf
notify	/etc/cron.d/integrity_check
notify	/etc/curlrc
notify	/etc/hosts
notify	/etc/iwarma-endpoint/emerg-files.txt
notify	/etc/iwarma-endpoint/general-config.yaml
notify	/etc/iwarma-endpoint/integrity-control-config.yaml
notify	/etc/logrotate.d/ngfwos-rsyslog
notify	/etc/modprobe.d/vyatta_nf_conntrack.conf
notify	/etc/motd
notify	/etc/nginx/sites-enabled/default
notify	/etc/nginx/sites-enabled/ngfw-web.conf
notify	/etc/nsswitch.conf
notify	/etc/resolv.conf
notify	/etc/rsyslog.d/00-ngfwos.conf

Действие	Объект
notify	/etc/ssh/ssh_config.d/91-ngfwos-ssh-client-options.conf
notify	/etc/systemd/journald.conf
notify	/etc/udev/rules.d/40-usb-autosuspend.rules
notify	/home/admin/.ssh/authorized_keys
notify	/usr/bin/
notify	/usr/bin/все файлы каталога
notify	/usr/lib/live/mount/persistence/boot/grub/grub.cfg.d/ngfwos-versions/имя_образа_системы.cfg
notify	/usr/sbin/
notify	/usr/sbin/все файлы каталога
notify	/usr/share/pam-configs/ngfwos_auth

Добавление объекта в список **КЦ** осуществляется с использованием конфигурационных команд в зависимости от требуемого действия при нарушении целостности:

- Для действия «уведомление» (**notify**):

```
set system integrity-control list notify path <path/to/file>
```

- Для действия «аварийный режим» (**emergency**):

```
set system integrity-control list emergency path <path/to/file>
```

где **<path/to/file>** – абсолютный путь к файлу или каталогу, который требуется включить в мониторинг **КЦ**.

Примечание:

При добавлении объектов в список контроля целостности в условиях высокой загрузки центрального процессора возможно нештатное завершение работы службы контроля целостности (**iwarma-endpoint**).

После выполнения команды добавления объектов рекомендуется убедиться в работоспособности службы контроля целостности. Для этого необходимо перейти в учётную запись суперпользователя:

```
admin@ngfwos:~$ sudo -i
root@ngfwos:~#
```

и проверить статус службы:

```
root@ngfwos:~# systemctl status iwarma-endpoint
```

В случае, если служба остановлена (статус «**inactive**» или «**failed**»), требуется её ручной запуск:

```
root@ngfwos:~# systemctl start iwarma-endpoint
```

После запуска необходимо повторно проверить статус службы. Пример корректного вывода при активном состоянии:

```
root@ngfwos:~# systemctl status iwarma-endpoint
• iwarma-endpoint.service - Infowatch ARMA EndPoint Linux
   Loaded: loaded (/lib/systemd/system/iwarma-endpoint.service; enabled;
   preset: enabled)
   Active: active (running) since Mon 2026-01-12 08:36:38 UTC; 2s ago
     Main PID: 513168 (endpointd)
        Tasks: 5 (limit: 13981)
       Memory: 4.4M
          CPU: 3.403s
      CGroup: /system.slice/iwarma-endpoint.service
              └─513168 /usr/sbin/endpointd

Jan      12      08:36:35      ngfwos      endpointd[513168]:
/home/admin/.ssh/authorized_keys
Jan 12 08:36:37 ngfwos endpointd[513168]: /usr/bin/
Jan      12      08:36:37      ngfwos      endpointd[513168]:
/usr/lib/live/mount/persistence/boot/grub/grub.cfg.d/ngfwos-versions/4.8.0-
1-g0a90>
Jan 12 08:36:38 ngfwos endpointd[513168]: /usr/sbin/
Jan 12 08:36:38 ngfwos endpointd[513168]: /usr/share/pam-
configs/ngfwos_auth
Jan 12 08:36:38 ngfwos endpointd[513168]: /config/config.boot
Jan      12      08:36:38      ngfwos      endpointd[513168]:
/opt/ngfwos/etc/config.boot.default
Jan      12      08:36:38      ngfwos      endpointd[513168]:
/opt/ngfwos/etc/config.boot.ssh_dhcp
Jan      12      08:36:38      ngfwos      endpointd[513168]:
/opt/ngfwos/etc/config.boot.ssh_dhcp_static_ips
Jan 12 08:36:38 ngfwos systemd[1]: Started iwarma-endpoint.service -
Infowatch ARMA EndPoint Linux.
lines 1-20/20 (END)
```

Удаление объекта из списка **КЦ** выполняется командой:

```
delete system integrity-control list notify path <path/to/file>
```

где **<path/to/file>** - абсолютный путь к файлу или каталогу, подлежащему исключению из мониторинга **КЦ**.

Примечание:

Система содержит предопределённый список объектов **КЦ** по умолчанию (см. [Таблица «Список контролируемых объектов по умолчанию»](#)). При обновлении программного обеспечения записи, входящие в этот исходный список, автоматически восстанавливаются в первоначальное состояние, даже если пользователь вносил в них изменения. Пользовательские объекты, добавленные дополнительно, сохраняются без изменений.

5.5.2 Регистрация событий КЦ

Верификация целостности объектов осуществляется путём сравнения текущего хэш-значения с эталонным, хранящимся в базе данных механизма **КЦ**.

В случае обнаружения несоответствия текущего хэш-значения объекта наблюдения эталонному значению в процессе функционирования системы **ARMA Стена**, система выведет предупреждающее сообщение и выполнит предусмотренные действия в отношении данного объекта: переход в аварийный режим (см. [Рисунок – Переход в аварийный режим при нарушении КЦ](#)) или вывод уведомления о нарушении целостности (см. [Рисунок – Предупреждение о нарушении КЦ](#))).

```
admin@ngfwos:~$  
Entering emergency state  
  
All network traffic was stopped
```

Рисунок – Переход в аварийный режим при нарушении КЦ

```
admin@ngfwos:~$  
Violation checking integrity of file, check logs for more information
```

Рисунок – Предупреждение о нарушении КЦ

Если при загрузке системы контролируемый объект не проходит проверку на целостность, то в зависимости от установленного для него действия (**notify** или **emergency**) после завершения загрузки система либо выводит предупреждение (см. [Рисунок – Не удалось выполнить проверку КЦ](#)), либо переходит в аварийный режим (см. [Рисунок – Аварийный режим. Не удалось выполнить проверку КЦ](#)).


```
Welcome to NGFWOS!

[ ]
[ ] NGFWOS 4.5.
[ ]

[ 58.340737] ngfwos-router[1153]: Error: integrity control check failed!
[ 58.341056] ngfwos-router[1153]: Your system might be compromised!
[ 58.341235] ngfwos-router[1153]: Check logs for details
admin@ngfwos:~$
```

Рисунок – Не удалось выполнить проверку КЦ

```
Starting systemd-update-utmp... Record Runlevel Change in UTMP...
[ OK ] Finished systemd-update-utmp - Record Runlevel Change in UTMP.
[ 55.751844] ngfwos-config[1047]: Configuration error

Welcome to NGFWOS - ngfwos tty1

ngfwos login: [ 55.804848] ngfwos-router[1621]: System was switched to emergency state caused by: Error loading config '/opt/vyatta/etc/config/config.boot'. Details: [[interfaces ethernet eth0]] failed
[ 55.805562] ngfwos-router[1621]: [[interfaces ethernet eth1]] failed
[ 55.805940] ngfwos-router[1621]: [[interfaces ethernet eth2]] failed
[ 55.806308] ngfwos-router[1621]: Commit failed
[ 56.276285] ngfwos-router[1044]: System is in emergency state
[ 56.276474] ngfwos-router[1044]: See logs & '/config/emergency_state' for more details
[ 56.276617] ngfwos-router[1044]: You can rollback to older config or load default
[ 56.276732] ngfwos-router[1044]: You can view errors with op-command 'emergency state reasons'
[ 56.276870] ngfwos-router[1044]: You can exit emergency state with op-command 'emergency exit'

Hint: Num Lock on

ngfwos login:
```

Рисунок – Аварийный режим. Не удалось выполнить проверку КЦ

Для идентификации объекта, не прошедшего проверку **КЦ**, в эксплуатационном режиме выполняется команда:

```
admin@ngfwos:~$ integrity-control run all
```

Пример вывода:

```
admin@ngfwos:~$ integrity-control run all

Violation checking integrity of file(s):
/usr/bin/apt
```

Данный вывод указывает на нарушение целостности файла «/usr/bin/apt».

Для проверки целостности конкретного объекта, входящего в список контролируемых, в эксплуатационном режиме используется команда:

```
admin@ngfwos:~$ integrity-control run <path/to/file>
```

где **<path/to/file>** – абсолютный путь к файлу или каталогу, подлежащему проверке.

5.5.3 Пересчёт эталонных значений КЦ

Пересчёт эталонных хэш-значений **КЦ** может выполняться автоматически или вручную.

Автоматический пересчёт

Осуществляется после выполнение команд: **«commit»**, **«save»**, **«load»**, **«rollback»**.

Примечание:

В аварийном режиме автоматический пересчёт не производится для команд **«commit»**, **«save»** и **«load»**.

Ручной пересчёт

Для пересчёта эталонных значений контроля целостности необходимо ввести команду:

```
admin@ngfwos:~$ integrity-control update <path/to/file | all>
```

где:

- **<path/to/file>** - путь к объекту, для которого требуется обновить эталонное значение;
- **<all>** - обновление эталонных значений для всех контролируемых объектов.

5.5.4 Диагностика и восстановление службы контроля целостности при загрузке

В случае невозможности запуска службы контроля целостности при загрузке системы **ARMA Стена** выводится одно из следующих предупреждающих сообщений в зависимости от состояния сервиса в systemd:

- Если systemd отметил сервис как **«failed»**:

Warning: failed to start integrity control service!

- Если systemd отметил сервис как **«dead»** (неактивен):

Warning: integrity control service is not running!

Сценарий 1: Сервис в состоянии failed

В этом случае рекомендуется выполнить следующие действия:

- Проверить журнал событий **КЦ** с помощью команды:

```
admin@ngfwos:~$ show logging arma-endpoint
```

- Если журнал не содержит диагностической информации, установить максимальный уровень детализации:

```
set system integrity-control log level trace  
commit  
save
```

- Перезагрузить систему - «**reboot**».
- После перезагрузки повторно проверить журнал событий.

На основании полученных данных либо устранить причину сбоя самостоятельно, либо обратиться в техническую поддержку **ООО «ИнфоВотч АРМА»**.

Сценарий 2: Сервис в состоянии dead

Для восстановления работоспособности службы необходимо выполнить следующие действия под встроенной учётной записью «**admin**»:

1. Получить права суперпользователя:

```
admin@ngfwos:~$ sudo -i
```

2. Включить службу в автозагрузку:

```
root@ngfwos:~# systemctl enable iwarma-endpoint
```

3. Запустить службу вручную:

```
root@ngfwos:~# systemctl start iwarma-endpoint
```

4. Проверить текущий статус службы:

```
root@ngfwos:~# systemctl status iwarma-endpoint
```

5. Если после выполнения указанных действий служба не переходит в активное состояние, требуется анализ системных журналов и, при необходимости, обращение в техническую поддержку.

6 УПРАВЛЕНИЕ ДОСТУПОМ

6.1 Аутентификация

Аутентификация – это процесс проверки подлинности введенных пользователем имени и пароля. В **ARMA Стена** возможна аутентификация с использованием локальной или внешней БД пользователей. Для хранения УЗ пользователей по умолчанию применяется локальная БД. В качестве внешней БД служат различные внешние серверы авторизации.

В системе **ARMA Стена** предусмотрена встроенная учётная запись «**admin**», обладающая правами суперпользователя и имеющая неограниченный доступ к системным функциям, включая выполнение команд с привилегиями `sudo`.

Использование данной учётной записи для повседневной административной деятельности не рекомендуется. В целях обеспечения повышенного уровня безопасности следует создать отдельную учётную запись администратора с необходимым набором прав.

6.2 Локальные учётные записи

6.2.1 Просмотр локальных учётных записей

Система **ARMA Стена** предоставляет команды для просмотра информации о локальных учётных записях, включая их статус, тип, класс, данные о последнем входе и другие атрибуты.

Просмотр пользовательских учётных записей

Для отображения списка пользовательских учётных записей, созданных в системе, используется команда:

```
admin@ngfwos:~$ show system login users ngfwos [json]
```

Username From	Full name Last login	Class	Type	Status
-----	-----	-----	-----	-----
admin		NGFW_Super_Administrators	ngfwos	Normal
192.168.21.2	Mon Aug 18 11:28:11 2025			
user1	test	Security_Engineers	ngfwos	Normal
172.16.14.9	Fri Aug 15 14:42:44 2025			
user2	test	Network_Administrators	ngfwos	Normal
172.16.14.25	Fri Aug 15 14:40:47 2025			
test1				

Опциональный параметр «json» позволяет вывести данные в формате JSON для программной обработки.

Формат вывода включает следующие поля:

- **Username** - имя учётной записи пользователя, использованное при аутентификации в системе.
- **Full name** - полное имя учётной записи пользователя.
- **Class** - класс учётной записи.
- **Type** - тип учётной записи.
- **Status** - состояние учётной записи на момент последнего входа.
Возможные значения:
 - **Normal** - учётная запись активна, ограничений нет;
 - **Temporarily locked** - учётная запись временно заблокирована вследствие превышения допустимого числа неудачных попыток аутентификации;
 - **Locked** - учётная запись заблокирована.
- **Tty** - идентификатор терминала или псевдотерминала, выделённого сессии пользователя. Допустимые значения:
 - **tty** - физические или виртуальные консоли (tty1–tty6), доступные при локальном подключении (KVM, serial-порт);
 - **pts/n** - псевдотерминалы, используемые для сетевых сессий (SSH);
 - **ttySn** - последовательные терминалы (при использовании последовательной консоли).
- **From** - IP-адрес хоста, с которого выполнен вход в систему.
- **Last login** - дата и время последней успешной аутентификации в формате: ДеньНедели Месяц День ЧЧ:ММ:СС ГГГГ, представленные по локальному времени системы.

Просмотр всех учётных записей в системе

Для отображения полного списка всех локальных учётных записей, включая системные и служебные, используется команда:

```
admin@ngfwos:~$ show system login users all [json]
```

Username	Full name	Class	Type
Status	From	Last login	

root		other
Locked	never logged in	
daemon		other
Locked	never logged in	
bin		other
Locked	never logged in	
sys		other
Locked	never logged in	
sync		other
Locked	never logged in	
games		other
Locked	never logged in	
man		other
Locked	never logged in	
lp		other
Locked	never logged in	
mail		other
Locked	never logged in	
news		other
Locked	never logged in	
uucp		other
Locked	never logged in	
proxy		other
Locked	never logged in	
www-data		other
Locked	never logged in	
backup		other
Locked	never logged in	
list		other
Locked	never logged in	
irc		other
Locked	never logged in	
_apt		other
Locked	never logged in	
nobody		other
Locked		
systemd-network		other
Locked	never logged in	
salt		other
Locked	never logged in	

telegraf		other
Locked	never logged in	
drweb		other
Locked	never logged in	
strongswan		other
Locked	never logged in	
arma-lc		other
Locked	never logged in	
zabbix		other
Locked	never logged in	
uuid		other
Locked	never logged in	
messagebus		other
Locked	never logged in	
tftp		other
Locked	never logged in	
tss		other
Locked	never logged in	
stunnel4		other
Locked	never logged in	
conservr		other
Locked	never logged in	
frr		other
Locked	never logged in	
ocserv		other
Locked	never logged in	
pdns		other
Locked	never logged in	
iperf3		other
Locked	never logged in	
_chrony		other
Locked	never logged in	
haproxy		other
Locked	never logged in	
Debian-snmp		other
Locked	never logged in	
_dnsmist		other
Locked	never logged in	
_lldpd		other
Locked	never logged in	
owamp		other
Locked	never logged in	

arpwatch		other
Locked	never logged in	
avahi		other
Locked	never logged in	
twamp		other
Locked	never logged in	
tcpdump		other
Locked	never logged in	
sshd		other
Locked	never logged in	
sstpc		other
Locked	never logged in	
polkitd		other
Locked	never logged in	
minion		other
Locked	never logged in	
openvpn		other
Locked	never logged in	
tacacs0		other
Locked	never logged in	
tacacs1		other
Locked	never logged in	
tacacs2		other
Locked	never logged in	
tacacs3		other
Locked	never logged in	
tacacs4		other
Locked	never logged in	
tacacs5		other
Locked	never logged in	
tacacs6		other
Locked	never logged in	
tacacs7		other
Locked	never logged in	
tacacs8		other
Locked	never logged in	
tacacs9		other
Locked	never logged in	
tacacs10		other
Locked	never logged in	
tacacs11		other
Locked	never logged in	

tacacs12					other
Locked			never logged in		
tacacs13					other
Locked			never logged in		
tacacs14					other
Locked			never logged in		
tacacs15					other
Locked			never logged in		
radius_user					other
Locked			never logged in		
radius_priv_user					other
Locked			never logged in		
dhcpd					other
Locked			never logged in		
admin				NGFW_Super_Administrators	ngfwos
Normal	192.168.21.2	Tue Aug 19 06:12:15 2025			
user1		test		Security_Engineers	ngfwos
Normal	172.16.20.9	Fri Aug 15 14:42:44 2025			
user2		test		Network_Administrators	ngfwos
Normal	172.16.20.9	Fri Aug 15 14:40:47 2025			
test				Network_Administrators	ngfwos
Locked	192.168.21.2	Tue Aug 19 06:23:53 2025			
test1					ngfwos
Normal					

Просмотр системных (служебных) учётных записей

Для фильтрации и отображения только технических учётных записей, используемых внутренними службами системы, применяется команда:

```
admin@ngfwos:~$ show system login users other [json]
```

Username	Full name	Class	Type	Status	From	Last login
root					other	Locked
never logged in						
daemon					other	Locked
never logged in						
bin					other	Locked
never logged in						
sys					other	Locked

never logged in sync			other	Locked
never logged in games			other	Locked
never logged in man			other	Locked
never logged in lp			other	Locked
never logged in mail			other	Locked
never logged in news			other	Locked
never logged in uucp			other	Locked
never logged in proxy			other	Locked
never logged in www-data			other	Locked
never logged in backup			other	Locked
never logged in list	other	Locked		never
logged in irc			other	Locked
never logged in _apt			other	Locked
never logged in nobody	other	Locked		
systemd-network			other	Locked
never logged in salt	other	Locked		never
logged in telegraf	other	Locked		never
logged in drweb			other	Locked
never logged in strongswan			other	Locked
never logged in arma-lc			other	Locked
never logged in zabbix			other	Locked
never logged in				

uidd		other	Locked
never logged in			
messagebus		other	Locked
never logged in			
tftp		other	Locked
never logged in			
tss		other	Locked
never logged in			
stunnel4		other	Locked
never logged in			
conservr		other	Locked
never logged in			
frr	other	Locked	never
logged in			
ocserv		other	Locked
never logged in			
pdns		other	Locked
never logged in			
iperf3		other	Locked
never logged in			
_chrony		other	Locked
never logged in			
haproxy		other	Locked
never logged in			
Debian-snmp		other	Locked
never logged in			
_dnsmasq		other	Locked
never logged in			
_lldpd		other	Locked
never logged in			
owamp		other	Locked
never logged in			
arpwatch		other	Locked
never logged in			
avahi		other	Locked
never logged in			
twamp		other	Locked
never logged in			
tcpdump		other	Locked
never logged in			
sshd		other	Locked
never logged in			

sstpc	other	Locked
never logged in		
polkitd	other	Locked
never logged in		
minion	other	Locked
never logged in		
openvpn	other	Locked
never logged in		
tacacs0	other	Locked
never logged in		
tacacs1	other	Locked
never logged in		
tacacs2	other	Locked
never logged in		
tacacs3	other	Locked
never logged in		
tacacs4	other	Locked
never logged in		
tacacs5	other	Locked
never logged in		
tacacs6	other	Locked
never logged in		
tacacs7	other	Locked
never logged in		
tacacs8	other	Locked
never logged in		
tacacs9	other	Locked
never logged in		
tacacs10	other	Locked
never logged in		
tacacs11	other	Locked
never logged in		
tacacs12	other	Locked
never logged in		
tacacs13	other	Locked
never logged in		
tacacs14	other	Locked
never logged in		
tacacs15	other	Locked
never logged in		
radius_user	other	Locked
logged in		never

radius_priv_user	other	Locked	never
logged in			
dhcpcd		other	Locked
never logged in			

Просмотр заблокированных учётных записей

Для отображения всех учётных записей, находящихся в состоянии блокировки, используется команда:

```
admin@ngfwos:~$ show system login users locked [json]
```

Username	Full name	Class	Type	Status	From	Last login
root					other	Locked
never logged in						
daemon					other	Locked
never logged in						
bin					other	Locked
never logged in						
sys					other	Locked
never logged in						
sync					other	Locked
never logged in						
games					other	Locked
never logged in						
man					other	Locked
never logged in						
lp					other	Locked
never logged in						
mail					other	Locked
never logged in						
news					other	Locked
never logged in						
uucp					other	Locked
never logged in						
proxy					other	Locked
never logged in						
www-data					other	Locked
never logged in						
backup					other	Locked

never logged in list		other	Locked
never logged in irc		other	Locked
never logged in _apt		other	Locked
never logged in nobody	other	Locked	
systemd-network		other	Locked
never logged in salt		other	Locked
never logged in telegraf		other	Locked
never logged in drweb		other	Locked
never logged in strongswan		other	Locked
never logged in arma-lc		other	Locked
never logged in zabbix		other	Locked
never logged in uuuid		other	Locked
never logged in messagebus		other	Locked
never logged in tftp		other	Locked
never logged in tss		other	Locked
never logged in stunnel4		other	Locked
never logged in conservr		other	Locked
never logged in frr		other	Locked
never logged in ocserv		other	Locked
never logged in pdns		other	Locked
never logged in iperf3		other	Locked
never logged in			

_chrony	other	Locked
never logged in		
haproxy	other	Locked
never logged in		
Debian-snmp	other	Locked
never logged in		
_dnsmist	other	Locked
never logged in		
_lldpd	other	Locked
never logged in		
owamp	other	Locked
never logged in		
arpwatch	other	Locked
never logged in		
avahi	other	Locked
never logged in		
twamp	other	Locked
never logged in		
tcpdump	other	Locked
never logged in		
sshd	other	Locked
never logged in		
sstpc	other	Locked
never logged in		
polkitd	other	Locked
never logged in		
minion	other	Locked
never logged in		
openvpn	other	Locked
never logged in		
tacacs0	other	Locked
never logged in		
tacacs1	other	Locked
never logged in		
tacacs2	other	Locked
never logged in		
tacacs3	other	Locked
never logged in		
tacacs4	other	Locked
never logged in		
tacacs5	other	Locked
never logged in		

tacacs6	other	Locked	
never logged in			
tacacs7	other	Locked	
never logged in			
tacacs8	other	Locked	
never logged in			
tacacs9	other	Locked	
never logged in			
tacacs10	other	Locked	
never logged in			
tacacs11	other	Locked	
never logged in			
tacacs12	other	Locked	
never logged in			
tacacs13	other	Locked	
never logged in			
tacacs14	other	Locked	
never logged in			
tacacs15	other	Locked	
never logged in			
radius_user	other	Locked	
never logged in			
radius_priv_user	other	Locked	never
logged in			
dhcpd	other	Locked	
never logged in			
test	Network_Administrators	ngfwos	Locked 192.168.2.2 Tue
Aug 19 06:23:53 2025			

6.2.2 Добавление пользовательских учётных записей

Для создания локальной учётной записи в системе необходимо выполнить следующую последовательность команд в режиме конфигурирования:

```
set system login user <user> full-name <text>
set system login user <user> authentication plaintext-password <password>
commit
save
```

где:

- **<user>** – имя пользователя (логин), используемое для аутентификации. Допустимые символы: буквы латинского алфавита (a–z, A–Z), цифры (0–

9), а также символы подчёркивания («_»), дефис («-») и точка («.»). Максимальная длина - «32» символа;

- **<text>** – отображаемое (полное) имя пользователя. Максимальная длина – «70» символов. В случае наличия пробелов значение должно быть заключено в двойные кавычки (например, "Иванов Иван"). Использование символа двоеточия («:») запрещено.
- **<password>** – пароль учётной записи в открытом виде. Допустимый набор символов включает:
 - латинские буквы (a–z, A–Z);
 - цифры (0–9);
 - специальные символы: «(», «)», «!», «#», «%», «*», «+», «,», «.», «/», «:», «;», «&», «>», «<», «_», «=», «@», «[», «]», «^», «{», «}», «|», «~», «\$», «`».

Примечание:

В случае, если в системе настроена политика паролей, требования к значению пароля применяются в соответствии с параметрами данной политики.

При создании учётной записи без указания пароля она автоматически переводится в заблокированное состояние и остаётся недоступной для входа. Блокировка снимается автоматически после назначения пароля.

Для просмотра конфигурации учётных записей необходимо выполнить следующую команду в конфигурационном режиме:

```
show system login user
```

#Пример вывода команды:

```
user admin {
    authentication {
        encrypted-password $6$rounds=6560...30
    }
    class NGFW_Super_Administrators
}
user test {
    authentication {
        encrypted-password $6$rounds=6560...j1
    }
}
```

Команда отображает полную конфигурацию всех учётных записей пользователей, включая зашифрованные пароли и назначенные классы.

6.2.3 Политика паролей учётных записей

Команды конфигурации политики паролей УЗ:

1. Указать максимальную длину пароля:

```
set system login password maximum-length <max>
```

где **<max>** - значение максимальной длины пароля. Возможно указать значение в диапазоне от «1» до «128». По умолчанию используется значение «128».

2. Указать минимальную длину пароля:

```
set system login password minimum-length <min>
```

где **<min>** - значение минимальной длины пароля. Возможно указать значение в диапазоне от «1» до «64». По умолчанию используется значение «1».

3. Указать минимальное количество цифр в пароле:

```
set system login password minimum-numeric <number>
```

где **<number>** - количество цифр в пароле. Возможно указать значение в диапазоне от «1» до «32». По умолчанию используется значение «0».

4. Указать минимальное количество специальных символов в пароле:

```
set system login password minimum-special <number>
```

где **<number>** - количество специальных символов. Возможно указать значение в диапазоне от «1» до «32». По умолчанию используется значение «0».

В пароле допускается использовать следующие специальные символы: «!», «#», «%», «&», «(», «)», «*», «+», «,», «.», «/», «:», «;», «<», «=», «>», «@», «[», «]», «^», «_», «{», «|», «}», «~», «`», «\$».

5. Указать минимальное количество букв в нижнем регистре в пароле:

```
set system login password minimum-lower-case <number>
```

где **<number>** - количество букв в нижнем регистре. Возможно указать значение в диапазоне от «1» до «32». По умолчанию используется значение «0».

6. Указать минимальное количество букв в верхнем регистре в пароле:

```
set system login password minimum-upper-case <number>
```

где **<number>** - количество букв в верхнем регистре. Возможно указать значение в диапазоне от «1» до «32». По умолчанию используется значение «0».

6.2.4 Временная блокировка учётных записей

Система **ARMA Стена** поддерживает механизм временной блокировки учётных записей в случае превышения допустимого количества неудачных попыток аутентификации. Настройки применяются ко всем локальным учётным записям и действуют при аутентификации через локальный вход или SSH.

Примечание:

Механизмы временной блокировки учётной записи в системе **ARMA Стена** не распространяются на пользователей с правами «NGFW_Super_Administrators».

Настройка количества попыток ввода пароля до блокировки

Для задания максимального числа неудачных попыток аутентификации перед блокировкой учётной записи используется команда:

```
set system login retry-options attemps-before-block <number>
```

где **<number>** - целочисленное значение в диапазоне от «1» до «100», определяющее количество допустимых неудачных попыток ввода пароля. Значение по умолчанию: «5» попыток.

Примечание:

Для повышения безопасности и снижения эффективности брутфорс-атак рекомендуется ограничить количество попыток ввода пароля для учётных записей пользователей.

Настройка продолжительности временной блокировки

Время блокировки после превышения лимита попыток устанавливается следующими командами:

```
set system login retry-options lockout-period seconds <sec>  
set system login retry-options lockout-period minutes <min>  
set system login retry-options lockout-period hours <hour>
```

где:

- **<sec>** - количество секунд. Возможно указать значение в диапазоне от «0» до «60»;
- **<min>** - количество минут. Возможно указать значение в диапазоне от «0» до «60»;

- **<hour>** - количество часов. Возможно указать значение в диапазоне от «0» до «168».

Общая длительность блокировки вычисляется как сумма всех активных компонентов: секунд, минут и часов. Максимально возможная длительность временной блокировки пользователя - 168 часов. По умолчанию учётная запись блокируется на 10 минут.

Примечание:

Настройки временной блокировки учётной записи в системе **ARMA Стена** действуют независимо от используемого метода аутентификации.

Разблокировка временно заблокированных учётных записей

Примечание:

Разблокировка может быть выполнена только пользователями с правами **«NGFW_Super_Administrators»**. Пользователь с правами **«NGFW_Super_Administrators»** может выдать права на использование команды для разблокировки временно заблокированных учётных записей другому классу пользователей с помощью следующей команды конфигурационного режима:

```
set system login class <class> operational-command 'clear lock'
```

Для отображения пользователей, находящихся в состоянии временной блокировки, используется команда:

```
admin@ngfwos:~$ show lock <users | ip | all>
```

где:

- **<users>** - список временно заблокированных пользователей (ssh-сессий);
- **<ip>** - список временно заблокированных IP-адресов (веб-сессий);
- **<all>** - список временно заблокированных пользователей и IP-адресов.

Пример работы команды show lock all:

```
admin@ngfwos:~$ show lock all
User name      Ip address      Ban time      Unban time
Remaining
-----
-
-              192.168.1.249  2025-10-16 09:26:37  2025-10-16 09:36:37
0:09:54
svs            -              2025-10-16 08:54:38  2025-10-16 10:04:38
0:37:55
```

Для разблокировки временно заблокированных учётных записей по имени пользователя используется команда:

```
admin@ngfwos:~$ clear lock user <user_name>
```

где **<user_name>** - имя пользователя, которого необходимо разблокировать.

Для разблокировки временно заблокированных IP-адресов используется команда:

```
admin@ngfwos:~$ clear lock user <ip-address>
```

где **<ip-address>** - IP-адрес, который необходимо разблокировать.

6.2.5 Назначение прав доступа пользовательским учётным записям

Для ограничения прав пользовательских учётных записей используются классы.

Класс представляет собой перечень разрешённых команд для использования в **ARMA Стена**.

В системе **ARMA Стена** по умолчанию предусмотрено четыре класса (см. [Таблица «Список классов по умолчанию»](#)).

Таблица «Список классов по умолчанию»

Класс	Описание	Список разрешённых команд
NGFW_Super_Administrators	Специальный класс для встроенной УЗ admin	ЭКСПЛУАТАЦИОННЫЙ РЕЖИМ: - полный доступ. КОНФИГУРАЦИОННЫЙ РЕЖИМ: - полный доступ.
NGFW_Administrators	Группа администраторов с полными правами	ЭКСПЛУАТАЦИОННЫЙ РЕЖИМ: - полный доступ, за исключением: - команды разблокировки УЗ и IP-адресов -

Класс	Описание	Список разрешённых команд
		<i>clear lock;</i> - команды пересчёта эталонных значений контроля целостности - <i>integrity-control update.</i> КОНФИГУРАЦИОННЫЙ РЕЖИМ: - полный доступ, за исключением: - команда редактирования - <i>edit;</i> - команда выключения блокировки сетевых интерфейсов в аварийном режиме - <i>set system option emergency remove-nics;</i> - команды конфигурирования службы контроля целостности - <i>set system integrity-control;</i> - команды конфигурирования VRRP - <i>set high-availability;</i>

Класс	Описание	Список разрешённых команд
		- команды конфигурирования службы балансировки нагрузки на WAN-интерфейсах - <i>set load-balancing;</i> - команды настройки планировщика задач - <i>set system task-scheduler.</i>
Network_Administrators	Группа администраторов сети	ЭКСПЛУАТАЦИОННЫЙ РЕЖИМ: - clear - console - dhcp-server - dns - flow-accounting - interfaces - ip - ipv6 - logging - session - force - arp - ipv6-nd - ipv6-rd - mtu - ntp - openconnect-server - owping

Класс	Описание	Список разрешённых команд
		• twping • vrf • generate • interfaces • ipsec • macsec • openconnect • openvpn • pki • public-key-command • ssh • system • tech-support • wireguard • import • monitor • mtr • ping • poweroff • reboot • release • renew • reset • restart • set • pppoe-server • show • arp • babel

Класс	Описание	Список разрешённых команд
		• bfd • bgp • bridge • conntrack • conntrack-sync • date • dhcp • dhcpv6 • dns • evpn • host • interfaces • ip • ipoe-server • ipv6 • isis • l2tp-server • lldp • logging ○ conntrack-sync ○ dhcp ○ dhcpv6 ○ dns ○ https ○ ipoe-server ○ lldp ○ nat ○ ntp

Класс	Описание	Список разрешённых команд
		○ pppoe ○ pppoe-server ○ snmp ○ ssh ○ vpn ○ vrrp ○ webproxy • monitoring • mpls • nat • nat66 • nhrp • ntp • openconnect-server • openvpn • permissions current • pki • policy • poweroff • pppoe-server • pptp-server • protocols • reboot • reverse-proxy • route-map • rpki • segment-routing • sflow

Класс	Описание	Список разрешённых команд
		• snmp • ssh • sstp-server • table • tech-support • version • vpn • vrf • vrrp • wan-load-balance • webproxy • zebra • telnet • traceroute • update • wake-on-lan КОНФИГУРАЦИОННЫЙ РЕЖИМ: • comment • copy/delete/rename/set/show • high-availability • interfaces • load-balancing • nat • nat64 • nat66 • pki • policy • protocols • qos • service

Класс	Описание	Список разрешённых команд
		○ active-sync-proxy ○ broadcast-relay ○ dhcp-relay ○ dhcp-server ○ dhcpv6-relay ○ dhcpv6-server ○ dns ○ event-handler ○ ipoe-server ○ lldp ○ mdns ○ ndp-proxy ○ ntp ○ pppoe-server ○ router-advert ○ snmp ○ ssh ○ stunnel ○ tftp-server

Класс	Описание	Список разрешённых команд
		○ webproxy • system ○ contract ○ flow-accounting ○ frr ○ ip ○ ipv6 ○ logging ○ name-server ○ proxy ○ sflow ○ static-host-mapping • third-party • vpn • vrf
Security_Engineers	Группа инженеров безопасности	ЭКСПЛУАТАЦИОННЫЙ РЕЖИМ: • generate • firewall • monitor • ping • poweroff • reboot • show • date • conntrack

Класс	Описание	Список разрешённых команд
		• firewall • flow-accounting • host • interfaces • logging ○ firewall ○ idps ○ nat • nat • nat66 • permissions current • pki • poweroff • reboot • tech-support • version • suricata • telnet • traceroute • update КОНФИГУРАЦИОННЫЙ РЕЖИМ: • comment • copy/delete/rename/set/show • nat • nat64 • nat66 • pki • service ○ event-handler

Класс	Описание	Список разрешённых команд
		○ ids ● suricata ● system ○ conntrack ○ logging ● set app-control ● show app-control

Примечание:

Класс пользователя «**NGFW_Super_Administrators**» предназначен исключительно для встроенной учётной записи «**admin**». Добавление других учётных записей в этот класс не допускается.

Класс пользователя «**NGFW_Super_Administrators**» не может быть изменён или удалён.

Для настройки классов необходимо ввести следующую команду в конфигурационном режиме:

```
set system login class <name_class> <operational-command | configure-command> <team>
```

где:

- **<name_class>** - уникальное имя класса;
- **<operational-command>** - установка прав на использование команд в эксплуатационном режиме;
- **<configure-command>** - установка прав на использование команд в конфигурационном режиме;
- **<team>** - разрешённая команда.

Для добавления описания класса следует ввести команду:

```
set system login class <name_class> description <text>
```

где **<text>** - текстовое описание класса. Описание не должно превышать «255» символов. Если описание содержит пробелы или символ «#», то его необходимо заключить в двойные кавычки.

Для добавления класса к учётной записи пользователя необходимо ввести команду:

```
set system login user <name_user> class <name_class>
```

где **<name_user>** - имя учётной записи пользователя.

Для каждой учётной записи пользователя возможно назначить только один класс.

Для просмотра списка разрешённых команд для класса необходимо в режиме конфигурации ввести команду:

```
show system login class [name_class] [operational-command | configure-command]
```

Для просмотра списка разрешённых команд для текущей учётной записи необходимо в эксплуатационном режиме ввести команду:

```
admin@ngfwos:~$ show permissions
```

Пример вывода списка разрешённых команд для учётной записи test:

```
test@ngfwos:~$ show permissions
```

```
=====
Current user permissions
=====
```

Configuration commands

```
commit
commit-check
commit-confirm
confirm
discard
exit
run configure
run exit
run show permissions
save
```

Operational commands

```
configure
exit
show permissions
```



```
=====
test@ngfwos:~$
```

Примечание:

Встроенной учётной записи «**admin**» запрещено изменять класс, удалять или отключать её.

Примечание:

При отсутствии назначенного класса доступа или наличии класса с пустым набором разрешённых команд, пользователь получает доступ к минимальному набору команд. Данный механизм обеспечивает необходимый минимум функционала для взаимодействия с системой в условиях отсутствия явных прав доступа.

Список разрешённых команд в **эксплуатационном режиме**:

- **configure** - войти в режим настройки;
- **show permissions** - вывести список разрешённых команд для данной УЗ;
- **exit** - выйти из системы.

Список разрешённых команд в **конфигурационном режиме**:

- **commit** - зафиксировать текущий набор изменений;
- **commit-check** - команда, предназначенная для анализа текущих конфигурационных изменений с целью выявления потенциальных ошибок или противоречий перед их фактическим применением;
- **commit-confirm** - зафиксировать текущий набор изменений с обязательным «подтверждением»;
- **confirm** - подтвердить предыдущую фиксацию - подтвердить;
- **discard** - отменить незафиксированные изменения;
- **exit** - выход с этого уровня конфигурации;
- **run configure** - выполнить команду эксплуатационного режима **configure**;
- **run exit** - выполнить команду эксплуатационного режима **exit**;
- **run show permissions** - выполнить команду эксплуатационного режима **show permissions**;
- **save** - сохранить конфигурацию в файл.

Пример настройки прав учётной записи пользователя

В качестве примера приведён список команд для создания учётной записи «test» с паролем «Password» и разрешением прав на использование команд: «ping», «set service dns», «delete service dns», «show service dns».

```
set system login user test authentication plaintext-password Password
set system login class c_dns
set system login class c_dns operational-command ping
set system login class c_dns operational-command configure
set system login class c_dns configure-command "set service dns"
set system login class c_dns configure-command "delete service dns"
set system login class c_dns configure-command "show service dns"
set system login user test class c_dns
commit
save
```

6.2.6 Тайм-аут пользовательской сессии

Для настройки периода бездействия, по истечении которого автоматически завершается сеанс локальной учётной записи, необходимо ввести в конфигурационном режиме следующую команду:

```
set system login timeout <time>
```

где **<time>** - значение тайм-аута в секундах. Возможно указание значения в диапазоне от «5» до «604800» (7 суток). По истечении указанного интервала неактивности сеанс пользователя автоматически завершается. Отсчёт времени начинается с момента выполнения последней команды.

Примечание:

На сессии, активные на момент применения данной конфигурации, новое значение тайм-аута не распространяется.

6.2.7 Блокировка пользователя

Система **ARMA Стена** поддерживает функцию блокирования локальных учётных записей с сохранением их конфигурационных параметров. Блокировка может быть выполнена немедленно или запланирована на заданное время, а также может быть ограничена определённым временным интервалом.

Немедленная блокирования УЗ

Для немедленного блокирования учётной записи используется команда:

```
set system login user <username> disable
commit
save
```

где **<username>** – имя блокируемой учётной записи.

Отложенная блокировка УЗ

Для активации блокировки учётной записи в заданное время применяется команда:

```
set system login user <username> lockout startdate "YYYY-MM-DD HH:MM"  
commit  
save
```

где **YYYY-MM-DD HH:MM** – дата и время начала блокировки в формате год-месяц-день часы:минуты, указываются в двойных кавычках.

Пример: блокировка учётной записи «test», запланированная на 15 августа 2025 года, с момента 00:00:

```
set system login user test lockout startdate "2025-08-15 00:00"  
commit  
save
```

После наступления указанного времени доступ по данной учётной записи будет заблокирован.

Блокировка УЗ на заданный временной интервал

Для временной блокировки учётной записи в указанный период используются следующие команды:

```
set system login user <username> lockout startdate "YYYY-MM-DD HH:MM"  
set system login user <username> lockout stopdate "YYYY-MM-DD HH:MM"  
commit  
save
```

где:

- **startdate "YYYY-MM-DD HH:MM"** – дата и время начала блокировки;
- **stopdate "YYYY-MM-DD HH:MM"** – дата и время окончания блокировки.

По истечении указанного периода учётная запись автоматически разблокируется.

При одновременном наличии параметров **disable** и **lockout** для одной учётной записи приоритет отдаётся состоянию, заданному параметром **disable**. Таким образом, если УЗ явно отключена с помощью параметра **disable**, она остаётся заблокированной независимо от настроек временной блокировки через **lockout**.

Автоматическая разблокировка по достижению времени **stopdate** не выполняется, пока активна постоянная блокировка, установленная через **disable**.

Примечание:

После применения блокировки учётной записи пользователь не сможет выполнить новый вход в систему. Однако, если пользователь уже авторизован и имеет одну или несколько активных сессий на момент активации блокировки, данные сессии не прерываются автоматически.

Пользователь сохраняет возможность продолжать работу в рамках существующих сессий до их естественного завершения (например, выхода из системы, истечения времени неактивности или ручного завершения сессии администратором).

Для немедленного прекращения доступа заблокированного пользователя необходимо вручную завершить его активные сессии (см. раздел [Управление пользовательскими сессиями](#)).

6.2.8 Управление пользовательскими сессиями

Данный раздел описывает процедуры просмотра и принудительного завершения активных пользовательских сессий в системе **ARMA Стена**, включая сессии в стандартной и последовательной консоли, а также сессии, установленные по протоколу SSH. Сессии пользователей, подключённых через веб-интерфейс, не отслеживаются.

Просмотр списка активных сессий

Для отображения списка активных пользовательских сессий используется команда:

```
admin@ngfwos:~$ show users sessions
```

Пример вывода:

SESSION	UID	USER	SEAT	TTY
12177	1002	admin	pts/0	
12178	1002	admin		
12203	1053	test	pts/1	
12205	1053	test		

Предусмотрен вывод в формате JSON:

```
admin@ngfwos:~$ show users sessions json
[{'session': '12177', 'uid': 1002, 'user': 'admin', 'seat': '', 'tty': 'pts/0'}, {'session': '12178', 'uid': 1002, 'user': 'admin', 'seat': '', 'tty': ''}, {'session': '12203', 'uid': 1053, 'user': 'test', 'seat': '', 'tty': 'pts/1'}, {'session': '12205', 'uid': 1053, 'user': 'test', 'seat': '', 'tty': ''}]
```

Примечание:

Сессии без указанного значения в поле ТТУ являются фоновыми и, как правило, используются системными службами (например, cron и другими демонами). Такие сессии не связаны с интерактивным входом пользователя.

Завершение пользовательской сессии.

Для завершения текущей сессии пользователя в эксплуатационном режиме следует выполнить команду:

```
admin@ngfwos:~$ exit
```

Принудительное завершение сессий

Система поддерживает принудительное завершение сессий по идентификатору сессии или по имени пользователя.

Завершение сессии по идентификатору

Для завершения конкретной сессии по её идентификатору используется команда:

```
admin@ngfwos:~$ reset sessions id <session>
```

где **<session>** – числовой идентификатор сессии (значение из поля SESSION).

Завершение всех сессий пользователя

Для завершения всех активных сессий указанного пользователя используется команда:

```
admin@ngfwos:~$ reset sessions username <username>
```

где **<username>** – имя пользователя, все сессии которого подлежат завершению.

Команда завершает все активные сессии, включая интерактивные и фоновые, ассоциированные с указанным пользователем.

Просмотр недавних сеансов входа

Для отображения списка пользователей, недавно выполнивших вход в систему **ARMA Стена**, используется команда:

```
admin@ngfwos:~$ show users recent [number]
```

где **<number>** – необязательный параметр, указывающий количество выводимых записей. Значение параметра – целое положительное число. Если параметр [number] не указан, по умолчанию выводится 10 последних записей.

Записи отображаются в порядке убывания времени входа (начиная с самой последней).

Пример вывода списка сессий:

```
admin@ngfwos:~$ show users recent
test      pts/1      Tue Aug 19 06:23:53 2025 - Tue Aug 19 07:24:56 2025
(01:01)    192.168.21.2
admin     pts/0      Tue Aug 19 06:12:15 2025      still logged in
192.168.21.2
admin     pts/0      Mon Aug 18 11:28:11 2025 - Tue Aug 19 06:12:00 2025
(18:43)    192.168.21.2
admin     pts/0      Mon Aug 18 10:19:51 2025 - Mon Aug 18 10:20:17 2025
(00:00)    192.168.21.2
admin     pts/0      Mon Aug 18 10:17:23 2025 - Mon Aug 18 10:18:59 2025
(00:01)    192.168.21.2
admin     pts/0      Mon Aug 18 06:01:23 2025 - Mon Aug 18 09:54:02 2025
(03:52)    172.16.10.9
user1     pts/1      Fri Aug 15 14:42:44 2025 - Fri Aug 15 14:43:14 2025 (00:00)
172.16.10.9
user3     pts/4      Fri Aug 15 14:42:19 2025 - Fri Aug 15 14:45:41 2025 (00:03)
172.16.10.9
user2     pts/3      Fri Aug 15 14:40:47 2025 - Fri Aug 15 14:44:51 2025 (00:04)
172.16.10.9
user4     pts/2      Fri Aug 15 14:30:39 2025 - Fri Aug 15 16:43:44 2025 (02:13)
172.16.10.9
```

6.3 Аутентификация RADIUS

RADIUS (Remote Authentication Dial-In User Service) – это сетевой протокол, который обеспечивает централизованную аутентификацию, авторизацию и учёт пользователей.

Система **ARMA Стена** поддерживает RADIUS-серверы в качестве серверной части для пользовательской аутентификации.

Атрибут «**cisco-avpair = shell:priv-lvl**» в **Radius**-сервере предназначен для определения уровня привилегий учётных записей. В системе **ARMA Стена** реализованы два уровня доступа для учётных записей **Radius**-сервера:

- **Полный доступ (priv-lvl=15)** - предоставляет разрешение на выполнение всех команд системы, за исключением команды «**sudo**».
- **Ограниченный доступ (priv-lvl=0-14)** - предоставляет разрешение на выполнение ограниченного набора команд, представленных [таблице](#)

«Список разрешённых команд для УЗ RADIUS-сервера с ограниченным доступом»).

Таблица «Список разрешённых команд для УЗ RADIUS-сервера с ограниченным доступом»

Режим работы	Команда	Краткое описание
Эксплуатационный	exit	Выход из системы
Эксплуатационный	monitor	Мониторинг системной информации
Эксплуатационный	ping	Отправить запрос эха ICMP
Эксплуатационный	show	Просмотр настроек и журнала событий системы
Эксплуатационный	telnet	Telnet к узлу
Эксплуатационный	traceroute	Трассировка сетевого пути к узлу

Перед началом настройки внешнего **Radius**-сервера необходимо убедиться в наличии сетевого доступа к данному серверу.

Примечание:

При обнаружении идентичных учётных записей в локальной базе данных пользователей и в **Radius**-сервере, система **ARMA Стена** осуществляет аутентификацию посредством локальной учётной записи.

6.3.1 Добавление внешнего Radius-сервера

Для добавления внешнего **Radius**-сервера необходимо выполнить следующие настройки:

1. Указать IP-адрес **Radius**-сервера и общий ключ, который используется для шифрования обмена данными между **ARMA Стена** и **Radius**-сервером:

```
set system login radius server <address> key <secret>
```

где:

- **<address>** - IP-адрес Radius-сервера в формате <x.x.x.x> для IPv4 или <h:h:h:h:h:h:h> для IPv6;
- **<secret>** - значение ключа, который используется для шифрования.

2. Указать порт, через который будет осуществляться доступ к **Radius**-серверу:

```
set system login radius server <address> port <port>
```

где **<port>** - номер порта. Возможно указать значение в диапазоне от «1» до «65535». По умолчанию используется порт «1812».

6.3.2 Дополнительные команды настройки Radius-сервера

- Указать приоритет **Radius**-серверу:

```
set system login radius server <address> priority <1-255>
```

где **<1-255>** - номер приоритета для указанного Radius-сервера. Возможно указать значение в диапазоне от «1» до «255». По умолчанию используется значение «255». Чем ниже число, тем выше приоритет сервера.

Используется для определения порядка обращения к Radius-серверам при аутентификации.

- Установить время ожидания для получения ответа от **Radius**-сервера:

```
set system login radius server <address> timeout <timeout>
```

где **<timeout>** - время ожидания в секундах. Возможно указать значение в диапазоне от «1» до «50». По умолчанию используется значение «2».

Определяет, как долго **ARMA Стена** будет ожидать ответа от Radius-сервера. Помогает предотвратить зависание системы при недоступности сервера. При отсутствии ответа в течение заданного времени система перейдёт к локальной аутентификации или к другим настроенным Radius-серверам.

При настройке тайм-аута необходимо определить значение, которое обеспечит оптимальное соотношение между скоростью проверки подлинности и безопасностью. Слишком малое значение тайм-аута может привести к ложным отказам при нормальной работе сети, а слишком большое – к замедлению процесса аутентификации.

- Временно отключить указанный **Radius**-сервера:

```
set system login radius server <address> disable
```

Команда временно отключает указанный Radius-сервер, в результате чего система перестаёт обращаться к нему при попытке аутентификации пользователей. Для отмены отключения сервера необходимо удалить данную настройку через команду «delete».

- Установить IP-адрес источника, с которого будут отправляться запросы к **Radius**-серверам:

```
set system login radius source-address <address>
```

где **<address>** – IP-адрес источника в формате <x.x.x.x> для IPv4 или <h:h:h:h:h:h> для IPv6.

Команда задаёт фиксированный IP-адрес, с которого **ARMA Стена** будет отправлять запросы ко всем настроенным Radius-серверам. Это особенно важно в случаях, когда Radius-серверы ограничивают доступ только с определённых IP-адресов.

- Определить режим безопасности для аутентификации Radius:

```
set system login radius security-mode optional
```

где **optional** - режим, при котором осуществляется первичная попытка аутентификации через Radius-сервер, а при неудаче производится попытка локальной аутентификации. Доступ к устройству сохраняется при недоступности Radius-сервера. Режим «**optional**» предоставляет баланс между безопасностью и доступностью, но требует дополнительного администрирования. Используется по умолчанию.

- Указать виртуальную сеть (VRF), через которую будет осуществляться подключение к **Radius**-серверу:

```
set system login radius vrf <vrf>
```

где **<vrf>** - имя виртуальной сети vrf.

Команда используется для указания, что все подключения к Radius-серверам должны исходить из указанной виртуальной сети (vrf). Это позволяет изолировать трафик аутентификации RADIUS в определённой виртуальной сети, что может быть полезно в сложных сетевых конфигурациях, где требуется сегментация трафика.

6.4 Multifactor Radius Adapter

ARMA Стена предоставляет возможность проводить аутентификацию пользователей на удалённом **Radius**-сервере. В данном примере в качестве **Radius**-сервера будет использоваться **Multifactor Radius Adapter**, который доступен в двух версиях: для Windows и для Linux.

6.4.1 Multifactor Radius Adapter - Windows

В качестве примера настройки Multifactor Radius Adapter для Windows будет использоваться стенд, представленный на рисунке (см. [Рисунок – Схема стенда для настройки Multifactor Radius Adapter - Windows](#)).

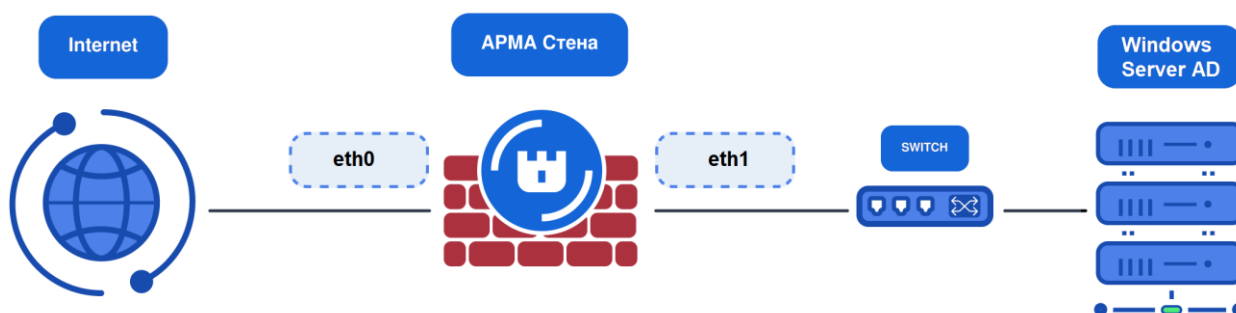


Рисунок – Схема стенда для настройки Multifactor Radius Adapter - Windows

Для получения доступа необходимо выполнить следующие шаги:

1. Настроить **ARMA Стена**.
2. Настроить Windows Server.
3. Проверка работы службы.

6.4.1.1 Настройка ARMA Стена

6.4.1.1.1 Настройка интерфейсов

На первом шаге необходимо предоставить **ARMA Стена** доступ к интернету. Для этого требуется подключить интерфейс «eth0» к корпоративной сети, назначить ему IP-адрес вручную или через DHCP-сервер и присвоить описание «WAN»:

```
set interfaces ethernet eth0 address <x.x.x.x/x | dhcp>
set interfaces ethernet eth0 description "WAN"
commit
save
```

Далее необходимо назначить интерфейсу «eth1», направленному в локальную подсеть, IP-адрес и присвоить ему описание «LAN»:

```
set interfaces ethernet eth1 address 192.168.1.1/24
set interfaces ethernet eth1 description "LAN"
commit
save
```

Для просмотра информации о настройках интерфейсов необходимо ввести следующую команду в эксплуатационном режиме (см. [Рисунок – Назначенные IP-адреса интерфейсам LAN и WAN](#)):

```
admin@ngfwos:~$ show interfaces
```

```
admin@ngfwos:~$ show interfaces
Codes: S - State, L - Link, u - Up, D - Down, A - Admin Down
Interface      IP Address      MAC              VRF      MTU    S/L    Descrip
tion
-----
eth0            172.16.230.95/24 00:50:56:bd:6b:29 default  1500   u/u    WAN
eth1            192.168.1.1/24   00:50:56:bd:6b:9a default  1500   u/u    LAN
lo              127.0.0.1/8      00:00:00:00:00:00 default  65536  u/u
```

Рисунок – Назначенные IP-адреса интерфейсам LAN и WAN

6.4.1.1.2 Настройка DHCP-сервера

Необходимо настроить DHCP-сервер на интерфейсе «eth1» для автоматической выдачи адресов устройствам в локальной сети:

```
set service dhcp-server shared-network-name LAN subnet 192.168.1.0/24 default-
router 192.168.1.1
set service dhcp-server shared-network-name LAN subnet 192.168.1.0/24 name-
server 192.168.1.1
set service dhcp-server shared-network-name LAN subnet 192.168.1.0/24 lease
86400
set service dhcp-server shared-network-name LAN subnet 192.168.1.0/24 range 0
start 192.168.1.100
set service dhcp-server shared-network-name LAN subnet 192.168.1.0/24 range 0
stop 192.168.1.150
commit
save
```

где:

- **LAN** - имя пула;
- **192.168.1.1** - IP-адрес шлюза по умолчанию;
- **86400** - время аренды IP-адресов в секундах;
- **192.168.1.100** - начальный IP-адрес пула адресов;
- **192.168.1.150** - конечный IP-адрес пула адресов.

6.4.1.1.3 Настройка DNS-ретрансляции

Команды настройки DNS-ретрансляции:

```
set service dns forwarding cache-size 0
set service dns forwarding listen-address 192.168.1.1
set service dns forwarding allow-from 192.168.1.0/24
commit
save
```

где:

- **cache-size 0** - запись в кэш DNS-ретрансляции отключена;
- **192.168.1.1** - IP-адрес интерфейса, на котором прослушиваются запросы DNS;
- **192.168.1.0/24** - подсеть, на которой разрешён доступ к DNS-ретрансляции.

6.4.1.1.4 Настройка NAT

Для настройки правил NAT необходимо ввести следующие команды:

```
set nat source rule 11 outbound-interface name eth1
set nat source rule 11 source address 192.168.1.0/24
set nat source rule 11 translation address masquerade
commit
save
```

6.4.1.1.5 Добавление DNS-сервера

Для настройки DNS-сервера необходимо ввести следующие команды:

```
set system name-server 8.8.8.8
set system name-server 172.16.230.11
commit
save
```

где:

- **8.8.8.8** - публичный DNS-сервер google;
- **172.16.230.11** - DNS-сервер корпоративной сети.

6.4.1.1.6 Настройка маршрутизации

Для настройки шлюза по умолчанию необходимо ввести следующую команду:

```
set protocols static route 0.0.0.0/0 next-hop 172.16.230.1
commit
save
```

6.4.1.1.7 Добавление Radius-server

Для добавления Radius-server необходимо ввести следующие команды:

```
set system login radius server <192.168.1.x> key <secretRadius>
set system login radius server <192.168.1.x> port 1812
commit
save
```

где:

- <192.168.1.x> - IP-адрес, который был выдан Windows Server;
- <secretRadius> - секретный ключ, который был указан при конфигурировании Radius адаптера.

6.4.1.2 Настройка Windows Server

6.4.1.2.1 Первичная настройка

Перед началом работы необходимо, чтобы был настроен контроллер домена с установленными доменными службами Active Directory.

6.4.1.2.1.1 Настройка контроллера домена под Windows Server

1. Открыть окно «Сетевые подключения». Для этого необходимо нажать сочетание клавиш «Win» + «R» и в открывшемся окне «Выполнить» ввести команду «ncpa.cpl».
2. Нажать ПКМ по сетевому адаптеру, выбрать пункт меню «Свойства» и в открывшемся окне «Свойства» перейти в параметры «IP версии 4 (TCP/IPv4)» двойным нажатием ЛКМ (см. [Рисунок – Окно свойств сетевого адаптера](#)). Изменить динамические параметры IP и DNS на статические и ввести необходимые значения.

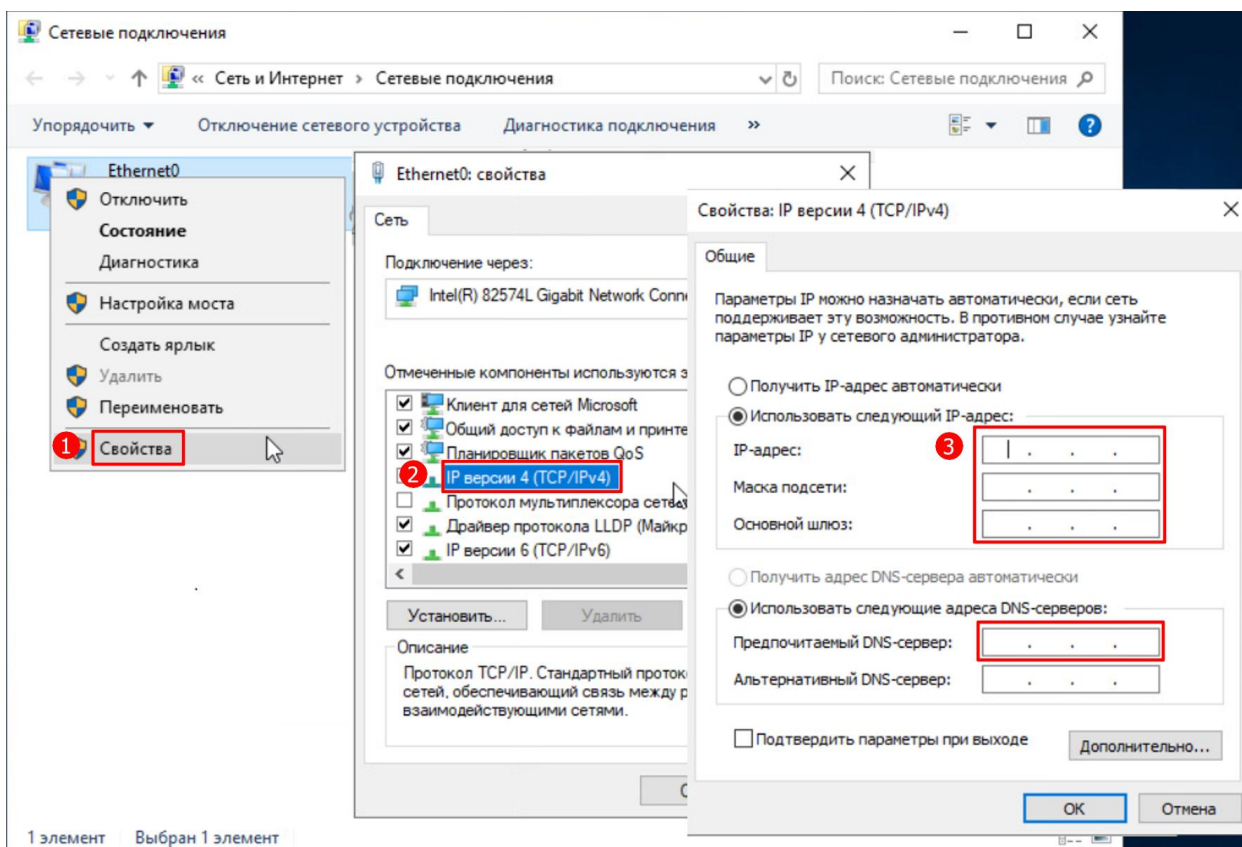


Рисунок – Окно свойств сетевого адаптера

3. Открыть окно «Свойство системы». Для этого необходимо нажать сочетание клавиш «Win» + «R» и в открывшемся окне «Выполнить» ввести команду «sysdm.cpl». Нажать кнопку «Изменить» и в окне «Изменение имени

компьютера или домена» переименовать компьютер в «DC1» (см. [Рисунок – Изменение имени хоста](#)).

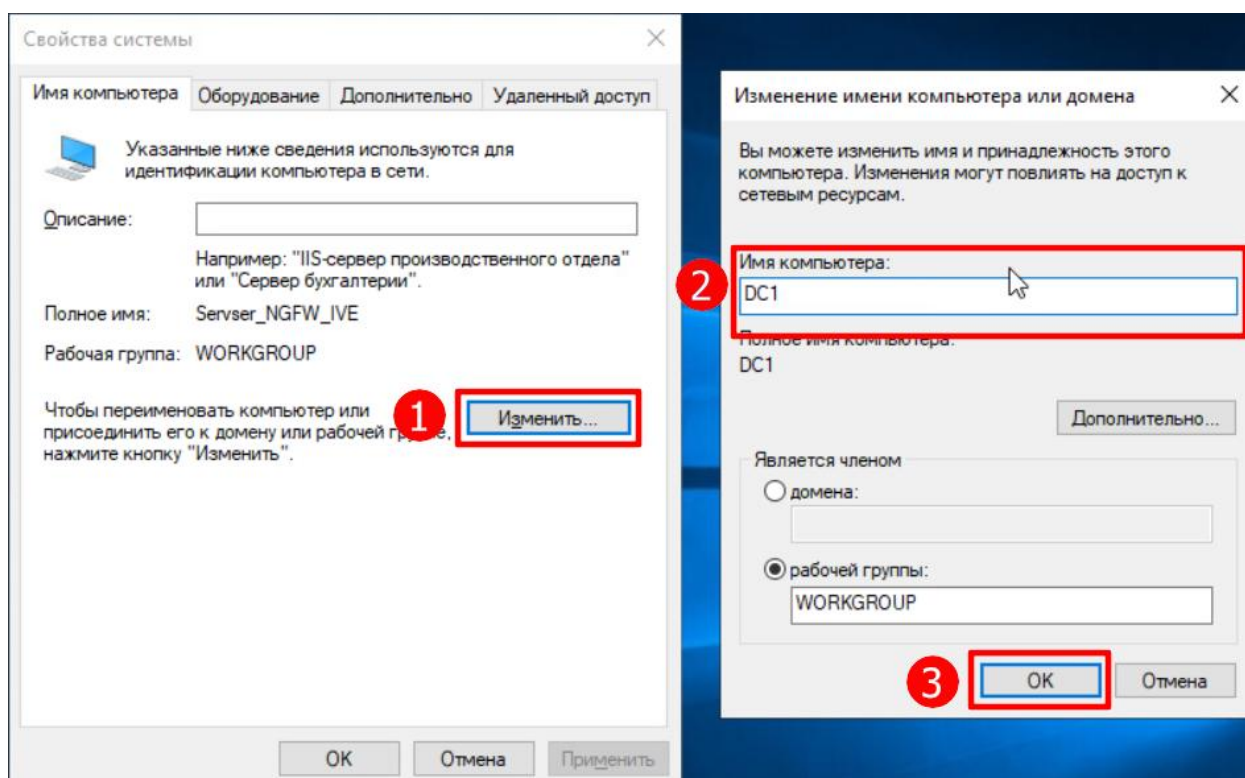


Рисунок – Изменение имени хоста

После применения настроек необходимо перезагрузить компьютер.

4. После перезагрузки компьютера необходимо открыть «Диспетчер серверов», выбрать опцию «Добавить роли и компоненты», указать сервер DC1 и нажать кнопку «Далее» (см. [Рисунок – Выбор целевого сервера](#)).

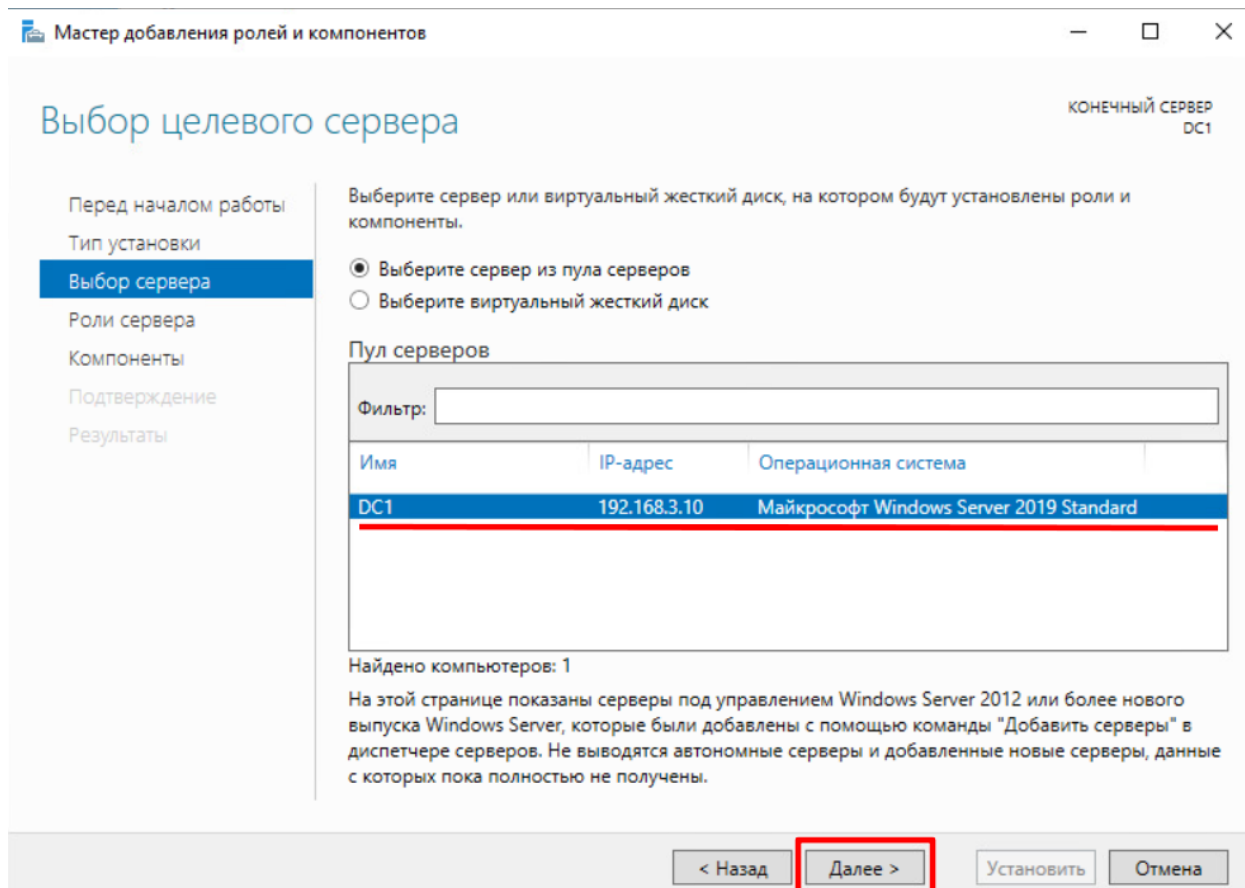


Рисунок – Выбор целевого сервера

5. В ролях выбрать «DNS-сервер» и «Доменные службы Active Directory», в компонентах оставить всё как есть и следовать мастеру установки (см. [Рисунок – Роли сервера](#)).

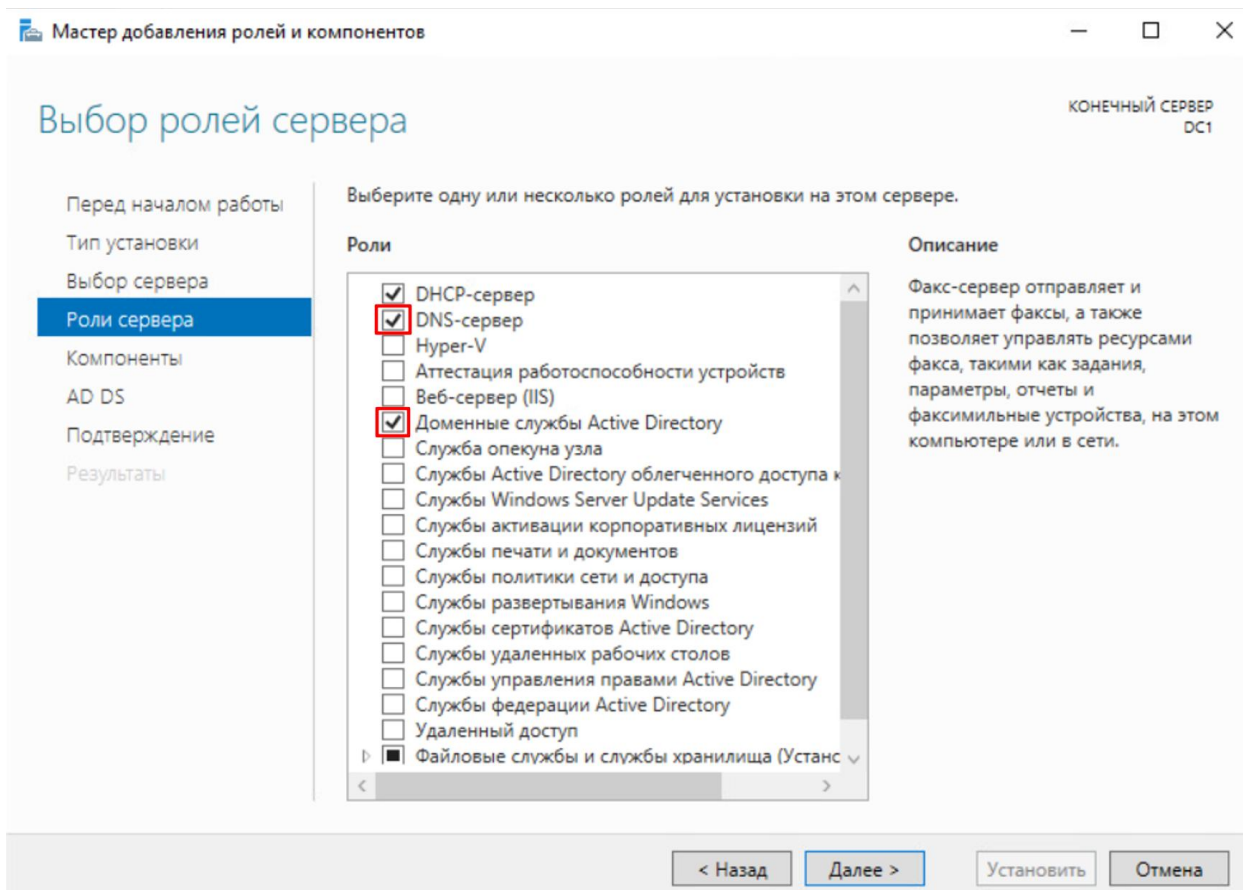


Рисунок – Роли сервера

6. Далее необходимо настроить Active Directory. Для этого требуется нажать на иконку флага с восклицательным знаком в Диспетчере устройств и выбрать «Повысить роль этого сервера до уровня контроллера домена» (см. [Рисунок – Настройка Active Directory](#)).

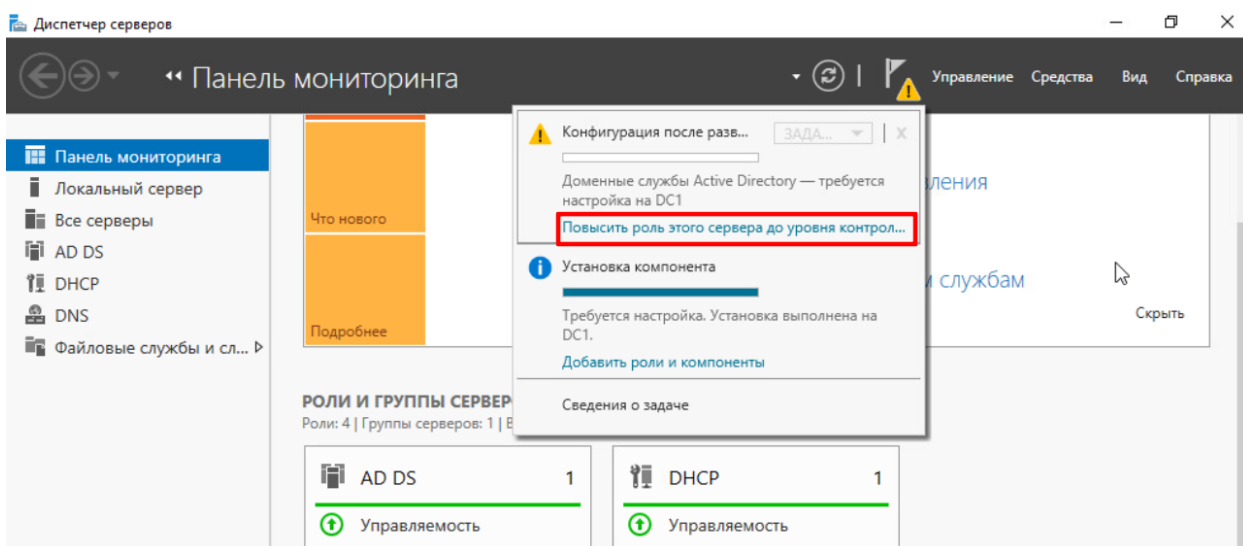


Рисунок – Настройка Active Directory

7. В открывшемся окне «Мастер настройки доменных служб Active Directory» выбрать «Добавить новый лес» и указать имя корневого домена. Имя

«IW2FA.ru» указано в качестве примера (см. [Рисунок – Конфигурация Active Directory](#)).

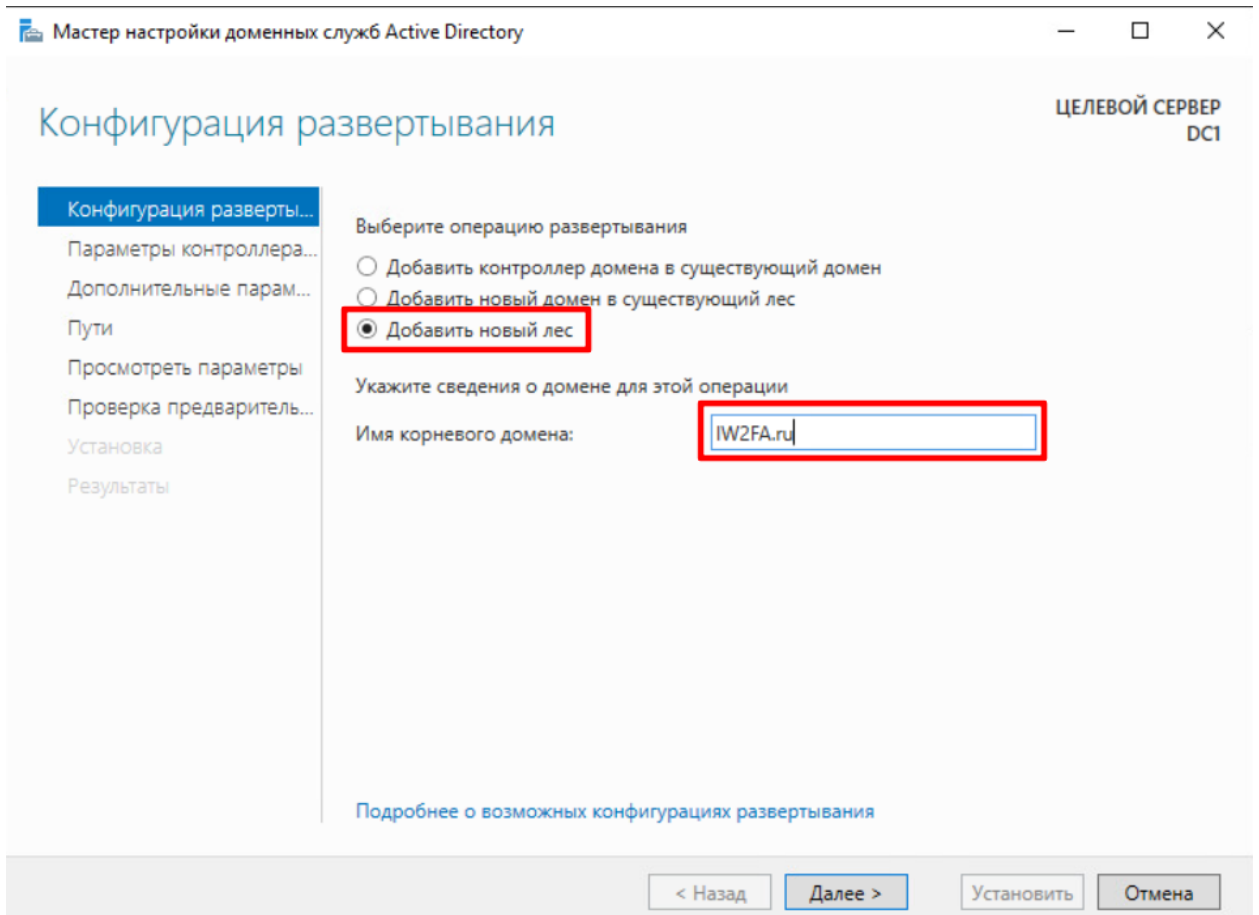


Рисунок – Конфигурация Active Directory

8. На следующем шаге необходимо придумать пароль для службы восстановления каталогов (см. [Рисунок – Пароль для службы восстановления каталогов](#)).

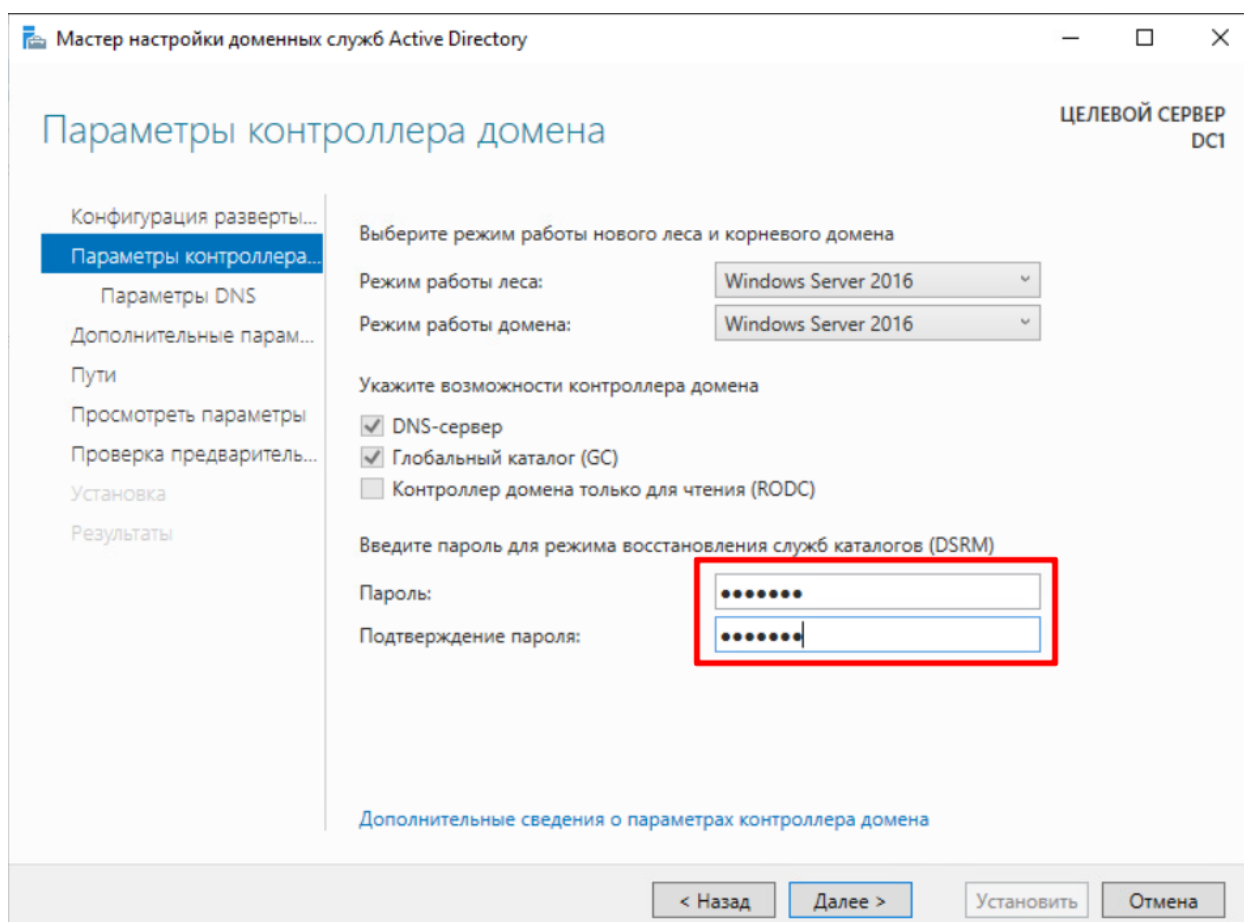


Рисунок – Пароль для службы восстановления каталогов

9. Мастер настройки предложит создать делегирование DNS. Однако в данном случае это не требуется, поэтому можно пропустить этот этап.
10. На следующем этапе мастер настройки автоматически пропишет имя домена NetBIOS. При необходимости возможно изменить его (см. [Рисунок – Имя домена NetBIOS](#)).

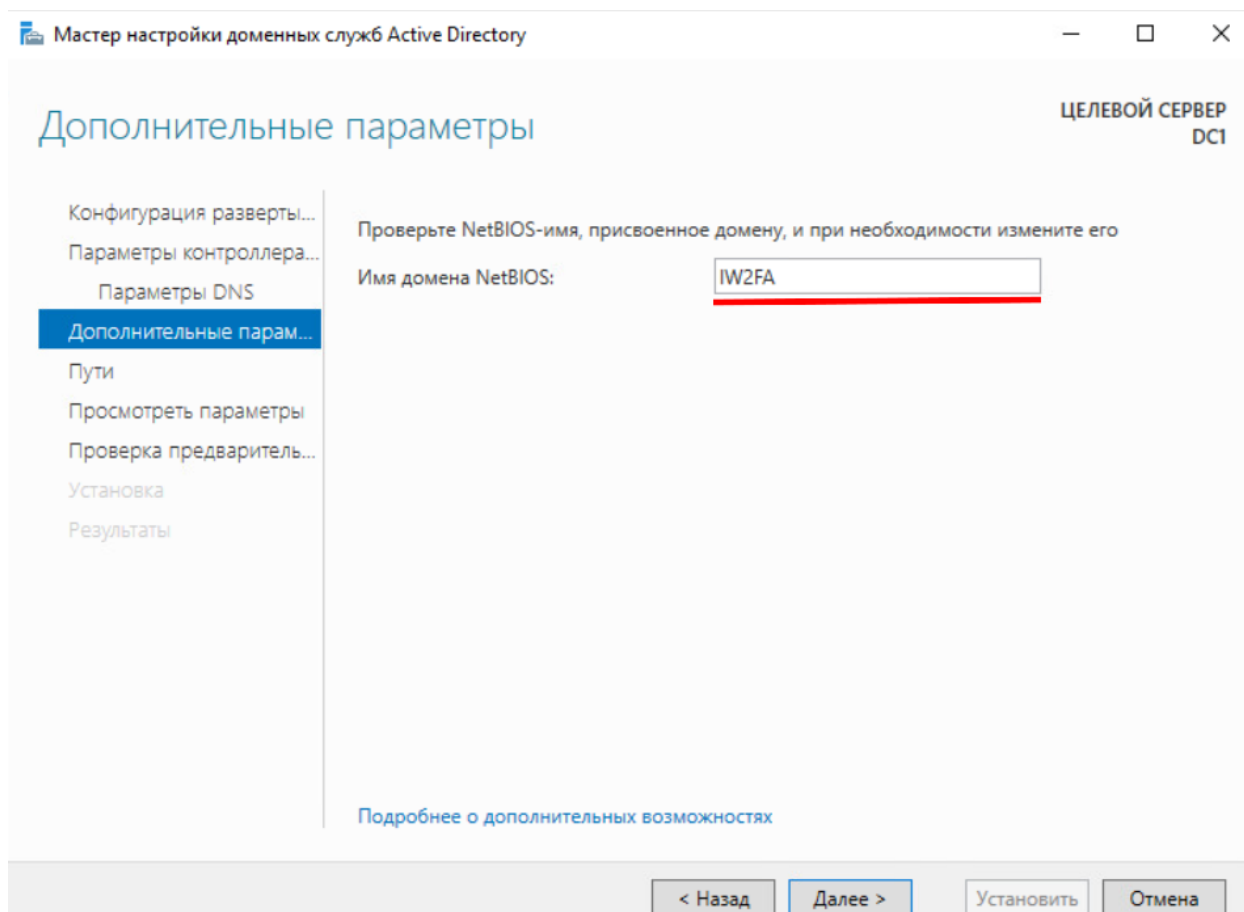


Рисунок – Имя домена NetBIOS

11. Выполнить настройку доменных служб Active Directory в соответствии с инструкциями мастера, не изменяя параметры по умолчанию. По завершении настройки перезагрузить компьютер.

6.4.1.2.1.2 Создание пользователей и групп Active Directory

1. Перейти в диспетчер серверов, открыть вкладку «Средства» и выбрать «Пользователи и компьютеры Active Directory» (см. [Рисунок – Настройка пользователей Active Directory](#)).

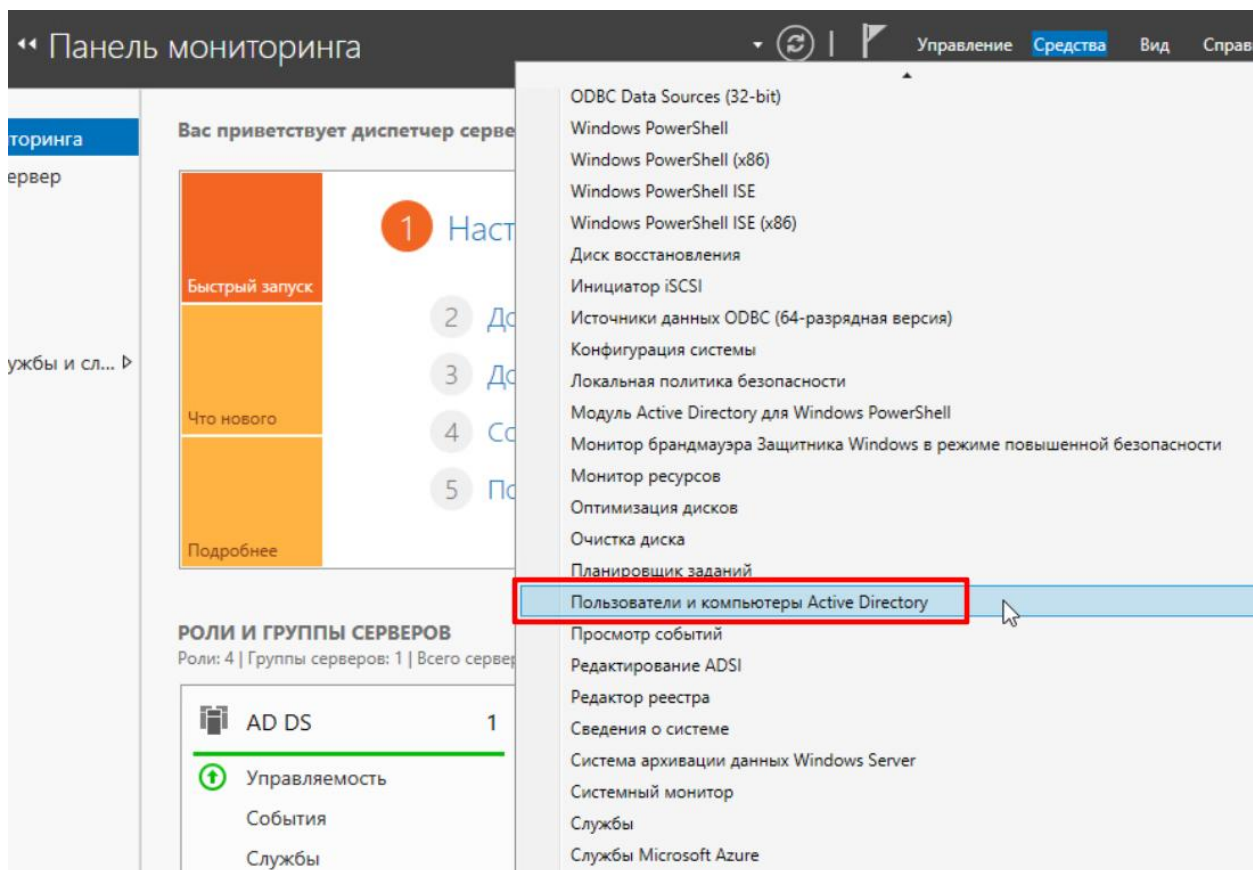


Рисунок – Настройка пользователей Active Directory

2. В открывшемся окне «Active Directory - пользователи и компьютеры» перейти в лес «IW2FA.ru», нажать ПКМ по директории «Users» и выбрать «Создать». В меню «Создать» выбрать «Пользователь» (см. [Рисунок – Добавление пользователя](#)).

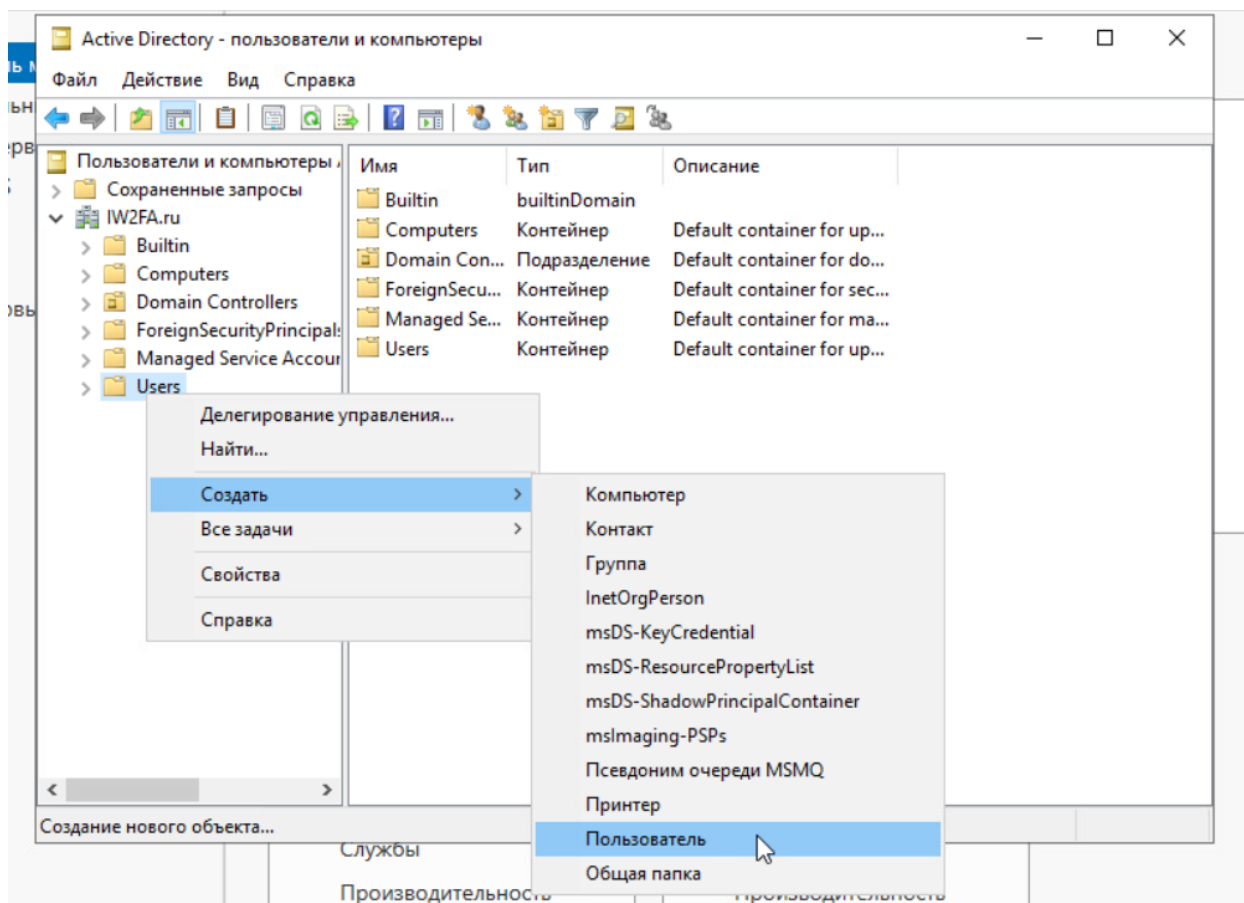


Рисунок – Добавление пользователя

3. Откроется окно «Новый объект - Пользователь». Заполнить поля: «Имя», в примере используется имя «User(6)01»; «Имя входа пользователя», в примере используется - «user01». По завершении ввода параметров, нажать кнопку «Далее». Ввести пароль для создаваемого пользователя и установить флажок в чекбокс «Срок действия пароля не ограничен».
4. По аналогии с созданием пользователей, для создания группы пользователей необходимо нажать ПКМ по директории «Users», выбрать «Создать», после чего выбрать «Группа».
5. В открывшемся окне «Новый объект - Группа» ввести название группы.
6. Для добавления пользователей в созданную группу необходимо нажать ПКМ по необходимой группе. В контекстном меню выберите пункт «Добавить в группу...» и в открывшемся окне найти и добавить требуемых пользователей.

6.4.1.2.2 Подготовка Radius адаптера

1. Необходимо скачать актуальную версию утилиты Radius адаптер с официального сайта <https://multifactor.ru>. Для этого в пункте «Теория» перейти во вкладку «RADIUS адаптер» и затем во вкладку «Windows версия», далее перейти по ссылке «сборка» (см. [Рисунок – Документация Radius адаптера](#)).

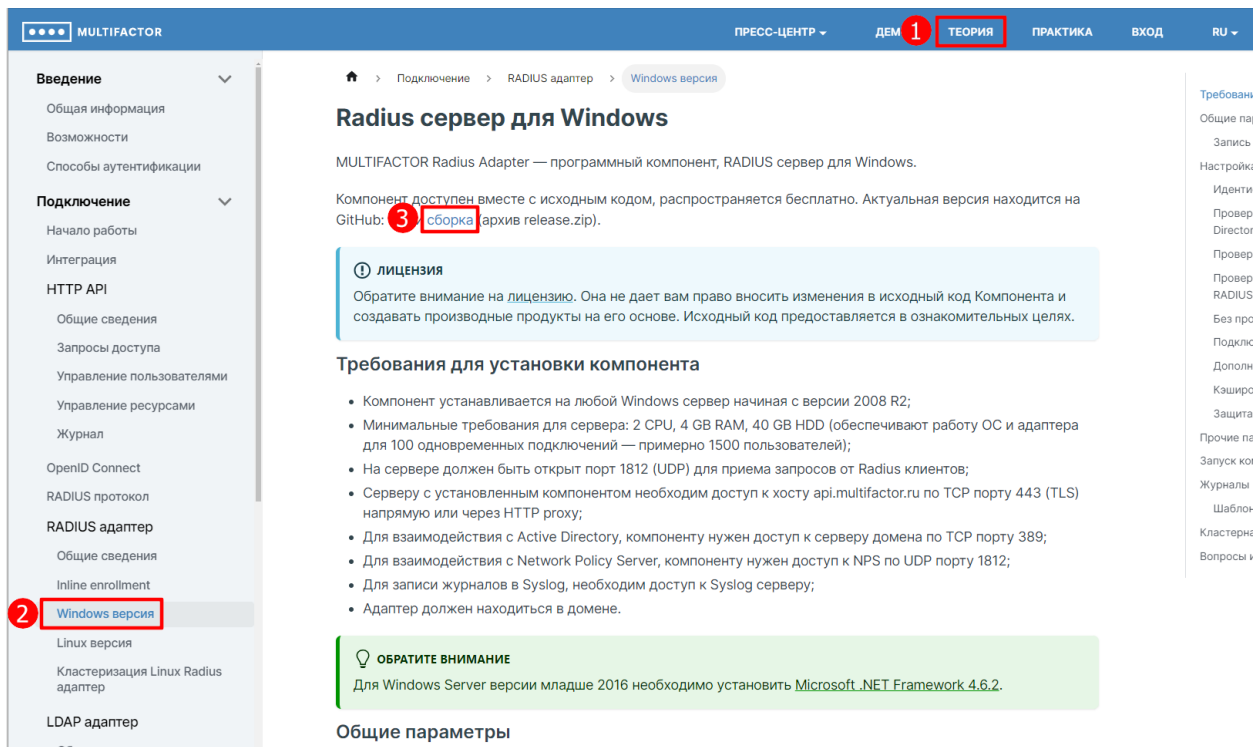
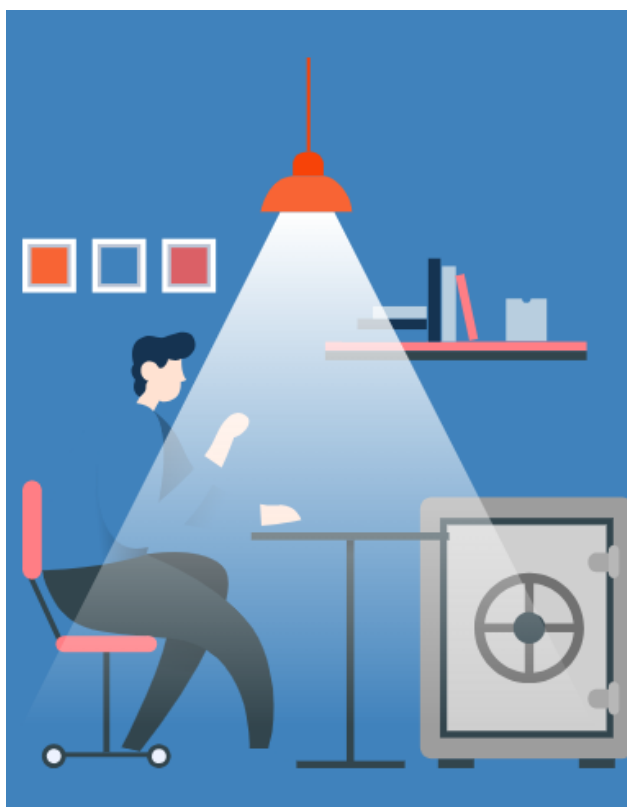


Рисунок – Документация Radius адаптера

- После загрузки, распаковать скачанный архив и поместить его в корневую папку диска C в Windows Server.

6.4.1.2.3 Добавление Multifactor Radius Adapter

- Перейти на сайт <https://admin.multifactor.ru/account/login> и зарегистрироваться (см. [Рисунок – Регистрация на сайте Multifactor](#)).



РЕГИСТРАЦИЯ В СИСТЕМЕ УПРАВЛЕНИЯ МУЛЬТИФАКТОРОМ

Регистрация для администраторов.
Если вы сотрудник компании, где внедряется
Мультифактор, пожалуйста, обратитесь в службу
технической поддержки вашей организации для
предоставления доступа.

 E-mail

 Пароль

 Еще раз пароль

Зарегистрироваться

Если у вас уже есть аккаунт, выполните [вход](#)

Рисунок – Регистрация на сайте Multifactor

- После завершения регистрации будет запущен мастер настройки многофакторной аутентификации для административной панели. Будет предложено установить приложение Multifactor на смартфон для входа на сайт (см. [Рисунок – Установка приложения Multifactor](#)). Если необходимо выбрать другой способ аутентификации, требуется нажать на значок в виде шестерёнки в правом верхнем углу окна настройки, перейти в раздел «Расширенные настройки» и выбрать подходящий способ аутентификации (см. [Рисунок – Расширенные настройки](#)).

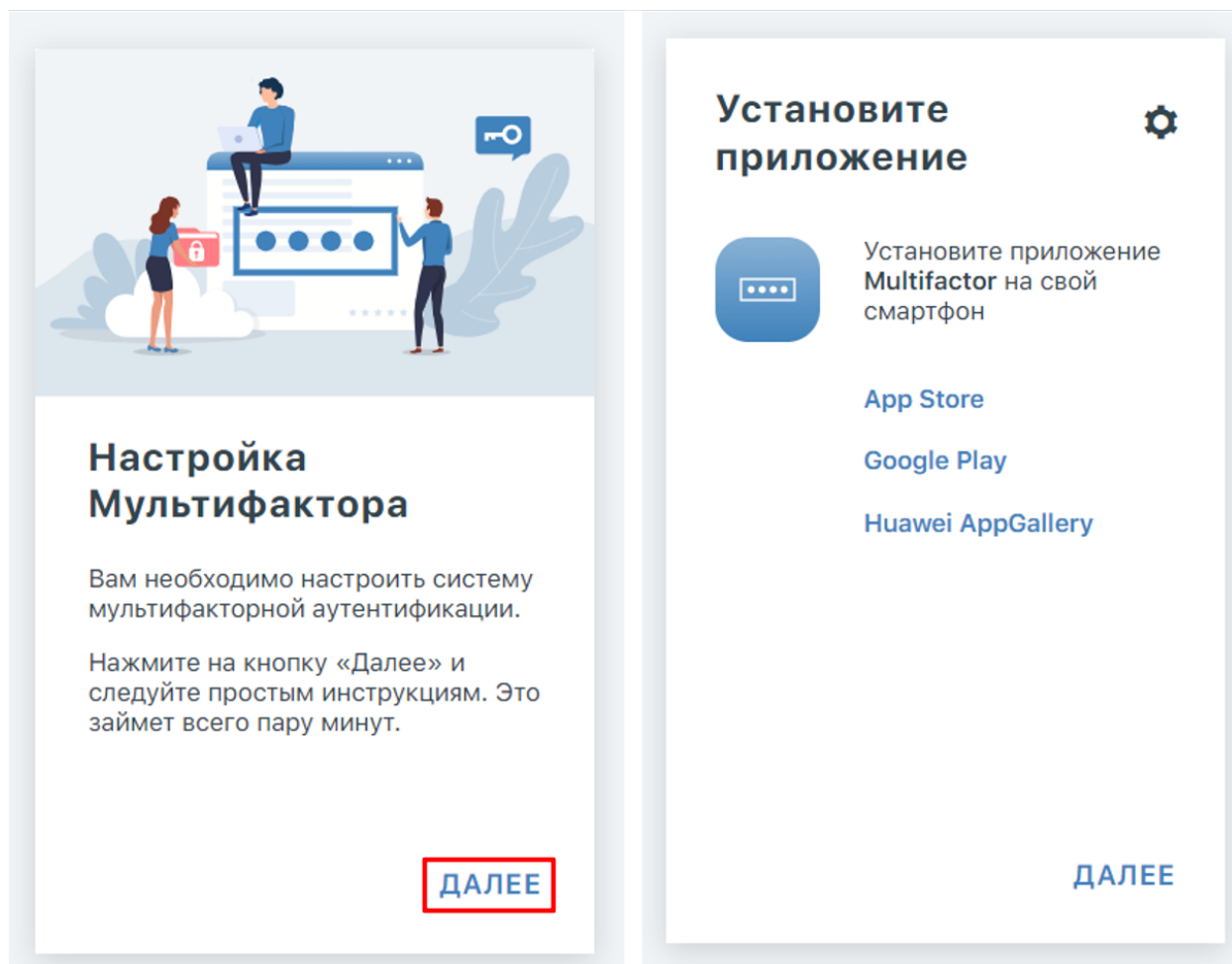


Рисунок – Установка приложения Multifactor

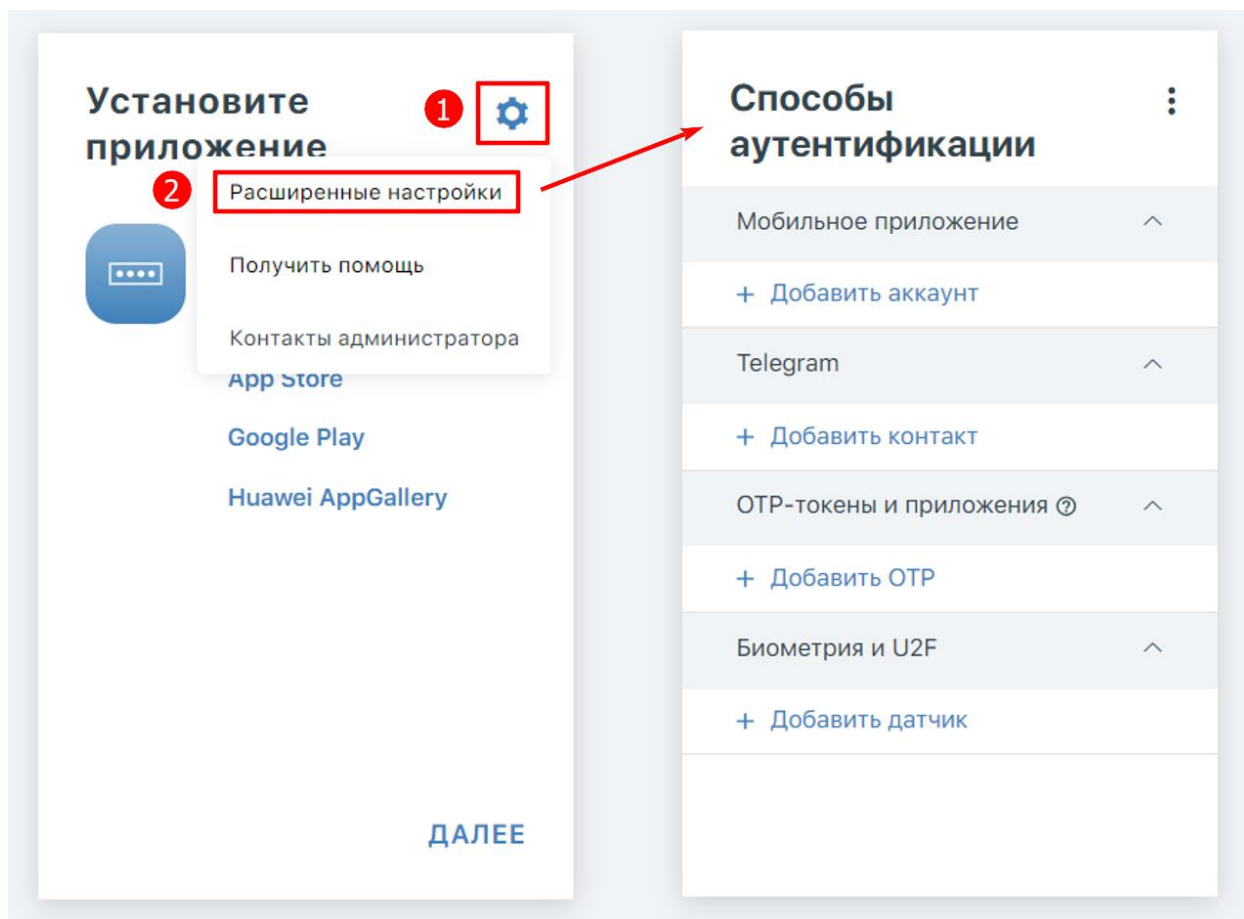


Рисунок – Расширенные настройки

3. После добавления способа аутентификации необходимо подтвердить вход в панель администратора с помощью выбранного ранее способа.
4. В панели администратора перейти в раздел «Ресурсы» и нажать кнопку «Добавить ресурсы» (см. [Рисунок – Добавление ресурсов](#)).

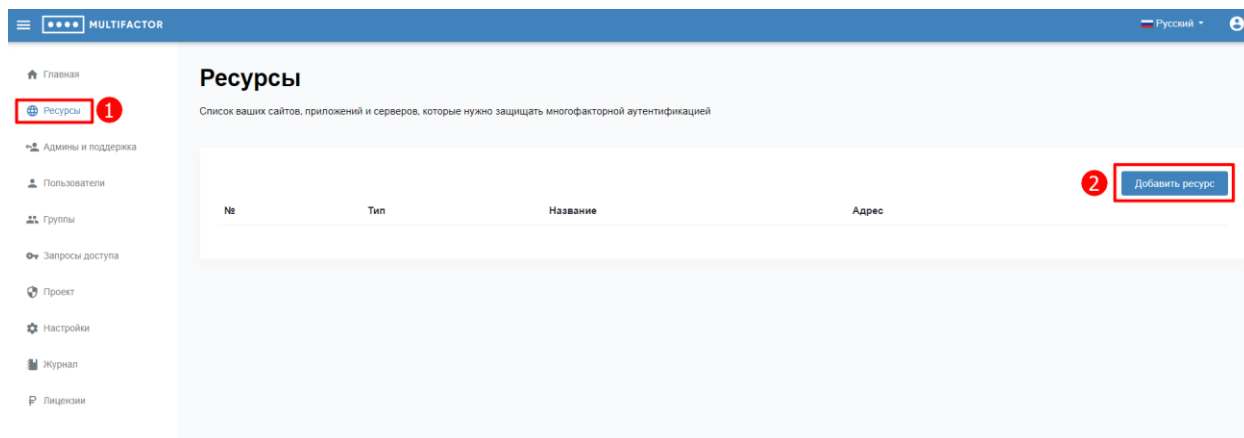


Рисунок – Добавление ресурсов

5. Выбрать добавление ресурса «Другое» и в открывшемся окне заполнить необходимые настройки (см. [Рисунок – Настройка ресурса](#)).

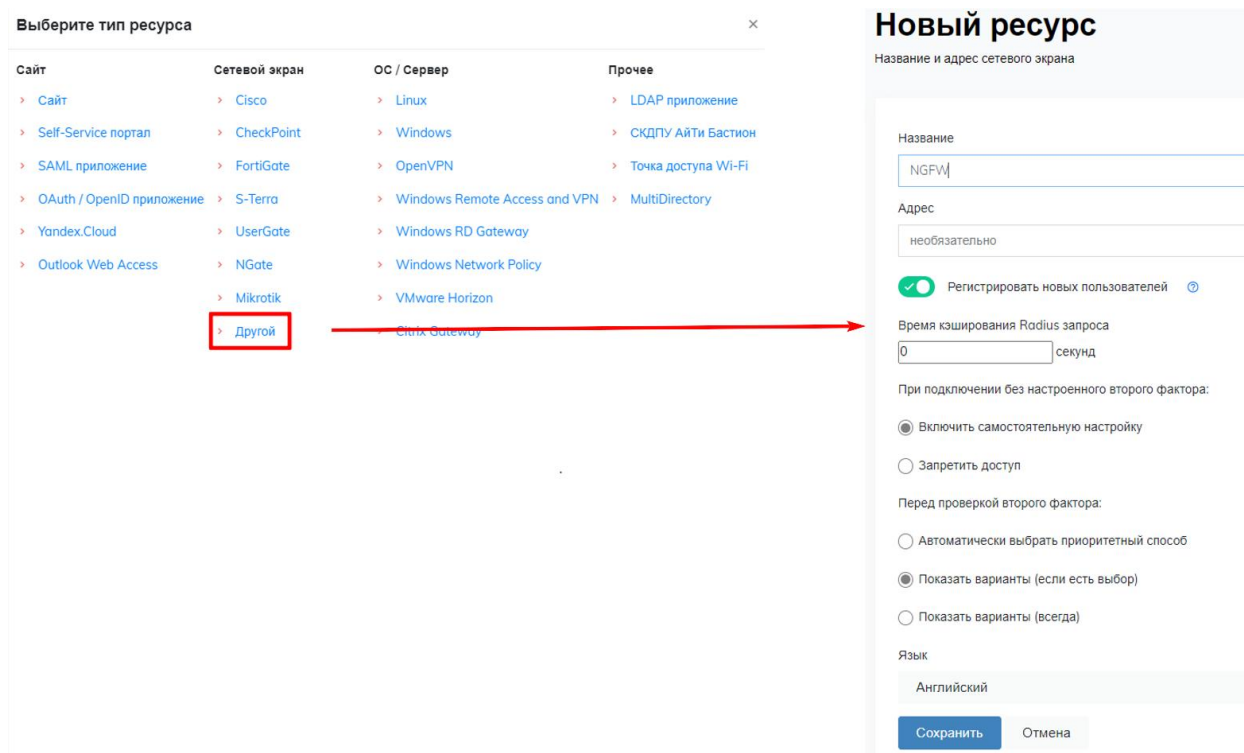


Рисунок – Настройка ресурса

- После добавления ресурса откроется окно с его параметрами. Необходимо скопировать параметры «NAS Identifier» и «Shared Secret» (см. [Рисунок – Параметры добавленного ресурса](#)). Они необходимы для конфигурирования Radius адаптер на Windows Server и для добавления Radius-server в **ARMA Стена**.

← NGFW

Информация о сетевом экране

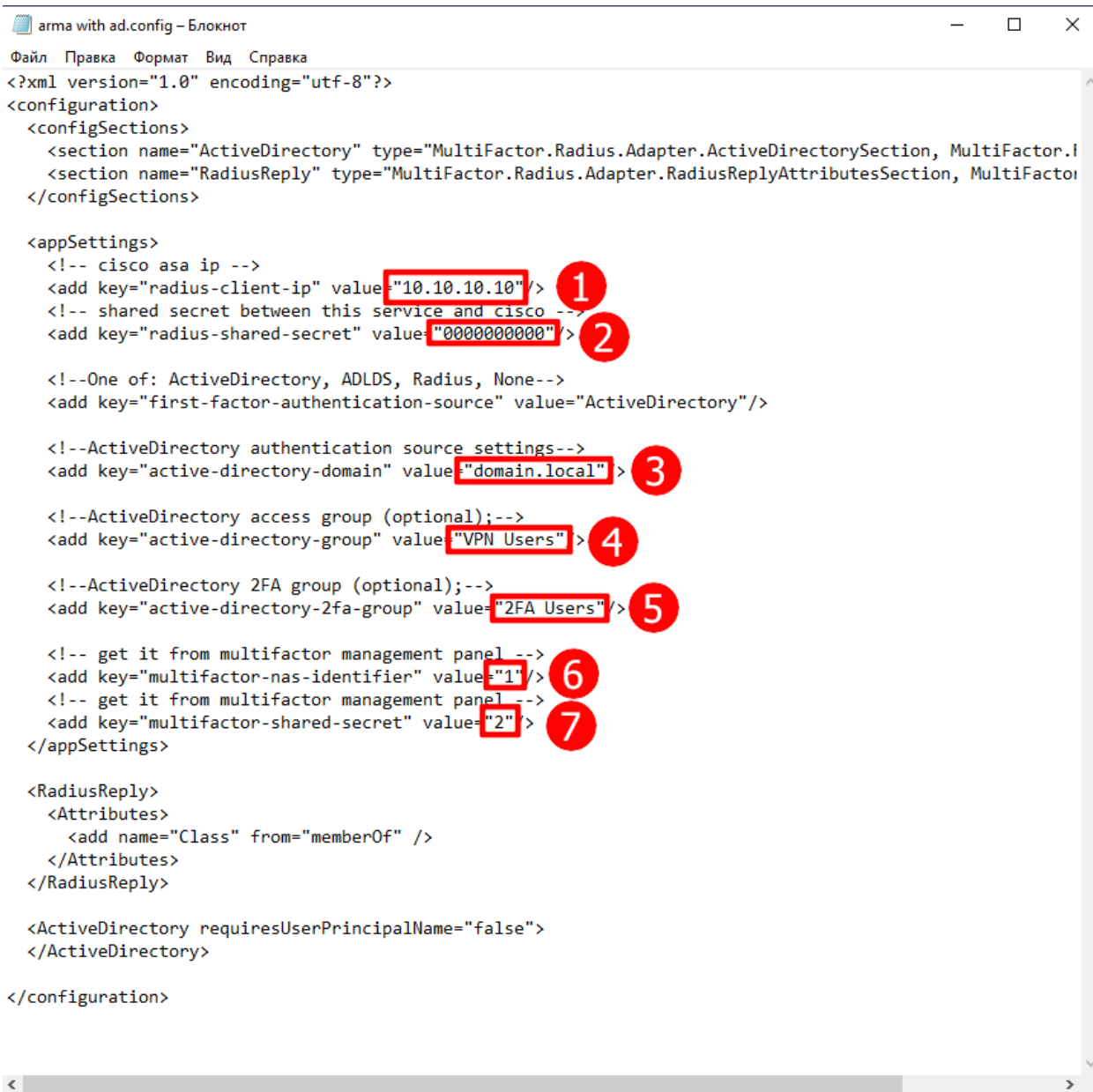
Название	NGFW
Адрес	
NAS Identifier	rs_415f8763e1a8190ee3c54e7126ddf
Shared Secret	Скопировать
Регистрация новых пользователей:	Включена
При подключении без настроенного второго фактора:	Включить самостоятельную настройку
Перед проверкой второго фактора:	Показать варианты (если есть выбор)
Язык	Английский
Время кэширования Radius запроса:	0 Секунд

Рисунок – Параметры добавленного ресурса

6.4.1.2.4 Конфигурирование Radius адаптера

1. Открыть директорию с ранее извлечёнными из архива файлами Radius адаптера. Скопировать файл «cisco with ad.config.template», расположенный в папке «Clients» и переименовать его в «arma with ad.config.template». Удалить расширение «.template», чтобы получилось «arma with ad.config». Таким образом, из предустановленного шаблона получится файл для конфигурации подключения адаптера к **ARMA Стена**.
2. Открыть полученный файл «arma with ad.config» для редактирования с помощью программы «Блокнот» и внести следующие изменения в файле (см. [Рисунок – Исходный шаблон конфигурации](#)):
 1. установить IP-адрес **ARMA Стена**;
 2. ввести придуманный секретный ключ, который будет использоваться при настройке Radius-сервера в **ARMA Стена**;
 3. внести имя домена Active Directory, по которому будет проводиться аутентификация;

4. указать группу, которой предоставляется доступ без второго фактора аутентификации;
5. указать группу, у которой будет запрашиваться второй фактор аутентификации;
6. ввести NAS Identifier, полученный на сайте Multifactor;
7. ввести Shared Secret, полученный на сайте Multifactor.



```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <configSections>
    <section name="ActiveDirectory" type="MultiFactor.Radius.Adapter.ActiveDirectorySection, MultiFactor.I
    <section name="RadiusReply" type="MultiFactor.Radius.Adapter.RadiusReplyAttributesSection, MultiFactor.I
  </configSections>

  <appSettings>
    <!-- cisco asa ip -->
    <add key="radius-client-ip" value="10.10.10.10"/>
    <!-- shared secret between this service and cisco -->
    <add key="radius-shared-secret" value="0000000000"/>

    <!--One of: ActiveDirectory, ADLDS, Radius, None-->
    <add key="first-factor-authentication-source" value="ActiveDirectory"/>

    <!--ActiveDirectory authentication source settings-->
    <add key="active-directory-domain" value="domain.local"/>

    <!--ActiveDirectory access group (optional);-->
    <add key="active-directory-group" value="VPN Users"/>

    <!--ActiveDirectory 2FA group (optional);-->
    <add key="active-directory-2fa-group" value="2FA Users"/>

    <!-- get it from multifactor management panel -->
    <add key="multifactor-nas-identifier" value="1"/>
    <!-- get it from multifactor management panel -->
    <add key="multifactor-shared-secret" value="2"/>
  </appSettings>

  <RadiusReply>
    <Attributes>
      <add name="Class" from="memberOf" />
    </Attributes>
  </RadiusReply>

  <ActiveDirectory requiresUserPrincipalName="false">
  </ActiveDirectory>
</configuration>
```

Рисунок – Исходный шаблон конфигурации

Пример конфигурационного файла, в котором не предусмотрена поддержка группы без второго фактора аутентификации (см. [Рисунок – Пример конфигурационного файла](#)):

```

*arma with ad.config – Блокнот
Файл Правка Формат Вид Справка
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <configSections>
    <section name="ActiveDirectory" type="MultiFactor.Radius.Adapter.ActiveDirectorySection, MultiFactor.I
    <section name="RadiusReply" type="MultiFactor.Radius.Adapter.RadiusReplyAttributesSection, MultiFactor
  </configSections>

  <appSettings>
    <!-- cisco asa ip -->
    <add key="radius-client-ip" value="192.168.1.1"/>
    <!-- shared secret between this service and cisco -->
    <add key="radius-shared-secret" value="if2a!"/>

    <!--One of: ActiveDirectory, ADLDS, Radius, None-->
    <add key="first-factor-authentication-source" value="ActiveDirectory"/>

    <!--ActiveDirectory authentication source settings-->
    <add key="active-directory-domain" value="iw2fa.ru"/>

    <!--ActiveDirectory access group (optional);-->

    <!--ActiveDirectory 2FA group (optional);-->
    <add key="active-directory-2fa-group" value="MyUsers"/>

    <!-- get it from multifactor management panel -->
    <add key="multifactor-nas-identifier" value="rs_415f8763e1a8190ee3c54e7126ddf"/>
    <!-- get it from multifactor management panel -->
    <add key="multifactor-shared-secret" value="4331d7cd21k88cb879b2c974f226d43b"/>
  </appSettings>

  <RadiusReply>
    <Attributes>
      <add name="Class" from="memberOf" />
    </Attributes>
  </RadiusReply>

  <ActiveDirectory requiresUserPrincipalName="false">
  </ActiveDirectory>
</configuration>

```

Рисунок – Пример конфигурационного файла

6.4.1.2.5 Запуск Radius адаптера

Компонент может работать как в режиме консоли, так и в качестве службы операционной системы Windows. Для запуска компонента в режиме консоли достаточно запустить приложение.

Для установки Radius адаптера в качестве службы Windows необходимо перейти в папку с файлами адаптера и выполнить команду с ключом «/i» от имени администратора: «MultiFactor.Radius.Adapter.exe /i».

Для удаления Radius адаптера необходимо выполнить команду от имени администратора: «sc delete MFRadiusAdapter».

6.4.1.3 Проверка работы службы

Примечание:

Перед началом работы необходимо отключить брандмауэр Windows!

При входе в NGFW и аутентификации с использованием учётных данных из группы, указанной в поле «active_directory_2fa_group» при настройке адаптера, система предложит зарегистрировать второй фактор аутентификации для пользователя (если он ещё не был зарегистрирован). В случае, если второй фактор уже зарегистрирован, система проверит его (см. [Рисунок – Аутентификация](#)):

```
ngfwos login: Pyatnitsa
Password:
To continue, configure second authentication factor. Enter number: 1 - Mobile ap
p; 2 - Telegram1
Install MultiFactor App on your phone. Then press + and enter the code: 71178327
0125
Welcome to NGFWOS!
Pyatnitsa@ngfwos:~$
```

Рисунок – Аутентификация

6.4.2 Multifactor Radius Adapter - Linux

В качестве примера настройки Multifactor Radius Adapter для CentOS будет использоваться стенд, представленный на рисунке (см. [Рисунок – Схема стенда для настройки Multifactor Radius Adapter - Linux](#)).

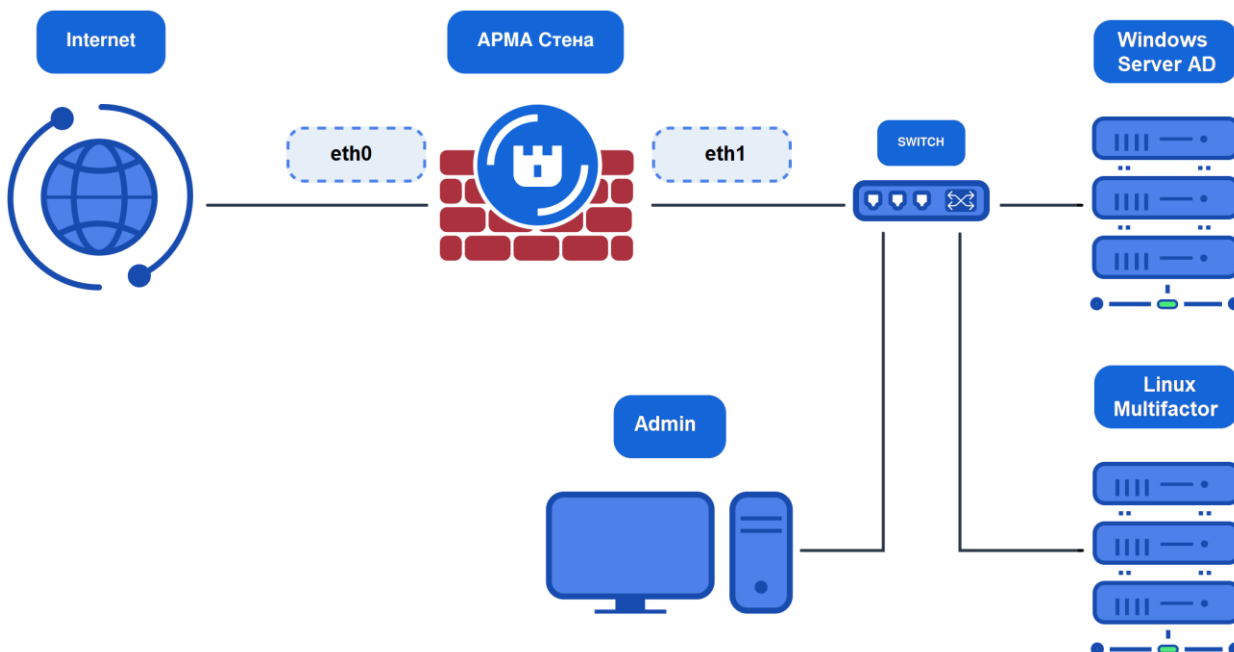


Рисунок – Схема стенда для настройки Multifactor Radius Adapter - Linux

Инструкции по настройке **ARMA Стена** и **Multifactor Radius Adapter** представлены в соответствующих разделах: «[Настройка ARMA Стена](#)» и «[Добавление Multifactor Radius Adapter](#)».

6.4.2.1 Настройка CentOS 7

Необходимо внести изменения в конфигурацию сетевого интерфейса CentOS. Для этого следует изменить параметр «ONBOOT» в файле «**/etc/sysconfig/network-scripts/ifcfg-eth0**» с «**ONBOOT=no**» на «**ONBOOT=yes**». После этого необходимо перезагрузить сетевую службу с помощью команды «**systemctl restart network**». Это позволит интерфейсу автоматически включаться при загрузке системы.

Для начала установки компонента **Multifactor Radius Adapter** необходимо обновить имеющиеся пакеты и проверить наличие доступа к репозиториям. Это осуществляется с помощью команды «**yum -y update && yum -y upgrade**». Однако при выполнении этой команды может возникнуть ошибка (см. [Рисунок – Возможная ошибка](#)).

```

root@centos ~]# yum -y update && yum -y upgrade
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
Could not retrieve mirrorlist http://mirrorlist.centos.org/?release=7&arch=x86_64&repo=os&infra=stock error was
14: curl#6 - "Could not resolve host: mirrorlist.centos.org; Unknown error"

One of the configured repositories failed (Unknown),
and yum doesn't have enough cached data to continue. At this point the only
safe thing yum can do is fail. There are a few ways to work "fix" this:

 1. Contact the upstream for the repository and get them to fix the problem.

 2. Reconfigure the baseurl/etc. for the repository, to point to a working
    upstream. This is most often useful if you are using a newer
    distribution release than is supported by the repository (and the
    packages for the previous distribution release still work).

 3. Run the command with the repository temporarily disabled
    yum --disablerepo=<repoid> ...

 4. Disable the repository permanently, so yum won't use it by default. Yum
    will then just ignore the repository until you permanently enable it
    again or use --enablerepo for temporary usage:

        yum-config-manager --disable <repoid>
    or
        subscription-manager repos --disable=<repoid>

 5. Configure the failing repository to be skipped, if it is unavailable.
    Note that yum will try to contact the repo. when it runs most commands,
    so will have to try and fail each time (and thus. yum will be be much
    slower). If it is a very temporary problem though, this is often a nice
    compromise:

        yum-config-manager --save --setopt=<repoid>.skip_if_unavailable=true

Cannot find a valid baseurl for repo: base/7/x86_64

```

Рисунок – Возможная ошибка

Это свидетельствует о том, что доменное имя зеркал репозитория не разрешается по неизвестной причине. Данная проблема может быть решена путём настройки других репозиториях, которые находятся в каталоге «**/etc/yum.repos.d/CentOS-Base.repo**». Вот так выглядят репозитории по умолчанию (см. [Рисунок – Репозитории по умолчанию](#)).


```
# CentOS-Base.repo
#
# The mirror system uses the connecting IP address of the client and the
# update status of each mirror to pick mirrors that are updated to and
# geographically close to the client. You should use this for CentOS updates
# unless you are manually picking other mirrors.
#
# If the mirrorlist= does not work for you, as a fall back you can try the
# remarked out baseurl= line instead.
#
#
[base]
name=CentOS-$releasever - Base
mirrorlist=http://mirrorlist.centos.org/?release=$releasever&arch=$basearch&repo=os&infra=$infra
#baseurl=http://mirror.centos.org/centos/$releasever/os/$basearch/
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-7

#released updates
[updates]
name=CentOS-$releasever - Updates
mirrorlist=http://mirrorlist.centos.org/?release=$releasever&arch=$basearch&repo=updates&infra=$infra
#baseurl=http://mirror.centos.org/centos/$releasever/updates/$basearch/
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-7

#additional packages that may be useful
[extras]
name=CentOS-$releasever - Extras
mirrorlist=http://mirrorlist.centos.org/?release=$releasever&arch=$basearch&repo=extras&infra=$infra
#baseurl=http://mirror.centos.org/centos/$releasever/extras/$basearch/
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-7

#additional packages that extend functionality of existing packages
[centosplus]
name=CentOS-$releasever - Plus
mirrorlist=http://mirrorlist.centos.org/?release=$releasever&arch=$basearch&repo=centosplus&infra=$infra
#baseurl=http://mirror.centos.org/centos/$releasever/centosplus/$basearch/
gpgcheck=1
enabled=0
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-7
-
```

Рисунок – Репозитории по умолчанию

Необходимо закомментировать имеющиеся зеркала и указать другие значения «**baseurl**» в каждом блоке. В данном примере используются архивы snapshot 2021 г. (см. [Рисунок – Комментирование имеющихся зеркал](#)).


```
# CentOS-Base.repo
#
# The mirror system uses the connecting IP address of the client and the
# update status of each mirror to pick mirrors that are updated to and
# geographically close to the client. You should use this for CentOS updates
# unless you are manually picking other mirrors.
#
# If the mirrorlist= does not work for you, as a fall back you can try the
# remarked out baseurl= line instead.
#
#
[base]
name=CentOS-$releasever - Base
#mirrorlist=http://mirrorlist.centos.org/?release=$releasever&arch=$basearch&repo=os&infra=$infra
#baseurl=http://mirror.centos.org/centos/$releasever/os/$basearch/
baseurl=http://vault.centos.org/7.9.2009/os/$basearch/
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-7

#released updates
[updates]
name=CentOS-$releasever - Updates
#mirrorlist=http://mirrorlist.centos.org/?release=$releasever&arch=$basearch&repo=updates&infra=$infra
#baseurl=http://mirror.centos.org/centos/$releasever/updates/$basearch/
baseurl=http://vault.centos.org/7.9.2009/updates/$basearch/
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-7

#additional packages that may be useful
[extras]
name=CentOS-$releasever - Extras
#mirrorlist=http://mirrorlist.centos.org/?release=$releasever&arch=$basearch&repo=extras&infra=$infra
#baseurl=http://mirror.centos.org/centos/$releasever/extras/$basearch/
baseurl=http://vault.centos.org/7.9.2009/extras/$basearch/
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-7

#additional packages that extend functionality of existing packages
[centosplus]
name=CentOS-$releasever - Plus
#mirrorlist=http://mirrorlist.centos.org/?release=$releasever&arch=$basearch&repo=centosplus&infra=$infra
#baseurl=http://mirror.centos.org/centos/$releasever/centosplus/$basearch/
baseurl=http://vault.centos.org/7.9.2009/centosplus/$basearch/
gpgcheck=1
enabled=0
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-7
```

Рисунок – Комментирование имеющихся зеркал

После этих действий команда «**yum -y update && yum -y upgrade**» выполнится без ошибок.

Далее необходимо установить среду выполнения APS.NET Core runtime версии 6:

```
sudo rpm -Uvh https://packages.microsoft.com/config/centos/7/packages-
microsoft-prod.rpm
sudo yum install aspnetcore-runtime-6.0
```

После этого необходимо сформировать каталог для файлов инструмента, скопировать сборку в созданную папку и создать учётную запись, под которой будет работать служба:

```
sudo mkdir /opt/multifactor /opt/multifactor/radius/opt/multifactor/radius/logs #  
создание папок для файлов адаптера  
sudo      wget      https:      github.com/MultifactorLab/multifactor-radius-  
adapter/releases/latest/download/release_linux_x64.zip # клонирование сборки  
sudo unzip release_linux_x64.zip -d /opt/multifactor/radius # распаковка архива  
sudo useradd -r mfa # создание пользователя  
sudo chown -R mfa:mfa /opt/multifactor/radius/ # присвоение директорий  
пользователю  
sudo chown -R mfa:mfa /opt/multifactor/radius/clients  
sudo chmod -R 700 /opt/multifactor/radius/ # изменять директории может только  
пользователь  
sudo chmod -R 700 /opt/multifactor/radius/clients
```

Необходимо создать службу «systemd» для адаптера. Для этого сначала требуется создать файл службы с помощью команды «**sudo vi /etc/systemd/system/multifactor-radius.service**», а затем изменить его содержимое:

```
[Unit]  
Description=Multifactor Radius Adapter  
  
[Service]  
WorkingDirectory=/opt/multifactor/radius/  
ExecStart=/usr/bin/dotnet /opt/multifactor/radius/multifactor-radius- adapter.dll  
Restart=always  
# Restart service after 10 seconds if the service crashes:  
RestartSec=10  
KillSignal=SIGINT  
SyslogIdentifier=multifactor-radius  
User=mfa  
Environment=ASPNETCORE_ENVIRONMENT=Production  
Environment=DOTNET_PRINT_TELEMETRY_MESSAGE=false  
  
# How many seconds to wait for the app to shut down after it receives the initial  
interrupt signal.  
# If the app doesn't shut down in this period, SIGKILL is issued to terminate the app.  
# The default timeout for most distributions is 90 seconds.  
TimeoutStopSec=30  
  
[Install]  
WantedBy=multi-user.target
```

После этого необходимо выполнить команду для запуска службы: **«sudo systemctl enable multifactor-radius»**.

Затем приступить к редактированию конфигурации серверов Radius. Общие параметры работы компонента хранятся в файле **«/opt/multifactor/radius/multifactor-radius-adapter.dll.config»** в формате «xml»:

```
<!-- Адрес и порт (UDP), по которому адаптер будет принимать запросы на
аутентификацию от клиентов -->
<add key="adapter-server-endpoint" value="0.0.0.0:1812"/>

<!-- Адрес API MULTIFACTOR -->
<add key="multifactor-api-url" value="https: api.multifactor.ru"/>

<!-- Доступ к API MULTIFACTOR через HTTP прокси (опционально) -->
<!-- <add key="multifactor-api-proxy" value="http: login:password@proxy:3128"/>
-->

<!-- Уровень логирования: 'Debug', 'Info', 'Warn', 'Error' -->
<add key="logging-level" value="Debug"/>
```

Шаблоны для настройки отдельных подключений находятся в каталоге **«/opt/multifactor/radius/clients»**. Для создания необходимой конфигурации, требуется скопировать имеющийся шаблон **«cisco with ad.config.template»** с помощью команды **«cp cisco/with/ad.config.template [указать имя].config»**. Таким образом, будет скопирован шаблон конфигурации для связи с Active Directory, содержащий следующие данные:

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <configSections>
    <section name="RadiusReply"
type="MultiFactor.Radius.Adapter.RadiusReplyAttributesSection, multifactor-radius-
adapter"/>
  </configSections>
  <appSettings>
    <!-- cisco asa ip -->
    <add key="radius-client-ip" value="10.10.10.10"/>
    <!-- shared secret between this service and cisco -->
    <add key="radius-shared-secret" value="0000000000"/>
    <!-- One of: ActiveDirectory, ADLDS, Radius, None -->
    <add key="first-factor-authentication-source" value="ActiveDirectory"/>
    <!-- ActiveDirectory authentication settings: for example domain local on host
10.0.0.4 -->
    <add key="active-directory-domain"
```

```
value="ldaps:10.0.0.4/DC=domain,DC=local"/>
  <!-- ActiveDirectory access group (optional): -->
  <add key="active-directory-group" value="UPN Users"/>
  <!-- ActiveDirectory 2FA group (optional) -->
  <add key="active-directory-2fa-group" value="2FA Users"/>
  <!-- get it from multifactor management panel -->
  <add key="multifactor-nas-identifier" value="1"/>
  <!-- get it from multifactor management panel -->
  <add key="multifactor-shared-secret" value="2"/>
</appSettings>
<RadiusReply>
  <Attributes>
    <add name="Class" from="memberOf"/>
  </Attributes>
</RadiusReply>
</configuration>
```

Необходимо внести следующие изменения в файл шаблона конфигурации:

- поле «**radius-client-ip**» должно быть изменено на «192.168.1.1», так как Radius-сервер находится в локальной сети, а клиентом является **ARMA Стена**;
- поле «**radius-shared-secret**» должно содержать значение, которое было придумано при настройке аутентификации Radius на **ARMA Стена**;
- поле «**active-directory-domain**» должно быть изменено в соответствии с доменом Active Directory, который присутствует в подсети;
- поле «**active-directory-group**» должно быть удалено, чтобы всегда использовался второй фактор аутентификации, указанный в поле «**active-directory-2fa-group**»;
- поля «**multifactor-nas-identifier**» и «**multifactor-shared-secret**» должны быть взяты из панели администратора при создании ресурса для аутентификации.

Необходимо перезагрузить подсистемы служб и созданную службу для применения изменений:

```
sudo systemctl daemon-reload
sudo systemctl restart multifactor-radius
```

6.4.2.2 Возможные ошибки

1. В случае возникновения ошибки «**Unable to load shared library „ldap.so.2“ or one of its dependencies**», необходимо внести коррективы в цепочку таким

образом, чтобы симлинк **«libldap.so.2»** в конечном итоге указывал на конкретную библиотеку **«libldap-2.X.so.2.Y.Z»**.

Пример: libldap.so.2 * libldap-2.4.so.2 это симлинк libldap-2.4.so.2 * libldap_r-2.4.so.2 это симлинк libldap_r-2.4.so.2 * libldap_r-2.4.so.2.11.5 это симлинк libldap_r-2.4.so.2.11.5 это сама библиотека.

Проверка и исправление символических ссылок: для проверки символических ссылок необходимо определить местоположение библиотеки **«libldap»**. Обычно она находится в каталоге **«/usr/lib/x86_64-linux-gnu»**.

Далее необходимо выполнить команду **«ls -la»**, чтобы просмотреть список всех файлов и символических ссылок. Необходимо найти информацию о том, как и кто ссылается на библиотеку **«libldap»**, а также определить, каких ссылок не хватает.

Чаще всего отсутствует одна ссылка – с **«libldap.so.2»** на основную версию библиотеки. Команды создания недостающего симлинка:

Для Debian и Ubuntu:

```
In      -s/usr/lib/x86_64-linux-gnu/libldap-2.4.so.2      /usr/lib/x86_64-linux-  
gnu/libldap.so.2
```

Для CentOS и REDOS:

```
In      -s  /usr/lib64/libldap_r-2.4.so.2.10.9  /usr/lib64/libldap.so.2  #Версии  
библиотек могут отличаться
```

Аналогичные действия выполняются с библиотекой **«liblber»**.

2. В случае возникновения ошибки **«Unable to start: Address already in use»**, существует два способа её устранения:

- Если используете запуск адаптера через **«/opt/multifactor/radius/multifactor-radius-adapter»**, то необходимо отключить адаптер как службу:

```
sudo systemctl stop multifactor-radius  
sudo systemctl disable multifactor-radius  
sudo rm /etc/systemd/system/multifactor-radius.service  
sudo systemctl daemon-reload
```

- Перейти в **«/opt/multifactor/radius/multifactor-radius-adapter.dll.config»** используя команду **«sudo nano /opt/multifactor/radius/multifactor-radius-adapter.dll.config»** и изменить порт в поле **«adapter-server-endpoint»**.

7 МАРШРУТИЗАЦИЯ

7.1 Маршрутизация

7.1.1 Настройка статического маршрута

Для настройки статического маршрута необходимо ввести следующую команду:

```
set protocols static route <x.x.x.x/x> next-hop <x.x.x.x>
```

где:

- **<x.x.x.x/x>** – IPv4-адрес сети;
- **<x.x.x.x>** – IPv4-адрес.

Например:

```
set protocols static route 172.16.43.0/24 next-hop 172.16.43.1
```

Поддерживается возможность настройки нескольких статических маршрутов.

Для указания дистанции для маршрута необходимо ввести следующую команду:

```
set protocols static route <x.x.x.x/x> next-hop <x.x.x.x> distance <num>
```

где **<num>** – значение дистанции. Возможно указание значения в диапазоне от «1» до «255».

Маршрут с присвоенным значением дистанции «1» будет иметь наивысший приоритет.

По умолчанию используется значение «1».

Для отключения статического маршрута необходимо ввести следующую команду:

```
set protocols static route <x.x.x.x/x> next-hop <x.x.x.x> disable
```

Для настройки статического маршрута IPv6 необходимо ввести следующую команду:

```
set protocols static route6 <h:h:h:h:h:h:h/x> next-hop <h:h:h:h:h:h:h>
```

где:

- **«route6»** – указывает на формат IPv6;
- **<h:h:h:h:h:h:h/x>** – IPv6-адрес сети;
- **<h:h:h:h:h:h:h>** – IPv6-адрес.

7.1.2 Настройка интерфейсного маршрута

Для настройки маршрута на основе интерфейса необходимо ввести следующую команду:

```
set protocols static route <x.x.x.x/x> interface <name>
```

где:

- **<x.x.x.x/x>** – IPv4-адрес сети;
- **<name>** – имя интерфейса, на который будет направлен трафик указанной сети.

Возможно указание IPv6-адреса сети:

```
set protocols static route6 <h:h:h:h:h:h:h/x> interface <name>
```

Для указания дистанции для маршрута на основе интерфейса необходимо ввести следующую команду:

```
set protocols static route <x.x.x.x/x> interface <name> distance <num>
```

где **<num>** – значение дистанции. Возможно указание значения в диапазоне от «1» до «255».

Маршрут с присвоенным значением дистанции «1» будет иметь наивысший приоритет.

По умолчанию используется значение «1».

Для отключения маршрута на основе интерфейса необходимо ввести следующую команду:

```
set protocols static route <x.x.x.x/x> interface <name> disable
```

Примечание:

Для обеспечения функционирования интерфейсной маршрутизации необходимо включить прокси ARP на используемом интерфейсе во всех задействованных **ARMA Стена**:

```
set interfaces ethernet <ethX> ip enable-proxy-arp
```

7.1.3 Настройка тупикового маршрута

Тупиковые маршруты используются для отбрасывания пакетов, направленных в сеть через внешний интерфейс.

Для настройки тупикового маршрута необходимо ввести следующую команду:

```
set protocols static route <x.x.x.x/x> blackhole
```

Для указания дистанции для тупикового маршрута необходимо ввести следующую команду:

```
set protocols static route <x.x.x.x/x> blackhole distance <num>
```

где **<num>** – значение дистанции. Возможно указание значения в диапазоне от «1» до «255».

Маршрут с присвоенным значением дистанции «1» будет иметь наивысший приоритет.

7.1.4 Настройка статической записи ARP

Для настройки ARP-маршрута необходимо ввести следующую команду:

```
set protocols static arp interface <name> address <x.x.x.x> mac <xx.xx.xx.xx.xx>
```

где **<xx.xx.xx.xx.xx>** – MAC-адрес.

7.2 Отказоустойчивая маршрутизация

Отказоустойчивая маршрутизации обеспечивает непрерывность работы сети при выходе из строя одного или нескольких маршрутизаторов. Непрерывность достигается за счет резервирования маршрутов и автоматического переключения на резервные пути в случае сбоя, что минимизирует время простоя и поддерживает доступность сети.

7.2.1 Добавление маршрута

1. Для добавления шлюза необходимо ввести следующую команду:

```
set protocols failover route <x.x.x.x/x> next-hop <x.x.x.x>
```

где:

- **<x.x.x.x/x>** – IPv4-адрес сети;
- **<x.x.x.x>** – IPv4-адрес шлюза.

Например:

```
set protocols failover route 192.168.100.0/24 next-hop 192.168.100.1
```

Поддерживается возможность настройки нескольких шлюзов.

2. Для указания, какой интерфейс следует использовать для доступа к указанному шлюзу, необходимо ввести следующую команду:

```
set protocols failover route <x.x.x.x/x> next-hop <x.x.x.x> interface <name>
```

где **<name>** – имя интерфейса, который будет использоваться для доступа к шлюзу.

3. Для указания, что шлюз находится в прямой видимости, необходимо ввести следующую команду:

```
set protocols failover route <x.x.x.x/y> next-hop <x.x.x.x> onlink
```


Примечание:

Адрес назначения считается доступным напрямую, если целевой адрес находится в той же подсети, что и отправитель, и пакет может быть передан непосредственно на этот адрес без использования маршрутизации.

4. Для настройки метрики маршрута необходимо ввести следующую команду:

```
set protocols failover route <x.x.x.x/y> next-hop <x.x.x.x> metric <metric>
```

где **<metric>** – значение метрики. Допускаются целые положительные числа в диапазоне от «1» до «255».

Примечание:

Если метрика шлюзов одинаковая, то маршрутизация будет выполняться в режиме балансировки. Если метрика шлюзов разная, то маршрутизация будет выполняться в режиме резервирования - чем ниже метрика, тем приоритетней маршрут.

7.2.2 Проверка доступности маршрута

1. Для добавления проверяемого узла необходимо ввести следующую команду:

```
set protocols failover route <x.x.x.x/y> next-hop <x.x.x.x> check target <x.x.x.x>
```

2. Для настройки типа проверки доступности узла необходимо ввести следующую команду:

```
set protocols failover route <x.x.x.x/y> next-hop <x.x.x.x> check type <check-type>
```

где **<check-type>** – тип проверки.

Возможно указание следующих типов проверки:

- «arp»;
- «icmp»;
- «tcp».

3. Для указания порта проверяемого узла необходимо ввести следующую команду:

```
set protocols failover route <x.x.x.x/y> next-hop <x.x.x.x> check port <port>
```

где **<port>** – порт узла. Допускаются целые положительные числа в диапазоне от «1» до «65535».

Примечание:

Порт узла обязателен для указания, если в качестве типа проверки **<check-type>** задано значение «tcp».

- Для настройки частоты проверки доступности узла необходимо ввести следующую команду:

```
set protocols failover route <x.x.x.x/y> next-hop <x.x.x.x> check timeout <timeout>
```

где **<timeout>** – частота проверки в секундах. Допускаются целые положительные числа в диапазоне от «1» до «300».

7.2.3 Пример настройки отказоустойчивой маршрутизации

В качестве примера приведена настройка отказоустойчивой маршрутизации с одним NGFW **ARMA Стена** и двумя шлюзами согласно схеме стенда, представленной на рисунке (см. [Рисунок – Схема стенда для настройки отказоустойчивой маршрутизации](#)).

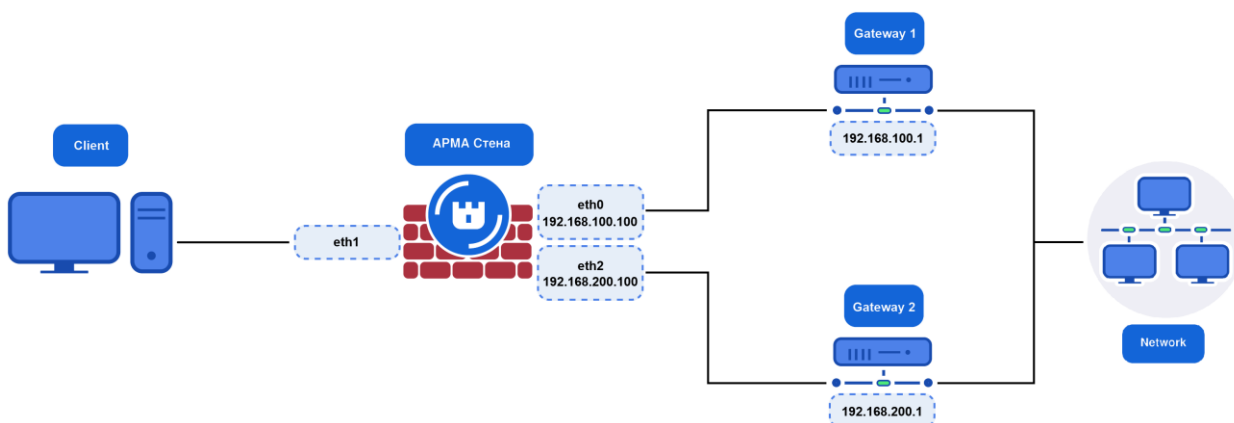


Рисунок – Схема стенда для настройки отказоустойчивой маршрутизации

Предварительная настройка

Для настройки отказоустойчивой маршрутизации необходимо предварительно задать статические маршруты, которые будут использоваться для обращения к шлюзам:

```
set protocols static route 0.0.0.0/0 next-hop 192.168.100.1 distance 210
set protocols static route 0.0.0.0/0 next-hop 192.168.200.1 distance 220

commit
save
```

Настройка маршрутов

- Для настройки маршрута к шлюзу №1 необходимо ввести список команд:

```
set protocols failover route 0.0.0.0/0 next-hop 192.168.100.1 check target  
'192.168.100.1'  
set protocols failover route 0.0.0.0/0 next-hop 192.168.100.1 check timeout '5'  
set protocols failover route 0.0.0.0/0 next-hop 192.168.100.1 check type 'icmp'  
set protocols failover route 0.0.0.0/0 next-hop 192.168.100.1 interface 'eth0'  
set protocols failover route 0.0.0.0/0 next-hop 192.168.100.1 metric '10'  
  
commit  
save
```

2. Для настройки маршрута к шлюзу №2 необходимо ввести список команд:

```
set protocols failover route 0.0.0.0/0 next-hop 192.168.200.1 check target  
'192.168.200.1'  
set protocols failover route 0.0.0.0/0 next-hop 192.168.200.1 check timeout '5'  
set protocols failover route 0.0.0.0/0 next-hop 192.168.200.1 check type 'icmp'  
set protocols failover route 0.0.0.0/0 next-hop 192.168.200.1 interface 'eth2'  
set protocols failover route 0.0.0.0/0 next-hop 192.168.200.1 metric '20'  
  
commit  
save
```

Для просмотра текущих настроек отказоустойчивой маршрутизации необходимо выполнить в эксплуатационном режиме команду «**show ip route 0.0.0.0/0**».

Для проверки работы отказоустойчивой маршрутизации необходимо любым способом ограничить доступность шлюза с наименьшей метрикой. Если пакеты продолжают передаваться через второй шлюз, то маршрутизация настроена корректно.

7.3 Протоколы маршрутизации

7.3.1 RIP

Протокол RIP является распространённым протоколом для маршрутизации внутри локальной сети. **ARMA Стена** поддерживает следующие версии протокола динамической маршрутизации RIP:

- RIPv1 – согласно спецификации «RFC 1058»;
- RIPv2 – согласно спецификации «RFC 2453».

7.3.1.1 Основные команды настройки RIP

1. Команда указания подсети для протокола RIP:

```
set protocols rip network <x.x.x.x/x>
```

2. Команда включения протокола RIP на интерфейсе:

```
set protocols rip interface <name_eth>
```

Разрешить передачу и приём пакетов RIP по интерфейсу **<name_eth>**.

3. Команда определения маршрутизатора, соседнего по RIP:

```
set protocols rip neighbor <x.x.x.x>
```

где **<x.x.x.x>** – адрес ближайшего маршрутизатора RIP.

4. Команда установки пассивного режима для указанного интерфейса:

```
set protocols rip passive-interface <name_eth>
```

В пассивном режиме все полученные пакеты интерфейсом **<name_eth>** обрабатываются как обычные. **ARMA Стена** не передаёт ни многоадресные, ни одноадресные RIP-пакеты, за исключением RIP-соседей, указанных командой **neighbor**.

5. Команда перевода всех интерфейсов в пассивный режим:

```
set protocols rip passive-interface default
```

7.3.1.2 Дополнительные команды настройки RIP

1. Команда установки административной дистанции для RIP:

```
set protocols rip default-distance <distance>
```

где **<distance>** – значение дистанции. Возможно указание значения в диапазоне от «1» до «255».

Примечание:

Маршруты с дистанцией «255» фактически не активны и не используются в **ARMA Стена**.

2. Команда указания административного расстояния до подсети RIP **<x.x.x.x/x>**:

```
set protocols rip network-distance <x.x.x.x/x> distance <distance>
```

3. Команда установки расстояния RIP по умолчанию на указанное значение, когда IP-адрес источника маршрута соответствует указанной подсети **<x.x.x.x/x>** и указанному списку доступа **<name>**:

```
set protocols rip network-distance <x.x.x.x/x> access-list <name>
```

4. Команда создания маршрута по умолчанию в область маршрутизации RIP:

```
set protocols rip default-information originate
```

5. Команда применения списка доступа **<number>** к фильтрации входящих («**in**») или исходящих («**out**») пакетов RIP:

```
set protocols rip distribute-list access-list <in|out> <number>
```

6. Команда применения списка доступа **<number>** к интерфейсу **<name_eth>** для фильтрации входящих или исходящих пакетов RIP:

```
set protocols rip distribute-list interface <name_eth> access-list <in|out> <number>
```

7. Команда применения списка префиксов **<name>** к фильтрации входящих или исходящих пакетов RIP:

```
set protocols rip distribute-list prefix-list <in|out> <name>
```

8. Команда применения списка префиксов **<name>** к интерфейсу **<name_eth>** для фильтрации входящих или исходящих пакетов RIP:

```
set protocols rip distribute-list interface <name_eth> prefix-list <in|out> <name>
```

9. Команда указания статического маршрута RIP:

```
set protocols rip route <x.x.x.x/x>
```

10. Команда установки таймера для обновления таблицы маршрутизации RIP:

```
set protocols rip timers update <seconds>
```

где **<seconds>** – значение таймера в секундах. Возможно указание значения в диапазоне от «5» до «2147483647». По умолчанию используется значение «30».

11. Команда установки таймера действия маршрута:

```
set protocols rip timers timeout <seconds>
```

где **<seconds>** – время в секундах, по истечении которого маршрут становится недействительным. Возможно указание значения в диапазоне от «5» до «2147483647». По умолчанию используется значение «180».

12. Команда установки таймера удаления недействительных маршрутов:

```
set protocols rip timers garbage-collection <seconds>
```

где **<seconds>** – время в секундах, по истечении которого недействительные маршруты удаляются из таблицы маршрутизации. Возможно указание значения в диапазоне от «5» до «2147483647». По умолчанию используется значение «120».

7.3.1.3 Команды перераспределения (redistribute) маршрутов

1. Команда перераспределения маршрутов из заданного источника в таблицу маршрутизации RIP:

```
set protocols rip redistribute <route source>
```

где **<route source>** – источник перераспределения.

Возможно указание следующих режимов источника:

- **«babel»;**
- **«bgp»;**
- **«connected»;**
- **«isis»;**
- **«kernel»;**
- **«ospf»;**
- **«static».**

2. Команда установки метрики для перераспределения маршрута из заданного источника в таблицу маршрутизации RIP:

```
set protocols rip redistribute <route source> metric <metric>
```

где **<metric>** – значение метрики. Возможно указание значения в диапазоне от «1» до «16».

3. Команда использования карт маршрутов для фильтрации перераспределённых маршрутов из заданного источника в таблицу маршрутизации RIP:

```
set protocols rip redistribute <route source> route-map <name>
```

где **<name>** – имя карты маршрутов.

4. Команда установки метрики по умолчанию для внешних маршрутов, перераспределённых на RIP:

```
set protocols rip default-metric <metric>
```

где **<name>** – значение метрики. Возможно указание значения в диапазоне «1» до «16». По умолчанию используется значение «1».

Для изменения значения метрики в подключённых маршрутах, используется команда **«redistribute connected metric»**.

7.3.1.4 Настройки интерфейсов

1. Команда выбора интерфейса, для которого в рамках протокола RIP, будет выполняться базовая аутентификация – аутентификация по паролю:

```
set protocols rip interface <intname> authentication plaintext-password <text>
```

где:

- **<intname>** – идентификатор интерфейса;
- **<text>** – пароль. Длина пароля не должна превышать «16» символов.

2. Команда указания интерфейса, для которого в рамках протокола RIP будет выполняться аутентификация по ключу MD5:

```
set protocols rip interface <intname> authentication md5 <id> password <text>
```

где:

- **<id>** – идентификатор ключа. Возможно указать значение в диапазоне от «1» до «255»;
- **<text>** – пароль. Длина пароля не должна превышать «16» символов.

3. Команда отключения на интерфейсе механизма «split horizon»:

```
set protocols rip interface <intname> split-horizon disable
```

4. Команда включения на интерфейсе механизма «poison-reverse»:

```
set protocols rip interface <intname> split-horizon poison-reverse
```

Если данный механизм работает совместно с механизмом «split horizon», операционная система анонсирует маршруты с интерфейса, с которого они были получены, как недостижимые.

5. Команда определения, какую версию протокола RIP использовать для отправки маршрутных обновлений через указанный интерфейс:

```
set protocols rip interface <intname> send version <1 | 2>
```

где **<1 | 2>** – версия протокола RIP. Возможно указать значение «1» (RIPv1) или «2» (RIPv2).

6. Команда определения, какую версию протокола RIP должен принимать указанный интерфейс при получении маршрутных обновлений:

```
set protocols rip interface <intname> receive version <1 | 2>
```

где **<1 | 2>** – версия протокола RIP. Возможно указать значение «1» (RIPv1) или «2» (RIPv2).

7.3.1.5 Команды мониторинга состояния настроек RIP

1. Команда отображения маршрутов RIP:

```
admin@ngfwos:~$ show ip rip
```

2. Команда отображения текущего состояния RIP:

```
admin@ngfwos:~$ show ip rip status
```

Выводится информация о таймере RIP, фильтрации, версии, включённом интерфейсе RIP и пире.

7.3.1.6 Пример настройки динамической маршрутизации RIP

В качестве примера приведена настройка динамической маршрутизации по протоколу RIP на трёх **ARMA Стена** согласно схеме стенда, представленной на рисунке (см. [Рисунок – Схема стенда для настройки динамической маршрутизации по протоколу RIP](#)).

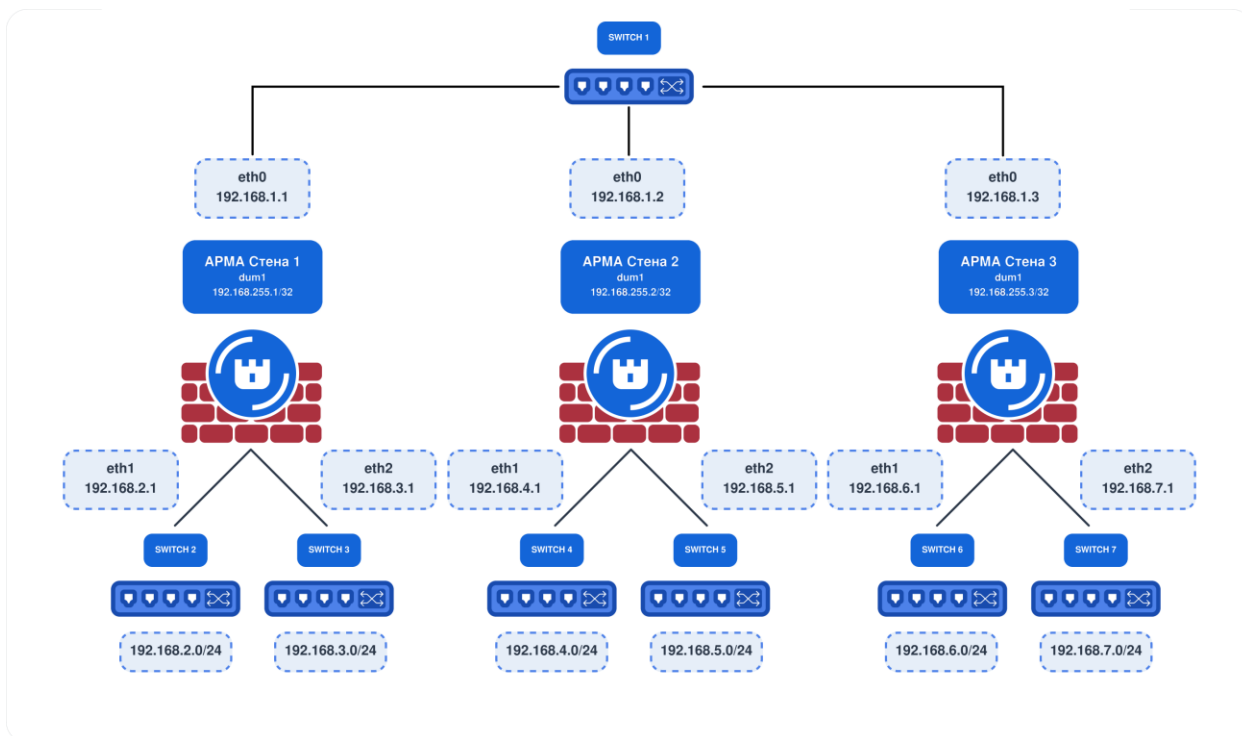


Рисунок – Схема стенда для настройки динамической маршрутизации по протоколу RIP

Перечень интерфейсов со значениями IP-адресов для каждой **ARMA Стена** приведён в таблице ([Таблица «Перечень интерфейсов»](#)):

Таблица «Перечень интерфейсов»

Интерфейс	ARMA Стена 1	ARMA Стена 2	ARMA Стена 3
eth0	192.168.1.1	192.168.1.2	192.168.1.3
eth1	192.168.2.1	192.168.4.1	192.168.6.1
eth2	192.168.3.1	192.168.5.1	192.168.7.1

Для настройки динамической маршрутизации по протоколу RIP необходимо выполнить следующие действия:

1. Для **ARMA Стена 1** необходимо ввести список команд настройки:

```
set protocols rip network 192.168.1.0/24
set protocols rip network 192.168.2.0/24
set protocols rip network 192.168.3.0/24

commit
save
```

2. Для **ARMA Стена 2** необходимо ввести список команд настройки:

```
set protocols rip network 192.168.1.0/24
set protocols rip network 192.168.4.0/24
set protocols rip network 192.168.5.0/24

commit
save
```

3. Для **ARMA Стена 3** необходимо ввести список команд настройки:

```
set protocols rip network 192.168.1.0/24
set protocols rip network 192.168.6.0/24
set protocols rip network 192.168.7.0/24

commit
save
```

Для проверки работоспособности динамической маршрутизации необходимо выполнить ping-запросы ко всем IP-адресам подсетей на устройстве «ARMA Стена 1».

7.3.2 OSPFv2

Протокол OSPFv2 работает в сетях на базе протокола IPv4.

7.3.2.1 Основные команды настройки OSPFv2

1. Команда активации протокола OSPFv2 на интерфейсе с IP-адресом, входящим в указанную сеть **<x.x.x.x/x>**:

```
set protocols ospf area <number> network <x.x.x.x/x>
```

где **<number>** – номер области. Возможно указание значения в диапазоне от «0» до «4294967295» или числа в формате IPv4-адреса **<x.x.x.x>**.

2. Команда установки полосы пропускания для расчёта стоимости канала:

```
set protocols ospf auto-cost reference-bandwidth <number>
```

где **<number>** – значение полосы пропускания в Мбит/с. Возможно указание значения в диапазоне от «1» до «4294967». По умолчанию используется значение «100».

Соединение с пропускной способностью 100 Мбит/с или более будет иметь стоимость «1». Стоимость соединений с меньшей пропускной способностью будет масштабироваться.

3. Команда установки значения идентификатора маршрутизатора для OSPFv2:

```
set protocols ospf parameters router-id <rid>
```

где **<rid>** – значение идентификатора маршрутизатора, используется IP-адрес или произвольное 32-разрядное число.

Примечание:

Идентификатор маршрутизатора должен быть уникальным в рамках всего OSPF домена. В противном случае возможно возникновение ошибок в работе OSPF.

7.3.2.2 Дополнительные команды настроек OSPFv2

1. Команда объявления о состоянии внешних каналов автономной системы (AS-External (type-5)):

```
set protocols ospf default-information originate [always] [metric <number>] [metric-type <1|2>] [route-map <name>]
```

где:

- **<number>** – значение метрики по умолчанию. Возможно указание значения в диапазоне от «0» до «16777214»;
- **<1|2>** – тип метрики OSPF для маршрутов по умолчанию. По умолчанию используется значение «2».

При указании аргумента **[always]**, сообщение распространяется всегда, даже если маршрут по умолчанию отсутствует в таблице маршрутизации.

Аргумент **[route-map <name>]** позволяет указать карту маршрутов **<name>**, при совпадении с которой будет распространяться сообщение с маршрутом по умолчанию.

2. Команда изменения значения расстояния для всего OSPF:

```
set protocols ospf distance global <distance>
```

где **<distance>** – значение расстояния. Возможно указание значения в диапазоне от «1» до «255».

3. Команда изменения значения расстояния для определённых маршрутов:

```
set protocols ospf distance ospf <external|inter-area|intra-area> <distance>
```

где:

- **<distance>** – значение расстояния. Возможно указание значения в диапазоне от «1» до «255»;
- **<external>** – внешних маршрутов;
- **<inter-area>** – маршрутов между областями;
- **<intra-area>** – маршрутов внутри области.

4. Команда регистрации изменения в смежности:

```
set protocols ospf log-adjacency-changes [detail]
```

С дополнительным аргументом **[detail]** отображаются все изменения в состоянии смежности. Без аргумента **[detail]** отображаются только полные изменения или регрессии.

5. Команды включения поддержки «RFC 3137»:

- включает поддержку «RFC 3137» на неограниченный период времени:

```
set protocols ospf max-metric router-lsa administrative
```

- включает поддержку «RFC 3137» на определённое время после запуска:

```
set protocols ospf max-metric router-lsa on-startup <seconds>
```

где **<seconds>** – время после запуска в секундах. Возможно указание значения в диапазоне от «5» до «86400».

- включает поддержку «RFC 3137» на определённое время перед выключением:

```
set protocols ospf max-metric router-lsa on-shutdown <seconds>
```

где **<seconds>** – время перед выключением в секундах. Возможно указание значения в диапазоне от «5» до «100».

6. Команда установки модели ABR:

```
set protocols ospf parameters abr-type <cisco|ibm|standard|shortcut>
```

Модель ABR:

- **<cisco>** (по умолчанию) – маршрутизатор будет считаться ABR, если он имеет несколько настроенных связей с сетями в разных областях, одна из которых является магистральной областью. Магистральная область должна быть активной. **<cisco>** используется по умолчанию;

- **<ibm>** – идентично модели «cisco», но в этом случае канал магистральной зоны не активен;
- **<standard>** – маршрутизатор имеет несколько активных связей с различными областями;
- **<shortcut>** – идентично «standard», но в этой модели маршрутизатору разрешено использовать топологию связанных областей без привлечения магистральной области для межобластных соединений.

7. Команда включения поддержки «RFC 1583»:

```
set protocols ospf parameters rfc1583-compatibility
```

8. Команда определения интерфейса **<interface>** в качестве пассивного:

```
set protocols ospf interface <interface> passive [disable]
```

Пассивный интерфейс **<interface>** сообщает свой адрес, но не выполняет протокол OSPF. **[disable]** - отключает пассивный режим.

9. Команда определения всех интерфейсов в качестве пассивных по умолчанию:

```
set protocols ospf passive-interface [disable]
```

[disable] - отключает пассивный режим.

10. Команда управления максимальным количеством путей с равнозначной стоимостью:

```
set protocols ospf maximum-paths <1-64>
```

По умолчанию используется значение «64». При установке значения параметра «1» режим ECMP будет отключён.

11. Команда установки значения порога для обновления информации в маршрутизации:

```
set protocols ospf refresh timers <seconds>
```

где **<seconds>** – пороговое значение в секундах. Возможно указание значения в диапазоне от «10» до «1800». По умолчанию используется значение «1800». Маршрутизатор автоматически обновит информацию, возраст которой превысит пороговое значение.

12. Команды настройки параметров удержания между расчётом SPF и событием, вызвавшим расчёт:

```
set protocols ospf timers throttle spf <delay|initial-holdtime|max-holdtime> <time>
```

где:

- **<delay>** – задаёт начальную задержку расписания SPF **<time>** в миллисекундах. Возможно указание значения в диапазоне от «0» до «600000». По умолчанию используется значение «200»;
- **<initial-holdtime>** – задаёт минимальное время удержания **<time>** между двумя последовательными вычислениями SPF в миллисекундах. Возможно указание значения в диапазоне от «0» до «600000». По умолчанию используется значение «1000»;
- **<max-holdtime>** – задаёт максимальное время ожидания **<time>** между двумя последовательными SPF-расчётами в миллисекундах. Возможно указание значения в диапазоне от «0» до «600000». По умолчанию используется значение «10000».

13. Команда включения синхронизации IGP-LDP для OSPF:

```
set protocols ospf ldp-sync
```

14. Команда устанавливает интервал удержания синхронизации IGP-LDP для OSPF:

```
set protocols ospf ldp-sync holddown <seconds>
```

где **<seconds>** – время ожидания в секундах. Возможно указание значения в диапазоне от «0» до «10000».

7.3.2.3 Команды настройки областей

1. Команда определяет область как тупиковую «Stub Area»:

```
set protocols ospf area <number> area-type stub
```

где **<number>** – номер области. Возможно указание значения в диапазоне от «0» до «4294967295» или числа в формате IPv4-адреса <x.x.x.x>.

2. Команда определяет область как полностью заглушенную «Totally Stub Area»:

```
set protocols ospf area <number> area-type stub no-summary
```

В дополнение к ограничениям тупиковой области, этот тип области не позволяет ABR инжектировать Network-Summary LSA 3-го типа в указанную тупиковую область. Разрешён только суммарный маршрут по умолчанию.

3. Команда устанавливает стоимость LSA по умолчанию, анонсируемых в тупиковых областях:

```
set protocols ospf area <number> area-type stub default-cost <num>
```

где **<num>** – стоимость. Возможно указание значения в диапазоне от «0» до «16777215».

4. Команда определяет область как NSSA:

```
set protocols ospf area <number> area-type nssa
```

5. Команда определяет область как «NSSA Totally Stub Area»:

```
set protocols ospf area <number> area-type nssa no-summary
```

6. Команда устанавливает стоимость по умолчанию для LSA, анонсируемых в области NSSA:

```
set protocols ospf area <number> area-type nssa default-cost <num>
```

где **<num>** – стоимость. Возможно указание значения в диапазоне от «0» до «16777215».

7. Команда указывает, будет ли данный пограничный маршрутизатор NSSA безусловно транслировать LSA 7-го типа в LSA 5-го типа:

```
set protocols ospf area <number> area-type nssa translate  
<always|candidate|never>
```

<always> – LSA 7-го типа транслируются в LSA 5-го типа независимо от состояния транслятора других пограничных маршрутизаторов NSSA;

<candidate> – маршрутизатор участвует в выборах транслятора, чтобы определить, будет ли он выполнять обязанности транслятора;

<never> – маршрутизатор не будет транслировать LSA 7-го типа в LSA 5-го типа.

8. Команда определяет, что для данной области должна использоваться аутентификация с помощью простого пароля:

```
set protocols ospf area <number> authentication plaintext-password
```

9. Команда определяет, что пакеты OSPF осуществляет аутентификацию с помощью MD5 HMAC в пределах указанной области:

```
set protocols ospf area <number> authentication md5
```

10. Команда суммирования пути из указанной области в один пакет LSA 3-го типа, анонсированный в другие области **<x.x.x.x/x>**:

```
set protocols ospf area <number> range <x.x.x.x/x> [cost <0-16777215>]
```

Команда используется только в ABR, и суммируются только маршрутные LSA 1-го типа и сетевые LSA 2-го типа.

Дополнительный аргумент **[cost <0-16777215>]** задаёт метрику агрегированного соединения, диапазон значений метрики от «0» до «16777215».

11. Команда фильтрации пути в указанной области:

```
set protocols ospf area <number> range <x.x.x.x/x> not-advertise
```

Пути из диапазона **<x.x.x.x/x>** не анонсируются в другие области.

12. Команда анонсирует в магистральную область один суммарный пакет LSA 3-го типа с информацией о маршрутизации **<y.y.y.y/y>**, если определённая область содержит хотя бы одну внутриобластную сеть из диапазона **<x.x.x.x/x>**:

```
set protocols ospf area <number> range <x.x.x.x/x> substitute <y.y.y.y/y>
```

13. Команда создания не магистральных, сокращённых маршрутов для межрайонных маршрутов:

```
set protocols ospf area <number> shortcut <default|disable|enable>
```

<default> - область **<number>** будет использоваться для короткого замыкания только в том случае, если ABR не имеет связи с магистральной областью или эта связь была потеряна;

<disable> - область **<number>** не используется ABR для сокращения маршрутов;

<enable> - область **<number>** будет использоваться для сокращения пути каждый раз, когда проходящий маршрут будет дешевле.

14. Команда обеспечивает согласованность магистральной области за счёт создания виртуальных каналов связи:

```
set protocols ospf area <number> virtual-link <x.x.x.x>
```

где **<x.x.x.x>** – идентификатор ABR, с которым устанавливается виртуальная связь. Виртуальная связь должна быть настроена на обоих маршрутизаторах.

7.3.2.4 Команды настройки интерфейсов

1. Команда включения OSPFv2 на интерфейс **<interface>** и назначения соответствующей области:

```
set protocols ospf interface <interface> area <number>
```

где **<number>** – номер области. Возможно указание значения в диапазоне от «0» до «4294967295» или числа в формате IPv4-адреса **<x.x.x.x>**.

2. Команда устанавливает пароль аутентификации OSPF на интерфейс:

```
set protocols ospf interface <interface> authentication plaintext-password <text>
```

где **<text>** – пароль, длина которого не должна превышать «8» символов.

3. Команда установки аутентификации MD5 HMAC на интерфейс:

```
set protocols ospf interface <interface> authentication md5 key-id <id> md5-key <text>
```

где:

- **<id>** – идентификатор ключа. Возможно указание значения в диапазоне от «1» до «255»;
- **<text>** – секретный ключ, используемый для создания дайджеста сообщения. Длина ключа не должна превышать «16» символов.

4. Команда установки пропускной способности интерфейса:

```
set protocols ospf interface <interface> bandwidth <number>
```

где **<number>** – значение пропускной способности интерфейса в Мбит/с. Возможно указание значения в диапазоне от «1» до «100000». Показатель используется для расчёта стоимости.

5. Команда установки стоимости соединения для интерфейса <interface>:

```
set protocols ospf interface <interface> cost <number>
```

где **<number>** – значение стоимости. Возможно указание значения в диапазоне от «1» до «65535».

6. Команда установки количества секунд для таймера отключения маршрутизатора, используемого для таймера ожидания и таймера бездействия:

```
set protocols ospf interface <interface> dead-interval <number>
```

где **<number>** – значение таймера в секундах. Возможно указание значения интервалов в диапазоне от «1» до «65535». По умолчанию используется значение «40». Значение должно быть одинаковым для всех маршрутизаторов, подключённых к общей сети.

7. Команда установки множителя сообщений Hello в секунду:

```
set protocols ospf interface <interface> hello-multiplier <number>
```

где **<number>** – значение множителя приветственных сообщений. Возможно указание значения в диапазоне от «1» до «10».

8. Команда установки количества секунд для значения таймера «Hello Interval»:

```
set protocols ospf interface <interface> hello-interval <number>
```

где **<number>** – значение интервала в секундах. Возможно указание значения в диапазоне от «1» до «65535». По умолчанию используется значение «10».

9. Команда отключения проверки значения MTU в пакетах OSPF DBD:


```
set protocols ospf interface <interface> mtu-ignore
```

10. Команда указания типа распределения для сети, подключённой к интерфейсу <interface>:

```
set protocols ospf interface <interface> network <type>
```

где **<type>** – тип распределения.

Возможно указание следующих типов распределения:

- **«broadcast»** – распределение широковещательных IP-адресов;
- **«non-broadcast»** – распределение адресов в топологии сетей NBMA;
- **«point-to-multipoint»** – распределение адресов в сетях типа «точка-многоточечная сеть»;
- **«point-to-point»** – распределение адресов в сетях «точка-точка».

11. Команда установки приоритета маршрутизатора:

```
set protocols ospf interface <interface> priority <number>
```

где **<number>** – значение приоритета. Возможно указание значения в диапазоне от «0» до «255». По умолчанию используется значение «1». При установленном значении «0» маршрутизатор не станет назначенным маршрутизатором.

12. Команда установки количества секунд для значения таймера «RxmtInterval»:

```
set protocols ospf interface <interface> retransmit-interval <number>
```

где **<number>** – значение таймера в секундах. Возможно указание значения в диапазоне от «1» до «65535». По умолчанию используется значение «5».

13. Команда установки количества секунд для значения таймера «InfTransDelay»:

```
set protocols ospf interface <interface> transmit-delay <number>
```

где **<number>** – значение таймера в секундах. Возможно указание значения в диапазоне от «1» до «65535». По умолчанию используется значение «1».

14. Команда отключения синхронизации IGP-LDP для интерфейса **<interface>**:

```
set protocols ospf interface <interface> ldp-sync disable
```

15. Команда устанавливает интервал удержания синхронизации IGP-LDP для интерфейса <interface>:

```
set protocols ospf interface <interface> ldp-sync holddown <seconds>
```

где **<seconds>** – время ожидания в секундах. Возможно указание значения в диапазоне от «0» до «10000».

7.3.2.5 Команды ручной настройки соседства маршрутизаторов в сетях NBMA

1. Команда установки IP-адреса соседнего устройства:

```
set protocols ospf neighbor <x.x.x.x>
```

где **<x.x.x.x>** – IP-адрес маршрутизатора.

2. Команда указания времени, в течение которого маршрутизатор посылает пакеты «hello» с интерфейса **<x.x.x.x>** до установления смежности с соседом:

```
set protocols ospf neighbor <x.x.x.x> poll-interval <seconds>
```

где **<seconds>** – значение времени в секундах. Возможно указание значения в диапазоне от «1» до «65535». По умолчанию используется значение «60».

3. Команда установки значения приоритета маршрутизатора для нешироковещательного соседа, связанного с IP-адресом **<x.x.x.x>**:

```
set protocols ospf neighbor <x.x.x.x> priority <number>
```

где **<number>** – значение приоритета. Возможно указание значения в диапазоне от «0» до «255» секунд. По умолчанию используется значение «0».

7.3.2.6 Команды настройки перераспределения (redistribute)

1. Команда перераспределения информации о маршруте из источника маршрута в процесс OSPF:

```
set protocols ospf redistribute <route source>
```

где **<route source>** – источник маршрутов. Возможно указание следующих режимов источника: «bgp», «connected», «kernel», «rip», «static», «babel», «isis», «table».

2. Команда установки метрики по умолчанию для перераспределённых маршрутов:

```
set protocols ospf default-metric <number>
```

где **<number>** – значение метрики. Возможно указание значения в диапазоне от «0» до «16777214».

3. Команда установки метрики для перераспределённых маршрутов из заданного источника маршрута:

```
set protocols ospf redistribute <route source> metric <number>
```

4. Команда установки типа метрики для перераспределённых маршрутов:

```
set protocols ospf redistribute <route source> metric-type <1|2>
```

где **<1|2>** – тип метрики. По умолчанию используется тип «2».

5. Команда использования карт маршрутов для фильтрации перераспределённых маршрутов из заданного источника маршрута:

```
set protocols ospf redistribute <route source> route-map <name>
```

где **<name>** – имя карты маршрутов.

7.3.2.7 Команды мониторинга состояния

1. Команда вывода краткой информации о состоянии соседних маршрутизаторов:

```
admin@ngfwos:~$ show ip ospf neighbor
```

2. Команда вывода подробной информации о состоянии соседних маршрутизаторов:

```
admin@ngfwos:~$ show ip ospf neighbor detail
```

3. Команда вывода подробной информации о состоянии определённого маршрутизатора:

```
admin@ngfwos:~$ show ip ospf neighbor <x.x.x.x>
```

где **<x.x.x.x>** – IP-адрес маршрутизатора.

4. Команда вывода подробной информации о состоянии соседних маршрутизаторов на указанном интерфейсе **<interface>**:

```
admin@ngfwos:~$ show ip ospf neighbor <interface>
```

5. Команда вывода информации о состоянии и конфигурации OSPF указанного интерфейса **<interface>** или всех интерфейсов, если интерфейс не указан:

```
admin@ngfwos:~$ show ip ospf interface [<interface>]
```

6. Команда вывода таблицы маршрутизации OSPF, определённую по последнему расчёту SPF:

```
admin@ngfwos:~$ show ip ospf route [detail]
```

С дополнительным аргументом **[detail]** будут показаны маршрутизатор-отправитель и атрибут сети каждого элемента маршрута.

7. Команда вывода таблицы путей к границам области и маршрутизаторам границ автономной системы:

```
admin@ngfwos:~$ show ip ospf border-routers
```

8. Команда вывода сводной таблицы с содержимым базы данных LSA:

```
admin@ngfwos:~$ show ip ospf database
```

9. Команда вывода содержимого базы данных для определённого типа анонсируемых соединений:

```
admin@ngfwos:~$ show ip ospf database <type>
```

где **<type>** – тип соединений. Возможно указание следующих типов: «asbr-summary», «external», «network», «nssa-external», «opaque-area», «opaque-as», «opaque-link», «router», «summary».

10. Команда вывода информации об LSA в списке «MaxAge»:

```
admin@ngfwos:~$ show ip ospf database max-age
```

7.3.2.8 Пример настройки динамической маршрутизации OSPFv2

В качестве примера приведена настройка динамической маршрутизации по протоколу OSPFv2 на трёх **ARMA Стена** согласно схеме стенда, представленной на рисунке (см. [Рисунок – Схема стенда для настройки динамической маршрутизации по протоколу OSPFv2](#)).

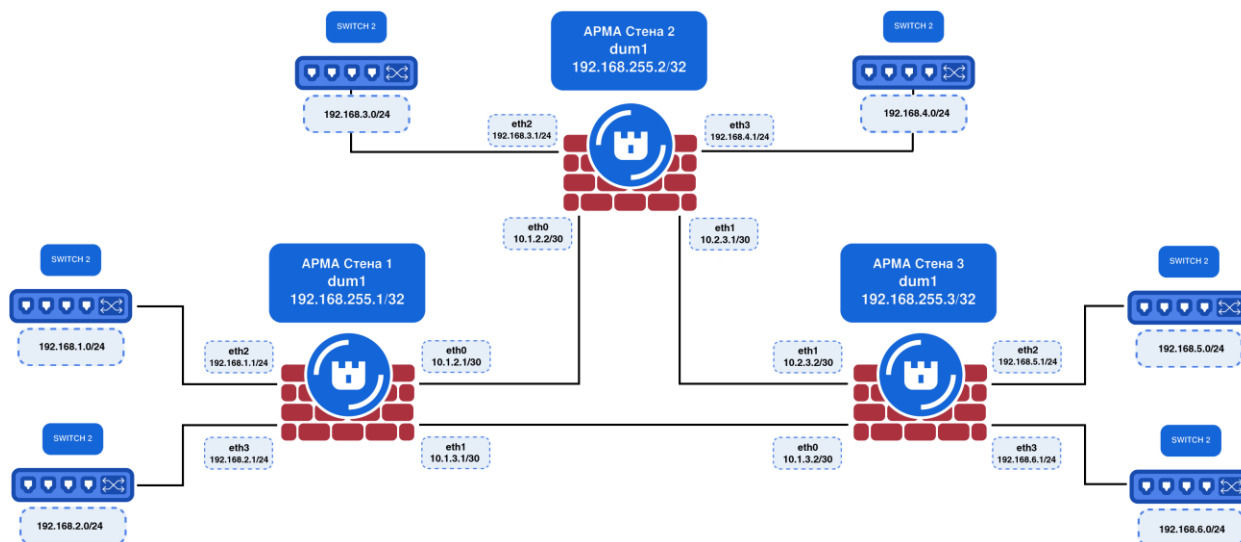


Рисунок – Схема стенда для настройки динамической маршрутизации по протоколу OSPFv2

Перечень интерфейсов со значениями IP-адресов для каждой **ARMA Стена** приведён в таблице ([Таблица «Перечень интерфейсов»](#)).

Таблица «Перечень интерфейсов»

Интерфейс	ARMA Стена 1	ARMA Стена 2	ARMA Стена 3
eth0	10.1.2.1/30	10.1.2.2/30	10.1.3.2/30
eth1	10.1.3.1/30	10.2.3.1/30	10.2.3.2/30

Интерфейс	ARMA Стена 1	ARMA Стена 2	ARMA Стена 3
eth2	192.168.1.1/24	192.168.3.1/24	192.168.5.1/24
eth3	192.168.2.1/24	192.168.4.1/24	192.168.6.1/24
dum0	192.168.255.1/32	192.168.255.2/32	192.168.255.3/32

Для настройки динамической маршрутизации по протоколу OSPFv2 необходимо выполнить следующие действия:

1. Для **ARMA Стена 1** необходимо ввести список команд настройки:

```
set interfaces ethernet eth0 address '10.1.2.1/30'
set interfaces ethernet eth1 address '10.1.3.1/30'
set interfaces ethernet eth2 address '192.168.1.1/24'
set interfaces ethernet eth3 address '192.168.2.1/24'
set interfaces dummy dum0 address 192.168.255.1/32

set protocols ospf interface dum0 area '0'
set protocols ospf interface eth0 area '0'
set protocols ospf interface eth1 area '0'
set protocols ospf interface eth2 area '0'
set protocols ospf interface eth3 area '0'
set protocols ospf interface eth0 network 'point-to-point'
set protocols ospf interface eth1 network 'point-to-point'
set protocols ospf interface eth2 passive
set protocols ospf interface eth3 passive
set protocols ospf parameters router-id '192.168.255.1'

commit
save
```

2. Для **ARMA Стена 2** необходимо ввести список команд настройки:

```
set interfaces ethernet eth0 address '10.1.2.2/30'
set interfaces ethernet eth1 address '10.2.3.1/30'
set interfaces ethernet eth2 address '192.168.3.1/24'
set interfaces ethernet eth3 address '192.168.4.1/24'
set interfaces dummy dum0 address '192.168.255.2/32'

set protocols ospf interface dum0 area '0'
set protocols ospf interface eth0 area '0'
set protocols ospf interface eth1 area '0'
set protocols ospf interface eth2 area '0'
set protocols ospf interface eth3 area '0'
set protocols ospf interface eth0 network 'point-to-point'
set protocols ospf interface eth1 network 'point-to-point'
set protocols ospf interface eth2 passive
set protocols ospf interface eth3 passive
set protocols ospf parameters router-id '192.168.255.2'

commit
save
```

3. Для **ARMA Стена 3** необходимо ввести список команд настройки:

```
set interfaces ethernet eth0 address '10.1.3.2/30'
set interfaces ethernet eth1 address '10.2.3.2/30'
set interfaces ethernet eth2 address '192.168.5.1/24'
set interfaces ethernet eth3 address '192.168.6.1/24'
set interfaces dummy dum0 address '192.168.255.3/32'

set protocols ospf interface dum0 area '0'
set protocols ospf interface eth0 area '0'
set protocols ospf interface eth1 area '0'
set protocols ospf interface eth2 area '0'
set protocols ospf interface eth3 area '0'
set protocols ospf interface eth0 network 'point-to-point'
set protocols ospf interface eth1 network 'point-to-point'
set protocols ospf interface eth2 passive
set protocols ospf interface eth3 passive
set protocols ospf parameters router-id '192.168.255.3'

commit
save
```

После завершения настройки необходимо выполнить проверку состояния соседних устройств и полученных маршрутов:

Проверка состояния соседства OSPF:

```
show ip ospf neighbor
```

Проверка маршрутов, полученных по протоколу OSPF:

```
show ip route ospf
```

7.3.3 OSPFv3

Для работы в сетях IPv6 используется протокол маршрутизации OSPFv3, большинство параметров которого аналогичны протоколу OSPFv2, работающему в сетях IPv4. Оба протокола работают на основе алгоритма SPF. OSPFv3 использует аутентификацию IPv6 по протоколу IPSec.

Процесс OSPFv3 запускается при настройке первого интерфейса с поддержкой OSPF.

7.3.3.1 Основные команды настройки OSPFv3

1. Команда указания интерфейса **<interface>** с поддержкой протокола OSPFv3:

```
set protocols ospfv3 interface <interface> area <number>
```

где **<number>** – номер области. Возможно указание значения в диапазоне от «0» до «4294967295» или числа в формате IPv4-адреса <x.x.x.x>.

2. Команда установки идентификатора маршрутизатора для процесса OSPFv3:

```
set protocols ospfv3 parameters router-id <rid>
```

где **<rid>** – идентификатор маршрутизатора. Возможно указание IP-адреса маршрутизатора или любого уникального 32-битного числа в формате <x.x.x.x>.

7.3.3.2 Дополнительные команды настройки OSPFv3

1. Команда изменения глобального административного расстояния в протоколе OSPFv3:

```
set protocols ospfv3 distance global <distance>
```

где **<distance>** – значение административного расстояния. Возможно указание значения в диапазоне от «1» до «255». По умолчанию для OSPFv3 это значение равно «110».

Административное расстояние определяет приоритет маршрутов, полученных через OSPFv3, по сравнению с маршрутами от других протоколов маршрутизации. Чем меньше значение, тем выше доверие к источнику маршрута. Изменение глобального расстояния влияет на все маршруты, полученные через OSPFv3.

2. Команды изменения значения расстояния в протоколе OSPFv3:

```
set protocols ospfv3 distance ospfv3 external <distance>  
set protocols ospfv3 distance ospfv3 inter-area <distance>  
set protocols ospfv3 distance ospfv3 intra-area <distance>
```

где:

- **<distance>** – расстояние. Возможно указание значения в диапазоне от «1» до «255»;
- **«external»** – для изменения значения расстояния внешних маршрутов;
- **«inter-area»** – для изменения значения расстояния междоменных маршрутов;
- **«intra-area»** – для изменения значения расстояния внутрименовых маршрутов.

7.3.3.3 Команды настройки области

Нижеуказанные команды суммирования и фильтрации используются только в режиме ABR.

1. Команда суммирования внутрисетевых маршрутов из указанной области в один междоменный маршрут с префиксом LSA типа 3, анонсируемый в другие зоны:

```
set protocols ospfv3 area <number> range <prefix>
```

где:

- **<number>** – номер области. Возможно указание значения в диапазоне от «0» до «4294967295» или числа в формате IPv4-адреса <x.x.x.x>;
 - **<prefix>** – префикс IPv6 в формате <h:h:h:h:h:h:h/x>.
2. Команда фильтрации внутриобластных путей из указанного диапазона, которые не объявляются в другие области:

```
set protocols ospfv3 area <number> range <prefix> not-advertise
```

7.3.3.4 Команды настройки интерфейсов

1. Команда установки стоимости соединения для интерфейса **<interface>**:

```
set protocols ospfv3 interface <interface> cost <number>
```

где **<number>** – значение стоимости соединения. Возможно указание значения в диапазоне от «1» до «65535».

Значение стоимости устанавливается в поле метрики router-LSA и используется для расчёта SPF.

2. Команда установки количества секунд для значения таймера «Dead Interval» маршрутизатора, используемого для таймера ожидания и таймера бездействия:

```
set protocols ospfv3 interface <interface> dead-interval <number>
```

где **<number>** – значение таймера в секундах. Возможно указание значения интервалов в диапазоне от «1» до «65535». По умолчанию используется значение «40». Это значение должно быть одинаковым для всех маршрутизаторов, подключённых к общей сети.

3. Команда установки количества секунд для значения таймера интервала приветствия на указанный интерфейс:

```
set protocols ospfv3 interface <interface> hello-interval <number>
```

где **<number>** – значение таймера интервала приветствия в секундах. Возможно указание значения интервалов в диапазоне от «1» до «65535». По умолчанию используется значение «10». Это значение должно быть одинаковым для всех маршрутизаторов, подключённых к общей сети.

4. Команда отключения проверки значения MTU в пакетах OSPF DBD:

```
set protocols ospfv3 interface <interface> mtu-ignore
```

Использование этой команды позволяет OSPF-связке достичь состояния FULL, даже если между двумя OSPF-маршрутизаторами имеется несоответствие MTU-интерфейса.

5. Команда указания типа рассылки для сети, подключённой к интерфейсу **<interface>**:

```
set protocols ospfv3 interface <interface> network <type>
```

где **<type>** – тип рассылки. Возможно указание следующих типов: «broadcast» – распределение широковещательных IP-адресов, «point-to-point» – распределение адресов в сетях типа «точка-точка».

6. Команда установки целочисленного значения приоритета маршрутизатора:

```
set protocols ospfv3 interface <interface> priority <number>
```

где **<number>** – значение приоритета маршрутизатора. Возможно указание значения в диапазоне от «0» до «255». По умолчанию используется значение «1».

Маршрутизатор с наивысшим приоритетом будет иметь больше возможностей стать назначенным маршрутизатором. Если установить значение «0», то маршрутизатор не будет иметь права стать назначенным маршрутизатором.

7. Команда определения интерфейса **<interface>** в качестве пассивного:

```
set protocols ospfv3 interface <interface> passive
```

Пассивный интерфейс сообщает свой адрес, но не поддерживает протокол OSPF, т.е. смежности не формируются и приветственные пакеты не генерируются.

8. Команда установки значения таймера «RxmtInterval»:

```
set protocols ospfv3 interface <interface> retransmit-interval <number>
```

где **<number>** – значение таймера в секундах. Возможно указание значения в диапазоне от «1» до «65535». По умолчанию используется значение «5».

9. Команда установки значения таймера «InfTransDelay»:

```
set protocols ospfv3 interface <interface> transmit-delay <number>
```

где **<number>** – значение таймера в секундах. Возможно указание значения в диапазоне от «1» до «65535». По умолчанию используется значение «1».

7.3.3.5 Команды настройки перераспределения (redistribution)

1. Команда перераспределения информации о маршруте из источника маршрутов в процессе OSPFv3:

```
set protocols ospfv3 redistribute <route source>
```

где **<route source>** – источник маршрута.

Возможно указание следующих режимов источника:

- «**babel**»;
- «**bgp**»;
- «**connected**»;
- «**isis**»;
- «**kernel**»;
- «**ospf**»;
- «**static**».

2. Команда установки карты маршрутов для фильтрации перераспределённых маршрутов из источника маршрутов:

```
set protocols ospf redistribute <route source> route-map <name>
```

где **<name>** – имя карты маршрутов.

7.3.3.6 Команды мониторинга состояния OSPFv3

1. Команда вывода информации о состоянии соседей:

```
admin@ngfwos:~$ show ipv6 ospfv3 neighbor
```

2. Команда вывода подробной информации о состоянии соседей:

```
admin@ngfwos:~$ show ipv6 ospfv3 neighbor detail
```

3. Команда вывода информации о состоянии и настройках OSPF для интерфейса **<interface>** или для всех интерфейсов, если интерфейс не указан:

```
admin@ngfwos:~$ show ipv6 ospfv3 interface [prefix][<interface> [prefix]]
```

Аргументом **[prefix]** выводит информацию о префиксах.

4. Команда вывода таблицы маршрутизации OSPF, определённой по последнему расчёту SPF:

```
admin@ngfwos:~$ show ipv6 ospfv3 route
```

5. Команда вывода таблицы путей к маршрутизаторам, граничащим с областью и автономной системой:

```
admin@ngfwos:~$ show ipv6 ospfv3 border-routers
```

6. Команда вывода сводной таблицы с содержимым базы данных LSA:

```
admin@ngfwos:~$ show ipv6 ospfv3 database
```

7. Команда вывода содержимого базы данных для определённого типа объявлений:

```
admin@ngfwos:~$ show ipv6 ospfv3 database <type> [x.x.x.x] [adv-router  
<x.x.x.x>|self-originate]
```

8. Команда вывода информации о перераспределённых маршрутах в OSPFv3:

```
admin@ngfwos:~$ show ipv6 ospfv3 redistribute
```

7.3.4 BGPv4

ARMA Стена использует протокол BGP версии 4. BGP поддерживает идентификатор семейства адресов для IPv4 и IPv6.

Одним из основных элементов протокола BGPv4 является ASN. BGP использует номер AS для определения того, является ли BGP-соединение внутренним или внешним. Процесс BGPv4 запускается при настройке первого BGP-соседа.

Команда установки номера локальной автономной системы, которую представляет маршрутизатор:

```
set protocols bgp system-as <asn>
```

где **<asn>** – номер AS.

7.3.4.1 Команды настройки BGP соседства

7.3.4.1.1 Определение BGP соседства

1. Команда создания нового соседа:

```
set protocols bgp neighbor <address|interface> remote-as <asn>
```

где **<address|interface>** – адрес соседа в формате: IPv4-адреса, IPv6-адреса или в виде имени интерфейса, который будет использоваться для соединения.

2. Команда создания нового соседа:

```
set protocols bgp neighbor <address|interface> remote-as internal
```

В соединении будет отказано в случае, если ASN соседа будет отличаться от собственного.

3. Команда создания нового соседа:

```
set protocols bgp neighbor <address|interface> remote-as external
```

В соединении будет отказано в случае, если ASN соседа совпадёт с собственным.

4. Команда определения конфигурации однонаправленных маршрутов для BGP:

```
set protocols bgp neighbor <address|interface> address-family <ipv4-unicast|ipv6-unicast>
```

где:

- **<ipv4-unicast>** – установление соседства по протоколу IPv4;
- **<ipv6-unicast>** – установление соседства по протоколу IPv6.

5. Команда назначения локальной роли BGP:

```
set protocols bgp neighbor <address|interface> local-role <role> [strict]
```

где **<role>** – локальная роль.

Возможно указание следующих ролей:

- **«customer»;**
- **«peer»;**
- **«provider»;**
- **«rs-client»;**
- **«rs-server».**

При использовании аргумента **[strict]** сеанс BGP не будет установлен, пока сосед BGP не установит локальную роль на своей стороне.

Основные пары ролей:

- **Provider – Customer;**
- **Peer – Peer;**
- **RS-Server – RS-Client.**

6. Команда отключения соседа или группы соседей BGP:

```
set protocols bgp neighbor <address|interface> shutdown
```

Для активации соседа BGP необходимо использовать контекст **«delete»** для данной команды.

7. Команда создания описания для соседа или группы соседей BGP:

```
set protocols bgp neighbor <address|interface> description <text>
```

8. Команда для указания адреса отправителя, который будет использоваться для BGP сессии с этим соседом:

```
set protocols bgp neighbor <address|interface> update-source <address|interface>
```

7.3.4.1.2 Согласование возможностей BGP соседства

1. Команда динамического обновления списка доступных функций в установленной BGP-сессии:

```
set protocols bgp neighbor <address|interface> capability dynamic
```

2. Команда установки разрешения для протокола BGP согласовывать расширенные возможности «nexthop» со своим соседом:

```
set protocols bgp neighbor <address|interface> capability extended-nexthop
```

3. Команда запрета отправки соседу сообщения «Capability Negotiation» в качестве необязательного параметра сообщения для установления соседства:

```
set protocols bgp neighbor <address|interface> disable-capability-negotiation
```

Команда действует только в случае, если для соседа задана конфигурация, отличная от одноадресной конфигурации IPv4.

Данная функция не позволяет использовать определённые функции протокола BGP, такие как: использование нумерованных интерфейсов, поддержка имён хостов, использование четырёхбайтных номеров АС, задание нескольких путей для одного и того же префикса, обновление маршрутов, фильтрация маршрутной информации, динамический список функций, плавный перезапуск.

4. Команда переопределяет результат согласования функций с помощью локальной конфигурации:

```
set protocols bgp neighbor <address|interface> override-capability
```

В этом случае список функций удалённого соседа BGP игнорируется.

5. Команда установки строгого сравнения списка доступных функций удалённого и локального соседей:

```
set protocols bgp neighbor <address|interface> strict-capability-match
```

Если список функций отличается, формируется ошибка «Unsupported Capability», а затем происходит сброс соединения.

7.3.4.1.3 Настройка параметров для BGP соседей

1. Команда для принятия входящего маршрута с AS-путём, содержащим AS-номер с тем же значением, что и текущая AS система:

```
set protocols bgp neighbor <address|interface> address-family <ipv4-unicast|ipv6-unicast> allowas-in number <number>
```

где **<number>** – количество допустимых вхождений системного AS-номера в AS-пути. Возможно указание значения в диапазоне от «1» до «10».

2. Команда замены AS-номера маршрутизатора-источника на локальный AS-номер:

```
set protocols bgp neighbor <address|interface> address-family <ipv4-unicast|ipv6-unicast> as-override
```

3. Команда определения атрибутов, которые должны оставаться неизменными при объявлении соседу или группе соседей BGP:

```
set protocols bgp neighbor <address|interface> address-family <ipv4-unicast|ipv6-unicast> attribute-unchanged <as-path|med|next-hop>
```

4. Команда установки максимального количества префиксов, которые возможно получить от указанного соседа BGP:

```
set protocols bgp neighbor <address|interface> address-family <ipv4-unicast|ipv6-unicast> maximum-prefix <number>
```

где **<number>** – число префиксов. Возможно указание значения в диапазоне от «1» до «4294967295».

Если указанное количество будет превышено, то BGP-сессия будет сброшена.

5. Команда для принуждения BGP-соседа, являющегося источником анонсов, сообщать о себе как о следующем узле для анонсируемого в адрес своего соседа маршрута:

```
set protocols bgp neighbor <address|interface> address-family <ipv4-unicast|ipv6-unicast> nexthop-sel
```

6. Команда удаления частных номеров ASN для маршрутов, анонсируемых сконфигурированному соседу:

```
set protocols bgp neighbor <address|interface> address-family <ipv4-unicast|ipv6-unicast> remove-private-as
```

7. Команда для определения, что обновления маршрутов, полученные от указанного соседа, будут храниться без изменений, независимо от входящей политики:

```
set protocols bgp neighbor <address|interface> address-family <ipv4-unicast|ipv6-unicast> soft-reconfiguration inbound
```

Примечание:

Для хранения обновлений маршрутов используется оперативная память. Если включить плавное внесение изменений в конфигурацию входящих маршрутов для нескольких соседей, объем используемой памяти может значительно возрасти.

8. Команда установки значения веса по умолчанию для маршрутов соседа:

```
set protocols bgp neighbor <address|interface> address-family <ipv4-unicast|ipv6-unicast> weight <number>
```

где **<number>** – вес. Возможно указание значения в диапазоне от «1» до «65535».

9. Команда установки минимального интервала между анонсами маршрутов для соседа:

```
set protocols bgp neighbor <address|interface> advertisement-interval <seconds>
```

где **<seconds>** – интервал в секундах. Возможно указание значения в диапазоне от «0» до «600». По умолчанию используется значение «0».

10. Команда для соединения между собой напрямую подключённых eBGP соседей с использованием Loopback адресов и без корректировки времени жизни TTL, которое по умолчанию равно «1»:

```
set protocols bgp neighbor <address|interface> disable-connected-check
```

11. Команда для определения, что атрибут «Community» не должен передаваться в обновлениях маршрутов, адресованных соседу:

```
set protocols bgp neighbor <address|interface> disable-send-community  
<extended|standard>
```

По умолчанию атрибут «Community» передаётся.

12. Команда установки соединения с eBGP соседями, даже если они находятся на удалении в несколько пересылок между узлами сети:

```
set protocols bgp neighbor <address|interface> ebgp-multihop <number>
```

где **<number>** – количество пересылок между узлами сети. Возможно указание значения в диапазоне от «1» до «255».

13. Команда установки альтернативного AS для BGP процесса при взаимодействии с указанным соседом или группой соседей:

```
set protocols bgp neighbor <address|interface> local-as <asn> [no-prepend]  
[replace-as]
```

Если указан аргумент **[no-prepend]**, то заданное значение параметра «local-as» не добавляется к входящему значению AS-Path.

Если указан аргумент **[replace-as]**, то при передаче обновлений локальных маршрутов соседу к значению AS-Path добавляется только заданное значение параметра «local-as».

Примечание:

Вышеуказанная команда применима только для eBGP соседей.

14. Команда настройки узла в качестве источника BGP анонсов:

```
set protocols bgp neighbor <address|interface> passive
```

Узел принимает только входящие соединения, но не инициирует исходящие соединения к соседу или группе соседей.

15. Команда установки пароля для TCP-сокета, кодированного алгоритмом MD5, используемого для соединения с удалённым соседом:

```
set protocols bgp neighbor <address|interface> password <text>
```

где **<text>** – MD5 пароль.

16. Команда реализации механизма безопасности GTSM согласно спецификации «RFC 5082»:

```
set protocols bgp neighbor <address|interface> ttl-security hops <number>
```


где **<number>** – количество пересылок между узлами сети. Возможно указание значения в диапазоне от «1» до «255».

7.3.4.1.4 Настройка группы BGP соседей

Объединение соседей в группы используется для улучшения масштабирования за счёт генерации одинаковой информации об обновлениях для всех членов группы. Соседи, не связанные ни с одной группой, воспринимаются как принадлежащие к группе соседей по умолчанию, и будут использовать общие обновления.

1. Команда для определения новой группы соседей:

```
set protocols bgp peer-group <name>
```

где **<name>** – имя новой группы.

2. Команда для связи определённой группы соседей с заданным именем:

```
set protocols bgp neighbor <address|interface> peer-group <name>
```

7.3.4.1.5 Настройка сетевых объявлений BGP

1. Команда для анонсирования сетей IPv4 или IPv6:

```
set protocols bgp address-family <ipv4-unicast|ipv6-unicast> network <prefix>
```

где **<prefix>** – значение префикса в формате: для IPv4 - <x.x.x.x>, для IPv6 - <h:h:h:h:h:h:h/x>.

Примечание:

По умолчанию префикс BGP анонсируется, даже если он отсутствует в таблице маршрутизации.

2. Команда изменения поведения оператора network:

```
set protocols bgp parameters network-import-check
```

3. Команда для анонсирования маршрута по умолчанию «0.0.0.0/0», который изначально не анонсируется, даже если он присутствует в таблице маршрутизации:

```
set protocols bgp neighbor <address|interface> address-family <ipv4-unicast|ipv6-unicast> default-originate [route-map <name>]
```

При использовании дополнительного аргумента **[route-map <name>]**, маршрут по умолчанию передаётся указанному соседу, если выполняются условия в карте маршрута **<name>**.

7.3.4.1.6 Настройка агрегации маршрутов

1. Команда установки агрегированного адреса:

```
set protocols bgp address-family <ipv4-unicast|ipv6-unicast> aggregate-address  
<prefix>
```

Маршрутизатор будет анонсировать более длинные префиксы внутри агрегированного адреса.

2. Команда установки агрегированного адреса с математическим набором автономных систем:

```
set protocols bgp address-family <ipv4-unicast|ipv6-unicast> aggregate-address  
<prefix> as-set
```

Команда суммирует атрибуты AS-Path для всех отдельных маршрутов.

3. Команда установки агрегированного адреса и обеспечения подавления более длинных префиксов внутри агрегированного адреса перед отправкой обновлений BGP соседям:

```
set protocols bgp address-family <ipv4-unicast|ipv6-unicast> aggregate-address  
<prefix> summary-only
```

4. Команда применения определённой карты маршрутов для выборочного исключения префиксов, подавленных в процессе суммирования:

```
set protocols bgp neighbor <address|interface> address-family <ipv4-unicast|ipv6-  
unicast> unsuppress-map <name>
```

7.3.4.1.7 Настройка перераспределения (redistribution)

1. Команда перераспределения маршрутной информации от указанного источника в процесс BGP:

```
set protocols bgp address-family <ipv4-unicast|ipv6-unicast> redistribute <route  
source>
```

где **<route source>** – источник маршрутов. Доступны следующие режимы источника: «babel», «connected», «isi», «kernel», «ospf», «rip», «static», «table».

2. Команда установки метрики MED для перераспределённых маршрутов:

```
set protocols bgp address-family <ipv4-unicast|ipv6-unicast> redistribute <route  
source> metric <number>
```

где **<number>** – метка MED. Возможно указание значения в диапазоне от «1» до «4294967295».

3. Команда использования карты маршрута для фильтрации перераспределённых маршрутов:

```
set protocols bgp address-family <ipv4-unicast|ipv6-unicast> redistribute <route source> route-map <name>
```

7.3.4.2 Базовые настройки BGP

7.3.4.2.1 Общие параметры

1. Команда установки идентификатора маршрутизатора router-ID:

```
set protocols bgp parameters router-id <x.x.x.x>
```

2. Команда установки максимального количества параллельных маршрутов, которое может поддерживаться процессом BGP:

```
set protocols bgp address-family <ipv4-unicast|ipv6-unicast> maximum-paths <ebgp|ibgp> <number>
```

где **<number>** – число параллельных маршрутов. Возможно указание значения в диапазоне от «1» до «256». При установке значения параметра «1» режим ECMP будет отключён.

3. Команда для включения логирования событий, содержащих информацию об изменении доступности соседей и причине сброса:

```
set protocols bgp parameters log-neighbor-changes
```

4. Команда отключения отражения маршрутов между клиентами:

```
set protocols bgp parameters no-client-to-client-reflection
```

5. Команда для отключения немедленного сброса сессий при отказе канала связи с соседом:

```
set protocols bgp parameters no-fast-external-failover
```

7.3.4.2.2 Административная дистанция

1. Команда изменения значения административной дистанции в BGP:

```
set protocols bgp parameters distance global <external|internal|local> <distance>
```

где **<distance>** – административная дистанция. Возможно указание значения в диапазоне от «1» до «255».

2. Команда изменения значения административной дистанции для указанного маршрута:

```
set protocols bgp parameters distance prefix <x.x.x.x/x> distance <distance>
```

7.3.4.2.3 Настройка таймеров

1. Команда установки времени удержания маршрутов в секундах:

```
set protocols bgp timers holdtime <seconds>
```

где **<seconds>** – значение таймера в секундах, диапазон - от «1» до «65535». По умолчанию используется значение «180».

Если указано значение «0», то удержание маршрутов не происходит.

2. Команда установки времени жизни маршрутов в секундах:

```
set protocols bgp timers keepalive <seconds>
```

где **<seconds>** – значение таймера в секундах, диапазон - от «1» до «65535». По умолчанию используется значение «60».

7.3.4.3 Мониторинг BGP

1. Команда вывода всех записей в таблице маршрутизации BGP:

```
admin@ngfwos:~$ show <ip|ipv6> bgp
```

2. Команда вывода информации об указанной записи в таблице маршрутизации BGP:

```
admin@ngfwos:~$ show <ip|ipv6> bgp <address|prefix>
```

3. Команда вывода списка маршрутов с бесклассовой междоменной маршрутизацией:

```
admin@ngfwos:~$ show ip bgp cidr-only
```

4. Команда вывода списка маршрутов, разрешённые списком сообществ BGP:

```
admin@ngfwos:~$ show <ip|ipv6> bgp community-list <name>
```

где **<name>** – идентификатор списка. Возможно указание имени списка или значения в диапазоне от «1» до «500».

5. Команда вывода списка маршрутов BGP, разрешённых указанным списком доступа AS-Path:

```
admin@ngfwos:~$ show ip bgp filter-list <name>
```

где **<name>** – имя списка доступа AS-Path.

6. Команда вывода списка маршрутов BGP, анонсируемых соседу:

```
admin@ngfwos:~$ show <ip|ipv6> bgp neighbors <address> advertised-routes
```

где **<address>** – имя соседа.

Примечание:

В системе существует упрощённая команда «show bgp neighbors <address> advertised-routes», без указания семейства адресов (ip или ipv6). Однако на текущий момент данная команда работает некорректно и её использование *не рекомендуется*. Для получения корректных данных необходимо явно указывать семейство протокола – ip для IPv4 или ipv6 для IPv6.

7. Команда вывода списка маршрутов BGP, полученных от указанного соседа, до применения политики входящих соединений:

```
admin@ngfwos:~$ show <ip|ipv6> bgp neighbors <address> received-routes
```

Примечание:

Для вывода списка маршрутов BGP необходимо предварительно сконфигурировать команду:

```
set protocols bgp neighbor <address|interface> address-family <ipv4-unicast|ipv6-unicast> soft-reconfiguration inbound
```

8. Команда вывода списка маршрутов BGP, полученных от указанного соседа после применения фильтрации:

```
admin@ngfwos:~$ show <ip|ipv6> bgp neighbors <address> routes
```

9. Команда вывода состояния всех BGP соединений:

```
admin@ngfwos:~$ show <ip|ipv6> bgp summary
```

10. Команда сброса всех BGP соединений на маршрутизаторе:

```
admin@ngfwos:~$ reset ip bgp all
```

11. Команда сброса всех внешних BGP соседства для маршрутизатора:

```
admin@ngfwos:~$ reset ip bgp external
```

7.3.4.4 Пример настройки протокола BGP

В качестве примера приведена настройка динамической маршрутизации по протоколу BGP на трёх **ARMA Стена** согласно схеме стенда, представленной на рисунке (см. [Рисунок – Схема стенда для настройки динамической маршрутизации по протоколу BGP](#)).

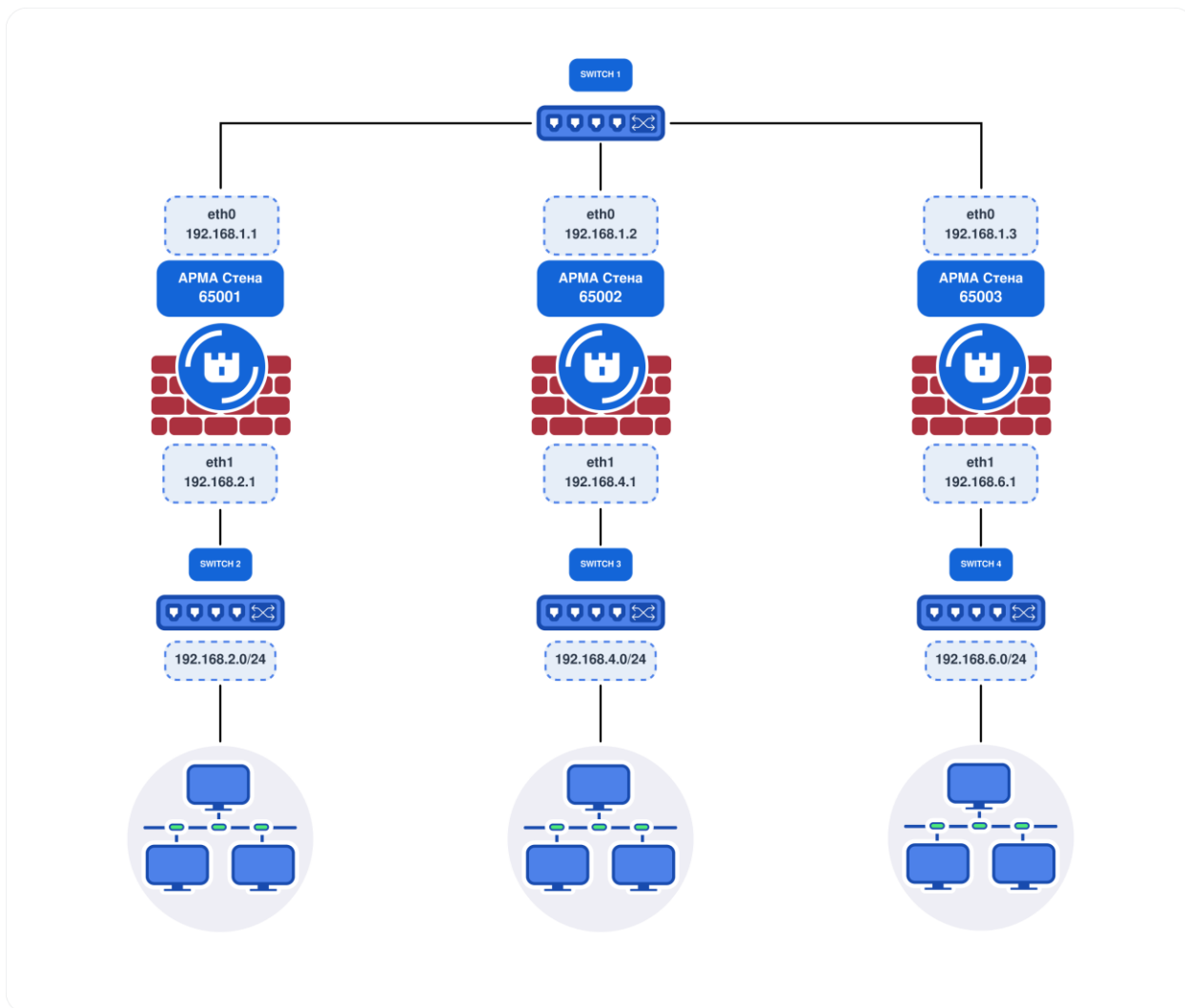


Рисунок – Схема стенда для настройки динамической маршрутизации по протоколу BGP

Перечень интерфейсов со значениями IP-адресов для каждой **ARMA Стена** приведён в таблице ([Таблица «Перечень интерфейсов»](#)).

Таблица «Перечень интерфейсов»

Интерфейс	ARMA Стена 1	ARMA Стена 2	ARMA Стена 3
eth0	192.168.1.1	192.168.1.2	192.168.1.3
eth1	192.168.2.1	192.168.4.1	192.168.6.1

Для настройки динамической маршрутизации по протоколу BGP необходимо выполнить следующие действия:

1. Для **ARMA Стена 1** необходимо ввести список команд настройки:

```
set protocols bgp system-as 65001
set protocols bgp neighbor 192.168.1.2 remote-as 65002
set protocols bgp neighbor 192.168.1.3 remote-as 65003
set protocols bgp neighbor 192.168.1.2 address-family ipv4-unicast
set protocols bgp neighbor 192.168.1.3 address-family ipv4-unicast
set protocols bgp address-family ipv4-unicast network 192.168.2.0/24

commit
save
```

2. Для **ARMA Стена 2** необходимо ввести список команд настройки:

```
set protocols bgp system-as 65002
set protocols bgp neighbor 192.168.1.1 remote-as 65001
set protocols bgp neighbor 192.168.1.3 remote-as 65003
set protocols bgp neighbor 192.168.1.1 address-family ipv4-unicast
set protocols bgp neighbor 192.168.1.3 address-family ipv4-unicast
set protocols bgp address-family ipv4-unicast network 192.168.4.0/24

commit
save
```

3. Для **ARMA Стена 3** необходимо ввести список команд настройки:

```
set protocols bgp system-as 65003
set protocols bgp neighbor 192.168.1.1 remote-as 65001
set protocols bgp neighbor 192.168.1.2 remote-as 65002
set protocols bgp neighbor 192.168.1.1 address-family ipv4-unicast
set protocols bgp neighbor 192.168.1.2 address-family ipv4-unicast
set protocols bgp address-family ipv4-unicast network 192.168.6.0/24

commit
save
```

Для проверки работоспособности динамической маршрутизации необходимо выполнить ping-запросы ко всем IP-адресам BGP-соседей на устройстве **ARMA Стена**.

7.4 ECMP

ECMP (Equal-Cost Multi-Path routing) – это механизм маршрутизации, который позволяет передавать пакеты к одному и тому же адресату по нескольким маршрутам, имеющим одинаковую метрику и рассматриваемым как равнозначные с точки зрения их стоимости. В отличие от методов выбора единственного оптимального маршрута или использования маршрутов с различными метриками,

ECMP обеспечивает балансировку нагрузки путём равномерного распределения трафика между всеми доступными равнозначными маршрутами. Такой подход способствует более эффективному использованию сетевых ресурсов, увеличению пропускной способности и повышению отказоустойчивости за счёт автоматического переключения на резервные маршруты в случае выхода из строя одного из них.

На представленной схеме стенда (см. [Рисунок – Схема сети](#)) устройство **ARMA Стена** функционирует в качестве шлюза для внутренней сети. Интерфейсы **eth0** и **eth1** подключены к внешнему маршрутизатору, обеспечивающему выход в интернет. Интерфейс **eth2** соединён с локальной сетью предприятия. Клиентское устройство, расположенное во внутренней сети, использует **ARMA Стену** в качестве шлюза по умолчанию.

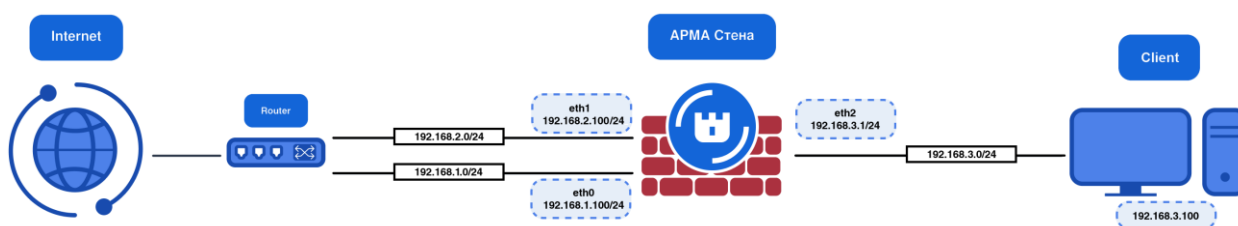


Рисунок – Схема сети

Конфигурация устройства ARMA Стена

```
# Настройка IP-адресов интерфейсов:
set interfaces ethernet eth0 address '192.168.1.100/24'
set interfaces ethernet eth1 address '192.168.2.100/24'
set interfaces ethernet eth2 address '192.168.3.1/24'

# Создание группы интерфейсов для NAT:
set firewall group interface-group WAN interface 'eth0'
set firewall group interface-group WAN interface 'eth1'

# Настройка Source NAT (masquerade):
set nat source rule 10 outbound-interface group 'WAN'
set nat source rule 10 translation address 'masquerade'

# Настройка статических маршрутов по умолчанию с использованием ECMP:
set protocols static route 0.0.0.0/0 next-hop 192.168.1.1
set protocols static route 0.0.0.0/0 next-hop 192.168.2.1
```

Указание нескольких next-hop для префикса 0.0.0.0/0 с одинаковой метрикой активирует механизм **ECMP**. Трафик к внешним сетям будет распределяться между двумя каналами связи через eth0 и eth1.

Конфигурация клиентского устройства

На клиентском устройстве необходимо задать следующие параметры сети (см. [Рисунок – Конфигурация IP-адреса и DNS](#)):

- IP-адрес 192.168.3.100/24;
- маску подсети: 255.255.255.0;
- шлюз по умолчанию: 192.168.3.1 (IP-адрес интерфейса eth2 устройства **ARMA Стена**);
- адрес DNS-сервера.

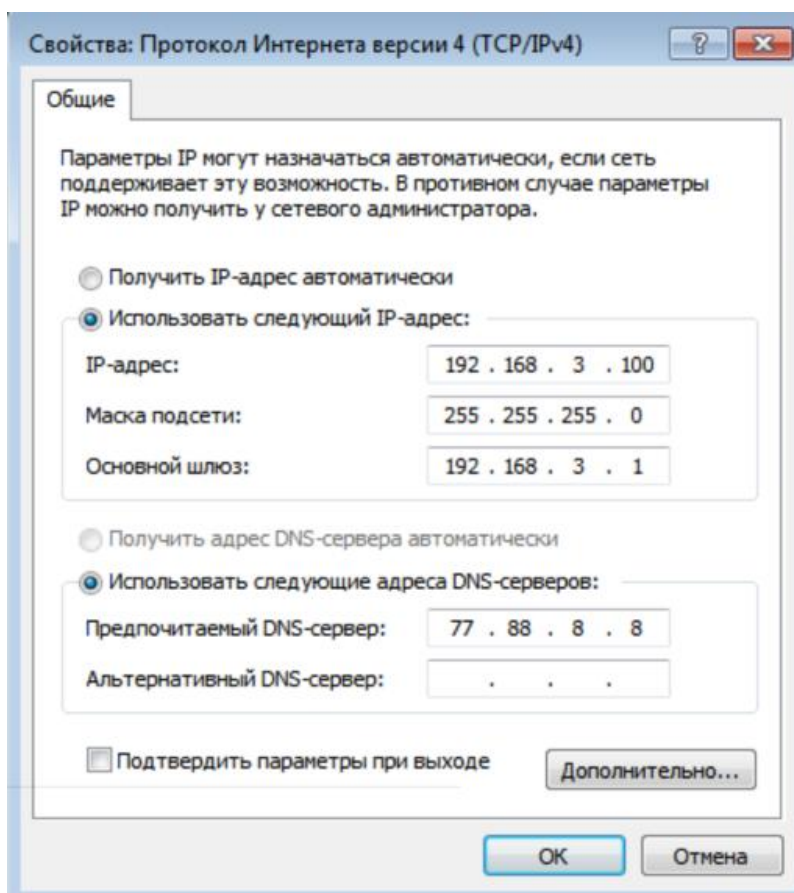


Рисунок – Конфигурация IP-адреса и DNS

Проверка работоспособности ESMР

Для верификации корректной работы механизма **ЕСМР** выполняется захват сетевого трафика на устройстве **ARMA Стена** с последующим анализом направления исходящих пакетов:

1. Запустить захват трафика на всех интерфейсах:

```
admin@ngfwos:~$ monitor traffic interface any save <file_name>
```

```
tcpdump: data link type LINUX_SLL2
```

```
tcpdump: listening on any, link-type LINUX_SLL2 (Linux cooked v2), snapshot  
length 262144 bytes
```

где **<file_name>** - название файла дампа трафика.

Примечание:

Файл с дампом трафика будет сохранён с именем «traffic_<file_name>.pcap» в каталог «/tmp/».

2. С клиентского устройства выполнить серии HTTP-запросов (например, открытие различных веб-ресурсов через браузер или использование утилиты curl).
3. После генерации достаточного объёма трафика процесс захвата необходимо остановить нажатием комбинации **клавиш «Ctrl» + «C»**. Система выведет статистику:

```
^C71496 packets captured
71767 packets received by filter
0 packets dropped by kernel
admin@ngfwos:~$
```

4. Анализ сохранённого дампа возможно произвести с помощью утилиты tcpdump:

```
admin@ngfwos:~$ sudo -i
root@ngfwos:~# tcpdump -r /home/admin/1.pcap -nn src 192.168.1.100 or
192.168.2.100
```

В выводе команды должны присутствовать пакеты с source IP «192.168.1.100» (через eth0) и «192.168.2.100» (через eth1). Наличие трафика с обоих адресов подтверждает, что **ЕСМР** активен и трафик распределяется между двумя маршрутами.

7.5 Политики фильтрации маршрутов

Политика фильтрации маршрутов – это механизм, позволяющий настраивать критерии, с которыми будет сравниваться получаемая маршрутная информация, а в случае соответствия определённому критерию – выполнять для маршрута одно или несколько действий.

В конфигурации **ARMA Стена** политики фильтрации маршрутов группируются под узлом «**policy**», который является контейнером для операторов политики. Операторы политики определяют правила, которые будут применяться к маршрутной информации.

7.5.1 Политика списка доступа

ARMA Стена позволяет выполнять фильтрацию с использованием списков ACL и списков префиксов.

ACL – список правил, определяющий доступ к объекту (программе, процессу или файлу), и какие именно операции разрешено или запрещено выполнять субъекту.

7.5.1.1 Основные команды настройки списков доступа

1. Определить список доступа:

```
set policy access-list <acl_number>
```

где **<acl_number>** – численный идентификатор списка доступа. Допустимые значения представлены в таблице (см. [Таблица «Значения идентификатора списка доступа»](#)).

Таблица «Значения идентификатора списка доступа»

Значение	Описание
<1-99>	Стандартный список доступа IPv4
<100-199>	Расширенный список доступа IPv4
<1300-1999>	Стандартный список доступа IPv4 (расширенный диапазон)
<2000-2699>	Расширенный список доступа IPv4 (расширенный диапазон)

2. Задать краткое описание списка доступа:

```
set policy access-list <acl_number> description <text>
```

где **<text>** - текстовое описание для списка доступа.

3. Создать правило списка доступа:

```
set policy access-list <acl_number> rule <rule_number>
```

где **<rule_number>** - численный идентификатор правила. Возможно указать значение в диапазоне от «1» до «65535».

4. Установить действие, которое должно быть выполнено для пакетов, соответствующих правилу списка доступа:

```
set policy access-list <acl_number> rule <rule_number> action <action>
```

где **<action>** - действие для адресов, соответствующих правилу. Возможно указать следующие значения:

- **<deny>** - пакеты, соответствующие данному правилу, игнорируются без каких-либо действий и сообщений;
- **<permit>** - пакеты, соответствующие данному правилу, передаются в дальнейшую обработку.

5. Задать краткое описание для правила списка доступа:

```
set policy access-list <acl_number> rule <rule_number> description <text>
```

6. Установить критерии соответствия в правиле списка доступа на основе получателя:

```
set policy access-list <acl_number> rule <rule_number> destination <recipient>
```

где **<recipient>** - параметры адреса назначения. Допустимые значения:

- **<any>** - соответствие для пакетов, предназначенных любому получателю;
- **<host <x.x.x.x>>** - соответствие для пакетов, предназначенных указанному узлу IPv4;
- **<inverse-mask <x.x.x.x>>** - соответствие для пакетов, предназначенных для подсетей, попадающих в указанную инвертированную маску;
- **<network <x.x.x.x/x>>** - соответствие для пакетов, предназначенных указанной подсети IPv4.

7. Установить критерии соответствия в правиле списка доступа на основе отправителя:

```
set policy access-list <acl_number> rule <rule_number> source <sender>
```

где **<sender>** - параметры адреса источника. Допустимые значения:

- **<any>** - соответствие для пакетов, приходящих от любого отправителя;
- **<host <x.x.x.x>>** - соответствие для пакетов, приходящих от указанного узла IPv4;
- **<inverse-mask <x.x.x.x>>** - соответствие для пакетов, приходящих от подсетей, попадающих в указанную инвертированную маску;
- **<network <x.x.x.x/x>>** - соответствие для пакетов, приходящих от указанной подсети IPv4.

7.5.1.2 Команды настройки списков доступа IPv6

1. Определить список доступа IPv6:

```
set policy access-list6 <acl_number>
```

где **<acl_number>** - имя списка доступа IPv6 в текстовом формате.

2. Задать краткое описание списка доступа IPv6:

```
set policy access-list6 <acl_number> description <text>
```

где **<text>** - текстовое описание для списка доступа IPv6.

3. Создать правило списка доступа IPv6:

```
set policy access-list6 <acl_number> rule <rule_number>
```

где **<rule_number>** - численный идентификатор правила. Возможно указать значение в диапазоне от «1» до «65535».

4. Установить действие, которое должно быть выполнено для пакетов, соответствующих правилу списка доступа IPv6:

```
set policy access-list6 <acl_number> rule <rule_number> action <action>
```

где **<action>** - действие для адресов, соответствующих правилу. Возможно указать следующие значения:

- **<deny>** - пакеты, соответствующие данному правилу, игнорируются без каких-либо действий и сообщений;
- **<permit>** - пакеты, соответствующие данному правилу, передаются в дальнейшую обработку.

5. Задать краткое описание для правила списка доступа IPv6:

```
set policy access-list6 <acl_number> rule <rule_number> description <text>
```

6. Установить критерии соответствия в правиле списка доступа IPv6 на основе отправителя:

```
set policy access-list6 <acl_number> rule <rule_number> source <sender>
```

где **<sender>** - параметры адреса источника. Допустимые значения:

- **<any>** - соответствие для пакетов, приходящих от любого отправителя;
- **<inverse-mask>** - соответствие для пакетов, приходящих от одного из префиксов подсетей;
- **<network <h:h:h:h:h:h:h/x>>** - соответствие для пакетов, приходящих от указанной подсети IPv6.

7.5.2 Политика списка префиксов

Списки префиксов представляют собой наиболее эффективный инструмент фильтрации на основе префиксов. Помимо функциональности списка доступа, список IP-префиксов также включает спецификацию диапазона длин префиксов. Фильтрация префиксов выполняется с помощью «**prefix-list**» и «**prefix-list6**».

Если список IP-префиксов не задан, то разрешение применяется автоматически. Если список IP-префиксов задан, но совпадения не найдены, то применяется запрет по умолчанию.

7.5.2.1 Основные команды настройки списков префиксов

1. Определить список префиксов:

```
set policy prefix-list <prefix>
```

где **<prefix>** - текстовый идентификатор для списка префиксов.

2. Задать краткое описание списка префиксов:

```
set policy prefix-list <prefix> description <text>
```

где **<text>** - текстовое описание для списка префиксов.

3. Создать правило списка префиксов:

```
set policy prefix-list <prefix> rule <rule_number>
```

где **<rule_number>** - численный идентификатор правила. Возможно указать значение в диапазоне от «1» до «65535».

4. Установить действие, которое должно быть выполнено для пакетов, соответствующих правилу списка префиксов:

```
set policy prefix-list <prefix> rule <rule_number> action <action>
```

где **<action>** - действие для пакетов, соответствующих правилу. Возможно указать следующие значения:

- **<deny>** - пакеты, соответствующие данному правилу, игнорируются без каких-либо действий и сообщений;
- **<permit>** - пакеты, соответствующие данному правилу, передаются в дальнейшую обработку.

5. Задать краткое описание для правила списка префиксов:

```
set policy prefix-list <prefix> rule <rule_number> description <text>
```

6. Установить критерии соответствия в правиле списка префиксов на основе численного сравнения со знаком больше или равен:

```
set policy prefix-list <prefix> rule <rule_number> ge <value>
```

где **<value>** - число, представляющее префикс подсети. Данному правилу будут соответствовать префиксы подсетей, превышающие указанное число или равные ему. Возможно указать значение в диапазоне от «0» до «32».

Если префикс не указан, считается, что все префиксы подсетей соответствуют правилу.

7. Установить критерии соответствия в правиле списка префиксов на основе численного сравнения со знаком меньше или равен:

```
set policy prefix-list <prefix> rule <rule_number> le <value>
```

где **<value>** - число, представляющее префикс подсети. Данному правилу будут соответствовать префиксы подсетей, не превышающие указанное число или равные ему. Возможно указать значение в диапазоне от «0» до «32».

Если префикс не указан, считается, что все префиксы подсетей соответствуют правилу.

8. Установить критерии соответствия в правиле списка префиксов на основе подсети IPv4:

```
set policy prefix-list <prefix> rule <rule_number> prefix <x.x.x.x/x>
```

где **<x.x.x.x/x>** - подсеть IPv4.

Если подсеть не указана, считается, что все подсети соответствуют правилу.

7.5.2.2 Основные команды настройки списков префиксов IPv6

1. Определить список префиксов IPv6:

```
set policy prefix-list6 <prefix>
```

где **<prefix>** - текстовый идентификатор для списка префиксов IPv6.

2. Задать краткое описание списка префиксов IPv6:

```
set policy prefix-list6 <prefix> description <text>
```

где **<text>** - текстовое описание для списка префиксов IPv6.

3. Создать правило списка префиксов IPv6:

```
set policy prefix-list6 <prefix> rule <rule_number>
```

где **<rule_number>** - численный идентификатор правила. Возможно указать значение в диапазоне от «1» до «65535».

4. Установить действие, которое должно быть выполнено для пакетов, соответствующих правилу списка префиксов IPv6:

```
set policy prefix-list6 <prefix> rule <rule_number> action <action>
```

где **<action>** - действие для пакетов, соответствующих правилу. Возможно указать следующие значения:

- **<deny>** - пакеты, соответствующие данному правилу, игнорируются без каких-либо действий и сообщений;

- **<permit>** - пакеты, соответствующие данному правилу, передаются в дальнейшую обработку.

5. Задать краткое описание для правила списка префиксов IPv6:

```
set policy prefix-list6 <prefix> rule <rule_number> description <text>
```

6. Установить критерии соответствия в правиле списка префиксов IPv6 на основе численного сравнения со знаком больше или равен:

```
policy prefix-list6 <prefix> rule <rule_number> ge <value>
```

где **<value>** - число, представляющее префикс подсети IPv6. Данному правилу будут соответствовать префиксы подсетей, превышающие указанное число или равные ему. Возможно указать значение в диапазоне от «0» до «128».

Если префикс не указан, считается, что все префиксы подсетей соответствуют правилу.

7. Установить критерии соответствия в правиле списка префиксов IPv6 на основе численного сравнения со знаком меньше или равен:

```
set policy prefix-list6 <prefix> rule <rule_number> le <value>
```

где **<value>** - число, представляющее префикс подсети IPv6. Данному правилу будут соответствовать префиксы подсетей, не превышающие указанное число или равные ему. Возможно указать значение в диапазоне от «0» до «128».

Если префикс не указан, считается, что все префиксы подсетей соответствуют правилу.

8. Установить критерии соответствия в правиле списка префиксов на основе подсети IPv4:

```
set policy prefix-list6 <prefix> rule <rule_number> prefix <h:h:h:h:h:h/h/x>
```

где **<h:h:h:h:h:h/h/x>** - подсеть IPv6.

Если подсеть не указана, считается, что все подсети соответствуют правилу.

7.5.3 Политика маршрутной карты

Route map представляет собой мощный инструмент, который предоставляет сетевым администраторам гибкие возможности для управления трафиком.

7.5.3.1 Основные команды настройки Route map

1. Определить карты маршрутов при маршрутизации на основе политик:

```
set policy route-map <name_card>
```

где **<name_card>** - текстовый идентификатор карты маршрутов.

2. Задать краткое описание карты маршрутов:

```
set policy route-map <name_card> description <text>
```

где **<text>** - текстовое описание для карты маршрутов.

3. Создать правило карты маршрутов:

```
set policy route-map <name_card> rule <rule_number>
```

где **<rule_number>** - численный идентификатор правила. Возможно указать значение в диапазоне от «1» до «65535».

4. Установить действие, которое должно быть выполнено над пакетами, соответствующими правилу карты маршрутов:

```
set policy route-map <name_card> rule <rule_number> action <action>
```

где **<action>** - действие для пакетов, соответствующих правилу. Возможно указать следующие значения:

- **<deny>** - пакеты, соответствующие данному правилу, игнорируются без каких-либо действий и сообщений;
- **<permit>** - пакеты, соответствующие данному правилу, передаются в дальнейшую обработку.

5. Вызов другой карты маршрутов:

```
set policy route-map <name_card> rule <rule_number> call <name>
```

где **<name>** - текстовый идентификатор вызываемой карты маршрутов.

6. Вызов другого правила в текущей карте маршрутов:

```
set policy route-map <name_card> rule <rule_number> continue <rule_number>
```

где **<rule_number>** - численный идентификатор вызываемого правила.

7. Указать краткое описание правила карты маршрутов:

```
set policy route-map <name_card> rule <rule_number> description <text>
```

где **<text>** - текстовое описание правила карты маршрутов.

8. Определение условия соответствия в карте маршрутов на основе списка путей AS:

```
set policy route-map <name_card> rule <rule_number> match as-path <name>
```

где **<name>** - имя списка путей AS.

Если ни одно условие соответствия по путям AS не определено, фильтрация пакетов по пути AS не выполняется.

9. Определение условия соответствия в карте маршрутов на основе сообществ BGP:

```
set policy route-map <name_card> rule <rule_number> match community  
community-list <list_number>
```

где **<list_number>** - численный идентификатор списка сообществ BGP. Политика сообществ BGP к этому моменту должна быть уже определена.

```
set policy route-map <name_card> rule <rule_number> match community exact-  
match
```

Устанавливает режим строгого соответствия списку сообществ BGP. При использовании данного параметра обязательно должен быть определён community-list.

10. Определение условия соответствия в карте маршрутов на основе интерфейса первого транзитного узла:

```
set policy route-map <name_card> rule <rule_number> match interface <interface>
```

где **<interface>** - интерфейс для сопоставления. Поддерживается любой маршрутизируемый интерфейс.

11. Определение условия соответствия в карте маршрутов на основе IP-адреса:

```
set policy route-map <name_card> rule <rule_number> match ip|ipv6 address  
<access-list <acl_number> | prefix-list <prefix> | prefix-len <0-32>>
```

где:

- **<access-list <acl_number>>** - IP-адрес отправителя или получателя маршрута проверяется на соответствие IP-адресам, разрешённым указанным списком доступа. Список доступа должен быть заранее определён;
- **<prefix-list <prefix>>** - подсеть отправителя или получателя маршрута проверяется на соответствие подсетям, разрешённым указанным списком префиксов. Список префиксов должен быть заранее определён;
- **<prefix-len <0-32>>** - IP-адрес отправителя или получателя маршрута проверяется на соответствие указанной длине префикса. Возможно указать значение в диапазоне от «0» до «32» для IPv4 и от «0» до «128» для IPv6. Не применяется к маршрутам протоколов динамической маршрутизации.

12. Определение условия соответствия в карте маршрутов на основе адреса следующего транзитного узла:

```
set policy route-map <name_card> rule <rule_number> match ip nexthop <access-list <acl_number> | prefix-list <prefix> | prefix-len <0-32> | address <x.x.x.x> | type blackhole>
```

где:

- **<access-list <acl_number>>** - IP-адрес следующего транзитного узла в маршруте проверяется на соответствие IP-адресам, разрешённым указанным списком доступа. Список доступа должен быть заранее определён;
- **<prefix-list <prefix>>** - IP-адрес следующего транзитного узла в маршруте проверяется на соответствие IP-адресам, разрешённым указанным списком префиксов. Список префиксов должен быть заранее определён;
- **<prefix-len <0-32>>** - IP-адрес следующего транзитного узла в маршруте проверяется на соответствие указанной длине префикса. Возможно указать значение в диапазоне от «0» до «32». Не применяется к маршрутам протоколов динамической маршрутизации;
- **<address <x.x.x.x>>** - IP-адрес следующего транзитного узла в маршруте проверяется на соответствие указанному IP-адресу;
- **<type blackhole>** - IP-адрес следующего транзитного узла в маршруте проверяется на соответствие указанному типу «blackhole».

13. Определение условия соответствия в карте маршрутов на основе IPv6-адреса следующего транзитного узла:

```
set policy route-map <name_card> rule <rule_number> match ipv6 nexthop <access-list <acl_number> | prefix-list <prefix> | address <address> | type blackhole>
```

где:

- **<access-list <acl_number>>** - IPv6-адрес следующего транзитного узла в маршруте проверяется на соответствие IPv6-адресам, разрешённым указанным списком доступа. Список доступа должен быть заранее определён;
- **<prefix-list <prefix>>** - IPv6-адрес следующего транзитного узла в маршруте проверяется на соответствие IPv6-адресам, разрешённым указанным списком префиксов. Список префиксов должен быть заранее определён;

- **<address <h:h:h:h:h:h:h>>** - IP-адрес следующего транзитного узла в маршруте проверяется на соответствие указанному IP-адресу;
- **<type blackhole>** - IP-адрес следующего транзитного узла в маршруте проверяется на соответствие указанному типу «blackhole».

14. Определение условия соответствия в карте маршрутов на основе адреса следующего транзитного узла:

```
set policy route-map <name_card> rule <rule_number> match ip route-source  
<access-list <acl_number> | prefix-list <prefix>>
```

где:

- **<access-list <acl_number>>** - считается найденным соответствие для маршрутов, объявляемых с адресов, содержащихся в указанном списке доступа. Список доступа должен быть заранее определён;
- **<prefix-list <prefix>>** - считается найденным соответствие для маршрутов, объявляемых с адресов, содержащихся в указанном списке префиксов. Список префиксов должен быть заранее определён.

15. Определение условия соответствия в карте маршрутов на основе метрики маршрута:

```
set policy route-map <name_card> rule <rule_number> match metric <metric>
```

где **<metric>** - число, представляющее метрику маршрута. Возможно указать значение в диапазоне от «1» до «65535».

16. Определение условия соответствия в карте маршрутов на основе способа получения маршрута:

```
set policy route-map <name_card> rule <rule_number> match origin  
<method_reception>
```

где **<method_reception>** - способ получения маршрута. Возможно указать следующие значения:

- **egp** - считается найденным соответствие для маршрутов, полученных по протоколу EGP;
- **igp** - считается найденным соответствие для маршрутов, полученных по протоколу IGP;
- **incomplete** - считается найденным соответствие для маршрутов, код BGP способа получения, которых неполон.

17. Определение условия соответствия в карте маршрутов на основе IP-адреса равноправного узла:

```
set policy route-map <name_card> rule <rule_number> match peer  
<x.x.x.x>|<h:h:h:h:h:h:h:h>
```

где **<x.x.x.x>|<h:h:h:h:h:h:h:h>** - IPv4-адрес или IPv6-адрес. На соответствие указанному адресу проверяется адрес равноправного узла в маршруте.

18. Определение условия соответствия в карте маршрутов на основе тега OSPF:

```
set policy route-map <name_card> rule <rule_number> match tag <tag>
```

где **<tag>** - число, представляющее тег OSPF. На соответствие этому значению проверяется содержимое поля внешнего тега LSA (Link-State Advertisement, объявление состояния канала) протокола OSPF в маршруте. Возможно указать значение в диапазоне от «1» до «65535».

19. Указание альтернативной политики выхода в карте маршрутов:

```
set policy route-map <name_card> rule <rule_number> on-match <goto  
<rule_number> | next>
```

где:

- **<goto <rule_number>>** - выход из текущего правила карты маршрутов, вызов правила, указанного данным параметром, и его выполнение. Переход на предшествующее правило списка маршрутов не разрешается;
- **<next>** - выход из текущего правила карты маршрутов, вызов следующего правила в последовательности и его выполнение.

20. Изменение атрибута агрегатора протокола BGP для маршрута:

```
set policy route-map <name_card> rule <rule_number> set aggregator <as|ip> <1-  
4294967295|x.x.x.x>
```

где:

- **<as <1-4294967295>>** - изменение номера автономной системы агрегатора BGP в маршруте на указанное значение. Возможно указать значение в диапазоне от «1» до «4294967295»;
- **<ip <x.x.x.x>>** - изменение IP-адреса агрегатора BGP в маршруте на указанный IPv4-адрес.

8 VRF

Система **ARMA Стена** поддерживает использование **VRF** (Virtual Routing and Forwarding), что позволяет создавать изолированные домены маршрутизации в пределах одного устройства. Одним из вариантов использования является решение задачи мультиарендности (multi-tenancy), когда требуется обеспечить изоляцию трафика между различными клиентами или отделами внутри одной организации. Каждый VRF-домен имеет собственную таблицу маршрутов, собственный набор интерфейсов и собственный шлюз по умолчанию.

8.1 Конфигурация

Необходимо создать устройство **VRF** с соответствующей таблицей маршрутов. Затем сетевые интерфейсы подключаются к устройству **VRF**.

Создание VRF-экземпляра

Для создания нового **VRF**-экземпляра необходимо ввести следующие команды:

```
set vrf name <vrf_name> table <100-65535>
```

где:

- **<vrf_name>** – имя **VRF**-экземпляра. Имя экземпляра VRF должно начинаться с буквы латинского алфавита, содержать не более 15 символов, не совпадать с именами стандартных сетевых интерфейсов (например, eth0, lo, wlan1 и т.п.) и может включать только латинские буквы, цифры и символ подчёркивания «_»;
- **<100-65535>** – идентификатор таблицы маршрутизации. Возможно указание значения в диапазоне от «100» до «65535».

Примечание:

Идентификатор таблицы маршрутов не может быть изменён после создания. Для изменения необходимо удалить и заново создать **VRF**-экземпляр.

Назначение интерфейса VRF

Назначить сетевой интерфейс **VRF**-экземпляру с помощью следующий команды:

```
set interfaces <type_interfaces> <name_interfaces> vrf <vrf_name>
```

где:

- **<type_interfaces>** – тип сетевого интерфейса. Возможно указание следующих типов интерфейсов: «bonding», «bridge», «dummy», «ethernet», «l2tpv3», «macsec», «openvpn», «pppoe», «pseudo-

ethernet», «sstpс», «tunnel», «virtual-ethernet», «vti», «vxlan», «wireguard», «wireless», «wwan».

- **<name_interfaces>** – имя сетевого интерфейса в соответствии с его типом.

Глобальная привязка портов

По умолчанию сетевые сервисы (например, SSH, SNMP и др.), запущенные в контексте основной **VRF**, могут принимать соединения только через интерфейсы, принадлежащие этой же **VRF**. Это ограничение связано с тем, что непривязанные сокет по умолчанию не соответствуют пакетам, приходящим через интерфейсы, принадлежащие другим **VRF**.

Для изменения этого поведения и обеспечения возможности приёма трафика из всех **VRF**-доменов используется следующая команда:

```
set vrf bind-to-all
```

Включение данной опции позволяет TCP- и UDP-сервисам, работающим в контексте основной **VRF** (т.е. не привязанные ни к одному устройству **VRF**), работать во всех **VRF**-доменов.

Фильтрация маршрутов ядра/Zebra

Демон Zebra в FRRouting (FRR) поддерживает использование префиксных списков (prefix-lists) и маршрутных политик (route-maps) для фильтрации маршрутов, полученных от других компонентов FRR. Эти механизмы позволяют точно контролировать, какие маршруты будут установлены в ядре операционной системы.

Для применения маршрутной политики к маршрутам определённого протокола, используйте следующую команду в конфигурационном режиме:

```
set vrf name <vrf_name> ip|ipv6 protocol <protocol> route-map <route-map>
```

где:

- **<protocol>** – протокол, маршруты которого будут фильтроваться. Поддерживаются следующие значения: «any», «babel», «bgp», «connected», «eigrp», «isis», «kernel», «ospf», «rip», «static», «table».
- **<route-map>** – имя применяемой маршрутной политики.

Если указано значение «any», маршрутная политика будет применена ко всем протоколам, отправляющим маршруты в Zebra.

Отслеживание следующего хопа (Nexthop Tracking)

По умолчанию отслеживание следующего хопа (Nexthop Tracking) разрешает адреса через маршрут по умолчанию. Эта функция включена по умолчанию в

типовой конфигурации FRR, используемой в системе **ARMA Стена**. Её возможно отключить, если требуется, например, запретить BGP устанавливать соседство через маршрут по умолчанию.

Команда отключения разрешения IPv4|IPv6-хопов через маршрут по умолчанию:

```
set vrf name <vrf_name> ip|ipv6 nht no-resolve-via-default
```

Настройка применяется индивидуально для каждого **VRF**.

Поддержка динамической маршрутизации

В Системе **ARMA Стена** реализована поддержка динамической маршрутизации внутри **VRF**.

Поддерживаемые протоколы динамической маршрутизации:

- **BGP**;
- **IS-IS**;
- **OSPF**;
- **OSPFv3 (IPv6)**;
- **Static**.

Конфигурация динамических протоколов в контексте **VRF** выполняется аналогично стандартной. Единственное различие состоит в том, что для каждого применяемого протокола маршрутизации необходимо указывать префикс с соответствующей командой «**vrf name <vrf_name>**»:

```
set vrf name <vrf_name> protocols bgp ...  
set vrf name <vrf_name> protocols isis ...  
set vrf name <vrf_name> protocols ospf ...  
set vrf name <vrf_name> protocols ospfv3 ...  
set vrf name <vrf_name> protocols static ...
```

8.2 Обслуживание VRF

Для обеспечения надлежащей функциональности **VRF** необходимо не только их первоначальная настройка, но и регулярное операционное обслуживание. В данном разделе представлены ключевые команды операционного режима, предназначенные для мониторинга и диагностики функционирования **VRF**.

1. Отобразить список всех созданных **VRF**-устройств с информацией о состоянии, MAC-адресе, флагах и назначенных интерфейсах (см. [Рисунок – Список всех созданных VRF-устройств](#)):

```
admin@ngfwos:~$ show vrf
```



```
admin@ngfwos:~$ show vrf
VRF name      state      mac address      flags      interfaces
-----
blue          up        00:53:12:d8:74:24  noarp, master, up, lower_up  dum200, eth0.302
red           up        00:53:de:02:df:aa  noarp, master, up, lower_up  dum100, eth0.300, bond0.100, peth0
```

Рисунок – Список всех созданных VRF-устройств

2. Отобразить детальную информацию по указанному **VRF** (см. [Рисунок – Детальная информация по VRF](#)):

```
admin@ngfwos:~$ show vrf <vrf_name>
```

```
admin@ngfwos:~$ show vrf name blue
VRF name      state      mac address      flags      interfaces
-----
blue          up        00:53:12:d8:74:24  noarp, master, up, lower_up  dum200, eth0.302
```

Рисунок – Детальная информация по VRF

3. Вывести IPv4-таблицу маршрутов, связанную с указанным **VRF** (см. [Рисунок – IPv4-таблица маршрутов VRF](#)):

```
admin@ngfwos:~$ show ip route vrf <vrf_name>
```

```
admin@ngfwos:~$ show ip route vrf blue
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, D - SHARP,
       F - PBR, f - OpenFabric,
       > - selected route, * - FIB route, q - queued route, r - rejected route

VRF blue:
K  0.0.0.0/0 [255/8192] unreachable (ICMP unreachable), 00:00:50
S>* 172.16.0.0/16 [1/0] via 192.0.2.1, dum1, 00:00:02
C>* 192.0.2.0/24 is directly connected, dum1, 00:00:06
```

Рисунок – IPv4-таблица маршрутов VRF

4. Вывести IPv6-таблицу маршрутов, связанную с указанным **VRF** (см. [Рисунок – IPv6-таблица маршрутов VRF](#)):

```
admin@ngfwos:~$ show ipv6 route vrf <vrf_name>
```

```
admin@ngfwos:~$ show ipv6 route vrf red
Codes: K - kernel route, C - connected, S - static, R - RIPng,
       O - OSPFv3, I - IS-IS, B - BGP, N - NHRP, T - Table,
       v - VNC, V - VNC-Direct, A - Babel, D - SHARP, F - PBR,
       f - OpenFabric,
       > - selected route, * - FIB route, q - queued route, r - rejected route

VRF red:
K  ::0 [255/8192] unreachable (ICMP unreachable), 00:43:20
C>* 2001:db8::/64 is directly connected, dum1, 00:02:19
C>* fe80::/64 is directly connected, dum1, 00:43:19
K>* ff00::/8 [0/256] is directly connected, dum1, 00:43:19
```

Рисунок – IPv6-таблица маршрутов VRF

5. Проверить доступность удалённого хоста в контексте указанного **VRF** (см. [Рисунок – Проверка доступность удалённого хоста](#)):

```
admin@ngfwos:~$ ping <host> vrf <vrf_name>
```

Команда может быть прервана в любой момент с помощью комбинации клавиш «**Ctrl**» + «**C**».

```
admin@ngfwos:~$ ping 192.0.2.1 vrf red
PING 192.0.2.1 (192.0.2.1) 56(84) bytes of data.
64 bytes from 192.0.2.1: icmp_seq=1 ttl=64 time=0.070 ms
64 bytes from 192.0.2.1: icmp_seq=2 ttl=64 time=0.078 ms
^C
--- 192.0.2.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 4ms
rtt min/avg/max/mdev = 0.070/0.074/0.078/0.004 ms
```

Рисунок – Проверка доступность удалённого хоста

6. Переключение в контекст **VRF**:

```
admin@ngfwos:~$ force vrf <vrf_name>
```

Переключает текущую оболочку в контекст указанного **VRF**. Все последующие команды будут выполняться в этом контексте до выхода из подоболочки.

При переключении командная строка обновляется, чтобы отразить текущий **VRF**:

```
admin@ngfwos:~$ force vrf red
admin@ngfwos(red):~$
```

8.3 Пример конфигурирования VRF

В качестве примера настройки **VRF** используется схема стенда, представленная на рисунке (см. [Рисунок – Пример схемы сети VRF](#)).

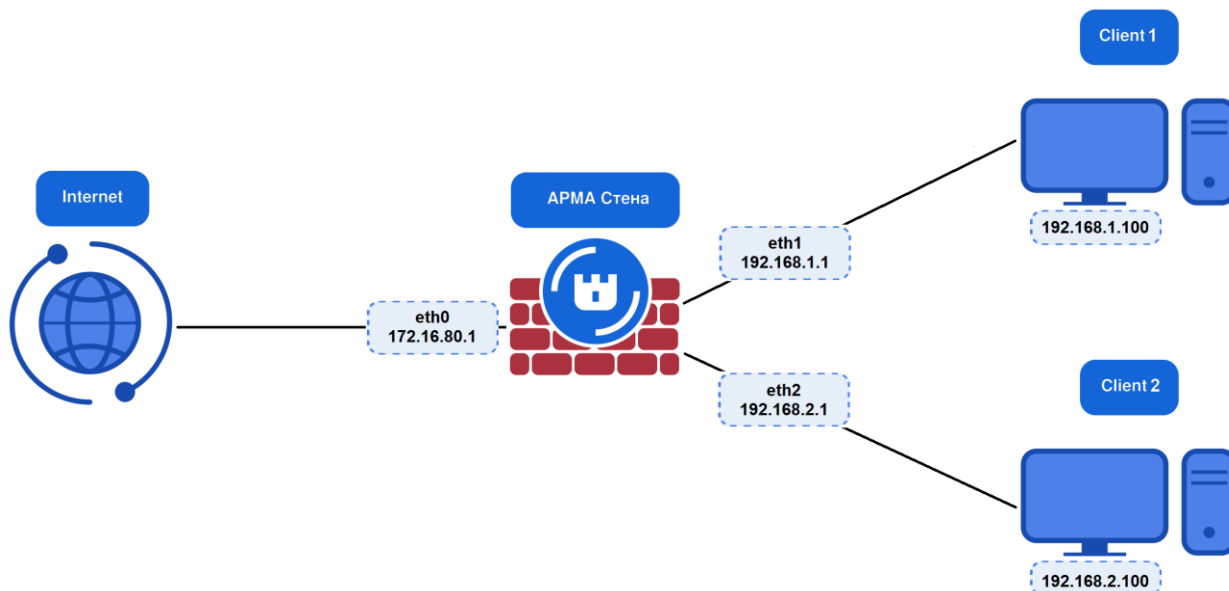


Рисунок – Пример схемы сети VRF

1. Настройки системы **АРМА Стена**:

```
#Присвоение IP-адресов и ассоциация интерфейсов с VRF:
set interfaces ethernet eth0 address '172.16.80.1/24'
```

```

set interfaces ethernet eth1 address '192.168.1.1/24'
set interfaces ethernet eth1 vrf 'vrf1'
set interfaces ethernet eth2 address '192.168.2.1/24'
set interfaces ethernet eth2 vrf 'vrf2'

#Обеспечение выхода трафика во внешнюю сеть через трансляцию адресов:
set nat source rule 10 outbound-interface name 'eth0'
set nat source rule 10 translation address 'masquerade'

#Добавление локального маршрута в основную таблицу маршрутизации для
сети vrf1:
set protocols static route 192.168.1.0/24 interface eth1 vrf 'vrf1'

#Настройка маршрута по умолчанию для vrf1 через шлюз в основном VRF:
set vrf name vrf1 protocols static route 0.0.0.0/0 next-hop 172.16.80.1 vrf 'default'

#Каждому VRF назначается уникальный номер таблицы маршрутизации:
set vrf name vrf1 table '200'
set vrf name vrf2 table '300'

#Применить и сохранить конфигурацию:
commit
save

```

Данная конфигурация реализует сегментацию сетевого трафика с использованием **VRF**. Обеспечивается полная изоляция между двумя внутренними сегментами (**vrf1** и **vrf2**) и предоставление доступа в интернет только для компьютера «**Client1**», подключённого к сети 192.168.1.0/24.

Вывести информацию о текущем состоянии **VRF**:

```

admin@ngfwos# run show vrf

```

Name	State	MAC address	Flags	Interfaces
vrf1	up	aa:9c:df:35:8a:5e	noarp, master, up, lower_up	eth1, pim6reg200
vrf2	up	b2:6b:d5:c4:d2:34	noarp, master, up, lower_up	eth2, pim6reg300

2. Настройка сетевых клиентов:

Для компьютеров «**Client1**» и «**Client2**», функционирующих под управлением операционной системы семейства Windows, необходимо произвести конфигурацию сетевых адаптеров (см. [Рисунок – Настройка IP-адреса](#)).

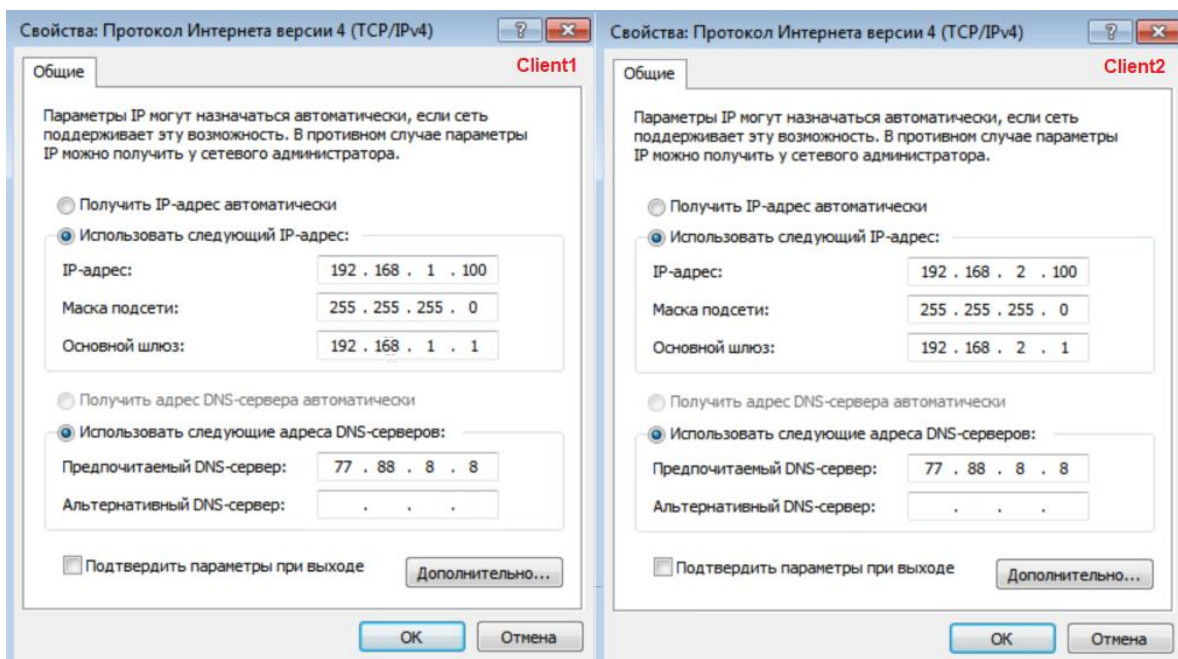


Рисунок – Настройка IP-адреса

По завершении процедуры настройки IP-адреса следует проверить доступность интернет-соединения на компьютере **«Client1»** посредством команды ICMP-запроса к DNS-серверу 8.8.8.8 (см. [Рисунок – Проверка доступа к сети Интернет](#)).

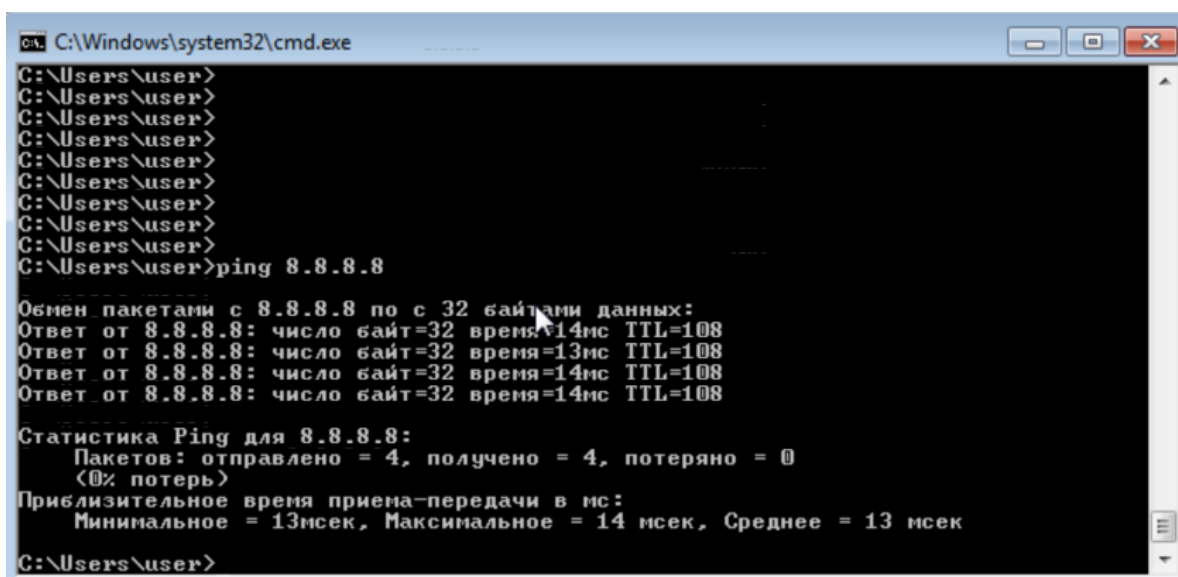


Рисунок – Проверка доступа к сети Интернет

9 ОТКАЗОУСТОЙЧИВОСТЬ

9.1 VRRP

В режиме отказоустойчивости несколько устройств **ARMA Стена** объединяются в кластер с использованием протокола **VRRP** в режиме «**активный/пассивный**».

Протокол **VRRP** (Virtual Router Redundancy Protocol) предназначен для повышения доступности маршрутизаторов, выполняющих функцию шлюза по умолчанию. Это достигается путём объединения группы маршрутизаторов в один виртуальный маршрутизатор и присвоения им общего IP-адреса, который будет использоваться в качестве шлюза по умолчанию для компьютеров в сети.

Примечание:

В связи с ограничениями, существующими в текущих реализациях протоколов **DHCP** и **VRRP**, их совместное использование на одном интерфейсе невозможно. При использовании протокола **VRRP** IP-адрес на интерфейсе должен быть задан статически.

Идентификатор виртуального маршрутизатора и VIP-адрес

При использовании **VRRP**, интерфейсы физических маршрутизаторов формируют «виртуальный маршрутизатор». Виртуальный маршрутизатор – это абстрактный объект, управляемый процессом **VRRP**. Каждый виртуальный маршрутизатор имеет уникальный цифровой идентификатор (Virtual router ID – **VRID**) и виртуальный IP-адрес (Virtual IP – **VIP**). Узлы в сети настраиваются таким образом, чтобы направлять пакеты на VIP-адрес виртуального маршрутизатора, вместо IP-адресов физических интерфейсов. Виртуальный маршрутизатор может состоять из кластера физических и/или виртуальных интерфейсов, обеспечивающих резервирование для первичного интерфейса (мастер-интерфейса). Как правило, интерфейсы, входящие в виртуальный маршрутизатор, находятся на разных маршрутизаторах. Резервированием управляет процесс **VRRP**, выполняемый в системе каждого маршрутизатора, состоящего в виртуальном маршрутизаторе.

Каждому виртуальному маршрутизатору может быть назначено до 20 **VIP-адресов**. Для обеспечения резервирования интерфейсам в составе виртуального маршрутизатора должен быть назначен одинаковый идентификатор и **VIP-адрес**. IP-адреса интерфейсов и **VIP-адрес** группы не обязательно должны находиться в одной подсети.

Виртуальный MAC-адрес

Каждому виртуальному маршрутизатору **VRRP** должен быть присвоен определённый 48-битный MAC-адрес. Виртуальный MAC-адрес создаётся на основе MAC-префиксов (описанных в спецификации протокола **VRRP**) и идентификатора виртуального маршрутизатора. Виртуальный MAC-адрес

выглядит как 0000:5E00:01xx, где «xx» – идентификатор виртуального маршрутизатора.

Главный маршрутизатор использует MAC-адрес виртуального маршрутизатора в качестве источника для отправляемых VRRP-пакетов. При получении статуса главного маршрутизатора, резервное устройство также начинает использовать MAC-адрес виртуального маршрутизатора.

Использование предопределённого MAC-адреса виртуального маршрутизатора позволяет не менять настройки ARP при сбое главного маршрутизатора.

Объявления VRRP и выбор главного маршрутизатора

Главный маршрутизатор использует объявления VRRP для передачи информации о своём текущем состоянии резервным маршрутизаторам. Объявления VRRP состоят из пакетов «heartbeat», которые содержат информацию о состоянии главного маршрутизатора и его приоритет. В каждом виртуальном маршрутизаторе только главный маршрутизатор отправляет периодические объявления VRRP на зарезервированный адрес 224.0.0.18. На канальном уровне в качестве MAC-адреса отправителя объявлений VRRP используется виртуальный MAC-адрес. Если резервные устройства не получают объявления VRRP в течение заданного периода (dead interval), то главный маршрутизатор считается неработоспособным, после чего статус главного маршрутизатора присваивается одному из резервных маршрутизаторов согласно выставленному значению приоритета.

В рамках виртуального маршрутизатора выбор главного устройства осуществляется автоматически на основе заданного приоритета. Если у двух устройств, входящих в состав виртуального маршрутизатора, значение приоритета будет одинаковым, главным назначается маршрутизатор с большим IP-адресом. Он получает виртуальный адрес для своего интерфейса, а остальные маршрутизаторы с меньшим приоритетом становятся резервными.

При отказе мастер-интерфейса, дублирующий интерфейс с наибольшим значением приоритета назначается мастер-интерфейсом и ему присваивается VIP-адрес виртуального маршрутизатора. Рекомендуется устанавливать значение приоритета мастер-интерфейса равным наибольшему значению приоритета дублирующего интерфейса плюс 50. Значение приоритета дублирующего интерфейса можно оставить равным значению по умолчанию, однако при наличии двух и более дублирующих интерфейсов, следует задать им разные значения приоритета.

Вытеснение

Если параметр вытеснения включён, резервный маршрутизатор с более высоким приоритетом, чем у текущего главного маршрутизатора, будет

замещать его, отправляя свои собственные объявления **VRRP**. Когда главный маршрутизатор обнаружит, что у дублирующего устройства установлено более высокое значение приоритета, он прекратит отправлять свои объявления **VRRP**. В результате дублирующий маршрутизатор с более высоким значением приоритета назначается главным маршрутизатором.

Вытеснение особенно полезно, когда в одном виртуальном маршрутизаторе находятся высокопроизводительный главный маршрутизатор и низкопроизводительный резервный. Например, в случае сбоя главного маршрутизатора, малопроизводительный резервный маршрутизатор становится главным до устранения сбоя. После устранения проблемы высокопроизводительный маршрутизатор с более высоким приоритетом автоматически назначается главным.

В системе **ARMA Стена** вытеснение включено по умолчанию. Это означает, что резервный маршрутизатор с более высоким приоритетом автоматически становится активным, как только переходит в рабочее состояние.

Для отключения режима вытеснения используется опция **«no-preempt»**:

```
set high-availability vrrp group <имя_группы> no-preempt
```

После применения данной конфигурации устройство с более высоким приоритетом не будет автоматически принимать роль активного узла, даже если оно находится в рабочем состоянии.

Для настройки временной задержки перед выполнением вытеснения предусмотрен параметр **«preempt-delay»**. Указанный интервал позволяет избежать частых переключений активной роли в условиях нестабильной доступности одного из узлов кластера. Например, для установки задержки в 180 секунд необходимо выполнить команду:

```
set high-availability vrrp group <имя_группы> preempt-delay 180
```

Допустимый диапазон значений параметра **«preempt-delay»** от «1» до «1000» секунд включительно.

Возможные состояния виртуального маршрутизатора на устройствах

- **«MASTER»** – главный маршрутизатор – это устройство, имеющее наибольший приоритет в рамках одного виртуального маршрутизатора. Отправляет на резервные маршрутизаторы объявления, содержащие в том числе, значение приоритета.
- **«BACKUP»** – резервный маршрутизатор – это устройство, которое имеет меньший приоритет чем главный маршрутизатор. При получении объявлений сравнивает приоритет в полученном объявлении со своим значением. Если было получено объявление с меньшим приоритетом или

объявления не были получены в течение установленного интервала – резервный маршрутизатор становится главным маршрутизатором.

- **«FAULT»** – состояние ошибки. Переход в статус **FAULT** происходит по следующим основным причинам:
 - *Проблемы с интерфейсом* – могут возникать вследствие административного отключения интерфейса (например, командой «set interfaces ethernet eth1 disable»), физической потери линка (обрыв кабеля, неисправность коммутатора), отключения на системном уровне или отсутствия поднятого канального уровня (L2), как, например, в случае с PPPoE- или VLAN-интерфейсами без установленного соединения, а также при отсутствии назначенного IP-адреса на интерфейсе.
 - *Потеря виртуального IP-адреса (VIP)* – если виртуальный IP-адрес, назначенный VRRP-группе, был удалён с интерфейса вручную или по иной причине, VRRP-процесс переходит в состояние **FAULT**.
 - *Проблемы с отслеживанием интерфейсов (Interface Tracking)* – переход отслеживаемого интерфейса (например, WAN-линка) в состояние down приводит к активации статуса **FAULT**.
 - *Срабатывание скрипта отслеживания (Track Script)* – выполнение пользовательского скрипта, настроенного для мониторинга (например, проверки доступности шлюза, загрузки процессора или наличия критического процесса), завершилось с ненулевым кодом возврата, что интерпретируется как сбой.
 - *Внутренние ошибки VRRP-демона* – в редких случаях возможны сбои в работе демона keeralived (используемого в системе **ARMA Стена** для реализации VRRP), приводящие к переходу в состояние **FAULT**.

Скрипты

Функциональность **VRRP** возможно расширить с помощью скриптов. Система **ARMA Стена** поддерживает два типа скриптов: скрипты проверки работоспособности и скрипты перехода.

Скрипты проверки работоспособности выполняют пользовательские проверки в дополнение к проверке работоспособности основного маршрутизатора.

Примеры настройки запуска скрипта проверки работоспособности:

1. Данный пример конфигурации укажет процессу **VRRP** выполнять скрипт «/config/scripts/vrrp-check.sh» каждые 60 секунд. Если скрипт

завершится с ненулевым статусом три раза подряд, группа VRRP «test1» будет переведена в состояние ошибки («FAULT»):

```
set high-availability vrrp group test1 health-check script /config/scripts/vrrp-check.sh
set high-availability vrrp group test1 health-check interval 60
set high-availability vrrp group test1 health-check failure-count 3
```

2. В случае, если группа VRRP входит в состав группы синхронизации, будет применяться только сценарий проверки работоспособности группы синхронизации. В данном примере показано, как настроить этот сценарий для группы синхронизации:

```
set high-availability vrrp sync-group test2 health-check script /config/scripts/vrrp-check.sh
set high-availability vrrp sync-group test2 health-check interval 60
set high-availability vrrp sync-group test2 health-check failure-count 3
```

Скрипты перехода выполняются при изменении состояния **VRRP** с основного на резервный или неисправный и наоборот. Они могут быть использованы для выполнения различных операций, таких как запуск и остановка служб, а также для изменения конфигурации системы **ARMA Стена** при переключении **VRRP**.

Примеры настройки запуска скриптов перехода при изменении состояния **VRRP**:

```
set high-availability vrrp group test transition-script master "/config/scripts/vrrp-master.sh test"
set high-availability vrrp group test transition-script backup "/config/scripts/vrrp-fail.sh test"
set high-availability vrrp group test transition-script fault "/config/scripts/vrrp-fail.sh test"
set high-availability vrrp group test transition-script master "/config/scripts/vrrp-master.sh test"
```

Данная конфигурация запускает выполнение файла «/config/scripts/vrrp-fail.sh» с аргументом «test» при сбое VRRP, а также файла «/config/scripts/vrrp-master.sh» при переходе системы в режим «MASTER».

Примечание:

Скрипт должен возвращать «0» для обозначения успешного результата и значение отличное от «0» – для неудачных результатов. Система перестанет отвечать на запросы, если выполнение скрипта не завершится!

Рекомендуется сохранять скрипты в каталоге «**/config/scripts**». Это позволит избежать потери файлов в случае обновления системы.

Алгоритм настройки VRRP-группы:

1. Указать IP-адреса и задать описание интерфейсов маршрутизатора.
2. Задать имя и описание для группы **VRRP**.
3. Указать интерфейс маршрутизатора, который будет являться участником группы **VRRP**.
4. Определить приоритет маршрутизатора для группы **VRRP**.
5. Задать виртуальный VIP-адрес для группы **VRRP**.
6. Указать общий номер группы **VRRP** (VRID).
7. Выполнить аналогичные настройки на втором маршрутизаторе.

9.1.1 Глобальные настройки

В большинстве случаев нет необходимости вносить изменения в параметры системы, и использование стандартных настроек является достаточным. Однако в некоторых случаях может потребоваться дополнительная настройка.

1. Указать используемую версию протокола VRRP:

```
set high-availability vrrp global-parameters version <2|3>
```

где **<2|3>** - номер версии протокола VRRP. Система **ARMA Стена** поддерживает протокол VRRP версий 2 и 3. По умолчанию применяется протокол VRRP версии 3. Для работы с IPv6 используется протокол VRRP версии 3, который обеспечивает поддержку как IPv4, так и IPv6.

Примечание:

При обновлении **ARMA Стена** и переносе настроек с более ранних версий системы (до версии 4.8) по умолчанию используется VRRP версии 2.

2. Определить задержку перед запуском экземпляра VRRP после старта Keepalived:

```
set high-availability vrrp global-parameters startup-delay <1-600>
```

где **<1-600>** - время ожидания в секундах, в течение которого VRRP не будет активен после запуска системы. Возможно указать значение в диапазоне от «1» до «600». Это значение помогает избежать преждевременного запуска VRRP, обеспечивая корректную инициализацию сетевых интерфейсов и других зависимых служб.

3. Включить экспорт состояния VRRP через SNMP:

```
set high-availability vrrp snmp
```

Данная команда активирует поддержку стандартного SNMP-мониторинга для групп VRRP. После её выполнения сведения о состоянии VRRP-групп (Master, Backup, Fault), их приоритете, идентификаторе VRID и виртуальных IP-адресах становятся доступны посредством SNMP-запросов к стандартным MIB-переменным.

Команда не включает SNMP-сервис. Для функционирования мониторинга требуется предварительная настройка SNMP-агента (см. раздел «[SNMP](#)» настоящего руководства).

9.1.2 Настройка Gratuitous ARP

Gratious ARP (GARP) – это механизм, используемый для обновления ARP-таблиц соседних устройств в сети. В контексте VRRP GARP помогает уведомлять сеть о том, что виртуальный маршрутизатор стал активным (MASTER). Настройка GARP в системе **ARMA Стена** не является обязательной, так как есть значения по умолчанию, но при необходимости их можно изменить.

Настройки GARP могут быть применены как глобально (для всех групп VRRP), так и для конкретной группы VRRP. Ниже приведены команды и их описание:

1. Установить задержку между отправкой сообщений GARP на интерфейс:

```
set high-availability vrrp global-parameters garp interval <0.000-1000>  
  
set high-availability vrrp group <name> garp interval <0.000-1000>
```

где:

- **<0.000-1000>** - значение задержки в секундах. Возможно указать значение в диапазоне от «0.000» до «1000». По умолчанию используется значение «0» - сообщения отправляются без задержки.
 - **<name>** - имя группы VRRP.
2. Установить задержку перед отправкой второго набора GARP после того, как маршрутизатор становится MASTER:

```
set high-availability vrrp global-parameters garp master-delay <1-255>  
  
set high-availability vrrp group <name> garp master-delay <1-255>
```

где **<1-255>** - значение задержки в секундах. Возможно указать значение в диапазоне от «1» до «255». По умолчанию используется значение «5».

3. Установить интервал обновления GARP в состоянии MASTER:

```
set high-availability vrrp global-parameters garp master-refresh <1-600>
```

```
set high-availability vrrp group <name> garp master-refresh <1-600>
```

где **<1-600>** - значение временного интервала в секундах. Возможно указать значение в диапазоне от «1» до «600». По умолчанию используется значение «0» - обновление отключено.

4. Установить количество сообщений GARP, отправляемых за один раз в состоянии MASTER:

```
set high-availability vrrp global-parameters garp master-refresh-repeat <1-600>
```

```
set high-availability vrrp group <name> garp master-refresh-repeat <1-600>
```

где **<1-600>** - количество сообщений GARP, отправляемых за один раз. Возможно указать значение в диапазоне от «1» до «600». По умолчанию используется значение «1».

5. Установить количество сообщений GARP, отправляемых за один раз после перехода в состояние MASTER:

```
set high-availability vrrp global-parameters garp master-repeat <1-600>
```

```
set high-availability vrrp group <name> garp master-repeat <1-600>
```

где **<1-600>** - количество сообщений GARP, отправляемых за один раз. Возможно указать значение в диапазоне от «1» до «600». По умолчанию используется значение «5».

Примечание:

Параметры, установленные для группы, обладают более высоким приоритетом по сравнению с глобальными параметрами. В случае, если параметр не определён ни на глобальном уровне, ни для группы, применяются значения по умолчанию.

9.1.3 Команды настройки группы VRRP

1. Назначение виртуального IP-адреса (VIP) для группы VRRP:

```
set high-availability vrrp group <имя_группы> address <address>
```

где:

- **<имя_группы>** – имя группы VRRP;
- **<address>** – формат виртуального IP-адреса зависит от версии VRRP:
 - VRRP версии 2

Поддерживается только IPv4. При указании адреса в формате <х.х.х.х> (без префикса) система автоматически применяет маску /32. Формат <х.х.х.х/х> также допустим, однако префикс не влияет на работу VRRPv2 и используется исключительно для внутренней маршрутизации или совместимости с конфигурацией интерфейса.

- VRRP версии 3

Поддерживается как IPv4, так и IPv6. Для IPv4 допустимы форматы <х.х.х.х> и <х.х.х.х/х>. Префикс может использоваться для корректной привязки виртуального адреса к подсети. Для IPv6 допустимы форматы <h:h:h:h:h:h:h> и <h:h:h:h:h:h:h/х>. Префикс учитывается при обработке многоадресного трафика и формировании ND (Neighbor Discovery) записей.

Смешанное использование IPv4 и IPv6 в одной группе VRRP недопустимо.

2. Привязка сетевого интерфейса к виртуальному IP-адресу в группе VRRP:

```
set high-availability vrrp group <имя_группы> address <address> interface <имя_интерфейса>
```

где **<имя_интерфейса>** – имя физического или логического сетевого интерфейса, на котором будет активен указанный виртуальный адрес.

В одной группе VRRP может быть настроено несколько виртуальных адресов, каждый из которых может быть привязан к отдельному интерфейсу.

3. Установка VRID для группы VRRP:

```
set high-availability vrrp group <имя_группы> vrid <1-255>
```

где **<1-255>** – целочисленное значение в диапазоне от «1» до «255», уникально определяющее виртуальный маршрутизатор в пределах одного широковещательного домена.

4. Указание интерфейса для группы VRRP:

```
set high-availability vrrp group <имя_группы> interface <имя_интерфейса>
```

где **<имя_интерфейса>** – имя физического или логического сетевого интерфейса, на котором будет работать группа VRRP.

5. Установка приоритета маршрутизатора в группе VRRP:

```
set high-availability vrrp group <имя_группы> priority <1-255>
```

где **<1-255>** – целочисленное значение приоритета узла (маршрутизатора) в рамках одной VRRP-группы. Возможно указать значение в диапазоне от «1» до «255». Это значение определяет, какой из узлов будет выступать в роли Master (активного маршрутизатора), а какие – в роли Backup (резервных). Узел с наибольшим приоритетом становится Master. По умолчанию приоритет равен «100».

6. Добавление описания группы VRRP:

```
set high-availability vrrp group <имя_группы> description <text>
```

где **<text>** – краткое текстовое описание. Допускается использование символов кириллического и латинского алфавитов. Описание не должно начинаться с последовательности «//». Запрещено использование символов «"», «'» и перенос строки. Максимальная длина значения – «127» символов. При наличии пробелов значение должно быть заключено в двойные кавычки.

7. Установка интервала отправки VRRP-объявлений:

```
set high-availability vrrp group <имя_группы> advertise-interval <interval>
```

где **<interval>** – интервал в секундах, с которым активный маршрутизатор (Master) отправляет VRRP-объявления в группе.

Для VRRP версии 2 возможно указать значение в диапазоне от «1» до «255». Значение по умолчанию – «1» секунда.

Для VRRP версии 3 поддерживается полный диапазон с точностью до микросекунды. Возможно указать значение в диапазоне от «0.010000» до «40.950000». Значение по умолчанию – «1.000000» секунда.

8. Настройка аутентификации в группе VRRP:

8.1 Указание типа аутентификации:

```
set high-availability vrrp group <имя_группы> authentication type <plaintext-password | ah>
```

где:

- **<plaintext-password>** – аутентификация по паролю. Применяется в заголовке VRRPv2 для базовой проверки принадлежности узлов к одной группе. Пароль передаётся в открытом виде, криптографическая защита не обеспечивается;
- **<ah>** – аутентификация с использованием IPsec Authentication Header. Метод не рекомендуется к применению.

8.2 Указание пароля аутентификации:

```
set high-availability vrrp group <имя_группы> authentication password  
<пароль>
```

где **<пароль>** – пароль длиной не более 8 символов, используемый для аутентификации VRRP-пакетов между узлами.

Примечание:

В версии VRRPv3 механизм аутентификации не поддерживается. Все параметры аутентификации игнорируются при использовании данной версии протокола.

9. Исключение IP-адреса из проверки дублирования:

```
set high-availability vrrp group <имя_группы> excluded-address <IP-адрес>  
interface <имя_интерфейса>
```

где:

- **<IP-адрес>** – IPv4 или IPv6-адрес (с префиксом или без), исключаемый из проверки на конфликт при инициализации VRRP;
- **<имя_интерфейса>** – сетевой интерфейс, на котором данный IP-адрес может быть назначен и не должен рассматриваться как конфликтующий с виртуальным адресом VRRP.

По умолчанию перед переходом узла в состояние Master выполняется проверка наличия дублирующихся виртуальных IP-адресов в локальном сетевом сегменте с использованием ARP (для IPv4) или NDP (для IPv6). Указание адреса в данном параметре отключает проверку дублирования на соответствующем интерфейсе, что исключает ложные срабатывания в случаях, когда физический и виртуальный IP-адреса совпадают.

В VRRPv2 проверка дублирования применяется только к IPv4-адресам и осуществляется исключительно посредством ARP-запросов. В VRRPv3 поддерживается как IPv4, так и IPv6, а проверка дублирования выполняется с использованием ARP (для IPv4) и NDP (Neighbor Discovery Protocol, для IPv6). Соответственно, при использовании VRRPv3 параметр excluded-address может применяться к адресам обоих семейств, тогда как в VRRPv2 – только к IPv4.

10. Настройка проверки работоспособности (health check) для группы VRRP:

10.1 Указание количества неудачных проверок до перехода в состояние FAULT:

```
set high-availability vrrp group <имя_группы> health-check failure-count  
<число>
```

где **<число>** – целое положительное число, задающее, количество последовательных сбоев health-check (ping или скрипт) должно произойти,

чтобы VRRP-группа перешла в состояние FAULT. Значение по умолчанию - «3».

После каждой неудачной проверки счётчик увеличивается. Если счётчик достигнет указанного значения – узел немедленно переходит в состояние FAULT. Успешная проверка сбрасывает счётчик.

10.2 Указание интервала между проверками:

```
set high-availability vrrp group <имя_группы> health-check interval  
<секунды>
```

где **<секунды>** – целое положительное число, задающее интервал в секундах между последовательными запусками health-check (ping или скрипт). Значение по умолчанию – «60».

10.3 Настройка ping-проверки:

```
set high-availability vrrp group <имя_группы> health-check ping <IP-адрес>
```

где **<IP-адрес>** – целевой IPv4- или IPv6-адрес для ICMP-проверки. IPv6-адреса допустимы только при использовании VRRPv3.

10.4 Указание пользовательского скрипта для проверки:

```
set high-availability vrrp group <имя_группы> health-check script  
<путь_к_скрипту>
```

где **<путь_к_скрипту>** – абсолютный путь к исполняемому файлу скрипта, который будет запускаться для проверки состояния узла.

Требования к скрипту:

- исполняемый файл;
- возвращает «0» при успешной проверке, иное – при сбое;
- завершается быстро (рекомендуется менее 1–2 секунд);
- не требует интерактивного ввода;
- рекомендуется расположение – «/config/scripts/», так как эта директория сохраняется при обновлениях системы.

Примечание:

На одну VRRP-группу может быть настроен только один тип health-check – либо ping, либо скрипт.

11. Отключение режима preempt:

```
set high-availability vrrp group <имя_группы> no-preempt
```


Отключает автоматическое возвращение роли Master узлу с более высоким приоритетом после его восстановления. Режим preempt включён по умолчанию.

12. Указание адреса однорангового узла (peer) для unicast-режима:

```
set high-availability vrrp group <имя_группы> peer-address <IP-адрес>
```

где **<IP-адрес>** – IPv4- или IPv6-адрес пира, с которым осуществляется обмен VRRP-пакетами в unicast-режиме. IPv6-адреса допустимы только в VRRPv3.

По умолчанию используется multicast-адресация (224.0.0.18 для IPv4, FF02::12 для IPv6). Указание peer-address переключает группу в unicast-режим.

13. Установка задержки перед preemption:

```
set high-availability vrrp group <имя_группы> preempt-delay <0-1000>
```

где **<0-1000>** – значение задержки в секундах, добавляемое к стандартному времени ожидания перехода в состояние Master. Допустимый диапазон – от «0» до «1000». Значение по умолчанию – «0».

По умолчанию, при обнаружении активного Master-узла с более низким приоритетом, резервный узел ожидает истечения advertisement timeout, рассчитываемого по формуле:

$$Advert\ timeout = 3 \times advert\_int + skew\_time,$$

$$\text{где } skew\_time = (256 - priority) / 256.$$

Например, при advert-interval = 1 и priority = 128 advertisement timeout составляет приблизительно 3,5 секунды.

Если параметр «preempt-delay» установлен в значение N, общая задержка перед переходом в состояние Master увеличивается до: *Advert timeout + N*.

Так, при preempt-delay 2 и предыдущем примере переход произойдёт примерно через 5,5 секунд.

Параметр «preempt-delay» игнорируется при активированном режиме «no-preempt».

Используется для предотвращения преждевременного перехода в Master при неготовности системы (например, при загрузке политик или сессий) или для подавления флаппинга.

14. Включение режима совместимости с RFC 3768:

```
set high-availability vrrp group <имя_группы> rfc3768-compatibility
```

RFC 3768 определяет виртуальный MAC-адрес для каждого виртуального маршрутизатора VRRP. Этот MAC-адрес используется в качестве источника во всех VRRP-объявлениях.

При активации этой опции создаётся отдельный виртуальный VRRP-интерфейс, на который автоматически назначаются:

- виртуальный MAC-адрес, определённый в RFC 3768 (00:00:5e:00:01:<VRID> для IPv4);
- виртуальный IP-адрес группы VRRP.

15. Настройка отслеживания состояния интерфейса:

```
set high-availability vrrp group <имя_группы> track interface <имя_интерфейса>
```

где **<имя_интерфейса>** – имя сетевого интерфейса, состояние которого будет отслеживаться.

При переходе отслеживаемого интерфейса в состояние down VRRP-группа немедленно переводится в состояние FAULT, независимо от текущего приоритета узла или состояния других интерфейсов. Это обеспечивает оперативное реагирование на отказ критически важных сетевых соединений и способствует корректному переключению роли Master на резервный узел в отказоустойчивой конфигурации.

16. Исключение основного VRRP-интерфейса из отслеживания:

```
set high-availability vrrp group <имя_группы> track exclude-vrrp-interface
```

Активация параметра предотвращает перевод группы в состояние FAULT при отключении основного VRRP-интерфейса.

17. Настройка скриптов для перехода между состояниями:

```
set high-availability vrrp group <имя_группы> transition-script <состояние>  
<путь_к_скрипту>
```

где:

- **<состояние>** – целевое состояние VRRP-группы, при достижении которого запускается скрипт. Допустимые значения:
 - **master** – при переходе в состояние Master;
 - **backup** – при переходе в состояние Backup;
 - **fault** – при переходе в состояние Fault;
 - **stop** – при остановке VRRP-группы.
- **<путь_к_скрипту>** – абсолютный путь к исполняемому файлу скрипта (например, «/config/scripts/vrrp-master.sh»). Скрипт должен иметь права на выполнение и быть доступен в момент срабатывания события.

Данная функциональность позволяет автоматизировать действия, связанные с изменением роли узла в отказоустойчивой конфигурации: обновление

маршрутов, переключение политик безопасности, уведомления, синхронизацию сессий и другие операции.

18. Временное отключение VRRP-группы:

```
set high-availability vrrp group <имя_группы> disable
```

Команда останавливает работу группы без удаления конфигурации. Все функции VRRP (объявления, переходы между состояниями и т.д.) приостанавливаются. Конфигурация сохраняется и может быть вновь активирована без повторной настройки.

9.1.4 Динамическая корректировка стоимости маршрута

Система **ARMA Стена** имеет возможность автоматически изменять настройки динамической маршрутизации в зависимости от текущего состояния VRRP-группы. Это позволяет исключить ситуации, когда резервный узел или узел, который находится в состоянии FAULT, продолжает объявлять маршруты или использоваться как основной. При настроенной динамической корректировке стоимости автоматически запускается служба «vrrp-routing-handler». Эта служба отслеживает состояние VRRP-группы и применяет соответствующие параметры маршрутизации.

На текущий момент поддерживается корректировка для следующих протоколов:

- «OSPF»;
- «OSPFv3»;
- «BGP».

1. Команда для настройки корректировки стоимости маршрутов для протокола OSPF:

```
set high-availability config-override vrrp group <vrrp-group> <master | backup>  
protocols ospf interface <interface> cost <cost>
```

где:

- **<vrrp-group>** - наименование VRRP-группы, для которой будет применяться корректировка.

Примечание:

VRRP-группа должна быть определена заранее с помощью команды «**set high-availability vrrp group**» (см. [Команды настройки группы VRRP](#)).

- **<master | backup>** - состояния виртуального маршрутизатора. Состояние «**BACKUP**» включает в себя также состояние «**FAULT**».
- **<interface>** - интерфейс, для которого будет применяться корректировка.

Примечание:

Один и тот же интерфейс не может использоваться в нескольких VRRP-группах, если для них включён config-override.

- **<cost>** - стоимость маршрута.
2. Команда для настройки корректировки стоимости маршрутов для протокола OSPFv3:

```
set high-availability config-override vrrp group <vrrp-group> <master | backup>  
protocols ospfv3 interface <interface> cost <cost>
```

3. Команда для настройки корректировки стоимости маршрутов для протокола BGP:

```
set high-availability config-override vrrp group <vrrp-group> <master | backup>  
policy route-map VRRP-BGP-OUT
```

Примечание:

Для протокола BGP не используется атрибут стоимости **<cost>**, вместо этого применяется **<route-map>**. В состоянии **«BACKUP»** route-map VRRP-BGP-OUT активен и подавляет анонсы маршрутов. В состоянии **«MASTER»** route-map удаляется, а маршруты анонсируются в обычном режиме. Route-map VRRP-BGP-OUT создаётся автоматически. Для просмотра route-map используется следующая команда:

```
show policy route-map VRRP-BGP-OUT
```

9.1.5 Группа синхронизации VRRP

Группа синхронизации VRRP (VRRP Sync Group) объединяет несколько VRRP-групп в единый логический блок, обеспечивая синхронное изменение их состояний (MASTER / BACKUP / FAULT). При переходе любого участника группы в новое состояние все остальные участники немедленно принимают то же состояние. Данная функциональность направлена на предотвращение рассогласования ролей, что могло бы привести к ситуации, когда часть сервисов функционирует на одном узле, а другая часть – на другом.

Требования и рекомендации к конфигурированию VRRP Sync Group:

- **Единообразие приоритетов**

Все VRRP-группы, входящие в одну VRRP Sync Group, должны иметь одинаковые значения приоритета на каждом узле. Несоблюдение данного условия может привести к нестабильности (flapping), вызванной конфликтом в выборе MASTER-ноды.

- **Единообразие ролей на узле**

На одном узле все VRRP-группы внутри VRRP Sync Group должны быть сконфигурированы с одинаковой ролью – либо все как MASTER, либо все как BACKUP. Смешанная конфигурация (часть групп в роли MASTER, часть – в роли BACKUP) недопустима. На резервном узле роли должны быть противоположными.

- **Запрет циклических или перекрёстных зависимостей**

Одна и та же VRRP-группа не может входить более чем в одну VRRP Sync Group. Также недопустимо создание косвенных зависимостей между sync-группами через общие интерфейсы или скрипты, которые могут вызвать взаимную блокировку или бесконечные переключения.

Команды конфигурации VRRP Sync Group:

1. Добавление VRRP-группы в синхронизированную группу:

```
set high-availability vrrp sync-group <имя_sync-группы> member <имя_группы>
```

где:

- **<имя_sync-группы>** – имя синхронизированной группы;
- **<имя_группы>** – имя ранее настроенной VRRP-группы.

2. Настройка скрипта, выполняемого при смене состояния синхронизированной группы:

```
set high-availability vrrp sync-group <имя_sync-группы> transition-script  
<состояние> <путь_к_скрипту>
```

где:

- **<состояние>** – целевое состояние, при наступлении которого запускается скрипт. Допустимые значения:
 - **master** – при переходе в состояние Master;
 - **backup** – при переходе в состояние Backup;
 - **fault** – при переходе в состояние Fault;
 - **stop** – при остановке VRRP-группы.
- **<путь_к_скрипту>** – абсолютный путь к исполняемому файлу скрипта (например, «/config/scripts/vrrp-master.sh»). Скрипт должен иметь права на выполнение и быть доступен в момент срабатывания события.

Данная функция позволяет автоматизировать сопутствующие действия: обновление маршрутов, переключение политик безопасности, отправку

уведомлений, синхронизацию сессий и прочие операции, зависящие от текущей роли узла в отказоустойчивой конфигурации.

3. Настройка проверки работоспособности (health-check) на уровне VRRP Sync Group:

Проверка работоспособности, заданная на уровне синхронизированной группы, применяется ко всем входящим в неё VRRP-группам. В случае сбоя вся группа одновременно переводится в состояние FAULT.

3.1 Установка количества неудачных проверок до перехода в FAULT:

```
set high-availability vrrp sync-group <имя_sync-группы> health-check failure-count <число>
```

где **<число>** – целое положительное значение, определяющее количество последовательных сбоев health-check, после которого группа переходит в состояние FAULT. Значение по умолчанию – «3».

Счётчик увеличивается при каждой неудачной проверке и сбрасывается при успешной.

3.2 Задание интервала между проверками:

```
set high-availability vrrp sync-group <имя_sync-группы> health-check interval <секунды>
```

где **<секунды>** – интервал в секундах между последовательными запусками health-check. Значение по умолчанию – «60».

3.3 Настройка ICMP-проверки (ping):

```
set high-availability vrrp sync-group <имя_sync-группы> health-check ping <IP-адрес>
```

где **<IP-адрес>** – целевой IPv4- или IPv6-адрес для ICMP-запроса. Использование IPv6 допустимо только при применении протокола VRRPv3.

3.4 Указание пользовательского скрипта для проверки:

```
set high-availability vrrp sync-group <имя_sync-группы> health-check script <путь_к_скрипту>
```

где **<путь_к_скрипту>** – абсолютный путь к исполняемому файлу, выполняющему проверку состояния узла.

Требования к скрипту:

- исполняемый файл;
- возвращает «0» при успешной проверке, иное – при сбое;

- завершается быстро (рекомендуется менее 1–2 секунд);
- не требует интерактивного ввода;
- рекомендуется расположение – «/config/scripts/», так как эта директория сохраняется при обновлениях системы.

Примечание:

Для одной VRRP Sync Group может быть настроен только один тип health-check: либо ping, либо script.

Health-check, настроенный на уровне VRRP Sync Group, имеет приоритет над индивидуальными проверками отдельных VRRP-групп. При достижении порога неудачных попыток (failure-count) все группы, входящие в синхронизированную группу, немедленно переходят в состояние FAULT, независимо от результатов их собственных health-check (если таковые заданы).

9.2 Синхронизация конфигурации

Функция синхронизации конфигурации (config sync) в системе **ARMA Стена** предназначена для автоматизации обмена параметрами конфигурации между двумя маршрутизаторами, функционирующими в режиме высокой доступности.

Основное назначение функции – исключение необходимости ручного переноса изменений конфигурации с основного маршрутизатора на резервный. Синхронизация выполняется посредством **HTTP API** системы **ARMA Стена**. Поддерживается выбор конкретных разделов конфигурации для синхронизации, а также определение режима применения изменений: замена или дополнение.

Перед настройкой синхронизации отдельных разделов конфигурации рекомендуется сначала выполнить настройку самой службы синхронизации, а затем уже конфигурировать те разделы, которые планируется включить в синхронизацию. Такой порядок действий упрощает процесс инициализации синхронизации: если сначала настроить сервис (например, webproху или suricata) и лишь после этого добавить соответствующий раздел в список синхронизируемых, то первоначальная передача конфигурации на резервное устройство произойдёт только после внесения каких-либо изменений в этот раздел. В противном случае, при корректной последовательности (сначала – служба синхронизации, затем – конфигурация разделов), конфигурация синхронизируется сразу при настройке соответствующих параметров.

Для корректного выполнения синхронизации оба устройства должны удовлетворять следующим требованиям:

- находиться в рабочем состоянии;
- быть подключёнными к сети;

- функционировать под управлением идентичной версии программного обеспечения **ARMA Стена**;
- иметь одинаковый набор сетевых интерфейсов;
- обеспечивать идентичную нумерацию физических и логических интерфейсов (например, eth0, eth1 и т.д.).

Совпадение имён интерфейсов гарантирует корректное применение правил межсетевого экрана, маршрутизации и других параметров конфигурации без риска их привязки к несоответствующим интерфейсам, что критически важно для стабильной и предсказуемой работы отказоустойчивой пары.

Поддерживается синхронизация следующих разделов конфигурации (**<name>**):

- **«firewall»** – настройки правил фильтрации трафика политиками межсетевого экрана.
- **«interfaces»** – конфигурация сетевых интерфейсов всех типов:
 - **«bonding»** – агрегированные интерфейсы (объединение нескольких физических интерфейсов в один логический).
 - **«bridge»** – создание моста между интерфейсами на канальном уровне.
 - **«dummy»** – виртуальные интерфейсы.
 - **«ethernet»** – стандартные физические Ethernet-интерфейсы.
 - **«geneve»** – туннельные интерфейсы для GENEVE (Generic Network Virtualization Encapsulation).
 - **«input»** – специальные интерфейсы для обработки входящего трафика в политике.
 - **«l2tpv3»** – интерфейсы для L2TPv3 (Layer 2 Tunneling Protocol version 3).
 - **«loopback»** – виртуальный интерфейс.
 - **«macsec»** – интерфейсы с поддержкой шифрования на канальном уровне (MACsec).
 - **«openvpn»** – интерфейсы для OpenVPN-туннелей.
 - **«pppoe»** – интерфейсы для подключения через PPPoE (например, у интернет-провайдера).
 - **«pseudo-ethernet»** – псевдо-Ethernet интерфейсы для задач виртуализации.
 - **«sstpc»** – интерфейсы SSTP-клиента (Secure Socket Tunneling Protocol).

- «**tunnel**» – туннельные интерфейсы.
- «**virtual-ethernet**» – виртуальные Ethernet-интерфейсы для внутренних соединений.
- «**vti**» – виртуальные туннельные интерфейсы для IPsec.
- «**vxlan**» – интерфейсы для VXLAN (Virtual Extensible LAN).
- «**wireguard**» – интерфейсы для WireGuard-VPN.
- «**wireless**» – беспроводные (Wi-Fi) интерфейсы.
- «**wwan**» – интерфейсы для мобильной связи.
- «**nat**» – настройки трансляции сетевых адресов для IPv4 (NAT).
- «**nat66**» – настройки трансляции адресов для IPv6 (NAT66).
- «**pki**» – управление сертификатами, ключами и центрами сертификации (PKI).
- «**policy**» – политики, используемые для фильтрации и управления трафиком.
- «**protocols**» – настройки сетевых протоколов маршрутизации:
 - «**babel**» – динамический протокол маршрутизации для mesh-сетей.
 - «**bfd**» – протокол быстрого обнаружения сбоев в соединениях (Bidirectional Forwarding Detection).
 - «**bgp**» – протокол граничного шлюза для межавтономных систем (Border Gateway Protocol).
 - «**failover**» – маршруты с приоритетом для резервирования соединений.
 - «**igmp-proxy**» – прокси для IGMP (управление multicast-группами).
 - «**isis**» – протокол маршрутизации IS-IS для крупных сетей.
 - «**mpls**» – настройки MPLS (Multiprotocol Label Switching).
 - «**nhrp**» – параметры протокола разрешения следующего прыжка (Next Hop Resolution Protocol).
 - «**ospf**» – протокол динамической маршрутизации OSPF для IPv4.
 - «**ospfv3**» – протокол OSPF для IPv6.
 - «**pim**» – протокол независимой многопоточной рассылки (PIM) и IGMP.
 - «**pim6**» – протокол PIM и MLD для IPv6.

- **«rip»** – параметры протокола маршрутизации RIP.
- **«ripng»** – параметры протокола маршрутизации RIPng (для IPv6).
- **«rpki»** – настройки инфраструктуры открытых ключей для ресурсов (Resource Public Key Infrastructure).
- **«segment-routing»** – параметры технологии Segment Routing.
- **«static»** – статические маршруты.
- **«qos»** – настройки приоритетов для разных классов и типов трафика:
 - **«interface»** – интерфейсы, к которым применяются политики QoS.
 - **«policy»** – определения политик QoS (очереди, приоритеты, shaping).
- **«service»** – служебные сервисы, предоставляемые устройством:
 - **«active-sync-proxy»** – настройки прокси для ActiveSync.
 - **«console-server»** – настройки сервера последовательных консолей.
 - **«dhcp-relay»** – агент ретрансляции DHCP-запросов.
 - **«dhcp-server»** – сервер динамической настройки хостов (DHCP) для IPv4.
 - **«dhcpv6-relay»** – агент ретрансляции DHCPv6-запросов.
 - **«dhcpv6-server»** – сервер DHCP для IPv6 (DHCPv6).
 - **«dns»** – сервисы, связанные с DNS.
 - **«https»** – настройки сервиса HTTPS.
 - **«lldp»** – настройки протокола LLDP.
 - **«mdns»** – параметры multicast DNS.
 - **«monitoring»** – сервисы мониторинга.
 - **«ndp-proxy»** – прокси для протокола обнаружения соседей (NDP) в IPv6.
 - **«ntp»** – настройка синхронизации времени по NTP.
 - **«snmp»** – настройки SNMP.
 - **«tftp-server»** – TFTP-сервер для передачи конфигураций и образов.
 - **«webproxy»** – настройки веб-прокси.
- **«suricata»** – настройки системы обнаружения и предотвращения вторжений Suricata (IDS/IPS). При синхронизации данного раздела на

резервное устройство также копируются все файлы правил COB (rule-files), указанные в конфигурации службы.

- «**system**» – системные параметры устройства:
 - «**conntrack**» – отслеживание состояния сетевых соединений.
 - «**flow-accounting**» – учёт сетевого трафика.
 - «**login**» – параметры аутентификации пользователей.
 - «**option**» – системные параметры.
 - «**sflow**» – сбор и передача sFlow-данных для анализа трафика.
 - «**static-host-mapping**» – статическое сопоставление имён хостов и IP-адресов.
 - «**sysctl**» – настройка параметров ядра Linux в режиме реального времени.
 - «**time-zone**» – выбор часового пояса устройства.
- «**vpn**» – настройки виртуальных частных сетей.
- «**vrf**» – виртуальные таблицы маршрутизации (Virtual Routing and Forwarding) для изоляции сетей.

При синхронизации разделов **active-sync-proxy** и **webproxy** на резервное устройство также передаются соответствующие keytab-файлы, используемые для аутентификации в доменной инфраструктуре.

Примечание:

При переключении активной ноды в кластере все активные TCP-сессии прерываются, поскольку резервный узел не обладает информацией о текущих соединениях. По умолчанию синхронизация таблицы отслеживания соединений (conntrack) между узлами не выполняется.

Для обеспечения сохранения активных сессий при переходе (failover) рекомендуется настроить синхронизацию состояний соединений с использованием сервиса **conntrack-sync**. Подробная инструкция приведена в разделе «[Отслеживание соединений](#)».

Примечание:

При синхронизации службы **Suricata**, если в параметре **rule-files** указаны шаблонные пути вида ***.rules** (например, «/config/files/configuration/suricata/rule-files/*.rules»), система не выполнит копирование файлов правил. В результате будет выведено сообщение об ошибке: «**ERROR: vyos config sync: File not found: /config/files/configuration/suricata/rule-files/*.rules**».

Для обеспечения корректной синхронизации необходимо указывать полные и точные пути к конкретным файлам правил в параметре **rule-files**, например: «*/config/files/configuration/suricata/rule-files/custom.rules*».

9.2.1 Команды настройки синхронизации конфигурации

1. Установка режима синхронизации:

```
set service config-sync mode <load|set>
```

где **<load|set>** – режим применения конфигурации на резервном устройстве:

- **load** – полная замена целевой секции конфигурации на содержимое, полученное от основного устройства;
- **set** – добавление или обновление параметров без удаления существующих настроек, отсутствующих в синхронизируемом фрагменте.

Примечание:

Требуется предварительный анализ топологии и функциональных требований для корректного выбора синхронизируемых разделов. В частности, полная синхронизация компонентов «*interfaces*» или «*service*» может вызвать нарушение работы кластера.

2. Указание раздела конфигурации для синхронизации:

```
set service config-sync section <name>
```

где **<name>** – идентификатор поддерживаемого раздела (перечислены выше).

3. Удаление раздела конфигурации из списка синхронизации:

```
delete service config-sync section <name>
```

Примечание:

Полное удаление раздела конфигурации необходимо в случае, если раздел содержит единственную или последнюю секцию для синхронизации. Например, если ранее в разделе «*service*» была настроена синхронизация конфигурации **только** для сервиса «*webproху*», для удаления этого раздела необходимо выполнить команду **delete service config-sync section service**. Во всех остальных случаях удаление возможно с указанием пути до конкретной секции раздела.

4. Указание адреса резервного устройства:

```
set service config-sync secondary address <address>
```

где **<address>** - сетевой адрес резервного устройства, задаваемый в одном из следующих форматов: IPv4, IPv6 или полное доменное имя (FQDN).

Адрес используется основным устройством для установления HTTP-соединения с целью передачи конфигурационных данных.

5. Настройка HTTP API-ключа аутентификации для подключения к резервному устройству:

```
set service config-sync secondary key <text>
```

где **<text>** - ключ API, сгенерированный для учётной записи «admin» на резервном устройстве.

6. Указание порта подключения к резервному устройству:

```
set service config-sync secondary port <port>
```

где **<port>** - номер TCP-порта. Возможно указать значение в диапазоне от «1» до «65535». По умолчанию используется порт «8082».

Примечание:

Изменение порта не рекомендуется, так как может нарушить работу механизма синхронизации.

7. Настройка таймаута подключения к резервному устройству:

```
set service config-sync secondary timeout <timeout>
```

где **<timeout>** - время ожидания ответа в секундах. Возможно указать значение в диапазоне от «1» до «3600». По умолчанию используется установлено «60» секунд.

Примечание:

При наличии сетевой нагрузки или большом размере конфигурационного файла рекомендуется увеличить значение до 120 или более.

8. Настройка интервала автоматической проверки доступности резервного устройства:

```
set service config-sync secondary daemon poll-interval <poll_int>
```

где **<poll_int>** - интервал проверки доступности резервного устройства в секундах. Возможно указать значение в диапазоне от «1» до «3600». По умолчанию используется значение «30».

Система **ARMA Стена** автоматически обнаруживает восстановление доступности резервного устройства и выполняет отложенную синхронизацию конфигурации после его возврата в рабочее состояние.

Для отключения автоматического опроса используется команда:

```
set service config-sync secondary daemon poll-interval disable
```

9.2.2 Точечная синхронизация конфигурации

Для отдельных разделов конфигурации реализована поддержка детализированной (точечной) синхронизации, позволяющая указывать конкретные подузлы конфигурационного дерева. Такой подход обеспечивает передачу лишь необходимых фрагментов конфигурации и исключает нежелательное воздействие на несвязанные параметры.

Точечная синхронизация доступна для следующих разделов:

- **protocols ospf;**
- **protocols ospfv3;**
- **service webproxy;**
- **service https;**
- **system login.**

Для указания конкретного пути в дереве конфигурации используется расширенный синтаксис команды:

```
set service config-sync section <раздел> <путь>
```

Пример:

```
set service config-sync section protocols ospf access-list 3 export
```

В приведённом примере синхронизируется только подузел `access-list 3 export` в разделе `protocols ospf`. Изменения в других подузлах (например, `access-list 4` или `area 0`) не передаются на резервное устройство.

Дополнительно реализована возможность исключения отдельных подузлов из синхронизации при выполнении полной синхронизации всего раздела. Для этого используется команда с ключевым словом «**exclude**»:

```
set service config-sync section <раздел>  
set service config-sync section exclude <раздел> <путь_исключения>
```

Пример:

```
set service config-sync section protocols ospf  
set service config-sync section exclude protocols ospf access-list 3
```

В данном случае выполняется синхронизация всего раздела protocols ospf, за исключением подузла access-list 3. Любые изменения внутри access-list 3 игнорируются при передаче конфигурации на резервное устройство.

Для упрощения ввода длинных и глубоко вложенных путей реализована функция автозаполнения (TAB-completion), идентичная используемой в основном CLI-интерфейсе системы **ARMA Стена**. Например, при вводе команды:

```
set service config-sync section exclude protocols ospf access-list [TAB]
```

система автоматически предложит доступные варианты автозаполнения, основанные на текущей структуре конфигурации. Подсказки формируются динамически и отражают актуальное состояние конфигурационного дерева.

Данная функциональность существенно упрощает настройку синхронизации в сложных конфигурациях, содержащих большое количество вложенных объектов и параметров.

Примечание:

При настройке точечной синхронизации необходимо учитывать наличие обязательных параметров для корректной работы синхронизируемой службы. Некоторые компоненты системы требуют минимального набора параметров для активации конфигурации. Если такие параметры не включены в синхронизацию (например, явно исключены или не указаны при точечной синхронизации), конфигурация на принимающем устройстве **не будет применена**, несмотря на успешное завершение процедуры передачи.

Например, для службы **webproxy** одним из обязательных параметров является **listen-address**. При его отсутствии в передаваемой конфигурации служба **webproxy** на резервном устройстве останется **неактивной**, поскольку не будет удовлетворено минимальное требование к конфигурации. При этом система **ARMA Стена** может вывести уведомление об успешной синхронизации, поскольку передача данных выполнена без ошибок на уровне протокола синхронизации. Однако фактическое применение конфигурации на принимающей стороне завершится неудачей из-за неполного набора параметров.

9.2.3 Настройка синхронизации конфигурации в отказоустойчивом кластере

Для настройки синхронизации конфигурации между устройствами **ARMA Стена**, входящими в отказоустойчивый кластер, необходимо выполнить следующие шаги:

1. На резервном устройстве создаётся API-ключ для учётной записи «admin»:

```
set service https api keys user admin key <api-key>
```

где **<api-key>** - секретный ключ (пароль) для учётной записи «admin», используемый при аутентификации через HTTP API.

Данный ключ будет использоваться основным устройством для установления соединения с резервным устройством.

Если API-ключ был задан на этапе первоначальной установки системы, повторное выполнение команды не требуется. В случае необходимости смены ключа команда выполняется с новым значением **<api-key>**.

2. На основном устройстве настраиваются параметры синхронизации:

```
set service config-sync secondary address <slave-address>
set service config-sync secondary key <api-key>
set service config-sync mode <load|set>
set service config-sync section <name>
commit
save
```

где:

- **<slave-address>** – сетевой адрес резервного устройства (в формате IPv4, IPv6 или FQDN);
- **<api-key>** – API-ключ, созданный на резервном устройстве;
- **<load|set>** – режим применения конфигурации;
- **<name>** – идентификатор синхронизируемого раздела конфигурации (см. перечень поддерживаемых разделов в разделе [Синхронизация конфигурации](#)).

Примечание:

При указании неверного API-ключа система сохранит конфигурацию и не выдаст ошибку на этапе выполнения **«commit»**, однако синхронизация не будет выполнена. В журнале HTTPS-сервиса резервного устройства появится запись об ошибке аутентификации.

При последующих изменениях в синхронизируемом разделе и выполнении команды **«commit»** на основном устройстве будет выведено сообщение, указывающее на недоступность резервного узла, например:

```
An error occurred: HTTPSPool(host='x.x.x.x', port=8082): Max
retries exceeded with url: /config-file (Caused by
NewConnectionError('<urllib3.connection.HTTPSConnection object at
0x7f40eeef90d0>: Failed to establish a new connection: [Errno 111]
Connection refused'))
```

Данное поведение обусловлено тем, что IP-адрес основного устройства был заблокирован на резервном устройстве вследствие превышения

допустимого количества неудачных попыток аутентификации через HTTP API. Блокировка применяется в целях защиты от брутфорс-атак и сохраняется в течение заданного интервала времени (в зависимости от настроек системы безопасности резервного узла). До разблокировки IP-адреса или сброса счётчика попыток синхронизация оставаться недоступной.

Примечание:

В случае несоответствия версий программного обеспечения основного и резервного устройств при выполнении команды **«commit»** будет выведено сообщение об ошибке:

```
ERROR:ngfwos_config_sync:The version of remote node (x.x.x.x) does not  
match current node's version. Cannot synchronize with it  
ERROR:ngfwos_config_sync:Please, provide correct remote node and try again
```

Конфигурация синхронизации будет сохранена, однако передача данных выполняться не будет до устранения расхождения версий. Указанное сообщение будет отображаться при каждом последующем выполнении **«commit»**, пока версии устройств не будут приведены к идентичному состоянию.

Примечание:

Если резервное устройство недоступно в момент выполнения **«commit»**, система выведет сообщение:

```
Remote node is not available, status code: 401  
Try sync with daemon
```

9.2.4 Особенности настройки устройств кластера

9.2.4.1 Настройка прокси-сервера ActiveSync в составе кластера

Для корректной работы **ARMA Стена**, настроенных в качестве прокси-сервера ActiveSync, входящих в состав отказоустойчивого кластера, необходимо выполнить следующие действия:

1. Настроить синхронизацию конфигураций сервиса **«active-sync-proxy»**:

```
set service config-sync section service active-sync-proxy
```

2. Настроить прокси-сервер ActiveSync на ведущей **ARMA Стена** (см. [Группы пользователей](#)).
3. После выполнения настроек на ведущей **ARMA Стена** в консоли будет выведена информация о том, что файл **«*.keytab»** скопирован в резервную **ARMA Стена**:

```
INFO:ngfwos_config_sync:Upload file '/config/files/configuration/service/active-sync-proxy/kerberos/keytab/test.keytab':  
{'success': True, 'data': '/config/files/configuration/service/active-sync-proxy/kerberos/keytab/test.keytab', 'error': None}, Secondary=x.x.x.x:8082
```

Для проверки успешного копирования файла необходимо перейти в каталог «/config/files/configuration/service/active-sync-proxy/kerberos/keytab/» на резервной **ARMA Стена** и найти файл «test.keytab».

9.2.4.2 Настройка сервера OpenConnect в составе кластера

Для корректной работы **ARMA Стена**, настроенных в качестве сервера OpenConnect, входящих в состав отказоустойчивого кластера, необходимо выполнить следующие действия:

1. На обоих **ARMA Стена** настроить виртуальный маршрутизатор и дополнительно ввести следующие команды:

```
set high-availability vrrp sync-group <syncname> member <nameVR>  
set service conntrack-sync accept-protocol tcp  
set service conntrack-sync accept-protocol udp  
set service conntrack-sync accept-protocol icmp  
set service conntrack-sync event-listen-queue-size 8  
set service conntrack-sync failover-mechanism vrrp sync-group <syncname>  
set service conntrack-sync interface <iname>  
set service conntrack-sync mcast-group 225.0.0.50  
set firewall global-options state-policy established action accept
```

где:

- **<syncname>** – имя группы синхронизации;
 - **<nameVR>** – имя виртуального маршрутизатора;
 - **<iname>** – имя интерфейса, используемого для синхронизации;
2. Для настройки синхронизации конфигураций «**vpn**» и «**pki**» ввести следующие команды:

```
set service https api keys user <username> key <examplepassword>  
set service config-sync mode load  
set service config-sync secondary address [<slave-address> | <fqdn>]  
set service config-sync secondary key <examplepassword>  
set service config-sync section vpn  
set service config-sync section pki
```

где **<username>** и **<examplepassword>** – учётные данные;

3. Настроить OpenConnect на ведущей **ARMA Стена** (см. [OpenConnect](#)).

Примечание:

При переключении устройств отказоустойчивого кластера происходит прерывание существующих VPN-соединений, так как новое активное устройство не обладает информацией об актуальных сессиях предыдущего устройства, что влечёт за собой необходимость повторного инициирования VPN-подключения пользователями.

9.3 Пример настройки отказоустойчивого кластера

В качестве примера приведён порядок настройки **ARMA Стена** в режиме отказоустойчивого кластера согласно схеме, представленной на рисунке (см. [Рисунок – Схема стенда для настройки режима отказоустойчивого кластера](#)).

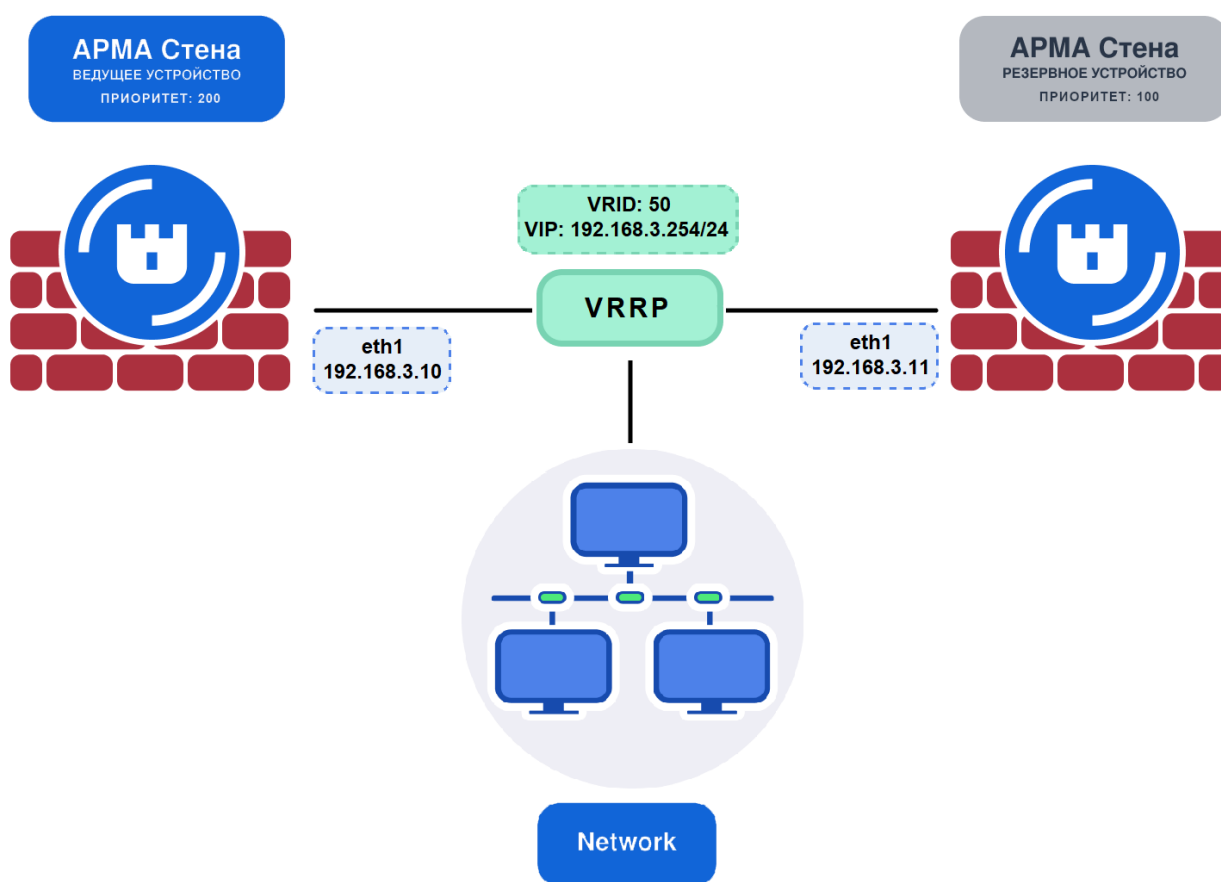


Рисунок – Схема стенда для настройки режима отказоустойчивого кластера

Для настройки работы в режиме отказоустойчивого кластера и создания виртуального маршрутизатора в сети «192.168.3.0/24» **на каждом устройстве ARMA Стена** необходимо выполнить следующие действия:

1. Включить возможность привязки сетевых приложений к IP-адресам, которые не существуют на сетевых интерфейсах или недоступным на момент инициализации служб:

```
set system sysctl parameter net.ipv4.ip_nonlocal_bind value 1
```

2. Назначить имя виртуального маршрутизатора и перейти к его настройке:

```
admin@ngfwos# set high-availability vrrp group <nameVR>
[edit]
admin@ngfwos# edit high-availability vrrp group <nameVR>
```

где **<nameVR>** – имя виртуального маршрутизатора. В качестве примера использовано имя **«vr1»**.

3. Назначить интерфейс:

```
[edit high-availability vrrp group vr1]
admin@ngfwos# set interface eth1
```

где **«eth1»** – имя интерфейса.

4. Назначить идентификатор:

```
[edit high-availability vrrp group vr1]
admin@ngfwos# set vrid 50
```

где **«50»** – идентификатор.

5. Назначить виртуальный адрес:

```
[edit high-availability vrrp group vr1]
admin@ngfwos# set address 192.168.3.254/24
```

где **«192.168.3.254/24»** – виртуальный IP-адрес в формате CIDR.

6. Указать приоритет для виртуального маршрутизатора:

```
[edit high-availability vrrp group vr1]
admin@ngfwos# set priority 200
```

где **«200»** – величина приоритета. Возможно указать значение в диапазоне от «1» до «255», при этом значение 255 соответствует наивысшему приоритету.

По умолчанию используется значение «100».

Примечание:

На резервной **ARMA Стена** необходимо указывать значение приоритета пониженное, относительно приоритета ведущей **ARMA Стена**.

7. Зафиксировать изменения с помощью ввода команд **«commit»** и **«save»**.

Для просмотра статуса необходимо ввести команду **«run show vrrp»**.

Для отключения виртуального маршрутизатора следует ввести команду:

```
set high-availability vrrp group <nameVR> disable
```

9.4 Пример настройки динамической корректировки стоимости маршрута

В качестве примера приведён порядок настройки динамической корректировки стоимости маршрута для протокола OSPF на двух **ARMA Стена**, которые работают в режиме отказоустойчивого кластера согласно схеме, представленной на рисунке (см. [Рисунок – Схема стенда для настройки динамической корректировки стоимости маршрута](#)).

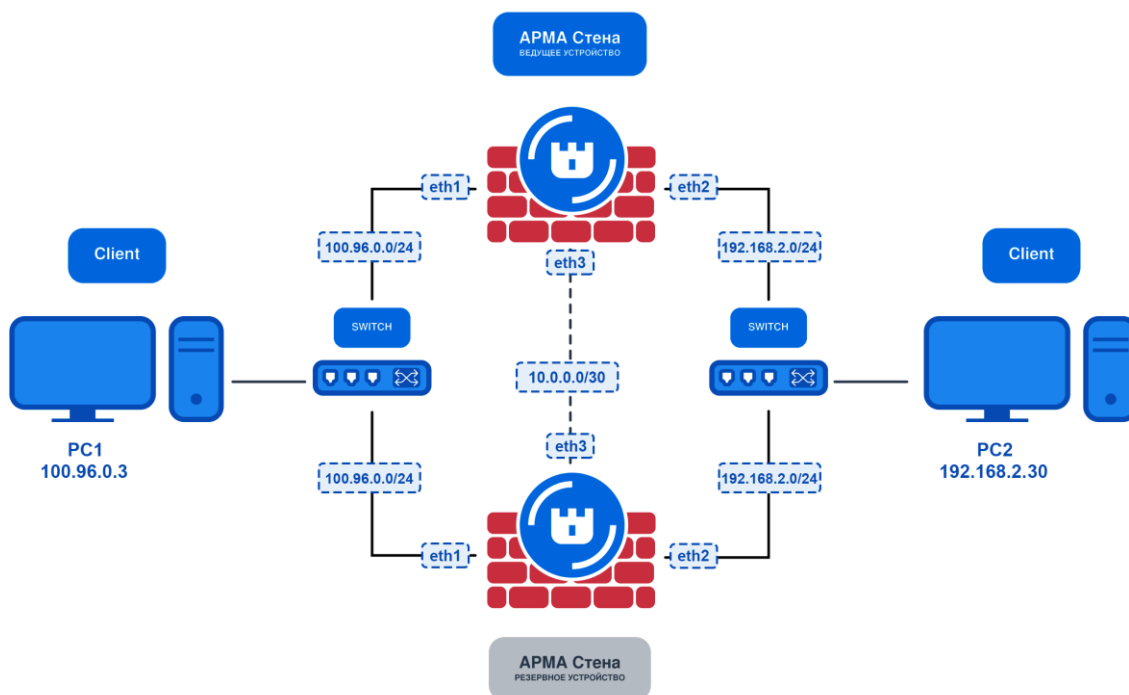


Рисунок – Схема стенда для настройки динамической корректировки стоимости маршрута

Пример настройки для протокола OSPF

Предварительно **на каждом устройстве ARMA Стена** необходимо выполнить следующие действия:

1. Задать адреса для сетевых интерфейсов.

- На ведущем устройстве **ARMA Стена**:

```
set interfaces ethernet eth3 address '10.0.0.1/30'
set interfaces ethernet eth1 address '100.96.0.1/24'
set interfaces ethernet eth2 address '192.168.2.1/24'
commit
save
```

- На резервном устройстве **ARMA Стена**:

```
set interfaces ethernet eth3 address '10.0.0.2/30'  
set interfaces ethernet eth1 address '100.96.0.2/24'  
set interfaces ethernet eth2 address '192.168.2.2/24'  
commit  
save
```

2. Выполнить настройку VRRP-групп, параметров кластеризации и протокола OSPF:

- На ведущем устройстве **ARMA Стена**:

```
set high-availability vrrp group External address 100.96.0.254/24  
set high-availability vrrp group External interface 'eth1'  
set high-availability vrrp group External vrid 10  
set high-availability vrrp group Internal address 192.168.2.254/24  
set high-availability vrrp group Internal interface 'eth2'  
set high-availability vrrp group Internal vrid '20'  
set high-availability vrrp sync-group CLUSTER member 'External'  
set high-availability vrrp sync-group CLUSTER member 'Internal'  
set protocols ospf parameters router-id 100.96.0.1  
set protocols ospf area 0 network '100.96.0.0/24'  
set protocols ospf area 0 network '192.168.2.0/24'  
set protocols ospf interface eth2 passive  
set protocols ospf interface eth1 hello-interval 1  
set protocols ospf interface eth1 dead-interval 4  
commit  
save
```

- На резервном устройстве **ARMA Стена**:

```
set high-availability vrrp group External address 100.96.0.254/24
set high-availability vrrp group External interface 'eth1'
set high-availability vrrp group External vrid 10
set high-availability vrrp group Internal address 192.168.2.254/24
set high-availability vrrp group Internal interface 'eth2'
set high-availability vrrp group Internal vrid '20'
set high-availability vrrp sync-group CLUSTER member 'External'
set high-availability vrrp sync-group CLUSTER member 'Internal'
set high-availability vrrp group External priority 50
set high-availability vrrp group Internal priority 50
set protocols ospf parameters router-id 100.96.0.2
set protocols ospf area 0 network '100.96.0.0/24'
set protocols ospf area 0 network '192.168.2.0/24'
set protocols ospf interface eth2 passive
set protocols ospf interface eth1 hello-interval 1
set protocols ospf interface eth1 dead-interval 4
commit
save
```

После выполнения предварительных настроек необходимо указать параметры динамической корректировки стоимости маршрута:

- На ведущем устройстве **ARMA Стена**:

```
#Назначить корректировку стоимости маршрута через установку значения
для мастер ноды для всех интерфейсов, которые используют соединение
OSPF:
set high-availability config-override vrrp group External master protocols ospf
interface eth1 cost 222
set high-availability config-override vrrp group Internal master protocols ospf
interface eth2 cost 222

#Назначить корректировку стоимости маршрута через установку значения
для бекап ноды для всех интерфейсов, которые используют соединение
OSPF:
set high-availability config-override vrrp group External backup protocols ospf
interface eth1 cost 22222
set high-availability config-override vrrp group Internal backup protocols ospf
interface eth2 cost 22222

commit
save
```

- На резервном устройстве **ARMA Стена**:

```
#Назначить корректировку стоимости маршрута через установку значения
для мастер ноды для всех интерфейсов, которые используют соединение
OSPF:
set high-availability config-override vrrp group External master protocols ospf
interface eth1 cost 333
set high-availability config-override vrrp group Internal master protocols ospf
interface eth2 cost 333

#Назначить корректировку стоимости маршрута через установку значения
для бекап ноды для всех интерфейсов, которые используют соединение
OSPF:
set high-availability config-override vrrp group External backup protocols ospf
interface eth1 cost 33333
set high-availability config-override vrrp group Internal backup protocols ospf
interface eth2 cost 33333

commit
save
```

Примечание:

Настройки для протокола OSPFv3 аналогичны настройкам протокола OSPF.

Пример настройки для протокола BGP

Предварительно **на каждом устройстве ARMA Стена** необходимо выполнить следующие действия:

1. Задать адреса для сетевых интерфейсов.

- На ведущем устройстве **ARMA Стена**:

```
set interfaces ethernet eth3 address '10.0.0.1/30'
set interfaces ethernet eth1 address '100.96.0.1/24'
set interfaces ethernet eth2 address '192.168.2.1/24'
commit
save
```

- На резервном устройстве **ARMA Стена**:


```
set interfaces ethernet eth3 address '10.0.0.2/30'  
set interfaces ethernet eth1 address '100.96.0.2/24'  
set interfaces ethernet eth2 address '192.168.2.2/24'  
commit  
save
```

2. Выполнить настройку VRRP-групп, параметров кластеризации и BGP соседства:

- На ведущем устройстве **ARMA Стена**:

```
set high-availability vrrp group External address 100.96.0.254/24  
set high-availability vrrp group External interface 'eth1'  
set high-availability vrrp group External vrid 10  
set high-availability vrrp group Internal address 192.168.2.254/24  
set high-availability vrrp group Internal interface 'eth2'  
set high-availability vrrp group Internal vrid '20'  
set high-availability vrrp sync-group CLUSTER member 'External'  
set high-availability vrrp sync-group CLUSTER member 'Internal'  
set protocols bgp address-family ipv4-unicast network 192.168.2.0/24  
set protocols bgp neighbor 100.96.0.3 address-family ipv4-unicast  
set protocols bgp neighbor 100.96.0.3 remote-as 65003  
set protocols bgp neighbor 100.96.0.3 timers connect 5  
set protocols bgp neighbor 100.96.0.3 timers holdtime 10  
set protocols bgp neighbor 100.96.0.3 timers keepalive 3  
set protocols bgp system-as 65001  
commit  
save
```

- На резервном устройстве **ARMA Стена**:

```
set high-availability vrrp group External address 100.96.0.254/24
set high-availability vrrp group External interface 'eth1'
set high-availability vrrp group External vrid 10
set high-availability vrrp group Internal address 192.168.2.254/24
set high-availability vrrp group Internal interface 'eth2'
set high-availability vrrp group Internal vrid '20'
set high-availability vrrp sync-group CLUSTER member 'External'
set high-availability vrrp sync-group CLUSTER member 'Internal'
set high-availability vrrp group External priority 50
set high-availability vrrp group Internal priority 50
set protocols bgp address-family ipv4-unicast network 192.168.2.0/24
set protocols bgp neighbor 100.96.0.3 address-family ipv4-unicast
route-map
set protocols bgp neighbor 100.96.0.3 remote-as 65003
set protocols bgp neighbor 100.96.0.3 timers connect 5
set protocols bgp neighbor 100.96.0.3 timers holdtime 10
set protocols bgp neighbor 100.96.0.3 timers keepalive 3
set protocols bgp system-as 65002
commit
save
```

После выполнения предварительных настроек необходимо указать параметры динамической корректировки стоимости маршрута:

- На ведущем устройстве **ARMA Стена**:

```
set high-availability config-override vrrp group External backup policy route-
map VRRP-BGP-OUT
set high-availability config-override vrrp group External master policy route-
map VRRP-BGP-OUT
set high-availability config-override vrrp group Internal backup policy route-
map VRRP-BGP-OUT
set high-availability config-override vrrp group Internal master policy route-map
VRRP-BGP-OUT

commit
save
```

- На резервном устройстве **ARMA Стена**:

```
set high-availability config-override vrrp group External backup policy route-  
map VRRP-BGP-OUT  
set high-availability config-override vrrp group External master policy route-  
map VRRP-BGP-OUT  
set high-availability config-override vrrp group Internal backup policy route-  
map VRRP-BGP-OUT  
set high-availability config-override vrrp group Internal master policy route-map  
VRRP-BGP-OUT  
  
commit  
save
```

10 БАЛАНСИРОВКА НАГРУЗКИ

10.1 Балансировка нагрузки на WAN-интерфейсах

Подсистема балансировки нагрузки автоматически добавляет маршруты для каждого пути в таблицу маршрутизации и балансирует трафик между настроенными интерфейсами в зависимости от работоспособности и веса интерфейса.

Минимально необходимая конфигурация для балансировки WAN-интерфейса должна включать в себя следующие элементы:

- требуется добавить как минимум один сетевой интерфейс маршрутизатора с заданным адресом и адресом следующего узла;
- необходимо добавить хотя бы одно правило с балансируемыми интерфейсами.

Примечание:

Балансировка нагрузки не используется совместно с динамической маршрутизацией. Сервис создаёт настраиваемые таблицы маршрутизации и правила брандмауэра, что делает его несовместимым с протоколами динамической маршрутизации.

10.1.1 Основные настройки

Основные настройки предназначены для изменения глобальных параметров балансировки на WAN-интерфейсах. Изменение глобальных настроек выполняется в конфигурационном режиме.

Примечание:

Изменение глобальных настроек требует наличия хотя бы одного интерфейса, для которого настроена проверка состояния (см. [Проверка состояния интерфейсов](#)).

1. Отключить механизм автоматической генерации правил SNAT:

```
set load-balancing wan disable-source-nat
```

По умолчанию интерфейсы, используемые в пуле балансировки нагрузки, заменяют IP-адрес источника исходящего пакета на свой собственный адрес, что гарантирует поступление ответов на один и тот же интерфейс. Это работает с помощью автоматически сгенерированных правил SNAT, которые применяются только к сбалансированному трафику. В тех случаях, когда такое поведение нежелательно, автоматическую генерацию правил SNAT возможно отключить.

2. Включить балансировку нагрузки WAN для локального трафика:

```
set load-balancing wan enable-local-traffic
```

3. Включить очистку таблиц отслеживания подключений при изменении состояния соединения:

```
set load-balancing wan flush-connections
```

Примечание:

Очистка таблицы соединений приведёт к тому, что будет выполняться балансировка пакетов вместо балансировки потоков до момента повторного установления соединений.

4. Указать пользовательский скрипт, который будет запускаться при изменении состояния балансируемого интерфейса:

```
set load-balancing wan hook /config/scripts/<file.script>
```

где **<file.script>** - имя файла скрипта в каталоге */config/scripts/*.

Примечание:

В названии файла скрипта недопустимо использовать символы: пробел, «'», «\». Максимальный размер файла не более 1 мегабайта.

Скрипт должен возвращать «0» для обозначения успешного результата и значение отличное от «0» - для неудачных результатов. Система перестанет отвечать на запросы, если выполнение скрипта не завершится!

5. Разрешить «липкие» сессии - возможность отправки ответных пакетов с сетевого интерфейса, входящего в группу балансировочных интерфейсов, откуда поступил запрос:

```
set load-balancing wan sticky-connections inbound
```

10.1.2 Проверка состояния интерфейсов

Работоспособность WAN-каналов, используемых сервисом балансировки, периодически проверяется несколькими способами:

1. Отправка сообщения ICMP Echo Request на удалённые хосты.
2. Мониторинг времени жизни сетевого пакета (TTL).
3. Выполнение специального пользовательского скрипта.

Если канал не проходит проверку, он исключается из списка используемых сервисом балансировки.

Каждая проверка настраивается для отдельного хоста-получателя и предполагает выполнение соответствующего теста. В случае необходимости проверки нескольких

хостов-получателей необходимо настроить несколько тестов, каждый из которых будет выполняться в определённом порядке.

Примечание:

Для корректной работы проверки состояния необходимо задать статический маршрут до следующего узла для каждого из проверяемых интерфейсов (см. [Настройка статического маршрута](#)).

Пример команды для настройки статического маршрута:

```
set protocols static route 8.8.8.8/32 next-hop 192.168.43.100 interface eth1
```

Для настройки параметров проверки состояния интерфейсов возможно использовать следующие команды:

1. Добавить проверяемый интерфейс:

```
set load-balancing wan interface-health <interface>
```

где **<interface>** - имя проверяемого интерфейса.

2. Задать количество проваленных ICMP-запросов после которого считается, что интерфейс не работоспособен:

```
set load-balancing wan interface-health <interface> failure-count <f_count>.
```

где **<f_count>** - количество ошибок. Возможно указать значение в диапазоне от «1» до «10». По умолчанию используется значение «1».

3. Задать количество успешных ICMP-запросов после которого считается, что интерфейс работоспособен:

```
interface-health <имя_интерфейса> success-count <s_count>
```

где **<s_count>** - количество успешных запросов. Возможно указать значение в диапазоне от «1» до «10». По умолчанию используется значение «1».

4. Задать адрес узла, через который будет осуществляться доступ к хосту-получателю:

```
set load-balancing wan interface-health <interface> nexthop <IPv4_address | dhcp>
```

Возможно указать **«IPv4-адрес»** узла или **«DHCP»**.

5. Указать номер правила в соответствии с его очередностью:

```
set load-balancing wan interface-health <interface> test <rule_number>
```

где **<rule_number>** - номер правила. Возможно указать значение в диапазоне от «0» до «4294967295».

6. Указать тип проверки доступности узла:

```
set load-balancing wan interface-health <interface> test <rule_number> type  
<check_type>
```

где **<check_type>** - тип проверки доступности узла. Возможно указать значение из списка:

- **«ping»**;
- **«TTL»**;
- **«user-defined»** - указать пользовательский скрипт, описывающий характер проверки.

7. Указать пользовательский скрипт, описывающий характер проверки, если в качестве типа проверки доступности выбрано **«user-defined»**:

```
set load-balancing wan interface-health <interface> test <rule_number> test-script  
<script_path>
```

где **<script_path>** - путь к файлу скрипта и его имя.

8. Указать значение максимального времени ожидания ответа на сообщение ICMP в секундах:

```
set load-balancing wan interface-health <interface> test <rule_number> resp-time  
<time>
```

где **<time>** - время отклика в секундах. Возможно указать значение в диапазоне от «1» до «30». По умолчанию используется значение «5».

9. Задать предельное время жизни (число узлов):

```
set load-balancing wan interface-health <interface> test <rule_number> ttl-limit  
<h_count>
```

где **<h_count>** - число прыжков. Возможно указать значение в диапазоне от «1» до «254». По умолчанию используется значение «1».

Примечание:

Параметр определяет количество переходов между каждой парой шлюзов на пути к хосту-получателю. Он используется для тестирования с протоколом UDP, когда выбирается тип тестирования **«TTL»**. Успешным результатом является получение в ответ сообщения ICMP Time Expired.

10. Задать IPv4-адрес хоста-получателя, на который будут отправляться сообщения ICMP Echo Request:

```
set load-balancing wan interface-health <interface> test <rule_number> target  
<IPv4-address>
```

10.1.3 Правила балансировки

Балансировка нагрузки представляет собой совокупность правил, определяющих тип трафика, подлежащего распределению, а также перечень таблиц маршрутизации и их значимости.

Каждое правило включает в себя критерии соответствия и таблицы маршрутизации с присвоенной значимостью. Правила пронумерованы и выполняются в установленном порядке, начиная с «1» и заканчивая «9999».

Примечание:

Номер правила является уникальным идентификатором, который не может быть изменён. Для изменения номера правила необходимо удалить его и создать заново с новым номером. Рекомендуется назначать номера правил балансировки нагрузки, оставляя свободные интервалы. Например, возможно создать набор правил с номерами 10, 20, 30 и т. д. Это позволит в случае необходимости добавить новое правило в определённое место в текущей последовательности без удаления текущего набора правил.

Общие настройки балансировки

Для изменения общих настроек балансировки введите в конфигурационном режиме следующие команды:

1. Задать приоритет правила балансировки:

```
set load-balancing wan rule <priority>
```

где **<priority>** - приоритет правила. Возможно указать значение в диапазоне от «1» до «9999».

2. Задать описание правила:

```
set load-balancing wan rule <priority> description <text>
```

где **<text>** - описание правила.

3. Задать режим резервирования канала в качестве режима балансировки:

```
set load-balancing wan rule <priority> failover
```

По умолчанию используется режим **балансировки** трафика - система выполняет распределение трафика пропорционально отношению значимости интерфейса.

При включении режима **резервирования канала** - весь трафик идёт через основной интерфейс, а в случае его отказа - через резервный. В этом случае вместо балансировки трафика между всеми работоспособными WAN каналами трафик передаётся только по активному. В случае отказа активного WAN канала на эту роль выбирается другой из списка резервных на основе состояния и значимости интерфейса. Оставшиеся WAN каналы становятся резервными по отношению к новому активному.

Примечание:

Роли WAN-каналов и соответствующих им интерфейсов могут быть выбраны на основе порядка правил балансировки. В связи с тем, что автоматическое перераспределение установленных ранее сессий между активными и резервными каналами WAN не осуществляется, необходимо включить параметр **«Очищать таблицы отслеживания подключений при изменении состояния соединения»** (см. [Основные настройки](#)).

4. Задать пакетный тип проверки трафика:

```
set load-balancing wan rule <priority> per-packet-balancing
```

По умолчанию используется **поточковый** тип проверки - для исходящего трафика по умолчанию применяется балансировка потоков в полном объёме. Для функционирования в данном режиме используется механизм отслеживания соединений на основе IP-адресов отправителя и получателя, а также номеров портов отправителя и получателя. Каждый поток связывается с определённым сетевым интерфейсом в соответствии с установленными правилами балансировки, в результате чего все сетевые пакеты, относящиеся к данному потоку, перенаправляются через этот интерфейс. Преимуществом данного режима работы является сохранение последовательности пакетов при использовании различных скоростей передачи данных для различных подключений.

Включение **пакетного** типа проверки балансировка пакетов для исходящего трафика позволяет достичь лучших показателей, но только при условии, что нарушение порядка пакетов не повлияет на функционирование сетевой инфраструктуры.

5. Включить режим, при котором трафик, соответствующий правилу, не будет перенаправляться:

```
set load-balancing wan rule <priority> exclude
```

«Небалансируемый трафик» - трафик, который соответствует правилу, не балансируется, а маршрутизируется в соответствии с записями в системной

таблице маршрутизации. Задать параметр возможно, если используется режим **балансировки трафика**.

Настройка балансируемых интерфейсов

Для настройки балансируемых интерфейсов введите в конфигурационном режиме следующие команды:

1. Задать интерфейс, который будет использоваться правилом:

```
set load-balancing wan rule <priority> interface <interface>
```

где **<interface>** - имя интерфейса. Допускается указание как физических, так и виртуальных интерфейсов.

2. Указать значимость интерфейса:

```
set load-balancing wan rule <priority> interface <interface> weight <weight>
```

где **<weight>** - значимость интерфейса. Возможно указать значение в диапазоне от «1» до «255»

Примечание:

Отношение значимостей интерфейсов будет применяться с помощью алгоритма взвешенного случайного распределения в балансировке трафика. Пример, значимости 2 и 1 балансируемых интерфейсов означают, что через первый пойдёт 66% трафика, а через второй - 33%.

3. Указать входящий интерфейс:

```
set load-balancing wan rule <priority> inbound-interface <interface>
```

Ограничение скорости

Примечание:

Настройки ограничения скорости применяются в том случае, если параметр **«Небалансируемый трафик»** не задан. Правило будет срабатывать, если скорость трафика будет соответствовать заданной.

Для настройки ограничения скорости введите в конфигурационном режиме следующие команды:

1. Задать вариант сравнения, выше или ниже заданного лимита скорости.

```
set load-balancing wan rule <priority> limit threshold <above | below>
```

где **<above | below>** - выше или ниже лимита соответственно.

2. Задать количество сетевых пакетов, которое используется для расчёта скорости:

```
set load-balancing wan rule <priority> limit rate <lim_rate>
```

где **<lim_rate>** - количество сетевых пакетов. Возможно указать значение в диапазоне от «0» до «4294967295».

3. Задать период времени, в течение которого производится расчёт скорости:

```
set load-balancing wan rule <priority> limit period <lim_period>
```

где **<lim_period>** - период времени, в течение которого производится расчёт. Возможно указать значение из списка:

- **«hour»** - в течение часа;
- **«minute»** - в течение минуты;
- **«second»** - в течение секунды.

4. Задать количество пакетов, допустимое для превышения лимита в течение указанного периода времени:

```
set load-balancing wan rule <priority> limit burst <lim_burst>
```

где **<lim_burst>** - допустимое превышение лимита. Возможно указать значение в диапазоне от «0» до «4294967295»

Транспортный протокол

Для настройки балансировки протоколов транспортного уровня, инкапсулируемых в IP протокол, введите в конфигурационном режиме следующие команды:

1. Указать номер или наименование протокола:

```
set load-balancing wan rule <priority> protocol <prot_num|prot_name>
```

где:

- **<prot_num>** - номер протокола. Возможно указать значение в диапазоне от «0» до «255».
- **<prot_name>** - наименование протокола. Пример допустимых значений:
 - **«all»**;
 - **«tcp_udp»**;
 - **«ethernet»**.

Примечание:

При указании наименования протокола возможно использовать **клавишу «Tab»** на клавиатуре для вывода информации о доступных к использованию параметрах.

2. Балансировка всех, кроме указанных протоколов:

```
set load-balancing wan rule <priority> protocol <!prot_num|!prot_name>
```

Параметры отправителя

Параметры отправителя позволяют настроить параметры правил в зависимости от источника трафика. Для настройки введите в конфигурационном режиме следующие команды:

1. Задать адрес отправителя:

```
set load-balancing wan rule <priority> source address <source_address>
```

где **<source_address>** - адрес отправителя. Возможно указать значения в следующих форматах:

- **<x.x.x.x>** - IPv4 адрес;
- **<x.x.x.x/x>** - IPv4 подсеть;
- **<x.x.x.x>-<x.x.x.x>** - диапазон IPv4 адресов;
- **!<x.x.x.x>** - все, кроме указанного адреса;
- **!<x.x.x.x/x>** - все, кроме указанной подсети;
- **!<x.x.x.x>-<x.x.x.x>** - все, кроме указанного диапазона адресов

2. Задать порт отправителя:

```
set load-balancing wan rule <priority> source port <source_port>
```

где **<source_port>** - порт отправителя. Возможно указать значение в диапазоне от «1» до «65535» в следующих форматах:

- **<xxxxxx>** - порт отправителя;
- **<xxxxxx>-<xxxxxx>** - диапазон портов;
- **!<xxxxxx>** - все, кроме указанного порта;
- **!<xxxxxx>-<xxxxxx>** - все, кроме указанного диапазона портов.

3. Указать используемый протокол:

```
set load-balancing wan rule <priority> source port <protocol>
```

где **<protocol>** - наименование протокола. Пример допустимых значений:

- **«echo»;**
- **«ssh»;**
- **«https».**

Примечание:

При указании наименования протокола возможно использовать **клавишу «Tab»** на клавиатуре для вывода информации о доступных к использованию параметрах.

Параметры получателя

Параметры получателя позволяют настроить параметры правил в зависимости от адресата трафика. Для настройки введите в конфигурационном режиме следующие команды:

1. Задать адрес получателя трафика:

```
set load-balancing wan rule <priority> destination address <destination_address>
```

где **<destination_address>** - адрес получателя трафика. Возможно указать значения в следующих форматах:

- **<x.x.x.x>** - IPv4 адрес;
- **<x.x.x.x/x>** - IPv4 подсеть;
- **<x.x.x.x>-<x.x.x.x>** - диапазон IPv4 адресов;
- **!<x.x.x.x>** - все, кроме указанного адреса;
- **!<x.x.x.x/x>** - все, кроме указанной подсети;
- **!<x.x.x.x>-<x.x.x.x>** - все, кроме указанного диапазона адресов.

2. Задать порт получателя трафика:

```
set load-balancing wan rule <priority> destination port <destination_port>
```

где **<destination_port>** - порт получателя трафика. Возможно указать значение в диапазоне от «1» до «65535» в следующих форматах:

- **<xxxxxx>** - порт получателя трафика;
- **<xxxxxx>-<xxxxxx>** - диапазон портов;
- **!<xxxxxx>** - все, кроме указанного порта;
- **!<xxxxxx>-<xxxxxx>** - все, кроме указанного диапазона портов.

3. Указать используемый протокол:

```
set load-balancing wan rule <priority> destination port <protocol>
```

где **<protocol>** - наименование протокола. Пример допустимых значений:

- **«echo»;**
- **«ssh»;**

- «https».

Примечание:

При указании наименования протокола возможно использовать **клавишу «Tab»** на клавиатуре для вывода информации о доступных к использованию параметрах.

10.1.4 Пример настройки

В качестве примера используется настройка резервирования канала и схема стенда, представленная на рисунке (см. [Рисунок – Схема стенда для настройки резервирования канала](#)).

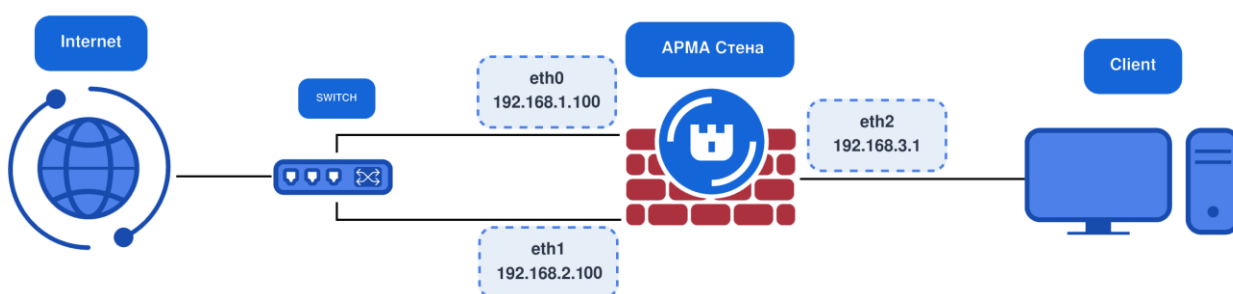


Рисунок – Схема стенда для настройки резервирования канала

Предварительно система **ARMA Стена** настроена следующим образом:

1. Созданы группы и заданы адреса для ethernet интерфейсов:

```
set firewall group interface-group WAN interface 'eth0'
set firewall group interface-group WAN interface 'eth1'
set interfaces ethernet eth0 address '192.168.1.100/24'
set interfaces ethernet eth1 address '192.168.2.100/24'
set interfaces ethernet eth2 address '192.168.3.1/24'
commit
save
```

2. Настроены правила NAT:

```
set nat source rule 10 outbound-interface group 'WAN'
set nat source rule 10 translation address 'masquerade'
commit
save
```

Список команд для настройки:

```
set load-balancing wan interface-health eth0 nexthop '192.168.1.1'  
set load-balancing wan interface-health eth1 nexthop '192.168.2.1'  
set load-balancing wan rule 10 failover  
set load-balancing wan rule 10 inbound-interface 'eth2'  
set load-balancing wan rule 10 interface eth0  
set load-balancing wan rule 10 interface eth1  
commit  
save
```

10.2 Обратный прокси-сервер

ARMA Стена включает в себя функциональность обратного прокси-сервера, обеспечивающего высокую доступность, распределение нагрузки и проксирование для приложений на основе TCP (уровень 4) и HTTP (уровень 7).

10.2.1 Основные настройки обратного прокси-сервера

10.2.1.1 Глобальные настройки

Блок **«Глобальные настройки»** предназначен для глобальных параметров обратного прокси-сервера - лимита подключений и используемого шифрования.

1. Задать лимит максимального количества подключений:

```
set load-balancing reverse-proxy global-parameters max-connections <number>
```

где **<number>** - лимит максимального количества подключений. Возможно указать значение в диапазоне от «1» до «2000000».

2. Задать алгоритм шифрования для соединений по протоколу SSL/TLS:

```
set load-balancing reverse-proxy global-parameters ssl-bind-ciphers <ciphers>
```

где **<ciphers>** - алгоритм шифрования. Возможно указать значение из списка:

- ecdhe-ecdsa-aes128-gcm-sha256;
- ecdhe-rsa-aes128-gcm-sha256;
- ecdhe-ecdsa-aes256-gcm-sha384;
- ecdhe-rsa-aes256-gcm-sha384;
- ecdhe-ecdsa-chacha20-poly1305;
- ecdhe-rsa-chacha20-poly1305;
- dhe-rsa-aes128-gcm-sha256;
- dhe-rsa-aes256-gcm-sha384.

3. Указать минимально необходимую версию TLS:

```
set load-balancing reverse-proxy global-parameters tls-version-min <version>
```

где **<version>** - версия TLS. Возможно указать значение «1.2» или «1.3».

10.2.1.2 Группы backend-серверов

Блок «Группы Backend-серверов» предназначен для конфигурации групп серверов, известных как бэкенд-серверы, которые обрабатывают входящие запросы, поступающие через обратный прокси-сервер. Основная функция данного блока заключается в реализации внутренней логики распределения трафика между серверами.

1. Задать имя для группы бэкенд-серверов:

```
set load-balancing reverse-proxy backend <backend_name>
```

где **<backend_name>** - имя группы. Ограничения:

- допускаются только строчные и прописные символы латинского алфавита и цифры;
- может содержать дефисы («-») и нижние подчёркивания («_»).

2. Задать описание для группы бэкенд-серверов:

```
set load-balancing reverse-proxy backend <name> description <description>
```

где **<description>** - описание группы. Длина описания не должна превышать 255 символов.

3. Задать алгоритм балансировки для бэкенд-сервера:

```
set load-balancing reverse-proxy backend <backend_name> balance <balance>
```

где **<balance>** - алгоритм балансировки. Возможно указать значение из списка:

- source-address;
- round-robin (по умолчанию);
- least-connection.

4. Задать режим работы бэкенд-сервера:

```
set load-balancing reverse-proxy backend <backend_name> mode <mode_type>
```

где **<mode_type>** - режим работы бэкенд-сервера. Возможно указать значение из списка:

- tcp;
- http.

5. Задать адрес бэкенд-сервера, на который будет перенаправляться входящий трафик:

```
set load-balancing reverse-proxy backend <backend_name> server <server_name>  
address <IP-address>
```

где:

- **<IP-address>** - IP-адрес сервера в формате IPv4 **<x.x.x.x>** и IPv6 **<h:h:h:h:h:h:h:h>**;
- **<server_name>** - имя сервера. Ограничения:
 - допускаются только строчные и прописные символы латинского алфавита и цифры;
 - может содержать дефисы («-») и нижние подчёркивания («_»).

6. Задать порт для бэкенд-сервера:

```
set load-balancing reverse-proxy backend <backend_name> server <server_name>  
port <port>
```

где **<port>** - порт. Возможно указать значение из диапазона от «1» до «65535»

7. Включить проверку работоспособности для бэкенд-сервера:

```
set load-balancing reverse-proxy backend <backend_name> server <server_name>  
check
```

По умолчанию функциональность выключена.

8. Отправить заголовок прокси-протокола 1 версии (текстовый формат):

```
set load-balancing reverse-proxy backend <backend_name> server <server_name>  
send-proxy
```

По умолчанию функциональность выключена.

9. Отправить заголовок прокси-протокола 2 версии (двоичный формат):

```
set load-balancing reverse-proxy backend <backend_name> server <server_name>  
send-proxy-v2
```

По умолчанию функциональность выключена.

10. Настроить использование SSL-шифрования и проверки подлинности серверной части с помощью корневого сертификата:

```
set load-balancing reverse-proxy backend <backend_name> ssl ca-certificate <ca-  
certificate>
```

где **<ca-certificate>** - имя сертификата.

11. Настроить использование SSL-шифрования без проверки сертификата сервера:

```
set load-balancing reverse-proxy backend <backend_name> ssl no-verify
```

12. Задать имя для заголовка HTTP ответа, который будет включаться во все ответы для запросов к бэкэнд-серверу:

```
set load-balancing reverse-proxy backend <backend_name> http-response-headers  
<header-name>
```

где **<header-name>** - значение заголовка HTTP-ответа. Допускается использование только латинские буквы, цифры и символы ASCII, за исключением «'», «"». Значение не должно начинаться с пробела или спецсимволов: «//», «-».

13. Задать заголовок HTTP ответа, который будет включаться во все ответы для запросов к бэкэнд-серверу:

```
set load-balancing reverse-proxy backend <backend_name> http-response-headers  
<header-name> value <header-value>
```

где **<header-value>** - заголовок HTTP ответа. Длина значения не должна превышать 64 символов.

14. Включить проверку работоспособности HTTP с использованием HTTP-запроса:

```
set load-balancing reverse-proxy backend <backend_name> http-check
```

В результате выполнения запроса система ожидает успешный код ответа в диапазоне от «200» до «399».

15. Задать HTTP-метод, который будет использоваться при проверке:

```
set load-balancing reverse-proxy backend <backend_name> http-check method  
<method>
```

где **<method>** - HTTP-метод, который будет использоваться при проверке. Возможно указать значение из списка:

- option;
- get;
- post;
- put.

16. Установить конечную точку, которая будет использоваться для проверки работоспособности:

```
set load-balancing reverse-proxy backend <backend_name> http-check uri <path>
```

где **<path>** - путь до конечной точки. Ограничения:

- должен начинаться с косой черты («/»);
- не должен содержать символ решётки («#») и пробелы.

17. Задать ожидаемый результат для определения работоспособности сервера:

```
set load-balancing reverse-proxy backend <backend_name> http-check expect status <condition>
```

где **<condition>** - ожидаемый результат. Возможно указать значение в диапазоне от «200» до «399».

18. Задать содержимое ответа при определении работоспособности сервера:

```
set load-balancing reverse-proxy backend <backend_name> http-check expect string <string>
```

где **<string>** - содержимое ответа.

19. Настроить проверку работоспособности для TCP-бэкендов:

```
set load-balancing reverse-proxy backend <backend_name> health-check <protocol>
```

где **<protocol>** - протокол, который использует TCP-бэкенд. Возможно указать значение из списка:

- ldap;
- redis;
- mysql;
- pgsql;
- smtp.

Примечание:

Если протокол не будет задан, система предпримет попытку базовой проверки работоспособности TCP. Сервер считается подключённым к сети, если он отвечает на попытку подключения действительным пакетом SYN/ACK.

20. Задать таймаут проверки установки соединения:

```
set load-balancing reverse-proxy backend <backend_name> timeout check <check_timeout>
```

где **<check_timeout>** - таймаут проверки установки соединения. Возможно указать значение в диапазоне от «1» до «3600».

21. Задать таймаут ожидания успешной попытки подключения к серверу:

```
set load-balancing reverse-proxy backend <backend_name> timeout connect  
<wait_timeout>
```

где **<wait_timeout>** - таймаут ожидания успешной попытки подключения. Возможно указать значение в диапазоне от «1» до «3600».

22. Задать таймаут бездействия на стороне сервера:

```
set load-balancing reverse-proxy backend <backend_name> timeout server  
<timeout>
```

где **<timeout>** - таймаут бездействия на стороне сервера. Возможно указать значение в диапазоне от «1» до «3600».

23. Использовать бэкенд сервер как резервный:

```
set load-balancing reverse-proxy backend <backend_name> server <server_name>  
backup
```

24. Задать номер правила для группы бэкенд-серверов:

```
set load-balancing reverse-proxy backend <backend_name> rule <rule_number>
```

где **<rule_number>** - номер правила. Возможно указать значение в диапазоне от «1» до «10000».

25. Задать URL для перенаправления:

```
set load-balancing reverse-proxy backend <backend_name> rule <rule_number> set  
redirect-location <URL>
```

где **<URL>** - адрес для перенаправления. Ограничения:

- длина значения не должна превышать 242 символа;
- должен начинаться с косой черты («/»);
- допускаются только строчные и прописные символы латинского алфавита и цифры;
- может содержать точки («.»), дефисы («-»), косые черты («/») и нижние подчёркивания («_»).

26. Задать параметры соответствия SSL:

```
set load-balancing reverse-proxy backend <backend_name> rule <rule_number> ssl  
<ssl_param>
```

где **<ssl_param>** - параметры соответствия SSL. Возможно указать значение из списка:

- req-ssl-sni;
- ssl-fc-sni;
- ssl-fc-sni-end.

27. Задать сервер для группы бэкенд-серверов:

```
set load-balancing reverse-proxy backend <backend_name> set server  
<server_name>
```

28. Задать режим поиска в URL:

```
set load-balancing reverse-proxy backend <backend_name> rule <rule_number>  
url-path <search_mod>
```

где **<search_mod>** - режим поиска. Возможно указать значение из списка:

- begin - совпадение в начале;
- end - совпадение в конце;
- exact - полное совпадение.

29. Задать содержимое шаблона поиска в URL:

```
set load-balancing reverse-proxy backend <backend_name> rule <rule_number>  
url-path <search_mod> <URL_sample>
```

где **<URL_sample>** - адрес для поиска. Ограничения:

- должен начинаться с косой черты («/»);
- допускаются только строчные и прописные символы латинского алфавита и цифры;
- может содержать точки («.»), дефисы («-»), косые черты («/»), нижние подчёркивания («_»).

30. Задать содержимое шаблона поиска в доменном имени:

```
set load-balancing reverse-proxy backend <backend_name> rule <rule_number>  
domain-name <domain_name>
```

где **<domain_name>** - доменное имя. Ограничения:

- длина доменного имени не должна превышать 242 символа;
- длина доменной группы не должна превышать 63 символа;
- может содержать дефисы («-») и точки («.»), но они не могут быть на первом и последнем месте;

- число групп, которые разделены точкой, не может быть больше 127.

10.2.1.3 Службы обратного прокси

Раздел «**Службы обратного прокси**» отвечает за определение параметров точек входа для внешнего сетевого трафика. Она включает указание IP-адреса и порта, на которых будет осуществляться мониторинг входящих соединений, а также выбор протоколов. Конфигурация также определяет параметры обработки для обеспечения защищённого взаимодействия с клиентами. Дополнительно она включает правила маршрутизации, такие как сопоставление доменных имён или путей запросов с соответствующими backend-серверами.

1. Указать имя службы:

```
set load-balancing reverse-proxy service <service_name>
```

где **<service_name>** - имя службы. Ограничения:

- допускаются только строчные и прописные символы латинского алфавита и цифры;
 - может содержать дефисы («-») и нижние подчёркивания («_»).
2. Указать группу бэкенд-серверов, которая будет использоваться для выбранной службы:

```
set load-balancing reverse-proxy service <service_name> backend  
<backend_name>
```

3. Добавить описание для выбранной службы:

```
set load-balancing reverse-proxy service <service_name> description <description>
```

4. Задать режим работы для выбранной службы:

```
set load-balancing reverse-proxy service <service_name> mode <mode_type>
```

где **<mode_type>** - режим работы для выбранной службы. Возможно указать значение из списка:

- http;
 - tcp.
5. Задать порт, на котором обратный прокси будет принимать входящие подключения для выбранной службы:

```
set load-balancing reverse-proxy service <service_name> port <port>
```

6. Перенаправить HTTP трафик на HTTPS для выбранной службы:

```
set load-balancing reverse-proxy service <service_name> redirect-http-to-https
```

7. Указать сертификат, который будет использоваться при перенаправлении HTTP трафика на HTTPS:

```
set load-balancing reverse-proxy service <service_name> ssl certificate <cert_name>
```

где **<cert_name>** - имя сертификата.

Примечание:

Для просмотра всех доступных сертификатов выполните команду
«**show pki certificate**».

8. Задать тайм-аут ожидания данных при контент-инспекции TCP-запроса для выбранной службы:

```
set load-balancing reverse-proxy service <service_name> tcp-request inspect-delay  
<timeout_in_ms>
```

где **<timeout_in_ms>** - таймаут ожидания данных. Возможно указать значение из диапазона от «1» до «65535».

9. Задать имя заголовка HTTP ответа для выбранной службы:

```
set load-balancing reverse-proxy service <service_name> http-response-headers  
<header_name>
```

10. Задать значение заголовка HTTP ответа для выбранной службы:

```
set load-balancing reverse-proxy service <service_name> http-response-headers  
<header_name> value <header_value>
```

где **<header_value>** - значение заголовка HTTP-ответа. Допускается использование только латинские буквы, цифры и символы ASCII, за исключением «'», «"». Значение не должно начинаться с пробела или спецсимволов: «//», «-».

11. Задать прослушиваемый IP-адрес для выбранной службы:

```
set load-balancing reverse-proxy service <service_name> listen-address  
<IP_address>
```

12. Задать номер правила для выбранной службы:

```
set load-balancing reverse-proxy service <service_name> rule <rule_number>
```

13. Задать группу бэкенд-серверов для выбранной службы и правила:

```
set load-balancing reverse-proxy service <service_name> rule <rule_number> set  
backend <backend_name>
```

14. Задать URL для перенаправления:

```
set load-balancing reverse-proxy service <service_name> rule <rule_number> set  
redirect-location <redirect_URL>
```

где **<redirect_URL>** - адрес для перенаправления. Ограничения:

- должен начинаться с косой черты («/»);
- допускаются только строчные и прописные символы латинского алфавита и цифры;
- может содержать точки («.»), дефисы («-»), косые черты («/»), нижние подчёркивания («_»).

15. Задать параметры соответствия SSL:

```
set load-balancing reverse-proxy service <service_name> rule <rule_number> ssl  
<ssl_param>
```

где **<ssl_param>** - параметры соответствия SSL. Возможно указать значение из списка:

- req-ssl-sni;
- ssl-fc-sni;
- ssl-fc-sni-end.

16. Задать режим поиска в URL:

```
set load-balancing reverse-proxy service <service_name> rule <rule_number> url-  
path <search_mod>
```

где **<search_mod>** - режим поиска. Возможно указать значение из списка:

- begin - совпадение в начале;
- end - совпадение в конце;
- exact - полное совпадение.

17. Задать содержимое шаблона поиска в URL:

```
set load-balancing reverse-proxy service <service_name> rule <rule_number> url-  
path <search_mod> <URL_sample>
```

где **<URL_sample>** - адрес для поиска. Ограничения:

- должен начинаться с косой черты («/»);
- не может начинаться с двойной косой черты («//»);
- допускаются только строчные и прописные символы латинского алфавита и цифры;

- может содержать точки («.»), дефисы («-»), косые черты («/»), нижние подчёркивания («_»).

18. Задать содержимое шаблона поиска в доменном имени:

```
set load-balancing reverse-proxy service <service_name> rule <rule_number>
domain-name <domain_name>
```

где **<domain_name>** - доменное имя. Ограничения:

- длина доменного имени не должна превышать 242 символа;
- длина доменной группы не должна превышать 63 символа;
- может содержать дефисы («-») и точки («.»), но они не могут быть на первом и последнем месте;
- число групп, которые разделены точкой, не может быть больше 127.

10.2.2 Пример настройки обратного прокси-сервера

В качестве примера настройки функций обратного прокси-сервера используется схема стенда, представленная на рисунке (см. [Рисунок – Схема стенда для настройки функций обратного прокси-сервера](#)).

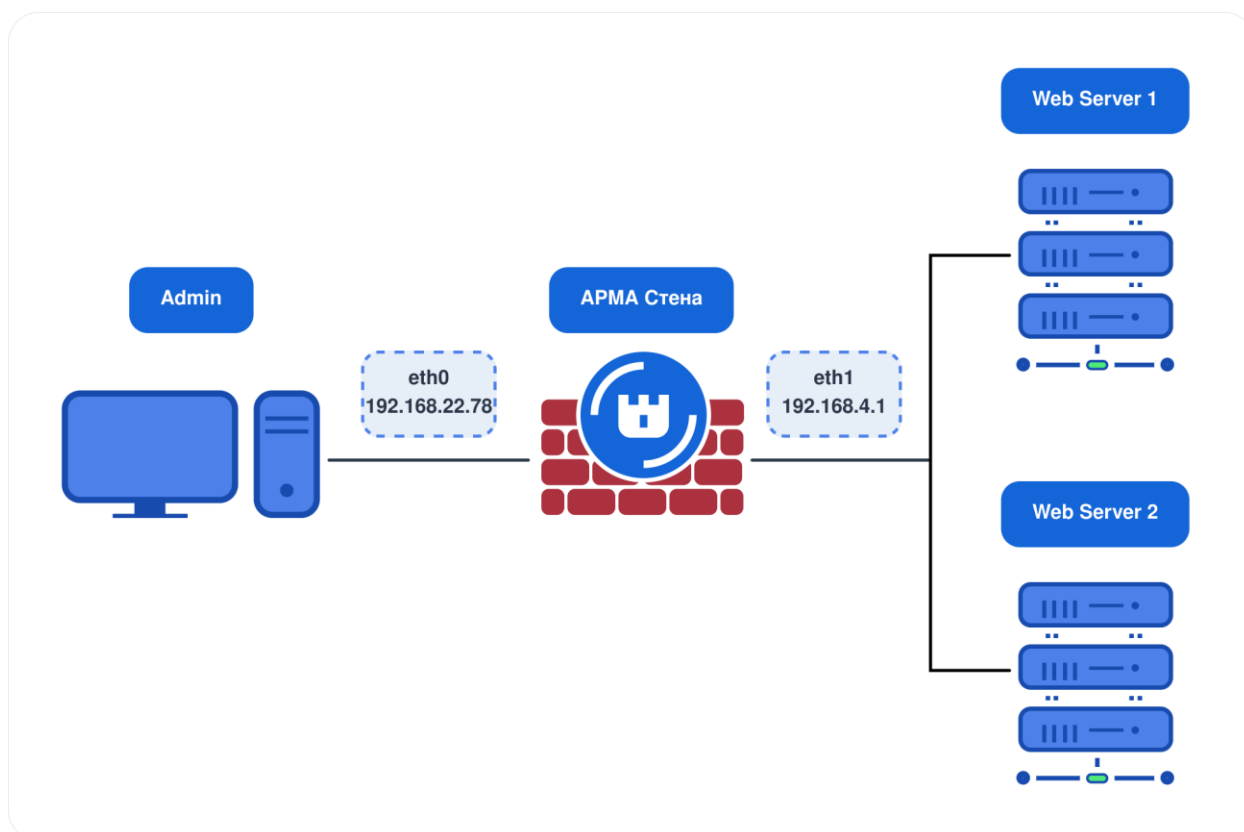


Рисунок – Схема стенда для настройки функций обратного прокси-сервера

Для настройки обратного прокси-сервера необходимо выполнить следующие команды в конфигурационном режиме:

1. Настройка backend-серверов:

```
set load-balancing reverse-proxy backend <backend_name> server <server_name1>  
address 192.168.4.10  
set load-balancing reverse-proxy backend <backend_name> server <server_name1>  
port 21  
  
set load-balancing reverse-proxy backend <backend_name> server <server_name2>  
address 192.168.4.20  
set load-balancing reverse-proxy backend <backend_name> server <server_name2>  
port 21  
  
set load-balancing reverse-proxy backend <backend_name> mode tcp
```

где:

- «**backend_name**» – имя, идентифицирующее группу серверов (backend-сервис);
- «**server_name1**», «**server_name2**» – имена отдельных серверов в группе;
- «**192.168.4.10**» – IP-адрес сервера «**Server 1**»;
- «**192.168.4.20**» – IP-адрес сервера «**Server 2**»;
- «**21**» – порт, на который будут перенаправляться клиентские запросы;
- «**tcp**» – режим проксирования, используемый для передачи данных на транспортном уровне. Допустимые значения:
 - **http** – для проксирования HTTP-трафика (работает на уровне приложений);
 - **tcp** – для проксирования произвольного TCP-трафика (работает на транспортном уровне).

2. Настройка сервиса обратного прокси:

```
set load-balancing reverse-proxy service <reverse-proxy_name> listen-address  
192.168.22.78  
set load-balancing reverse-proxy service <reverse-proxy_name> mode tcp  
set load-balancing reverse-proxy service <reverse-proxy_name> port 21  
set load-balancing reverse-proxy service <reverse-proxy_name> backend  
<backend_name>
```

где:

- «**reverse-proxy_name**» – имя создаваемого сервиса обратного прокси;
- «**192.168.22.78**» – IP-адрес сетевого интерфейса, ожидающего входящие соединения;

- «21» – порт, на котором будет приниматься внешний трафик для последующего проксирования.
3. Применить и сохранить изменения с помощью команд «**commit**» и «**save**» соответственно.

11 VPN

VPN – это обобщённое название технологий, позволяющих обеспечить одно или несколько сетевых соединений поверх другой сети, например сети Интернет.

11.1 OpenConnect

OpenConnect – ПО с открытым исходным кодом, используемое для реализации VPN.

11.1.1 Подключение через VPN-клиент

В качестве примера приведён порядок настройки OpenConnect на **ARMA Стена**.

Примечание:

На ПК **«Client»** предварительно должно быть установлено соответствующее ПО OpenConnect.

Для настройки подключения через VPN-клиент OpenConnect необходимо выполнить следующие шаги:

1. Сгенерировать ключи и сертификаты.
2. Настроить OpenConnect.

Примечание:

В случае необходимости настройки OpenConnect на **ARMA Стена**, входящих в состав отказоустойчивого кластера, следует учитывать особенности настройки, указанные в п. [Настройка сервера OpenConnect в составе кластера](#) настоящего руководства.

11.1.1.1 Генерация ключей и сертификатов

Для генерации ключа и сертификата центра сертификации необходимо в режиме конфигурирования ввести следующую команду:

```
run generate pki ca install CAname
```

где **«CAname»** – имя сертификата центра сертификации. Приведено в качестве примера.

После ввода вышеуказанной команды потребуется указать следующие значения параметра сертификата центра сертификации, нажимая для подтверждения **клавишу «ENTER»**:

- нажать **клавишу «ENTER»** на запрос:

```
Enter private key type: [rsa, dsa, ec] (Default: rsa)
```

- нажать **клавишу «ENTER»** на запрос:

```
Enter private key bits: (Default: 2048)
```

- ввести «**RU**» на запрос:

Enter country code: (Default: GB)

- ввести «**MO**» на запрос:

Enter state: (Default: Some-State)

- ввести «**Moscow**» на запрос:

Enter locality: (Default: Some-City)

- нажать **клавишу «ENTER»** на запрос:

Enter organization name: (Default: NGFWOS)

- ввести «**example.ru**» на запрос:

Enter common name: (Default: ngfwos.net)

- ввести «**365**» на запрос:

Enter how many days certificate will be valid: (Default: 1825)

- ввести «**n**» на запрос:

Do you want to encrypt the private key with a passphrase? [y/N]

Значения параметров сертификата приведены в качестве примера.

Зафиксировать изменения с помощью ввода команд «**commit**» и «**save**».

Для просмотра содержимого сертификатов и закрытых ключей необходимо ввести команду «**show pki**» в режиме конфигурирования.

Для просмотра информации о параметрах сертификатов необходимо ввести команду «**run show pki**» в режиме конфигурирования или «**show pki**» в режиме эксплуатации.

Для генерации ключа и сертификата сервера необходимо в режиме конфигурирования ввести следующую команду:

```
run generate pki certificate sign CAname install CERTname
```

где «**CERTname**» – имя сертификата. Приведено в качестве примера.

После ввода вышеуказанной команды потребуется указать следующие значения параметра сертификата, нажимая для подтверждения **клавишу «ENTER»**:

- ввести «**n**» на запрос:

Do you already have a certificate request? [y/N]

- нажать **клавишу «ENTER»** на запрос:

Enter private key type: [rsa, dsa, ec] (Default: rsa)

- нажать **клавишу «ENTER»** на запрос:

Enter private key bits: (Default: 2048)

- ввести **«RU»** на запрос:

Enter country code: (Default: GB)

- ввести **«MO»** на запрос:

Enter state: (Default: Some-State)

- ввести **«Moscow»** на запрос:

Enter locality: (Default: Some-City)

- ввести **«IWARMA»** на запрос:

Enter organization name: (Default: NGFWOS)

- ввести **«example.ru»** на запрос:

Enter common name: (Default: ngfwos.net)

- ввести **«n»** на запрос:

Do you want to configure Subject Alternative Names? [y/N]

- ввести **«365»** на запрос:

Enter how many days certificate will be valid: (Default: 365)

- нажать **клавишу «ENTER»** на запрос:

Enter certificate type: (client, server) (Default: server)

- ввести **«n»** на запрос:

Do you want to encrypt the private key with a passphrase? [y/N]

Значения параметров сертификата приведены в качестве примера.

Зафиксировать изменения с помощью ввода команд **«commit»** и **«save»**.

11.1.1.2 Настройка OpenConnect

Для настройки OpenConnect необходимо ввести следующие команды:

```
set vpn openconnect authentication local-users username User1 password
example123
set vpn openconnect authentication mode local password
```

где:

- «**User1**» – логин;
- «**example123**» – пароль. Учётные данные приведены в качестве примера.

```
set vpn openconnect network-settings client-ip-settings subnet 100.64.0.0/24
set vpn openconnect network-settings name-server 192.168.1.1
set vpn openconnect network-settings name-server 10.1.1.2
set vpn openconnect ssl ca-certificate CAname
set vpn openconnect ssl certificate CERTname
```

где:

- «**CAname**» – имя сертификата центра сертификации;
- «**CERTname**» – имя сертификата.

Зафиксировать изменения с помощью ввода команд «**commit**» и «**save**».

Для указания порта, который будет использоваться для клиентских подключений, необходимо ввести следующую команду:

```
set vpn openconnect listen-ports <tcp|udp> <number>
```

где **<number>** – номер порта для приёма соединений. Возможно указать значение в диапазоне от «1» до «65535». По умолчанию используется порт «443».

Для указания прослушиваемого адреса необходимо ввести следующую команду:

```
set vpn openconnect listen-address <IP-address>
```

где **<IP-address>** – IP-адрес.

Дополнительно возможно указать параметр «**default-domain**» для OpenConnect с помощью команды:

```
set vpn openconnect network-settings default-domain <domain>
```

где **<domain>** – доменное имя, которое будет автоматически добавляться к неполным именам доменов.

Параметр «default-domain» в конфигурации OpenConnect определяет домен по умолчанию для всех подключающихся клиентов, обеспечивая корректное разрешение имён внутри VPN-сети. Данный параметр необходим для

формирования полных доменных имён (FQDN) при обращении к сетевым ресурсам и позволяет клиентам использовать сокращённые имена хостов без указания полного доменного имени.

Примечание:

Для применения настройки указанного прослушиваемого адреса требуется перезапустить сервис «OpenConnect» с помощью ввода в режиме эксплуатации команды **«restart openconnect-server»**.

Примечание:

При подключении клиентов к серверу, сервис «OpenConnect» для каждого пользователя создаёт отдельный интерфейс, именованный в формате «sslvpnX», где «X» – идентификатор интерфейса.

11.1.1.2.1 Настройка времени сессии пользователя

Для настройки времени подключения до аутентификации необходимо ввести следующую команду:

```
set vpn openconnect timeout auth <number>
```

где **<number>** – время в секундах. Возможно указание значения в диапазоне от «1» до «2592000».

Для настройки времени, по истечении которого произойдёт разрыв сессии пользователя в случае отсутствия трафика необходимо ввести следующую команду:

```
set vpn openconnect timeout idle <number>
```

где **<number>** – время в секундах. Возможно указание значения в диапазоне от «1» до «2592000».

Для настройки времени сессии пользователя необходимо ввести следующую команду:

```
set vpn openconnect timeout session <number>
```

где **<number>** – время в секундах. Возможно указание значения в диапазоне от «1» до «2592000».

11.1.1.3 Подключение клиента

Для подключения на ПК **«Client»** выполнить следующие действия:

- перейти в раздел настройки сетевых параметров;
- выбрать «MultiProtocol VPN OpenConnect» для нового подключения;
- указать IP-адрес интерфейса с доступом к сети Интернет «203.0.113.87» в поле параметра **«Шлюз»**;

- сохранить, включить и пройти аутентификацию в появившемся окне, введя учётные данные «User1» и «example123».

где «203.0.113.87» – IP-адрес, приведён в качестве примера.

В случае появления при первом подключении предупреждающего окна нажать кнопку «**Connect anyway**».

11.1.1.4 Завершение сессии пользователя

В случае необходимости принудительного завершения сессии пользователя следует в режиме эксплуатации ввести следующую команду:

```
admin@ngfwos:~$ force openconnect-server disconnect-user <name>
```

где **<name>** – имя пользователя.

Для просмотра актуальной информации о текущих подключениях пользователей необходимо в режиме эксплуатации ввести команду «**show openconnect-server sessions**».

11.2 OpenVPN

11.2.1 Site-to-Site

В качестве примера приведён порядок настройки OpenVPN для маршрутизации трафика VPN на подсеть.

В качестве примера настройки OpenVPN будет использоваться схема стенда, представленная на рисунке (см. [Рисунок – Схема стенда для настройки VPN в режиме «сеть - сеть»](#)).

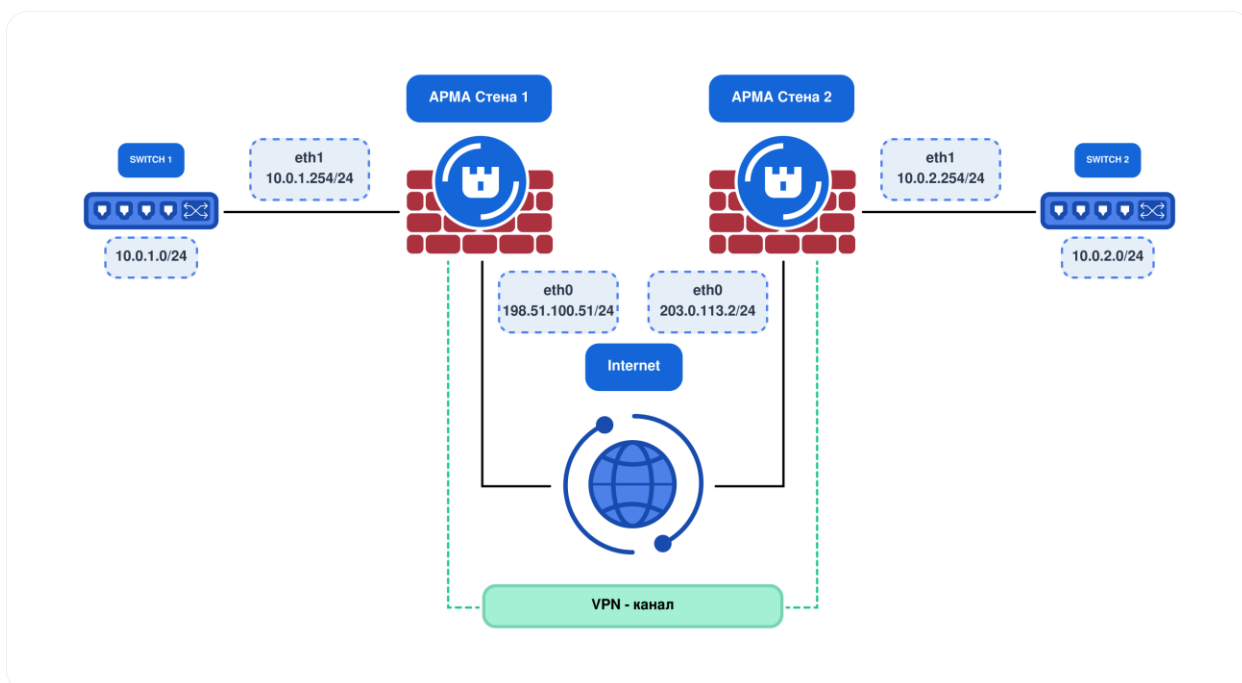


Рисунок – Схема стенда для настройки VPN в режиме «сеть - сеть»

На обоих устройствах **ARMA Стена** необходимо создать разрешающие межсетевые правила для установления соединений по протоколам SSH и OpenVPN:

- SSH:

```
set firewall ipv4 input filter rule 30 action accept
set firewall ipv4 input filter rule 30 description 'Allow_SSH'
set firewall ipv4 input filter rule 30 destination address <IP-address>/32
set firewall ipv4 input filter rule 30 destination port 22
set firewall ipv4 input filter rule 30 inbound-interface name eth0
set firewall ipv4 input filter rule 30 protocol tcp
set firewall ipv4 input filter rule 30 log
```

где **<IP-address>** – IP-адрес, назначенный для интерфейса «eth0» **ARMA Стена**, на котором выполняется настройка. В примере указаны IP-адреса «198.51.100.51» и «203.0.113.2» на **ARMA Стена 1** и **ARMA Стена 2** соответственно.

- OpenVPN:

```
set firewall ipv4 forward filter rule 30 action accept
set firewall ipv4 forward filter rule 30 description 'OpenVPN'
set firewall ipv4 forward filter rule 30 destination port 1194
set firewall ipv4 forward filter rule 30 protocol udp
set firewall ipv4 forward filter rule 30 log
```

где **<1194>** - порт, на котором ожидается соединение с удалённым сервером OpenVPN.

11.2.1.1 Настройка ARMA Стена 1

11.2.1.1.1 Генерация самоподписанного сертификата

Для генерации самоподписанного сертификата необходимо ввести следующую команду:

```
run generate pki certificate self-signed install openvpn-local
```

где **«openvpn-local»** – имя сертификата. Приведено в качестве примера.

После ввода вышеуказанной команды потребуется указать следующие значения параметра сертификата центра сертификации, нажимая для подтверждения **клавишу «ENTER»**:

- ввести **«ec»** на запрос:

```
Enter private key type: [rsa, dsa, ec] (Default: rsa)
```

- нажать **клавишу «ENTER»** на запрос:

Enter private key bits: (Default: 256)

- ввести «**RU**» на запрос:

Enter country code: (Default: GB)

- ввести «**MO**» на запрос:

Enter state: (Default: Some-State)

- ввести «**Moscow**» на запрос:

Enter locality: (Default: Some-City)

- нажать **клавишу «ENTER»** на запрос:

Enter organization name: (Default: NGFWOS)

- ввести «**example.ru**» на запрос:

Enter common name: (Default: ngfwos.net)

- ввести «**n**» на запрос:

Do you want to configure Subject Alternative Names? [y/N]

- ввести «**365**» на запрос:

Enter how many days certificate will be valid: (Default: 365)

- нажать **клавишу «ENTER»** на запрос:

Enter certificate type: (client, server) (Default: server)

- ввести «**n**» на запрос:

Do you want to encrypt the private key with a passphrase? [y/N]

Значения параметров сертификата приведены в качестве примера.

Зафиксировать изменения с помощью ввода команд «**commit**» и «**save**».

Для просмотра содержимого сертификатов и закрытых ключей необходимо ввести команду «**show pki**» в режиме конфигурирования.

Для просмотра информации о параметрах сертификатов необходимо ввести команду «**run show pki**» в режиме конфигурирования или «**show pki**» в режиме эксплуатации.

Для вывода уникального идентификатора **ARMA Стена 1** для криптографического ключа необходимо ввести следующую команду:

```
run show pki certificate openvpn-local fingerprint sha256
```

где «**sha256**» – алгоритм хеширования.

11.2.1.1.2 Настройка туннеля

Для настройки туннеля необходимо ввести следующие команды:

```
set interfaces openvpn vtun0 mode site-to-site
set interfaces openvpn vtun0 persistent-tunnel
set interfaces openvpn vtun0 local-address 10.0.1.254
set interfaces openvpn vtun0 local-port 1194
set interfaces openvpn vtun0 protocol udp
set interfaces openvpn vtun0 remote-address 10.0.2.254
set interfaces openvpn vtun0 remote-host 203.0.113.2
set interfaces openvpn vtun0 remote-port 1194
```

где:

- «**vtun0**» – имя туннеля;
- «**site-to-site**» – режим «сеть - сеть»;
- «**10.0.1.254**» – локальный IP-адрес;
- «**1194**» – порт;
- «**udp**» – протокол;
- «**10.0.2.254**» – удалённый IP-адрес;
- «**203.0.113.2**» – IP-адрес интерфейса **ARMA Стена 2** с доступом к сети Интернет.

Для указания ключа и криптографических установок необходимо ввести следующие команды:

```
set interfaces openvpn vtun0 tls certificate openvpn-local
set interfaces openvpn vtun0 tls peer-fingerprint <client cert fingerprint>
set interfaces openvpn vtun0 tls role active
```

где:

- <**client cert fingerprint**> – уникальный идентификатор **ARMA Стена 2**;
- «**active**» – роль инициатора соединения.

Зафиксировать изменения с помощью ввода команд «**commit**» и «**save**».

11.2.1.1.3 Настройка маршрута

Для указания маршрута необходимо ввести следующую команду:

```
set protocols static route 10.0.2.0/24 interface vtun0
```

где «10.0.2.0/24» – удалённая сеть.

Зафиксировать изменения с помощью ввода команд **«commit»** и **«save»**.

11.2.1.1.4 Настройка правил МЭ

Для настройки правил МЭ, разрешающих обмен данными через VPN-туннель, необходимо ввести следующие команды:

```
set firewall ipv4 input filter default-action drop
set firewall ipv4 input filter default-log
set firewall ipv4 input filter rule 10 action accept
set firewall ipv4 input filter rule 10 description 'Allow_established/related'
set firewall ipv4 input filter rule 10 state established
set firewall ipv4 input filter rule 10 state related
set firewall ipv4 input filter rule 10 inbound-interface name eth0
set firewall ipv4 input filter rule 10 log
set firewall ipv4 input filter rule 20 action accept
set firewall ipv4 input filter rule 20 description 'OpenVPN_IN'
set firewall ipv4 input filter rule 20 destination port 1194
set firewall ipv4 input filter rule 20 inbound-interface name eth0
set firewall ipv4 input filter rule 20 protocol udp
set firewall ipv4 input filter rule 20 log
```

Зафиксировать изменения с помощью ввода команд **«commit»** и **«save»**.

11.2.1.2 Настройка ARMA Стена 2

11.2.1.2.1 Генерация самоподписанного сертификата

Для генерации самоподписанного сертификата необходимо ввести следующую команду:

```
run generate pki certificate self-signed install openvpn-remote
```

где **«openvpn-remote»** – имя сертификата. Приведено в качестве примера.

После ввода вышеуказанной команды потребуется указать следующие значения параметра сертификата центра сертификации, нажимая для подтверждения **клавишу «ENTER»**:

- ввести **«ec»** на запрос:

```
Enter private key type: [rsa, dsa, ec] (Default: rsa)
```

- нажать **клавишу «ENTER»** на запрос:

```
Enter private key bits: (Default: 256)
```

- ввести «**RU**» на запрос:

Enter country code: (Default: GB)

- ввести «**MO**» на запрос:

Enter state: (Default: Some-State)

- ввести «**Moscow**» на запрос:

Enter locality: (Default: Some-City)

- нажать **клавишу «ENTER»** на запрос:

Enter organization name: (Default: NGFWOS)

- ввести «**example.ru**» на запрос:

Enter common name: (Default: ngfwos.net)

- ввести «**n**» на запрос:

Do you want to configure Subject Alternative Names? [y/N]

- ввести «**365**» на запрос:

Enter how many days certificate will be valid: (Default: 365)

- ввести «**client**» на запрос:

Enter certificate type: (client, server) (Default: server)

- ввести «**n**» на запрос:

Do you want to encrypt the private key with a passphrase? [y/N]

Значения параметров сертификата приведены в качестве примера.

Зафиксировать изменения с помощью ввода команд «**commit**» и «**save**».

Для просмотра содержимого сертификатов и закрытых ключей необходимо ввести команду «**show pki**» в режиме конфигурирования.

Для просмотра информации о параметрах сертификатов необходимо ввести команду «**run show pki**» в режиме конфигурирования или «**show pki**» в режиме эксплуатации.

Для вывода уникального идентификатора **ARMA Стена 2** для криптографического ключа необходимо ввести следующую команду:

```
run show pki certificate openvpn-remote fingerprint sha256
```

где «**sha256**» – алгоритм хеширования.

11.2.1.2.2 Настройка туннеля

Для настройки туннеля необходимо ввести следующие команды:

```
set interfaces openvpn vtun0 mode site-to-site
set interfaces openvpn vtun0 persistent-tunnel
set interfaces openvpn vtun0 local-address 10.0.2.254
set interfaces openvpn vtun0 local-port 1194
set interfaces openvpn vtun0 protocol udp
set interfaces openvpn vtun0 remote-address 10.0.1.254
set interfaces openvpn vtun0 remote-host 198.51.100.51
set interfaces openvpn vtun0 remote-port 1194
```

где:

- «**vtun0**» – имя туннеля;
- «**site-to-site**» – режим «сеть - сеть»;
- «**10.0.2.254**» – локальный IP-адрес;
- «**1194**» – порт;
- «**udp**» – протокол;
- «**10.0.1.254**» – удалённый IP-адрес;
- «**198.51.100.51**» – IP-адрес интерфейса **ARMA Стена 1** с доступом к сети Интернет.

Для указания ключа и криптографических установок необходимо ввести следующие команды:

```
set interfaces openvpn vtun0 tls certificate openvpn-remote
set interfaces openvpn vtun0 tls peer-fingerprint <server cert fingerprint>
set interfaces openvpn vtun0 tls role passive
```

где:

- <**server cert fingerprint**> – уникальный идентификатор **ARMA Стена 1**;
- «**passive**» – роль ожидающего соединения.

Зафиксировать изменения с помощью ввода команд «**commit**» и «**save**».

11.2.1.2.3 Настройка маршрута

Для указания маршрута необходимо ввести следующую команду:

```
set protocols static route 10.0.1.0/24 interface vtun0
```

где «**10.0.1.0/24**» – удалённая сеть.

Зафиксировать изменения с помощью ввода команд **«commit»** и **«save»**.

11.2.1.2.4 Настройка правил МЭ

Для настройки правил МЭ, разрешающих обмен данными через VPN-туннель, необходимо ввести следующие команды:

```
set firewall ipv4 input filter default-action drop
set firewall ipv4 input filter default-log
set firewall ipv4 input filter rule 10 action accept
set firewall ipv4 input filter rule 10 description 'Allow_established/related'
set firewall ipv4 input filter rule 10 state established
set firewall ipv4 input filter rule 10 state related
set firewall ipv4 input filter rule 10 inbound-interface name eth0
set firewall ipv4 input filter rule 10 log
set firewall ipv4 input filter rule 20 action accept
set firewall ipv4 input filter rule 20 description 'OpenVPN_IN'
set firewall ipv4 input filter rule 20 destination port 1194
set firewall ipv4 input filter rule 20 inbound-interface name eth0
set firewall ipv4 input filter rule 20 protocol udp
set firewall ipv4 input filter rule 20 log
```

Зафиксировать изменения с помощью ввода команд **«commit»** и **«save»**.

11.2.2 Сервер - Клиент

В качестве примера настройки OpenVPN будет использоваться схема стенда, представленная на рисунке (см. [Рисунок – Схема стенда для настройки VPN в режиме «Сервер - Клиент»](#)).

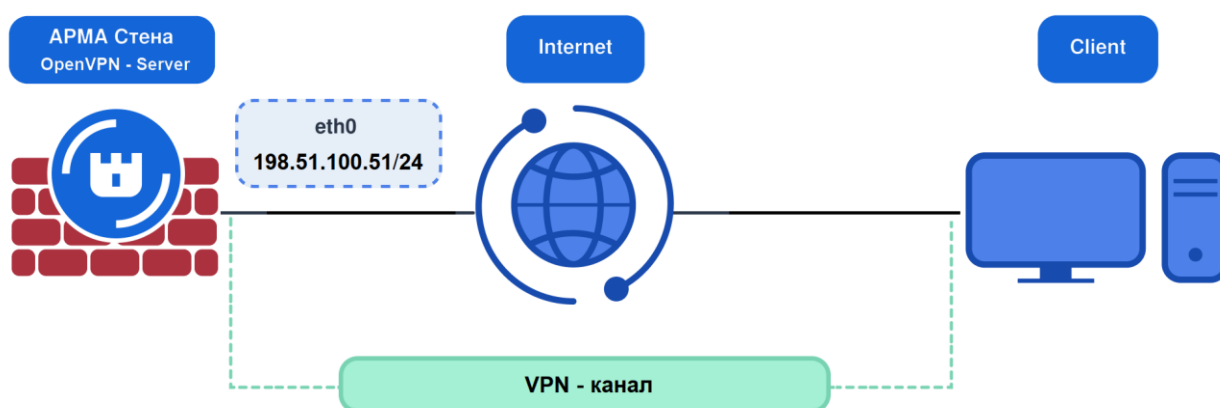


Рисунок – Схема стенда для настройки VPN в режиме «Сервер - Клиент»

11.2.2.1 Настройка ARMA Стена

11.2.2.1.1 Генерация сертификатов

Для реализации безопасного соединения необходимо сгенерировать и установить центр сертификации (CA), а также создать и подписать с его помощью серверный и

клиентский сертификаты. Помимо этого, следует сформировать параметры шифрования Диффи-Хеллмана (DH). Указанные действия выполняются в конфигурационном режиме с использованием следующих команд:

1. Сгенерировать и установить центр сертификации:

```
run generate pki ca install openvpn-server
```

где **«openvpn-server»** – имя центра сертификации. Приведено в качестве примера.

После выполнения указанной команды система запросит ввод параметров сертификата. Эти параметры могут быть оставлены без изменений, если не требуется их корректировка. Подтверждение ввода параметров осуществляется посредством нажатия **клавиши «Enter»**:

```
Enter private key type: [rsa, dsa, ec] (Default: rsa) 'rsa'
Enter private key bits: (Default: 2048) '2048'
Enter country code: (Default: GB) 'GB'
Enter state: (Default: Some-State) 'Some-State'
Enter organization name: (Default: NGFWOS) 'NGFWOS'
Enter common name: (Default: ngfwos.net) 'ngfwos.net'
Enter how many days certificate will be valid: (Default: 1825) '1825'
Note: If you plan to use the generated key on this router, do not encrypt the
private key.
Do you want to encrypt the private key with a passphrase? [y/N] 'n'
2 value(s) installed. Use "compare" to see the pending changes, and "commit"
to apply.
```

Зафиксировать изменения с помощью ввода команд **«commit»** и **«save»**.

2. Сгенерировать и установить корневой сертификат, используя для этого созданный ранее центр сертификации «openvpn-server»:

```
run generate pki certificate sign 'openvpn-server' install 'server.crt'  
# Имя «server.crt» приведено в качестве примера.
```

```
Do you already have a certificate request? [y/N] 'n'  
Enter private key type: [rsa, dsa, ec] (Default: rsa) 'rsa'  
Enter private key bits: (Default: 2048) '2048'  
Enter country code: (Default: GB) 'GB'  
Enter state: (Default: Some-State) 'Some-State'  
Enter locality: (Default: Some-City) 'Some-City'  
Enter organization name: (Default: NGFWOS) 'NGFWOS'  
Enter common name: (Default: ngfwos.net) 'ngfwos.net'  
Do you want to configure Subject Alternative Names? [y/N] 'n'  
Enter how many days certificate will be valid: (Default: 365) '365'  
Enter certificate type: (client, server) (Default: server) 'server'  
Note: If you plan to use the generated key on this router, do not encrypt the  
private key.  
Do you want to encrypt the private key with a passphrase? [y/N] 'n'  
2 value(s) installed. Use "compare" to see the pending changes, and "commit"  
to apply.
```

Зафиксировать изменения с помощью ввода команд **«commit»** и **«save»**.

3. Сгенерировать и установить клиентский сертификат, используя для этого созданный ранее центр сертификации «openvpn-server»:

```
run generate pki certificate sign 'openvpn-server' install 'client_crt'
# Имя «client_crt» приведено в качестве примера.

Do you already have a certificate request? [y/N] 'n'
Enter private key type: [rsa, dsa, ec] (Default: rsa) 'rsa'
Enter private key bits: (Default: 2048) '2048'
Enter country code: (Default: GB) 'GB'
Enter state: (Default: Some-State) 'Some-State'
Enter locality: (Default: Some-City) 'Some-City'
Enter organization name: (Default: NGFWOS) 'NGFWOS'
Enter common name: (Default: ngfwos.net) 'ngfwos.net'
Do you want to configure Subject Alternative Names? [y/N] 'n'
Enter how many days certificate will be valid: (Default: 365) '365'
Enter certificate type: (client, server) (Default: server) 'client'
Note: If you plan to use the generated key on this router, do not encrypt the
private key.
Do you want to encrypt the private key with a passphrase? [y/N] 'n'
2 value(s) installed. Use "compare" to see the pending changes, and "commit"
to apply.
```

Зафиксировать изменения с помощью ввода команд **«commit»** и **«save»**.

4. Сгенерировать и установить параметры криптографического протокола DH:

```
run generate pki dh install 'DH'
# Имя «DH» приведено в качестве примера.

Enter DH parameters key size: (Default: 2048)
Generating parameters...
1 value(s) installed. Use "compare" to see the pending changes, and "commit"
to apply.
```

Зафиксировать изменения с помощью ввода команд **«commit»** и **«save»**.

11.2.2.1.2 Настройка OpenVPN-сервера

Для настройки OpenVPN-сервера необходимо ввести следующие команды:

```
# Указать адрес OpenVPN-сервера:
set interfaces openvpn vtun0 local-host '198.51.100.51'

# Указать прослушиваемый порт OpenVPN-сервером:
set interfaces openvpn vtun0 local-port '1122'
```

```
# Указать режим работы OpenVPN:
set interfaces openvpn vtun0 mode 'server'

# Указать транспортный протокол:
set interfaces openvpn vtun0 protocol 'udp'

# Заменить маршрут по умолчанию для интерфейса vtun0 маршрутом через
туннель OpenVPN:
set interfaces openvpn vtun0 replace-default-route

# Указать адреса DNS-сервера:
set interfaces openvpn vtun0 server name-server '8.8.8.8'

# Указать подсеть, из которой будут выделяться клиентские IP-адреса:
set interfaces openvpn vtun0 server subnet '10.0.10.0/24'
```

Установить алгоритм шифрования:

```
set interfaces openvpn vtun0 encryption cipher 'aes-256-gcm'
```

где **aes-256-gcm** - выбранный алгоритм шифрования.

Для OpenVPN рекомендуется использовать следующие алгоритмы шифрования:

- **aes-256-gcm;**
- **aes-128-gcm;**
- **chacha20-poly1305.**

Система **ARMA Стена** так же поддерживает следующие алгоритмы шифрования:

- **aes-128-cbc;**
- **aes-128-cfb;**
- **aes-128-cfb1;**
- **aes-128-cfb8;**
- **aes-128-ofb;**
- **aes-192-cbc;**
- **aes-192-cfb;**
- **aes-192-cfb1;**
- **aes-192-cfb8;**
- **aes-192-gcm;**

- **aes-192-ofb;**
- **aes-256-cbc;**
- **aes-256-cfb;**
- **aes-256-cfb1;**
- **aes-256-cfb8;**
- **aes-256-ofb;**
- **aria-128-cbc;**
- **aria-128-cfb;**
- **aria-128-cfb1;**
- **aria-128-cfb8;**
- **aria-128-gcm;**
- **aria-128-ofb;**
- **aria-192-cbc;**
- **aria-192-cfb;**
- **aria-192-cfb1;**
- **aria-192-cfb8;**
- **aria-192-gcm;**
- **aria-192-ofb;**
- **aria-256-cbc;**
- **aria-256-cfb;**
- **aria-256-cfb1;**
- **aria-256-cfb8;**
- **aria-256-gcm;**
- **aria-256-ofb;**
- **camellia-128-cbc;**
- **camellia-128-cfb;**
- **camellia-128-cfb1;**
- **camellia-128-cfb8;**
- **camellia-128-ofb;**
- **camellia-192-cbc;**
- **camellia-192-cfb;**

- **camellia-192-cfb1;**
- **camellia-192-cfb8;**
- **camellia-192-ofb;**
- **camellia-256-cbc;**
- **camellia-256-cfb;**
- **camellia-256-cfb1;**
- **camellia-256-cfb8;**
- **camellia-256-ofb;**
- **des-edc-cbc;**
- **des-edc-cfb;**
- **des-edc-ofb;**
- **des-edc3-cbc;**
- **des-edc3-cfb;**
- **des-edc3-cfb1;**
- **des-edc3-cfb8;**
- **des-edc3-ofb.**

Примечание:

Для использования не рекомендованных алгоритмов шифрования необходимо дополнительно ввести следующую команду:

```
set interfaces openvpn vtun0 encryption ncp-ciphers  
<имя_алгоритма_шифрования>
```

Установить алгоритм хеширования:

```
set interfaces openvpn vtun0 hash 'sha256'
```

где **sha256** - выбранный алгоритм хеширования.

Система **ARMA Стена** поддерживает следующие алгоритмы хеширования:

- **sha3-512;**
- **sha512-256;**
- **sha224;**
- **sha3-224;**
- **sha1;**
- **sha3-384;**

- **ripemd160;**
- **sha512;**
- **sha512-224;**
- **shake256;**
- **sha384;**
- **sm3;**
- **sha3-256;**
- **md5;**
- **blake2s256;**
- **sha256;**
- **blake2b512;**
- **md5-sha1;**
- **shake128;**
- **keccak-kmac-128;**
- **keccak-kmac-256.**

Настройка TLS-аутентификации:

```
# Указать TLS-сертификат для аутентификации пользователей:
set interfaces openvpn vtun0 tls ca-certificate 'openvpn-server'

# Указать корневой сертификат:
set interfaces openvpn vtun0 tls certificate 'server.crt'

# Указать алгоритма DH:
set interfaces openvpn vtun0 tls dh-params 'DH'
```

Зафиксировать изменения с помощью ввода команд «**commit**» и «**save**».

Система **ARMA Стена** позволяет сгенерировать конфигурационный файл, который будет использоваться для настройки клиентского ПО. Для этого необходимо ввести следующую команду в конфигурационном режиме:

```
run generate openvpn client-config interface vtun0 ca openvpn-server certificate
client.crt
```

Команда отобразит настройки, которые необходимо скопировать в пользовательский файл «client.ovpn» (имя файла приведено в качестве

примера). После этого данный файл должен быть передан на клиентский компьютер.

Пример содержимого конфигурационного файла:

```
client
nobind
remote 198.51.100.51 1122
remote-cert-tls server
proto udp
dev tun
dev-type tun
persist-key
persist-tun
verb 3

# Encryption options
cipher AES-256-GCM

auth sha256
comp-lzo no

<ca>
-----BEGIN CERTIFICATE-----
MIIDPzCCAo+gAwIBAgIUM4Q8rpWrvlyupV4qswu6/uiJIMUwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCR0IxIzEzARBgNVBAMCMCINvbWUtU3RhdGUxIjAQBgNVB
AcMCVNvbWUtQ2I0eTEPMA0GA1UECgwGTkdGV09TMRMwEQYDVQQDDApuZ2Z3
b3MubmV0MB4XDTI1MDYwMjE0NTk0MFoXDTMwMDYwMTE0NTk0MFowXDELMA
kGA1UEBhMCR0IxIzEzARBgNVBAMCMCINvbWUtU3RhdGUxIjAQBgNVBAMCVCNvbWU
tQ2I0eTEPMA0GA1UECgwGTkdGV09TMRMwEQYDVQQDDApuZ2Z3b3MubmV0MII
BIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEApmtURw2j0aGSWE0xrwP+Pa
EEhbT+uFamYnqRTGW3ESvOPaMiU5ESb+tIPdDkdbdr8PTIMnNAGzC2oVL9dFIEsrhiE
1FIXvl/CS/lhb/9JJR6TdtiquAeAcE86dXjP7VzqXvAOB1rqc8mNNII1vCWK1ecQHwqVq
xDY/TxhztwuJxT9SReShpK2roCwZbZiGpFmtE8kg7EluDz6WsokNhYnK3NU9O+GOez
4XtWj69IWCUuJCjYj5gACY2z9O4pLG3XfmEv6N34+LFneXYb1BtPgrktCJoAtMD6vd
KvffEz8pW2zPR40FMqpGO1vEcylXex8mOsFIG/8yWwbTCdDGswIDAQABo2EwXzAPB
gNVHRMBAf8EBTADAQH/MA4GA1UdDwEB/wQEAwIBhjAdBgNVHSUEFjAUBggrBgE
FBQcDAgYIKwYBBQUHAAwEwHQYDVR0OBBYEF9sl79+o1ZaBm4z0lFOjVlyyMh1MA
0GCSqGSIb3DQEBCwUAA4IBAQAAdPOITFQOiPW+wei0nXj9HW+QOib3YNizwakSS5I
WP5Cmj1mS7BXddy0LA6lIFDssEOL3fnFhJPCr1XTkCrFLZ5RzSr0V7wOm2Bj8CLGnsD
WgLgtCMSM54Q2FDMJeHnKnv/Rf3uTi4F2SSyHu2Kjp0naz8N20aBQuHnEZxzBoJS
omDrvJMVlZTFd5GzVjH565xa1Vmtx52fj0MEB1i2owcxpMAG6LEMAJH2oqMS31bOo
z1dldbQ+9lfoYWIhybe9gyG3omM4v74/c8pUNQO1JMwB62ZjBexhltUrOZ5I/L7GLyu
```


x+Ort8DsabyA4eZUfxdmyNil94hlDelcJWufX

-----END CERTIFICATE-----

</ca>

<cert>

-----BEGIN CERTIFICATE-----

MIIIDuzCCAqOgAwIbAgIUaQcmhoYHQnl21sWXxFgjBZ1h5GMwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCROlxEzARBgNVBAgMCINvbWUtU3RhdGUxEjAQBgNVB
AcMCVNvbWUtQ2I0eTEPMA0GA1UECgwGTkdGV09TMRMwEQYDVQQDDApuZ2Z3
b3MubmV0MB4XDTI1MDYwMzE0MDE1MFoXDTI2MDYwMzE0MDE1MFowXDELMA
kGA1UEBhMCROlxEzARBgNVBAgMCINvbWUtU3RhdGUxEjAQBgNVBAcMCVNvbWU
tQ2I0eTEPMA0GA1UECgwGTkdGV09TMRMwEQYDVQQDDApuZ2Z3b3MubmV0MII
BIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAXPtS7EXdphd7W6qCup2Yh9h
ZII72U71Vp0s/WCvL4BJN9M5eYCMF1f8pWMnwdXzWTUtW6FRHvZAUfn/fe8TZVg4
8rcelm1nlxIUM18EMJ9goKpsjNabfcCnNXtBUUT0Gv4oTr9LiR2MjBtL7WOnklgMBOa
4AsQmp+m0mgFpKtPybiy4pZcUmwFYGAjNm1UGdQPK+NACrggVB716Aww2Y/+H
8pehD4TGLs+u1KP58PRfo/ROYNLCbP4wblEAWKJpUGtokRAfVJeZv6i1SmfrnCthXd/
hROxazpyHgC5yXhLSBfRs6sgNW26qnHMYE2G2q06hWPh0dS73f6hS4cMJ81QIDAQ
ABo3UwczAMBgNVHRMBAf8EAjAAMA4GA1UdDwEB/wQEAwIHgDATBgNVHSUED
DAKBggrBgEFBQcDAjAdBgNVHQ4EFgQUySgLwruDSVFhjN0gylZJifgi6W0wHwYDVR
OjBBGwFoAUT2yXv36jVloGbjPSUU6NUjLlyHUwDQYJKoZIhvcNAQELBQADggEBAJyP
Wtov5SkROiIVXuIIj5s6w01lr1fMWhq6XfM9is90xs1pEVa+Q0yNeOrWii6K12fNkL4oA
liJCs3BF0eW4bm/ju6irKtIH8SHusX2uzPfbUmBjOFiUFpdcuAm5mjFRsmYsFGoLGJ/djk
iAxqUlo8MtPFTOfBdXhADTmkmd3tBXzWEdAAX5m2edWi84Yck5gJE2fUa3YQFYmLn
OAJ671Rfn1b9tED3ebQOA5ktd5T4n96IP3pSydua9PeqUaF9Q5kDTbwqX8t2Z8ob5Ai
fZDP4C0rgyEqmE0kB0CjgilP0rsSAD1q13j4jZVSN+Y3I0v8lxWhTw60LgS2humdztc=

-----END CERTIFICATE-----

</cert>

<key>

-----BEGIN PRIVATE KEY-----

MIIIEvgIBADANBgkqhkiG9w0BAQEFAASCBAKgwggSkAgEAAoIBAQDE+1LsRd2mF3tb
qoK6nZiH2FmWXvZTvVWnSz9YK8vgEk30zl5glwXV/yIYyfB1fNZNS1boVEe9kBR+
f997xNIWDjytx4ibWeXGVQzXwQwn2CgqmyM1pt9wKc1e0FRRPQa/ihOv0uJHYyMG
0vtY6eSWAwE5rgCxCAN6bSaAWkq0/JuLLillxSbAVgYCM2bVQZ1A8r40AKuCBUHv
XoDDDZj/4fyl6EPHMYuz67Uo/nw9F+j9E5g0sJs/jBuUQBYomlQa2iREB9UI5m/q
LVKZ+ucK2Fd3+FE7FrOnleALnJeEtIF9GzqyA1bbqqccxgTYbarTqFY+HR1Lvd/q
FLhwwnzVAgMBAAECggEACEJATQs12pWf9K0uu3vJjiKGSQ10tviYe4HmZ0A41U13
KsUvREkboMgluAIJfKeOBalbw/RqqJo+nbonSNVtRIQk+6VCxz6q6VieB/q+U3pW
3shv3rs/IYEDLQ8/hcNxab1ci3HkTllr+ciFRMpTrO110vEGcuXEIG0YoOeIO9PL

```
pixZDKcpVEQ5dtH5Ac3JH28G3F/s04ne/R2Xsu6pqklme3dtzUEe6QL02n51F8bT
UspNUH3GrEoJNhCojYQnYtWVcF2f8lnCUCcuxQONRhJTdNKhwmEwOKiXGX6wnlwf
qyQYyabDhYEPqR12QwdUPc915iiFL5pypCJohFz+6QKBgQDt1en5TjpmCbruVX3y
RdlsbLyr9tQD7C2NDTkRo6SnPuhdMPDGn10SqWvldlahS/m2cJqQtKpEbx9Cskbf
wzNDIZVdeheP8O2P+J5tw+ijmT7OxV5JEOkwh5uxehyztRenPzOZMqs/3ragEaZk
/+Cv3dP0T8XG3e4zdM33kLyZrQKBgQDUBqXsODIZg514VNW1DXtAEIvZyfJWKR8X
5eN9MEk8M6JrV6Cb9kFer4jPthfKtX+kFdv8gJk/Ig9OrulqekyjpKcE47F+QDPz
ZoGx1QozdD7nLba+NldJpEH4nd0j6UIiWhAqSk3NUIQ1zYEAWDpQ3uRFdRd2d4jj
9GwvslekyQKBgQDL6VSyL/T32S3Q+7GBD4wLXusgUP6T4mFnhsfALNqVneThSX2V
/bpxrpo/glCPaDFPzxlMkc+13sQhjflgFR8VvmzWeUBMZBd6EYHbwFTsNw5Xf3al
FJypxAqjzntfREtkVFar6XpTx2lyuQ89lviQMBNyaxa5mzulGIQi1pAs/QKBgB9I
0KJXfR6IX+dW4MLL+UI2ac9ZmXpq4oDeeT6rrNyuZMnykwUIhW6pHeBsfb91+y3o
Ushkns0Mwr2LJIDWBY1iL52lvsM1OSHdGIKPBV8jGgdm+c1Et4D5gUUE5Bi1XIS
zvwEPts9piZ1hTnw1sntB+7FNTFE6E+hFW5kPOIJAoGBAKyuLCWFyKnW9fyBpYCV
FA6R/D6L4E85cTdr3PB6h5e7MUHJZ/i0UChi3MeDiYIBg/Eqjcr8X6mvIKPywjvL
okssSuMgS394YTfZ+XMLTRHoM4O0s9TyzlrSAWhnyApBBS8YFwVK4qk/V7dEKW+
Zqf/xixw7Jurj5t4rY17022S
-----END PRIVATE KEY-----

</key>
```

Примечание:

Для избежания ошибок при взаимодействии между устройством-клиентом и сервером OpenVPN, необходимо перед сохранением в файл удалить из сгенерированной конфигурации клиента строку **«comp-lzo no»**.

11.2.2.2 Настройка OpenVPN клиента

Рассмотрим процесс настройки клиентского оборудования на примере персонального компьютера, работающего под управлением операционной системы Windows, с установленным программным обеспечением OpenVPN Connect. Для установления соединения с OpenVPN-сервером необходимо выполнить следующие шаги:

1. Скопировать конфигурационный файл «client.ovpn» на клиентский компьютер.
2. Запустить приложение OpenVPN Connect и загрузить файл «client.ovpn».
3. В интерфейсе программы выбрать импортированный профиль и нажать кнопку «Connect» для установления соединения.
4. В процессе подключения приложение отобразит текущий статус соединения (см. [Рисунок – OpenVPN Connect](#)).

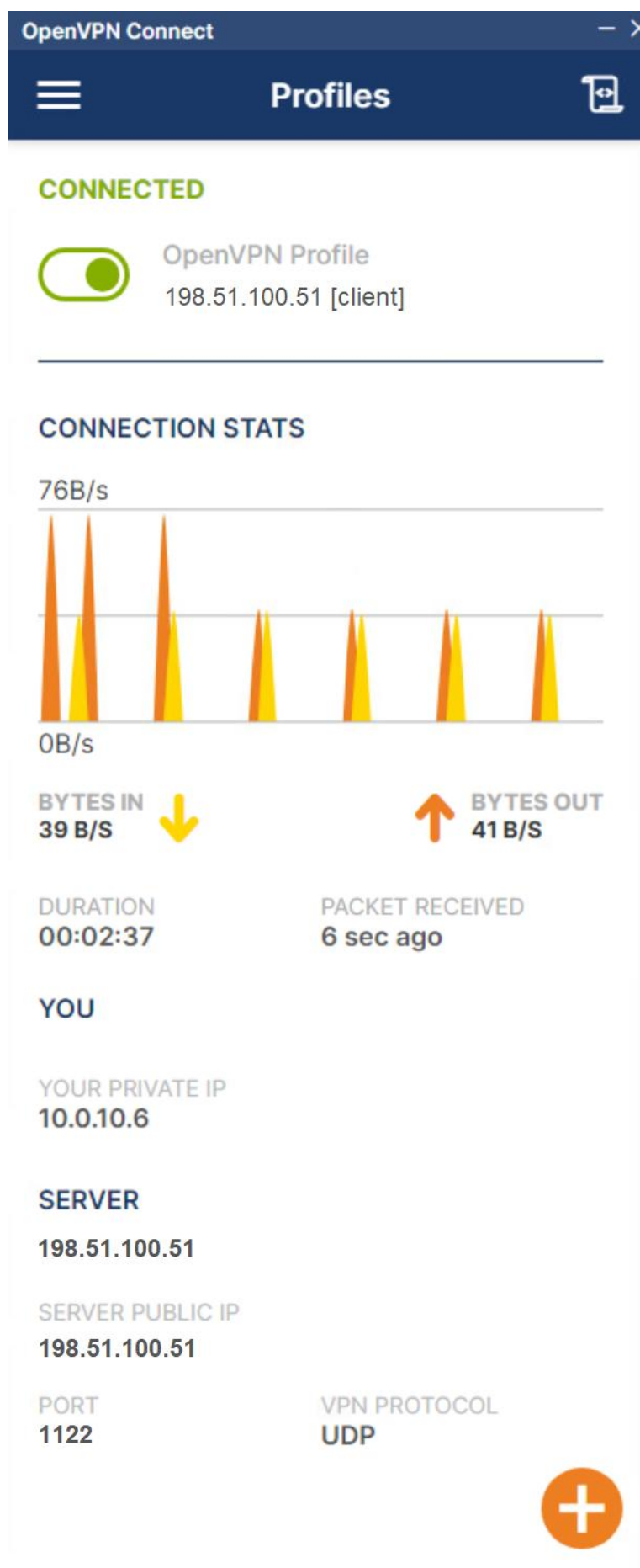


Рисунок – OpenVPN Connect

11.2.2.3 Мониторинг подключений

Для отображения списка подключённых клиентов к OpenVPN-серверу необходимо выполнить следующую команду в эксплуатационном режиме:

```
admin@ngfwos# run show openvpn server
```

Пример списка подключённых клиентов:

OpenVPN status on vtun0

Client CN	Remote Host	Tunnel IP	Local Host	TX bytes
RX bytes	Connected Since			
-----	-----	-----	-----	-----
ngfwos.net	172.30.130.29:53363	10.0.10.6	198.51.100.51:1122	4.8 KB
36.4 KB	2025-06-04 15:26:51			

11.3 IPsec

IPsec – набор протоколов для обеспечения защиты данных, передаваемых по межсетевому протоколу IP.

Установка подключения IPsec происходит в два этапа, называемые фазами IKE:

1. В первой фазе IKE две оконечные точки аутентифицируют друг друга и согласовывают ключевой материал. В результате устанавливается защищённый туннель, используемый во второй фазе для согласования защищённых соединений ESP.
2. Во второй фазе IKE две оконечные точки используют защищённый туннель, созданный в первой фазе, для согласования защищённых соединений ESP (ESP SA). ESP SA используются для шифрования пользовательских данных, передающихся между двумя оконечными точками.

Список команд глобальной настройки IPsec:

1. Отключить автоматическую установку маршрутов к удалённым сетям:

```
set vpn ipsec options disable-route-autoinstall
```

2. Разрешить отправку полезной нагрузки FlexVPN (только IKEv2):

```
set vpn ipsec options flexvpn
```

3. Указать интерфейс, на котором будут установлены виртуальные IP-адреса:

```
set vpn ipsec options interface <ethX>
```

где **<ethX>** - имя интерфейса. Если параметр не указан, адреса будут установлены на исходящем интерфейсе.

4. Разрешить установку виртуальных IP-адресов:

```
set vpn ipsec options virtual-ip
```

5. Включить журналирование:

```
set vpn ipsec log [level <value> | subsystem <value>]
```

Уровень ведения журнала возможно настроить с помощью дополнительных параметров **«level»** и **«subsystem»**:

- **level <value>** – глобальный уровень ведения журнала IPsec. Возможно указать следующие значения уровня:
 - **0** – показывает только основные события (создание/удаление SA), используется по умолчанию;
 - **1** – добавляет общие сообщения об ошибках;
 - **2** – предоставляет расширенную информацию для отладки.
- **subsystem <value>** – уровень ведения журнала подсистемы. Возможно указать следующие значения:
 - **dmn** – настройка, очистка и обработка сигналов основного демона;
 - **mgr** – менеджер IKE_SA, обработка синхронизации для доступа к IKE_SA;
 - **ike** – IKE_SA/ISAKMP SA;
 - **chd** – CHILD_SA/IPsec SA;
 - **job** – постановка задач в очередь, обработка и управление пулом потоков;
 - **cfg** – управление конфигурацией и плагинами;
 - **knl** – интерфейс ядра IPsec/сетевой интерфейс;
 - **net** – сетевая коммуникация IKE;
 - **asn** – низкоуровневое кодирование/декодирование (ASN.1, X.509 и т.д.);
 - **enc** – операции кодирования/декодирования пакетов, шифрование/дешифрование;
 - **lib** – сообщения библиотеки libstrongswan;
 - **esp** – сообщения библиотеки libipsec;

- **tls** – сообщения библиотеки libtls;
- **tnc** – Trusted Network Connect;
- **imc** – сборщик измерений целостности;
- **imv** – верификатор измерений целостности;
- **pts** – служба доверия платформы;
- **any** – любая подсистема.

11.3.1 IKE

IKE выполняет процедуру взаимной аутентификации между двумя сторонами и создаёт ассоциацию безопасности IKE (SA), которая включает в себя общую секретную информацию, используемую для быстрого установления SAS (Security Association) для полезной нагрузки безопасности Encapsulating (ESP) или заголовка аутентификации (AH). SA также включает в себя набор криптографических алгоритмов, которые будут использоваться сторонами для защиты трафика, передаваемого по SA.

В **ARMA Стена** атрибуты IKE определяются с помощью IKE-групп. В рамках одной группы возможно задать несколько предложений.

Основные команды настройки IKE-групп:

1. Определение поименованной настройки IKE для согласований первой фазы IKE:

```
set vpn ipsec ike-group <name>
```

где **<name>** - имя, используемое для обозначения настройки IKE.

2. Определение действия, которое следует предпринять, если дочерний SA недоступен:

```
set vpn ipsec ike-group <name> close-action <action>
```

где **<action>** - действие. Возможно указать следующие значения:

- **none** - ничего не предпринимать, используется по умолчанию;
- **trap** - попытка повторного согласования при обнаружении совпадающего трафика;
- **start** - восстановить соединение.

3. Определение поведения системы в том случае, если узел VPN становится недоступен:

```
set    vpn    ipsec    ike-group    <name>    dead-peer-detection    <action  
<meaning>|interval|timeout>
```

где:

- **action <meaning>** - действие по сохранению работоспособности системы в случае сбоя. Возможно указать следующие значения:
 - **action trap** - попытка повторного согласования при обнаружении совпадающего трафика;
 - **action clear** - удалить соединение, применяется по умолчанию;
 - **action restart** - перезапустить соединение;
 - **interval** - интервал времени, в секундах, через который узлам VPN будут отправляться сообщения IKE, подтверждающие активность. Возможно указать значение в диапазоне от «2» до «86400». По умолчанию используется значение «30»;
 - **timeout** - интервал времени, в секундах, по истечении которого, в том случае если узел не отвечает, осуществляется попытка перезапуска туннеля. Возможно указать значение в диапазоне от «2» до «86400». По умолчанию используется значение «120».
4. Включение повторной аутентификации удалённого узла во время операции повторного ввода IKE-ключа (только для IKEv2):

```
set vpn ipsec ike-group <name> ikev2-reauth
```

5. Выбор версии протокола IKE:

```
set vpn ipsec ike-group <name> key-exchange <version>
```

где **<version>** - версия протокола IKE. Возможно указать следующие значения:

- **ikev1** - использовать IKEv1 для обмена ключами;
- **ikev2** - использовать IKEv2 для обмена ключами.

В случае отсутствия заданного значения используются оба протокола. При инициализации соединения используется IKEv2, в ответе принимается любая версия протокола.

6. Установить время жизни ключа IKE:

```
set vpn ipsec ike-group <name> lifetime <time>
```

где **<time>** - время жизни ключа IKE в секундах. Возможно указать значение в диапазоне от «0» до «86400». По умолчанию используется значение «28800».

7. Отключение поддержки MOBIKE:

```
set vpn ipsec ike-group <name> disable-mobike
```

MOBIKE используется в IKEv2 и включён по умолчанию.

8. Установить режим IKEv1:

```
set vpn ipsec ike-group <name> mode <parameter>
```

где **<parameter>** - режим IKEv1. Возможно указать следующие значения:

- **<main>** - использовать основной режим для обмена ключами по протоколу IKEv1. Используется по умолчанию;
- **<aggressive>** - использовать агрессивный режим для обмена ключами по протоколу IKEv1.

9. Указание номера предложения группы IKE первой фазы:

```
set vpn ipsec ike-group <name> proposal <number>
```

где: **<number>** - уникальное целое число идентифицирующее предложение IKE. Возможно указать значение в диапазоне от «1» до «65535».

10. Указание группы, которая будет предложена для ключевого обмена Диффи-Хеллмана:

```
set vpn ipsec ike-group <name> proposal <number> dh-group <group>
```

где: **<group>** - группа, используемая при ключевом обмене Диффи-Хеллмана. Возможно указать следующие значения:

- **1** - Diffie-Hellman group 1 (modp768);
- **2** - Diffie-Hellman group 2 (modp1024), используется по умолчанию;
- **5** - Diffie-Hellman group 5 (modp1536);
- **14** - Diffie-Hellman group 14 (modp2048);
- **15** - Diffie-Hellman group 15 (modp3072);
- **16** - Diffie-Hellman group 16 (modp4096);
- **17** - Diffie-Hellman group 17 (modp6144);
- **18** - Diffie-Hellman group 18 (modp8192);
- **19** - Diffie-Hellman group 19 (ecp256);
- **20** - Diffie-Hellman group 20 (ecp384);
- **21** - Diffie-Hellman group 21 (ecp521);
- **22** - Diffie-Hellman group 22 (modp1024s160);
- **23** - Diffie-Hellman group 23 (modp2048s224);
- **24** - Diffie-Hellman group 24 (modp2048s256);
- **25** - Diffie-Hellman group 25 (ecp192);

- **26** - Diffie-Hellman group 26 (ecp224);
- **27** - Diffie-Hellman group 27 (ecp224bp);
- **28** - Diffie-Hellman group 28 (ecp256bp);
- **29** - Diffie-Hellman group 29 (ecp384bp);
- **30** - Diffie-Hellman group 30 (ecp512bp);
- **31** - Diffie-Hellman group 31 (curve25519);
- **32** - Diffie-Hellman group 32 (curve448).

11. Указание алгоритма шифрования, использование которого будет предлагаться при согласовании первой фазы IKE:

```
set vpn ipsec ike-group <name> proposal <number> encryption <algorithm>
```

где: **<algorithm>** - алгоритм шифрования. Список поддерживаемых алгоритмов шифрования представлен в таблице (см. [Таблица «Поддерживаемые алгоритмы шифрования»](#)). По умолчанию используется алгоритм шифрования «aes128».

Таблица «Поддерживаемые алгоритмы шифрования»

Алгоритм шифрования	Алгоритм шифрования	Алгоритм шифрования
null	aes128	aes192
aes256	aes128ctr	aes192ctr
aes256ctr	aes128ccm64	aes192ccm64
aes256ccm64	aes128ccm96	aes192ccm96
aes256ccm96	aes128ccm128	aes192ccm128
aes256ccm128	aes128gcm64	aes192gcm64
aes256gcm64	aes128gcm96	aes192gcm96
aes256gcm96	aes128gcm128	aes192gcm128
aes256gcm128	aes128gmac	aes192gmac
aes256gmac	3des	blowfish128
blowfish192	blowfish256	camellia128
camellia192	camellia256	camellia128ctr
camellia192ctr	camellia256ctr	camellia128ccm64
camellia192ccm64	camellia256ccm64	camellia128ccm96
camellia192ccm96	camellia256ccm96	camellia128ccm128
camellia192ccm128	camellia256ccm128	serpent128

Алгоритм шифрования	Алгоритм шифрования	Алгоритм шифрования
serpent192	serpent256	twofish128
twofish192	twofish256	cast128
chacha20poly1305		

12. Указание алгоритма хеширования для предложения:

```
set vpn ipsec ike-group <name> proposal <number> hash <algorithm>
```

где: **<algorithm>** - используемый алгоритм хеширования. Возможно указать следующие значения:

- **md5;**
- **md5_128;**
- **sha1** - используется по умолчанию;
- **sha1_160;**
- **sha256;**
- **sha256_96;**
- **sha384;**
- **sha512;**
- **aesxcbc;**
- **aescmac;**
- **aes128gmac;**
- **aes192gmac;**
- **aes256gmac.**

13. Указание псевдослучайной функции для предложения:

```
set vpn ipsec ike-group <name> proposal <number> prf <function>
```

где: **<function>** - используемая псевдослучайная функция. Возможно указать следующие значения:

- **prfmd5;**
- **prfsha1;**
- **prfaesxcbc;**
- **prfaescmac;**
- **prfsha256;**

- **prfsha384;**
- **prfsha512.**

11.3.2 ESP

ESP используется для обеспечения конфиденциальности, аутентификации источника данных, целостности данных без установления соединения, защиты от повторного воспроизведения (форма обеспечения частичной целостности последовательности) и ограниченной конфиденциальности трафика.

В **ARMA Стена** атрибуты ESP определяются с помощью ESP-групп. В рамках одной группы возможно задать несколько предложений.

Основные команды настройки ESP-групп:

1. Определение поименованной настройки IKE для согласований первой фазы IKE:

```
set vpn ipsec esp-group <name>
```

где **<name>** - имя, используемое для обозначения настройки ESP.

2. Включение протокола IPComp, который позволяет сжимать содержимое IP-пакетов:

```
set vpn ipsec esp-group <name> compression
```

3. Установить срок действия ESP в зависимости от объема трафика:

```
set vpn ipsec esp-group <name> life-bytes <value>
```

где **<value>** - количество байтов, переданных по IPsec SA до истечения срока действия ESP. Возможно указать значение в диапазоне от «1024» до «26843545600000».

4. Установить срок действия ESP в зависимости от переданных пакетов:

```
set vpn ipsec esp-group <name> life-packets <value>
```

где **<value>** - количество пакетов, переданных по IPsec SA до истечения срока действия ESP. Возможно указать значение в диапазоне от «1000» до «26843545600000».

5. Указание времени жизни ключа ESP:

```
set vpn ipsec esp-group <name> lifetime <time>
```

где **<time>** - время, в секундах, в течение которого ключ, созданный при согласовании второй фазы IKE, остаётся в силе. Возможно указать значение в диапазоне от «30» до «86400». По умолчанию используется значение «3600».

6. Указание режима подключения IPsec:

```
set vpn ipsec esp-group <name> mode <type>
```

где **<type>** - режим подключения IPsec. Возможно указать значения: «tunnel» - туннельный режим, «transport» - транспортный режим. По умолчанию используется значение «tunnel».

7. Определение использования механизма PFS:

```
set vpn ipsec esp-group <name> pfs <group>
```

где **<group>** - включение/отключение PFS. Возможно указать следующие значения:

- **enable** наследование группы Диффи-Хеллмана от IKE-группы. Используется по умолчанию;
- **dh-group1** use Diffie-Hellman group 1 (modp768);
- **dh-group2** use Diffie-Hellman group 2 (modp1024);
- **dh-group5** use Diffie-Hellman group 5 (modp1536);
- **dh-group14** use Diffie-Hellman group 14 (modp2048);
- **dh-group15** use Diffie-Hellman group 15 (modp3072);
- **dh-group16** use Diffie-Hellman group 16 (modp4096);
- **dh-group17** use Diffie-Hellman group 17 (modp6144);
- **dh-group18** use Diffie-Hellman group 18 (modp8192);
- **dh-group19** use Diffie-Hellman group 19 (ecp256);
- **dh-group20** use Diffie-Hellman group 20 (ecp384);
- **dh-group21** use Diffie-Hellman group 21 (ecp521);
- **dh-group22** use Diffie-Hellman group 22 (modp1024s160);
- **dh-group23** use Diffie-Hellman group 23 (modp2048s224);
- **dh-group24** use Diffie-Hellman group 24 (modp2048s256);
- **dh-group25** use Diffie-Hellman group 25 (ecp192);
- **dh-group26** use Diffie-Hellman group 26 (ecp224);
- **dh-group27** use Diffie-Hellman group 27 (ecp224bp);
- **dh-group28** use Diffie-Hellman group 28 (ecp256bp);
- **dh-group29** use Diffie-Hellman group 29 (ecp384bp);
- **dh-group30** use Diffie-Hellman group 30 (ecp512bp);
- **dh-group31** use Diffie-Hellman group 31 (curve25519);

- **dh-group32** use Diffie-Hellman group 32 (curve448);
- **disable.**

8. Определение предложения группы ESP для согласования второй фазы IKE:

```
set vpn ipsec esp-group <name> proposal <number>
```

где: **<number>** - уникальное целое число идентифицирующее предложение, используемое при согласовании второй фазы IKE. Возможно указать значение в диапазоне от «1» до «65535».

9. Указание алгоритма шифрования для предложения ESP:

```
set vpn ipsec esp-group <name> proposal <number> encryption <algorithm>
```

где: **<algorithm>** - алгоритм шифрования. Список поддерживаемых алгоритмов шифрования представлен в таблице (см. [Таблица «Поддерживаемые алгоритмы шифрования»](#)). По умолчанию используется алгоритм шифрования «aes128».

10. Указание алгоритма хеширования для предложения ESP:

```
set vpn ipsec esp-group <name> proposal <number> hash <algorithm>
```

где: **<algorithm>** - используемый алгоритм хеширования. Возможно указать следующие значения:

- **md5;**
- **md5_128;**
- **sha1** - используется по умолчанию;
- **sha1_160;**
- **sha256;**
- **sha256_96;**
- **sha384;**
- **sha512;**
- **aesxcbc;**
- **aesctmac;**
- **aes128gmac;**
- **aes192gmac;**
- **aes256gmac.**

11. Отключить автоматическую замену криптографических ключей:

```
set vpn ipsec esp-group <name> disable-rekey
```

11.3.3 GRE over IPSEC

Технология **GRE over IPsec** обеспечивает интеграцию функциональных возможностей **GRE** и **IPsec**, где **GRE** предоставляет поддержку многоадресной и широковещательной передачи данных, а **IPsec** гарантирует конфиденциальность посредством шифрования передаваемых данных. В процессе функционирования данного решения осуществляется последовательная инкапсуляция трафика: первичная инкапсуляция производится с использованием протокола **GRE**, после чего выполняется вторичная инкапсуляция с применением механизмов **IPsec** для обеспечения защищённого канала передачи данных.

В качестве примера настройки соединения **GRE over IPSEC**, используется схема стенда, представленная на рисунке (см. [Рисунок – Схема стенда для настройки соединения GRE over IPSEC](#)).

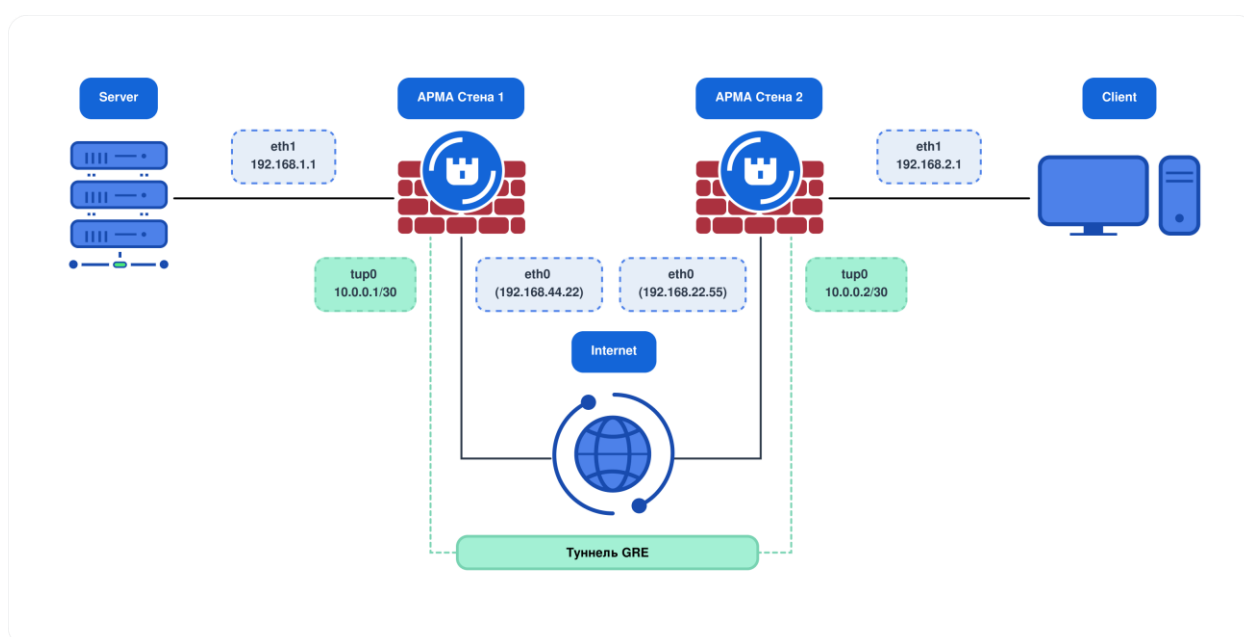


Рисунок – Схема стенда для настройки соединения GRE over IPSEC

Используемые IP-адреса приведены в качестве примера.

Для настройки **GRE over IPSEC** необходимо выполнить следующие шаги:

1. Настроить конфигурацию на **ARMA Стена1**:

- Настроить GRE:

```
set interfaces ethernet eth1 address 192.168.1.1/32
set interfaces tunnel tun0 address '10.0.0.1/30'
set interfaces tunnel tun0 encapsulation 'gre'
set interfaces tunnel tun0 remote '192.168.22.55'
set interfaces tunnel tun0 source-address '192.168.44.22'
```

- Настроить маршрутизацию:

```
set protocols static route 192.168.2.1/32 interface tun0
```

- Настроить IPSec:

```
# Настройка предварительных общих секретов (Pre-Shared Keys):
```

```
# создать PSK с именем TEST_PSK для узла 192.168.44.22
set vpn ipsec authentication psk TEST_PSK id '192.168.44.22'
```

```
# создать PSK с именем TEST_PSK для узла 192.168.22.55
set vpn ipsec authentication psk TEST_PSK id '192.168.22.55'
```

```
# установить секрет для PSK TEST_PSK со значением 'test'
set vpn ipsec authentication psk TEST_PSK secret 'test'
```

```
# Настройка групп шифрования ESP (для защиты транспортного потока):
```

```
# создать группу шифрования TestESP в режиме transport
set vpn ipsec esp-group TestESP mode 'transport'
```

```
# настроить предложение шифрования с использованием AES-128 для
шифрования
set vpn ipsec esp-group TestESP proposal 1 encryption 'aes128'
```

```
# настроить предложение шифрования с использованием SHA1 для
хеширования
set vpn ipsec esp-group TestESP proposal 1 hash 'sha1'
```

```
# Настройка группы IKE (для установления безопасного соединения):
```

```
# создать группу IKE TestIKE с предложением DH-группа 2 (1024-bit MODP)
set vpn ipsec ike-group TestIKE proposal 1 dh-group '2'
```

```
# создать группу IKE TestIKE с предложением AES-128 для шифрования
set vpn ipsec ike-group TestIKE proposal 1 encryption 'aes128'
```

```
# создать группу IKE TestIKE с предложением SHA1 для хеширования
set vpn ipsec ike-group TestIKE proposal 1 hash 'sha1'
```

```
# Назначить интерфейс eth0 для работы IPsec
set vpn ipsec interface 'eth0'

# Настройка site-to-site соединения:

# Для удаленного пира настроить аутентификацию по предварительному
секрету
set vpn ipsec site-to-site peer right authentication mode 'pre-shared-secret'

# удаленный идентификатор установить как 192.168.22.55
set vpn ipsec site-to-site peer right authentication remote-id '192.168.22.55'

# назначить группу шифрования TestESP как дефолтную
set vpn ipsec site-to-site peer right default-esp-group 'TestESP'

# назначить группу IKE TestIKE
set vpn ipsec site-to-site peer right ike-group 'TestIKE'

# установить локальный IP-адрес 192.168.44.22
set vpn ipsec site-to-site peer right local-address '192.168.44.22'

# установить удалённый IP-адрес 192.168.22.55
set vpn ipsec site-to-site peer right remote-address '192.168.22.55'

# создать GRE-туннель с номером 10 через IPsec
set vpn ipsec site-to-site peer right tunnel 10 protocol 'gre'

commit
save
```

2. Настроить конфигурацию на **ARMA Стена2**:

- Настроить GRE:

```
set interfaces ethernet eth1 address 192.168.2.1/32
set interfaces tunnel tun0 address '10.0.0.2/30'
set interfaces tunnel tun0 encapsulation 'gre'
set interfaces tunnel tun0 remote '192.168.44.22'
set interfaces tunnel tun0 source-address '192.168.22.55'
```

- Настроить маршрутизацию:

```
set protocols static route 192.168.1.1/32 interface tun0
```


- Настроить IPsec:

```
set vpn ipsec authentication psk TEST_PSK id '192.168.44.22'
set vpn ipsec authentication psk TEST_PSK id '192.168.22.55'
set vpn ipsec authentication psk TEST_PSK secret 'test'
set vpn ipsec esp-group TestESP mode 'transport'
set vpn ipsec esp-group TestESP proposal 1 encryption 'aes128'
set vpn ipsec esp-group TestESP proposal 1 hash 'sha1'
set vpn ipsec ike-group TestIKE proposal 1 dh-group '2'
set vpn ipsec ike-group TestIKE proposal 1 encryption 'aes128'
set vpn ipsec ike-group TestIKE proposal 1 hash 'sha1'
set vpn ipsec interface 'eth0'
set vpn ipsec site-to-site peer left authentication mode 'pre-shared-secret'
set vpn ipsec site-to-site peer left authentication remote-id '192.168.44.22'
set vpn ipsec site-to-site peer left connection-type 'respond'
set vpn ipsec site-to-site peer left default-esp-group 'TestESP'
set vpn ipsec site-to-site peer left ike-group 'TestIKE'
set vpn ipsec site-to-site peer left local-address '192.168.22.55'
set vpn ipsec site-to-site peer left remote-address '192.168.44.22'
set vpn ipsec site-to-site peer left tunnel 10 protocol 'gre'

commit
save
```

Создаётся защищённый **IPsec**-туннель между узлами 192.168.44.22 и 192.168.22.55, через который проходит **GRE**-трафик. Все данные, передаваемые через туннель tun0, будут:

- инкапсулированы в GRE;
- зашифрованы с использованием AES-128;
- аутентифицированы с использованием SHA1;
- защищены с помощью DH-группы 2 для обмена ключами.

Мониторинг соединения GRE over IPsec:

1. Проверить статус соединения между **ARMA Стена1** и **ARMA Стена2**:

- **ARMA Стена1**:

```
admin@ngfwos:~$ show vpn ipsec connections
```

Connection	State	Type	Remote address	Local TS
Remote TS		Local id	Remote id	Proposal
left	up		IKEv1/2	192.168.22.55
-				192.168.22.55
AES_CBC/128/HMAC_SHA1_96/MODP_1024				
left-tunnel-10	up	IPsec	192.168.22.55	192.168.44.22/32[gre]
192.168.22.55/32[gre]				192.168.22.55
AES_CBC/128/HMAC_SHA1_96/None				

```
admin@ngfwos:~$
```

- **ARMA Стена2:**

```
admin@ngfwos:~$ show vpn ipsec connections
```

Connection	State	Type	Remote address	Local TS
Remote TS		Local id	Remote id	Proposal
left	up		IKEv1/2	192.168.44.22
-				192.168.44.22
AES_CBC/128/HMAC_SHA1_96/MODP_1024				
left-tunnel-10	up	IPsec	192.168.44.22	192.168.22.55/32[gre]
192.168.44.22/32[gre]				192.168.44.22
AES_CBC/128/HMAC_SHA1_96/None				

```
admin@ngfwos:~$
```

2. Вывести детальную информацию о текущих наборах параметров безопасности (SA), используемых для шифрования и аутентификации трафика в **IPsec**:

- **ARMA Стена1:**

```
admin@ngfwos:~$ show vpn ipsec sa detail

left: #1, ESTABLISHED, IKEv2, 5a8690c8f1baffbd_i 737d8a361c96c3ac_r*
  local  '192.168.44.22' @ 192.168.44.22[4500]
  remote '192.168.22.55' @ 192.168.22.55[4500]
  AES_CBC-128/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_1024
  established 408s ago, rekeying in 27736s
left-tunnel-10: #2, reqid 1, INSTALLED, TRANSPORT, ESP:AES_CBC-
128/HMAC_SHA1_96
  installed 408s ago, rekeying in 2555s, expires in 3193s
  in  c2833b8c,  9918 bytes,    80 packets,    13s ago
  out c187396b,  704 bytes,    8 packets,    160s ago
  local 192.168.44.22/32[gre]
  remote 192.168.22.55/32[gre]

admin@ngfwos:~$
```

- **ARMA Стена2:**

```
admin@ngfwos:~$ show vpn ipsec sa detail

left: #1, ESTABLISHED, IKEv2, 5a8690c8f1baffbd_i* 737d8a361c96c3ac_r
  local  '192.168.22.55' @ 192.168.22.55[4500]
  remote '192.168.44.22' @ 192.168.44.22[4500]
  AES_CBC-128/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_1024
  established 461s ago, rekeying in 28273s
left-tunnel-10: #2, reqid 1, INSTALLED, TRANSPORT, ESP:AES_CBC-
128/HMAC_SHA1_96
  installed 462s ago, rekeying in 2613s, expires in 3139s
  in  c187396b,  704 bytes,    8 packets,    213s ago
  out c2833b8c, 10590 bytes,   86 packets,    6s ago
  local 192.168.22.55/32[gre]
  remote 192.168.44.22/32[gre]

admin@ngfwos:~$
```

11.3.4 IPSEC Site-to-Site (Policy Based)

IPSec Site-to-Site представляет собой комплексное решение для создания защищённых каналов связи между распределёнными сетями.

В качестве примера настройки VPN-соединения **IPSEC Site-to-Site**, используется схема стенда, представленная на рисунке (см. [Рисунок – Схема стенда для настройки GRE over IPSEC](#)).

Используемые IP-адреса приведены в качестве примера.

Для корректной реализации **IPSEC Site-to-Site** соединения требуется последовательная конфигурация обоих узлов - **ARMA Стена1** и **ARMA Стена2**:

1. Конфигурация узла **ARMA Стена1**:

```
# Настройка сетевых интерфейсов:
set interfaces ethernet eth0 address '192.168.44.22/24'
set interfaces ethernet eth1 address '192.168.1.1/24'

# Настройка аутентификации:
set vpn ipsec authentication psk NGFW id '192.168.44.22'
set vpn ipsec authentication psk NGFW id '192.168.22.55'
set vpn ipsec authentication psk NGFW secret 'p4ssw0rd'

# Настройка групп шифрования ESP (для защиты транспортного потока):
set vpn ipsec esp-group ESP-GROUP mode 'tunnel'
set vpn ipsec esp-group ESP-GROUP proposal 1 encryption 'aes256'
set vpn ipsec esp-group ESP-GROUP proposal 1 hash 'sha256'

# Настройка IKE-группы:
set vpn ipsec ike-group IKE-GROUP key-exchange 'ikev2'
set vpn ipsec ike-group IKE-GROUP proposal 1 dh-group '14'
set vpn ipsec ike-group IKE-GROUP proposal 1 encryption 'aes256'
set vpn ipsec ike-group IKE-GROUP proposal 1 hash 'sha256'

# Назначить интерфейс eth0 для работы IPsec
set vpn ipsec interface 'eth0'

# Настройка site-to-site соединения:
set vpn ipsec site-to-site peer NGFW authentication mode 'pre-shared-secret'
set vpn ipsec site-to-site peer NGFW connection-type 'initiate'
set vpn ipsec site-to-site peer NGFW default-esp-group 'ESP-GROUP'
set vpn ipsec site-to-site peer NGFW ike-group 'IKE-GROUP'
set vpn ipsec site-to-site peer NGFW local-address 'any'
set vpn ipsec site-to-site peer NGFW remote-address '192.168.22.55'
set vpn ipsec site-to-site peer NGFW tunnel 0 local prefix '192.168.1.0/24'
set vpn ipsec site-to-site peer NGFW tunnel 0 remote prefix '192.168.2.0/24'

commit
save
```

При наличии в системе **ARMA Стена1** настроенных правил **SNAT** необходимо обеспечить приоритетное применение правила, исключающего трансляцию адресов для диапазона 192.168.2.0/24. Для корректного функционирования политики маршрутизации данное правило должно обладать более высоким приоритетом по сравнению с остальными SNAT-правилами, что достигается назначением меньшего порядкового номера. Обработка правил SNAT выполняется последовательно сверху вниз, поэтому исключающее правило должно быть размещено до всех правил, применяющих трансляцию.

Для корректной конфигурации следует использовать следующую последовательность команд:

```
set nat source rule 2 destination address '192.168.2.0/24'  
set nat source rule 2 exclude  
set nat source rule 2 outbound-interface name 'eth0'  
set nat source rule 2 source address '192.168.1.0/24'  
  
set nat source rule 3 outbound-interface name 'eth0'  
set nat source rule 3 source address '192.168.1.0/24'  
set nat source rule 3 translation address 'masquerade'
```

Правило с номером 2 определяет условие исключения из трансляции источника (параметр «exclude») для трафика, исходящего из подсети 192.168.1.0/24 и направляющегося в сеть 192.168.2.0/24, при передаче через интерфейс eth0. Это предотвращает выполнение SNAT для указанного сегмента.

Правило с номером 3 задаёт маскирование исходного IP-адреса (masquerade) для всего остального трафика из подсети 192.168.1.0/24, направляемого через интерфейс eth0.

Корректность работы политики NAT зависит от строгого соблюдения порядка правил: правило с «exclude» должно иметь меньший номер (более высокий приоритет), чем правило с «masquerade», чтобы исключить нежелательную трансляцию адресов в защищённом диапазоне.

2. Конфигурация узла **ARMA Стена2**:

```
set interfaces ethernet eth0 address '192.168.22.55/24'  
set interfaces ethernet eth1 address '192.168.2.1/24'  
  
set vpn ipsec authentication psk NGFW id '192.168.22.55'  
set vpn ipsec authentication psk NGFW id '192.168.44.22'  
set vpn ipsec authentication psk NGFW secret 'p4ssw0rd'  
  
set vpn ipsec esp-group ESP-GROUP mode 'tunnel'  
set vpn ipsec esp-group ESP-GROUP proposal 1 encryption 'aes256'
```

```
set vpn ipsec esp-group ESP-GROUP proposal 1 hash 'sha256'

set vpn ipsec ike-group IKE-GROUP key-exchange 'ikev2'
set vpn ipsec ike-group IKE-GROUP proposal 1 dh-group '14'
set vpn ipsec ike-group IKE-GROUP proposal 1 encryption 'aes256'
set vpn ipsec ike-group IKE-GROUP proposal 1 hash 'sha256'

set vpn ipsec interface 'eth0'

set vpn ipsec site-to-site peer NGFW authentication mode 'pre-shared-secret'
set vpn ipsec site-to-site peer NGFW connection-type 'initiate'
set vpn ipsec site-to-site peer NGFW default-esp-group 'ESP-GROUP'
set vpn ipsec site-to-site peer NGFW ike-group 'IKE-GROUP'
set vpn ipsec site-to-site peer NGFW local-address 'any'
set vpn ipsec site-to-site peer NGFW remote-address '192.168.44.22'
set vpn ipsec site-to-site peer NGFW tunnel 0 local prefix '192.168.2.0/24'
set vpn ipsec site-to-site peer NGFW tunnel 0 remote prefix '192.168.1.0/24'

commit
save
```

При наличии в системе **ARMA Стена2** настроенных правил **SNAT** необходимо обеспечить приоритетное применение правила, исключающего трансляцию адресов для диапазона 192.168.1.0/24. Для корректного функционирования политики маршрутизации данное правило должно обладать более высоким приоритетом по сравнению с остальными SNAT-правилами, что достигается назначением меньшего порядкового номера. Обработка правил SNAT выполняется последовательно сверху вниз, поэтому исключающее правило должно быть размещено до всех правил, применяющих трансляцию.

Для корректной конфигурации следует использовать следующую последовательность команд:

```
set nat source rule 2 destination address '192.168.1.0/24'
set nat source rule 2 exclude
set nat source rule 2 outbound-interface name 'eth0'
set nat source rule 2 source address '192.168.2.0/24'

set nat source rule 3 outbound-interface name 'eth0'
set nat source rule 3 source address '192.168.2.0/24'
set nat source rule 3 translation address 'masquerade'
```

Мониторинг VPN-соединения IPSEC Site-to-Site:

1. Для проверки корректности конфигурации и работоспособности **IKE**-части VPN необходимо ввести следующую команду:

- **ARMA Стена1:**

```
admin@ngfwos:~$ show vpn ike sa
```

Peer ID / IP		Local ID / IP						
-----		-----						
192.168.22.55	192.168.22.55	192.168.44.22	192.168.44.22					
State	IKEVer	Encrypt	Hash	D-H Group	NAT-T			
A-Time	L-Time							
-----	-----	-----	----	-----	-----	-----	----	----

up	IKEv2	AES_CBC_256	HMAC_SHA2_256_128	MODP_2048				
no	125	27375						

```
admin@ngfwos:~$
```

- **ARMA Стена2:**

```
admin@ngfwos:~$ show vpn ike sa
```

Peer ID / IP		Local ID / IP						
-----		-----						
192.168.44.22	192.168.44.22	192.168.22.55	192.168.22.55					
State	IKEVer	Encrypt	Hash	D-H Group	NAT-T			
A-Time	L-Time							
-----	-----	-----	----	-----	-----	-----	----	----

up	IKEv2	AES_CBC_256	HMAC_SHA2_256_128	MODP_2048				
no	270	28164						

```
admin@ngfwos:~$
```

2. Для проверки корректности конфигурации и работоспособности **IPsec**-части VPN необходимо ввести следующую команду:

- **ARMA Стена1:**

```
admin@ngfwos:~$ show vpn ipsec sa
```

Connection	State	Uptime	Bytes In/Out	Packets In/Out
Remote address	Remote ID	Proposal		
NGFW-tunnel-0	up	5m37s	504B/504B	6/6
192.168.22.55	192.168.22.55	AES_CBC_256/HMAC_SHA2_256_128		

```
admin@ngfwos:~$
```

- **ARMA Стена2:**

```
admin@ngfwos:~$ show vpn ipsec sa
```

Connection	State	Uptime	Bytes In/Out	Packets In/Out
Remote address	Remote ID	Proposal		
NGFW-tunnel-0	up	7m53s	504B/504B	6/6
192.168.44.22	192.168.44.22	AES_CBC_256/HMAC_SHA2_256_128		

```
admin@ngfwos:~$
```

3. Для детального анализа работы **IPsec** необходимо ввести следующую команду:

- **ARMA Стена1:**

```
admin@ngfwos:~$ show vpn ipsec sa detail
```

```
NGFW: #4, ESTABLISHED, IKEv2, 1e14825c46b682bf_i a1de5b9d037bcc6e_r*
local '192.168.44.22' @ 192.168.44.22[4500]
remote '192.168.22.55' @ 192.168.22.55[4500]
AES_CBC-256/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/MODP_2048
established 577s ago, rekeying in 26923s
NGFW-tunnel-0: #2, reqid 1, INSTALLED, TUNNEL, ESP:AES_CBC-
256/HMAC_SHA2_256_128
installed 577s ago, rekeying in 2503s, expires in 3023s
in c20787e0, 504 bytes, 6 packets, 533s ago
out cf5f6cc7, 504 bytes, 6 packets, 533s ago
local 192.168.1.0/24
remote 192.168.2.0/24
```

```
admin@ngfwos:~$
```


- **ARMA Стена2:**

```
admin@ngfwos:~$ show vpn ipsec sa detail

NGFW: #4, ESTABLISHED, IKEv2, 1e14825c46b682bf_i* a1de5b9d037bcc6e_r
  local  '192.168.22.55' @ 192.168.22.55[4500]
  remote '192.168.44.22' @ 192.168.44.22[4500]
  AES_CBC-256/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/MODP_2048
  established 530s ago, rekeying in 27904s
  NGFW-tunnel-0: #3, reqid 1, INSTALLED, TUNNEL, ESP:AES_CBC-
256/HMAC_SHA2_256_128
    installed 530s ago, rekeying in 2626s, expires in 3070s
    in  cf5f6cc7,    504 bytes,    6 packets,    486s ago
    out c20787e0,    504 bytes,    6 packets,    486s ago
    local 192.168.2.0/24
    remote 192.168.1.0/24

admin@ngfwos:~$
```

4. Для отображения общего состояния **IPsec**-подсистемы необходимо ввести следующую команду:

- **ARMA Стена1:**

```
admin@ngfwos:~$ show vpn ipsec state

src 192.168.44.22 dst 192.168.22.55
    proto esp spi 0xcf5f6cc7 reqid 1 mode tunnel
    replay-window 0 flag af-unspec
    auth-trunc                                     hmac(sha256)
0x35fdb0df730b7f67b6a64eb6a87e210efd59194020c0a2d4d94d48fc107a1e50
128
    enc                                             cbc(aes)
0x3fcd3e1cb25e754ae3f90ba692f93f696852bf1128c7284f610379a3103da73d
    lastused 2025-03-05 07:35:41
    anti-replay context: seq 0x0, oseq 0x6, bitmap 0x00000000
src 192.168.22.55 dst 192.168.44.22
    proto esp spi 0xc20787e0 reqid 1 mode tunnel
    replay-window 32 flag af-unspec
    auth-trunc                                     hmac(sha256)
0x521dcf97c48a7259ce28a7ea281bb15b2e393b390d13b8dd2b3136acbad29a6
c 128
    enc                                             cbc(aes)
0xe470d3eab56346dd517514305a39204078438812ef9d623642a90dfdb444d9e
0
    lastused 2025-03-05 07:35:41
    anti-replay context: seq 0x6, oseq 0x0, bitmap 0x0000003f

admin@ngfwos:~$
```

- **ARMA Стена2:**

```
admin@ngfwos:~$ show vpn ipsec state
src 192.168.22.55 dst 192.168.44.22
    proto esp spi 0xc20787e0 reqid 1 mode tunnel
    replay-window 0 flag af-unspec
    auth-trunc                                     hmac(sha256)
0x521dcf97c48a7259ce28a7ea281bb15b2e393b390d13b8dd2b3136acbad29a6
c 128
    enc                                             cbc(aes)
0xe470d3eab56346dd517514305a39204078438812ef9d623642a90dfdb444d9e
0
    lastused 2025-03-05 07:35:41
    anti-replay context: seq 0x0, oseq 0x6, bitmap 0x00000000
src 192.168.44.22 dst 192.168.22.55
    proto esp spi 0xcf5f6cc7 reqid 1 mode tunnel
    replay-window 32 flag af-unspec
    auth-trunc                                     hmac(sha256)
0x35fdb0df730b7f67b6a64eb6a87e210efd59194020c0a2d4d94d48fc107a1e50
128
    enc                                             cbc(aes)
0x3fcd3e1cb25e754ae3f90ba692f93f696852bf1128c7284f610379a3103da73d
    lastused 2025-03-05 07:35:41
    anti-replay context: seq 0x6, oseq 0x0, bitmap 0x0000003f
admin@ngfwos:~$
```

12 МЕЖСЕТЕВОЙ ЭКРАН

12.1 Межсетевой экран

Одной из ключевых функций **ARMA Стена** является фильтрация сетевого трафика с использованием встроенного межсетевого экрана (МЭ). Система основана на Linux и использует механизм фильтрации пакетов nftables, реализованный в ядре операционной системы. Благодаря этому становится возможным гибкое и высокопроизводительное управление потоками данных непосредственно на уровне ядра.

В **ARMA Стена** применяется подход на основе зон безопасности, который расширяет стандартные возможности управления трафиком. Обработка пакетов может выполняться на нескольких этапах – начиная с момента их приёма сетевым интерфейсом и драйвером и вплоть до передачи конечному получателю (например, веб-серверу или другому сетевому устройству).

Для наглядного представления логики обработки пакетов и возможных маршрутов их прохождения ниже приведена упрощённая схема потока трафика, основанная на стандартной архитектуре обработки пакетов Netfilter (см. [Рисунок – Схема потока трафика](#)).

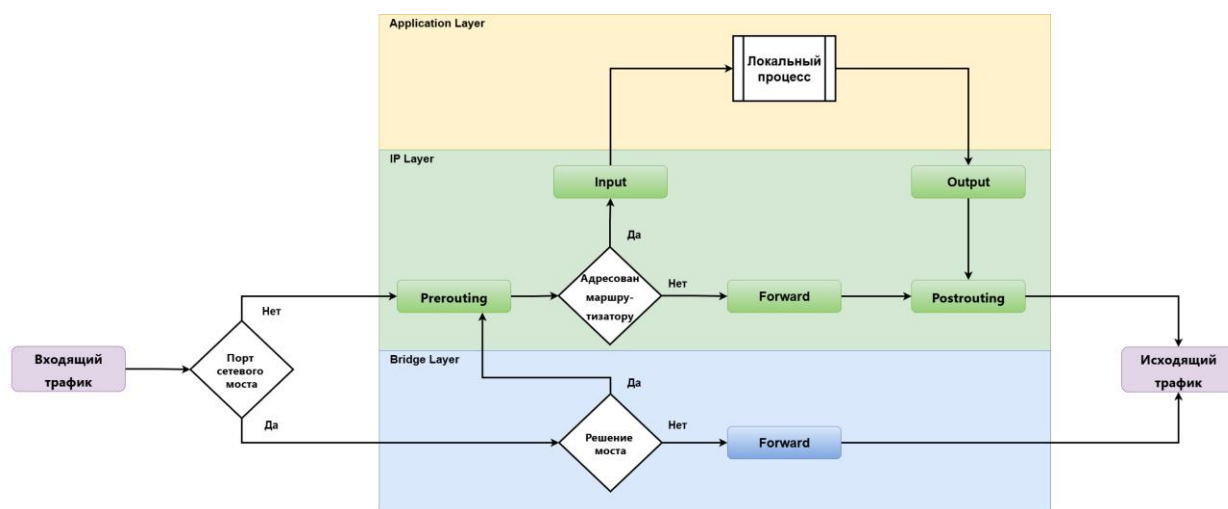


Рисунок – Схема потока трафика

Примечание:

По умолчанию в системе ARMA Стена разрешён весь входящий и исходящий трафик. Транзитный трафик по умолчанию блокируется.

Для изменения политики обработки трафика по умолчанию (установка действия «drop» или «accept») необходимо выполнить в конфигурационном режиме команду: `<set firewall <ipv4 | ipv6 | bridge> <forward filter | input filter | output filter> default-action accept>`.

В **МЭ** реализованы две политики фильтрации сетевого трафика:

1. Стандартная политика на основе системных наборов правил.

Системные наборы правил представляют собой predetermined пакеты правил, входящие в состав **МЭ**. В зависимости от направления и назначения сетевого трафика, применяются следующие системные наборы правил:

- **«Input»** - набор правил для фильтрации входящего IPv4/IPv6-трафика, адресованного самой системе **ARMA Стена**.
- **«Output»** - набор правил для фильтрации исходящего IPv4/IPv6-трафика, инициированного самой системой **ARMA Стена**, например, ответы на внешние запросы (SSH, ICMP и др.).
- **«Forward»** - набор правил для фильтрации транзитного IPv4/IPv6-трафика, проходящего через устройство **ARMA Стена**.

2. Политика на основе зон сети.

В рамках архитектуры, основанной на зонах безопасности, сетевые интерфейсы объединяются в логические группы – зоны, в соответствии с их функциональным или сегментационным назначением. Правила фильтрации трафика между зонами определяются кастомными наборами правил, назначенными для каждой пары взаимодействующих зон. Такой подход обеспечивает гибкое и детализированное управление доступом, позволяя задавать различные уровни разрешений и политик безопасности для каждой конкретной зоны и межзонового взаимодействия.

Примечание:

Стандартная политика фильтрации трафика имеет приоритет над политикой на основе зон сети и применяется по умолчанию.

По умолчанию сетевой трафик сначала обрабатывается на уровне системных наборов правил. Для использования исключительно политики на основе зон необходимо разрешить весь трафик на уровне системных наборов правил. Это осуществляется путём установки параметра **«Действие по умолчанию»** в значение **«accept»** и удаления (или отключения) всех правил в каждом из системных наборов **Input, Output** и **Forward**.

При конфигурации **МЭ** требуется обеспечить доступность определённого набора сетевых портов, необходимых для стабильного функционирования системных сервисов и взаимодействия с другими компонентами инфраструктуры. Перечень используемых портов приведён в таблице [«Служебные порты системы ARMA Стена»](#).

Таблица «Служебные порты системы **ARMA Стена**»

Порт	Протокол	Описание
22	TCP	Порт для удалённого доступа к системе по протоколу SSH
123	UDP	Порт службы синхронизации времени NTP

Порт	Протокол	Описание
443	TCP	Порт, используемый для онлайн-активации системы и получения обновлений правил COB
3128	TCP	Порт прокси-сервера для обработки HTTP-запросов
3129	TCP	Порт прокси-сервера для обработки HTTPS-запросов
5000	TCP	Порт взаимодействия системы ARMA Стена с ARMA MC
8082	TCP	Порт, предназначенный для синхронизации конфигураций и служебного взаимодействия с ARMA MC

Примечание:

Рекомендуется применять строгую политику фильтрации сетевого трафика на уровне межсетевого экрана, предполагающую по умолчанию запрет всего входящего, исходящего и транзитного трафика. Доступ должен быть разрешён только на основании принципа минимальных привилегий.

В случае применения политик, блокирующих весь входящий или исходящий сетевой трафик в системе **ARMA Стена**, необходимо создать разрешающее правило для сетевого интерфейса localhost (127.0.0.1) для обеспечения взаимодействия между внутренними компонентами системы.

Пример разрешающих правил для взаимодействия системы **ARMA Стена** с **ARMA MC** при блокировке всего входящего IPv4-трафика:

```
# Открыть порт 5000 для взаимодействия системы ARMA Стена с ARMA MC:
set firewall ipv4 input filter rule 10 action 'accept'
set firewall ipv4 input filter rule 10 destination port '5000'
set firewall ipv4 input filter rule 10 protocol 'tcp'

# Разрешающее правило для взаимодействия между внутренними сервисами
ARMA Стена:
set firewall ipv4 input filter rule 30 action 'accept'
set firewall ipv4 input filter rule 30 destination address '127.0.0.1'
```

Пример разрешающих правил для взаимодействия системы **ARMA Стена** с **ARMA MC** при блокировке всего исходящего IPv4-трафика:

```
# Открыть порт 5000 для взаимодействия системы ARMA Стена с ARMA MC:
set firewall ipv4 output filter rule 10 action 'accept'
set firewall ipv4 output filter rule 10 source port '5000'
set firewall ipv4 output filter rule 10 protocol 'tcp'

# Открыть порт, указанный при добавлении источника ARMA Стена (NGFW) в
ARMA MC,
для отправки событий в ARMA MC:
set firewall ipv4 output filter rule 20 action 'accept'
set firewall ipv4 output filter rule 20 source port 'номер_порта_в_ARMA_MC'
set firewall ipv4 output filter rule 20 protocol 'tcp'

# Разрешающее правило для взаимодействия между внутренними сервисами
ARMA Стена:
set firewall ipv4 output filter rule 30 action 'accept'
set firewall ipv4 output filter rule 30 source address '127.0.0.1'
```

12.1.1 Глобальные настройки

Для глобальной настройки обработки пакетов в рамках соединения необходимо ввести следующую команду:

```
set firewall global-options state-policy <category> action <act>
```

где:

- **<category>** – категория соединения, к которому относятся сетевые пакеты;
- **<act>** – действие.

Поддерживается применение действий над пакетами следующих категорий соединений (**<category>**):

- **«established»** – установленного соединения;
- **«invalid»** – недопустимого соединения;
- **«related»** – связанного соединения.

Правилами МЭ предусмотрены следующие действия над сетевыми пакетами (**<act>**):

- **«accept»** – разрешить;
- **«drop»** – заблокировать;
- **«reject»** – отклонить.

По умолчанию для пакетов каждой категории соединений используется действие **«accept»**.

Для просмотра событий, связанных с глобальной настройкой обработки пакетов, необходимо ввести следующую команду в эксплуатационном режиме:

```
admin@ngfwos:~$ show logging kernel |match STATE-POLICY
```

Поддерживается включение/отключение следующих опций:

1. Отправление **ARMA Стена** ответов на локальные ICMP-запросы:

```
set firewall global-options all-ping [enable | disable]
```

Включено по умолчанию.

2. Отправление **ARMA Стена** ответов на широковещательные ICMP-запросы:

```
set firewall global-options broadcast-ping [enable | disable]
```

Отключено по умолчанию.

3. Обработка IPv4-пакетов, содержащих информацию об исходном маршруте:

```
set firewall global-options ip-src-route [enable | disable]
```

Отключено по умолчанию.

4. Обработка IPv6-пакетов, содержащих информацию об исходном маршруте:

```
set firewall global-options ipv6-src-route [enable | disable]
```

Отключено по умолчанию.

5. Обработка входящих перенаправляющих сообщений ICMPv4:

```
set firewall global-options receive-redirects [enable | disable]
```

Отключено по умолчанию.

6. Обработка входящих перенаправляющих сообщений ICMPv6:

```
set firewall global-options ipv6-receive-redirects [enable | disable]
```

Включено по умолчанию.

7. Использование перенаправляющих сообщений ICMPv4:

```
set firewall global-options send-redirects [enable | disable]
```

Включено по умолчанию.

8. Логирование марсианских IPv4-пакетов:

```
set firewall global-options log-martians [enable | disable]
```

Включено по умолчанию.

9. Проверка источников по обратному пути:

```
set firewall global-options source-validation [strict | loose | disable]
```

где:

- **«strict»** – строгая;
- **«loose»** – мягкая.

Отключено по умолчанию.

10. Использование IPv4 TCP SYN cookies:

```
set firewall global-options syn-cookies [enable | disable]
```

Включено по умолчанию.

11. Защита от угрозы прерывания по времени в TCP:

```
set firewall global-options twa-hazards-protection [enable | disable]
```

Отключено по умолчанию.

12.1.2 Группы

Группы – удобный инструмент объединения множества сетей, хостов и портов с целью дальнейшего использования в правилах МЭ и NAT.

12.1.2.1 Создание группы

Для создания группы необходимо ввести следующую команду:

```
set firewall group <typealias> <name>
```

где:

- **<typealias>** – тип группы;
- **<name>** – имя группы. Должно быть уникальным в рамках своего типа, не превышать «31» символа, начинаться только с латинской буквы или цифры, не может начинаться с символов «-» или «!», и не должно содержать символы «|», «;», «:», «&», «\$», «<», «>».

Поддерживается создание групп следующих типов (**<typealias>**):

- **«address-group»** – «IPv4-адреса»;
- **«domain-group»** – «Домены»;
- **«dynamic-group»** – «Динамические адреса»;
- **«interface-group»** – «Интерфейсы»;
- **«ipv6-address-group»** – «IPv6-адреса»;
- **«ipv6-network-group»** – «IPv6-сети»;

- «**mac-group**» – «Мас-адреса»;
- «**network-group**» – «IPv4-сети»;
- «**port-group**» – «Порты».

Для добавления описания группы необходимо ввести следующую команду:

```
set firewall group <typealias> <name> description <text>
```

где **<text>** – описание группы.

Для добавления группы в другую группу необходимо ввести следующую команду:

```
set firewall group <typealias> <name1> include <name2>
```

где **<name2>** – имя группы, которую требуется добавить в группу **<name1>**.

12.1.2.1.1 Группа IPv4-адресов

Для создания группы типа «IPv4-адреса» необходимо ввести следующую команду:

```
set firewall group address-group <name> address <x.x.x.x>
```

где **<x.x.x.x>** – IPv4-адрес. Возможно указание диапазона адресов, разделённых знаком «-».

12.1.2.1.2 Группа IPv6-адресов

Для создания группы типа «IPv6-адреса» необходимо ввести следующую команду:

```
set firewall group ipv6-address-group <name> address <h:h:h:h:h:h:h>
```

где **<h:h:h:h:h:h:h>** – IPv6-адрес. Возможно указание диапазона адресов, разделённых знаком «-».

12.1.2.1.3 Группа IPv4-сетей

Для создания группы типа «IPv4-сети» необходимо ввести следующую команду:

```
set firewall group network-group <name> network <x.x.x.x/x>
```

где **<x.x.x.x/x>** – IPv4-адрес сети.

12.1.2.1.4 Группа IPv6-сетей

Для создания группы типа «IPv6-сети» необходимо ввести следующую команду:

```
set firewall group ipv6-network-group <name> network <h:h:h:h:h:h:h/x>
```

где **<h:h:h:h:h:h:h/x>** – IPv6-адрес сети.

12.1.2.1.5 Группа портов

Для создания группы типа «Порты» необходимо ввести следующую команду:

```
set firewall group port-group <name> port <num>
```

где **<num>** – номер порта или диапазон портов, разделённых знаком «-». Возможно указание значения в диапазоне от «1» до «65535».

Поддерживается указание имени, определённого в «/etc/services», например, **«set firewall group port-group <name> port http»**.

12.1.2.1.6 Группа интерфейсов

Для создания группы типа «Интерфейсы» необходимо ввести следующую команду:

```
set firewall group interface-group <name> interface <intName>
```

где **<intName>** – имя интерфейса.

Поддерживается указание имени интерфейса с использованием знака «!» для инверсии или подстановочного символа «*», например:

- **«!eth0»** – интерфейсы кроме «eth0»;
- **«eth2*»** – интерфейсы, с именами начинающимися на «eth2».

12.1.2.1.7 Группа доменов

Для создания группы типа «Домены» необходимо ввести следующую команду:

```
set firewall group domain-group <name> address <domain>
```

где **<domain>** – доменное имя.

12.1.2.1.8 Группа MAC-адресов

Для создания группы типа «MAC-адреса» необходимо ввести следующую команду:

```
set firewall group mac-group <name> mac-address <h:h:h:h:h>
```

где **<h:h:h:h:h>** – MAC-адрес.

12.1.2.1.9 Динамическая группа

Динамические группы отличаются от всех ранее определённых групп тем, что они не только могут выступать в качестве источника или назначения в правилах МЭ, но и их состав не определяется статически посредством конфигурации системы. Вместо этого члены этих групп добавляются динамически с использованием правил МЭ.

Динамические группы, как и любые другие группы брандмауэра, могут использоваться в правилах фильтрации в качестве условий сопоставления, позволяя создавать гибкие правила на основе динамически обновляемых списков IP-адресов.

Поддержка динамических групп реализована для IPv4 и IPv6. Команды для создания групп:

```
set firewall group dynamic-group address-group <name> # Для IPv4  
  
set firewall group dynamic-group ipv6-address-group <name> # Для IPv6
```

Для добавления описания группы необходимо ввести следующую команду:

```
set firewall group dynamic-group address-group <name> description <text> #  
Для IPv4  
  
set firewall group dynamic-group ipv6-address-group <name> description <text>  
# Для IPv6
```

где **<text>** – текстовое описание динамической группы.

Добавление элементов в динамические группы

Элементы добавляются в динамические группы через правила брандмауэра. Для добавления IP-адресов источника или назначения используются следующие команды:

- Добавление адреса назначения:

```
# Правило в системных наборах правил:  
set firewall ipv4 [forward | input | output] filter rule <1-999999> add-address-  
to-group destination-address address-group <name>  
set firewall ipv6 [forward | input | output] filter rule <1-999999> add-address-  
to-group destination-address address-group <name>  
  
# Правило в кастомном наборе правил:  
set firewall ipv4 name <name> rule <1-999999> add-address-to-group  
destination-address address-group <name>  
set firewall ipv6 name <name> rule <1-999999> add-address-to-group  
destination-address address-group <name>
```

- Добавление адреса источника:

```
# Правило в системных наборах правил:
set firewall ipv4 [forward | input | output] filter rule <1-999999> add-address-to-group source-address address-group <name>
set firewall ipv6 [forward | input | output] filter rule <1-999999> add-address-to-group source-address address-group <name>

# Правило в кастомном наборе правил:
set firewall ipv4 name <name> rule <1-999999> add-address-to-group source-address address-group <name>
set firewall ipv6 name <name> rule <1-999999> add-address-to-group source-address address-group <name>
```

Для каждого правила возможно задать определённый тайм-аут. Если адрес источника или назначения соответствует правилу, он будет добавлен в группу и останется в ней до истечения заданного времени. Если тайм-аут не указан, элемент будет находиться в группе до следующей перезагрузки системы **ARMA Стена** или до внесения изменений в конфигурацию МЭ, которые приведут к обновлению статуса элемента.

Для установки таймаута необходимо ввести следующие команды:

```
# Правило в системных наборах правил:
set firewall ipv4 [forward | input | output] filter rule <1-999999> add-address-to-group [destination-address | source-address] timeout <timeout>
set firewall ipv6 [forward | input | output] filter rule <1-999999> add-address-to-group [destination-address | source-address] timeout <timeout>

# Правило в кастомном наборе правил:
set firewall ipv4 name <name> rule <1-999999> add-address-to-group [destination-address | source-address] timeout <timeout>
set firewall ipv6 name <name> rule <1-999999> add-address-to-group [destination-address | source-address] timeout <timeout>
```

где **<timeout>** - значение таймаута. Тайм-аут может быть определён с помощью секунд, минут, часов или дней:

- **<number>s** - значение таймаута в секундах;
- **<number>m** - значение таймаута в минутах;
- **<number>h** - значение таймаута в часах;
- **<number>d** - значение таймаута в днях.

Допустимые диапазоны значений **<number>** в зависимости от единицы измерения:

- **секунды** - от «0» до «99 999 999»;
- **минуты** - от «0» до «99 999 999»;
- **часы** - от «0» до «5 124 095»;
- **дни** - от «0» до «213 503».

12.1.2.2 Просмотр групп

Для вывода информации о настроенных группах МЭ необходимо ввести следующую команду в эксплуатационном режиме:

```
admin@ngfwos:~$ show firewall group
```

Firewall Groups

Name	Type	References	Members
Timeout	Expires		
-----	-----	-----	-----

SERVERS	address_group		nat-destination-101
198.51.100.101			
198.51.100.102			
ALLOWED	address_group(dynamic)	ipv4-input-filter-30	192.168.77.39
7200	7174		
PN_01	address_group(dynamic)	ipv4-input-filter-10	192.168.0.245
120	112		
192.168.77.39	120	85	
PN_02	address_group(dynamic)	ipv4-input-filter-20	192.168.77.39
180	151		
LAN	interface_group	ipv4-output-filter-10	bon0
		nat-destination-101	eth2.2001
TRUSTEDv6	ipv6_network_group	ipv6-input-filter-10	2001:db8::/64
TRUSTEDv4	network_group	ipv4-forward-filter-20	192.0.2.0/30
203.0.113.128/25			
PORT-SERVERS	port_group	route-PBR-201	443
		route-PBR-201	5000-5010
		nat-destination-101	http

```
admin@ngfwos:~$
```

Таймаут (Timeout) и срок действия (Expiration) присутствуют только в динамических группах.

Для получения информации о конкретной группе МЭ необходимо ввести следующую команду в эксплуатационном режиме:

```
admin@ngfwos:~$ show firewall group <name>
```

12.1.2.3 Копирование группы

Для копирования группы необходимо ввести следующие команды:

```
admin@ngfwos# edit firewall group  
[edit firewall group]  
admin@ngfwos# copy <typealias> <name1> to <typealias> <name2>
```

где:

- **<name1>** – имя оригинальной группы;
- **<name2>** – имя создаваемой копии группы.

12.1.2.4 Переименование группы

Для переименования группы необходимо ввести следующие команды:

```
admin@ngfwos# edit firewall group  
[edit firewall group]  
admin@ngfwos# rename <typealias> <name1> to <typealias> <name2>
```

где:

- **<name1>** – изначальное имя группы;
- **<name2>** – новое имя группы.

12.1.2.5 Группы в правилах МЭ

Для добавления группы в правило МЭ необходимо ввести команду, в зависимости от направления трафика:

```
set firewall <ipv4 | ipv6 | bridge> <rule_set> rule <num> source group <typealias>  
[<name> | <!name>]  
set firewall <ipv4 | ipv6 | bridge> <rule_set> rule <num> destination group  
<typealias> [<name> | <!name>]
```

где:

- **«destination»** – назначение;
- **«source»** – источник;
- **<rule_set>** – тип набора правил (см. [Стандартная политика на основе системных наборов правил](#));
- **<name>** – имя группы;

- **<!name>** – имя группы с отрицанием.

Примечание:

В случае попытки удаления групп, используемых в правилах NAT или МЭ, система выдаст сообщение о невозможности выполнения данной операции. Необходимо сначала исключить удаляемую группу из правил, после чего повторить удаление.

12.1.3 Стандартная политика на основе системных наборов правил

12.1.3.1 Наборы правил МЭ

Набор правил – это именованный пакет правил МЭ.

В зависимости от принадлежности трафика существуют следующие наборы правил (**<rule_set>**):

1. **«input»** – системный набор правил, предназначенные для фильтрации входящих в **ARMA Стена** пакетов.
2. **«output»** – системный набор правил, предназначенные для фильтрации исходящих от **ARMA Стена** пакетов.
3. **«forward»** – системный набор правил, предназначенные для фильтрации транзитных пакетов.
4. **«name»** – кастомный набор правил. Используется во всех вариантах работы МЭ, включая системные наборы **«input»**, **«output»** и **«forward»**, реализуемый через действия правила **«jump»**.

В конфигурации по умолчанию системы **ARMA Стена** доступны системные наборы правил: **«input»**, **«output»** и **«forward»**. Эти наборы изначально не содержат никаких правил МЭ.

Для создания кастомного набора правил МЭ необходимо ввести следующую команду:

```
set firewall <type> name <nameset>
```

где:

- **<type>** – поддерживается настройка **МЭ** по следующим типам:
 - **«ipv4»** (см. [Критерии соответствия в правилах МЭ «ipv4» и «ipv6»](#));
 - **«ipv6»** (см. [Критерии соответствия в правилах МЭ «ipv4» и «ipv6»](#));
 - **«bridge»** (см. [Критерии соответствия в правилах МЭ «bridge»](#)).
- **<nameset>** – имя кастомного набора правил. Максимально допустимая длина значения «28» символов. Допускается

использование только латинских букв (A–Z, a–z), цифр (0–9) и специальных символов: подчёркивание («_») и точка («.»). Значение должно начинаться с латинской буквы или цифры.

Набор правил содержит действие по умолчанию, которое применяется к сетевому пакету, если ни одно из правил в наборе не сработало.

Для назначения действия по умолчанию для набора правил МЭ, необходимо ввести следующую команду:

- для системных наборов правил:

```
set firewall <type> <input | output | forward> filter default-action <act>
```

- для кастомного набора правил:

```
set firewall <type> name <nameset> default-action <act>
```

где **<act>** – действие по умолчанию.

Для системных наборов правил **«input»**, **«output»** и **«forward»** возможно установить следующие значения действия по умолчанию (**<act>**):

- **accept** - разрешить;
- **drop** - отбросить.

По умолчанию для наборов правил **«input»** и **«output»** выполняется действие **«accept»**, в то время как для наборов **«forward»** установлено действие **«drop»**.

Для кастомных наборов правил (**«name»**) возможно установить следующие значения действия по умолчанию (**<act>**):

- **drop** - отбросить, значение установлено по умолчанию;
- **jump** - перейти;
- **reject** - отклонить;
- **return** - вернуться;
- **accept** - разрешить;
- **continue** - продолжить.

Для добавления описания в набор правил МЭ необходимо ввести следующую команду:

- для кастомного набора правил:

```
set firewall <type> name <nameset> description <text>
```

- для системных наборов правил:

```
set firewall <type> <input | output | forward> filter description <text>
```

где **<text>** – описание набора правил.

Для включения журналирования действия по умолчанию для набора правил МЭ необходимо ввести следующую команду:

- для кастомного набора правил:

```
set firewall <type> name <nameset> default-log
```

- для системных наборов правил:

```
set firewall <type> <input | output | forward> filter default-log
```

Примечание:

При сохранении настроек после удаления набора правил, если набор назначен на направление трафика между зонами сети или используется в других наборах и правилах для переадресации на них, система выдаст ошибку с запретом на удаление. Сохранение не будет выполнено.

12.1.3.2 Правила МЭ

12.1.3.2.1 Создание правил МЭ

Правила МЭ необходимо создавать, придерживаясь следующего формата:

```
set firewall <type> <rule_set> rule <num> action <act>
```

где:

- **<rule_set>** – набор правил, к которому будет относиться правило. Возможно указать следующие значения: **«input filter»**, **«output filter»**, **«forward filter»** или **«name»**;
- **<num>** – числовой идентификатор правила. Возможно указание значения в диапазоне от «1» до «999999». Пакеты данных обрабатываются последовательно, начиная с «1» номера правила. В случае обнаружения первого соответствия с правилом, выполняется предписанное действие, после чего дальнейшая обработка данного пакета данных прекращается;
- **<act>** – действие, применяемое к пакету.

Посредством правил МЭ поддерживается выполнение следующих действий (**<act>**) над пакетом данных:

- **«accept»** – разрешить.
- **«continue»** – продолжить разбор следующего правила.
- **«drop»** – отбросить пакет.

- «**reject**» – отклонить пакет.
- «**jump**» – перейти к кастомному набору правил.

При назначении действия «**jump**» требуется указать имя целевого кастомного набора правил с помощью дополнительной команды:

```
set firewall <type> <rule_set> rule <num> jump-target  
<nameset>
```

Примечание:

Целевой набор правил, на который ссылается правило, должен быть создан заранее. В противном случае при попытке сохранить правило система выдаст ошибку, что набор <nameset> не существует: «**Invalid jump-target. Firewall ipv4 name <nameset> does not exist on the system.**».

- «**return**» – вернуться к набору правил предыдущего уровня и продолжить разбор следующего правила.

Примечание:

Действие «**return**» доступно только для кастомных наборов правил.

- «**queue**» - отправляет пакет в пользовательское пространство для дальнейшей обработки.

Данный оператор отправляет пакет в пространство пользователя с использованием функции «nfnetlink_queue». Пакет помещается в очередь, идентифицируемую по 16-разрядному номеру. Пользовательское пространство может при необходимости просмотреть и изменить пакет. Затем пользовательское пространство должно удалить пакет или повторно отправить его в ядро. Также предусмотрена возможность активации опции обхода, которая позволит не выполнять операцию записи пакета в пользовательское пространство, если в очереди нет приложений, ожидающих обработки пакета. В таком случае правило будет действовать аналогично действию «Разрешить (ассерт)», если не обнаружено приложений, ожидающих пакет.

- «**offload**» - определяет, какие потоки добавляются в таблицу потоков.

Таблицы потоков позволяют ускорить передачу пакетов в программном обеспечении (и в аппаратном обеспечении, если сетевой адаптер поддерживает эту функцию) за счёт обхода сетевого стека на основе conntrack. Записи представляются в виде кортежа, состоящего из входного интерфейса, адреса источника и

назначения, порта источника и назначения, а также протоколов уровня 3/4. Каждая запись также кэширует информацию об интерфейсе назначения и адресе шлюза (для обновления адреса назначения на канальном уровне) с целью пересылки пакетов. Поля TTL и hoplimit также декрементируются. Таким образом, таблицы потоков обеспечивают альтернативный путь, позволяющий пакетам обойти классический путь пересылки. После установления состояния потоки разгружаются. Это означает, что первый ответный пакет обычно создаёт запись в таблице потоков. Для приёма исходного трафика требуется правило межсетевого экрана. Выражение потока в прямой цепочке должно соответствовать обратному трафику из исходного соединения. Следует иметь в виду, что обратный маршрут определяется на основе пакета, который создаёт запись в таблице потоков. Если используются определённые правила IP, необходимо убедиться, что они соответствуют как трафику ответного пакета, так и исходному трафику.

Примечание:

Действие **«offload»** доступно только для наборов **«forward»** и **«name»**.

Сетевой адаптер Intel серии **X710** в системе **ARMA Стена** не поддерживает режим **«offload»**.

- **«synproxy»** – это механизм защиты от SYN flood-атак, реализованный в ядре Linux и доступный через nftables.

При получении SYN-пакета synproxy отвечает SYN/ACK с использованием SYN cookie (зашифрованного номера последовательности). Если клиент возвращает корректный ACK, соединение считается легитимным, и в таблицу conntrack добавляется обычная запись. После этого пакеты передаются напрямую реальному серверному приложению на том же хосте, без проксирования или «сшивания» соединений. Это предотвращает исчерпание ресурсов conntrack при атаках, поскольку записи создаются только после завершения handshake.

Примечание:

Действие **«synproxy»** поддерживается только в наборах **«input»** и **«forward»**.

Примечание:

Для правил типа «**bridge**» поддерживаются следующие действия над пакетом: «**accept**», «**continue**», «**jump**», «**return**», «**drop**», «**queue**».

Для добавления описания правила МЭ необходимо ввести следующую команду:

```
set firewall <type> <rule_set> rule <num> description <text>
```

где **<text>** – описание.

Для включения логирования правила необходимо ввести следующую команду:

```
set firewall <type> <rule_set> rule <num> log
```

Дополнительно возможно указать уровень логирования журнала правил МЭ:

```
set firewall <type> <rule_set> rule <num> log-options level <emerg | alert | crit  
| err | warn | notice | info | debug>
```

где:

- **emerg** - уровень лога, предназначенный для записи сообщений о критических аварийных ситуациях;
- **alert** - уровень лога, фиксирующий важные предупреждения;
- **crit** - уровень лога, отображающий критические системные сообщения;
- **err** - уровень лога, регистрирующий ошибки и неисправности в работе системы;
- **warn** - уровень лога, используемый для записи предупреждений о потенциальных проблемах;
- **notice** - уровень лога, предназначенный для уведомления о значимых событиях;
- **info** - уровень лога, отображающий общую информацию о функционировании системы;
- **debug** - уровень лога, фиксирующий детализированные отладочные данные.

Для отключения правила МЭ необходимо ввести следующую команду:

```
set firewall <type> <rule_set> rule <num> disable
```

12.1.3.2.2 Копирование правила МЭ

Копирование правил позволяет значительно ускорить процесс настройки МЭ.

Для копирования правила МЭ необходимо ввести следующие команды:

- для кастомного набора правил:

```
admin@ngfwos# edit firewall <type> name <nameset>

[edit firewall <type> name <nameset>]
admin@ngfwos# copy rule <num1> to rule <num2>

[edit firewall <type> name <nameset>]
admin@ngfwos# exit

[edit]
admin@ngfwos#
```

- для системных наборов правил:

```
admin@ngfwos# edit firewall <type> <input | output | forward> filter

[edit firewall <type> <input | output | forward> filter]
admin@ngfwos# copy rule <num1> to rule <num2>

[edit firewall <type> <input | output | forward> filter]
admin@ngfwos# exit

[edit]
admin@ngfwos#
```

где:

- **<num1>** – идентификатор оригинального правила;
- **<num2>** – идентификатор создаваемой копии правила.

12.1.3.2.3 Переименование правила МЭ

Переименование правила межсетевого экрана (изменение его идентификатора) выполняется в режиме конфигурации через командную строку. Порядок действий определяется типом набора правил.

- Переименование правила в кастомном наборе правил:

```
admin@ngfwos# edit firewall <type> name <nameset>

[edit firewall <type> name <nameset>]
admin@ngfwos# rename rule <num1> to rule <num2>

[edit firewall <type> name <nameset>]
admin@ngfwos# exit

[edit]
admin@ngfwos#
```

- Переименование правила в системном наборе правил:

```
admin@ngfwos# edit firewall <type> <input | output | forward> filter

[edit firewall <type> <input | output | forward> filter]
admin@ngfwos# rename rule <num1> to rule <num2>

[edit firewall <type> <input | output | forward> filter]
admin@ngfwos# exit

[edit]
admin@ngfwos#
```

где:

- **<num1>** – исходный идентификатор правила;
- **<num2>** – новый идентификатор правила.

Групповая перенумерация правил МЭ

Для массового изменения идентификаторов всех правил МЭ применяется процедура групповой перенумерации. Все действия рекомендуется выполнять в SSH-сессии для удобства копирования и вставки команд.

Примечание:

В процессе применения новой конфигурации (выполнения команды **«commit»**) может наблюдаться временный период, в течение которого часть правил межсетевого экрана не применяется или обрабатывает некорректно. Это может привести к неконтролируемому прохождению сетевого трафика через интерфейсы устройства. В связи с этим процедуру групповой перенумерации рекомендуется выполнять в периоды минимальной нагрузки на сеть или в рамках планового технического окна, когда

влияние на безопасность и стабильность инфраструктуры сведено к минимуму.

1. Генерация новой последовательности идентификаторов.

В эксплуатационном режиме выполнить команду:

```
admin@ngfwos:~$ generate firewall rule-resequence [start <1-1000 > step  
<1-1000 >]
```

По умолчанию перенумерация выполняется с начального значения «100» и шагом «10».

Необязательные параметры:

- **start** – определяет начальный номер первого правила в последовательности (диапазон: 1–1000);
- **step** – задаёт интервал между номерами последовательных правил (диапазон: 1–1000).

2. Просмотр и копирование сгенерированного списка команд.

Система выводит список команд в формате `set`, соответствующих обновлённой нумерации правил. Данный список следует скопировать в буфер обмена.

3. Удаление текущей конфигурации МЭ.

Переход в режим конфигурации и удаление всех правил межсетевого экрана:

```
admin@ngfwos# delete firewall  
Must specify config path  
[edit]  
admin@ngfwos#
```

4. Применение новой конфигурации.

Скопированные команды применяются в режиме конфигурации – вставляются по одной или группой.

5. Сохранение изменений:

```
admin@ngfwos# commit  
admin@ngfwos# save
```

Пример групповой перенумерации:

1. Исходная конфигурация:


```
admin@ngfwos# show firewall
bridge {
    forward {
        filter {
            default-action drop {
            }
            rule 1 {
                destination {
                    mac-address 01:23:45:67:89:AB {
                    }
                }
                log {
                }
                action accept {
                }
            }
            rule 2 {
                destination {
                    mac-address 01:B2:C3:D4:E5:F6 {
                    }
                }
                log {
                }
                action accept {
                }
            }
        }
    }
}
ipv4 {
    forward {
        filter {
            default-action drop {
            }
        }
    }
    input {
        filter {
            rule 1 {
                icmp {
                    type 1 {
                    }
                }
            }
        }
    }
}
```

```
    }  
    log {  
    }  
    action drop {  
    }  
  }  
}  
}  
[edit]
```

2. Выполнение команды генерации:

```
admin@ngfwos:~$ generate firewall rule-resequence
```

3. Результат генерации:

```
set firewall bridge forward filter default-action 'drop'  
set firewall bridge forward filter rule 100 action 'accept'  
set firewall bridge forward filter rule 100 destination mac-address  
'01:23:45:67:89:AB'  
set firewall bridge forward filter rule 100 log  
set firewall bridge forward filter rule 110 action 'accept'  
set firewall bridge forward filter rule 110 destination mac-address  
'01:B2:C3:D4:E5:F6'  
set firewall bridge forward filter rule 110 log  
set firewall ipv4 forward filter default-action 'drop'  
set firewall ipv4 input filter rule 100 action 'drop'  
set firewall ipv4 input filter rule 100 icmp type '1'  
set firewall ipv4 input filter rule 100 log
```

Результат необходимо скопировать в буфер обмена (рекомендуется использовать SSH-клиент с поддержкой копирования текста).

4. Удаление текущей конфигурации:

```
admin@ngfwos# delete firewall  
Must specify config path  
[edit]  
admin@ngfwos#
```

5. Применение сгенерированных команд (вставка по одной или группой в конфигурационный режим).

```
admin@ngfwos# set firewall bridge forward filter default-action 'drop'  
set firewall bridge forward filter rule 100 action 'accept'
```

```
set firewall bridge forward filter rule 100 destination mac-address
'01:23:45:67:89:AB'
set firewall bridge forward filter rule 100 log
set firewall bridge forward filter rule 110 action 'accept'
set firewall bridge forward filter rule 110 destination mac-address
'01:B2:C3:D4:E5:F6'
set firewall bridge forward filter rule 110 log
set firewall ipv4 forward filter default-action 'drop'
set firewall ipv4 input filter rule 100 action 'drop'
set firewall ipv4 input filter rule 100 icmp type '1'
set firewall ipv4 input filter rule 100 log
[edit]
admin@ngfwos# set firewall bridge forward filter rule 100 action 'accept'
[edit]
admin@ngfwos# set firewall bridge forward filter rule 100 destination mac-
address '01:23:45:67:89:AB'
[edit]
admin@ngfwos# set firewall bridge forward filter rule 100 log
[edit]
admin@ngfwos# set firewall bridge forward filter rule 110 action 'accept'
[edit]
admin@ngfwos# set firewall bridge forward filter rule 110 destination mac-
address '01:B2:C3:D4:E5:F6'
[edit]
admin@ngfwos# set firewall bridge forward filter rule 110 log
[edit]
admin@ngfwos# set firewall ipv4 forward filter default-action 'drop'
[edit]
admin@ngfwos# set firewall ipv4 input filter rule 100 action 'drop'
[edit]
admin@ngfwos# set firewall ipv4 input filter rule 100 icmp type '1'
[edit]
admin@ngfwos# set firewall ipv4 input filter rule 100 log
[edit]
```

6. Применить и сохранить настройки:

```
admin@ngfwos# commit
admin@ngfwos# save
```

7. Проверка результата:

```
admin@ngfwos# show firewall
bridge {
    forward {
        filter {
            default-action drop {
            }
            rule 100 {
                destination {
                    mac-address 01:23:45:67:89:AB {
                    }
                }
                log {
                }
                action accept {
                }
            }
            rule 110 {
                destination {
                    mac-address 01:B2:C3:D4:E5:F6 {
                    }
                }
                log {
                }
                action accept {
                }
            }
        }
    }
}
ipv4 {
    forward {
        filter {
            default-action drop {
            }
        }
    }
    input {
        filter {
            rule 100 {
                icmp {
                    type 1 {
                    }
                }
            }
        }
    }
}
```

```

    }
    log {
    }
    action drop {
    }
  }
}
[edit]

```

Групповая перенумерация правил межсетевого экрана завершена успешно.

12.1.3.3 Критерии соответствия в правилах МЭ «ipv4» и «ipv6»

ARMA Стена поддерживает возможность указания в правилах МЭ типа «**ipv4**» и «**ipv6**» различных критериев соответствия, по которым выполняется фильтрация.

При указании в одном правиле нескольких критериев соответствия применяется логическое условие **И (AND)**: правило срабатывает только в случае одновременного совпадения всех заданных критериев.

Это требует особого внимания при проектировании правил. Например, если в одном правиле в качестве домена источника и домена назначения указан один и тот же адрес – например, «example.com» – и для правила задано действие «drop», то блокировка применена не будет к обычному трафику пользователей, направленному к «example.com». Правило в данном случае будет соответствовать только тем сетевым соединениям, у которых и источник, и получатель принадлежат домену example.com, что в типовой сетевой инфраструктуре маловероятно.

12.1.3.3.1 Адрес источника

Для указания адреса источника в качестве критерия соответствия необходимо ввести следующую команду:

```
set firewall ipv4|ipv6 <rule_set> rule <num> source address [<IPv4-address> | <addressrange> | <IPv6-address>]
```

где:

- **<IPv4-address>** – IPv4-адрес источника. Возможно указание в следующих форматах: <x.x.x.x>, <x.x.x.x/x>;
- **<addressrange>** – диапазон IP-адресов. В зависимости от версии IP возможно указание в следующих форматах: <x.x.x.x>-<x.x.x.x>, <h:h:h:h:h:h:h>-<h:h:h:h:h:h:h>;
- **<IPv6-address>** – IPv6-адрес источника. Возможно указание в следующих форматах: <h:h:h:h:h:h:h>, <h:h:h:h:h:h:h/x>.

12.1.3.3.2 Адрес назначения

Для указания адреса назначения в качестве критерия соответствия необходимо ввести следующую команду:

```
set firewall ipv4|ipv6 <rule_set> rule <num> destination address [<IPv4-address> |  
<addressrange> | <IPv6-address>]
```

где:

- **<IPv4-address>** – IPv4-адрес назначения. Возможно указание в следующих форматах: <x.x.x.x>, <x.x.x.x/x>;
- **<addressrange>** – диапазон IP-адресов. В зависимости от версии IP возможно указание в следующих форматах: <x.x.x.x>-<x.x.x.x>, <h:h:h:h:h:h:h>-<h:h:h:h:h:h:h>;
- **<IPv6-address>** – IPv6-адрес назначения. Возможно указание в следующих форматах: <h:h:h:h:h:h:h>, <h:h:h:h:h:h:h/x>.

12.1.3.3.3 Протокол

Для указания протокола в качестве критерия соответствия необходимо ввести следующую команду:

```
set firewall ipv4|ipv6 <rule_set> rule <num> protocol [<protocolname> | tcp_udp |  
all | <number>]
```

где:

- **<protocolname>** – протокол, определённый в «/etc/protocols»;
- **<tcp_udp>** – протоколы TCP и UDP;
- **<all>** – все протоколы;
- **<number>** – номер протокола, определённый в «/etc/protocols». Возможно указание значения в диапазоне от «0» до «255».

Примечание:

Поддерживается указание значение **<protocolname>** с использованием знака «!» для инверсии, например, **<!icmp>**.

Для указания протокола **<icmp>** в качестве критерия соответствия необходимо ввести следующую команду:

```
set firewall ipv4|ipv6 <rule_set> rule <num> icmp|icmpv6 <code <0-255> | type <0-  
255>>
```

где:

- **<code>** – номер кода icmp. Возможно указание значения в диапазоне от «0» до «255»;
- **<type>** – номер типа icmp. Возможно указание значения в диапазоне от «0» до «255»;

Поддерживается указание имени типа **«icmp»** в качестве критерия соответствия:

```
set firewall ipv4|ipv6 <rule_set> rule <num> icmp|icmpv6 type-name <text>
```

где **<text>** – имя типа icmp.

Для **«icmp»** возможно указать следующие значения:

- **echo-reply** – ICMP тип 0;
- **destination-unreachable** – ICMP тип 3;
- **source-quench** – ICMP тип 4;
- **redirect** – ICMP тип 5;
- **echo-request** – ICMP тип 8;
- **router-advertisement** – ICMP тип 9;
- **router-solicitation** – ICMP тип 10;
- **time-exceeded** – ICMP тип 11;
- **parameter-problem** – ICMP тип 12;
- **timestamp-request** – ICMP тип 13;
- **timestamp-reply** – ICMP тип 14;
- **info-request** – ICMP тип 15;
- **info-reply** – ICMP тип 16;
- **address-mask-request** – ICMP тип 17;
- **address-mask-reply** – ICMP тип 18.

Для **«icmpv6»** возможно указать следующие значения:

- **destination-unreachable** – ICMPv6 тип 1;
- **packet-too-big** – ICMPv6 тип 2;
- **time-exceeded** – ICMPv6 тип 3;
- **echo-request** – ICMPv6 тип 128;
- **echo-reply** – ICMPv6 тип 129;
- **mld-listener-query** – ICMPv6 тип 130;
- **mld-listener-report** – ICMPv6 тип 131;

- **mld-listener-reduction** – ICMPv6 тип 132;
- **nd-router-solicit** – ICMPv6 тип 133;
- **nd-router-advert** – ICMPv6 тип 134;
- **nd-neighbor-solicit** – ICMPv6 тип 135;
- **nd-neighbor-advert** – ICMPv6 тип 136;
- **nd-redirect** – ICMPv6 тип 137;
- **parameter-problem** – ICMPv6 тип 4;
- **router-renumbering** – ICMPv6 тип 138;
- **ind-neighbor-solicit** – ICMPv6 тип 141;
- **ind-neighbor-advert** – ICMPv6 тип 142;
- **mld2-listener-report** – ICMPv6 тип 143.

Для указания флага протокола «**tcp**» в качестве критерия соответствия необходимо ввести следующую команду:

```
set firewall ipv4|ipv6 <rule_set> rule <num> tcp flags <flags>
```

где **<flags>** – флаг TCP.

Поддерживается указание следующих флагов:

- «**ack**»;
- «**cwr**»;
- «**ecn**»;
- «**fin**»;
- «**psh**»;
- «**rst**»;
- «**syn**»;
- «**urg**».

Для указания флага с инверсией необходимо ввести следующую команду:

```
set firewall ipv4|ipv6 <rule_set> rule <num> tcp flags not <flags>
```

Для указания максимального размера сегмента в качестве дополнительного параметра протокола «**tcp**» необходимо ввести следующую команду:

```
set firewall ipv4|ipv6 <rule_set> rule <num> tcp mss <number>
```

где **<number>** – максимальный размер сегмента. Возможно указание значения в диапазоне от «1» до «16384».

Поддерживается указание диапазона значений, разделённых знаком «-».

Для указания протокола «IPsec» в качестве критерия соответствия необходимо ввести следующую команду:

```
set firewall ipv4|ipv6 <rule_set> rule <num> ipsec [match-ipsec | match-none]
```

где:

- **<match-ipsec>** – входящие пакеты IPsec;
- **<match-none>** – входящие пакеты, не соответствующие IPsec.

Примечание:

В случае необходимости изменения протокола, указанного в качестве критерия соответствия, требуется предварительно удалить значения дополнительных параметров заменяемого протокола.

12.1.3.3.4 Порт источника

Назначение порта источника в качестве критерия соответствия поддерживается только в случае указания следующих значений протокола: «**tcp**», «**udp**», «**tcp_udp**».

Для указания порта источника в качестве критерия соответствия необходимо ввести следующую команду:

```
set firewall ipv4|ipv6 <rule_set> rule <num> source port [<portnumber> | <portname> | <rangenumbers>]
```

где:

- **<portnumber>** – номер порта источника. Возможно указание значения в диапазоне от «1» до «65535»;
- **<portname>** – имя, определённое в «/etc/services»;
- **<rangenumbers>** – диапазон портов, разделённых знаком «-».

Примечание:

Поддерживается указание нескольких значений портов, разделённых знаком «,», например:

```
set firewall ipv4|ipv6 <rule_set> rule <num> source port http,1100-1200,25
```

12.1.3.3.5 Порт назначения

Назначение порта назначения в качестве критерия соответствия поддерживается только в случае указания следующих значений протокола: «**tcp**», «**udp**», «**tcp_udp**».

Для указания порта назначения в качестве критерия соответствия необходимо ввести следующую команду:

```
set firewall ipv4|ipv6 <rule_set> rule <num> destination port [<portnumber> |  
<portname> | <rangenumbers>]
```

где:

- **<portnumber>** – номер порта назначения. Возможно указание значения в диапазоне от «1» до «65535»;
- **<portname>** – имя, определённое в «/etc/services»;
- **<rangenumbers>** – диапазон портов, разделённых знаком «-».

Примечание:

Поддерживается указание нескольких значений портов, разделённых знаком «,».

12.1.3.3.6 Входящий интерфейс

Для указания входящего интерфейса в качестве критерия соответствия необходимо ввести следующую команду:

```
set firewall ipv4|ipv6 <rule_set> rule <num> inbound-interface name <interface>
```

где **<interface>** – имя интерфейса.

Примечание:

Поддерживается указание входящего интерфейса в качестве критерия соответствия для правил категорий: «**name**», «**forward filter**», «**input filter**».

12.1.3.3.7 Исходящий интерфейс

Для указания исходящего интерфейса в качестве критерия соответствия необходимо ввести следующую команду:

```
set firewall ipv4|ipv6 <rule_set> rule <num> outbound-interface name <interface>
```

где **<interface>** – имя интерфейса.

Примечание:

Поддерживается указание исходящего интерфейса в качестве критерия соответствия для правил категорий: «**name**», «**forward filter**», «**output filter**».

12.1.3.3.8 Статус пакета

Для указания статуса пакета в качестве критерия соответствия необходимо ввести следующую команду:

```
set firewall ipv4|ipv6 <rule_set> rule <num> state [established | invalid | new | related]
```

где:

- «**established**» – установленный;
- «**invalid**» – недопустимый;
- «**new**» – новый;
- «**related**» – связанный.

12.1.3.3.9 Доменное имя источника

Для указания доменного имени источника в качестве критерия соответствия необходимо ввести следующую команду:

```
set firewall ipv4|ipv6 <rule_set> rule <num> source fqdn <fqdn>
```

где **<fqdn>** – доменное имя.

12.1.3.3.10 Доменное имя назначения

Для указания доменного имени назначения в качестве критерия соответствия необходимо ввести следующую команду:

```
set firewall ipv4|ipv6 <rule_set> rule <num> destination fqdn <fqdn>
```

12.1.3.3.11 GeoIP

Технология GeoIP позволяет создавать правила межсетевого экрана в зависимости от того, к какой стране или региону принадлежит адрес хоста.

Для указания **GeoIP источника** в качестве критерия соответствия необходимо ввести следующую команду:

```
set firewall ipv4|ipv6 <rule_set> rule <num> source geoip country-code <country>
```

где **<country>** – код страны, например, «ru». Перечень кодов стран приведён в таблице (см. [Таблица «Коды стран»](#)).

Для инверсии правила необходимо ввести следующую команду:

```
set firewall ipv4|ipv6 <rule_set> rule <num> source geoip inverse-match
```

Правило будет распространяться на IP-адреса, соответствующие всем геолокациям, кроме указанных в правиле.

Для указания **GeoIP назначения** в качестве критерия соответствия необходимо ввести следующую команду:

```
set firewall ipv4|ipv6 <rule_set> rule <num> destination geoip country-code <country>
```

Для инверсии правила необходимо ввести следующую команду:

```
set firewall ipv4|ipv6 <rule_set> rule <num> destination geoip inverse-match
```

В рамках технологии GeoIP локальным подсетям, находящимся в диапазонах «10.0.0.0-10.255.255.255», «172.16.0.0-172.31.255.255», «192.168.0.0-192.168.255.255», «fc00::-fdff:ffff:ffff:ffff:ffff:ffff:ffff:ffff», присвоен код страны **«ZZ»**. Это необходимо учитывать при фильтрации сетевого трафика на основе принадлежности к определённым кодам стран. В случае необходимости следует создавать правила с более высоким приоритетом для разрешения пакетов с локальными IP-адресами. Пример:

```
set firewall ipv4 forward filter default-action 'accept'
set firewall ipv4 forward filter default-log
set firewall ipv4 forward filter rule 10 action 'accept'
set firewall ipv4 forward filter rule 10 destination address '192.168.0.0/16'
set firewall ipv4 forward filter rule 20 action 'drop'
set firewall ipv4 forward filter rule 20 destination geoip country-code 'ru'
set firewall ipv4 forward filter rule 20 destination geoip inverse-match
set firewall ipv4 forward filter rule 20 log
```

Правило 20 блокирует весь сетевой трафик, за исключением пакетов, содержащих IP-адреса, находящиеся в Российской Федерации. Поскольку IP-адреса локальной подсети предприятия не входят в список адресов с кодом страны RU, необходимо создать правило 10, разрешающее сетевой трафик для частной подсети 192.168.0.0/16, используемой на данном предприятии.

Таблица «Коды стран»

Код	Страна	Код	Страна
AD	Андорра	AE	Объединённые Арабские Эмираты
AF	Афганистан	AG	Антигуа и Барбуда
AI	Ангилья	AL	Албания
AM	Армения	AO	Ангола
AQ	Антарктида	AR	Аргентина
AS	Американское Самоа	AT	Австрия
AU	Австралия	AW	Аруба
AX	Эландские острова	AZ	Азербайджан

Код	Страна	Код	Страна
BA	Босния и Герцеговина	BB	Барбадос
BD	Бангладеш	BE	Бельгия
BF	Буркина-Фасо	BG	Болгария
BH	Бахрейн	BI	Бурунди
BJ	Бенин	BL	Сен-Бартельми
BM	Бермуды	BN	Бруней-Даруссалам
BO	Боливия	BR	Бразилия
BQ	Бонайре, Саба и Синт-Эстатиус	BS	Багамские острова
BT	Бутан	BV	Остров Буве
BW	Ботсвана	BY	Беларусь
BZ	Белиз	CA	Канада
CC	Кокосовые острова (Килинг)	CD	ДР Конго
CF	ЦАР	CG	Конго
CH	Швейцария	CI	Республика Кот д'Ивуар
CK	Острова Кука	CL	Чили
CM	Камерун	CN	Китай
CO	Колумбия	CR	Коста-Рика
CU	Куба	CV	Кабо-Верде
CW	Кюрасао	CX	Остров Рождества
CY	Кипр	CZ	Чешская Республика
DE	Германия	DJ	Джибути
DK	Дания	DM	Доминика
DO	Доминиканская Республика	DZ	Алжир
EC	Эквадор	EE	Эстония
EG	Египет	EH	Западная Сахара
ER	Эритрея	ES	Испания
ET	Эфиопия	FI	Финляндия

Код	Страна	Код	Страна
FJ	Республика островов Фиджи	FK	Фолклендские острова
FM	Микронезия	FO	Фарерские острова
FR	Франция	GA	Габон
GB	Великобритания	GD	Гренада
GE	Грузия	GF	Французская Гвиана
GG	Гернси	GH	Гана
GI	Гибралтар	GL	Гренландия
GM	Гамбия	GN	Гвинея
GP	Гваделупа	GQ	Экваториальная Гвинея
GR	Греция	GS	Юж-я Георгия и Юж-е Сандвичевы о-ва
GT	Гватемала	GU	Гуам
GW	Гвинея-Бисау	GY	Гайана
HK	Гонконг	HM	Остров Херд и острова Макдональд
HN	Гондурас	HR	Хорватия
HT	Гаити	HU	Венгрия
ID	Индонезия	IE	Ирландия
IL	Израиль	IM	Остров Мэн
IN	Индия	IO	Британская тер. в Индийском океане
IQ	Ирак	IR	Иран, Исламская Республика
IS	Исландия	IT	Италия
JE	Джерси	JM	Ямайка
JO	Иордания	JP	Япония
KE	Кения	KG	Кыргызстан
KH	Камбоджа	KI	Кирибати
KM	Коморские острова	KN	Сент-Китс и Невис
KP	КНДР	KR	Республика Корея
KW	Кувейт	KY	Каймановы острова

Код	Страна	Код	Страна
KZ	Казахстан	LA	Лаос
LB	Ливан	LC	Сент-Люсия
LI	Лихтенштейн	LK	Шри-Ланка
LR	Либерия	LS	Лесото
LT	Литва	LU	Люксембург
LV	Латвия	LY	Ливийская Арабская Республика
MA	Марокко	MC	Монако
MD	Республика Молдова	ME	Республика Черногория
MF	Сен-Мартен	MG	Мадагаскар
MH	Маршалловы острова	MK	Республика Македония
ML	Мали	MM	Мьянма
MN	Монголия	MO	Макао
MP	Северные Марианские острова	MQ	Мартиника
MR	Мавритания	MS	Монтсеррат
MT	Мальта	MU	Маврикий
MV	Мальдивы	MW	Малави
MX	Мексика	MY	Малайзия
MZ	Мозамбик	NA	Намибия
NC	Новая Каледония	NE	Республика Нигер
NF	Остров Норфолк	NG	Нигерия
NI	Никарагуа	NL	Нидерланды
NO	Норвегия	NP	Непал
NR	Науру	NU	Ниуэ
NZ	Новая Зеландия	OM	Оман
PA	Панама	PE	Перу
PF	Французская Полинезия	PG	Папуа-Новая Гвинея
PH	Филиппины	PK	Пакистан
PL	Польша	PM	Сент-Пьер и Микелон
PN	Питкэрн	PR	Пуэрто-Рико

Код	Страна	Код	Страна
PS	Палестинская территория	PT	Португалия
PW	Палау	PY	Парагвай
QA	Катар	RE	Реюньон
RO	Румыния	RS	Сербия
RU	Российская Федерация	RW	Руанда
SA	Саудовская Аравия	SB	Соломоновы Острова
SC	Сейшельские Острова	SD	Судан
SE	Швеция	SG	Сингапур
SH	Острова Св. Елены	SI	Словения
SJ	Шпицберген и Ян-Майен	SK	Словакия
SL	Сьерра-Леоне	SM	Сан-Марино
SN	Сенегал	SO	Сомали
SR	Суринам	SS	Южный Судан
ST	Сан-Томе и Принсипи	SV	Республика Эль-Сальвадор
SX	Синт-Мартен	SY	Сирийская Арабская Республика
SZ	Королевство Эсватини	TC	Острова Тёркс и Кайкос
TD	Республика Чад	TF	ФЮАТ
TG	Того	TH	Таиланд
TJ	Таджикистан	TK	Токелау
TL	Восточный Тимор	TM	Туркменистан
TN	Тунис	TO	Тонга
TR	Турция	TT	Тринидад и Тобаго
TV	Тувалу	TW	Тайвань
TZ	Танзания	UA	Украина
UG	Уганда	UM	Внешние малые острова США
US	Соединённые Штаты Америки	UY	Уругвай
UZ	Узбекистан	VA	Государство Ватикан
VC	Сент-Винсент и Гренадины	VE	Венесуэла

Код	Страна	Код	Страна
VG	Британские Виргинские острова	VI	Виргинские острова (США)
VN	Вьетнам	VU	Вануату
WF	Уоллис и Футуна	WS	Независимое Государство Самоа
YE	Йемен	YT	Майотта
ZA	Южно-Африканская Республика	ZM	Замбия
ZW	Зимбабве		

Для обновления базы данных GeoIP необходимо в режиме эксплуатации ввести следующую команду:

```
admin@ngfwos:~$ update geoip
```

Примечание:

База данных GeoIP обновляется с ресурса «download.db-ip.com» на основании лицензии **CC-BY-4.0**.

Для обеспечения корректного процесса обновления требуется предварительная настройка DNS-сервера. Для этого следует выполнить команду:

```
set system name-server <address>
```

где **<address>** – IP-адрес DNS-сервера.

12.1.3.3.12 MAC-адрес источника

Для указания MAC-адреса источника в качестве критерия соответствия необходимо ввести следующую команду:

```
set firewall ipv4|ipv6 <rule_set> rule <num> source mac-address <h:h:h:h:h>
```

где **<h:h:h:h:h>** – MAC-адрес источника.

12.1.3.3.13 Значение DSCP

Для указания значения DSCP в качестве критерия соответствия необходимо ввести следующую команду:

```
set firewall ipv4|ipv6 <rule_set> rule <num> dscp [<0-63> | <start-end>]
```

где:

- **<0-63>** - номер класса трафика. Возможно указание значения в диапазоне от «0» до «63»;
- **<start-end>** - диапазон значений класса трафика, разделённых знаком «-».

Для указания значения DSCP с инверсией необходимо ввести следующую команду:

```
set firewall ipv4|ipv6 <rule_set> rule <num> dscp-exclude [<0-63> | <start-end>]
```

12.1.3.4 Критерии соответствия в правилах МЭ «bridge»

Система **ARMA Стена** поддерживает задание различных критериев соответствия в правилах межсетевого экрана типа «**bridge**», по которым осуществляется фильтрация сетевого трафика на уровне канала передачи данных (L2).

12.1.3.4.1 MAC-адрес назначения

Для задания MAC-адреса назначения в качестве критерия соответствия используется команда:

```
set firewall bridge <rule_set> rule <num> destination mac-address <h:h:h:h:h:h>
```

где **<h:h:h:h:h:h>** – MAC-адрес назначения в формате шести шестнадцатеричных октетов, разделённых двоеточиями.

Поддерживается инверсия условия с использованием символа «!», например: **<!00:11:22:33:44:55>**.

12.1.3.4.2 MAC-адрес источника

Для задания MAC-адреса источника в качестве критерия соответствия используется команда:

```
set firewall bridge <rule_set> rule <num> source mac-address <h:h:h:h:h:h>
```

где **<h:h:h:h:h:h>** – MAC-адрес источника в формате шести шестнадцатеричных октетов, разделённых двоеточиями.

Поддерживается инверсия условия с использованием символа «!».

12.1.3.4.3 Входящий интерфейс

Для задания входящего интерфейса в качестве критерия соответствия используется команда:

```
set firewall bridge <rule_set> rule <num> inbound-interface name <interface>
```

где **<interface>** – имя логического или физического интерфейса.

Поддерживается указание имени интерфейса с использованием знака «!» для инверсии или подстановочного символа «*», например:

- «!eth0» – все интерфейсы, кроме «eth0»;
- «eth2*» – все интерфейсы, имена которых начинаются с «eth2».

12.1.3.4.4 Исходящий интерфейс

Для задания исходящего интерфейса в качестве критерия соответствия используется команда:

```
set firewall bridge <rule_set> rule <num> outbound-interface name <interface>
```

где **<interface>** – имя логического или физического интерфейса.

Поддерживаются инверсия с помощью символа «!» и использование подстановочного символа «*», аналогично входящему интерфейсу.

12.1.3.4.5 Идентификатор VLAN

Для задания идентификатора VLAN в качестве критерия соответствия используется команда:

```
set firewall bridge <rule_set> rule <num> vlan id <vlan-id>
```

где **<vlan-id>** – идентификатор VLAN. Возможно указание значений в диапазоне от «0» до «4096». Допускается указание диапазона значений, разделённых символом «-».

12.1.3.4.6 Приоритет VLAN

Для задания приоритета VLAN в качестве критерия соответствия используется команда:

```
set firewall bridge <rule_set> rule <num> vlan priority <number>
```

где **<number>** – значение приоритета VLAN. Возможно указание значений в диапазоне от «0» до «7». Допускается указание диапазона значений, разделённых символом «-».

12.1.3.4.7 EtherType

Для использования значения поля EtherType в качестве критерия фильтрации применяется команда:

```
set firewall bridge <rule_set> rule <num> [vlan] ethernet-type <text>
```

где:

- **<text>** - значение поля EtherType, задаваемое в формате «0xXXXX», где «XXXX» представляет собой двухбайтовое шестнадцатеричное число.

Вместо шестнадцатеричного представления допускается использование следующих predefined символьных имён:

- **802.1q** – соответствует 0x8100 (VLAN Tagged Frame);
 - **802.1ad** – соответствует 0x88A8 (Provider Bridging);
 - **arp** – соответствует 0x0806 (Address Resolution Protocol);
 - **ipv4** – соответствует 0x0800 (IPv4);
 - **ipv6** – соответствует 0x86DD (IPv6);
 - **ethercat** – соответствует 0x88A4 (EtherCAT).
- **[vlan]** – необязательный параметр, определяющий, что анализируемое значение EtherType расположено во внутреннем заголовке кадра, следующем непосредственно за тегом VLAN (802.1Q или 802.1ad).

Поддерживается инверсия условия фильтрации с использованием символа «!». Пример: «!0x0800» – сопоставление всех кадров, за исключением IPv4.

Особенности обработки EtherType в зависимости от наличия параметра vlan:

- *Без указания параметра vlan* – анализируется внешнее поле EtherType. Например, для кадра с VLAN-тегом значением будет «0x8100».
- *С указанием параметра vlan* – анализируется поле EtherType, расположенное после VLAN-тега. Например, для IPv4-пакета, инкапсулированного в VLAN, значением будет «0x0800».

Такой подход обеспечивает корректную фильтрацию инкапсулированного трафика (ARP, IPv4, IPv6 и др.) в сетях с использованием VLAN.

12.1.3.5 Срабатывание правил по расписанию

Для задания временных условий активности правила в системе ARMA Стена используется параметр **«time»**, позволяющий определить точные дату и время начала и окончания действия правила, а также указать дни недели, в течение которых правило должно быть активным.

Все временные параметры интерпретируются относительно системного времени устройства **ARMA Стена**.

Команды настройки параметра **«time»**:

1. Установка даты начала действия правила:

```
set firewall ipv4|ipv6 <rule_set> rule <num> time startdate <text>
```

где **<text>** – дата начала действия правила в формате **«YYYY-MM-DD»**.

2. Установка времени начала действия правила:

```
set firewall ipv4|ipv6 <rule_set> rule <num> time starttime <text>
```

где **<text>** – время начала действия правила в формате **«hh:mm:ss»**.

3. Установка даты окончания действия правила:

```
set firewall ipv4|ipv6 <rule_set> rule <num> time stopdate <text>
```

где **<text>** – дата окончания действия правила в формате «**YYYY-MM-DD**».

4. Установка времени окончания действия правила:

```
set firewall ipv4|ipv6 <rule_set> rule <num> time stoptime <text>
```

где **<text>** – время окончания действия правила в формате «**hh:mm:ss**».

5. Установка дней недели для действия правила:

```
set firewall ipv4|ipv6 <rule_set> rule <num> time weekdays <text>
```

где **<text>** – список дней недели, в течение которых правило применяется.

Допустимые форматы значений:

- Текстовые обозначения дней недели:
«**Monday**», «**Tuesday**», «**Wednesday**», «**Thursday**», «**Friday**»,
«**Saturday**», «**Sunday**».
- Числовые обозначения дней недели:
Диапазон от «**0**» (воскресенье) до «**6**» (суббота).

Поддерживаются следующие способы указания списка:

- Перечисление значений через запятую **без пробелов**, например:
«Monday,Wednesday,Friday».
- Смешанное использование текстовых и числовых обозначений,
например: «Monday,Wednesday,5».

12.1.4 Политика на основе зон

В качестве альтернативы непосредственному применению политик к сетевым интерфейсам может быть создана зонная модель брандмауэра. Эта модель упрощает конфигурацию в ситуациях, когда несколько интерфейсов принадлежат одной зоне безопасности. Вместо применения наборов правил к интерфейсам, правила применяются к парам «исходная зона – целевая зона». Правила настраиваются для зон, а не для отдельных интерфейсов, что снижает сложность конфигурации при большом количестве интерфейсов.

В МЭ на основе зон реализована новая концепция, дополнительно к стандартным входящим и исходящим потокам трафика был добавлен локальный поток. Он предназначен для входящего и исходящего трафика **ARMA Стена**. Это предоставляет возможность установить дополнительные правила МЭ, которые будут защищать сам брандмауэр от внешних угроз сети, дополняя уже существующие входящие и исходящие правила МЭ.

Основные тезисы:

- перед назначением интерфейса зоне необходимо выполнить её конфигурацию;
- интерфейс может быть назначен только одной зоне;
- в пределах зоны разрешён весь входящий и исходящий трафик интерфейса;
- трафик между зонами зависит от существующих политик;
- трафик не может передаваться между интерфейсом-участником зоны и любым интерфейсом, который не является участником этой зоны;
- для каждого направления трафика необходимо задать отдельную политику.

В общем случае алгоритм настройки работы МЭ на основе зон сети выглядит следующим образом:

1. Создать **кастомные наборы правил МЭ**, в которых будут содержаться правила.
2. Создать **правила МЭ**, указать в них критерии соответствия, действия с сетевыми пакетами и привязать эти правила к кастомным наборам.
3. Объединить интерфейсы в **зоны**.
4. Создать два **направления трафика между зонами сети** (входящий и исходящий трафик) и назначить на них созданные кастомные наборы правил.

12.1.4.1 Конфигурация зон

1. Назначение интерфейсов зоне:

```
set firewall zone <name> interface <interface>
```

где:

- **<name>** – имя зоны. Максимальная длина значения – «18» символов. Допускается использование только латинских букв (A–Z, a–z), цифр (0–9) и специальных символов: подчёркивание («_») и точка («.»). Значение должно начинаться с латинской буквы или цифры.
- **<interface>** – имя сетевого интерфейса **ARMA Стена**.

Одна зона может содержать несколько интерфейсов, но каждый интерфейс может быть назначен только одной зоне.

2. Определение локальной зоны:

```
set firewall zone <name> local-zone
```

Команда определяет зону <name> как локальную. Локальная зона не содержит интерфейсов и применяется непосредственно к системе **ARMA Стена**.

Примечание:

Добавление локальной зоны в МЭ приведёт к полной блокировке сетевого доступа к системе **ARMA Стена**. После выполнения данной операции управление устройством будет осуществляться исключительно через интерфейс командной строки (CLI) с использованием физического подключения (монитор и клавиатура). Доступ к устройству через локальную сеть будет полностью заблокирован. Для восстановления сетевого доступа необходимо применить кастомные наборы правил к локальной зоне, включающие разрешающие правила для сетевого трафика.

3. Настройка действия по умолчанию:

```
set firewall zone <name> default-action <drop | reject>
```

где **<drop | reject>** - действие по умолчанию для трафика, который не соответствует ни одному правилу. Возможно указать следующие значения:

- **drop** - пакеты отбрасываются без уведомления отправителя;
- **reject** - отправителю возвращается сообщение об ошибке.

Примечание:

По умолчанию, если на трафик между зонами не назначены правила, весь входящий в зону трафик блокируется.

4. Указать описание зоны:

```
set firewall zone <name> description <text>
```

где **<text>** - текстовое описание зоны.

12.1.4.2 Применение набора правил к зоне

Перед применением набора правил к зоне необходимо предварительно создать и настроить сами зоны.

Кастомные наборы правил применяются к трафику, перемещающемуся между зонами, и должны быть описаны с точки зрения направления: исходная зона -> целевая зона. Это означает, что правила создаются для управления потоком данных из одной зоны в другую.

Для применения кастомного набора правил к зонам необходимо ввести следующую команду:

- для IPv4:

```
set firewall zone <Destination Zone> from <Source Zone> firewall name  
<nameset>
```

- для IPv6:

```
set firewall zone <Destination Zone> from <Source Zone> firewall ipv6-  
name <nameset>
```

где:

- **<Destination Zone>** - целевая зона, куда направляется трафик;
- **<Source Zone>** - исходная зона, откуда исходит трафик;
- **<nameset>** - имя кастомного набора правил, который будет применяться к указанному направлению трафика.

Для каждой уникальной пары «Исходная зона -> Целевая зона» рекомендуется создавать отдельный набор правил. Это обеспечивает гибкость и точность настройки политик безопасности.

В качестве примера приведён список команд для разрешения доступа из локальной сети в сеть Интернет:

```
set firewall zone LAN local-zone  
set firewall zone WAN interface eth0  
set firewall ipv4 name allow rule 10 action accept  
set firewall ipv4 name allow default-action accept  
set firewall zone LAN from WAN firewall name allow  
set firewall zone WAN from LAN firewall name allow
```

где:

- **«LAN»** и **«WAN»** – имена зон;
- **«eth0»** – интерфейс с доступом к сети Интернет;
- **«allow»** – имя набора правил.

12.1.5 Мониторинг срабатывания правил

Система **ARMA Стена** позволяет отслеживать количество срабатываний правил межсетевого экрана.

Для получения сведений о количестве срабатываний каждого правила межсетевого экрана за различные временные интервалы необходимо выполнить следующую команду в эксплуатационном режиме:

```
admin@ngfwos:~$ show firewall hitcount
```

#Пример вывода информации:

```
Last update: 2025-05-12T13:20:01
```


ipv4 Firewall "forward filter"

Rule	Action	Day Hitcount	Week Hitcount	Month Hitcount
default	drop	15	149	149

ipv4 Firewall "input filter"

Rule	Action	Day Hitcount	Week Hitcount	Month Hitcount
10	accept	0	0	0
default	accept	79779	471212	471212

ipv4 Firewall "output filter"

Rule	Action	Day Hitcount	Week Hitcount	Month Hitcount
default	accept	76240	445097	445097

ipv6 Firewall "forward filter"

Rule	Action	Day Hitcount	Week Hitcount	Month Hitcount
default	drop	0	0	0

ipv6 Firewall "input filter"

Rule	Action	Day Hitcount	Week Hitcount	Month Hitcount
default	accept	3163	18787	18787

ipv6 Firewall "output filter"

Rule	Action	Day Hitcount	Week Hitcount	Month Hitcount
default	accept	1132	6720	6720

bridge Firewall "forward filter"

Rule	Action	Day Hitcount	Week Hitcount	Month Hitcount
default	drop	0	0	0

ipv4 Firewall "name test"

Rule	Action	Day Hitcount	Week Hitcount	Month Hitcount
10	accept	4	4	4
default	drop	15	149	149

Таблица сведений о количестве срабатываний каждого правила межсетевого экрана состоит из следующих столбцов:

- «**Rule**» - номер правила **МЭ**;
- «**Action**» - действие, применяемое к пакетам;
- «**Day Hitcount**» - количество срабатывания правила за сегодня;
- «**Week Hitcount**» - количество срабатывания правила за последние 7 дней;
- «**Month Hitcount**» - количество срабатывания правила за последние 30 дней.

Данные в таблице обновляются с периодичностью в 20 минут (в XX:00, XX:20, XX:40 минут). При перезагрузке системы информация о количестве срабатываний правил МЭ сохраняется.

12.1.6 Журнал межсетевого экрана

Для просмотра событий межсетевого экрана в эксплуатационном режиме необходимо выполнить следующую команду:

```
admin@ngfwos:~$ show logging firewall [| <filter>]
```

где **<filter>** - необязательный параметр фильтрации, позволяющий уточнить и обработать выводимые данные. Возможно применить следующие фильтры:

- **count** - подсчитывает количество строк, соответствующих текущему запросу, и выводит это число на экран. Позволяет быстро определить объем данных без необходимости их просмотра.
- **json** - преобразует вывод в формате JSON. Используется при интеграции с внешними системами мониторинга или автоматизации.
- **match <pattern>** - отображает только те строки, которые содержат заданный текстовый шаблон **<pattern>**. Позволяет выполнять точечный поиск событий по ключевым словам или кодам ошибок.
- **no-match <pattern>** - исключает из вывода строки, содержащие указанный текстовый шаблон **<pattern>**. Позволяет скрывать информационные сообщения или другие несущественные записи.
- **more** - активирует постраничный вывод результатов. Удобен при работе с длинными списками записей в консоли.
- **no-more** - отключает постраничный вывод, обеспечивая немедленное отображение всего результата. Используется при необходимости получить полный вывод без пауз.

- **strip-private** - производит маскировку или удаление персональных и конфиденциальных данных из записей журнала, включая IP-адреса, имена пользователей, идентификаторы сессий и другие чувствительные атрибуты. Применяется при подготовке логов для экспорта, например, в службу технической поддержки, с целью соблюдения требований к защите персональных данных.

Результат выполнения команды отображает журнал событий межсетевого экрана, структура которого представлена на [Рисунке – Логи межсетевого экрана](#).

```
admin@ngfwos:~$ show logging firewall
02.10.2025 12:00:41 1759406441620184 ngfwos kernel[0]: [ipv6-OUT-filter-default-A]IN= OUT=lo SRC=0000:0000:0000:0000:0000:0000:0000:0001 DST=0000:0000:0000:0000:0000:0000:0000:0001 LEN=343 TC=0 HOPLIMIT=64 FLOWLBL=553151 PROTO=TCP SPT=8082 DPT=41208 WINDOW=579 RES=0x00 ACK PSH URGP=0
02.10.2025 12:00:41 1759406441620279 ngfwos kernel[0]: [ipv6-OUT-filter-default-A]IN= OUT=lo SRC=0000:0000:0000:0000:0000:0000:0000:0001 DST=0000:0000:0000:0000:0000:0000:0000:0001 LEN=114 TC=0 HOPLIMIT=64 FLOWLBL=553151 PROTO=TCP SPT=8082 DPT=41208 WINDOW=579 RES=0x00 ACK PSH URGP=0
02.10.2025 12:00:41 1759406441620307 ngfwos kernel[0]: [ipv6-OUT-filter-default-A]IN= OUT=lo SRC=0000:0000:0000:0000:0000:0000:0000:0001 DST=0000:0000:0000:0000:0000:0000:0000:0001 LEN=96 TC=0 HOPLIMIT=64 FLOWLBL=553151 PROTO=TCP SPT=8082 DPT=41208 WINDOW=579 RES=0x00 ACK PSH URGP=0
02.10.2025 12:00:41 1759406441620351 ngfwos kernel[0]: [ipv6-OUT-filter-default-A]IN= OUT=lo SRC=0000:0000:0000:0000:0000:0000:0000:0001 DST=0000:0000:0000:0000:0000:0000:0000:0001 LEN=72 TC=0 HOPLIMIT=64 FLOWLBL=553151 PROTO=TCP SPT=8082 DPT=41208 WINDOW=579 RES=0x00 ACK FIN URGP=0
02.10.2025 12:00:41 1759406441620391 ngfwos kernel[0]: [ipv6-OUT-filter-default-A]IN= OUT=lo SRC=0000:0000:0000:0000:0000:0000:0000:0001 DST=0000:0000:0000:0000:0000:0000:0000:0001 LEN=72 TC=0 HOPLIMIT=64 FLOWLBL=699774 PROTO=TCP SPT=41208 DPT=8082 WINDOW=603 RES=0x00 ACK URGP=0
02.10.2025 12:00:41 1759406441622141 ngfwos kernel[0]: [ipv6-OUT-filter-default-A]IN= OUT=lo SRC=0000:0000:0000:0000:0000:0000:0000:0001 DST=0000:0000:0000:0000:0000:0000:0000:0001 LEN=96 TC=0 HOPLIMIT=64 FLOWLBL=699774 PROTO=TCP SPT=41208 DPT=8082 WINDOW=603 RES=0x00 ACK PSH URGP=0
02.10.2025 12:00:41 1759406441623136 ngfwos kernel[0]: [ipv6-OUT-filter-default-A]IN= OUT=lo SRC=0000:0000:0000:0000:0000:0000:0000:0001 DST=0000:0000:0000:0000:0000:0000:0000:0001 LEN=72 TC=0 HOPLIMIT=64 FLOWLBL=699774 PROTO=TCP SPT=41208 DPT=8082 WINDOW=603 RES=0x00 ACK FIN URGP=0
02.10.2025 12:00:41 1759406441623184 ngfwos kernel[0]: [ipv6-OUT-filter-default-A]IN= OUT=lo SRC=0000:0000:0000:0000:0000:0000:0000:0001 DST=0000:0000:0000:0000:0000:0000:0000:0001 LEN=72 TC=0 HOPLIMIT=64 FLOWLBL=553151 PROTO=TCP SPT=8082 DPT=41208 WINDOW=579 RES=0x00 ACK URGP=0
02.10.2025 12:00:41 1759406441629147 ngfwos kernel[0]: [ipv6-OUT-filter-default-A]IN= OUT=lo SRC=0000:0000:0000:0000:0000:0000:0000:0001 DST=0000:0000:0000:0000:0000:0000:0000:0001 LEN=80 TC=0 HOPLIMIT=64 FLOWLBL=520380 PROTO=TCP SPT=42146 DPT=8082 WINDOW=65476 RES=0x00 SYN URGP=0
```

Рисунок – Логи межсетевого экрана

Формат строки лога межсетевого экрана:

```
26.08.2025 09:13:04 1756199584513067 ngfwos kernel[0]: [ipv4-FWD-appctrl-
default-D]IN=eth1 OUT=eth0 MAC=... SRC=... DST=... LEN=... TOS=... PREC=... TTL=...
ID=... DF PROTO=TCP SPT=... DPT=... WINDOW=... RES=... SYN URGP=0
```

Описание полей записи лога:

1. **Временная метка события (Timestamp)** – дата и время регистрации сетевого пакета в системе. Формат: ДД.ММ.ГГГГ ЧЧ:ММ:СС. Пример: «26.08.2025 09:13:04».
2. **Идентификатор события (Event ID)** – уникальный числовой идентификатор записи в журнале, присваиваемый системой для однозначной идентификации события. Пример: «1756199584513067».
3. **Источник события (Source)** – имя устройства и компонента, сгенерировавшего запись. Поле содержит наименование устройства и идентификатор процесса ядра. Пример: «ngfwos kernel[0]».
4. **Цепочка правил (Rule Chain)** – имя цепочки правил межсетевого экрана, в которой было обработано событие, а также действие, применённое к пакету. Отражает путь пакета через систему фильтрации. Пример: [ipv4-FWD-appctrl-default-D], где:
 - ipv4 – семейство протоколов сетевого уровня. Указывает, что правило применяется к трафику IPv4.
 - FWD – направление обработки пакета. Обозначает цепочку forward («транзит»), то есть пакет проходит через устройство и не предназначен ему самому.

- `arpctrl` – модуль или функциональный компонент, обрабатывающий пакет. В данном случае – подсистема Application Control (контроль приложений).
 - `default` – указывает, что применено правило из стандартного («по умолчанию») набора политики Application Control.
 - `D` – действие, применённое к пакету. `D (Drop)` – пакет отброшен (заблокирован).
5. **Входной интерфейс (IN)** – интерфейс сетевого взаимодействия, через который пакет поступил в устройство. Пример: `IN=eth1`.
 6. **Выходной интерфейс (OUT)** – интерфейс, через который пакет был передан далее по маршруту. Пример: `OUT=eth0`.
 7. **MAC-адреса (MAC)** – аппаратные адреса участников коммуникации и тип Ethernet-кадра. Первые 6 байт – MAC-адрес источника, следующие 6 байт – MAC-адрес назначения. Пример: `MAC=00:50:56:bd:a0:36:00:50:56:bd:16:96:08:00`.
 8. **IP-адрес источника (SRC)** – IP-адрес отправителя пакета. Пример: `SRC=192.168.1.21`.
 9. **IP-адрес назначения (DST)** – IP-адрес получателя пакета. Пример: `DST=77.88.44.242`.
 10. **Длина пакета (LEN)** – общая длина IP-пакета в байтах, включая заголовки и полезную нагрузку. Пример: `LEN=60`.
 11. **Тип сервиса (TOS)** – значение поля Type of Service из заголовка IPv4, определяющее параметры качества обслуживания (QoS). Пример: `TOS=0x00`.
 12. **Приоритет (PREC)** – поле Precedence заголовка IPv4, указывающее приоритет пакета. Пример: `PREC=0x00`.
 13. **Время жизни (TTL)** – значение Time To Live, ограничивающее количество маршрутизаторов (хопов), которые может пройти пакет. При достижении нуля пакет отбрасывается. Пример: `TTL=63`.
 14. **Идентификатор пакета (ID)** – уникальный идентификатор IP-пакета, используемый при фрагментации и сборке. Пример: `ID=10888`.
 15. **Флаг «Don't Fragment» (DF)** – флаг, запрещающий фрагментацию пакета при передаче через сети с меньшим MTU. Пример: `DF`.
 16. **Транспортный протокол (PROTO)** – протокол транспортного уровня, используемый в пакете. Пример: `PROTO=TCP`.
 17. **Исходный порт (SPT)** – номер порта источника в транспортном протоколе. Пример: `SPT=43442`.

18. **Порт назначения (DPT)** – номер порта получателя. Значение 443 соответствует HTTPS. Пример: *DPT=443*.
19. **Размер окна TCP (WINDOW)** – размер приёмного окна TCP в байтах, определяющий объём данных, который может быть принят без подтверждения. Пример: *WINDOW=64240*.
20. **Зарезервированные биты (RES)** – зарезервированное поле в заголовке TCP. Значение 0x00 указывает на отсутствие специальных флагов. Пример: *RES=0x00*.
21. **Флаг TCP (SYN)** – флаг синхронизации соединения. Указание на начало установления TCP-сессии. Пример: *SYN*.
22. **Указатель срочности (URGP)** – поле Urgent Pointer в заголовке TCP. Значение 0 означает, что срочные данные отсутствуют. Пример: *URGP=0*.

Дополнительный параметр «timestamp» («show logging firewall timestamp») предназначен исключительно для служебного использования и применяется для передачи событий межсетевого экрана в веб-интерфейс системы. Данный режим обеспечивает пакетную выдачу логических записей с корректными временными метками, необходимыми для отображения и обработки в графической подсистеме. Использование параметра «timestamp» в командной строке (CLI) не предусмотрено и не рекомендуется.

12.2 NAT

Трансляция сетевых адресов, сокращённо NAT – это технология преобразования IP-адресов внутренней сети «LAN» в IP-адреса внешней сети «WAN».

NAT настраивается посредством создания правил. Правила NAT нумеруются и исполняются в соответствующем порядке. Следует учесть, что в настроенном правиле NAT номер является неизменяемым идентификатором. Для изменения номера правила NAT следует удалить правило и создать его заново с новым номером.

В связи с этим рекомендуется присваивать правилам NAT номера, оставляя между ними незаполненные промежутки. Например, можно сформировать набор правил NAT с номерами 10, 20, 30 и 40. Такой подход обеспечит возможность добавления дополнительного правила в определённую позицию последовательности без необходимости удаления существующих правил.

Для просмотра конфигурации NAT необходимо в режиме конфигурирования ввести команду «**show nat**».

12.2.1 Правила NAT

ARMA Стена поддерживает создание правил NAT следующих типов **<typeNAT>**: «**source**», «**destination**».

При создании правил NAT возможно применять следующие атрибуты:

1. **«outbound-interface»** – применяется только для трансляции адреса отправителя. Позволяет указывать интерфейс, используемый для исходящего внешнего трафика, к которому должны применяться правила NAT:

```
set nat source rule <num> outbound-interface name <iname>
```

где:

- **<num>** – номер приоритета правила. Возможно указать значение в диапазоне от «1» до «999999».
- **<iname>** – имя интерфейса.

Поддерживается указание групп интерфейсов:

```
set nat source rule <num> outbound-interface group <grname>
```

где **<grname>** – имя группы интерфейсов.

Поддерживается указание имени интерфейса или группы интерфейсов с использованием знака «!» для инверсии или подстановочного символа «*», например:

- **«!eth0»** – интерфейсы кроме «eth0»;
- **«eth2*»** – интерфейсы, с именами начинающимися на «eth2».

2. **«inbound-interface»** – применяется только для трансляции адреса получателя. Позволяет указывать входящий интерфейс для трафика, к которому должны применяться правила NAT:

```
set nat destination rule <num> inbound-interface name <iname>
```

Поддерживается указание групп интерфейсов:

```
set nat destination rule <num> inbound-interface group <grname>
```

где **<grname>** – имя группы интерфейсов.

Поддерживается указание имени интерфейса или группы интерфейсов с использованием знака «!» для инверсии или подстановочного символа «*».

3. **«protocol»** – позволяет указывать протоколы передачи трафика, к которому должны применяться правила NAT:

```
set nat <typeNAT> rule <num> protocol [<protocolname> | tcp_udp | all |  
<number>]
```

где:

- **<typeNAT>** – тип NAT;
- **<protocolname>** – протокол, определённый в «/etc/protocols»;

- **«tcp_udp»** – протоколы TCP и UDP;
- **«all»** – все протоколы;
- **<number>** – номер протокола. Возможно указание значения в диапазоне от «0» до «255».

По умолчанию правило относится ко всем протоколам.

4. **«source»** – позволяет указывать адрес и порт источника трафика, к которому должны применяться правила NAT:

```
set nat <typeNAT> rule <num> source address [<IPv4-address> | <addressrange>]  
set nat <typeNAT> rule <num> source port [<portnumber> | <portname> |  
<rangenumbers>]
```

где:

- **<IPv4-address>** – IPv4-адрес. Возможно указание в следующих форматах: <x.x.x.x> и <x.x.x.x/x>;
- **<addressrange>** – диапазон адресов, разделённых знаком «-». Возможно указание в формате <x.x.x.x>-<x.x.x.x>;
- **<portnumber>** – номер порта источника. Возможно указание значения в диапазоне от «1» до «65535»;
- **<portname>** – имя, определённое в «/etc/services»;
- **<rangenumbers>** – диапазон портов, разделённых знаком «-».

Примечание:

Поддерживается указание нескольких значений портов, разделённых знаком «,», например:

```
set nat <typeNAT> rule <num> source port http,1100-1200,25
```

5. **«destination»** – позволяет указывать адрес и порт получателя трафика, к которому должны применяться правила NAT:

```
set nat <typeNAT> rule <num> destination address <x.x.x.x>  
set nat <typeNAT> rule <num> destination port [<portnumber> | <portname> |  
<rangenumbers>]
```

По умолчанию, если адрес и порт получателя трафика не указаны, правило NAT будет применяться к любому адресу и порту.

6. **«translation»** – позволяет указывать адрес и порт, используемые при замене адресной информации в пакете:

```
set nat source rule <num> translation address [masquerade | <IPv4-address> |  
<addressrange>]  
set nat destination rule <num> translation address [<IPv4-address> |  
<addressrange>]  
set nat destination rule <num> translation port [<number> | <rangenumbers>]  
set nat destination rule <num> translation redirect port [<portnumber> |  
<rangenumbers>]
```

где:

- «**masquerade**» – NAT по основному адресу «**outbound-interface**». Поддерживается указание только для типа «**source**»;
- **<IPv4-address>** – IPv4-адрес. Возможно указание в следующих форматах: <x.x.x.x> и <x.x.x.x/x>;
- **<addressrange>** – диапазон адресов, разделённых знаком «-». Возможно указание в формате <x.x.x.x>-<x.x.x.x>;
- **<portnumber>** – порт для перенаправления на локальный хост;
- **<number>** – номер порта. Возможно указать значение в диапазоне от «1» до «65535»;
- **<rangenumbers>** – диапазон портов, разделённых знаком «-».

Для включения логирования правила NAT необходимо ввести следующую команду:

```
set nat <typeNAT> rule <num> log
```

12.2.1.1 Копирование правила NAT

Для копирования правила NAT необходимо ввести следующие команды:

```
[edit]  
admin@ngfwos# edit nat <typeNAT>  
[edit nat <typeNAT>]  
admin@ngfwos# copy rule <num1> to rule <num2>
```

где:

- **<num1>** – идентификатор оригинального правила;
- **<num2>** – идентификатор создаваемой копии правила.

12.2.1.2 Переименование правила NAT

Для переименования правила NAT необходимо ввести следующие команды:


```
[edit]
admin@ngfwos# edit nat <typeNAT>
[edit nat <typeNAT>]
admin@ngfwos# rename rule <num1> to rule <num2>
```

где:

- **<num1>** – изначальный идентификатор правила;
- **<num2>** – идентификатор переименованного правила.

Для автоматической перенумерации правил в эксплуатационном режиме следует выполнить команду:

```
admin@ngfwos:~$ generate <nat | nat64 | nat66> rule-resequence
```

При выполнении команды происходит перенумерация правил с шагом 10, начиная с номера 100.

12.2.2 Примеры создания правил NAT

12.2.2.1 Преобразование адреса источника

В качестве примера приведён список команд для создания правила NAT, преобразующего адрес источника:

```
set nat source rule 11 outbound-interface name eth0
set nat source rule 11 source address 192.168.43.0/24
set nat source rule 11 translation address masquerade
```

где:

- **«eth0»** – интерфейс с доступом к сети Интернет;
- **«192.168.43.0/24»** – адрес сети LAN в формате CIDR.

12.2.2.2 Переадресация портов

В качестве примера приведён список команд для создания правила NAT, которое перенаправляет HTTP-трафик по протоколу «TCP» с порта «8080» интерфейса «eth0» на порт «80» внутреннего веб-сервера с IP-адресом «192.168.3.112»:

```
set nat destination rule 21 description 'Port Forward: HTTP to 192.168.3.112'
set nat destination rule 21 destination port 8080
set nat destination rule 21 inbound-interface name eth0
set nat destination rule 21 protocol tcp
set nat destination rule 21 translation port 80
set nat destination rule 21 translation address 192.168.3.112
```

12.2.2.3 Один-к-одному

Статический NAT «Один-к-одному» сопоставляет один внешний IP-адрес, в большинстве случаев общедоступный, с одним внутренним IP-адресом, в большинстве случаев частным.

В качестве примера приведён **ARMA Стена**, сетевые интерфейсы которого настроены следующим образом:

```
[edit]
admin@ngfwos# show interfaces
  ethernet eth0 {
    address 203.0.113.87/24
    description WAN
    hw-id 00:50:56:bd:ca:9e
  }
  ethernet eth1 {
    address 192.168.2.1/24
    description LAN
    hw-id 00:50:56:bd:f5:cd
  }
  loopback lo {
  }
```

Для создания правила NAT «один-к-одному» следует ввести следующие команды:

```
set nat static rule 10 destination address '203.0.113.87'
set nat static rule 10 inbound-interface 'eth0'
set nat static rule 10 translation address '192.168.2.11' # IP-адрес ПК пользователя.
```

13 COB (IDS/IPS)

Функциональность системы обнаружения и предотвращения вторжений (**COB**) в **ARMA Стена** реализуется посредством ПО с открытым исходным кодом «Suricata» и использованием метода захвата пакетов «Netmap» для повышения производительности и минимизации загрузки ЦП.

Система обнаружения и предотвращения вторжений в **ARMA Стена** позволяет решать следующие задачи:

- обнаружение и предотвращение использования эксплойтов и уязвимостей сетевых приложений;
- обнаружение и предотвращение эксплуатации уязвимостей в поддерживаемых протоколах;
- обнаружение и предотвращение сетевого сканирования;
- обнаружение и фильтрация трафика от скомпрометированных хостов;
- обнаружение и фильтрация трафика от хостов, заражённых троянским ПО и сетевыми червями;
- обнаружение и предотвращение DOS-атак.

Suricata использует многоуровневую архитектуру анализа сетевого трафика, в которой каждый уровень отвечает за обработку определённого типа протоколов:

- **L2**-парсеры обрабатывают канальный уровень (Ethernet, VLAN и др.), извлекая MAC-адреса и метки тегов.
- **IP**-парсеры анализируют заголовки IPv4/IPv6, восстанавливают фрагменты и определяют протоколы транспортного уровня.
- **App-layer** парсеры выполняют глубокий разбор прикладных протоколов (HTTP, DNS, TLS и др.), извлекают метаданные, реконструируют сессии и обеспечивают обнаружение угроз внутри приложений.

Совместная работа этих уровней обеспечивает сквозную видимость сетевого трафика и эффективное выявление сетевых аномалий и угроз.

13.1 Включение IDS/IPS

Для корректной работы системы **IDS/IPS** необходимо выполнить следующие минимальные настройки **Suricata**:

1. Указать интерфейс, на котором будет включён захват пакетов с помощью NETMAP:

```
set suricata netmap interface <iname>
```

где **<iname>** - имя интерфейса система **ARMA Стена**, на котором будет включён захват пакетов с помощью NETMAP.

2. Определить режим захвата трафика:

- для определённого интерфейса системы **ARMA Стена**:

```
set suricata netmap interface <iname> copy-mode <ips | tap>
```

- по умолчанию для сетевых интерфейсов, на которых режим не задан в явном виде, но активирована служба **Suricata**:

```
set suricata netmap parameters copy-mode <ips | tap>
```

где **<ips | tap>** - режим захвата трафика. Возможно указать следующие значения:

- **ips** - режим сетевой безопасности, обеспечивающий активный мониторинг и предотвращение подозрительной активности путём модификации, блокировки или отбрасывания трафика в реальном времени на основе правил безопасности;
- **tap (ids)** - режим пассивного мониторинга сетевого трафика, направленный на обнаружение подозрительной активности и генерацию оповещений при совпадении с заданными правилами безопасности, без вмешательства в проходящий трафик.

Примечание:

Необходимо явно установить режим захвата трафика по умолчанию либо указать данный параметр для конкретного интерфейса, на котором будет активирована Suricata. В случае отсутствия указанных настроек, сетевой интерфейс, используемый для работы со службой **Suricata**, будет исключён из обработки стандартного сетевого стека. Это может привести к потере возможности выполнения базовых сетевых операций, включая передачу данных и управление системой через протокол SSH, при условии, что данный интерфейс задействован для этих целей. Подобное поведение обусловлено особенностью технологии NetMap, которая блокирует сетевой интерфейс для всех внешних процессов и операций, включая сетевые подключения.

3. Указать файл с правилами, которые будут использоваться в Suricata:

```
set suricata rule-files file-name /config/files/configuration/suricata/rule-files/*.rules
```

Система **Suricata** загрузит и будет использовать все правила, которые найдёт в файлах с расширением «**rules**», расположенных в каталоге «**/config/files/configuration/suricata/rule-files/**». Данный каталог используется системой по умолчанию.

После выполнения минимальных настроек **Suricata** для запуска **COB**, необходимо ввести следующую команду в режиме конфигурации:

```
set suricata enable yes
```

Зафиксировать изменения с помощью ввода команд «**commit**» и «**save**».

Для просмотра статуса **COB** необходимо ввести следующую команду в эксплуатационном режиме под УЗ «**admin**»:

```
admin@ngfwos:~$ sudo systemctl status suricata
```

#Пример выводимой информации:

- suricata.service - Suricata Service

Loaded: loaded (/lib/systemd/system/suricata.service; disabled; preset: enabled)

Active: active (running) since Mon 2025-03-03 10:05:45 UTC; 21h ago

Main PID: 2596 (Suricata-Main)

Tasks: 12 (limit: 4668)

Memory: 1.5G

CPU: 13min 54.448s

CGroup: /system.slice/suricata.service

└─2596 /bin/suricata -c /etc/suricata/suricata.yaml --pidfile /var/run/suricata.pid --netmap

Mar 03 15:24:51 ngfwos idps-rule[2596]: [Alert] [1:19559:16] INDICATOR-SCAN SSH brute force login attempt [Classification: Misc activ>

Mar 04 07:14:04 ngfwos idps-rule[2596]: [Alert] [1:3701703:0] ARMA SSH INIT SESSION Key exchange [Classification: (null)] [Priority: >

Mar 04 07:14:16 ngfwos idps-rule[2596]: [Alert] [1:3701704:0] ARMA End of SSH session flag FIN [Classification: (null)] [Priority: 3]>

Mar 04 07:14:17 ngfwos idps-rule[2596]: [Alert] [1:19559:16] INDICATOR-SCAN SSH brute force login attempt [Classification: Misc activ>

Mar 04 07:14:22 ngfwos idps-rule[2596]: [Alert] [1:19559:16] INDICATOR-SCAN SSH brute force login attempt [Classification: Misc activ>

Mar 04 07:14:22 ngfwos idps-rule[2596]: [Alert] [1:19559:16] INDICATOR-SCAN SSH brute force login attempt [Classification: Misc activ>

Mar 04 07:14:23 ngfwos idps-rule[2596]: [Alert] [1:19559:16] INDICATOR-SCAN SSH brute force login attempt [Classification: Misc activ>

```
Mar 04 07:14:23 ngfwos idps-rule[2596]: [Alert] [1:33654:6] SERVER-OTHER OpenSSH  
maxstartup threshold potential connection exhaustion>  
Mar 04 07:14:23 ngfwos idps-rule[2596]: [Alert] [1:19559:16] INDICATOR-SCAN SSH  
brute force login attempt [Classification: Misc activ>  
lines 1-20/20 (END)
```

Для выхода из режима просмотра необходимо нажать комбинацию клавиш «**Ctrl**» + «**C**».

Для получения статистики по загруженным правилам **Suricata**, включая количество активных, сбойных и пропущенных правил, в эксплуатационном режиме системы выполняется команда:

```
admin@ngfwos:~$ show idps ruleset-stats [json]  
  
Rules loaded: 61118  
Rules failed: 171  
Rules skipped: 0
```

Необязательный параметр «json» позволяет представить статистику в формате JSON.

Для просмотра статистики о деятельности и производительности системы **IDS/IPS** необходимо ввести следующую команду:

```
admin@ngfwos:~$ show idps stats [json]  
uptime: 326146  
ips:  
accepted: 439057  
blocked: 0  
rejected: 0  
replaced: 0  
drop_reason:  
    decode_error: 0  
    defrag_error: 0  
    defrag_memcap: 0  
    flow_memcap: 0
```

Необязательный параметр «json» обеспечивает вывод статистики в формате JSON.

Примечание:

Отображение статистики возможно только при условии, что в конфигурации системы включён сбор статистических данных. Для этого должно быть установлено значение: «**set suricata stats enabled yes**».

После включения параметра требуется некоторое время для накопления начальных данных, прежде чем статистика станет доступной для отображения.

Корректная перезагрузка сервиса COB выполняется в строгом соответствии со следующей последовательностью команд:

```
set suricata enable no
commit

set suricata enable yes
commit
save
```

13.1.1 Примеры настройки включения COB

Включение COB на физическом интерфейсе eth0:

```
set suricata netmap interface eth0
set suricata netmap parameters copy-mode ips
set suricata rule-files file-name /config/files/configuration/suricata/rule-
files/suricata.rules
set suricata enable yes
commit
save
```

При активации **Suricata** в режиме netmap на физическом интерфейсе **eth0** обработка трафика через **VLAN-интерфейсы** (например, **eth0.100**) становится невозможной. Трафик, направляемый через такие VLAN-интерфейсы, не будет проходить, поскольку netmap захватывает поток пакетов на уровне физического интерфейса, и кадры с VLAN-тегами могут не доставляться до стека, либо не обрабатываться корректно в контексте VLAN-интерфейсов.

Включение COB на VLAN-интерфейсе eth0.100:

```
set suricata netmap interface eth0.100
set suricata netmap parameters copy-mode ips
set suricata rule-files file-name /config/files/configuration/suricata/rule-
files/suricata.rules
set suricata enable yes
commit
save
```

В данной конфигурации **Suricata** осуществляет детектирование трафика исключительно на VLAN-интерфейсе **eth0.100**. Пакеты, проходящие через физический интерфейс **eth0**, при этом не блокируются и продолжают

обрабатываться сетевым стеком в штатном режиме, однако не подвергаются анализу со стороны **Suricata**.

Включение COB на интерфейсах **eth0** и **eth0.100**:

```
set suricata netmap interface eth0
set suricata netmap interface eth0.100
set suricata netmap parameters copy-mode ips
set suricata rule-files file-name /config/files/configuration/suricata/rule-
files/suricata.rules
set suricata enable yes
commit
save
```

В данной конфигурации детектирование трафика осуществляется только на физическом интерфейсе **eth0**. Трафик, проходящий через VLAN-интерфейс **eth0.100**, не будет обрабатываться, несмотря на его указание в конфигурации **Suricata**, и фактически блокируется на уровне обработки пакетов.

Для обеспечения детектирования трафика как на физическом интерфейсе **eth0**, так и на VLAN-интерфейсе **eth0.100**, требуется отключить аппаратное ускорение обработки VLAN-тегов (rxvlan и txvlan) на физическом интерфейсе перед активацией **Suricata**. Для отключения аппаратного ускорения необходимо ввести следующие команды от имени **УЗ «admin»**:

```
admin@ngfwos:~$ sudo -i
root@ngfwos:~# ethtool --offload eth0 rxvlan off txvlan off
root@ngfwos:~# exit
admin@ngfwos:~$
```

Примечание:

Изменение параметров **offload** необходимо выполнять до включения **Suricata**, так как настройки netmap применяются на этапе инициализации драйвера.

После выполнения данной команды аппаратная фильтрация и обработка VLAN-тегов на интерфейсе **eth0** будет отключена, что позволит драйверу сетевого интерфейса и приложению **Suricata** получать полный трафик, включая кадры с VLAN-метками, через механизм netmap. В этом случае **Suricata** сможет корректно обрабатывать трафик на обоих интерфейсах – **eth0** и **eth0.100**.

Включение COB на агрегированном интерфейсе **bond1**:


```
set suricata netmap interface bond1
set suricata netmap parameters copy-mode ips
set suricata rule-files file-name /config/files/configuration/suricata/rule-
files/suricata.rules
set suricata enable yes
commit
save
```

При активации **Suricata** в режиме netmap на агрегированном интерфейсе **bond1** захват трафика осуществляется на уровне интерфейса bond, что исключает возможность корректной обработки VLAN-интерфейсов, ассоциированных с **bond1** (например, **bond1.100**). Трафик на VLAN-интерфейсах блокируется.

Включение COB на VLAN-подинтерфейсе bond1.200:

```
set suricata netmap interface bond1.200
set suricata netmap parameters copy-mode ips
set suricata rule-files file-name /config/files/configuration/suricata/rule-
files/suricata.rules
set suricata enable yes
commit
save
```

Suricata в данном режиме анализирует трафик только на VLAN-интерфейсе **bond1.200**. Трафик, проходящий через интерфейс **bond1**, не перехватывается и обрабатывается стандартным сетевым стеком.

Включение COB на интерфейсах bond1 и bond1.200:

1. Конфигурация агрегированного интерфейса **bond1**:

```
# Создание агрегированного интерфейса «bond1» с методом хеширования
«layer2+3»:
set interfaces bonding bond1 hash-policy 'layer2+3'

# Включение сетевых интерфейсов «eth2» и «eth3» в состав интерфейса
«bond1»:
set interfaces bonding bond1 member interface 'eth2'
set interfaces bonding bond1 member interface 'eth3'

# Создание интерфейса VLAN на агрегированном интерфейсе и назначение
ему IP-адрес:
set interfaces bonding bond1 vif 200 address '10.23.5.250/29'
```

2. Отключение аппаратного ускорения VLAN-обработки на физических интерфейсах.

Необходимо отключить аппаратное ускорение приёма/передачи VLAN-тегов на физических интерфейсах «**eth2**» и «**eth3**», входящих в интерфейс «**bond1**». Это обеспечит корректную обработку VLAN-маркированного трафика на уровне ядра.

Для отключения аппаратного ускорения необходимо ввести следующие команды от имени **УЗ «admin»**:

```
admin@ngfwos:~$ sudo -i
root@ngfwos:~# ethtool --offload eth2 rxvlan off txvlan off
root@ngfwos:~# ethtool --offload eth3 rxvlan off txvlan off
root@ngfwos:~# exit
admin@ngfwos:~$
```

3. Конфигурация **Suricata**:

```
set suricata netmap interface eth2
set suricata netmap interface eth3
set suricata netmap parameters checksum-checks 'no'
set suricata netmap parameters copy-mode 'ips'
set suricata rule-files file-name /config/files/configuration/suricata/rule-
files/suricata.rules
set suricata enable 'yes'
```

Примечание:

Если указать интерфейсы **bond1** и **bond1.200**:

```
set suricata netmap interface bond1
set suricata netmap interface bond1.200
```

то обработка и детектирование трафика осуществляются исключительно на интерфейсе «**bond1**». Трафик, поступающий через интерфейс «**bond1.200**», будет заблокирован, несмотря на наличие конфигурационной команды «set suricata netmap interface bond1.200».

13.2 Правила Suricata

Система **Suricata** имеет две директории конфигурации: *активная* и *рабочая*.

Рабочая директория - содержит рабочую конфигурацию **Suricata**, которая в данный момент редактируется. Здесь отображаются все правила, созданные пользователем в интерфейсе командной строки (**CLI**). К этим правилам возможно применять команды редактирования: добавлять правила, изменять действия правил, активировать и деактивировать правила, удалять правила или файлы с правилами.

Изменения, внесённые в рабочую конфигурацию, не вступают в силу до тех пор, пока они не будут зафиксированы командой «**suricata commit-rules**». В этот момент рабочая конфигурация становится активной конфигурацией.

Активная директория - содержит активную конфигурацию **Suricata**, которая в данный момент загружена и используется. Команда «**suricata save-rules**» сохраняет активную конфигурацию в файл для последующего использования.

Для просмотра всех правил, прописанных в рабочей или активной директории **Suricata**, необходимо ввести команду:

```
admin@ngfwos:~$ suricata show-rules directory <active | working>

SIDS
/config/files/configuration/suricata/rule-files/suricata.rules
1337
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"HTTP GET Request
Containing Rule in URI"; flow:established,to_server; http.method;
content:"GET"; http.uri; content:"rule"; fast_pattern; classtype:bad-unknown; rev:1;)
IDS

admin@ngfwos:~$
```

где **<active | working>** - выбор директории расположения правил. Возможно указать следующие значения:

- **active** - все правила в активной директории **Suricata**;
- **working** - все правила в рабочей директории **Suricata**.

Для просмотра списка всех файлов с правилами **Suricata**, расположенных в каталоге по умолчанию (default-rule-path), необходимо ввести в эксплуатационном режиме следующую команду:

```
admin@ngfwos:~$ suricata show-list-rules

# Пример вывода списка файлов с правилами:
/config/files/configuration/suricata/rule-files/.gitkeep
/config/files/configuration/suricata/rule-files/3coresec.rules
/config/files/configuration/suricata/rule-files/AGENT_TESLA.rules
/config/files/configuration/suricata/rule-files/APT31_IP.rules
/config/files/configuration/suricata/rule-files/ASYNCRAT.rules
/config/files/configuration/suricata/rule-files/AZORULT.rules
/config/files/configuration/suricata/rule-files/AdobeCommerce_XMLi_CE.rules
/config/files/configuration/suricata/rule-files/ApacheHGS_Bypass.rules
/config/files/configuration/suricata/rule-files/ApacheNiFi_RCE.rules
```

```
/config/files/configuration/suricata/rule-files/ApacheStruts_RCE.rules
/config/files/configuration/suricata/rule-files/ApacheTC_SQLi.rules
/config/files/configuration/suricata/rule-files/ApacheTomCat_RCE.rules
/config/files/configuration/suricata/rule-
files/Apache_ActiveMQ_SourceCodeDisclosure.rules
...
/config/files/configuration/suricata/rule-files/worm.rules
/config/files/configuration/suricata/rule-files/xfreerdp.rules

admin@ngfwos:~$
```

13.2.1 Создание правила Suricata

Для создания правила **Suricata** с помощью командной строки необходимо выполнить следующие действия:

1. Ввести в режиме эксплуатации команду «**suricata add-rules file-path**», указав необходимые параметры для создаваемого правила. Например:

```
admin@ngfwos:~$ suricata add-rules file-path
/config/files/configuration/suricata/rule-files/test.rules sid 1337
      text 'alert http $HOME_NET any -> $EXTERNAL_NET any
      (msg:"HTTP GET Request Containing Rule in URI";
flow:established,to_server;
      http.method; content:"GET"; http.uri; content:"rule"; fast_pattern;
      classtype:bad-unknown; rev:1;)'

Success: Rules added. #Уведомление об успешном добавлении правила.
admin@ngfwos:~$
```

Примечание:

Допускается не указывать **sid**, система автоматически присвоит следующий доступный идентификатор.

В случае возникновения необходимости в отмене введенного правила, применяется следующая команда:

```
admin@ngfwos:~$ suricata reset-changes
```

Данная команда удаляет все правила, которые были добавлены в систему командой «**suricata add-rules**», но не были зафиксированы командой «**suricata commit-rules**».

2. Зафиксировать изменения с помощью ввода команд:

```
admin@ngfwos:~$ suricata commit-rules
Success: Rules successfully committed in active database.

admin@ngfwos:~$ suricata save-rules
Success: All rules saved successfully in /config/files/configuration/suricata/rule-
files/test.rules.

admin@ngfwos:~$
```

Если в каталоге «/config/files/configuration/suricata/rule-files/» отсутствует файл с именем «test.rules», то такой файл будет создан, и в него будет добавлено создаваемое правило.

3. Добавить новый файл правил в активный список файлов с правилами, используемых **Suricata** для анализа сетевого трафика, введя следующую команду в конфигурационном режиме:

```
set suricata rule-files file-name /config/files/configuration/suricata/rule-
files/test.rules
```

4. Для применения нового правила **Suricata** необходимо ввести команду:

```
admin@ngfwos:~$ suricata apply-rules

Success: Rules apply
admin@ngfwos:~$
```

Данная команда посылает сигнал SIGUSR2 в **Suricata**. В системе **Suricata** сигнал SIGUSR2 используется для перезагрузки правил без необходимости полного перезапуска приложения. При получении этого сигнала **Suricata** перечитывает файл правил и применяет их, не прерывая работу. Таким образом, правила безопасности обновляются без нарушения текущего мониторинга сетевой активности.

Примечание:

При выполнении команды «**suricata apply-rules**» существует вероятность неполного применения правил системы **Suricata** к процессу активной фильтрации сетевого трафика в момент перезапуска правил.

После создания правила включается регистрация событий, связанных с этим правилом. Эти события возможно просмотреть в глобальном журнале.

Переменные в правилах COB

В системе **ARMA Стена** реализована поддержка переменных при настройке правил **COB**, на основе **Suricata**. Данный механизм обеспечивает гибкость при

определении сетевых диапазонов, к которым применяются правила, и исключает необходимость дублирования IP-адресов в каждом отдельном правиле. Это способствует унификации конфигурации, повышению эффективности фильтрации трафика и упрощению администрирования политик безопасности.

Переменные используются в правилах **Suricata** для обозначения источников, получателей и зон анализа сетевой активности – таких как внутренние сети организации и внешние хосты. Применение переменных позволяет ограничить область действия правил заданными сетевыми сегментами, что снижает нагрузку на систему и повышает производительность обработки трафика.

На текущий момент в **ARMA Стена** поддерживаются следующие переменные:

- **HOME_NET** – определяет доверенную внутреннюю сеть организации. Правила, ссылающиеся на данную переменную, применяются исключительно к сетевому трафику, источник или назначение которого принадлежит указанным подсетям.
- **EXTERNAL_NET** – задаёт внешние сети, находящиеся за пределами доверенной зоны. Используется для описания внешних хостов и адресов, не входящих в состав **HOME_NET**.

Для изменения значений переменных необходимо выполнить соответствующие команды в конфигурационном режиме:

```
set suricata vars address-groups home_net address <home_net_address>  
set suricata vars address-groups external_net address <external_net_address>
```

где:

- **<home_net_address>** – список IPv4-адресов и сетей в формате CIDR, разделённых запятыми. Поддерживаются также специальные символы и выражения. Для задания значений переменных разрешены: цифры (0–9), буквы латинского алфавита (a–z, A–Z), специальные символы «/», «\$», «!», «,», «.». Значение по умолчанию «192.168.0.0/16,10.0.0.0/8,172.16.0.0/12».
- **<external_net_address>** – внешние сети. Поддерживаются те же символы, что и для **HOME_NET**. Значение по умолчанию «!\$HOME_NET» – все IP-адреса, кроме тех, что входят в **HOME_NET**.

13.2.2 Создание правила IDS/IPS для фильтрации L7 по протоколу

ARMA Стена позволяет выполнять фильтрацию трафика по протоколу с помощью правил **IDS/IPS**, в состав которых могут входить фильтры по содержимому «content», регулярные выражения «pcre» и значения «app-layer-protocol».

13.2.2.1 Фильтр по содержимому

Фильтр по содержимому «content» в правило **IDS/IPS** необходимо добавлять в следующем формате:

- «content:"[example]";»

где «"[example]"» – сопоставляемое значение.

Возможно добавление нескольких фильтров в одно правило.

В качестве примера приведено правило, предназначенное для фильтрации трафика, направленного по протоколу HTTP:

- **alert http any any -> any any (flow:to_server; http.protocol; content:"HTTP/1.0"; sid:9876654321;)**

где «content:"HTTP/1.0"» – фильтр.

По умолчанию сравнение с шаблоном производится с учётом регистра.

Дополнительные сведения о применении в правилах фильтрации по содержанию представлены на официальном сайте ПО «Suricata» (см. <https://docs.suricata.io/en/suricata-7.0.10/rules/payload-keywords.html#content>).

13.2.2.2 Регулярные выражения

Для фильтрации трафика возможно использование правил **IDS/IPS** с регулярными выражениями «pcre» в следующем формате:

- «pcre:"/[regex]/opts";»

где:

- «[regex]» – шаблон;
- «opts» – модификатор.

Поддерживается добавление нескольких регулярных выражений в одно правило.

В качестве примера приведено правило, предназначенное для обнаружения возможного использования скриптов Powershell с расширением «.ps1» по протоколу SMB:

- **alert smb any any -> \$HOME_NET 445 (msg:"ET POLICY Possible Powershell .ps1 Script Use Over SMB"; flow:established,to_server; pcre:"/SMB/"; depth:8; pcre:"/.ps1/"; nocase; distance:0; classtype:bad-unknown; rev:2; metadata:created_at 2019_04_16, updated_at 2019_04_16;)**

где «pcre:"/SMB/"» и «pcre:"/.ps1/"» – регулярные выражения.

Примечание:

Применение правила **IDS/IPS**, содержащего сложное регулярное выражение «pcre», может негативно влиять на производительность системы.

Дополнительные сведения о применении регулярных выражений в правилах представлены на официальном сайте ПО «Suricata» (см. <https://docs.suricata.io/en/suricata-7.0.10/rules/payload-keywords.html#pcre-perl-compatible-regular-expressions>).

13.2.2.3 Указание протокола прикладного уровня

Указывать протокол прикладного уровня в правилах **IDS/IPS** необходимо в следующем формате:

- «app-layer-protocol:<protocolname>;»

где **<protocolname>** – протокол прикладного уровня.

Для просмотра списка поддерживаемых протоколов прикладного уровня необходимо в режиме эксплуатации ввести следующую команду:

```
admin@ngfwos:~$ sudo suricata --list-app-layer-protos
```

В качестве примера приведено правило, предназначенное для определения трафика, направленного по протоколу SSH через нестандартный порт:

- **alert tcp any any -> any ![22,830] (msg:"PAW - Suspicious SSH traffic on unusual SSH port"; flow:to_server, stateless; app-layer-protocol:ssh; threshold: type limit, track by_src, seconds 60, count 1; reference: url,https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers; metadata:created_at 2022_02_11, updated_at 2022_06_15; sid:9876544321; rev:5; classtype:policy-violation;)**

где «ssh» – протокол прикладного уровня.

13.2.3 Редактирование правил Suricata

В случае необходимости изменения действия сохранённых правил, добавленных через интерфейс командной строки (CLI), например, ранее созданного правила 1337, необходимо выполнить следующую команду:


```
admin@ngfwos:~$ suricata change-rules-action sid 1337 new-action drop
```

```
Success: Rules changed.
```

```
# Зафиксировать изменения.
```

```
admin@ngfwos:~$ suricata commit-rules
```

```
Success: Rules successfully committed in active database.
```

```
admin@ngfwos:~$ suricata save-rules
```

```
Success: All rules saved successfully in /config/files/configuration/suricata/rule-  
files/test.rules.
```

```
admin@ngfwos:~$
```

В данном случае действие правила было изменено с «alert» на «drop».

Примечание:

В случае необходимости изменения действия правил в файлах, добавленных не через интерфейс командной строки (CLI), необходимо добавить эти правила в рабочую директорию системы **Suricata** с помощью следующей команды:

```
admin@ngfwos:~$ suricata scan-rules dir-path <каталог> recursive <no  
| yes>
```

где:

- **<каталог>** - каталог для поиска правил Suricata, например - «/config/files/configuration/suricata/rule-files/»;
- **recursive <no | yes>** - параметр, определяющий, будет ли выполняться поиск во вложенных папках. Если установить значение «**no**», поиск во вложенных папках производиться не будет.

Данная команда производит анализ указанного каталога на предмет наличия правил **Suricata** и прописывает обнаруженные правила в рабочую директорию. Это позволит в дальнейшем редактировать действия для обнаруженных правил.

Рекомендуется не сканировать каталоги, содержащие более 30 000 правил, так как это приводит к ошибкам и сбоям в процессе сканирования. Если существует такой каталог, рекомендуется распределить файлы на несколько каталогов, в каждом из которых будет не более 30 000 правил.

13.2.4 Выключение правил Suricata

В случае необходимости выключения определённого правила, добавленного через интерфейс командной строки (CLI), необходимо выполнить следующую команду:

```
admin@ngfwos:~$ suricata disable-rules sid <sid>

Success: Rules disabled.

admin@ngfwos:~$

# Зафиксировать изменения.

admin@ngfwos:~$ suricata commit-rules
Success: Rules successfully committed in active database.

admin@ngfwos:~$ suricata save-rules
Success: All rules saved successfully in /config/files/configuration/suricata/rule-
files/suricata.rules.

admin@ngfwos:~$
```

Строка, содержащая указанное правило, будет закомментирована в файле с помощью специального символа «#»:

```
admin@ngfwos:~$ suricata show-rules directory active
SIDS
/config/files/configuration/suricata/rule-files/suricata.rules
1377
#alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"HTTP GET Request
Containing Rule in URI";
  flow:established,to_server; http.method; content:"GET"; http.uri; content:"rule";
  fast_pattern; classtype:bad-unknown; rev:1;)
IDS

admin@ngfwos:~$
```

Для отключения всех правил, содержащихся в файле «suricata.rules» (указан в качестве примера), необходимо выполнить следующую команду:

```
admin@ngfwos:~$ suricata disable-rules file-path
/config/files/configuration/suricata/rule-files/suricata.rules

Success: Rules disabled.

admin@ngfwos:~$

# Зафиксировать изменения.

admin@ngfwos:~$ suricata commit-rules
Success: Rules successfully committed in active database.

admin@ngfwos:~$ suricata save-rules
Success: All rules saved successfully in /config/files/configuration/suricata/rule-
files/suricata.rules.

admin@ngfwos:~$
```

Для активации ранее отключённых правил необходимо выполнить следующую команду:

```
# Включить все правила, указанные в файле suricata.rules.
admin@ngfwos:~$ suricata enable-rules file-path
/config/files/configuration/suricata/rule-files/suricata.rules

# Включить правила с идентификатором <sid>
admin@ngfwos:~$ suricata disable-rules sid <sid>
```

Зафиксировать изменения:

```
admin@ngfwos:~$ suricata commit-rules
Success: Rules successfully committed in active database.

admin@ngfwos:~$ suricata save-rules
Success: All rules saved successfully in /config/files/configuration/suricata/rule-
files/suricata.rules.

admin@ngfwos:~$
```

Примечание:

В случае необходимости отключения правил в файлах, добавленных не через интерфейс командной строки (CLI), необходимо добавить эти правила в рабочую директорию системы **Suricata**.

13.2.5 Удаление правила Suricata

В случае необходимости удаления файла с правила **Suricata**, добавленного через интерфейс командной строки (CLI), например, ранее созданного файла «test.rules», необходимо выполнить следующую команду:

```
admin@ngfwos:~$ suricata del-rules file-path
/config/files/configuration/suricata/rule-files/test.rules

Success: Rules removed.

# Зафиксировать изменения.

admin@ngfwos:~$ suricata commit-rules
Success: Rules successfully committed in active database.

admin@ngfwos:~$ suricata save-rules
Success: All rules saved successfully in /config/files/configuration/suricata/rule-
files/test.rules.

admin@ngfwos:~$
```

В случае необходимости удаления определённого правила **Suricata**, добавленного через интерфейс командной строки (CLI), необходимо выполнить следующую команду:

```
admin@ngfwos:~$ suricata del-rules sid <sid>

Success: Rules removed.

# Зафиксировать изменения.

admin@ngfwos:~$ suricata commit-rules
Success: Rules successfully committed in active database.

admin@ngfwos:~$ suricata save-rules
Success: All rules saved successfully in /config/files/configuration/suricata/rule-
files/suricata.rules.

admin@ngfwos:~$
```

Примечание:

В случае необходимости удаления правила или файла с правилами, добавленных не через интерфейс командной строки (CLI), необходимо добавить эти правила в рабочую директорию системы **Suricata**.

13.2.6 Обновление правил Suricata

Конфигурация источника правил:

- **Удалённый источник:**

Для настройки обновления правил с удалённого сервера необходимо ввести следующие команды:

```
set suricata update-rules remote-server Server1 authentication http-
basic login admin1
set suricata update-rules remote-server Server1 authentication http-
basic password examplePassw
set suricata update-rules remote-server Server1 url example.net
```

где:

- **«Server1»** – имя сервера обновлений. Максимальная длина – «256» символов.
- **«admin1»** – логин. Максимальная длина – «256» символов.
- **«examplePassw»** – пароль. Максимальная длина – «256» символов.

- «**example.net**» – URL ресурса. Приведены в качестве примера. Максимальная длина – «2000» символов.

Примечание:

Файлы обновлений правил безопасности **Suricata** загружаются в каталог «**/config/files/configuration/suricata/rule-files/**».

- **Локальный источник:**

Для настройки обновления правил с локального хранилища необходимо ввести следующую команду:

```
set suricata update-rules local-storage LOCAL path  
</path/to/storage>
```

где:

- «**LOCAL**» – имя локального хранилища. Максимальная длина – «256» символов.
- **</path/to/storage>** – путь к локальному хранилищу. Максимальная длина – «2000» символов.

Примечание:

Для успешного обновления правил, хранящихся в локальном хранилище, необходимо извлечь их из архива.

После настройки источника правил необходимо запустить процесс обновления.

- **Обновление с удалённого источника:**

Для импорта правила с конкретного удалённого сервера необходимо ввести следующую команду:

```
admin@ngfwos:~$ suricata update-rules remote-server Server1
```

где «**Server1**» – имя настроенного сервера обновлений.

Для импорта правила со всех настроенных удалённых серверов необходимо ввести следующую команду:

```
admin@ngfwos:~$ suricata update-rules remote-server all
```

- **Обновление с локального источника:**

Для импорта правила с конкретного локального хранилища необходимо ввести следующую команду:

```
admin@ngfwos:~$ suricata update-rules local-storage LOCAL
```

где «**LOCAL**» – имя локального хранилища.

Для импорта правила из всех настроенных локальных хранилищ необходимо ввести следующую команду:

```
admin@ngfwos:~$ suricata update-rules local-storage all
```

Для изменения каталога, используемого по умолчанию для хранения правил **Suricata**, необходимо ввести следующую команду:

```
set suricata default-rule-path /var/lib/suricata/rules/test/
```

где **</var/lib/suricata/rules/test/>** – новый каталог хранения правил по умолчанию.

По умолчанию используется каталог **«/config/files/configuration/suricata/rule-files/»**.

Для указания пути к файлу с правилами, который будет использоваться системой **Suricata** для анализа сетевого трафика и обнаружения потенциальных угроз, необходимо выполнить следующую команду:

```
set suricata rule-files file-name <test.rules>
```

где **<test.rules>** – имя файла с правилами **Suricata** (приведён в качестве примера), расположенного в каталоге по умолчанию: **«/config/files/configuration/suricata/rule-files/»**. Если файл правил находится в другом каталоге, необходимо указать полный путь к нему. Пример: «set suricata rule-files file-name /path/to/rules/test.rules».

Для настройки **Suricata** на использование всех файлов правил из определённого каталога, применяется следующая команда:

```
set suricata rule-files file-name /config/files/configuration/suricata/rule-files/*.rules
```

После выполнения данной команды система **Suricata** автоматически загрузит и активирует все правила, содержащиеся в файлах с расширением **«.rules»**, расположенных в каталоге **«/config/files/configuration/suricata/rule-files/»**.

13.3 Команды настройки Suricata

Примечание:

При работе Suricata в режиме IPS с использованием драйвера netmap перезагрузка конфигурации приводит к кратковременному разрыву активных сетевых сессий на интерфейсах, где включён IPS-режим.

Это обусловлено архитектурными особенностями IPS: Suricata располагается непосредственно на пути прохождения трафика на таких интерфейсах, обеспечивая его прямую обработку и пересылку. В ходе

перезагрузки конфигурации сетевые интерфейсы с активированным IPS временно отключаются, передача трафика приостанавливается, а состояние активных соединений (connection tracking) сбрасывается. В результате TCP- и UDP-сессии, проходящие через эти интерфейсы, могут быть прерваны.

В режиме IDS (TAB) Suricata анализирует лишь копию трафика и не участвует в его пересылке. Следовательно, перезагрузка конфигурации не оказывает влияния на стабильность сетевых соединений на интерфейсах, работающих в этом режиме.

В системах, где на отдельных интерфейсах включён IPS-режим, рекомендуется избегать частых перезагрузок Suricata. Обновление конфигурации следует выполнять в периоды минимальной сетевой нагрузки с целью минимизации воздействия на пользовательские сессии и критически важные сервисы, трафик которых проходит через указанные интерфейсы.

Обновление правил COB не приводит к перезапуску службы Suricata, однако инициирует внутреннюю перезагрузку правил в рамках работающего процесса. В момент перезагрузки правил возможна кратковременная несогласованность между текущим состоянием фильтрации и новым набором правил, что может повлиять на корректность обработки активных сессий. Рекомендуется учитывать этот фактор при планировании обновлений правил в высоконагруженных или критически важных сегментах сети.

Включение и выключение какого-либо параметра **IDS/IPS** осуществляется с помощью атрибутов «**yes**» и «**no**» соответственно.

1. Для включения сбора статистики о деятельности и производительности системы **IDS/IPS** необходимо ввести следующую команду:

```
set suricata stats enabled yes
```

2. Для установки интервала сбора статистики необходимо ввести следующую команду:

```
set suricata stats interval <interval>
```

где **<interval>** - значение интервала сбора статистики в секундах. По умолчанию используется значение «8».

3. Для включения записи событий и предупреждений **IDS/IPS** в глобальный журнал системы **ARMA Стена** необходимо ввести следующую команду:

```
set suricata outputs syslog enabled yes
```


По умолчанию запись событий и предупреждений IDS/IPS в глобальный журнал включена.

Дополнительные команды настройки включения записи событий и предупреждений IDS/IPS:

- Включить запись уведомлений о срабатывании событий **IDS/IPS** в формате JSON через rsyslog:

```
set suricata outputs eve-log enabled yes
```

При включении записи уведомлений в rsyslog они остаются в формате JSON, но оборачиваются в syslog-сообщение и имеют следующий вид:

```
05.11.2025 11:23:54 1762341834802752 ngfwos idps-rule[687302]:  
{"timestamp":"2025-11-  
05T11:23:54.802333+0000","flow_id":2090258090346303,...}}
```

- Включить запись уведомлений о срабатывании событий **IDS/IPS** в более простой текстовый файл «**fast.log**» журнала:

```
set suricata outputs fast enabled yes
```

Команда, предписывающая Suricata вносить все новые данные в существующий файл «**fast.log**», не заменяя его:

```
set suricata outputs fast append yes
```

- Включить запись статистики **IDS/IPS** в файл «**stats.log**»:

```
set suricata outputs stats enabled yes
```

Команда, предписывающая Suricata вносить все новые данные в существующий файл «**stats.log**», не заменяя его:

```
set suricata outputs stats append yes
```

- Включить журналирование HTTP-трафика в файл «**http.log**»:

```
set suricata outputs http-log enabled yes
```

Команда, предписывающая Suricata вносить все новые данные в существующий файл «**http.log**», не заменяя его:

```
set suricata outputs http-log append yes
```

- Включить запись информации о TLS-трафике в файл «**tls.log**»:

```
set suricata outputs tls-log enabled yes
```

Команда, предписывающая Suricata вносить все новые данные в существующий файл **«tls.log»**, не заменяя его:

```
set suricata outputs tls-log append yes
```

- Включить запись предупреждений в системе **IDS/IPS** в файл **«alert-debug.log»**:

```
set suricata outputs alert-debug enabled yes
```

Команда, предписывающая Suricata вносить все новые данные в существующий файл **«alert-debug.log»**, не заменяя его:

```
set suricata outputs alert-debug append yes
```

- Включить запись сертификатов TLS-сессий в системе **IDS/IPS**:

```
set suricata outputs tls-store enabled yes
```

Сертификаты сохраняются в каталоге **«/var/log/suricata/certs/»**.

- Включить сохранение всех пакетов, зарегистрированных в системе **IDS/IPS**, в файл журнала **«_log(n).pcap_»**:

```
set suricata outputs pcap-log enabled yes
```

Команда настройки размера файла **«_log(n).pcap_»**:

```
set suricata outputs pcap-log limit <limit>
```

где **<limit>** - максимальный размер файла в байтах. Возможно указать значение в диапазоне от «0» до «18446744073709553664». Допускается указать единицы измерения: kb - килобайт (возможный диапазон значений от «0» до «18014398509481986»), mb - мегабайт (возможный диапазон значений от «0» до «17592186044416») или gb - гигабайт (возможный диапазон значений от «0» до «17179869184»). По умолчанию используется значение «1000mb». В случае, если размер файла достигнет установленного лимита, произойдёт его ротация, и будет создан новый файл.

Команда ограничения максимального количества файлов pcap:

```
set suricata outputs pcap-log max-files <max>
```

где **<max>** - максимальное количество файлов pcap. Возможно указать значение в диапазоне от «1» до «4294967295». По умолчанию используется значение «2000».

Примечание:

Настройки «limit» и «max-files» применяются для каждого потока. Таким образом, ограничение объема для восьми потоков с 2000 файлами с размером 1000 мегабайт каждый составит 16 терабайт.

- Включить запись данных TCP после установления соединения в статусе «established» в файл «**tcp-data.log**»:

```
set suricata outputs tcp-data enabled yes
```

- Включить запись данных тела HTTP после установления соединения в статусе «established» в файл «**http-body-data.log**»:

```
set suricata outputs http-body-data enabled yes
```

Примечание:

При активации дополнительных файлов журналов уведомлений о срабатывании системы **IDS/IPS**, будут сохраняться в каталоге «**/var/log/suricata**».

4. Включить логирование системных событий работы Suricata в глобальный журнал системы **ARMA Стена**:

```
set suricata logging outputs syslog enabled yes
```

Дополнительные команды настройки включения логирования системных событий работы Suricata:

- Включить вывод журнала системных событий работы Suricata в окне терминала, в котором запущена система **ARMA Стена**:

```
set suricata logging outputs console enabled yes
```

- Включить логирование системных событий работы Suricata в файл «**suricata.log**»:

```
set suricata logging outputs file enabled yes
```

Файл «**suricata.log**» сохраняется в каталоге «**/var/log/suricata/**».

Установить уровень ведения журнала в файле «**suricata.log**»:

```
set suricata logging outputs file level <level>
```

где **<level>** - уровень ведения журнала. По умолчанию используется уровень «info».

5. Установить уровень ведения журнала по умолчанию:

```
set suricata logging default-log-level <level>
```

где **<level>** - уровень ведения журнала. По умолчанию используется уровень «notice». Возможно указать следующие значения:

- «**error**» - уровень ошибок, которые могут оказать влияние на работу системы;
- «**warning**» - уровень предупреждений о потенциальных проблемах;
- «**notice**» - уровень для общих уведомлений о важных событиях;
- «**info**» - уровень для информационных сообщений;
- «**perf**» - уровень для сообщений и событий, связанных с производительностью и работой системы Suricata;
- «**config**» - уровень конфигурации Suricata;
- «**debug**» - уровень для отладочной информации.

6. Включить/отключить обнаружение пакетов, переданных по определённому протоколу прикладного уровня:

```
set suricata app-layer protocols <protocolname> enabled yes|no
```

где **<protocolname>** – протокол.

Поддерживается обнаружение пакетов, переданных по следующим протоколам:

- «**ads**»;
- «**alphalink**» - по умолчанию отключён;
- «**bittorrent-dht**»;
- «**dcerpc**»;
- «**dhcp**»;
- «**dnp3**»;
- «**dns tcp**»;
- «**dns udp**»;
- «**enip**»;
- «**focas**»;
- «**ftp**»;
- «**hdlc**» - по умолчанию отключён;
- «**http**»;
- «**http2**»;

- «iec104»;
- «ike»;
- «imap»;
- «krb5»;
- «modbus» - по умолчанию отключён;
- «modbus2» - по умолчанию отключён;
- «mqtt»;
- «nfs»;
- «ntp»;
- «opc-ua»;
- «pgsql»;
- «quic»;
- «rdp»
- «rfb»;
- «sip»;
- «smb»;
- «smtp»;
- «snmp»;
- «ssh»;
- «telnet»;
- «tftp»;
- «tls»;
- «tpkt» (S7 Communication, S7 Communication Plus, MMS);
- «unet2» - по умолчанию отключён.

7. Для указания портов назначения, используемых при обнаружении пакетов по протоколу **ads**, необходимо ввести следующую команду:

```
set suricata app-layer protocols ads detection-ports dst-port <portnumber>
```

где **<portnumber>** – номер порта. По умолчанию используется порт «48898».

Возможно указание порта назначения при обнаружении пакетов по следующим протоколам:

- «alphalink», по умолчанию используются порты: «4388», «4389»;

- «**dnp3**», по умолчанию используется порт «20000»;
- «**dns tcp**» – DNS поверх TCP, по умолчанию используется порт «53»;
- «**dns udp**» – DNS поверх UDP, по умолчанию используется порт «53»;
- «**enip**», по умолчанию используется порт «44818»;
- «**focas**», по умолчанию используется порт «8193»;
- «**hdlc**», по умолчанию используются порты: «4060», «4061»;
- «**iec104**», по умолчанию используется порт «2404»;
- «**modbus**», по умолчанию используется порт «502»;
- «**modbus2**», по умолчанию используется порт «502»;
- «**opc-ua**», по умолчанию используются порты: «4840», «48020»;
- «**rfb**», по умолчанию используются порты: 5900, 5901, 5902, 5903, 5904, 5905, 5906, 5907, 5908, 5909;
- «**smb**», по умолчанию используются порты: «139», «445»;
- «**tls**», по умолчанию используется порт «443»;
- «**tpkt**» (**S7 Communication, S7 Communication Plus, MMS**), по умолчанию используется порт «102»;
- «**unet2**», по умолчанию используется порт «6000».

8. Для протокола **enip** существует возможность настроить порт источника:

```
set suricata app-layer protocols enip detection-ports src-port <portnumber>
```

где **<portnumber>** - номер порта. По умолчанию используется порт «44818».

Примечание:

При удалении ранее заданного пользователем значения порта назначения (dst-port) или порта источника (src-port) система автоматически восстанавливает для соответствующего протокола значения по умолчанию.

9. Для протокола **http** возможно настроить дополнительные параметры:

- определить размер скользящего окна для проверки тела запроса:

```
set suricata app-layer protocols http request-body-inspect-window  
<value>
```

где **<value>** - значение размера скользящего окна. По умолчанию используется значение «4kb».

- установить максимальный размер тела запроса:

```
set suricata app-layer protocols http request-body-limit <value>
```

где **<value>** - значение максимального размера тела запроса. По умолчанию используется значение «3072».

- установить минимальный размер тела запроса для начала проверки:

```
set suricata app-layer protocols http request-body-minimal-inspect-size <value>
```

где **<value>** - значение минимального размера тела запроса. По умолчанию используется значение «8kb».

- определить размер скользящего окна для проверки ответа:

```
set suricata app-layer protocols http response-body-inspect-window <value>
```

где **<value>** - значение минимального размера ответа. По умолчанию используется значение «4kb».

- установить максимальный размер тела ответа:

```
set suricata app-layer protocols http response-body-limit <value>
```

где **<value>** - значение максимального размера тела ответа. По умолчанию используется значение «3072».

- установить минимальный размер тела ответа для начала проверки:

```
set suricata app-layer protocols http response-body-minimal-inspect-size <value>
```

где **<value>** - значение минимального размера тела ответа. По умолчанию используется значение «8kb».

10. Для протокола **tls** возможно настроить дополнительные параметры:

- установить параметр, который определяет обработку трафика после установлении TLS сессии:

```
set suricata app-layer protocols tls encryption-handling <parameter>
```

где **<parameter>** - параметр поведения. Парсер прикладного уровня TLS имеет возможность прекратить обработку зашифрованного трафика после первоначального подтверждения связи. Возможно указать следующие параметры поведения:

- **default** - продолжить мониторинг TLS-сессии, выявить аномалии в протоколе, проверить ключевые слова TLS_*.

Отключить проверку немодифицированных сигнатур «content»;

- **bypass** - прекратить обработку этого потока настолько, насколько это возможно. Не проводить дальнейший анализ и проверку TLS. По возможности, обработку потока выполнять либо в ядре, либо в аппаратном обеспечении;
- **full** - продолжать отслеживание и проверку в обычном режиме. Сигнатуры ключевых слов немодифицированного содержимого также проверяются;

- включить поддержку JA3:

```
set suricata app-layer protocols tls ja3-fingerprints yes
```

11. Для протокола **smtp** возможно настроить дополнительные параметры:

- установить минимальный размер анализируемого сообщения:

```
set suricata app-layer protocols smtp inspected-tracker content-inspect-min-size <value>
```

где **<value>** - значение минимального размера сообщения в байтах. По умолчанию используется значение «32768».

- установить размера скользящего окна, в котором будет просматриваться сообщение:

```
set suricata app-layer protocols smtp inspected-tracker content-inspect-window <value>
```

где **<value>** - значение размера скользящего окна в байтах. По умолчанию используется значение «4096».

- установить максимального размера анализируемого сообщения:

```
set suricata app-layer protocols smtp inspected-tracker content-limit <value>
```

где **<value>** - значение максимального размера сообщения в байтах. По умолчанию используется значение «100000».

- включить пересчёт md5 для сообщения:

```
set suricata app-layer protocols smtp mime body-md5 yes
```

- включить декодирование сообщений MIME в формате Base64:

```
set suricata app-layer protocols smtp mime decode-base64 yes
```


- включить декодирование MIME-сообщений:

```
set suricata app-layer protocols smtp mime decode-mime yes
```

- включить декодирование quoted MIME-сообщений:

```
set suricata app-layer protocols smtp mime decode-quoted-printable yes
```

- включить сохранение URL из сообщений:

```
set suricata app-layer protocols smtp mime extract-urls yes
```

- указать максимальное количество байт для каждого значения данных заголовка, хранящегося в структуре данных:

```
set suricata app-layer protocols smtp mime header-value-depth <value>
```

где **<value>** - значение максимального количества байт. По умолчанию используется значение «2000».

- включить извлечение всех сырых smtp-сообщений (не совместимо с настройкой mime decode-mime):

```
set suricata app-layer protocols smtp raw-extraction yes
```

12. Команда настройки политики исключений для сессий, которые были захвачены в середине потока:

```
set suricata stream midstream-policy <policy>
```

где **<policy>** - значение политики исключений и результирующего поведения. Возможно указать следующие значения:

- **ignore** - не применять политику исключений. Используется по умолчанию;
- **drop-packet** - отбрасывает только текущий пакет, не затрагивая остальные пакеты в потоке;
- **drop-flow** - отключить проверку для всего потока (пакеты, полезная нагрузка, протокол прикладного уровня);
- **reject** - аналогично **drop-flow**, но дополнительно отклоняет текущий пакет;
- **pass-flow** - пропустить поток. Поток будет повторно собран, а его синтаксический анализ и протоколирование продолжены на уровне приложения;
- **bypass** - обход потока, дальнейший анализ потока не выполняется;

- **pass-packet** - отключает детектирование для текущего пакета, но продолжает выполнять обновления состояния потока и разбор прикладного уровня.

13. Команда настройки политики обработки ошибок, возникающих на прикладном уровне в Suricata:

```
set suricata app-layer error-policy <policy>
```

где **<policy>** - действие над пакетом. Возможно указать следующие значения:

- **drop-flow** - отключает проверку для всего потока (flow), включая пакеты, полезную нагрузку и протоколы прикладного уровня. Отбрасывает текущий пакет и все последующие пакеты в этом потоке. Применяется в ситуациях, требующих обеспечения высокого уровня защиты и оперативного блокирования потенциально вредоносного трафика;
- **pass-flow** - отключает проверку полезной нагрузки и пакетов, но продолжает выполнять сборку потока (stream reassembly), анализ прикладного уровня (app-layer parsing) и логирование;
- **bypass** - обходит (игнорирует) весь поток, отключая дальнейшую проверку. Используется для минимизации влияния ошибок на производительность, но может снижать безопасность;
- **drop-packet** - отбрасывает только текущий пакет, вызвавший ошибку;
- **pass-packet** - отключает детектирование для текущего пакета, но продолжает обновление потока и анализ прикладного уровня (в зависимости от того, какая политика была активирована). Позволяет изолировать ошибку, не затрагивая остальной трафик;
- **reject** - аналогично drop-flow, но также отправляет TCP-сброс (RST) или ICMP-сообщение об ошибке для завершения соединения. Уведомляет участников соединения о блокировке;
- **ignore** - игнорировать ошибку в приложении и продолжать обработку данных. Значение используется по умолчанию.

14. Команды настроек метода захвата сетевого трафика NetMap:

14.1 Для настройки режима захвата на определённом интерфейсе необходимо ввести следующую команду:

```
set suricata netmap interface <iname> copy-mode [ips | tap]
```

где:

- **<iname>** – имя интерфейса;

- **ips** – режим сетевой безопасности, обеспечивающий активный мониторинг и предотвращение подозрительной активности путём модификации, блокировки или отбрасывания трафика в реальном времени на основе правил безопасности;
- **tap** (ids) – режим пассивного мониторинга сетевого трафика, направленный на обнаружение подозрительной активности и генерацию оповещений при совпадении с заданными правилами безопасности, без вмешательства в проходящий трафик.

Примечание:

В случае, если для конкретного интерфейса не будет явно указан режим захвата, будет применяться глобальный режим захвата по умолчанию, установленный для всех интерфейсов. Если глобальный режим захвата для всех интерфейсов не будет определён, система выдаст сообщение об ошибке при попытке применения конфигурации:

```
admin@ngfwos# set suricata netmap interface eth1
[edit]
admin@ngfwos# commit
[ suricata ]
copy-mode must be configured for interface "eth1" or globally in
netmap parameters

[[suricata]] failed
Commit failed
[edit]
admin@ngfwos#
```

14.2 Для настройки режима захвата для всех интерфейсов, для которых режим захвата не задан локально, необходимо ввести следующую команду:

```
set suricata netmap parameters copy-mode [ips | tap]
```

14.3 Для указания количества потоков, используемых для обработки сетевых пакетов, необходимо ввести следующую команду:

```
set suricata netmap parameters threads <value>
```

где **<value>** - количество потоков. Возможно указать значение в диапазоне от «1» до «9999» или установлено как «auto». По умолчанию используется значение «auto». Рекомендуется выбирать значение, равное единице, либо использовать режим «auto», либо устанавливать значение, соответствующее числу RSS-очереди на интерфейсе. По умолчанию

используется настройка «auto». В случае несоответствия количества RSS-очередей, указанных в конфигурации, фактическому числу RSS-очередей на интерфейсе, функционирование Suricata может быть нестабильным или недостаточно эффективным.

14.4 Для настройки проверки контрольных сумм TCP-пакетов необходимо ввести следующую команду:

```
set suricata netmap parameters checksum-checks <yes | no | auto>
```

где **<yes | no | auto>** - параметр проверки контрольных сумм при работе Suricata в режиме NetMap. Возможно указать следующие значения:

- **yes** - включает проверку контрольных сумм (надёжность, но ниже производительность). Проверка контрольных сумм TCP-пакетов оказывает значительное влияние на производительность системы;
- **no** - отключает проверку (высокая производительность, но возможны ошибки);
- **auto** - автоматический выбор (оптимизация под оборудование и условия). Используется по умолчанию.

Примечание:

В режиме **<auto>** Suricata статистически определяет, можно ли доверять контрольным суммам пакетов для каждого интерфейса и протокола (IP/TCP/UDP) через анализ соотношения корректных и некорректных контрольных сумм. При обнаружении признаков аппаратного checksum offload (перенос функций расчёта контрольных сумм пакетов на контроллер сетевого адаптера) Suricata не использует checksum для отбрасывания пакетов и продолжает анализ, чтобы избежать потери трафика и алертов. При этом поведение **<auto>** равнозначно режиму **<no>**. Если признаки offload отсутствуют и большинство контрольных сумм корректны, некорректные контрольные суммы считаются ошибками, а поведение **<auto>** равнозначно режиму **<yes>**. Решение адаптируется со временем при изменении сетевого окружения или конфигурации оборудования.

Примечание:

Проверка контрольных сумм TCP-пакетов оказывает значительное влияние на производительность системы.

14.5 Настроить политику параметров драйвера сетевой карты при использовании метода захвата трафика NETMAP в Suricata.

```
set suricata netmap parameters driver-settings-policy <low | mid | high>.
```

где **<low | mid | high>** – блок настроек позволяющим оптимизировать работу NETMAP, регулируя уровень производительности и ресурсов, выделяемых для обработки сетевого трафика. Возможно указать следующие значения:

- **low** – подходит для сетей с низкой нагрузкой или ограниченными ресурсами оборудования. Минимизирует использование оперативной памяти и CPU:

if_num = 100 – количество интерфейсов, которые могут быть обработаны одновременно; **buf_num = 163840** – общее количество буферов для хранения пакетов; **if_size = 1024** – размер кольцевого буфера (ring buffer) для каждого интерфейса.

- **mid** (по умолчанию) – оптимальное решение для большинства сценариев, особенно при использовании сетей средней пропускной способности (до 10 Гбит/с):

if_num = 500 – увеличенное количество интерфейсов для обработки большего числа потоков данных; **buf_num = 491520** – увеличение объёма буферов для временного хранения пакетов; **if_size = 2048** – увеличенный размер кольцевого буфера для каждого интерфейса, снижая вероятность потери пакетов.

- **high** – рекомендовано для использования в высокоскоростных сетях со скоростью передачи данных 10 Гбит/с и выше, где требуется максимальная пропускная способность и минимальные потери данных:

if_num = 1000 – максимальное количество интерфейсов, которые могут быть обработаны одновременно; **buf_num = 983040** – увеличение объёма буферов для минимизации потерь пакетов при высокой нагрузке; **if_size = 4096** – максимальный размер кольцевого буфера, обеспечивающий минимальные задержки и максимальную пропускную способность.

14.6 Команда глобальной конфигурации действий с пакетами и потоками (*политика исключений*), возникающими в процессе работы Suricata (нехватка памяти, неподдерживаемый протокол, разрыв соединения и т.д.):

```
set suricata exception-policy <policy>
```

где **<policy>** – действие над пакетом. Возможно указать следующие значения:

- **auto** (используется по умолчанию);
- **drop-flow**;
- **pass-flow**;
- **bypass**;
- **drop-packet**;
- **pass-packet**;
- **reject**;
- **ignore**.

Примечание:

В случае если политика исключений не включена, Suricata не осуществляет регистрацию статистических данных, связанных с данной политикой.

15. Указать режим захвата сетевого трафика для Suricata:

```
set suricata capture-method <af-packet | netmap>
```

где **<af-packet | netmap>** - режим захвата сетевого трафика. Возможно указать следующие режимы:

- **netmap** - высокопроизводительный фреймворк для захвата и обработки сетевых пакетов, который минимизирует задержки и потери данных, обеспечивая максимальную эффективность на высокоскоростных сетях. Установлен по умолчанию.
- **af-packet** - режим перехвата трафика в Suricata, который требует наличия нескольких сетевых интерфейсов и работает в режиме шлюза.

16. Для оптимизации производительности сервера при работе с **IDS/IPS** возможно настроить один из предопределённых профилей производительности системы, введя следующую команду:

```
set system option performance <throughput | latency>
```

где:

- **«throughput»** - профиль сервера, ориентированный на повышение пропускной способности сети, акцентируясь на производительности в ущерб энергосбережению. Профиль содержит следующие основные настройки:
 - драйвер «intel_pstate» настраивается на максимальную производительность, в параметр «max_perf_pct» устанавливается значение «100» %;

- буферы ядра сети увеличиваются для улучшения пропускной способности;
 - включены Transparent Huge Pages (THP) для оптимизации работы с большими страницами памяти;
 - параметр «cripower» настраивается на режим «performance» для повышения производительности процессора;
 - в параметр «kernel.sched_min_granularity_ns» устанавливается значение «10» мкс для повышения точности планирования задач;
 - в параметр «kernel.sched_wakeup_granularity_ns» устанавливается значение «15» мкс для повышения скорости реакции на пробуждение задач;
 - в параметр «vm.dirty_ratio» устанавливается значение «40» % для повышения производительности дисковой подсистемы за счёт увеличенного кэша;
- **«latency»** - профиль сервера, ориентированный на снижение задержки сети, акцентируясь на производительности в ущерб энергосбережению. Профиль содержит следующие основные настройки:
 - драйвер «intel_pstate» настраивается на поддержание минимальной частоты процессора, в параметр «min_perf_pct» устанавливается значение «100» % для обеспечения минимальной задержки;
 - отключаются Transparent Huge Pages (THP);
 - отключается автоматический баланс нагрузки между узлами для уменьшения задержек;
 - параметр «cripower» настраивается на режим «performance» для повышения производительности процессора;
 - в параметр «cpu_dma_latency» устанавливается значение «1» для минимизации задержки при работе с памятью;
 - в параметры «busy_read» и «busy_poll» устанавливаются значения «50» мкс для ускорения операций ввода-вывода;
 - в параметр «tcp_fastopen» устанавливается значение «3» для ускорения установки TCP-соединений.

13.4 Контроль протоколов

Функция контроля протоколов реализована на основе технологии глубокой инспекции трафика на уровне прикладных протоколов, включая специализированные протоколы.

Механизм анализа и идентификации протоколов основан на сигнатурном методе обнаружения, обеспечивая интеллектуальное распознавание протоколов в реальном времени. Обнаружение и классификация трафика осуществляются с использованием правил системы сетевой инспекции **Suricata**, что позволяет эффективно выявлять и контролировать нештатное использование протоколов, а также потенциально вредоносную активность, связанную с ними.

Данная функциональность позволяет обеспечить видимость и контроль использования промышленных протоколов в сетях предприятия, предотвратить несанкционированный доступ к критическим системам и повысить уровень безопасности в средах ICS/SCADA.

Система **ARMA Стена** поддерживает следующие протоколы:

-  **ADS** - включён по умолчанию;
-  **Alpha.Link** - отключён по умолчанию;
-  **AoE (ADS over EtherCAT)** - включён;
- **Bittorrent-DHT** - включён по умолчанию;
- **DCERPC** - включён по умолчанию;
- **DHCP** - включён по умолчанию;
-  **DNP3** - включён по умолчанию;
- **DNS** - включён по умолчанию;
-  **ENIP/CIP** - включён по умолчанию;
-  **EtherCAT** - включён;
-  **Fanuc FOCAS** - включён по умолчанию;
- **FTP** - включён;
-  **GOOSE** - включён;
- **HTTP** - включён по умолчанию;
- **HTTP2** - включён по умолчанию;
-  **IEC 60870-5-104 (IEC-104)** - включён по умолчанию;
- **IKE** - включён по умолчанию;

- **IMAP** - включён по умолчанию;
- **KRB5** - включён по умолчанию;
-  **KRUG** - включён;
-  **Modbus** - отключён по умолчанию;
- **MQTT** - включён по умолчанию;
- **NFS** - включён по умолчанию;
- **NTP** - включён по умолчанию;
-  **OPC DA (только L3/IP Layer)** - включён;
-  **OPC UA** - включён по умолчанию;
- **PgSQL** - включён по умолчанию;
- **QUIC** - включён по умолчанию;
- **RDP** - включён по умолчанию;
- **RFB** - включён по умолчанию;
- **SIP** - включён по умолчанию;
- **SMB** - включён по умолчанию;
- **SMTP** - включён по умолчанию;
- **SNMP** - включён по умолчанию;
- **SSH** - включён по умолчанию;
- **Telnet** - включён по умолчанию;
- **TFTP** - включён по умолчанию;
- **TLS/SSL** - включён по умолчанию;
-  **TPKT (S7COMM, S7COMM Plus, MMS)** - включён по умолчанию;
-  **UMAS** - включён;
-  **UNET 2** - отключён по умолчанию.

13.4.1 ADS

ADS (Automation Device Specification) – протокол, используемый для обмена данными между устройствами в промышленных системах автоматизации. Протокол поддерживает два типа транспортных соединений:

- **TCP;**
- **UDP.**

События, связанные с передачей сообщений по протоколу **ADS**, могут быть обнаружены и обработаны на основе следующих признаков:

- **AMS NetId** – уникальный идентификатор целевого устройства.
- **AMS Port** – порт целевого устройства.
- **Команды ADS** – тип выполняемой команды.
- **Тип сообщения** – запрос (REQUEST) или ответ (RESPONSE).

В зависимости от используемой команды **ADS**, возможно указание дополнительных параметров в правиле:

- Команды **ADS Read, ADS Write, ADS Add Device Notification, ADS Read Write** поддерживают следующие параметры:
 - ADS Index Group;
 - ADS Index Offset.
- Команда **ADS Write Control** поддерживает следующие параметры:
 - ADS State – состояние ADS-соединения. Возможно использовать следующие значения:
 - 0 - ADSSTATE_INVALID;
 - 1 - ADSSTATE_IDLE;
 - 2 - ADSSTATE_RESET;
 - 3 - ADSSTATE_INIT;
 - 4 - ADSSTATE_START;
 - 5 - ADSSTATE_RUN;
 - 6 - ADSSTATE_STOP;
 - 7 - ADSSTATE_SAVECFG;
 - 8 - ADSSTATE_LOADCFG;
 - 9 - ADSSTATE_POWERFAILURE;
 - 10 - ADSSTATE_POWERGOOD;
 - 11 - ADSSTATE_ERROR;
 - 12 - ADSSTATE_SHUTDOWN;
 - 13 - ADSSTATE_SUSPEND;
 - 14 - ADSSTATE_RESUME;
 - 15 - ADSSTATE_CONFIG;
 - 16 - ADSSTATE_RECONFIG;

- диапазон 0 - 16.
- Device State – состояние устройства.
- Команда **ADS Add Device Notification** поддерживает параметр **Transmission Mode** (режим передачи уведомлений). Доступные значения:
 - «TRANSMISSION_MODE_NO_TRANS»;
 - «TRANSMISSION_MODE_CLIENT_CYCLE»;
 - «TRANSMISSION_MODE_CLIENT_1_REQ»;
 - «TRANSMISSION_MODE_SERVER_CYCLE»;
 - «TRANSMISSION_MODE_SERVER_ON_CHA».

Примечание:

Для обеспечения фильтрации сетевого трафика по протоколу **ADS** необходимо проверить, что распознавание пакетов данного протокола включено в системе **Suricata**. Это можно проверить и при необходимости активировать с помощью следующей команды в конфигурационном режиме:

```
set suricata app-layer protocols ads enabled yes
```

Обнаружение трафика по протоколу **ADS** в системе **Suricata** по умолчанию включено.

Примеры правил:

- AMS NetId - позволяет задать правило на основе идентификатора устройства (NetID):

```
# Блокировать TCP-пакеты, предназначенные устройству с NetID 5.99.54.158.1.1:
admin@ngfwos:~$ suricata add-rules file-path ads.rules text 'drop tcp any
any <> any any (ads_ip: NET_ID_TARGET[5.99.54.158.1.1:5.99.54.158.1.1];
rev: 1;)'
```

```
# Блокировать исходящие пакеты от устройств с NetID с 11.11.11.11.1.1
по 77.77.77.77.1.1:
admin@ngfwos:~$ suricata add-rules file-path ads.rules text 'drop tcp any
any <> any any (ads_ip: NET_ID_SOURCE[11.11.11.11.1.1:77.77.77.77.1.1];
rev: 1;)'
```

```
# Блокировать пакеты, отправленные от устройств с NetID с
11.11.11.11.1.1 по 77.77.77.77.1.1 к устройству с NetID 5.99.54.158.1.1:
admin@ngfwos:~$ suricata add-rules file-path ads.rules text 'drop tcp any
any <> any any (ads_ip: NET_ID_SOURCE[11.11.11.11.1.1:77.77.77.77.1.1],
NET_ID_TARGET[5.99.54.158.1.1:5.99.54.158.1.1]; rev: 1;)'
```

- AMS Port:

```
# Блокировать все TCP-пакеты, отправленные с порта 300:
admin@ngfwos:~$ suricata add-rules file-path ads.rules text 'drop tcp any
any <> any any (ads_ip: PORT_SOURCE[300:300]; rev: 1;)'
```

```
# Блокировать пакеты, адресованные на порты с 300 до 65535:
admin@ngfwos:~$ suricata add-rules file-path ads.rules text 'drop tcp any
any <> any any (ads_ip: PORT_TARGET[300:65535]; rev: 1;)'
```

- Command Id:

```
# Блокировать команду ADS Read Device Info (Command ID = 1):
admin@ngfwos:~$ suricata add-rules file-path ads.rules text 'drop tcp any
any <> any any (ads_ip: COMMAND_ID[1:1]; rev: 1;)'
```

```
# Блокировать команду ADS Read (Command ID = 2):
admin@ngfwos:~$ suricata add-rules file-path ads.rules text 'drop tcp any
any <> any any (ads_ip: COMMAND_ID[2:2]; rev: 1;)'
```

```
# Блокировать команду ADS Write (Command ID = 3):
admin@ngfwos:~$ suricata add-rules file-path ads.rules text 'drop tcp any
any <> any any (ads_ip: COMMAND_ID[3:3]; rev: 1;)'
```

```
# Блокировать команду ADS Read State (Command ID = 4):
```

```
admin@ngfwos:~$ suricata add-rules file-path ads.rules text 'drop tcp any  
any <> any any (ads_ip: COMMAND_ID[4:4]; rev: 1;)'
```

Блокировать команду ADS Write Control (Command ID = 5):

```
admin@ngfwos:~$ suricata add-rules file-path ads.rules text 'drop tcp any  
any <> any any (ads_ip: COMMAND_ID[5:5]; rev: 1;)'
```

Блокировать команду ADS Add Device Notification (Command ID = 6):

```
admin@ngfwos:~$ suricata add-rules file-path ads.rules text 'drop tcp any  
any <> any any (ads_ip: COMMAND_ID[6:6]; rev: 1;)'
```

Блокировать команду ADS Delete Device Notification (Command ID = 7):

```
admin@ngfwos:~$ suricata add-rules file-path ads.rules text 'drop tcp any  
any <> any any (ads_ip: COMMAND_ID[7:7]; rev: 1;)'
```

Блокировать команду ADS Device Notification (Command ID = 8):

```
admin@ngfwos:~$ suricata add-rules file-path ads.rules text 'drop tcp any  
any <> any any (ads_ip: COMMAND_ID[8:8]; rev: 1;)'
```

Блокировать команду ADS Read Write (Command ID = 9):

```
admin@ngfwos:~$ suricata add-rules file-path ads.rules text 'drop tcp any  
any <> any any (ads_ip: COMMAND_ID[9:9]; rev: 1;)'
```

Блокировать любые команды с ID от 1 до 10:

```
admin@ngfwos:~$ suricata add-rules file-path ads.rules text 'drop tcp any  
any <> any any (ads_ip: COMMAND_ID[1:10]; rev: 1;)'
```

- Message Type:

Блокировать все ADS-запросы:

```
admin@ngfwos:~$ suricata add-rules file-path ads.rules text 'drop tcp any  
any <> any any (ads_ip: REQUEST; rev: 1;)'
```

Блокировать все ADS-ответы:

```
admin@ngfwos:~$ suricata add-rules file-path ads.rules text 'drop tcp any  
any <> any any (ads_ip: RESPONSE; rev: 1;)'
```

Примечание:

Не допускается использовать «REQUEST» и «RESPONSE» одновременно в одном правиле, такое правило будет считаться невалидным.

- ADS Index:

```
# Блокировать команду ADS Read, если используется смещение индекса
от 5 до 1000:
admin@ngfwos:~$ suricata add-rules file-path ads.rules text 'drop tcp any
any <> any any (ads_ip: COMMAND_ID[2:2], INDEX_OFFSET[5:1000]; rev: 1;)'

# Блокировать команду ADS Write, если указано смещение от 5 до 1000:
admin@ngfwos:~$ suricata add-rules file-path ads.rules text 'drop tcp any
any <> any any (ads_ip: COMMAND_ID[3:3], INDEX_GROUP[5:1000]; rev: 1;)'

# Блокировать команду ADS Add Device Notification, если указано
смещение от 5 до 1000:
admin@ngfwos:~$ suricata add-rules file-path ads.rules text 'drop tcp any
any <> any any (ads_ip: COMMAND_ID[6:6], INDEX_OFFSET[5:1000]; rev: 1;)'

# Блокировать команду ADS Read Write, если указана группа индекса от
5 до 1000:
admin@ngfwos:~$ suricata add-rules file-path ads.rules text 'drop tcp any
any <> any any (ads_ip: COMMAND_ID[9:9], INDEX_GROUP[5:1000]; rev: 1;)'
```

- ADS State:

```
# Блокировать команду ADS Write Control, если состояние ADS
находится в диапазоне от 5 до 17:
admin@ngfwos:~$ suricata add-rules file-path ads.rules
text 'drop tcp any any <> any any (ads_ip: COMMAND_ID[5:5],
ADS_STATE[5:17]; rev: 1;)'
```

- Transmission mode:

```
# Блокировать команду ADS Add Device Notification, если используется
режим NO TRANS:
admin@ngfwos:~$ suricata add-rules file-path ads.rules text 'drop tcp any
any      <>      any      any      (ads_ip:      COMMAND_ID[6:6],
TRANSMISSION_MODE_NO_TRANS; rev: 1;)'

# Блокировать команду ADS Add Device Notification в режиме
циклического опроса клиента:
admin@ngfwos:~$ suricata add-rules file-path ads.rules text 'drop tcp any
any      <>      any      any      (ads_ip:      COMMAND_ID[6:6],
TRANSMISSION_MODE_CLIENT_CYCLE; rev: 1;)'

# Блокировать команду ADS Add Device Notification, если клиент
ожидает одно событие:
admin@ngfwos:~$ suricata add-rules file-path ads.rules text 'drop tcp any
any      <>      any      any      (ads_ip:      COMMAND_ID[6:6],
TRANSMISSION_MODE_CLIENT_1_REQ; rev: 1;)'

# Блокировать команду ADS Add Device Notification в режиме
циклической рассылки сервера:
admin@ngfwos:~$ suricata add-rules file-path ads.rules text 'drop tcp any
any      <>      any      any      (ads_ip:      COMMAND_ID[6:6],
TRANSMISSION_MODE_SERVER_CYCLE; rev: 1;)'

# Блокировать команду ADS Add Device Notification, если сервер
работает в режиме уведомления по изменению:
admin@ngfwos:~$ suricata add-rules file-path ads.rules text 'drop tcp any
any      <>      any      any      (ads_ip:      COMMAND_ID[6:6],
TRANSMISSION_MODE_SERVER_ON_CHA; rev: 1;)'
```

13.4.2 Alpha Link

Поддерживается работа на прикладном или сетевом уровне.

Для анализа и фильтрации сообщений по протоколу **Alpha Link** доступны следующие параметры сопоставления:

- ANY/NOT – универсальное совпадение или его отрицание;
- CMD (Command) – значение команды или диапазон значений (CMD = x / CMD [x:y]);
- CMD_TYPE (Тип команды) – определённое значение типа команды (CMD_TYPE = x / CMD_TYPE [x:y]);

Примечание:

Для обеспечения фильтрации сетевого трафика по протоколу **Alpha Link** необходимо активировать распознавание пакетов этого протокола с помощью следующей команды в конфигурационном режиме:

```
set suricata app-layer protocols alphaslink enabled yes
```

По умолчанию обнаружение пакетов протокола **Alpha Link** в **Suricata** отключено.

Пример правила:

- ANY/NOT:

```
admin@ngfwos:~$ suricata add-rules file-path alphaslink.rules text 'drop tcp  
any any -> any any (alphalink: ANY; rev: 1;)'
```

Правило блокирует весь исходящий TCP-трафик, если пакет соответствует условию «ANY» модуля alphaslink.

- Команда:

```
admin@ngfwos:~$ suricata add-rules file-path alphaslink.rules text 'drop tcp  
any any <- any any (alphalink: COUNTERS(0|2|8), CMD [5:15]; rev: 1;)'
```

Команда добавляет в файл «alphalink.rules» правило для Suricata, которое блокирует входящий TCP-трафик (от любого источника к локальному хосту), если через модуль alphaslink обнаружены «COUNTERS» со значениями «0», «2» или «8» и значение команды (CMD) находится в диапазоне от «5» до «15».

- Тип команды:

```
admin@ngfwos:~$ suricata add-rules file-path alphaslink.rules text 'drop tcp  
any any <> any any (alphalink: COUNTERS(0|2|8), CMD_TYPE = 5; rev: 1;)'
```

Данное правило блокирует TCP-трафик в обоих направлениях, если в пакете содержатся указанные значения счётчиков (COUNTERS = 0, 2, 8) и тип команды (CMD_TYPE) равный «5».

13.4.3 AoE

AoE (ADS over Ethercat) – сетевой протокол прикладного уровня, работающий поверх EtherCAT и использующий его механизм почтовых ящиков (Mailbox). Предназначен для передачи команд ADS (Automation Device Specification) между устройствами в промышленных сетях. AoE инкапсулирует ADS-запросы и ответы (чтение/запись регистров, управление состоянием) в EtherCAT-фреймы,

обеспечивая стандартизированный доступ к данным и функциям промышленных устройств.

Примеры правил:

```
# Правило блокирует AoE-фреймы, содержащие запросы к конкретному ADS-
регистру (Index Group = 0xF0030000, Index Offset = 0x00000100)
admin@ngfwos:~$ suricata add-rules file-path aoe.rules text 'drop ether any any ->
any          any          (ethercat.mbx_type:0x02;          aoe.index_group:0xF0030000;
aoe.index_offset:0x00000100; rev:1;)'

# Правило генерирует алерт при обнаружении AoE-запросов на чтение
(ADS_ReadReq, Service ID = 0x04)
admin@ngfwos:~$ suricata add-rules file-path aoe.rules text 'alert ether any any ->
any any (ethercat.mbx_type:0x02; aoe.service_id:0x04; rev:1;)'
```

13.4.4 DNP3

Протокол DNP3 (Distributed Network Protocol 3) поддерживает фильтрацию сетевых пакетов по следующим критериям:

- **Функция** – выполняемая команда.

Функции определяют тип операции, например чтение данных или перезагрузку устройства. Список функций представлен в [таблице «Список функций DNP3»](#).

Таблица «Список функций DNP3»

Hex	Значение	Метка
0	0	confirm
1	1	read
2	2	write
3	3	select
4	4	operate
5	5	direct_operate
6	6	direct_operate_nr
7	7	immed_freeze
8	8	immed_freeze_nr
9	9	freeze_clear
A	10	freeze_clear_nr
B	11	freeze_at_time

Hex	Значение	Метка
C	12	freeze_at_time_nr
D	13	cold_restart
E	14	warm_restart
F	15	initialize_data
10	16	initialize_appl
11	17	start_appl
12	18	stop_appl
13	19	save_config
14	20	enable_unsolicited
15	21	disable_unsolicited
16	22	assign_class
17	23	delay_measure
18	24	record_current_time
19	25	open_file
1A	26	close_file
1B	27	delete_file
1C	28	get_file_info
1D	29	authenticate_file
1E	30	abort_file
1F	31	activate_config
20	32	authenticate_req
21	33	authenticate_err
81	129	response
82	130	unsolicited_response
83	131	authenticate_resp

Примеры правил:

```
# Правило срабатывает при выполнении команды read:
admin@ngfwos:~$ suricata add-rules file-path dnp3.rules text 'alert dnp3
any any -> any any (dnp3_func:read; rev: 1;)'

# Правило срабатывает при выполнении команды start_appl:
admin@ngfwos:~$ suricata add-rules file-path dnp3.rules text 'alert dnp3
any any -> any any (dnp3_func:17; rev: 1;)'
```

Примечание:

В рамках одного правила не допускается использование нескольких меток.

- **Объект** – группа и вариация объекта, к которому обращаются.

Примеры правил:

```
# Правило срабатывает при обращении к объектам группы 2:
admin@ngfwos:~$ suricata add-rules file-path dnp3.rules text 'alert dnp3
any any -> any any (dnp3_obj:2; rev: 1;)'

# Правило срабатывает при обращении к объектам группы 2, вариации
3:
admin@ngfwos:~$ suricata add-rules file-path dnp3.rules text 'alert dnp3
any any -> any any (dnp3_obj:2,3; rev: 1;)'
```

- **Внутренняя индикация** – состояние устройства.

Внутренние индикации используются для передачи состояния устройства. Перечень внутренних индикаций протокола DNP3 приведён в [таблице «Список внутренних индикаций протокола DNP3»](#).

Таблица «Список внутренних индикаций протокола DNP3»

Hex	Метка
0x8000	device_restart
0x4000	device_trouble
0x2000	local_control
0x1000	need_time
0x0800	class_3_events
0x0400	class_2_events
0x0200	class_1_events
0x0100	all_stations

Hex	Метка
0x0080	reserved_1
0x0040	reserved_2
0x0020	config_corrupt
0x0010	already_executing
0x0008	event_buffer_overflow
0x0004	parameter_error
0x0002	object_unknown
0x0001	no_func_code_support

Примеры правил:

```
# Правило срабатывает при перезагрузке устройства:
admin@ngfwos:~$ suricata add-rules file-path dnp3.rules text 'alert dnp3
any any -> any any (dnp3_ind:device_restart; rev: 1;)'

# Правило срабатывает при необходимости синхронизации времени
или неизвестной команде:
admin@ngfwos:~$ suricata add-rules file-path dnp3.rules text 'alert dnp3
any any -> any any (dnp3_ind:need_time,no_func_code_support; rev: 1;)'
```

- **Контент** – содержательная часть пакета в шестнадцатеричном виде.

Для анализа содержательной части пакета используется механизм сопоставления с образцом. Указывается шестнадцатеричный поток данных.

Примеры правил:

```
# Правило срабатывает при наличии последовательности c6 02 в теле
пакета:
admin@ngfwos:~$ suricata add-rules file-path dnp3.rules text 'alert dnp3
any any -> any any (dnp3_data; content:"|c6 02|"; rev: 1;)'

# Правило срабатывает при наличии указанной шестнадцатеричной
последовательности:
admin@ngfwos:~$ suricata add-rules file-path dnp3.rules text 'alert dnp3
any any -> any any (dnp3_data; content:"|01 01 01 00 00 00 00 00 00 00|";
rev: 1;)'
```

13.4.5 ENIP/CIP

Для **ENIP (Ethernet/IP)** доступны следующие правила:

- Фильтрация по любому пакету **ENIP/CIP**.

Пример правила:

```
# Правило для обнаружения любого пакета протокола ENIP/CIP:
admin@ngfwos:~$ suricata add-rules file-path enip-cip.rules text 'alert
enip any any <> any any (msg: "Any ENIP/CIP packet detected"; rev: 1;)'
```

- Фильтрация по команде **ENIP (enip_command)**.

Каждый пакет **ENIP** содержит поле **Command**, определяющее тип выполняемой операции. Значение команды задаётся в диапазоне от «0» до «65535».

Примеры правил:

```
# Правило срабатывает при обнаружении команды 0x0070 (Send
Unit Data):
admin@ngfwos:~$ suricata add-rules file-path enip-cip.rules text 'alert
enip any any <> any any (enip_command: 112; rev: 1;)'

# Правило срабатывает при обнаружении команды 0x006F (Send
RR Data):
admin@ngfwos:~$ suricata add-rules file-path enip-cip.rules text 'alert
enip any any <> any any (enip_command: 111; rev: 1;)'
```

В протоколе **CIP (Common Industrial Protocol)** фильтрация возможна по следующим параметрам:

- **Сервис (cip_service)** - определяет тип запроса в протоколе **CIP**. Возможный диапазон значений - от «0» до «127».

Примеры правил:

```
# Правило срабатывает при обнаружении сервиса 0x0A (Multiple
Service Packet):
admin@ngfwos:~$ suricata add-rules file-path enip-cip.rules text 'alert
enip any any <> any any (cip_service: 10; rev: 1;)'

# Правило срабатывает при обнаружении команды сервиса 0x03
(Get Attribute List):
admin@ngfwos:~$ suricata add-rules file-path enip-cip.rules text 'alert
enip any any <> any any (cip_service: 3; rev: 1;)'
```

- **Класс (cip_class)** - используется совместно с сервисом. Возможный диапазон значений - от «1» до «65535». Указывается сразу после сервиса. Фильтрация только по классу без указания сервиса не поддерживается.

Список сервисов, поддерживающих фильтрацию по классу:

- «0x03 (Get Attribute List)»;
- «0x04 (Set Attribute List)»;
- «0x0E (Get Attribute Single)»;
- «0x10 (Set Attribute Single)».

Пример правила:

```
# Правило срабатывает при обнаружении сервиса 0x03 (Get Attribute List) и класса 0xAC:  
admin@ngfwos:~$ suricata add-rules file-path enip-cip.rules text 'alert  
enip any any <> any any (cip_service: 3,172; rev: 1;)'
```

- **Атрибут (cip_attribute)** - указывается после сервиса и класса. Возможный диапазон значений - от «0» до «65535». Фильтрация только по атрибуту без указания сервиса и класса не поддерживается.

Поддерживаются только следующие сервисы:

- «0x03 (Get Attribute List)»;
- «0x04 (Set Attribute List)»;
- «0x0E (Get Attribute Single)»;
- «0x10 (Set Attribute Single)».

Пример правила:

```
# Правило срабатывает при обнаружении сервиса 0x03 (Get Attribute List), класса 0xAC и атрибута 0x0005:  
admin@ngfwos:~$ suricata add-rules file-path enip-cip.rules text 'alert  
enip any any <> any any (cip_service: 3,172,5; rev: 1;)'
```

- **ANSI сегмент (cip: ANSI:)**

Позволяет анализировать содержимое вложенных пакетов **CIP**. Указывается как строковое значение.

Пример правила:

```
# Правило срабатывает при обнаружении в трафике EtherNet/IP CIP-сервис 82 и строки "F60" в ANSI-кодировке внутри сообщения:  
admin@ngfwos:~$ suricata add-rules file-path enip-cip.rules text 'alert  
enip any any <> any any (cip_service: 82; cip: ANSI: "F60"; rev: 1;)'
```

- **Порт (cip: PORT)**

Позволяет фильтровать порты во вложенных пакетах **CIP**. Поддерживаются операторы сравнения: «=», «!=», «>», «<», а также точное указание диапазона «[value:length]».

В сервисе 0x52 (Unconnected Send) содержится вложенный пакет. Порт обычно находится в заголовке первого пакета, а ANSI-сегмент – во втором. Это необходимо учитывать при анализе структуры пакетов и настройке фильтров.

Пример правила:

```
# Правило срабатывает при обнаружении пакетов протокола ENIP
с CIP-сервисом 0x52 (Unconnected Send), содержащие во
вложенном запросе порт, отличный от значения 10:
admin@ngfwos:~$ suricata add-rules file-path enip-cip.rules text 'alert
enip any any <> any any (cip_service: 82; cip: PORT != 10; rev: 1;)'
```

Для одновременной фильтрации пакета по **порту** и по **ANSI-сегменту** необходимо использовать два отдельных правила, связанных через механизм флагов состояния. Это связано с тем, что указанные параметры относятся к разным уровням вложенных протоколов и не могут быть проверены в рамках одного правила.

Пример правил:

```
# Правило устанавливает флаг cip_matreshka при обнаружении
порта 9:
admin@ngfwos:~$ suricata add-rules file-path enip-cip.rules text 'alert
enip any any <> any any (flowbits: set, cip_matreshka; cip_service: 82;
cip: PORT = 9; rev: 1;)'

# Второе правило проверяет наличие ANSI-сегмента "N69" при
установленном флаге:
admin@ngfwos:~$ suricata add-rules file-path enip-cip.rules text 'alert
enip any any <> any any (flowbits: isset, cip_matreshka; cip_service: 76;
cip: ANSI: "N69"; rev: 1;)'
```

Цепочка правил применяется последовательно: второе правило активируется только при выполнении условия первого.

Возможно одновременно указывать фильтры для протоколов **ENIP** и **CIP**, разделяя их точкой с запятой внутри одного правила.

Пример правила:

```
# Правило фильтрует ENIP команду 0x0070 (Send Unit Data) и CIP сервис 0x03  
(Get Attribute List) с классом 0xAC и атрибутом 0x0005:  
admin@ngfwos:~$ suricata add-rules file-path enip-cip.rules text 'alert enip any  
any <> any any (enip_command: 112; cip_service: 3,172,5; rev: 1;)'
```

13.4.6 EtherCAT

Для фильтрации пакетов с использованием протокола **EtherCAT** могут применяться следующие параметры:

- **Команда (CMD).**

Для реализации фильтрации по значению команды применяется правило типа диапазон.

Пример правил:

```
# Правило срабатывает при обнаружении пакетов с командой EtherCAT,  
равной 1:  
admin@ngfwos:~$ suricata add-rules file-path ethercat.rules text 'alert ip any  
any -> any any (ethercat: CMD[1:1]; rev: 1;)'  
  
# Правило срабатывает при обнаружении пакетов с командой EtherCAT в  
диапазоне от 1 до 13:  
admin@ngfwos:~$ suricata add-rules file-path ethercat.rules text 'alert ip any  
any -> any any (ethercat: CMD[1:13]; rev: 1;)'
```

- **Логический адрес (ADDR).**

Фильтрация по логическому адресу также выполняется с использованием правила типа диапазон.

Пример правил:

```
# Правило срабатывает при обнаружении пакетов с логическим адресом  
65535:  
admin@ngfwos:~$ suricata add-rules file-path ethercat.rules text 'alert ip any  
any -> any any (ethercat: ADDR[65535:65535]; rev: 1;)'  
  
# Правило срабатывает при обнаружении пакетов с логическим адресом  
69632:  
admin@ngfwos:~$ suricata add-rules file-path ethercat.rules text 'alert ip any  
any -> any any (ethercat: ADDR[69632:69632]; rev: 1;)'
```

- **Составной адрес (SLAVE, OFFSET).**

Составной адрес представляет собой комбинацию идентификатора устройства (**Slave**) и смещения (**Offset**), указывающего на конкретный регистр памяти внутри этого устройства.

Slave – числовой идентификатор, однозначно определяющий устройство в сети **EtherCAT**.

Пример правил:

```
# Правило срабатывает при обнаружении пакетов, направленные на
устройство с номером Slave = 3:
admin@ngfwos:~$ suricata add-rules file-path ethercat.rules text 'alert ip any
any -> any any (ethercat: SLAVE[3:3]; rev: 1;)'
```

```
# Правило срабатывает при обнаружении пакетов, направленные на
устройство с номером Slave = 65534:
admin@ngfwos:~$ suricata add-rules file-path ethercat.rules text 'alert ip any
any -> any any (ethercat: SLAVE[65534:65534]; rev: 1;)'
```

Offset – адрес регистра или области памяти внутри указанного устройства.

Пример правил:

```
# Правило срабатывает при обнаружении пакетов с обращением к регистру
Offset = 304:
admin@ngfwos:~$ suricata add-rules file-path ethercat.rules text 'alert ip any
any -> any any (ethercat: OFFSET[304:304]; rev: 1;)'
```

```
# Правило срабатывает при обнаружении пакетов с обращением к регистру
Offset = 1282:
admin@ngfwos:~$ suricata add-rules file-path ethercat.rules text 'alert ip any
any -> any any (ethercat: OFFSET[1282:1282]; rev: 1;)'
```

- **Значение поля данных (DATA).**

Предусмотрена возможность поиска шестнадцатеричного потока в поле данных датаграммы **EtherCAT**. Область поиска включает данные между заголовком датаграммы и счётчиком WKC.

Таким образом возможно обнаруживать:

- данные, передаваемые с использованием логического адреса;
- данные, относящиеся к профилям коммуникации (например, AoE, CoE);
- содержимое регистров.

Пример правил:

```
# Правило срабатывает при обнаружении пакетов, содержащие
последовательность 08 00 в поле данных:
admin@ngfwos:~$ suricata add-rules file-path ethercat.rules text 'alert ip any
any -> any any (ethercat: DATA:|08 00|; rev: 1;)'

# Правило срабатывает при обнаружении пакетов с данными,
соответствующими определённому профилю CoE:
admin@ngfwos:~$ suricata add-rules file-path ethercat.rules text 'alert ip any
any -> any any (ethercat: DATA:|0A 00 03 10 00 03 00 20 2F 12 1C 00 00 00 00
00|; rev: 1;)'
```

- **Регистры.**

Список поддерживаемых регистров:

- **0x0120** - управляющий регистр. Фильтрация выполняется с использованием правил типа диапазон и метки.

Пример правил:

```
# Правило срабатывает при обнаружении обращений к биту
CTRL регистра 0x0120 со значением 5:
admin@ngfwos:~$ suricata add-rules file-path ethercat.rules text
'alert ip any any -> any any (ethercat: 120_CTRL[5:5]; rev: 1;)'

# Правило срабатывает при обнаружении установки флага
ERROR_ACK регистра 0x0120 в состояние TRUE:
admin@ngfwos:~$ suricata add-rules file-path ethercat.rules text
'alert ip any any -> any any (ethercat: 120_ERROR_ACK_TRUE; rev:
1;)'

# Правило срабатывает при обнаружении сброса флага ID
регистра 0x0120 в состояние FALSE:
admin@ngfwos:~$ suricata add-rules file-path ethercat.rules text
'alert ip any any -> any any (ethercat: 120_ID_FALSE; rev: 1;)'
```

- **0x0130** - статусный регистр. Фильтрация выполняется с использованием правил типа диапазон и метки.

Пример правил:

```
# Правило срабатывает при обнаружении обращений к биту  
STATUS регистра 0x0130 со значением 5:
```

```
admin@ngfwos:~$ suricata add-rules file-path ethercat.rules text  
'alert ip any any -> any any (ethercat: 130_STATUS[5:5]; rev: 1;)'
```

```
# Правило срабатывает при обнаружении установки флага  
ERROR регистра 0x0130 в состояние TRUE:
```

```
admin@ngfwos:~$ suricata add-rules file-path ethercat.rules text  
'alert ip any any -> any any (ethercat: 130_ERROR_TRUE; rev: 1;)'
```

```
# Правило срабатывает при обнаружении сброса флага ID  
регистра 0x0130 в состояние FALSE:
```

```
admin@ngfwos:~$ suricata add-rules file-path ethercat.rules text  
'alert ip any any -> any any (ethercat: 130_ID_FALSE; rev: 1;)'
```

- **0x0200** - регистр состояния контроллера. Фильтрация выполняется с использованием правил типа метки.

Пример правил:

```
# Правило срабатывает при обнаружении указанного  
<Значение> EtherCAT, связанных с событием LATCH:  
admin@ngfwos:~$ suricata add-rules file-path ethercat.rules  
text 'alert ip any any -> any any (ethercat:  
200_LATCH_Значение; rev: 1;)'
```

```
# Правило срабатывает при регистрации статуса ESK в  
пакете EtherCAT с заданным логическим значением:  
admin@ngfwos:~$ suricata add-rules file-path ethercat.rules  
text 'alert ip any any -> any any (ethercat:  
200_ESK_STATUS_Значение; rev: 1;)'
```

```
# Правило срабатывает при появлении указанного AL-  
статуса <Значение>:  
admin@ngfwos:~$ suricata add-rules file-path ethercat.rules  
text 'alert ip any any -> any any (ethercat:  
200_AL_STATUS_Значение; rev: 1;)'
```

```
# Правило срабатывает при наличии в трафике EtherCAT  
значения IRQ для указанного SM-модуля с указанным  
номером <Номер>:  
admin@ngfwos:~$ suricata add-rules file-path ethercat.rules  
text 'alert ip any any -> any any (ethercat:  
200_SM_Номер_IRQ_Значение; rev: 1;)'
```

где:

- **<Значение>** - может принимать значения **TRUE** или **FALSE**, в зависимости от состояния флага в поле регистра;
- **<Номер>** - число в диапазоне от «0» до «7».
- **0x0300** - регистр CRC. Фильтрация выполняется с использованием правил типа диапазон.

Пример правил:

```
# Правило срабатывает при обнаружении ошибки RX_ERROR
канала CRC <Номер> со значением 5:
admin@ngfwos:~$ suricata add-rules file-path ethercat.rules text
'alert ip any any -> any any (ethercat:
300_CRC_Номер_INV_FRAME[5:5]; rev: 1;)'
```

```
# Правило срабатывает при обнаружении ошибки
INV_FRAME канала CRC <Номер> со значением 5:
admin@ngfwos:~$ suricata add-rules file-path ethercat.rules text
'alert ip any any -> any any (ethercat:
300_CRC_Номер_RX_ERROR[5:5]; rev: 1;)'
```

где **<Номер>** - число в диапазоне от «0» до «3».

- **0x0502** - регистр конфигурации EEPROM. Фильтрация выполняется с использованием правил типа метки.

Пример правил:

```
# Правило срабатывает при обнаружении установленного
уровня разрешения на запись 1 в регистре 0x0502:
admin@ngfwos:~$ suricata add-rules file-path ethercat.rules text
'alert ip any any -> any any (ethercat:
502_WRITE_ACCESS_1_Значение; rev: 1;)'
```

```
# Правило срабатывает при обнаружении включения или
отключения эмуляции EEPROM через соответствующий флаг
регистра 0x0502:
admin@ngfwos:~$ suricata add-rules file-path ethercat.rules text
'alert ip any any -> any any (ethercat:
502_EEPROM_EMUL_Значение; rev: 1;)'
```

```
# Правило срабатывает при разрешения доступа к данным
размером 8 байт:
admin@ngfwos:~$ suricata add-rules file-path ethercat.rules text
'alert ip any any -> any any (ethercat:
502_8_B_ACCESS_Значение; rev: 1;)'
```

```
# Правило срабатывает при обнаружении обращения к
адресу, использующему 2-байтовый формат:
admin@ngfwos:~$ suricata add-rules file-path ethercat.rules text
'alert ip any any -> any any (ethercat:
502_2_B_ADDRESS_Значение; rev: 1;)'
```

Правило срабатывает при обнаружении попытки чтения из регистра 0x0502:

```
admin@ngfwos:~$ suricata add-rules file-path ethercat.rules text  
'alert ip any any -> any any (ethercat:  
502_READ_ACCESS_Значение; rev: 1;)'
```

Правило срабатывает при обнаружении второго уровня разрешения на запись данных в регистр:

```
admin@ngfwos:~$ suricata add-rules file-path ethercat.rules text  
'alert ip any any -> any any (ethercat:  
502_WRITE_ACCESS_2_Значение; rev: 1;)'
```

Правило срабатывает при попытке перезагрузки конфигурации EEPROM:

```
admin@ngfwos:~$ suricata add-rules file-path ethercat.rules text  
'alert ip any any -> any any (ethercat:  
502_RELOAD_ACCESS_Значение; rev: 1;)'
```

Правило срабатывает при обнаружении наличия ошибки CRC в пакете EtherCAT:

```
admin@ngfwos:~$ suricata add-rules file-path ethercat.rules text  
'alert ip any any -> any any (ethercat:  
502_CRC_ERROR_Значение; rev: 1;)'
```

Правило срабатывает при возникновении ошибки загрузки данных EEPROM:

```
admin@ngfwos:~$ suricata add-rules file-path ethercat.rules text  
'alert ip any any -> any any (ethercat:  
502_LOAD_ERROR_Значение; rev: 1;)'
```

Правило срабатывает при обнаружении ошибки выполнения команды в контексте EEPROM:

```
admin@ngfwos:~$ suricata add-rules file-path ethercat.rules text  
'alert ip any any -> any any (ethercat:  
502_CMD_ERROR_Значение; rev: 1;)'
```

Правило срабатывает при ошибке записи данных в EEPROM:

```
admin@ngfwos:~$ suricata add-rules file-path ethercat.rules text  
'alert ip any any -> any any (ethercat:  
502_WRITE_ERROR_Значение; rev: 1;)'
```

Правило срабатывает при обнаружении статуса занятости

EEPROM в текущем пакете:

```
admin@ngfwos:~$ suricata add-rules file-path ethercat.rules text  
'aalert ip any any -> any any (ethercat: 502_BUSY_Значение; rev:  
1;)'
```

где **<Значение>** - может принимать значения **TRUE** или **FALSE**, в зависимости от состояния флага в поле регистра.

- **0x0504–0x050E** - расширенные регистры. Фильтрация выполняется с использованием правил типа диапазон.

Пример правил:

```
# Правило срабатывает при обращении к регистру 0x0504 с  
значением поля, равным 5:
```

```
admin@ngfwos:~$ suricata add-rules file-path ethercat.rules text  
'alert ip any any -> any any (ethercat: 504[5:5]; rev: 1;)'
```

```
# Правило срабатывает при обнаружении обращения к  
регистру 0x0506 с установленным значением поля 5:
```

```
admin@ngfwos:~$ suricata add-rules file-path ethercat.rules text  
'alert ip any any -> any any (ethercat: 506[5:5]; rev: 1;)'
```

```
# Правило срабатывает при обнаружении обращения к  
регистру 0x0508, если значение соответствует 5:
```

```
admin@ngfwos:~$ suricata add-rules file-path ethercat.rules text  
'alert ip any any -> any any (ethercat: 508[5:5]; rev: 1;)'
```

```
# Правило срабатывает при обнаружении обращения к  
регистру 0x050A с заданным значением 5 в поле данных:
```

```
admin@ngfwos:~$ suricata add-rules file-path ethercat.rules text  
'alert ip any any -> any any (ethercat: 50A[5:5]; rev: 1;)'
```

```
# Правило срабатывает при обнаружении обращения к  
регистру 0x050C, где значение равно 5.:
```

```
admin@ngfwos:~$ suricata add-rules file-path ethercat.rules text  
'alert ip any any -> any any (ethercat: 50C[5:5]; rev: 1;)'
```

```
# Правило срабатывает при обнаружении обращения к  
регистру 0x050E с полем, равным 5:
```

```
admin@ngfwos:~$ suricata add-rules file-path ethercat.rules text  
'alert ip any any -> any any (ethercat: 50E[5:5]; rev: 1;)'
```

13.4.7 Fanuc FOCAS

Для **Fanuc FOCAS** возможно задать правило обнаружения по следующим типам фильтрации:

- **ANY/NOT.**

Используется для задания общего условия срабатывания правила (**ANY** – любое значение, **NOT** – исключить указанное значение). Применяется как базовая метка для фильтрации пакетов без детализации содержимого.

Пример правил:

```
# Правило срабатывает на любой пакет протокола FOCAS:
admin@ngfwos:~$ suricata add-rules file-path focas.rules text 'alert tcp any
any -> any any (focas: ANY; rev: 1;)'

# Правило срабатывает, если пакет НЕ соответствует протоколу FOCAS:
admin@ngfwos:~$ suricata add-rules file-path focas.rules text 'alert tcp any
any -> any any (focas: NOT; rev: 1;)'
```

- **Направление (REQUEST / RESPONSE).**

Фильтрует пакеты по направлению: запрос (**REQUEST**) или ответ (**RESPONSE**).

Пример правил:

```
# Правило срабатывает на все запросы клиента:
admin@ngfwos:~$ suricata add-rules file-path focas.rules text 'alert tcp any any
-> any any (focas: REQUEST; rev: 1;)'
```

Фильтруются только запросы: **21 01** (команды), **11 01** (загрузка программы), **15 01** (скачивание программы). Возможность добавления новых значений реализована через модификацию исходного кода.

```
# Правило срабатывает на все ответы сервера:
admin@ngfwos:~$ suricata add-rules file-path focas.rules text 'alert tcp any any
-> any any (focas: RESPONSE; rev: 1;)'
```

Фильтруются только ответы: **21 02** (ответ на команды), **11 02** (подтверждение на загрузку), **15 02** (подтверждение на скачивание). Возможность добавления новых значений реализована через модификацию исходного кода.

- **Запрос (REQUEST).**

Позволяет фильтровать конкретные запросы по их числовому идентификатору, используя правило типа диапазон.

Пример правил:

```
# Фильтрация запроса 11 01 (загрузка программы):
admin@ngfwos:~$ suricata add-rules file-path focas.rules text 'alert tcp any any
-> any any (focas: REQUEST[4353:4353]; rev: 1;)'

# Фильтрация запроса 15 01 (скачивание программы):
admin@ngfwos:~$ suricata add-rules file-path focas.rules text 'alert tcp any any
-> any any (focas: REQUEST[5377:5377]; rev: 1;)'

# Фильтрация запроса 21 01 (команды к ЧПУ):
admin@ngfwos:~$ suricata add-rules file-path focas.rules text 'alert tcp any any
-> any any (focas: REQUEST[8449:8449]; rev: 1;)'
```

- **Ответ (RESPONSE).**

Позволяет фильтровать конкретные ответы по их числовому идентификатору, используя правило типа диапазон.

Пример правил:

```
# Фильтрация ответа 11 02 (подтверждение загрузки программы):
admin@ngfwos:~$ suricata add-rules file-path focas.rules text 'alert tcp any any
-> any any (focas: RESPONSE[4354:4354]; rev: 1;)'

# Фильтрация ответа 15 02 (подтверждение скачивания программы):
admin@ngfwos:~$ suricata add-rules file-path focas.rules text 'alert tcp any any
-> any any (focas: RESPONSE[5378:5378]; rev: 1;)'

# Фильтрация ответа 21 02 (ответы на команды от ЧПУ):
admin@ngfwos:~$ suricata add-rules file-path focas.rules text 'alert tcp any any
-> any any (focas: RESPONSE[8450:8450]; rev: 1;)'
```

- **Команда (FUNC).**

Позволяет фильтровать пакеты по конкретной команде, используя её числовой идентификатор или строковые параметры, такие как пути к файлам.

Пример правил:

```
# Фильтрация команды 00 01 00 B3 (список файлов/программ):
admin@ngfwos:~$ suricata add-rules file-path focas.rules text 'alert tcp any any
-> any any (focas: FUNC[65715:65715]; rev: 1;)'

# Фильтрация команды 00 01 80 01 (чтение регистра):
admin@ngfwos:~$ suricata add-rules file-path focas.rules text 'alert tcp any any
-> any any (focas: FUNC[98305:98305]; rev: 1;)'

# Фильтрация команды 00 01 00 30 (диагностические данные):
admin@ngfwos:~$ suricata add-rules file-path focas.rules text 'alert tcp any any
-> any any (focas: GETDIAG_START[918:918], GETDIAG_END[919:919],
GETDIAG_AXIS[1:1]; rev: 1;)'

# Фильтрация команды 00 01 00 B3 (список файлов/программ):
admin@ngfwos:~$ suricata add-rules file-path focas.rules text 'alert tcp any any
-> any any (focas: REaddir:"N://CNC_MEM/USER/TESTS", ARG4[1:1]; rev: 1;)'

# Фильтрация команды 00 01 00 B6 (удалить папку/файл/программу):
admin@ngfwos:~$ suricata add-rules file-path focas.rules text 'alert tcp any any
-> any any (focas: DELETE:"//CNC_MEM/USER/TESTS/O00000002"; rev: 1;)'

# Фильтрация команды 00 01 80 01 (чтение регистров):
admin@ngfwos:~$ suricata add-rules file-path focas.rules text 'alert tcp any any
-> any any (focas: READPMC_START[2204:2204], READPMC_END[2205:2205],
READPMC_MEMORY_TYPE[9:9], READPMC_DATA_TYPE[1:1]; rev: 1;)'
```

- **Аргументы команды (ARG1, ARG2...).**

Позволяет фильтровать аргументы команды, используя правила типа диапазон. Доступно до пяти аргументов. Возможно использоваться совместно с фильтром команд.

Пример правил:

```
# Фильтрация аргумента №N (где N — число от 1 до 5 включительно):  
admin@ngfwos:~$ suricata add-rules file-path focas.rules text 'alert tcp any any  
-> any any (focas: ARGN[1000:1000]; rev: 1;)'
```

```
# Фильтрация только части аргументов:  
admin@ngfwos:~$ suricata add-rules file-path focas.rules text 'alert tcp any any  
-> any any (focas: ARG3[9:9], ARG4[1:1]; rev: 1;)'
```

```
# Фильтрация всех 5 аргументов:  
admin@ngfwos:~$ suricata add-rules file-path focas.rules text 'alert tcp any any  
-> any any (focas: ARG1[1000:1000], ARG2[1002:1002], ARG3[9:9], ARG4[1:1],  
ARG5[0:0]; rev: 1;)'
```

Пример использования правила с командой:

```
# Фильтрация команды чтения регистров с конкретными аргументами:  
admin@ngfwos:~$ suricata add-rules file-path focas.rules text 'alert tcp any any  
-> any any (focas: FUNC[98305:98305], ARG1[1000:1000], ARG2[1002:1002],  
ARG3[9:9], ARG4[1:1], ARG5[0:0]; rev: 1;)'
```

Правило отфильтровывает пакеты с командой 00 01 80 01 (чтение регистров) и указанными аргументами. Для данной команды аргументы означают: «ARG1» – «Start Address», «ARG2» – «End Address», «ARG3» – «Memory Type», «ARG4» – «Data Type», «ARG5» – не используется.

13.4.8 GOOSE

Примечание:

Для включения записи событий срабатывания правил **COB** по протоколу **GOOSE** требуется включить запись уведомлений о срабатывании событий IDS/IPS в формате JSON. Включение выполняется в конфигурационном режиме с помощью следующей команды:

```
set suricata outputs eve-log enabled yes
```

Для настройки правил обнаружения трафика по протоколу **GOOSE** (IEC 61850-8-1), доступны следующие типы фильтрации:

- **ANY/NOT.**

Используется для задания общего условия срабатывания правила (**ANY** – любое значение, **NOT** – исключить указанное значение). Применяется как базовая метка для фильтрации пакетов без детализации содержимого.

Пример правил:

```
# правило срабатывает на любой пакет протокола GOOSE:
admin@ngfwos:~$ suricata add-rules file-path focas.rules text 'alert ip any any
-> any any (goose:ANY; msg:"GOOSE ANY"; sid:1; rev:1;)'
```

```
# Правило срабатывает, если пакет НЕ соответствует протоколу GOOSE:
admin@ngfwos:~$ suricata add-rules file-path focas.rules text 'alert ip any any
-> any any (goose:NOT; msg:"GOOSE NOT"; rev: 1;)'
```

При использовании метки **NOT**, возможны ложные срабатывания из-за особенностей обработки не TCP/IP трафика в **Suricata**. Метка **ANY** не вызывает ложных срабатываний.

- **Идентификатор приложения (APPID).**

Фильтрация пакетов по идентификатору приложения (**APPID**) с использованием правила типа диапазон.

Пример правил:

```
# Фильтрация по определённому APPID:
admin@ngfwos:~$ suricata add-rules file-path goose.rules text 'alert ip any any
-> any any (goose:APPID[1000:1000]; msg:"GOOSE APPID[1000:1000]"; rev: 1;)'
```

```
# Фильтрация по всем APPID в пределах указанного диапазона:
admin@ngfwos:~$ suricata add-rules file-path goose.rules text 'alert ip any any
-> any any (goose:APPID[:1000]; msg:"GOOSE APPID[:1000]"; rev: 1;)'
```

- **Значение атрибута «Dataset».**

Для фильтрации данных по атрибуту **DATSET** применяется правило следующего формата: **DATSET «Значение»**. Значение данного атрибута должно быть обязательным и содержать не более 150 символов. Он может включать в себя латинские буквы, пробелы, запятые и другие допустимые символы. Запрещается использование кавычек и непечатных символов.

Пример правил:

```
# Правило срабатывает при обнаружении GOOSE-сообщения, где атрибут  
DATSET равен "D063MLINCTRL/LLN0$DSAUV":  
admin@ngfwos:~$ suricata add-rules file-path goose.rules text 'alert ip any any  
-> any any (goose:DATSET "D063MLINCTRL/LLN0$DSAUV"; msg:"GOOSE  
DATSET"; rev: 1;)'
```

```
# Правило срабатывает при обнаружении GOOSE-сообщения, где атрибута  
DATSET равен "D058MPTRCTRL/LLN0$DSAUV":  
admin@ngfwos:~$ suricata add-rules file-path goose.rules text 'alert ip any any  
-> any any (goose:DATSET "D058MPTRCTRL/LLN0$DSAUV"; msg:"GOOSE  
DATSET"; rev: 1;)'
```

- **Значение атрибута «GoCBRef».**

Для фильтрации данных по атрибуту **GoCBRef** применяется правило следующего формата: **GOCBREF «Значение»**. Значение данного атрибута должно быть обязательным и содержать не более 150 символов.

Пример правил:

```
# Правило срабатывает при обнаружении GOOSE-сообщения, где атрибут  
GOCBREF равен "D063MLINCTRL/LLN0$GO$gcbB":  
admin@ngfwos:~$ suricata add-rules file-path goose.rules text 'alert ip any any  
-> any any (goose:GOCBREF "D063MLINCTRL/LLN0$GO$gcbB"; msg:"GOOSE  
GOCBREF"; rev: 1;)'
```

```
# Правило срабатывает при обнаружении GOOSE-сообщения, где атрибут  
GOCBREF равен "D058MPTRCTRL/LLN0$GO$gcbB":  
admin@ngfwos:~$ suricata add-rules file-path goose.rules text 'alert ip any any  
-> any any (goose:GOCBREF "D058MPTRCTRL/LLN0$GO$gcbB"; msg:"GOOSE  
GOCBREF"; rev: 1;)'
```

- **Значение атрибута «GoID»**

Для фильтрации данных по значению атрибута **GoID** применяется правило следующего формата: **GoID «Значение»**. Значение данного атрибута должно быть обязательным и содержать не более 150 символов.

Пример правил:

```
# Правило срабатывает при обнаружении GOOSE-сообщения, где атрибут  
GOID равен "D001ELINCTRL/LLN0$GO$gcbA":  
admin@ngfwos:~$ suricata add-rules file-path goose.rules text 'alert ip any any  
-> any any (goose:GOID "D001ELINCTRL/LLN0$GO$gcbA"; msg:"GOOSE GOID";  
rev: 1;)'
```

```
# Правило срабатывает при обнаружении GOOSE-сообщения, где атрибут  
GOID равен "gcbG":  
admin@ngfwos:~$ suricata add-rules file-path goose.rules text 'alert ip any any  
-> any any (goose:GOID "gcbG"; msg:"GOOSE GOID"; rev: 1;)'
```

- **Значение атрибута «t»** – относительно текущего времени (UTC).

Для фильтрации по значению атрибута «t» относительно текущего времени (UTC) применяется правило следующего формата: **CURR_DATE_TIME_DELTA[дельта]**. В данном контексте атрибут «дельта» должен быть заполнен и содержать корректную запись временной разницы. Запись атрибута «дельта» состоит из двух компонентов: количество секунд (положительное число от 1 до 9 цифр) и количество наносекунд (положительное число из 9 цифр), разделённых точкой, например: «1234.000000001».

Пример правил:

```
# Правило срабатывает при обнаружении GOOSE-сообщения с  
временным смещением 1234.000000001:  
admin@ngfwos:~$ suricata add-rules file-path goose.rules text 'alert ip any  
any -> any any (goose:CURR_DATE_TIME_DELTA[1234.000000001];  
msg:"goose CURR_DATE_TIME_DELTA"; rev: 1;)'
```

```
# Правило срабатывает при обнаружении GOOSE-сообщения с  
временным смещением 56780.000000001:  
admin@ngfwos:~$ suricata add-rules file-path goose.rules text 'alert ip any  
any -> any any (goose:CURR_DATE_TIME_DELTA[56780.000000001];  
msg:"goose CURR_DATE_TIME_DELTA"; rev: 1;)'
```

Правила срабатывают, если значение поля «t» выходит за пределы указанного интервала или является некорректным.

- **Значение атрибута «t»** – относительно заданного времени (UTC).

Для фильтрации данных по значению атрибута «t» относительно заданного времени (UTC) применяется правило следующего вида: **YYYYMMDDHHMMSS.SSSSSSSS_TIME_DELTA [время в указанном формате : дельта]**. Атрибуты времени в указанном формате и дельта

не могут быть пустыми и должны содержать корректно оформленные значения времени и временной разницы.

Формат записи атрибута времени включает в себя значение года, месяца, дня, часа, минуты и секунды заданного времени (14 символов), после чего через разделительный знак «.» указывается количество наносекунд (положительное число, состоящее из 9 цифр), например: «20191007120042.237304687».

Формат записи дельты состоит из количества секунд (положительное число, содержащее от 1 до 9 цифр), после которого через разделительный знак «.» указывается количество наносекунд (положительное число, состоящее из 9 цифр), например: «1234.000000001».

Пример правил:

```
# Правило срабатывает при обнаружении GOOSE-сообщения с меткой
времени 20191016142511.595703125 и допуском 0.005 сек:
admin@ngfwos:~$ suricata add-rules file-path goose.rules text 'alert ip any
any                                ->                                any                                any
(goose:YYYYMMDDHHMMSS_SSSSSSSSS_TIME_DELTA[20191016142511.5
95703125:0.005000000]);                                                msg:"goose
YYYYMMDDHHMMSS_SSSSSSSSS_TIME_DELTA"; rev: 1;)'

# Правило срабатывает при обнаружении GOOSE-сообщения с меткой
времени 20190925124044.148437500 и допуском 0.002003 сек:
admin@ngfwos:~$ suricata add-rules file-path goose.rules text 'alert ip any
any                                ->                                any                                any
(goose:YYYYMMDDHHMMSS_SSSSSSSSS_TIME_DELTA[20190925124044.1
48437500:0.002003000]);                                                msg:"goose
YYYYMMDDHHMMSS_SSSSSSSSS_TIME_DELTA"; rev: 1;)'

# Правило срабатывает при обнаружении GOOSE-сообщения с
меткой времени 20190925124044.148437500 и большим допуском
86400.002 сек:
admin@ngfwos:~$ suricata add-rules file-path goose.rules text 'alert ip any
any                                ->                                any                                any
(goose:YYYYMMDDHHMMSS_SSSSSSSSS_TIME_DELTA[20190925124044.1
48437500:86400.002000000]);                                                msg:"goose
YYYYMMDDHHMMSS_SSSSSSSSS_TIME_DELTA"; rev: 1;)'
```

Правила срабатывают, если значение поля «t» выходит за пределы указанного интервала или является некорректным.

13.4.9 IEC 60870-5-104

Стандарт – ГОСТ Р МЭК 60870-5-104-2004.

Сообщения по протоколу IEC 60870-5-104 могут быть определены по типу пакета:

- полный APDU;
- для целей управления – только поля APCI.

При классификации по типу пакета APCI возможен выбор формата пакета:

- **любой**;
- **«U-format (unnumbered control functions)»** – функции управления без нумерации;
- **«S-format (numbered supervisory functions)»** – функции контроля с нумерацией.

При классификации по типу пакета ASDU возможно задание:

- диапазона разрешённых входящих пакетов (RX);
- диапазона разрешённых исходящих пакетов (TX);
- типа данных ASDU;
- COT (Cause of Transmission) – причины передачи;
- AD – ASDU адреса (условие).

Возможно задать правила для полей объектов информации:

- **IOA** – адрес (диапазон);
- **IOA_V** – значение (целые числа) (условие);
- **VALUE** – значение (целые и дробные числа) (условие и диапазон);
- **QDS, SP_QDS, DP_QDS** – описатели качества;
- **SINGLE_CMD, DOUBLE_CMD** – одиночная команда, двойная команда;
- **QLF, QLF_COUNTER, QLF_MEASURED** – квалификатор;
- **CP16TIME, CP24TIME, CP56TIME, CP56TIME_BEGIN, CP56TIME_END** – метки времени;
- **FILE** – для файловых типов данных;
- **COI** – причина инициализации;
- **VTI** – значение с индикацией переходного состояния (с поддержкой отрицательных чисел);
- **SEP_SINGLE** – одиночное событие релейной защиты.

В том числе с помощью типизированных правил:

- IOA_V SIQ;
- QDS, QDP, SIQ, SEP, OCI.

13.4.10 KRUG

Для реализации фильтрации сетевых пакетов по значениям определённых полей протокола **KRUG** используется правило типа диапазон. Поддерживаются следующие поля и диапазоны значений:

- **Поле «COMMAND»** - диапазон значений [0:255].

Пример правила:

```
# Правило срабатывает при COMMAND = 0:
admin@ngfwos:~$ suricata add-rules file-path krug.rules text 'alert
udp any any -> any any (krug_pc_ctr_ip: COMMAND[0:0]; rev: 1;)'
```

- **Поле «CMD»** - диапазон значений [0:255].

Пример правила:

```
# Правило срабатывает при CMD = 2:
admin@ngfwos:~$ suricata add-rules file-path krug.rules text 'alert
udp any any -> any any (krug_pc_ctr_ip: CMD[2:2]; rev: 1;)'
```

- **Поле «PORT»** - диапазон значений [0:65535].

Пример правила:

```
# Правило срабатывает при PORT = 5:
admin@ngfwos:~$ suricata add-rules file-path krug.rules text 'alert
udp any any -> any any (krug_pc_ctr_ip: PORT[5:5]; rev: 1;)'
```

- **Поле «ACCESS»** - диапазон значений [0:65535].

Пример правила:

```
# Правило срабатывает при ACCESS = 15:
admin@ngfwos:~$ suricata add-rules file-path krug.rules text 'alert
udp any any -> any any (krug_pc_ctr_ip: ACCESS[15:15]; rev: 1;)'
```

- **Поле «MODE»** - диапазон значений [0:65535].

Пример правила:

```
# Правило срабатывает при MODE = 21:
admin@ngfwos:~$ suricata add-rules file-path krug.rules text 'alert
udp any any -> any any (krug_pc_ctr_ip: MODE[21:21]; rev: 1;)'
```

- **Поле «ERRCODE»** - диапазон значений [0:65535].

Пример правила:

```
# Правило срабатывает при ERRCODE = 33:  
admin@ngfwos:~$ suricata add-rules file-path krug.rules text 'alert  
udp any any -> any any (krug_pc_ctr_ip: ERRCODE[33:33]; rev: 1;)'
```

Пример комбинированного правила:

```
# Правило срабатывает при наличии COMMAND=0 , CMD=2 и ERRCODE=33 в  
одном пакете:  
admin@ngfwos:~$ suricata add-rules file-path krug.rules text 'alert udp any any ->  
any any (krug_pc_ctr_ip: COMMAND[0:0], CMD[2:2], ERRCODE[33:33]; rev: 1;)'
```

13.4.11 MMS

Стандарт – IEC 61850-8-1.

Сообщения по протоколу MMS разделяются по типу сообщения. При создании правил для протокола MMS возможно использовать следующие типы сообщений:

- **«CANCEL_REQUEST»;**
- **«CANCEL_RESPONSE»;**
- **«CANCEL_ERROR»;**
- **«CONFIRMED_REQUEST»;**
- **«CONFIRMED_RESPONSE»;**
- **«CONFIRMED_ERROR»;**
- **«UNCONFIRMED»;**
- **«REJECT»;**
- **«INITIATE_REQUEST»;**
- **«INITIATE_RESPONSE»;**
- **«INITIATE_ERROR»;**
- **«CONCLUDE_REQUEST»;**
- **«CONCLUDE_RESPONSE»;**
- **«CONCLUDE_ERROR».**

При использовании типа сообщения «CONFIRMED_REQUEST» возможно задать типы используемых служб, которые приведены в таблице (см. [Таблица «Доступные типы служб»](#)).

Таблица «Доступные типы служб»

Значение	Значение
STATUS	KILL
GETNAMELIST	GETPROGRAMINVOCATIONATTRIBUTES
IDENTIFY	OBTAINFILE
RENAME	DEFINEEVENTCONDITION
READ	DELETEEVENTCONDITION
WRITE	GETEVENTCONDITIONATTRIBUTES
GETVARIABLEACCESSATTRIBUTES	REPORTEVENTCONDITIONSTATUS
DEFINENAMEDVARIABLE	ALTEREVENTCONDITIONMONITORING
DEFINESCATTEREDACCESS	TRIGGEREVENT
GETSCATTEREDACCESSATTRIBUTES	DEFINEEVENTACTION
DELETEVARIABLEACCESS	DELETEEVENTACTION
DEFINENAMEDVARIABLELIST	GETEVENTACTIONATTRIBUTES
GETNAMEDVARIABLELISTATTRIBUTES	REPORTEVENTACTIONSTATUS
DELETENAMEDVARIABLELIST	DEFINEEVENTENROLLMENT
DEFINENAMEDTYPE	DELETEEVENTENROLLMENT
GETNAMEDTYPEATTRIBUTES	ALTEREVENTENROLLMENT
DELETENAMEDTYPE	REPORTEVENTENROLLMENTSTATUS
INPUT	GETEVENTENROLLMENTATTRIBUTES
OUTPUT	ACKNOWLEDGEEVENTNOTIFICATION
TAKECONTROL	GETALARMSUMMARY
RELINQUISHCONTROL	GETALARMENROLLMENTSUMMARY
DEFINESEMAPHORE	READJOURNAL
DELETESEMAPHORE	WRITEJOURNAL
REPORTSEMAPHORESTATUS	INITIALIZEJOURNAL
REPORTPOOLSEMAPHORESTATUS	REPORTJOURNALSTATUS
REPORTSEMAPHOREENTRYSTATUS	CREATEJOURNAL
INITIATEDOWNLOADSEQUENCE	DELETEJOURNAL
DOWNLOADSEGMENT	GETCAPABILITYLIST
TERMINATEDOWNLOADSEQUENCE	FILEOPEN

Значение	Значение
INITIATEUPLOADSEQUENCE	FILEREAD
UPLOADSEGMENT	FILECLOSE
TERMINATEUPLOADSEQUENCE	FILERENAME
REQUESTDOMAINDOWNLOAD	FILEDELETE
REQUESTDOMAINUPLOAD	FILEDIRECTORY
LOADDOMAINCONTENT	ADDITIONALSERVICE
STOREDOMAINCONTENT	GETDATAEXCHANGEATTRIBUTES
DELETEDOMAIN	EXCHANGEDATA
GETDOMAINATTRIBUTES	DEFINEACCESSCONTROLLIST
CREATEPROGRAMINVOCATION	GETACCESSCONTROLLISTATTRIBUTES
DELETEPROGRAMINVOCATION	REPORTACCESSCONTROLLEDOBJECTS
START	DELETEACCESSCONTROLLIST
STOP	CHANGEACCESSCONTROL
RESUME	RECONFIGUREPROGRAMINVOCATION
RESET	

При использовании в правиле типа службы «ADDITIONALSERVICE» возможно указать типы дополнительного сервиса, представленные в таблице (см. [Таблица «Типы дополнительного сервиса»](#)).

Таблица «Типы дополнительного сервиса»

Значение	Значение
VMDSTOP	GETUCATTRIBUTES
VMDRESET	LOADUCFROMFILE
SELECT	STOREUCTOFILE
ALTERPI	DELETEUC
INITIATEUCLOAD	DEFINEECL
UCLOAD	DELETEECL
UCUPLOAD	ADDECLREFERENCE
STARTUC	REMOVEECLREFERENCE
STOPUC	GETECLATTRIBUTES
CREATEUC	REPORTDECLSTATUS

ADDTouc	ALTERECLMONITORING
REMOVEFROMUC	

При использовании в правиле типа службы «READ» возможно указать следующие параметры:

- **«Item ID запроса чтения»**. Максимальное количество символов - «32».
- **«Domain ID запроса чтения»**. Максимальное количество символов - «32».
- **«Адрес запроса чтения»**. Максимальное количество символов - «32».

При использовании в правиле типа службы «WRITE» возможно указать следующие параметры:

- **«Item ID запроса записи»**. Максимальное количество символов - «32».
- **«Domain ID запроса записи»**. Максимальное количество символов - «32».

Примеры правил:

```
#Правило с фильтрацией запроса чтения по адресу
admin@ngfwos:~$ suricata add-rules file-path mms.rules text 'alert tcp any any ->
any any (mms:READADDRESS "Bilateral_Table_ID"; msg:"MMS Read"; sid: 1; rev: 1;)
alert tcp any any -> any any (mms:READADDRESS "400"; msg:"MMS Read"; sid: 2; rev:
1;)'

#Правило с фильтрацией запроса по имени переменной
suricata add-rules file-path mms.rules text 'alert tcp any any -> any any (mms:WRITE
"CITEC_TS0"@ "KIRKLAND"; msg:"MMS Write"; sid: 1; rev: 1;) alert tcp any any -> any
any (mms:WRITE "EMSICCP_TS0"@ "BELLEVUE"; msg:"MMS Write"; sid: 2; rev: 1;)'
```

13.4.12 Modbus TCP

Стандарт – MODBUS Application Protocol Specification V1.1b3.

Для сообщений по протоколу Modbus TCP можно задать правило обнаружения на основе признака совпадения:

- свойство функции – код или категория функции;
- тип доступа к данным – тип доступа и основная модель данных;
- диапазон функции – ввод кода функции, адреса и значения переменной вручную.

При обнаружении по свойству функции возможно задать дополнительные опции:

- используемую функцию, подфункцию;
- категорию кодов функции.

В качестве кодов функции возможно указать следующие значения:

- «01:Read Coils»;
- «02:Read Discrete Inputs»;
- «03:Read Holding Register»;
- «04:Read Input Register»;
- «05:Write Single Coil»;
- «07:Read Exception Status»;
- «08:Diagnostic»;
- «0B:Get Com event counter»;
- «0C:Get Com Event Log»;
- «0F:Write Multiple Coils»;
- «10:Write Multiple Registers»;
- «11:Report Server ID»;
- «14:Read File record»;
- «15:Write File record»;
- «16:Mask Write Register»;
- «17:Read/Write Multiple Registers»;
- «18:Read FIFO queue».

Категории кодов функции:

- назначенная – коды функций, которые определены в Modbus спецификации;
- неназначенная – общедоступная, стандартные и организационные коды;
- пользовательская – два диапазона кодов, для которых возможно назначить произвольную функцию;
- зарезервированная – коды функций, не являющихся стандартными;
- все категории.

При классификации по доступу к данным возможно задать следующие дополнительные опции:

- тип доступа к данным – записать или считать;

Модель данных:

- «Регистры флагов (Coils)» – битовые данные, доступ чтение/запись;
- «Регистры хранения (Holding Registers)» – 16 битовые данные, доступ чтение/запись;

- «**Дискретные входы (Discrete Inputs)**» – битовые данные, доступ чтение;
- «**Регистры ввода (Input Registers)**» – 16 битовые данные, доступ чтение.

Примеры правил:

```
#Правило для фильтрации по значению
admin@ngfwos:~$ suricata add-rules file-path modbus.rules text 'alert tcp any any
<> any 502 (modbus2:VAL[0:300]; msg:"Modbus VAL[0:300]"; sid:5; rev:1;)'

#Правило для фильтрации по номеру функции
admin@ngfwos:~$ suricata add-rules file-path modbus.rules text 'alert tcp any any
<> any 502 (modbus2:FUNC[1:2]; msg:"Modbus FUNC[1:2]"; sid:5; rev:1;)'
```

13.4.13 OPC DA (только L3/IP Layer)

Фильтрация по протоколу OPC DA поддерживается только по IP Layer.

Сообщения по протоколу **OPC DA** разделяются по типу сообщения:

- REQUEST;
- PING;
- RESPONSE;
- FAULT;
- WORKING;
- NOCALL;
- REJECT;
- ACK;
- CI_CANCEL;
- FACK;
- CANCEL_ACK;
- BIND;
- BIND_ACK;
- BIND_NACK;
- ALTER_CONTEXT;
- ALTER_CONTEXT_RESP;
- SHUTDOWN;
- AUTH3;
- CO_CANCEL;

- ORPHANED.

При указании типа сообщения «REQUEST» возможно задать идентификатор вызываемого объекта и номер вызываемой функции объекта.

Поддерживается детектирование операций над тегом (по имени тега):

- Запись;
- Чтение.

13.4.14 OPC UA

Стандарт – IEC 62541.

Сообщения по протоколу OPC UA разделяются по типу сообщения:

- «**HELLO**» – маркер начала передачи данных между клиентом и сервером;
- «**ACKNOWLEDGE**» – ответ на сообщение типа HELLO;
- «**OPEN**» – открытие канала передачи данных с предложенным методом шифрования данных;
- «**MESSAGE**» – передаваемое сообщение;
- «**CLOSE**» – конец сессии.

При указании типа сообщения «**OPEN**» возможно задать политику безопасности. Допускается указание следующих политик:

- «**NONE**»;
- «**BASIC128RSA15**»;
- «**BASIC256**»;
- «**BASIC256SHA256**»;
- «**AES128_SHA256_RSAAEP**»;
- «**PUBSUB_AES128_CTR**»;
- «**PUBSUB_AES256_CTR**».

При указании типа сообщения «**MESSAGE**» возможно задать тип запроса. Допускается указание следующих типов запросов:

- «**FINDSERVERS**» - запрос известных серверов;
- «**FINDSERVERSONNETWORK**» - запрос известных работающих серверов;
- «**GETENDPOINTS**» - запрос на поддерживаемые сервером конечные точки;
- «**REGISTERSERVER**» - запрос на регистрацию сервера;
- «**REGISTERSERVER2**» - запрос на регистрацию сервера с дополнительной информацией для «**FINDSERVERSONNETWORK**»;

- «**CREATESESSION**» - запрос на создание сессии;
- «**ACTIVATESESSION**» - запрос на создание сессии (передача идентификационных данных клиента);
- «**CLOSESESSION**» - запрос на завершение сессии;
- «**CANCEL**» - запрос отмены невыполненных запросов на обслуживание;
- «**ADDNODES**» - запрос на добавление узла как дочерний в адресное пространство;
- «**ADDREFERENCES**» - запрос на добавление ссылки на узел;
- «**DELETENODES**» - запрос на удаление узла из адресного пространства;
- «**DELETEREFERENCES**» - запрос на удаление ссылки узла;
- «**BROWSE**» - запрос на просмотр узлов;
- «**BROWSENEXT**» - запрос на продолжение просмотра результата запроса BROWSE, если результат этого запроса превышает максимальное значение;
- «**TRANSLATEBROWSEPATHSTONODEIDS**» - запрос на преобразование пути узла в идентификатор узла;
- «**REGISTERNODES**» - запрос на регистрацию узла, например, узла, информация о котором пользователю известна;
- «**UNREGISTERNODES**» - запрос на отмену регистрации узла;
- «**QUERYFIRST**» - запрос просмотр данных из определённого экземпляра;
- «**QUERYNEXT**» - запрос на продолжение просмотра результата запроса «QUERYFIRST», если результат этого запроса превышает максимальное значение;
- «**READ**» - запрос на чтение данных;
- «**HISTORYREAD**» - запрос на просмотр значений или событий узлов;
- «**WRITE**» - запрос на изменение узла;
- «**HISTORYUPDATE**» - запрос на обновление значений или событий узлов;
- «**CALLMETHOD**» - запрос на получение результатов вызова удалённой процедуры;
- «**CALL**» - запрос на вызов удалённой процедуры;
- «**MONITOREDITEMCREATE**» - запрос на начало подписки на событие;
- «**CREATEMONITOREDITEMS**» - запрос на подписку на событие;
- «**MONITOREDITEMMODIFY**» - запрос на изменение параметров подписки на события;
- «**MODIFYMONITOREDITEMS**» - запрос на изменение подписки;

- «**SETMONITORINGMODE**» - запрос на установку режима подписки;
- «**SETTRIGGERING**» - запрос на создание связи между событием и узлом;
- «**DELETEMONITOREDITEMS**» - запрос на завершение подписки;
- «**CREATESUBSCRIPTION**» - запрос на создание подписки на событие;
- «**MODIFYSUBSCRIPTION**» - запрос на изменение подписки на событие;
- «**SETPUBLISHINGMODE**» - запрос на включение отправки уведомлений по подпискам на событие;
- «**PUBLISH**» - запрос на подтверждение получения уведомлений по подпискам на события;
- «**REPUBLISH**» - запрос на повторную отправку уведомлений по подпискам на события;
- «**TRANSFERSUBSCRIPTIONS**» - запрос на передачу подписки на событие из одной сессии в другую;
- «**DELETESUBSCRIPTIONS**» - запрос на удаление подписки на событие.

При использовании типов запроса «**BROWSE**» и «**READ**» в качестве типа запроса возможно указание типа идентификатора узла и идентификатор пространства имён.

При использовании типа запроса «**WRITE**» в качестве типа запроса возможно указание идентификатора пространства имён, типа идентификатора узла и типа значений.

При использовании типа запроса «**CALL**» в качестве типа запроса возможно указание типа идентификатора узла вызываемого объекта и типа идентификатора узла вызываемого метода.

Примеры правил:

```
#Правило с указанием GUID с меткой ReadNode для GUID-идентификаторов
admin@ngfwos:~$ suricata add-rules file-path opc_ua.rules text 'alert tcp any any -
> any any (opc_ua:ReadNode guid C496578A-0DFE-4B8F-870A-745238C6AEAE;
sid:1; rev:1;)'

#Правило для просмотра узлов типа диапазон с меткой BrowseNode для
целочисленных идентификаторов
admin@ngfwos:~$ suricata add-rules file-path opc_ua.rules text 'alert tcp any any -
> any any (opc_ua:BrowseNode[10:10]; sid:1; rev:1;)'
```

13.4.15 S7comm

Стандарт протокола связи коммуникационных модулей серий Siemens SIMATIC S7-300/400.

В качестве типа сообщения при создании правила возможно использовать следующие типы:

- «**JOBREQUEST**» - пакет с запросом на выполнение функции;
- «**ACK**» - пакет с результатом выполнения операции;
- «**ACKDATA**» - пакет с ответом на запрос;
- «**USERDATA**» - пакет с данными пользователя.

При использовании типа сообщения «JOBREQUEST» возможно указать следующие функции:

- «**CPUSERVICE**» - сервисы ЦП;
- «**SETUPCOMM**» - запрос на подключение к ПЛК;
- «**READVAR**» - запрос на чтение;
- «**WRITEVAR**» - запрос на запись;
- «**REQUESTDOWNLOAD**» - запрос на загрузку прошивки;
- «**DOWNLOADBLOCK**» - загрузка прошивки на ПЛК;
- «**DOWNLOADEND**» - запрос на завершение загрузки прошивки на ПЛК;
- «**STARTUPLOAD**» - запрос на выгрузку прошивки;
- «**UPLOAD**» - выгрузка прошивки с ПЛК;
- «**ENDUPLOAD**» - окончание выгрузки прошивки с ПЛК;
- «**PLCCONTROL**» - управление ПЛК;
- «**PLCSTOP**» - остановка ПЛК;
- «**ANY**».

При использовании функции «READVAR» или «WRITEVAR» возможно указать типы области, представленные в таблице (см. [Таблица «Типы области»](#)).

Таблица «Типы области»

Тип области	Описание
ANY	Любая область чтения
SI (System info)	Системная информация
SF (System flags)	Системные флаги
AI (Аналоговые входы)	Аналоговые входы
AO (Аналоговые выходы)	Аналоговые выходы
C (Counters)	Счётчики
T (Timers)	Таймеры

Тип области	Описание
IC (IEC Counters)	Счётчики IEC
IT (IEC Timers)	Таймеры IEC
P (Direct peripheral access)	Прямой доступ к периферии
I (Inputs)	Ввод
Q (Outputs)	Вывод
M (Flags)	Флаги
DB (Data blocks)	Блоки данных
DI (Instance data blocks)	Блоки данных экземпляра
LV (Local data)	Локальные данные

При использовании в качестве типа области любого значения, кроме значения «any», дополнительно возможно указать:

- «Имя области»;
- «Тип данных»;
- «Количество данных»;
- «Смещение данных».

Имя области принимает значения от «0» до «65535».

В качестве значения для типа данных доступны типы данных, представленные в таблице (см. [Таблица «Доступные типы данных»](#)).

Таблица «Доступные типы данных»

Значение	Значение	Значение
BIT	DINT	DATETIME
BYTE	REAL	COUNTER
CHAR	DATE	TIMER
WORD	TOD	IECTIMER
INT	TIME	IECCOUNTER
DWORD	S5TIME	HSCOUNTER

В качестве значения для количества данных возможно указать значения от «0» до «65535».

В качестве значения для смещения данных возможно указать целочисленное значение в шестнадцатеричной системе счисления в формате «0x000000».

При использовании в правиле функции «WRITEVAR» и любого значения типа области, кроме значения «any», возможно задать дополнительные параметры:

- «**Тип передаваемого значения**»;
- «**Количество передаваемых данных**»;
- «**Список значений данных**».

Для типа передаваемого значения доступны следующие типы значений:

- «**NULL**» - не выбрано;
- «**BIT**» - значение в битах;
- «**BYTE**» - значение в байтах;
- «**INT**» - целочисленное значение;
- «**REAL**» - вещественное;
- «**STR**» - строковое значение.

В качестве списка значений данных возможно указать список значений в шестнадцатеричной системе счисления.

При использовании в правиле функций «REQUESTDOWNLOAD», «DOWNLOADBLOCK», «STARTUPLOAD» возможно задать тип блока, номер блока и целевую файловую систему.

Возможно задать следующие типы блока:

- «**OB**» - организационный блок, хранит главные программы;
- «**DB**» - блок данных, хранит необходимые для ПЛК программ данные;
- «**SDB**» - блок данных системы, хранит необходимые для ПЛК программ данные;
- «**FC**» - функция, функции без состояния - не имеют собственной памяти, могут быть запущены из других программ;
- «**SFC**» - системная функция, функции без состояния - не имеют собственной памяти, могут быть вызваны из других программ;
- «**FB**» - блок функции, функции с состоянием, обычно имеют ассоциированный SDB;
- «**SFB**» - блок системной функции, функции с состоянием, обычно имеют ассоциированный SDB;
- «**ANY**».

Номер блока принимает значения от «0» до «99999».

В качестве значения целевой файловой системы доступны две опции:

- «**P**» - пассивная, блок требует активации после скачивания;

- «**A**» - активная, блок будет активизирован после скачивания.

При использовании в правиле функции «PLCCONTROL» возможно задать следующие функции управления ПЛК:

- «**ANY**»;
- «**INSE**» - активация скачанного блока, параметром выступает имя блока;
- «**DELE**» - удаление блока, параметром выступает имя блока;
- «**PPROGRAM**» - запуск программы, параметром выступает имя программы;
- «**GARB**» - сжатие памяти;
- «**MODU**» - копирование RAM в ROM, параметр содержит идентификаторы файловой системы A/E/P;
- «**OFF**» - выключение ПЛК;
- «**ON**» - включение ПЛК.

Примеры правил:

```
#Правило для запроса загрузки блока (STARTUPLOAD)
admin@ngfwos:~$ suricata add-rules file-path s7com.rules text 'alert tcp any any ->
any any (s7com:Upload SFC00000P; sid:1; rev:1;)'

#Правило для запроса скачивания блока (REQUESTDOWNLOAD,
DOWNLOADBLOCK)
admin@ngfwos:~$ suricata add-rules file-path s7com.rules text 'alert tcp any any ->
any any (s7com:Download SFC00000P; sid:1; rev:1;)'
```

13.4.16 S7comm Plus

Стандарт протокола связи коммуникационных модулей серий Siemens SIMATIC S7-1200 и S7-1500.

Сообщения по протоколу S7comm Plus разделяются по типу сообщения:

- «**REQUEST**»;
- «**RESPONSE**»;
- «**NOTIFY**»;
- «**RESPONSE2**».

По типу взаимодействия:

- «**CONNECT**»;
- «**DATA**»;
- «**DATAFW1_5**»;

- «**KEEPALIVE**»;
- «**EXT_KEEPALIVE**».

По функции:

- «**EXPLORE**»;
- «**CREATEOBJECT**»;
- «**DELETEOBJECT**»;
- «**SETVARIABLE**»;
- «**GETLINK**»;
- «**SETMULTIVAR**»;
- «**GETMULTIVAR**»;
- «**BEGINSEQUENCE**»;
- «**ENDSEQUENCE**»;
- «**INVOKE**»;
- «**GETVARSUBSTR**».

При использовании функции «**EXPLORE**» возможно указать диапазоны для параметров «EXPLORE_AREA» и «EXPLORE_ATTR_ID».

При использовании функции «**CREATEOBJECT**» возможно указать диапазон для параметра «CREATEOBJECT_ATTR_ID».

При использовании функции «**DELETEOBJECT**» возможно указать диапазоны для параметров «DELETEOBJECT_OBJ_ID» и «DELETEOBJECT_ATTR_ID».

При использовании функции «**GETLINK**» возможно указать диапазон для параметра «GETLINK_ATTR_ID».

При использовании функции «**SETMULTIVAR**» возможно указать диапазон для параметра «SETMULTIVAR_ATTR_ID».

При использовании функции «**GETMULTIVAR**» возможно указать диапазон для параметра «GETMULTIVAR_ATTR_ID».

При использовании функции «**GETVARSUBSTR**» возможно указать диапазон для параметра «GETVARSUBSTR_ATTR_ID».

Примеры правил:

```
#Правило для фильтрации по идентификаторам атрибутов сообщения типа  
CREATEOBJECT с диапазоном с меткой CREATEOBJECTATTRID  
admin@ngfwos:~$ suricata add-rules file-path s7com_plus.rules text 'alert tcp any  
any <> any any (s7com_plus:CREATEOBJECT_ATTR_ID[233:233]; msg:"S7COMPLUS  
createobject"; sid:1; rev:1;)'
```

```
#Правило для указания функции GETLINK  
admin@ngfwos:~$ suricata add-rules file-path s7com_plus.rules text 'alert tcp any  
any <> any any (s7com_plus:GETLINK; msg:"S7COMPLUS GETLINK"; sid:1; rev:1;)'
```

13.4.17 UMAS

Основан на протоколе Xway Unite. Протокол Umas используется для настройки и мониторинга ПЛК Schneider-Electric.

Сообщения по протоколу UMAS разделяются по функциям:

- **«INIT_COMM»** - инициализация UMAS сессии;
- **«READ_ID»** - запрос ПЛК ID;
- **«READ_PROJECT_INFO»** - чтение информации о проекте;
- **«READ_PLC_INFO»** - чтение внутренней информации ПЛК;
- **«READ_CARD_INFO»** - чтение информации о внутренней SD карты ПЛК;
- **«REPEAT»** - отправить информацию обратно ПЛК. Используется для синхронизации;
- **«TAKE_PLC_RESERVATION»** - назначить ПЛК владельца;
- **«RELEASE_PLC_RESERVATION»** - снять владельца ПЛК;
- **«KEEP_ALIVE»** - поддержка активного соединения;
- **«READ_MEMORY_BLOCK»** - чтение блока памяти с ПЛК;
- **«READ_VARIABLES»** - чтение системных битов, системных слов и переменных;
- **«WRITE_VARIABLES»** - запись системных битов, системных слов и переменных;
- **«READ_COILS_REGISTERS»** - чтение coils и регистров с ПЛК;
- **«WRITE_COILS_REGISTERS»** - запись катушек и регистров в ПЛК;
- **«INITIALIZE_UPLOAD»** - инициализация загрузки (копирования с инженерного ПК на ПЛК);
- **«UPLOAD_BLOCK»** - загрузка блока данных с инженерного ПК на ПЛК;

- **«END_STRATEGY_UPLOAD»** - завершение загрузки (копирования с инженерного ПК на ПЛК);
- **«INITIALIZE_DOWNLOAD»** - инициализация скачивания (копирования с ПЛК на инженерный ПК);
- **«DOWNLOAD_BLOCK»** - скачивание блока данных с ПЛК на инженерный ПК;
- **«END_STRATEGY_DOWNLOAD»** - конец скачивания (копирования с ПЛК на инженерный ПК);
- **«READ_ETH_MASTER_DATA»** - чтение Ethernet Master Data;
- **«START_PLC»** - включение ПЛК;
- **«STOP_PLC»** - выключение ПЛК;
- **«MONITOR_PLC»** - мониторинг системных битов, системных слов и переменных;
- **«CHECK_PLC»** - проверка статуса подключения ПЛК;
- **«READ_IO_OBJECT»** - чтение IO объекта;
- **«WRITE_IO_OBJECT»** - запись IO объекта;
- **«GET_STATUS_MODULE»** - получение статуса модуля.

Параметр **«Информация о проекте»** принимает значения от «0» до «65535» или диапазон значений.

В качестве значения типа сообщения доступны два типа сообщений:

- **«REQ»** - запрос;
- **«RES»** - ответ.

При использовании функции **«READ_MEMORY_BLOCK»** возможно указать дополнительные параметры:

- **«Номер блока»** - принимает значения от «0» до «65535» или диапазон значений;
- **«Количество данных»** - принимает значения от «0» до «65535» или диапазон значений;
- **«Смещение»** - принимает значения от «0» до «65535» или диапазон значений.

При использовании функции **«READ_VARIABLES»** возможно указать дополнительные параметры:

- **«Базовое смещение»** - принимает значения от «0» до «65535» или диапазон значений;

- **«Относительное смещение»** - принимает значения от «0» до «65535» или диапазон значений;
- **«Номер блока»**;
- **«Количество значений»** - принимает значения от «0» до «65535» или диапазон значений;
- **«Тип значений»**.

Для типа значений доступны три типа значений:

- **«BIT»**;
- **«WORD»**;
- **«DWORD»**.

При использовании функции «WRITE_VARIABLES» возможно использовать дополнительные параметры:

- **«Номер блока»**;
- **«Смещение»**;
- **«Тип значений»**;
- **«Значение»** - принимает значения от «0» до «65535» или диапазон значений.

При использовании функций «READ_COILS_REGISTERS» и «WRITE_COILS_REGISTERS» возможно указать дополнительные параметры:

- **«Условие (значение)»** - только для «WRITE_COILS_REGISTERS»;
- **«Номер регистров флагов (Coils)»** - принимает значения от «0» до «65535» или диапазон значений;
- **«Смещение»**;
- **«Тип значений»**.

Примеры правил:

```
#Правило для фильтрации по номеру блока команды READ_MEMORY_BLOCK с диапазоном с меткой RMB_BLOCK
admin@ngfwos:~$ suricata add-rules file-path umas.rules text 'alert tcp any any -> any 502 (umas:RMB_BLOCK[10:10]; sid:1; rev:1;)'

#Правило для фильтрации по количеству данных команды READ_MEMORY_BLOCK с диапазоном с меткой RMB_BYTES
admin@ngfwos:~$ suricata add-rules file-path umas.rules text 'alert tcp any any -> any 502 (umas:RMB_BYTES[10:10]; sid:1; rev:1;)'
```

13.5 Просмотр журнала событий IDS/IPS

Для просмотра всех событий системы **IDS/IPS** из глобального журнала в локальном консольном интерфейсе необходимо ввести в эксплуатационном режиме команду (см. [Рисунок – Журнал системы IDS/IPS](#)):

```
admin@ngfwos:~$ show logging idps
```

```
admin@ngfwos:~$ show logging idps
18.10.2024 11:01:04 1729249264890096 ngfwos idps-rule[4490]: [4490] <Notice> -- Threads created -> RX: 2 W: 4 FM: 1 FR
: 1 Engine started.
18.10.2024 11:01:23 1729249283505508 ngfwos idps-rule[4490]: [4490] <Notice> -- Signal Received. Stopping engine.
18.10.2024 11:16:33 1729250193730732 ngfwos idps-rule[6077]: [6077] <Notice> -- Threads created -> RX: 2 W: 4 FM: 1 FR
: 1 Engine started.
18.10.2024 11:16:42 1729250202281663 ngfwos idps-rule[6077]: [1:2100197:4] ICMP [Classification: Misc activity] [Prior
ity: 3] {IPv6-ICMP} fe80:0000:0000:0000:a6a9:30ff:fe7d:7b40:134 -> ff02:0000:0000:0000:0000:0000:0000:0001:133
18.10.2024 11:17:03 1729250223550980 ngfwos idps-rule[6077]: [1:2100197:4] ICMP [Classification: Misc activity] [Prior
ity: 3] {ICMP} 192.168.10.184:8 -> 192.168.10.165:0
18.10.2024 11:17:03 1729250223555653 ngfwos idps-rule[6077]: [1:2100197:4] ICMP [Classification: Misc activity] [Prior
ity: 3] {ICMP} 192.168.10.184:8 -> 192.168.10.165:0
18.10.2024 11:17:03 1729250223556951 ngfwos idps-rule[6077]: [1:2100197:4] ICMP [Classification: Misc activity] [Prior
ity: 3] {ICMP} 192.168.10.184:8 -> 192.168.10.165:0
```

Рисунок – Журнал системы IDS/IPS

Журнал событий системы **IDS/IPS** возможно отфильтровать с помощью дополнительных фильтров:

- **engine** - вывод событий запуска Suricata:

```
admin@ngfwos:~$ show logging idps engine [class <> | level <>]
```

- **rules** - вывод событий срабатывания правил Suricata согласно настройкам ведения журнала (по умолчанию используется уровень «notice»):

```
admin@ngfwos:~$ show logging idps rules [class <> | level <>]
```

- **server** - вывод событий, связанных с настройками Suricata:

```
admin@ngfwos:~$ show logging idps server [class <> | level <>]
```

- **update-rules** - вывод событий, связанных с обновлением правил Suricata:

```
admin@ngfwos:~$ show logging idps update-rules [class <> | level <>]
```

Подробное описание дополнительных фильтров «**class**» и «**level**» представлено в разделе «Логирование» настоящего руководства (см. [Просмотр глобального журнала](#)).

13.6 Настройка интерфейса для анализа зеркального трафика (SPAN) в COB

При использовании системы **ARMA Стена** в качестве точки приёма зеркального трафика (**SPAN**) для его последующего анализа с помощью службы **Suricata** требуется включить на соответствующем сетевом интерфейсе **смешанный (promiscuous) режим**. Данный режим позволяет сетевому интерфейсу принимать все кадры, проходящие по сегменту сети, включая те, которые не адресованы

устройству напрямую – что является необходимым условием для корректного анализа зеркалированного трафика.

Для активации смешанного режима необходимо выполнить следующие действия:

Перейти в учётную запись суперпользователя:

```
admin@ngfwos:~$ sudo -i  
root@ngfwos:~#
```

Включить promiscuous-режим на интерфейсе, принимающем зеркальный трафик (например, ethX, где X – идентификатор интерфейса):

```
root@ngfwos:~# ifconfig ethX promisc
```

Примечание:

Указанная настройка носит временный характер и не сохраняется после перезагрузки устройства. В случае перезапуска системы **ARMA Стена** необходимо повторно включать смешанный режим на соответствующем интерфейсе.

Смешанный режим является обязательным для корректной работы **Suricata** в конфигурации, основанной на анализе зеркалированного трафика, поскольку без него сетевой интерфейс отбрасывает пакеты, не предназначенные ему по MAC-адресу, что делает невозможным полноценный сетевой мониторинг и обнаружение угроз.

14 КОНТРОЛЬ ПРИЛОЖЕНИЙ И ДОМЕНОВ

14.1 Контроль приложений

Служба **«Контроль приложений»** предназначена для фильтрации и ограничения использования сетевых приложений в трафике, проходящем через систему **ARMA Стена**. На основе заданных политик служба обеспечивает блокировку приложений по категориям, включая мессенджеры, социальные сети, облачные сервисы и другие типы приложений.

Функциональность реализована на базе системы **Suricata**, осуществляющей глубокий анализ сетевого трафика. Классификация приложений производится по сигнатурам и поведенческим шаблонам.

Фильтрация трафика с использованием службы **«Контроль приложений»** применяется исключительно к тем сетевым интерфейсам, которые включены в конфигурацию **Suricata** и для которых установлен режим захвата трафика **IPS**.

Примечание:

Перед активацией службы **«Контроль приложений»** требуется выполнить предварительную настройку **Suricata**: указать интерфейсы, подлежащие мониторингу, и установить для них режим захвата трафика **IPS**.

При использовании режима **IDS** на каком-либо интерфейсе фильтрация трафика посредством службы **«Контроль приложений»** на данном интерфейсе не производится.

Для отображения полного перечня доступных категорий приложений используется команда:

```
admin@ngfwos:~$ show app-control categories
```

Для просмотра списка приложений, входящих в конкретную категорию, применяется команда:

```
admin@ngfwos:~$ show app-control applications <категория>
```

где **<категория>** - имя категории.

Перечень поддерживаемых категорий и соответствующих им приложений приведён в таблице (см. [Таблица «Список приложений»](#)).

Таблица «Список приложений»

Наименование	Категория	Приложение
Искусственный интеллект	ai	deepseek
Букмекерские конторы	betting	winline

Наименование	Категория	Приложение
Облачные ресурсы	cloud	digital-ocean
CRM-системы	crm	bitrix24
Криптовалюты и кошельки	crypto	mining
Файлообменники	filehosting	1337x.tw 4shared Internxt-drive adrive bit-comet bit-torrent box-com dropsend e-donkey falcobrowser filecloud fileden filefactory filepost firestorage flash-get fotolub gnutella google-drive hightail jottacloud media-fire media-get mega my-files one-drive p-cloud sendanywhere sendspace smartfile soul-seek source-forge spider-oak sync-com transferbigfiles transferxl transfiles.ru vuze

Наименование	Категория	Приложение
		yandex-disk yunpan zona
Форумы и блоги	forums-and-blogs	geeksforgeeks pikabu
Онлайн-гемблинг	gambling	casino stoloto
Игровые платформы	games	battle-net ea epic fortnite gameasy gog riot rockstar steam ubi xbox
Системы управления версиями	git	github gitlab
Почтовые сервисы	mail	outlook yandex-mail
Карты и навигация	maps	2-gis google-maps
Маркетплейсы	marketplace	aliexpress wildberries
Мессенджеры	messenger	amazon-chime amo bop-up-messenger express-messenger ice-chat icq imoim rocket-chat skype tada-team tamtam tango team-speak telegram

Наименование	Категория	Приложение
		viber whatsapp xchat yandex-messenger zulip
Музыкальные стриминговые сервисы	music	spotify
Новостные ресурсы	news	abcnews new-york-post
Офисные приложения	office	google-docs
Прочие приложения	other	ads anonymizer anonymox archive-org astrology avira-update bootsnipp botnets c2c codesandbox croxyproxy delivery-club dodopizza dr-web-update edadeal elma365 fasts-tunnel free-proxy-list freemybrowser from-doc-to-pdf ghostery gismeteo gosuslugi hi-ru howtogeek ideone jsbin jsfiddle kaspersky-update kproxy kraken local-xpose

Наименование	Категория	Приложение
		microsoft-store miro nalog news ngrok npr online-video-converter packetriot page-kite pastebin pdf-drive phishing polycom portable-apps raketu smallpdf softonic speedify star-force stealthy-com symantec-update talk-me tapin-radio teletype trend-micro-update vexacion vpn-proxy-site w3schools ways-online word-press yandex-taxi yoomoney zerotier
Протоколы связи	protocols	ip-6-to-4 quic smb smtp syslog tftp xmpp
Удалённое управление	remote-control	1c-connect aeroadmin alpemix

Наименование	Категория	Приложение
		ammyy-admin anydesk get-screen jump-desktop log-me-in radmin simple-help sunlogin teleconsole ultra-viewer
Поисковые системы	search-engines	onion-search-engine rambler
Социальные сети	social	camfrog dating discord facebook fandom flickr g-mail-chat imgur intranetus mirapolis-virtual-room my-own-conference odnoklassniki tik-tok tumblr vkontakte whereby
Видеосвязь	vcs	clickmeeting free-conference-call go-meet-now google-meet mts-link true-conf video-grace web-ex yandex-telemost
Видеохостинги	video	adults-18 amediateka ivi megomult msn-video

Наименование	Категория	Приложение
		okko real-player rutube twitch y-2-mate youtube
VPN	vpn	123-vpn 1clickvpn beepass-vpn best-vpn-ssh browsec continent-ap cyber-ghost-vpn dot-vpn droid-vpn fly-vpn free-open-vpn hide-my-ip hola-vpn hoxx i-top-vpn openvpnssh systweak-vpn tcp-vpn thunder-vpn touch-vpn tuxler-vpn u-vpn ultra-vpn vpn-book vpn-city vpn-jantlt vpn-ki vpn-professional vpn-udp wireguard your-freedom-vpn
Сканеры уязвимостей	vuln-scanners	metasploit nmap

Активация службы «**Контроль приложений**» выполняется в следующем порядке:

1. Настроить и включить систему **Suricata** на сетевых интерфейсах, где требуется блокировка приложений.
2. Указать приложения, подлежащие блокировке, с помощью одной из следующих команд в конфигурационном режиме:

- для блокировки конкретного приложения из заданной категории:

```
set app-control category <категория> app <приложение>
```

где:

- **<категория>** - имя категории приложений, представляющей логическую группу приложений, объединённых по функциональному или иному признаку;
 - **<приложение>** - имя приложения из указанной категории.
- для блокировки всех приложений в заданной категории:

```
set app-control category <категория> all
```

Полный перечень доступных категорий и приложений приведён в [таблице «Список приложений»](#).

Состав поддерживаемых приложений может быть расширен при обновлении системы **Suricata** с сервера компании ООО «ИнфоВотч **АРМА**».

3. Включить службу «**Контроль приложений**» с помощью команды:

```
set app-control enable
```

4. Применить и сохранить конфигурацию с использованием команд **commit** и **save** соответственно.

После успешного применения конфигурации указанные приложения блокируются на всех интерфейсах системы **ARMA Стена**, где **Suricata** работает в режиме **IPS**.

Для отключения контроля приложений необходимо удалить команду активации службы:

```
delete app-control enable  
commit  
save
```

Удаление приложений из списка блокируемых выполняется с помощью одной из следующих команд:

- удаление всех приложений из указанной категории:

```
delete app-control category <категория>
```

Команда удалит указанную категорию из списка блокировки.

- удаление определённого приложения из указанной категории:

```
delete app-control category <категория> app <приложение>
```

Примечание:

В случае, если в категории приложений остаётся только одно приложение, использование команды для удаления конкретного приложения приведёт к возникновению системной ошибки, указывающей на невозможность удаления последнего элемента в данной категории. Для успешного удаления последнего приложения в категории необходимо применить команду для удаления всей категории из списка блокировки.

События срабатывания правил блокировки приложений записываются в глобальный журнал системы **ARMA Стена**, если включено логирование в системе **Suricata**.

Для включения логирования системы **Suricata** используется следующая команда в конфигурационном режиме:

```
set suricata outputs syslog enabled yes
```

Просмотр записей о срабатывании правил блокировки приложений осуществляется с помощью команды:

```
admin@ngfwos:~$ show logging idps
```

Данная команда предоставляет доступ к логам, связанным с системой **Suricata**, включая события, инициированные службой «**Контроль приложений**».

14.2 Контроль доменов

Служба «**Контроль доменов**» реализует блокировку трафика на основе доменных имён. Блокировка осуществляется через механизм межсетевого экрана (**МЭ**). Домены могут быть заданы индивидуально или в виде списка, загружаемого из текстового файла.

Служба «**Контроль доменов**» обладает более высоким приоритетом по сравнению с правилами **МЭ**. Если домен включён в список блокировки, доступ к нему запрещается даже при наличии разрешающего правила **МЭ**.

Блокировка отдельного домена

Для добавления одного домена в список блокируемых используется следующая команда в конфигурационном режиме:

```
set app-control domain address <url>
```

где **<url>** - доменное имя, подлежащее блокировке. Указывать протокол (**Ошибка! Недопустимый объект гиперссылки., Ошибка! Недопустимый объект гиперссылки.**) не требуется.

Пример команды:

```
set app-control domain address vk.ru
```

Блокировка списка доменов

Для массовой блокировки доменов предусмотрен механизм загрузки списка из текстового файла. Файл должен соответствовать следующим требованиям:

- каждый домен указывается в отдельной строке;
- не допускается указывать протокол (**Ошибка! Недопустимый объект гиперссылки., Ошибка! Недопустимый объект гиперссылки.**);
- файл должен иметь расширение «.txt».

Пример содержимого файла:

```
ya.ru  
mail.ru  
vk.ru
```

Файл должен быть предварительно скопирован в файловую систему устройства **ARMA Стена** в один из доступных пользователю каталогов.

Для применения списка доменов используется следующая команда в конфигурационном режиме:

```
set app-control domain text-file <file>
```

где **<file>** - полный путь к текстовому файлу с перечнем доменов.

Пример команды:

```
set app-control domain text-file /config/domains-blocklist.txt
```

Примечание:

Путь к файлу должен быть корректным и указывать на существующий файл в файловой системе устройства. Поддерживается только формат обычного текстового файла (.txt), без специальных кодировок.

Логирование событий

Для включения записи событий, связанных с блокировкой доменов, используется команда в конфигурационном режиме:

```
set app-control domain log
```

После активации параметра все события, связанные с блокировкой доменов, будут записываться в глобальный журнал системы.

Просмотр событий осуществляется с помощью команды в эксплуатационном режиме:

```
admin@ngfwos:~$ show logging firewall
```

15 СЕРВИСЫ

15.1 DHCP

15.1.1 DHCP-сервер

DHCP-сервер используется для автоматического предоставления клиентам IP-адреса и других параметров, необходимых для работы в сети TCP/IP.

Для создания DHCP-сервера на **ARMA Стена** необходимо указать подсети и задать диапазон выдаваемых IP-адресов с помощью ввода следующих команд:

```
set service dhcp-server shared-network-name Net1 subnet 192.168.70.0/24 default-  
router 192.168.70.1  
set service dhcp-server shared-network-name Net1 subnet 192.168.70.0/24 range 0 start  
192.168.70.10  
set service dhcp-server shared-network-name Net1 subnet 192.168.70.0/24 range 0 stop  
192.168.70.100
```

где:

- «**192.168.70.0/24**» – адрес сети;
- «**192.168.70.1**» – IP-адрес шлюза по умолчанию для клиентов, получающих IP-адреса через DHCP из указанной подсети;
- «**192.168.70.10**» – начальное значение диапазона IP-адресов;
- «**192.168.70.100**» – конечное значение диапазона IP-адресов.

Значения приведены в качестве примера.

Зафиксировать изменения с помощью ввода команд «**commit**» и «**save**».

На ПК «**Client**» получить IP-адрес по протоколу DHCP.

15.1.2 DHCP-ретранслятор

Ретрансляция DHCP применяется в ситуациях, когда клиент DHCP не может напрямую обратиться к серверу DHCP, например, если они находятся в разных широковещательных доменах.

15.1.2.1 Команды настройки DHCP-ретранслятора

1. Указание интерфейса для прослушивания запросов от клиентов DHCP:

```
set service dhcp-relay listen-interface <interface>
```

где **<interface>** - имя интерфейса.

2. Указание интерфейса для пересылки запросов на DHCP-сервер:

```
set service dhcp-relay upstream-interface <interface>
```


3. Указание IP-адреса DHCP-сервера, которому будут передаваться запросы от клиентов DHCP:

```
set service dhcp-relay server <x.x.x.x>
```

где **<x.x.x.x>** - IP-адрес DHCP-сервера.

4. Просмотр настроек DHCP-ретрансляции:

```
show service dhcp-relay
```

5. Отключение DHCP-ретрансляции с сохранением настроек:

```
set service dhcp-relay disable
```

6. Команда перезапуска DHCP relay-агента:

```
admin@ngfwos:~$ restart dhcp relay-agent
```

15.1.2.2 Команды настройки DHCPv6-ретранслятора

1. Указать интерфейс для прослушивания запросов от клиентов DHCPv6:

```
set service dhcpv6-relay listen-interface <interface> address <IP_DHCPv6-server>
```

2. Указать интерфейс для пересылки запросов на DHCPv6-сервер:

```
set service dhcpv6-relay upstream-interface <interface> address <IP_DHCPv6-server>
```

3. Отключения DHCPv6-ретрансляции с сохранением настроек:

```
set service dhcpv6-relay disable
```

4. Команда перезапуска DHCPv6 relay-агента:

```
admin@ngfwos:~$ restart dhcpv6 relay-agent
```

Дополнительные параметры:

1. Установить число прыжков перед отбрасыванием пакета:

```
set service dhcpv6-relay max-hop-count <count>
```

где **<count>** - число прыжков перед отбрасыванием пакета. Возможно указать значение в диапазоне от «1» до «255». По умолчанию используется значение «10».

2. Включить вставку идентификатора интерфейса:

```
set service dhcpv6-relay use-interface-id-option
```

Если параметр активирован, агент ретрансляции будет включать идентификатор интерфейса. Данный параметр активируется автоматически при использовании более одного прослушивающего интерфейса. В случае, если в запросе на ретрансляцию DHCPv6 присутствует значение идентификатора интерфейса, сервер копирует его в ответное сообщение. Идентификатор интерфейса позволяет определить, с какого интерфейса был получен запрос DHCPv6. Этот параметр следует использовать, когда IPv6-адрес интерфейса, на котором выполняется ретрансляция DHCPv6, не может быть однозначно идентифицирован.

15.1.2.3 Пример настройки DHCP-ретранслятора

В качестве примера настройки ретрансляции DHCP, используется схема стенда, представленная на рисунке (см. [Рисунок – Схема стенда для настройки DHCP-ретранслятора](#)).

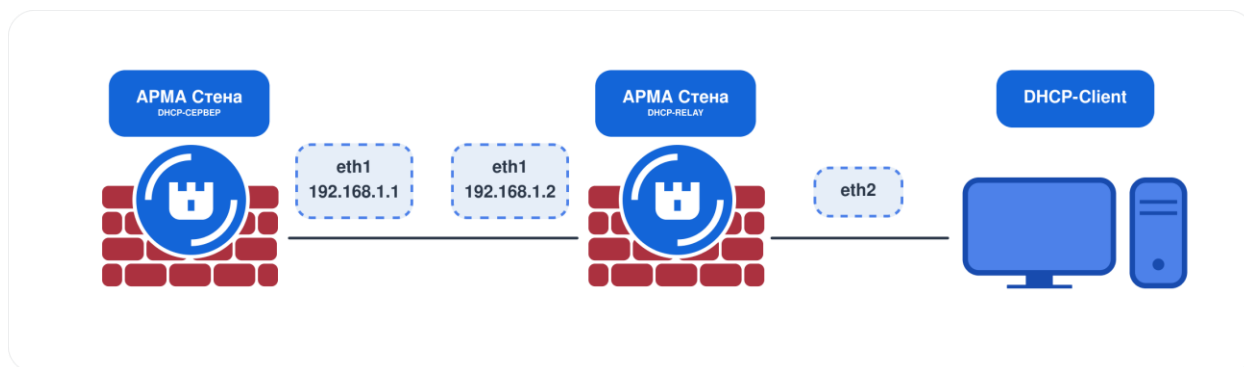


Рисунок – Схема стенда для настройки DHCP-ретранслятора

Для настройки DHCP-ретранслятора необходимо выполнить следующие шаги:

1. Настроить DHCP-сервер **ARMA Стена 1**, определив диапазон IP-адресов от «192.168.2.10» до «192.168.2.100»:

```
set service dhcp-server listen-address '192.168.1.1'
set service dhcp-server shared-network-name TEST subnet 192.168.2.0/24 range test
start '192.168.2.10'
set service dhcp-server shared-network-name TEST subnet 192.168.2.0/24 range test
stop '192.168.2.100'
```

2. Настроить DHCP-ретранслятор на **ARMA Стена 2**:

```
set service dhcp-relay listen-interface 'eth2'
set service dhcp-relay server '192.168.1.1'
set service dhcp-relay upstream-interface 'eth1'
```

3. На пользовательских компьютерах установить автоматический режим получения IP-адреса.

15.2 Отслеживание соединений

Служба отслеживания соединений, как и вся система Netfilter, функционирует в ядре операционной системы. В контролируемой ядром области оперативной памяти хранится актуальная информация о соединениях. Ядро не обеспечивает резервирование, но предоставляет возможности для загрузки и выгрузки информации о соединениях в режиме реального времени. После этого остаётся лишь передать эту информацию между системами кластера. За эту работу отвечает служба «conntrackd», которая работает вне ядра. В конфигурации **ARMA Стена** эта служба доступна как «**conntrack-sync**».

Для синхронизации трафика можно использовать либо многоадресную «**multicast**», либо одноадресную «**unicast**» рассылку. В большинстве случаев используется «**multicast**», но возможно указать и «**unicast**». Для этого после имени интерфейса необходимо использовать ключ «**peer**», как показано в следующем примере:

```
set service conntrack-sync interface eth0 peer 192.168.0.250
```

В связи с тем, что одни и те же механизмы используются для различных целей, в общем случае невозможно одновременно управлять сохранением состояния соединений и осуществлять распределение трафика по нескольким исходящим интерфейсам для балансировки нагрузки на каналы (WAN load balancing). В частности, очистка буферов в рамках управления или настройки службы отслеживания соединений может привести к сбою в работе системы распределения трафика, которая использует учёт соединений для определения фактической загруженности конкретного интерфейса (и, как следствие, канала, к которому этот интерфейс подключён).

15.2.1 Основные настройки

1. Определение протоколов, для которых будут синхронизироваться локальные записи службы отслеживания состояния:

```
set service conntrack-sync accept-protocol <proto>
```

где **<proto>** – имя протокола. Возможно указать следующие значения: «tcp», «udp», «icmp», «icmp6», «sctp», «dccp».

2. Установка размера буфера для сообщений от службы отслеживания соединений:

```
set service conntrack-sync event-listen-queue-size <size>
```

где **<size>** – размер буфера в Мбайтах. Возможно указать значение в диапазоне от «0» до «4294967295».

3. Определение протокола, для которого необходимо синхронизировать записи ожиданий:

```
set service conntrack-sync expect-sync <proto>
```

где **<proto>** – имя протокола. Возможно указать следующие значения: «all», «ftp», «h323», «nfs», «sip», «sqlnet».

4. Включить механизм отказоустойчивости, используемый для службы отслеживания состояния:

```
set service conntrack-sync failover-mechanism vrrp sync-group <group>
```

где **<group>** – имя группы.

5. Указать IP-адрес или подсеть, для которых локальные записи службы отслеживания состояния не будут синхронизироваться:

```
set service conntrack-sync ignore-address <address>
```

где **<address>** – IP-адрес или подсеть в формате: «x.x.x.x»/«x.x.x.x/x» - для IPv4, «h:h:h:h:h:h:h:h»/«h:h:h:h:h:h:h:h/x» - для IPv6.

6. Указать интерфейс, используемый для синхронизации записей службы отслеживания состояния:

```
set service conntrack-sync interface <name>
```

где **<name>** – имя сетевого интерфейса.

Примечание:

Для предотвращения ошибок при изменении HWID сетевой карты, которые могут привести к блокировке загрузки системы, необходимо отключить автоматическое назначение MAC-адреса сетевой карте. Это возможно сделать с помощью команды «**set interfaces ethernet ethN hw-id-auto-pinning false**».

7. Указать номер порта для интерфейса, используемого для синхронизации записей службы отслеживания состояния:

```
set service conntrack-sync interface <name> port <port>
```

где **<port>** – номер порта. Возможно указать значение в диапазоне от «1» до «65535».

8. Указать локальный IPv4-адрес прослушивания входящих соединений для службы отслеживания состояния:

```
set service conntrack-sync listen-address <ipv4address>
```

где **<ipv4address>** – IPv4-адрес.

9. Указать адрес для группы многоадресной трансляции, используемой для синхронизации записей службы отслеживания состояния:

```
set service conntrack-sync mcast-group <x.x.x.x>
```

где **<x.x.x.x>** – IPv4-адрес назначения многоадресной («multicast») передачи. По умолчанию используется значение «225.0.0.50».

10. Указать адрес узла отправки одноадресных UDP сообщений для службы отслеживания состояния:

```
set service conntrack-sync interface <name> peer <x.x.x.x>
```

где **<x.x.x.x>** – IPv4-адрес.

11. Указать размера буфера для синхронизации записей службы отслеживания состояния:

```
set service conntrack-sync sync-queue-size <size>
```

где **<size>** – размер буфера в Мбайтах. Возможно указать значение в диапазоне от «0» до «4294967295».

12. Отключить внешний кэш и напрямую передать состояния потока в службе отслеживания соединений в ядро резервного межсетевого экрана:

```
set service conntrack-sync disable-external-cache
```

13. Отключить запись сообщений в syslog:

```
set service conntrack-sync disable-syslog
```

14. При запуске разрешить conntrackd выполнить полную синхронизацию таблицы conntrack с другим узлом:

```
set service conntrack-sync startup-resync
```

15.2.2 Мониторинг состояния

1. Вывести таблицу службы отслеживания состояния для протокола IP:

```
show conntrack table ipv4|ipv6
```

Примечание:

В случае отсутствия записей об активных соединениях в таблице и появления предупреждения, это указывает на то, что служба отслеживания состояния не активирована. Для её активации необходимо создать правило трансляции NAT или правило межсетевого экрана.

2. Вывести записи внешнего кэша синхронизации соединений службы отслеживания состояния:

```
show conntrack-sync cache external
```

3. Вывести записи внутреннего кэша синхронизации соединений службы отслеживания состояния:

```
show conntrack-sync cache internal
```

4. Вывести актуальную статистику службы отслеживания соединений:

```
show conntrack-sync statistics
```

5. Вывести информацию об актуальном состоянии службы отслеживания соединений:

```
show conntrack-sync status
```

15.3 Учёт сетевого трафика

ARMA Стена предоставляет механизм по сбору статистики и предоставлению отчётов о сетевом трафике как IPv4, так и IPv6. Данные учёта могут быть выведены как локально, так и экспортированы на удалённые сервера сбора и анализа данных.

ARMA Стена поддерживает учёт данных в формате NetFlow (версии 5, 9 и 10/IPFIX) и sFlow.

15.3.1 NetFlow

NetFlow предоставляет администраторам доступ к информации о потоках IP в сети передачи данных. Поток данных определяется как однонаправленная последовательность пакетов с неким общим набором свойств, проходящих через сетевое устройство.

Для сбора информации о трафике по протоколу NetFlow требуются следующие компоненты:

экспортер – собирает статистику по проходящему через него трафику, объединяет пакеты в потоки и экспортирует записи потоков в один или несколько коллекторов (сборщиков) потоков;

коллектор – собирает получаемые от экспортера данные и помещает их в хранилище;

анализатор – анализирует собранные коллектором данные и формирует пригодные для чтения человеком отчёты.

Для сетевых протоколов без установления соединения таких как **ICMP** и **UDP**, сетевой поток считается завершённым если в течение указанного интервала ожидания не принят ни один пакет, относящийся к данному потоку.

Включение учёта сетевого трафика осуществляется отдельно для каждого интерфейса. Все пакеты, полученные на интерфейсе, будут учтены и представлены в статистических данных для интерфейса. При этом следует учитывать, что просмотр всех пакетов потребует значительных вычислительных ресурсов. В качестве альтернативы, позволяющей снизить нагрузку на систему, возможно учитывать каждый n -ный пакет (n – частота выборки), и производить оценку на основе выбранных пакетов. Это позволит снизить потребляемые ресурсы по сравнению с учётом всех пакетов, при этом обеспечивая приемлемую точность.

Примечание:

Использование технологии NetFlow в **ARMA Стена** с большим потоком трафика может привести к повышенной нагрузке на центральный процессор, что негативно повлияет на производительность устройства. В этой ситуации рекомендуется использовать технологию sFlow.

15.3.1.1 Команды настройки NetFlow

1. Указание интерфейса, для которого производится учёт входящего трафика:

```
set system flow-accounting interface <interface>
```

где **<interface>** – интерфейс, для которого осуществляется учёт входящего трафика. Интерфейс должен быть заранее настроен. Возможно настроить несколько интерфейсов, которые будут участвовать в учёте входящего трафика.

2. Включить учёт исходящего трафика:

```
set system flow-accounting enable-egress
```

3. Отключить использование локальной таблицы во внутренней памяти:

```
set system flow-accounting disable-imt
```

По умолчанию записанные потоки сохраняются во внутренней памяти и могут быть перечислены с помощью команды CLI.

4. Увеличить буфер обмена данными между основным процессом и плагином:

```
set system flow-accounting buffer-size <size>
```

где **<size>** – размер буфера в мегабайтах. Возможно указать значение в диапазоне от «0» до «4294967295». По умолчанию используется значение «10».

5. Указание типов сообщений, относящихся к учёту трафика, которые будут регистрироваться в журнале:

```
set system flow-accounting syslog-facility <facility>
```

где **<facility>** – источник сообщений, от имени которого сообщения, связанные с учётом трафика, будут регистрироваться в журнале. Возможно указать следующие значения:

- **«auth»** – проверка подлинности и авторизация;
- **«authpriv»** – несистемная авторизация;
- **«cron»** – служба cron;
- **«daemon»** – системные службы;
- **«kern»** – ядро;
- **«lpr»** – буфер построчного принтера;
- **«mail»** – подсистема электронной почты;
- **«mark»** – сообщения mark;
- **«news»** – подсистема USENET;
- **«protocols»** – протоколы маршрутизации (local7);
- **«security»** – подсистема безопасности;
- **«syslog»** – системная регистрация;
- **«user»** – прикладные процессы;
- **«uucp»** – подсистема UUCPP;
- **«local0»** – локальный сервис 0;
- **«local1»** – локальный сервис 1;
- **«local2»** – локальный сервис 2;
- **«local3»** – локальный сервис 3;
- **«local4»** – локальный сервис 4;
- **«local5»** – локальный сервис 5;
- **«local6»** – локальный сервис 6;
- **«local7»** – локальный сервис 7;
- **«all»** – все типы источников сообщений.

6. Указание формата NetFlow, в котором будут экспортированы данные учёта:

```
set system flow-accounting netflow version <version>
```

где **<version>** – номер версии NetFlow, в формате которой будут экспортированы данные учёта. Возможно указать следующие значения: «5», «9», «10». По умолчанию используется значение «9».

7. Указание сервера сбора данных об учёте трафика (коллектора) для экспорта данных NetFlow:

```
set system flow-accounting netflow server <address> port <number>
```

где:

- **<address>** – IP-адреса коллектора для экспорта данных NetFlow. Формат ввода IP-адреса: **<x.x.x.x>** – для IPv4, **<h:h:h:h:h:h:h>** – для IPv6;
- **<number>** – порт, на котором коллектор NetFlow принимает отчёты. Возможно указать значение в диапазоне от «1025» до «65535».

8. Указание IP-адреса источника пакетов NetFlow:

```
set system flow-accounting netflow source-ip <address>
```

где **<address>** – IP-адреса источника пакетов NetFlow. Формат ввода IP-адреса: **<x.x.x.x>** – для IPv4, **<h:h:h:h:h:h:h>** – для IPv6.

9. Указание идентификатора системы, который будет включён в данные NetFlow:

```
set system flow-accounting netflow engine-id <id>
```

где **<id>** – идентификатор системы, который указывается в данных NetFlow, позволяющий идентифицировать маршрутизатор, отправивший отчёт. Возможно указать следующие значения:

- для **NetFlow v5** – возможно указать значение в диапазоне от «0» до «255». Допускается указать множественное значение, разделённое знаком «:» (0-255:0-255);
- для **NetFlow v9/IPFIX** – возможно указать значение в диапазоне от «0» до «4294967295».

10. Указание частоты регистрации событий для NetFlow, с которой сетевые пакеты будут учитываться в статистике:

```
set system flow-accounting netflow sampling-rate <rate>
```

где **<rate>** – частота, с которой будут отбираться пакеты. Учитывается каждый n-ый пакет, где n – значение sampling-rate, настроенное для узла. Возможно указать значение в диапазоне от «0» до «4294967295». По умолчанию используется значение «1».

11. Указание интервала, через который будут отправляться отчёты коллектору данных NetFlow:

```
set system flow-accounting netflow timeout expiry-interval <interval>
```

где **<interval>** – интервал времени, в секундах, через который будут отправляться отчёты коллектору NetFlow. Возможно указать значение в диапазоне от «0» до «2147483647». По умолчанию используется значение «60».

12. Указание таймаута сетевого потока для трафика IP:

```
set system flow-accounting netflow timeout flow-generic <timeout>
```

где **<timeout>** – таймаут для сетевого потока, в секундах, для общего трафика IP. Действует для трафика IP за исключением трафика протоколов TCP, UDP и ICMP. Возможно указать значение в диапазоне от «0» до «2147483647».

13. Указание таймаута сетевого потока для трафика ICMP:

```
set system flow-accounting netflow timeout flow-generic <timeout>
```

где **<timeout>** – таймаут сетевого потока, в секундах, для трафика ICMP. Возможно указать значение в диапазоне от «0» до «2147483647».

14. Указание максимального интервала времени, в течение которого будет учитываться трафик, относящийся к сетевому потоку:

```
set system flow-accounting netflow timeout max-active-life <interval>
```

где **<interval>** – интервал времени, в секундах, определяющий максимальное время учёта трафика, относящегося к сетевому потоку любого типа. Возможно указать значение в диапазоне от «0» до «2147483647».

15. Указание таймаута сетевого потока TCP после получения пакета TCP с флагом FIN:

```
set system flow-accounting netflow timeout tcp-fin <timeout>
```

где **<timeout>** – таймаут сетевого потока, в секундах, после получения пакета TCP с флагом FIN. Возможно указать значение в диапазоне от «0» до «2147483647».

16. Указание таймаута сетевого потока TCP:

```
set system flow-accounting netflow timeout tcp-generic <timeout>
```

где **<timeout>** – таймаут для потока TCP, в секундах. Возможно указать значение в диапазоне от «0» до «2147483647».

17. Указание таймаута сетевого потока TCP после получения пакета TCP с флагом RST:

```
set system flow-accounting netflow timeout tcp-rst <timeout>
```

где **<timeout>** – таймаут сетевого потока, в секундах, после получения пакета TCP RST. Возможно указать значение в диапазоне от «0» до «2147483647».

18. Указание таймаута сетевого потока для трафика UDP:

```
set system flow-accounting netflow timeout udp <timeout>
```

где **<timeout>** – таймаут сетевого потока для трафика UDP, в секундах. Возможно указать значение в диапазоне от «0» до «2147483647».

19. Указание максимального количества потоков, отслеживаемых одновременно:

```
set system flow-accounting netflow max-flows <number>
```

где **<number>** – задаёт максимальное количество потоков системы NetFlow. Возможно указать значение в диапазоне от «0» до «4294967295».

20. Вывести информацию об учёте потока для данного интерфейса:

```
admin@ngfwos:~$ show flow-accounting interface <ethN>
```

где **<ethN>** – имя интерфейса.

21. Вывести информацию об учёте потока для данного интерфейса только для определённого хоста:

```
admin@ngfwos:~$ show flow-accounting interface <ethN> host <address>
```

где **<address>** – IP-адреса в формате: **<x.x.x.x>** - для IPv4, **<h:h:h:h:h:h:h>** - для IPv6.

15.3.2 sFlow

Система мониторинга sFlow включает следующие компоненты:

агент – обеспечивает интерфейс для настройки измерительного процесса, связанного с источником данных на устройстве, отвечает за поддержку сеансов измерения с коллекторами sFlow, собирает учётные данные в дейтаграммы sFlow для передачи коллекторам;

коллектор – получает дейтаграммы sFlow от одного или множества агентов sFlow.

15.3.2.1 Команды настройки sFlow

1. Указание IP-адреса агента sFlow:

```
set system flow-accounting sflow agent-address <address>
```

где **<address>** – IP-адрес агента sFlow, который будет указан в пакетах, отправляемых коллектору sFlow. Возможно указать следующие значения:

- **auto** – автоматически выбирается IP-адрес одного из настроенных интерфейсов;
- **<x.x.x.x>** – IPv4-адрес.

2. Указание частоты выборки для статистики sFlow:

```
set system flow-accounting sflow sampling-rate <rate>
```

где **<rate>** – частота, с которой будут отбираться пакеты. Учитывается каждый n-ый пакет, где n – значение **sampling-rate**, настроенное для узла. Возможно указать значение в диапазоне от «0» до «4294967295».

3. Указание адреса коллектора sFlow для экспорта данных учёта:

```
set system flow-accounting sflow server <address> port <number>
```

где:

- **<address>** – IP-адреса коллектора для экспорта данных sFlow. Формат ввода IP-адреса: **<x.x.x.x>** – для IPv4, **<h:h:h:h:h:h:h>** – для IPv6;
- **<number>** – порт, на котором коллектор sFlow принимает отчёты. Возможно указать значение в диапазоне от «1025» до «65535».

4. Указание исходного IP-адреса выходных пакетов sFlow:

```
set system flow-accounting sflow source-address <address>
```

где **<address>** – исходный IP-адрес отправленных sFlow пакетов. Формат ввода IP-адреса: **<x.x.x.x>** – для IPv4, **<h:h:h:h:h:h:h>** – для IPv6. По умолчанию исходный адрес выходных sFlow пакетов – это локальный IP-адрес, который используется для пинга адреса назначения.

15.4 Приоритизация трафика

QoS позволяет приоритизировать поток данных, передаваемый по каналам связи IP, обеспечивая трафик необходимым сервисом обслуживания в соответствии с заданными техническими рамками.

15.4.1 Общие принципы работы

Для работы QoS в **ARMA Стена** необходимо соблюдать следующую последовательность действий:

- создать политику обработки трафика;
- применить политику обработки трафика к входящему или исходящему интерфейсу.

После настройки QoS система автоматически начинает регистрировать события в трёх направлениях:

- журналирование команд tc;
- регистрация изменений конфигурации QoS;
- мониторинг текущего состояния QoS.

Для просмотра в консоли событий, связанных с изменениями конфигурации QoS и командами tc в глобальном журнале, возможно использовать утилиту **grep**, указав следующий шаблон: «**show logging | grep -E "\sngfwos\s+qos(\[[:])"**». Команда выполняется в терминале суперпользователя:

```
admin@ngfwos:~$ sudo -i
root@ngfwos:~# show logging | grep -E "\sngfwos\s+qos(\[[:])"
```

Записи об изменениях конфигурации QoS в глобальном журнале возможно просмотреть в консоли, выполнив в эксплуатационном режиме команду «**show logging users**».

15.4.1.1 Единицы измерения

При настройке политики обработки трафика необходимо задавать скорость передачи данных. **ARMA Стена** оперирует следующими префиксами и суффиксами единиц измерения скорости передачи данных:

- **Префиксы** – возможно указать в десятичном или двоичном формате:

- десятичный формат:

kbit	(10^3)	килобит в секунду
mbit	(10^6)	мегабит в секунду
gbit	(10^9)	гигабит в секунду
tbit	(10^12)	терабит в секунду
kbps	(8*10^3)	килобит в секунду
mbps	(8*10^6)	мегабит в секунду
gbps	(8*10^9)	гигабит в секунду
tbps	(8*10^12)	терабит в секунду

- двоичный формат:

kibit ($2^{10} = 1024$)	кибибит в секунду
mibit ($2^{20} = 1024^2$)	мебибит в секунду
gibit ($2^{30} = 1024^3$)	гибибит в секунду
tbit ($2^{40} = 1024^4$)	тебибит в секунду
kibps ($1024 \cdot 8$)	кибибит в секунду
mibps ($1024^2 \cdot 8$)	мебибит в секунду
gibps ($1024^3 \cdot 8$)	гибибит в секунду
tibps ($1024^4 \cdot 8$)	тебибит в секунду

- **Суффиксы** – указываются в битах или байтах:

- «bit» – краткое обозначение битов:

kbit	килобит в секунду
mbit	мегабит в секунду
gbit	гигабит в секунду
tbit	терабит в секунду

- «b» – краткое обозначение байтов:

kbps	килобайт в секунду
mbps	мегабайт в секунду
gbps	гигабайт в секунду

15.4.1.2 Классы

QoS позволяет классифицировать трафик в соответствии с заданными параметрами.

Для определения, к какому классу относится трафик, необходимо установить критерии соответствия. Пакет ассоциируется с определённым классом в том случае, если обнаруживается правило с подходящим классификатором.

Каждый класс обладает числовым идентификатором, который задаётся в процессе его настройки. Классу возможно назначить несколько классификаторов. Классификатор содержит множественные критерии соответствия. Трафик считается подошедшим, если все установленные критерии выполняются одновременно.

Для классификации трафика возможно использовать следующие параметры:

- **«ether»** – протокол. Возможно указать следующие параметры для классификации:
 - MAC-адрес отправителя;
 - MAC-адрес получателя;
- **«interface»** – имя интерфейса;

- **«ip»** – протокол IPv4. Возможно указать следующие параметры для классификации:
 - метка DSCP;
 - максимальная длина тела пакета;
 - протокол, IPv4-адрес отправителя;
 - IPv4-адрес получателя;
 - номер порта отправителя;
 - номер порта получателя;
 - флаги TCP;
- **«ipv6»** – протокол IPv6. Возможно указать следующие параметры для классификации:
 - метка DSCP;
 - максимальная длина тела пакета;
 - протокол;
 - IPv6-адрес отправителя;
- **«mark»** – метка межсетевого экрана;
- **«vif»** – идентификатор VLAN-интерфейса.

При задании классификатора возможно использовать **клавишу «Tab»** на клавиатуре для вывода информации о доступных к использованию параметрах команды. Пример:

[edit]

```
admin@ngfwos# set qos policy shaper test class 2 match test
```

Possible completions:

description	Description
> ether	Ethernet header match
interface	Interface to use
> ip	Match IP protocol header
> ipv6	Match IPv6 protocol header
mark	Match on mark applied by firewall
vif	Virtual Local Area Network (VLAN) ID for this match

Примечание:

Классификатор с установленным параметром «IPv4» - «TCP» соответствует IPv4-пакетам с длиной заголовка 20 байт.

Классификатор с установленным параметром «IPv6» - «TCP» соответствует IPv6-пакетам, не имеющим расширенных заголовков.

Трафик, который не соответствует ни одному назначенному классу, обрабатывается классом по умолчанию.

15.4.2 Создание политики обработки трафика

ARMA Стена поддерживает следующие политики обработки трафика:

- «Drop Tail»;
- «Fair Queue»;
- «FQ-CoDel»;
- «Limiter»;
- «Network Emulator»;
- «Priority Queue»;
- «Random Detect»;
- «Rate Control»;
- «Round Robin»;
- «Shaper»;
- «Cake».

Возможно настроить любое количество политик, но для каждого интерфейса, входящего или исходящего с учётом направления трафика, применима только одна политика.

Некоторые политики обработки трафика могут быть объединены с помощью встраивания, после чего встроенная политика будет применена к классу трафика, соответствующему основной политике.

Примечание:

Если необходимо выбрать политику для исходящего трафика, но при этом нет понимания, какая именно политика необходима в конкретном случае, рекомендуется использовать политику «Shaper», оставив по умолчанию встроенную в её очереди политику «FQ-CoDel».

15.4.2.1 Drop Tail

Порядок организации трафика: PFIFO.

Применение к направлению трафика: исходящий трафик.

Drop Tail – наиболее простой механизм управления очередью – отбрасываются все вновь пришедшие пакеты, не помещающиеся в буфер. Политика требует наименьших ресурсов, но используется крайне редко вследствие неэффективной обработки трафика.

Для настройки фильтрации трафика по алгоритму Drop Tail необходимо ввести команду:

```
set qos policy drop-tail <policy-name> queue-limit <number-of-packets>
```

где:

- **<policy-name>** – уникальное имя политики;
- **<number-of-packets>** – размер очереди, измеряемый в пакетах. Возможно указать значение в диапазоне от «1» до «4294967295».

15.4.2.2 Fair Queue

Порядок организации трафика: SFQ.

Применение к направлению трафика: исходящий трафик.

Fair Queue – планировщик пакетов, который распределяет пакеты по очередям на основе потоков. Он балансирует трафик в равной степени между дочерними очередями, чтобы пакеты из каждого потока отправлялись строго по очереди, не позволяя таким образом одному потоку преобладать над другими.

Для создания фильтрации трафика по алгоритму Fair Queue необходимо ввести команду:

```
set qos policy fair-queue <policy-name>
```

где **<policy-name>** - уникальное имя политики.

Для распределения трафика по очередям Fair Queue использует классификатор, основанный на адресе отправителя, адресе получателя и номере порта отправителя. Алгоритм распределения использует специальные хеш-блоки. Каждый пакет должен принадлежать уникальному потоку. Поскольку несколько потоков могут попасть в один хеш-блок, алгоритм хеширования задействуется через настраиваемые интервалы времени. Рекомендуемое значение временного интервала составляет «10» секунд.

Для установки времени, через которое будет задействован алгоритм хеширования необходимо ввести команду:

```
set qos policy fair-queue <policy-name> hash-interval <seconds>
```

где **<seconds>** – время в секундах. Возможно указать значение в диапазоне от «1» до «4294967295».

При завершении очереди каждый хеш-блок с данными используется в кольцевом порядке следования. Возможно сконфигурировать длину очереди, используя параметр **«queue-limit»** в следующей команде:

```
set qos policy fair-queue <policy-name> queue-limit <limit>
```

где **<limit>** – максимальное количество пакетов, ожидающих обработки в очереди. Возможно указать значение в диапазоне от «1» до «127».

Fair Queue – политика без шейпинга, используется только в случае, если исходящий интерфейс действительно перегружен трафиком. Если в канале есть доступная для использования полоса пропускания, то существует возможность встроить Fair Queue в политику с шейпингом на основе классов.

15.4.2.3 FQ-CoDel

Порядок организации трафика: Fair/Flow Queue CoDel.

Применение к направлению трафика: исходящий трафик.

Политика FQ-CoDel направлена на борьбу с переполнением буфера и на снижение задержек.

Политика использует стохастическую модель распределения для классификации входящих пакетов на различные потоки и применяется для обеспечения равных долей пропускной способности всем потокам. Каждый поток обрабатывается в соответствии с дисциплиной CoDel. Переупорядочение пакетов в составе потока исключено, поскольку дисциплина CoDel использует внутреннюю очередь FIFO.

Политика FQ-CoDel позволяет эффективное использование с параметрами по умолчанию на скорости 10 Гбит/сек.

При скорости 1 Гбит/сек и ниже рекомендуется уменьшить значение параметра **«queue-limit»** до «1000» пакетов или меньше.

При скорости 10 Мбит/сек рекомендуется установить значение параметра **«queue-limit»** в «600» пакетов.

При скорости 100 Мбит/сек и выше, если политика FQ-CoDel встроена в политику Shaper, рекомендуется установить значение параметра **«quantum»** в «8000» байт для снижения нагрузки на процессор.

При скорости менее 40 Мбит/сек рекомендуется уменьшить значение параметра **«quantum»** до «300» байт.

При скорости менее 3 Мбит/сек рекомендуется: уменьшить значение параметра **«quantum»** до «300» байт; увеличить значение параметра **«target»** до «15» миллисекунд и увеличить значение параметра **«interval»** до «150» миллисекунд.

Список команд настройки FQ-CoDel:

1. Команда присвоения уникального имени для политики фильтрации трафика FQ-CoDel:

```
set qos policy fq-codel <policy name>
```

2. Команда установки максимального количества байт, извлекаемых из очереди за один раз:

```
set qos policy fq-codel <policy name> codel-quantum <bytes>
```

где **<bytes>** – количество байт. Возможно указать значение в диапазоне от «0» до «1048576». По умолчанию используется значение «1514».

3. Команда установки количества дочерних очередей, в которые будут помещаться классифицированные пакеты:

```
set qos policy fq-codel <policy name> flows <number-of-flows>
```

где **<number-of-flows>** – значение количества дочерних очередей. Возможно указать значение в диапазоне от «1» до «65536». По умолчанию используется значение «1024».

4. Команда установки периода времени, используемого управляющим циклом CoDel:

```
set qos policy fq-codel <policy name> interval <milliseconds>
```

где **<milliseconds>** – значение периода времени в миллисекундах. Возможно указать значение в диапазоне от «0» до «4294967295». По умолчанию используется значение «100».

Период времени необходим для обнаружения устоявшихся очередей и исключения значительного увеличения минимально определённой задержки.

5. Команда установки предельного размера очереди:

```
set qos policy fq-codel <policy-name> queue-limit <number-of-packets>
```

где **<number-of-packets>** – значение предельного размера очереди в пакетах. Возможно указать значение в диапазоне от «2» до «10999». По умолчанию используется значение «1024».

При достижении предельного размера все новые пакеты отбрасываются.

6. Команда установки минимально допустимой задержки в ожидающей/устоявшейся очереди:

```
set qos policy fq-codel <policy-name> target <milliseconds>
```

где **<milliseconds>** – значение минимально допустимой задержки в миллисекундах. Возможно указать значение в диапазоне от «0» до «4294967295». По умолчанию используется значение «5».

15.4.2.4 Limiter

Порядок организации трафика: Ingress Policer.

Применение к направлению трафика: входящий трафик.

Политика Limiter подразумевает простое ограничение входящих потоков трафика. Возможно определить несколько классов трафика и применить к каждому классу свои ограничения. Механизм не имеет возможность удерживать пакеты, как это делает механизм шейпинга. Трафик, превышающий установленные ограничения полосы пропускания, отбрасывается.

Допускается настроить до 4090 классов с различными настройками и политикой по умолчанию, которая будет применяться к любому трафику, не соответствующему ни одному из настроенных классов.

Список команд настройки Limiter:

1. Команда присвоения уникального имени для политики фильтрации трафика Limiter:

```
set qos policy limiter <policy-name>
```

2. Команда установки числового идентификатора класса:

```
set qos policy limiter <policy-name> class <class id>
```

где **<class id>** – значение идентификатора класса. Возможно указать значение в диапазоне от «1» до «4090».

3. Команда, устанавливающая имя и описание правилу в указанном классе:

```
set qos policy limiter <policy-name> class <class ID> match <match-name>  
description <description>
```

где:

- **<match-name>** – имя правила;
- **<description>** – описание правила.

4. Команда установки максимально допустимой полосы пропускания для класса:

```
set qos policy limiter <policy-name> class <class-ID> bandwidth <number>
```

где **<number>** – значение максимально допустимой полосы пропускания.

Возможные варианты указания значения максимально допустимой полосы пропускания:

```
<number>      бит в секунду  
<number>bit    бит в секунду;  
<number>kbit   килобит в секунду;  
<number>mbit   мегабит в секунду;  
<number>gbit   гигабит в секунду;  
<number>tbit   терабит в секунду;  
<number>%      процент от скорости соединения интерфейса.
```

5. Команда установки размера всплеска трафика для класса:

```
set qos policy limiter <policy-name> class <class-ID> burst <burst-size>
```

где **<burst-size>** – значение размера всплеска трафика в байтах. По умолчанию используется значение «15».

Возможные варианты указания значения размера всплеска трафика:

```
<burst-size>    байт;  
<burst-size>kb  килобайт;  
<burst-size>mb  мегабайт;  
<burst-size>gb  гигабайт.
```

6. Команда установки приоритета правила:

```
set qos policy limiter <policy-name> class <class ID> priority <value>
```

где **<value>** – значение приоритета, при котором выполняется оценка правила (чем меньше число, тем выше приоритет). Возможно указать значение в диапазоне от «0» до «20». По умолчанию используется значение «20».

Для обработки входящего трафика на интерфейсе возможно применить только одну политику – политика Limiter. Отсутствует возможность применения политики с шейпингом к входящему трафику на любом интерфейсе, поскольку шейпинг работает исключительно для исходящего трафика.

Существует сценарий, позволяющий применить политику с шейпингом к входящему трафику, перенаправив его на промежуточный виртуальный интерфейс «Intermediate Functional Block». К этому виртуальному интерфейсу возможно применить любую политику, которая работает для исходящего трафика.

Примечание:

Механизм «Intermediate Functional Block» необходимо настроить после установки параметров конфигурации политики обработки трафика. В противном случае возникнет ошибка «**RTNETLINK answer: File exists**». Для исправления этой ошибки необходимо ввести команду «**sudo ip link delete ifb0**».

15.4.2.5 Network Emulator

Порядок организации трафика: Network Emulator + Token Bucket Filter.

Применение к направлению трафика: исходящий трафик.

Политика Network Emulator имитирует условия эксплуатации реальной сети. Политика позволяет сконфигурировать следующие параметры:

- пропускную способность;
- всплеск трафика;
- задержку при передаче данных;
- процент потери пакетов;
- неправильные пакеты или пакеты с нарушением порядка следования.

Данная политика используется для определения поведения приложения в конкретных условиях эксплуатации сети.

Список команд настройки Network Emulator:

1. Команда присвоения уникального имени для политики фильтрации трафика Limiter:

```
set qos policy network-emulator <policy-name>
```

2. Команда установки пропускной способности для политики фильтрации трафика:

```
set qos policy network-emulator <policy-name> bandwidth <number>
```

3. Команда установки задержки пакетов, отправляемых из интерфейса:

```
set qos policy network-emulator <policy-name> delay <delay>
```

где **<delay>** – значение времени задержки пакета в миллисекундах. По умолчанию используется значение «50».

4. Команда установки в процентном соотношении количества неправильных пакетов:

```
set qos policy network-emulator <policy-name> corruption <percent>
```

где **<percent>** – значение неправильных пакетов в процентах.

В случайном порядке для выбранного процента пакетов вводится случайная ошибка.

5. Команда установки допустимых потерь пакетов:

```
set qos policy network-emulator <policy-name> loss <percent>
```

где **<percent>** – значение допустимой потери пакетов в процентах.

6. Команда установки количества пакетов с нарушенным порядком следования:

```
set qos policy network-emulator <policy-name> reordering <percent>
```

где **<percent>** – количество пакетов с нарушенным порядком следования в процентах.

7. Команда для установки максимального числа пакетов, которые одновременно находятся в очереди:

```
set qos policy network-emulator <policy-name> queue-limit <limit>
```

где **<limit>** – количество пакетов в очереди. Возможно использовать значение в диапазоне от «1» до «4294967295».

15.4.2.6 Priority Queue

Порядок организации трафика: PRIO.

Применение к направлению трафика: исходящий трафик.

Политика Priority Queue является классовой политикой планирования. При использовании данной политики пакеты не задерживаются, а удаляются из очередей в соответствии с заданным приоритетом. Priority Queue не является политикой с шейпингом.

Возможно настроить до 7 очередей, которые определяются как классы с различными приоритетами. Пакеты помещаются в очереди в соответствии с заданным классификатором. Пакеты передаются из очередей в порядке приоритета. Если классы с высоким приоритетом заполняются пакетами, пакеты из классов с пониженным приоритетом будут передаваться только после уменьшения объема трафика из классов с более высоким приоритетом.

Примечание:

Политика Priority Queue предусматривает задание числового идентификатора класса для обозначения приоритета от «1» до «7». Чем ниже значение, тем выше приоритет.

Priority Queue позволяет определить различные типы соответствующих классам правил:

- **«ether»** – соответствие протоколам Ethernet;
- **«interface»** – идентификатор интерфейса;
- **«ip»** – соответствие протоколу IPv4;
- **«ipv6»** – соответствие протоколу IPv6;
- **«mark»** – соответствие по метке, установленной брандмауэром;
- **«vif»** – идентификатор виртуальной локальной сети.

В Priority Queue возможно встраивать другие политики в классы, включая класс по умолчанию, с помощью параметра «**queue-type**»:

```
admin@ngfwos# set qos policy priority-queue <policy-name> class <class-id>  
queue-type
```

Possible completions:

drop-tail	First-In-First-Out - используется по умолчанию;
fair-queue	Stochastic Fair Queue;
fq-codel	Fair Queue Codel;
priority	Priority queuing;
random-detect	Random Early Detection.

Список команд настройки Priority Queue:

1. Команда присвоения уникального имени для политики фильтрации трафика Priority Queue:

```
set qos policy priority-queue <policy-name>
```

2. Команда установки числового идентификатора класса:

```
set qos policy priority-queue <policy-name> class <class-id>
```

где **<class id>** – значение идентификатора класса. Возможно указать значение в диапазоне от «1» до «7».

3. Команда установки максимально допустимого размера очереди:

```
set qos policy priority-queue <policy-name> class <class-id> queue-limit <limit>
```

где **<limit>** – размер очереди. Возможно указать значение в диапазоне от «1» до «4294967295».

При достижении ограничения новые пакеты отбрасываются.

15.4.2.7 Random-Detect

Порядок организации трафика: Generalized Random Early Drop.

Применение к направлению трафика: исходящий трафик.

При использовании политики Random Detect пакеты случайным образом отбрасываются из очереди перед тем, как она будет заполнена. Политика Random Detect не является политикой с шейпингом. В отличие от стандартной дисциплины RED, политика Random Detect использует обобщённую политику случайного раннего обнаружения, которая предоставляет различные виртуальные очереди в зависимости от значения приоритета IP. Благодаря этому некоторые виртуальные очереди могут пропускать больше пакетов, чем другие. Это достигается за счёт использования первых трёх бит поля «ToS» для классификации потоков данных и принятия решения в соответствии с заданными параметрами приоритета IP.

Уровни приоритета, определённые в «RFC 791» (см. [Таблица «Уровни приоритета»](#)).

Таблица «Уровни приоритета»

Уровень	Имя
7	Network Control
6	Internetwork Control
5	CRITIC/ECP
4	Flash Override
3	Flash
2	Immediate
1	Priority
0	Routine

Список команд настройки Random-Detect:

1. Команда присвоения уникального имени для политики фильтрации трафика Random-Detect:

```
set qos policy random-detect <policy-name>
```

2. Команда установки пропускной способности для политики фильтрации трафика Random-Detect:

```
set qos policy random-detect <policy-name> bandwidth <number>
```

Значение должно соответствовать полосе пропускания сетевого интерфейса.

3. Команда установки значения приоритета IP:

```
set qos policy random-detect <policy-name> precedence <IP-precedence-value>
```

где **<IP-precedence-value>** – значение приоритета IP. Возможно указать значение в диапазоне от «0» до «7».

Примечание:

Чем больше значение приоритета, тем выше приоритет.

4. Команда установки среднего размера пакета:

```
set qos policy random-detect <policy-name> precedence <IP-precedence-value>  
average-packet <bytes>
```

где **<bytes>** – значение размера пакета в байтах. Возможно указать значение в диапазоне от «16» до «10240». По умолчанию используется значение «1024».

5. Команда установки вероятности отбрасывания пакетов:

```
set qos policy random-detect <policy-name> precedence <IP-precedence-value>  
mark-probability <value>
```

где **<value>** – значение «N» в дробном выражении «1/N». Возможно указать значение в диапазоне от «0» до «4294967295». По умолчанию используется значение «10».

6. Команда установки максимального количества пакетов для случайного отбрасывания:

```
set qos policy random-detect <policy-name> precedence <IP-precedence-value>  
maximum-threshold <packets>
```

где **<packets>** – количество пакетов. Возможно указать значение в диапазоне от «0» до «4096». По умолчанию используется значение «18».

При заданном пороговом количестве вероятность отбрасывания будет максимальной.

7. Команда установки минимального количества пакетов для случайного отбрасывания:

```
set qos policy random-detect <policy-name> precedence <IP-precedence-value>  
minimum-threshold <packets>
```

где **<packets>** – количество пакетов. Возможно указать значение в диапазоне от «0» до «4096».

Если заданное пороговое значение превышает, пакеты будут отбрасываться.

Значение минимального порога по умолчанию зависит от приоритета IP (см. [Таблица «Значение минимального порога»](#)).

Таблица «Значение минимального порога»

Приоритет	Значение по умолчанию
7	16
6	15
5	14
4	13
3	12
2	11
1	10
0	9

8. Команда установки максимального размера очереди:

```
set qos policy random-detect <policy-name> precedence <IP-precedence-value>  
queue-limit <packets>
```

где **<packets>** – значение размера очереди, измеряемое в пакетах. Возможно указать значение в диапазоне от «1» до «4294967295».

При достижении заданного значения все новые пакеты отбрасываются.

Если средний размер очереди ниже значения параметра **«minimum-threshold»**, поступающий пакет будет помещён в очередь.

Если средний размер очереди находится в диапазоне значений параметров **«minimum-threshold»** и **«maximum-threshold»**, поступающий пакет будет помещён в очередь или отброшен. Это зависит от значения параметра **«mark-probability»**.

Если значение параметра **«maximum-threshold»** установлено, а значение параметра **«minimum-threshold»** не определено, то последний определяется как 50% от значения параметра **«maximum-threshold»**.

Для данных параметров рекомендовано соблюдать следующее неравенство: **«minimum-threshold» < «maximum-threshold» < «queue-limit»**.

15.4.2.8 Rate Control

Порядок организации трафика: Token Bucket Filter.

Применение к направлению трафика: исходящий трафик.

Политика Rate Control является бесклассовой политикой, ограничивающей поток пакетов установленной скоростью. Обработка трафика осуществляется путём контроля расхода токенов. Токены в некоторой степени соответствуют байтам.

Допустимо превышение лимита короткими пакетами. Политика Rate Control накапливает токены, количество которых соответствует объёму трафика при однократном проходе. Токены поступают с постоянной скоростью, пока буфер не заполнится.

Список команд настройки Rate Control:

1. Команда присвоения уникального имени для политики фильтрации трафика Rate Control:

```
set qos policy rate-control <policy-name>
```

2. Команда установки пропускной способности для политики фильтрации трафика Rate Control:

```
set qos policy rate-control <policy-name> bandwidth <number>
```

3. Команда установки размера буфера для пакетной передачи:

```
set qos policy rate-control <policy-name> burst <burst-size>
```

где **<burst-size>** – значение размера буфера в байтах.

Возможные варианты указания значения размера буфера:

```
<burst-size>    байт;  
<burst-size>kb  килобайт;  
<burst-size>mb  мегабайт;  
<burst-size>gb  гигабайт.
```

Примечание:

Для сетевых адаптеров с технической пропускной способностью в 10 Мбит/сек необходимо установить буфер ёмкостью в 10 килобайт для достижения заданной скорости. Буфер меньшей ёмкости быстро приведёт к отбрасыванию пакетов.

4. Команда установки максимально допустимой задержки пакетов в очереди:

```
set qos policy rate-control <policy-name> latency <number>
```

где **<number>** – значение задержки в миллисекундах. Возможно указать значение в диапазоне от «0» до «4096». По умолчанию используется значение «50».

15.4.2.9 Round Robin

Порядок организации трафика: Deficit Round Robin.

Применение к направлению трафика: исходящий трафик.

Политика Round Robin является политикой, распределяющей трафик по различным классам. Возможно встроить политику Round Robin в каждый из доступных классов, включая класс по умолчанию.

Каждому классу назначается специальный счётчик дефицита данных (количество байт, которые передаются в рамках потока при его обработке), инициализируемый параметром – квант. Квант – это фиксированное количество байт, предоставляемых счётчику на каждом цикле его работы. Затем политика Round Robin начинает перемещать указатель по очередям. Если счётчик дефицита данных превышает размер пакета в начале очереди, пакет будет отправлен, а значение счётчика – уменьшено на размер пакета. Затем размер следующего пакета снова сравнивается со значением счётчика, и процесс повторяется. Как только очередь окажется пустой или текущего значения счётчика будет недостаточно для сравнения, указатель будет перемещён к следующей очереди. Если очередь пустая, то значение счётчика дефицита данных сбрасывается к нулевому значению.

Список команд настройки Round Robin:

1. Команда присвоения уникального имени для политики фильтрации трафика типа Round Robin:

```
set qos policy round-robin <policy name>
```

2. Команда установки числового идентификатора класса:

```
set qos policy round-robin <policy name> class <class-id>
```

где **<class id>** – значение идентификатора класса. Возможно указать значение в диапазоне от «1» до «4095».

3. Команда установки размера кванта для определённого идентификатора класса:

```
set qos policy round-robin <policy name> class <class-ID> quantum <packets>
```

где **<packets>** – значение размера кванта. Возможно указать значение в диапазоне от «0» до «4294967295».

Значение будет добавляться на каждом цикле работы счётчика дефицита данных.

4. Команда установки размера очереди:

```
set qos policy round-robin <policy name> class <class ID> queue-limit <packets>
```

где **<packets>** – количество пакетов в очереди. Возможно указать значение в диапазоне от «1» до «4294967295».

Политику Round Robin возможно встроить в класс другой политики с помощью параметра **«queue-type»**:

```
admin@ngfwos# set qos policy round-robin <policy name> class <class-ID> queue-type
```

Possible completions:

drop-tail	First-In-First-Out (FIFO) (default)
fair-queue	Stochastic Fair Queue (SFQ)
fq-codel	Fair Queue Codel
priority	Priority queuing
random-detect	Random Early Detection (RED)

15.4.2.10 Shaper

Порядок организации трафика: Hierarchical Token Bucket.

Применение к направлению трафика: исходящий трафик.

Политика Shaper не гарантирует низкую задержку, но гарантирует определённую полосу пропускания для различных классов трафика.

Каждый класс имеет гарантированную часть общей пропускной способности, определённой для всей политики. Совокупность всех этих ресурсов, не должна превышать предельную пропускную способность политики.

Если для класса обеспечен гарантированный трафик и доступна дополнительная пропускная способность, возможно использовать параметр **«ceiling»**. Параметр **«ceiling»** применяется для определения объёма дополнительной полосы пропускания, который возможно предоставить.

Если несколько классов запрашивают дополнительную полосу пропускания, то порядок распределения дополнительного трафика определяется настройкой приоритета. Приоритет указывается в диапазоне от «0» до «7», где «0» – это самый высокий приоритет, а «7» – самый низкий.

Список команд настройки Shaper:

1. Команда присвоения уникального имени для политики фильтрации трафика Shaper:

```
set qos policy shaper <policy-name>
```

2. Команда установки гарантированной полосы пропускания для всего трафика без учёта классов:

```
set qos policy shaper <policy-name> bandwidth <number>
```

где **<number>** – значение максимально допустимой полосы пропускания.

Возможные варианты указания значения гарантированной полосы пропускания:

```
<number>      бит в секунду
<number>bit   бит в секунду;
<number>kbit  килобит в секунду;
<number>mbit  мегабит в секунду;
<number>gbit  гигабит в секунду;
<number>tbit  терабит в секунду;
<number>%     процент от скорости соединения интерфейса.
```

3. Команда установки числового идентификатора класса:

```
set qos policy shaper <policy-name> class <class-id>
```

где **<class id>** – значение идентификатора класса.

4. Команда установки гарантированной полосы пропускания для трафика определённого класса:

```
set qos policy shaper <policy-name> class <class-ID> bandwidth <number>
```

5. Команда установки размера буфера:

```
set qos policy shaper <policy-name> class <class-ID> burst <bytes>
```

где **<bytes>** – значение размера буфера в байтах. По умолчанию используется значение «15» килобайт.

Возможные варианты указания значения размера буфера:

```
<burst-size>    байт;  
<burst-size>kb  килобайт;  
<burst-size>mb  мегабайт;  
<burst-size>gb  гигабайт.
```

6. Команда установки максимально возможной скорости для определённого класса:

```
set qos policy shaper <policy-name> class <class-ID> ceiling <bandwidth>
```

где **<bandwidth>** – значение максимально возможной скорости.

Возможные варианты указания значения максимально возможной скорости:

<number>	килобит в секунду
<number>%	процент от общей скорости
<number>bit	bit(1), kbit(10 ³), mbit(10 ⁶), gbit, tbit
<number>ibit	kibit(1024), mibit(1024 ²), gibit(1024 ³), tbit(1024 ⁴)
<number>ibps	kibps(1024*8), mibps(1024 ² *8), gibps, tibps -
Byte/sec	
<number>bps	bps(8),kbps(8*10 ³),mbps(8*10 ⁶), gbps, tbps -
Byte/sec	

7. Команда установки приоритета использования доступной полосы пропускания при условии, что обеспечена гарантированная полоса:

```
set qos policy shaper <policy-name> class <class-ID> priority <0-7>
```

где **<0-7>** – значение приоритета. Возможно указать значение в диапазоне от «0» до «7». По умолчанию используется значение «0».

Политику Shaper возможно встроить в класс другой политики с помощью параметра **«queue-type»**:

```
admin@ngfwos# set qos policy shaper <policy-name> class <class-ID> queue-type
```

Possible completions:

drop-tail	First-In-First-Out (FIFO)
fair-queue	Stochastic Fair Queue (SFQ)
fq-codel	Fair Queue Codel (default)
priority	Priority queuing
random-detect	Random Early Detection (RED)

Примечание:

Если сконфигурирован класс для трафика VoIP, не рекомендуется устанавливать для него параметр **«ceiling»**. Возможны обрывы соединения вызовов VoIP, когда другие классы начинают использовать выделенную им полосу пропускания.

Для просмотра информации по доступным Shaper политикам для выбранного интерфейса необходимо в эксплуатационном режиме ввести следующую команду:

```
admin@ngfwos:~$ show qos shaper interface ethN
```

Пример настройки политики с шейпингом к входящему трафику на интерфейсе «eth0»:

```
set qos policy shaper <my-ingress-shaping> bandwidth 1000kbit
set qos policy shaper <my-ingress-shaping> default bandwidth 1000kbit
set qos policy shaper <my-ingress-shaping> default queue-type fair-queue

set qos interface ifb0 egress <my-ingress-shaping>
set interfaces ethernet eth0 redirect ifb0
```

15.4.2.11 CAKE

Порядок организации трафика: Deficit mode.

Применение к направлению трафика: исходящий трафик.

CAKE – Common Applications Kept Enhanced – это комплексная система управления очередями, реализованная в виде дисциплины очередей qdisc для ядра Linux. Она предназначена для замены и улучшения сложной иерархии простых дисков, которая требуется для эффективного решения проблемы переполнения буфера на границе сети.

Список команд настройки CAKE:

1. Команда присвоения уникального имени для политики CAKE:

```
set qos policy cake <policy name>
```

2. Команда установки пропускной способности для политики CAKE:


```
set qos policy cake <policy name> bandwidth <number>
```

где **<number>** – значение пропускной способности.

Возможные варианты указания значения пропускной способности:

```
<number>          бит в секунду  
<number>bit       бит в секунду;  
<number>kbit       килобит в секунду;  
<number>mbit       мегабит в секунду;  
<number>gbit       гигабит в секунду;  
<number>tbit       терабит в секунду;  
<number>%         процент от скорости соединения интерфейса.
```

3. Команда добавления описания:

```
set qos policy cake <policy name> description <text>
```

4. Команда отключения разделения потока:

```
set qos policy cake <policy name> flow-isolation blind
```

Весь трафик проходит через одну очередь.

5. Команда определения потока адресом назначения:

```
set qos policy cake <policy name> flow-isolation dst-host
```

6. Команда определения потока 5-tuple – IP-адрес назначения:

```
set qos policy cake <policy name> flow-isolation dual-dst-host
```

Принимаются сначала к адресам назначения, затем к отдельным потокам.

7. Команда определения потока 5-tuple – IP-адрес источника:

```
set qos policy cake <policy name> flow-isolation dual-src-host
```

Принимаются сначала к адресам источников, затем к отдельным потокам.

8. Команда определения потока всеми атрибутами 5-tuple:

```
set qos policy cake <policy name> flow-isolation flow
```

Потоки определяются всеми атрибутами 5-tuple: IP-адрес источника, порт источника, IP-адрес назначения, порт назначения, транспортный протокол.

9. Команда определения потока парой хостов источник – назначение:

```
set qos policy cake <policy name> flow-isolation host
```

10. Команда поиска NAT перед применением правил изоляции потоков:

```
set qos policy cake <policy name> flow-isolation nat
```

11. Команда определения потока по адресу источника:

```
set qos policy cake <policy name> flow-isolation src-host
```

12. Команда определения потока 5-tuple:

```
set qos policy cake <policy name> flow-isolation triple-isolate
```

Применяется к адресам источника, назначения и к отдельным потокам. Параметр используется по умолчанию.

13. Команда для определения времени прохождения пакетов в оба конца, используемая для активного управления очередью:

```
set qos policy cake <policy name> rtt <rtt>
```

где **<rtt>** – значение времени в миллисекундах. Возможно указать значение в диапазоне от «1» до «3600000». По умолчанию используется значение «100».

14. Для просмотра информации по доступным CAKE политикам для выбранного интерфейса необходимо в эксплуатационном режиме ввести следующую команду:

```
admin@ngfwos:~$ show qos cake interface ethN
```

15.4.3 Применение политики

После конфигурирования политики обработки трафика её необходимо применить к соответствующему интерфейсу:

```
set qos interface <ethN> egress <policy name>
```

где:

- **<ethN>** – идентификатор интерфейса;
- **<policy name>** – имя политики.

Возможно применить только одну политику для каждого интерфейса и направления. Допускается использовать одну политику для разных интерфейсов и направлений:

```
set qos interface eth0 ingress WAN-IN
set qos interface eth0 egress WAN-OUT
set qos interface eth1 ingress LAN-IN
set qos interface eth1 egress LAN-OUT
set qos interface eth2 ingress LAN-IN
set qos interface eth2 egress LAN-OUT
set qos interface eth3 ingress TWO-WAY-POLICY
set qos interface eth3 egress TWO-WAY-POLICY
set qos interface eth4 ingress TWO-WAY-POLICY
set qos interface eth4 egress TWO-WAY-POLICY
```

15.4.4 Примеры настройки политик

Ограничение скорости входящего и исходящего соединений

В качестве примера настройки ограничения скорости будет использоваться схема стенда, представленная на рисунке (см. [Рисунок – Схема стенда для настройки ограничения скорости](#)).

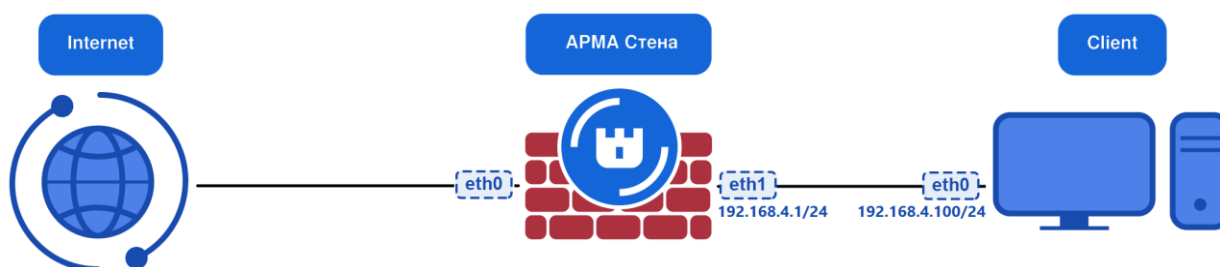


Рисунок – Схема стенда для настройки ограничения скорости

Предварительные настройки **ARMA Стена**:

1. Выполнены настройки получения IP-адресов для интерфейсов eth0 и eth1:

```
set interfaces ethernet eth0 address 'dhcp'
set interfaces ethernet eth0 hw-id-auto-pinning 'false'
set interfaces ethernet eth1 address '192.168.4.1/24'
commit
save
```

2. Выполнены настройки NAT:

```
set nat source rule 10 outbound-interface name 'eth0'
set nat source rule 10 translation address 'masquerade'
commit
save
```

Для ограничения скорости применяются политики **Shaper** для исходящего трафика и **Limiter** для входящего со следующими параметрами:

```
set qos interface eth0 egress 'OUTPUT'
set qos interface eth0 ingress 'INPUT'
set qos policy limiter INPUT default bandwidth '10mbit'
set qos policy shaper OUTPUT default bandwidth '10mbit'
commit
save
```

Маркировка и классификация трафика

В качестве примера настройки маркировки и классификации трафика будет использоваться схема стенда, представленная на рисунке (см. [Рисунок – Схема стенда для настройки маркировки и классификации трафика](#)).

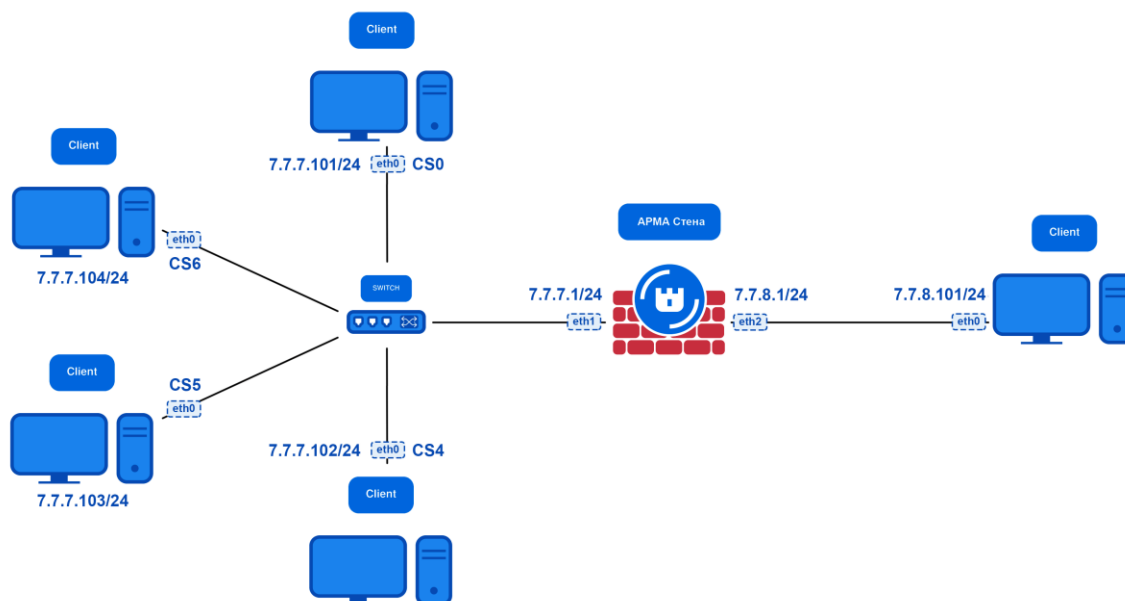


Рисунок – Схема стенда для настройки маркировки и классификации трафика

На **ARMA Стена** предварительно выполнена настройка статического маршрута и разрешён транзитный трафик:

```
set protocols static route 7.7.7.0/24 next-hop 7.7.8.101
set firewall ipv4 forward filter default-action accept
commit
save
```

Для настройки классификации и маркировки трафика необходимо выполнить следующие шаги на **ARMA Стена**:

```
set qos policy shaper ngfw class 10 match ADDRESS10 ip source address
'7.7.7.102/32'
set qos policy shaper ngfw class 10 set-dscp 'CS4'
set qos policy shaper ngfw class 20 match ADDRESS20 ip source address
'7.7.7.103/32'
set qos policy shaper ngfw class 20 set-dscp 'CS5'
set qos policy shaper ngfw class 30 match ADDRESS30 ip source address
'7.7.7.104/32'
set qos policy shaper ngfw class 30 set-dscp 'CS6'
set qos policy shaper ngfw default bandwidth '10%'
set qos policy shaper ngfw default ceiling '100%'
set qos policy shaper ngfw default priority '7'
set qos policy shaper ngfw default queue-type 'fair-queue'
set qos interface eth2 egress 'ngfw'
commit
save
```

Для проверки маркировки и классификации трафика на одном из устройств-клиентов, которые подключены к eth1 **ARMA Стена**, необходимо ввести команду:

```
ping 7.7.8.101
```

Для того, чтобы просмотреть маркировку трафика на **ARMA Стена** в режиме суперпользователя необходимо ввести следующую команду:

```
root@ngfwos:~# tcpdump -i eth2 -v -n -c 10 'ip'
tcpdump: listening on eth2, link-type EN10MB (Ethernet), snapshot length 262144
bytes
14:04:50.981357 IP (tos 0x80, ttl 63, id 18797, offset 0, flags [DF], proto ICMP (1),
length 84)
    7.7.7.102 > 7.7.8.101: ICMP echo request, id 37571, seq 3, length 64
14:04:50.982143 IP (tos 0x80, ttl 64, id 29747, offset 0, flags [none], proto ICMP (1),
length 84)
    7.7.8.101 > 7.7.7.102: ICMP echo reply, id 37571, seq 3, length 64
14:04:51.983178 IP (tos 0x80, ttl 63, id 18978, offset 0, flags [DF], proto ICMP (1),
length 84)
```

В приведенном примере маркировка **tos 0x80** соответствует DSCP **CS4**.

15.5 SNMP

Протокол **SNMP** (Simple Network Management Protocol) предназначен для сбора, организации и управления информацией об управляемых сетевых устройствах в IP-сетях. Протокол позволяет осуществлять мониторинг состояния оборудования,

получение данных о конфигурации и, при необходимости, изменение параметров устройства.

Системы **ARMA Стена** поддерживает **SNMP** версий **SNMPv2c** и **SNMPv3**. Поддерживается работа как в IPv4, так и в IPv6 сетях.

15.5.1 SNMPv2c

SNMPv2c – устаревшая, но широко распространённая версия протокола. Аутентификация осуществляется по строке сообщества (community string), передаваемой в открытом виде. Отсутствует шифрование трафика.

15.5.1.1 Конфигурация SNMPv2c

1. Определить имя сообщества SNMP и уровень доступа:

```
set service snmp community <имя_сообщества> authorization <ro | rw>
```

где:

- **<имя_сообщества>** – имя сообщества SNMP;
- **<ro | rw>** – уровень доступа: **ro** (только чтение) или **rw** (чтение и запись).

2. Разрешить доступ к SNMP-агенту для всех хостов в указанной подсети (IPv4 или IPv6):

```
set service snmp community <имя_сообщества> network <CIDR>
```

где: **<CIDR>** – адрес подсети в формате **<x.x.x.x/x>** или **<h:h:h:h:h:h:h/x>**.

3. Разрешить доступ к SNMP-агенту только с указанного IP-адреса:

```
set service snmp community <имя_сообщества> client <IP-адрес>
```

где: **<IP-адрес>** – IP-адрес SNMP-клиента.

4. Установить текстовое описание физического местоположения устройства:

```
set service snmp location "<местоположение>"
```

где: **<местоположение>** – краткое описание местоположения устройства.

5. Указать контактную информацию администратора:

```
set service snmp contact "<контакт>"
```

где: **<контакт>** – контактную информацию администратора (например, email).

6. Задать адрес NMS:

```
set service snmp trap-target <IP-адрес_цели>
```

где: **<IP-адрес_цели>** – адрес NMS в формате <x.x.x.x> или <h:h:h:h:h:h:h>, на который устройство будет отправлять асинхронные уведомления (traps) при наступлении событий.

7. Ограничить прослушивание SNMP-агента указанным IP-адресом и портом:

```
set service snmp listen-address <IP-адрес> port <порт>
```

где:

- **<IP-адрес>** – IP-адрес в формате <x.x.x.x> или <h:h:h:h:h:h:h>. По умолчанию – 0.0.0.0;
- **<порт>** – номер порта. Возможно указать значения в диапазоне от «1» до «65535». По умолчанию используется 161 порт.

Примечание:

В качестве адреса прослушивания рекомендуется указывать только статические IP-адреса. Применение динамических адресов, предоставляемых протоколом DHCP, или виртуальных IP-адресов, распределяемых группой VRRP, может привести к невозможности запуска службы SNMP после перезагрузки устройства, что, в свою очередь, может вызвать переход системы в аварийный режим.

15.5.2 SNMPv3

SNMPv3 обеспечивает повышенный уровень безопасности за счёт поддержки аутентификации, шифрования и контроля целостности сообщений.

Поддерживаемые механизмы безопасности:

- Аутентификация: **SHA** или **MD5**.
- Шифрование (privacy): **AES** (128 бит) или **DES**.
- Уровни безопасности:
 - **noAuthNoPriv** – без аутентификации и шифрования;
 - **authNoPriv** – аутентификация, без шифрования;
 - **authPriv** – аутентификация и шифрование (рекомендуется).

15.5.2.1 Конфигурация SNMPv3

1. Задать уникальный идентификатор **SNMP**-агента (Engine ID) в шестнадцатеричном формате:

```
set service snmp v3 engineid <HEX-строка>
```

где **<HEX-строка>** - уникальный идентификатор SNMP-агента. Необходим для корректной работы SNMPv3, особенно при шифровании.

2. Создать группу пользователей **SNMPv3** с указанным уровнем доступа:

```
set service snmp v3 group <имя_группы> mode <ro | rw>
```

где:

- **<имя_группы>** - имя группы пользователей **SNMPv3**;
- **<ro | rw>** - уровень доступа: **ro** (только чтение) или **rw** (чтение и запись).

3. Связать группу с представлением (view), определяющим, какие OID доступны для просмотра:

```
set service snmp v3 group <имя_группы> view <имя_представления>
```

4. Установить пароль аутентификации для пользователя:

```
set service snmp v3 user <имя_пользователя> auth plaintext-password <пароль>
```

где:

- **<имя_пользователя>** – имя пользователя;
- **<пароль>** – значение пароля для пользователя.

5. Определить алгоритм хеширования для аутентификации:

```
set service snmp v3 user <имя_пользователя> auth type <sha | md5>
```

где **<sha | md5>** – алгоритм хеширования для аутентификации: «sha» или «md5» (по умолчанию).

6. Установить пароль шифрования (privacy password) для защиты данных при передаче:

```
set service snmp v3 user <имя_пользователя> privacy plaintext-password <пароль>
```

где **<пароль>** – значение пароля.

7. Указать алгоритм шифрования:

```
set service snmp v3 user <имя_пользователя> privacy type <aes | des>
```

где **<aes | des>** – алгоритм шифрования: «aes» или «des» (по умолчанию).

8. Назначить пользователя в указанную группу, наследуя её права доступа и настройки:

```
set service snmp v3 user <имя_пользователя> group <имя_группы>
```


9. Определить дерево OID, доступное в рамках данного представления:

```
set service snmp v3 view <имя_представления> oid <OID>
```

где **<OID>** – дерево OID. При указании значения «1» открывается доступ ко всем OID.

15.5.2.2 Пример настройки SNMPv3

Настроить демон SNMP на прослушивание только IP-адреса 10.10.10.100. Создать нового пользователя SNMP с именем «арма» и паролём «Fr424!dfT». Новый пользователь будет использовать SHA/AES для аутентификации и шифрования.

1. Настройка системы **ARMA Стена**.

```
set service snmp listen-address 10.10.10.100
set service snmp location 'ARMA'
set service snmp v3 engineid '000000000000000000000002'
set service snmp v3 group default mode 'ro'
set service snmp v3 group default view 'default'
set service snmp v3 user arma auth plaintext-password 'Fr424!dfT'
set service snmp v3 user arma auth type 'sha'
set service snmp v3 user arma group 'default'
set service snmp v3 user arma privacy plaintext-password 'Fr424!dfT'
set service snmp v3 user arma privacy type 'aes'
set service snmp v3 view default oid 1

commit
save
```

2. Настройка SNMP-менеджера.

На пользовательском компьютере под управлением операционной системы семейства Windows установлено ПО мониторинга «PowerSNMP Free Manager».

Для корректного отображения дерева объектов **ARMA Стена** в «PowerSNMP Free Manager» следует импортировать все файлы из каталога «**/usr/share/snmp/mibs/**» системы **ARMA Стена**.

Для проверки работы **SNMPv.3** необходимо выполнить следующие действия:

1. В ПО «PowerSNMP Free Manager» нажать **правой кнопкой мыши** на строку «**SNMP Agents**» и выбрать «**Add Agent**».
2. В нижней части открывшегося окна нажать кнопку «**Add Agent**», ввести IP-адрес **ARMA Стена**, выбрать версию протокола «3», указать данные для аутентификации, заданные ранее в системе **ARMA Стена**, нажать «**ОК**» (см. [Рисунок – Добавление SNMP агента \(SNMP v.3\)](#)) и нажать «**ОК**».

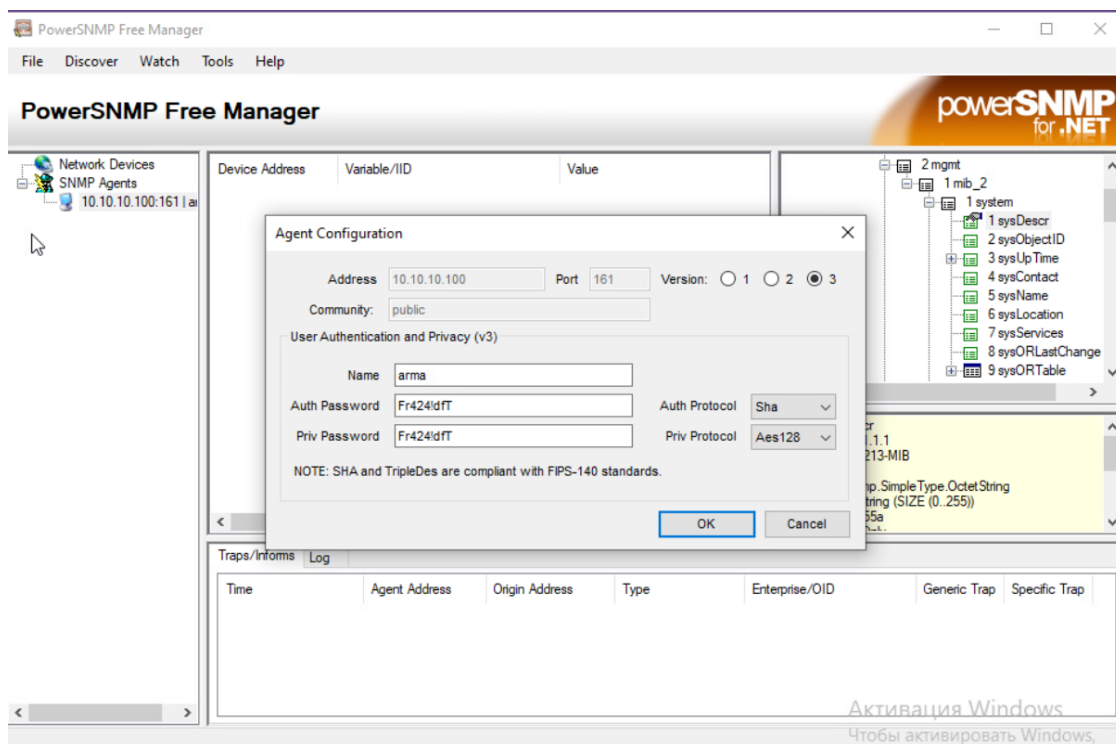


Рисунок – Добавление SNMP агента (SNMPv.3)

3. В правой области окна, в дереве доступных данных выбрать поле «1 sysDescr», нажать **правой кнопкой мыши** по IP-адресу **ARMA Стена** в левой области окна и выбрать «Query...». Результатом будет получение информации о версии системы **ARMA Стена**.

15.5.3 MIB-файлы

MIB-файл представляет собой БД, содержащую информацию об объектах устройства, с которым предстоит работа по протоколу SNMP. MIB-файл может быть использован при работе с ПО мониторинга SNMP.

MIB-файлы, описывающие OID-дерево системы **ARMA Стена**, доступны в системе по пути: «**/usr/share/snmp/mibs/**»

15.6 Stunnel

Stunnel позволяет обеспечить шифрование сетевого трафика с использованием протокола **TLS**, создавая защищённый туннель между клиентами и серверами. В системе **ARMA Стена Stunnel** реализован как прозрачная обёртка, добавляющая поддержку безопасных соединений для сервисов, изначально не предусматривающих шифрование – таких как POP3, IMAP, SMTP и других.

Для корректной работы требуется установка **Stunnel** как на клиентской, так и на серверной стороне, а также использование единого сертификата на обоих концах соединения.

Конфигурирование хранилища сертификатов

Для регистрации сертификатов в системе необходимо выполнить следующие команды:

```
set pki ca <ca_name> certificate <namecertserver>
```

где:

- **<ca_name>** – имя корневого центра сертификации (CA);
- **<namecertserver>** – имя сертификата.

```
set pki certificate <namecertserver> certificate <ExampleContentServCert>
```

где:

- **<ExampleContentServCert>** – содержимое сертификата в формате PEM, извлечённое из файла «*.pem», за исключением строк «BEGIN CERTIFICATE» и «END CERTIFICATE», без пробелов и переносов строк.

```
set pki certificate <namekeyserver> private key <ExampleContentServKey>
```

где:

- **<ExampleContentServKey>** – содержимое закрытого ключа из файла «*.key», указанное без строк «BEGIN CERTIFICATE» и «END CERTIFICATE», без пробелов и переносов строк.

15.6.1 Общие настройки stunnel

Установка уровня журналирования:

```
set service stunnel log level <level>
```

где **<level>** – уровень детализации логирования. Допустимые значения:

- **«emerg»** – чрезвычайная ситуация;
- **«alert»** – тревога;
- **«crit»** – критическое состояние;
- **«err»** – ошибка;
- **«warning»** – предупреждение;
- **«notice»** – уведомление (по умолчанию);
- **«info»** – информационное сообщение;
- **«debug»** – отладочная информация.

Включение/отключение записи событий **Stunnel** в глобальный системный журнал:

```
set service stunnel log syslog yes|no
```

По умолчанию для параметра установлено значение «**yes**» – запись событий в системный журнал включена.

15.6.2 Настройка серверного режима

Задание адреса и порта удалённого сервера, к которому будет перенаправлен трафик через защищённый SSL/TLS-туннель:

```
set service stunnel server <name_server> connect address <address>
set service stunnel server <name_server> connect port <port>
```

где:

- **<name_server>** – пользовательское имя логического контейнера экземпляра **Stunnel**, объединяющего параметры одного туннелируемого соединения;
- **<address>** – IP-адрес (IPv4) или имя хоста (FQDN) целевого сервера. При отсутствии значения используется «localhost»;
- **<port>** – TCP-порт удалённого сервера (обязательный параметр). Возможно указать значение в диапазоне от «1» до «65535».

Настройка адреса и порта, на котором **Stunnel** принимает входящие соединения:

```
set service stunnel server <name_server> listen address <address>
set service stunnel server <name_server> listen port <port>
```

где:

- **<address>** – IP-адрес или имя хоста (FQDN), на котором ожидается подключение. По умолчанию используется привязка ко всем IPv4-адресам локального хоста. Для прослушивания всех IPv6-адресов необходимо использовать значение «::»;
- **<port>** – указать TCP-порт, на котором осуществляется приём соединений (обязательный параметр). Возможно указать значение в диапазоне от «1» до «65535».

Указание прикладного протокола для согласования TLS-сессии:

```
set service stunnel server <name_server> protocol <protocol>
```

где **<protocol>** – имя поддерживаемого прикладного протокола. Поддерживаемые значения:

- **cifs** – проприетарное расширение протокола CIFS (Common Internet File System), требующее специальной обработки перед началом TLS;
- **imap** – поддержка RFC 2595 (STARTTLS для IMAP);

- **pgsql** – протокол PostgreSQL с запросом шифрования через SSLRequest;
- **pop3** – поддержка RFC 2449 (STLS для POP3);
- **proxy** – протокол HAProxy PROXY v1, сохраняющий исходный IP-адрес клиента;
- **smtp** – поддержка TLS по RFC 2487 – SMTP Service Extension for Secure SMTP over TLS. Клиент отправляет команду STARTTLS, после чего сервер инициирует переход к шифрованию;
- **socks** – поддержка SOCKS-протоколов версий 4, 4a и 5, шифрование устанавливается до начала передачи данных.

Настройка сертификатов для установления TLS-соединения:

```
set service stunnel server <name_server> ssl ca-certificate <ca_name>  
set service stunnel server <name_server> ssl certificate <namecertserver>
```

где:

- **<ca_name>** – имя СА, используемого для проверки клиентских сертификатов при включённой аутентификации;
- **<namecertserver>** – имя сертификата сервера, представленного клиенту. Параметр является обязательным.

Уровень проверки сертификата удалённой стороны (пира):

```
set service stunnel server <name_server> verify <number>
```

где **<number>** - целое число. Доступные значения:

- **0** – запрашивать сертификат пира, но игнорировать цепочку (установлено по умолчанию). Сервер может запросить сертификат у клиента, но не проверяет его подлинность.
- **1** – проверять цепочку сертификатов пира, если она предоставлена. Если клиент представил сертификат, stunnel проверяет его цепочку доверия. Если сертификат отсутствует – соединение разрешается.
- **2** – обязательно проверять цепочку сертификатов пира. Клиент обязан предоставить действительный сертификат, подписанный доверенным СА, указанным в параметре ca-certificate. Без корректного сертификата соединение будет отклонено.
- **3** – проверять цепочку и сравнивать конечный сертификат с локально установленным. Помимо проверки цепочки доверия, stunnel дополнительно сверяет представленный клиентский сертификат с конкретным сертификатом, заранее размещённым в системе.

Обеспечивает высокий уровень безопасности – допускаются только заранее известные клиенты.

- **4** – игнорировать цепочку, но проверять конечный сертификат по локальной копии. Цепочка сертификатов не проверяется, но stunnel требует, чтобы клиент представил сертификат, идентичный одному из локально установленных.

15.6.3 Настройка клиентского режима

Указание адреса и порта удалённого сервера:

```
set service stunnel client <name_client> connect address <address>
set service stunnel client <name_client> connect port <port>
```

где:

- **<name_client>** – имя логического контейнера клиентского экземпляра **Stunnel**;
- **<address>** – IP-адрес (IPv4) или имя хоста (FQDN) целевого сервера. Если параметр не задан, используется значение по умолчанию – «localhost»;
- **<port>** – TCP-порт назначения (обязательный параметр). Возможно указать значение в диапазоне от «1» до «65535».

Указание адреса и порта для приёма входящих соединений на клиенте:

```
set service stunnel client <name_client> listen address <address>
set service stunnel client <name_client> listen port <port>
```

где:

- **<address>** – IP-адрес или имя хоста (FQDN), на котором будет ожидаться входящее соединение. При отсутствии указания хоста по умолчанию используется привязка ко всем IPv4-адресам локального хоста. Для прослушивания всех IPv6-адресов необходимо использовать значение «::»;
- **<port>** – TCP-порт наприёма соединений (обязательный параметр). Возможно указать значение в диапазоне от «1» до «65535».

Указание прикладного протокола для согласования TLS-сессии:

```
set service stunnel client <name_client> protocol <protocol>
```

где **<protocol>** – имя поддерживаемого прикладного протокола. Поддерживаемые значения:

- **cifs** – проприетарное расширение протокола CIFS (Common Internet File System), требующее специальной обработки перед началом TLS;
- **connect** – реализация механизма туннелирования по методу CONNECT, описанному в RFC 2817 (раздел 5.2), предназначенному для перехода на TLS в рамках HTTP/1.1;
- **imap** – поддержка защищённого соединения для протокола IMAP в соответствии с RFC 2595;
- **nnntp** – интеграция с NNTP с применением TLS согласно RFC 4642;
- **pgsql** – поддержка протокола взаимодействия между клиентом и сервером СУБД PostgreSQL;
- **pop3** – обеспечение безопасного соединения для POP3 на основе механизма расширений, описанного в RFC 2449;
- **proxy** – передача исходного IP-адреса клиента с использованием HAProxy PROXY-протокола версии 1;
- **smtp** – реализация расширения SMTP для работы поверх TLS в соответствии с RFC 2487;
- **socks** – поддержка SOCKS-протоколов версий 4, 4a и 5, шифрование устанавливается до начала передачи данных.

Настройка сертификатов для клиентского соединения:

```
set service stunnel client <name_client> ssl ca-certificate <ca_name>  
set service stunnel client <name_client> ssl certificate <namecertserver>
```

где:

- **<ca_name>** – имя CA для проверки сертификата сервера;
- **<namecertserver>** – имя клиентского сертификата, предоставляемого серверу при двухсторонней аутентификации.

Уровень проверки сертификата сервера:

```
set service stunnel client <name_client> verify <number>
```

где **<number>** – целое число. Доступные значения:

- **0** – запрашивать сертификат пира, но игнорировать цепочку (установлено по умолчанию). Сервер может запросить сертификат у клиента, но не проверяет его подлинность.
- **1** – проверять цепочку сертификатов пира, если она предоставлена. Если клиент представил сертификат, stunnel проверяет его цепочку доверия. Если сертификат отсутствует – соединение разрешается.

- **2** – обязательно проверять цепочку сертификатов пира. Клиент обязан предоставить действительный сертификат, подписанный доверенным СА, указанным в параметре `ca-certificate`. Без корректного сертификата соединение будет отклонено.
- **3** – проверять цепочку и сравнивать конечный сертификат с локально установленным. Помимо проверки цепочки доверия, `stunnel` дополнительно сверяет представленный клиентский сертификат с конкретным сертификатом, заранее размещённым в системе. Обеспечивает высокий уровень безопасности – допускаются только заранее известные клиенты.
- **4** – игнорировать цепочку, но проверять конечный сертификат по локальной копии. Цепочка сертификатов не проверяется, но `stunnel` требует, чтобы клиент представил сертификат, идентичный одному из локально установленных.

Определить метод аутентификации, используемый при взаимодействии с промежуточным сервером (например, HTTP-прокси или SMTP-сервер) в рамках протоколов, поддерживающих авторизацию:

```
set service stunnel client <name_client> options authentication <method>
```

где **<method>** – метод аутентификации. Поддерживаемые методы:

- **basic** – протокол connect – HTTP Basic Auth (RFC 7617), используется по умолчанию для протокола connect;
- **ntlm** – протокол connect – NTLM-аутентификация, более безопасна, чем basic;
- **plain** – протокол smtp – механизм PLAIN (RFC 4616), применяется по умолчанию для SMTP при включённой авторизации;
- **login** – протокол smtp – классическая SMTP-аутентификация с последовательной передачей логина и пароля.

Параметр применяется только для протоколов, поддерживающих аутентификацию (connect, smtp), и выполняется до установления TLS-туннеля.

Указание домена для NTLM-аутентификации:

```
set service stunnel client <name_client> options domain <fqdn>
```

где **<fqdn>** – полное доменное имя, используемое при NTLM-аутентификации через HTTP-прокси.

Целевой хост и порт для прокси-подключения:


```
set service stunnel client <name_client> options host address <address>  
set service stunnel client <name_client> options host port <port>
```

где:

- **<address>** – IP-адрес (IPv4) или имя хоста (FQDN) конечного сервера, доступ к которому осуществляется через прокси;
- **<port>** – TCP-порт конечного сервера. Возможно указать значение в диапазоне от «1» до «65535».

Учётные данные для аутентификации на промежуточном сервере:

```
set service stunnel client <name_client> options username <username>  
set service stunnel client <name_client> options password <password>
```

где:

- **<username>** – имя пользователя;
- **<password>** – пароль.

Данные параметры используются при необходимости прохождения аутентификации на HTTP-прокси или SMTP-сервере.

15.7 LLDP

LLDP (Link Layer Discovery Protocol) – это независимый от производителя протокол канального уровня в стеке протоколов Интернета, используемый сетевыми устройствами для объявления своей идентичности, возможностей и поиска соседей в локальной сети.

Информация, собранная с помощью LLDP, хранится на устройстве в виде MIB (Management Information Base) и может быть запрошена с помощью SNMP.

Служба LLDP – это демон, позволяющий **ARMA Стена** посредством протокола LLDP идентифицировать устройства локальной сети и обмениваться информацией о своих характеристиках.

К информации, которую можно получить, относятся:

- Имя и описание системы.
- Имя и описание порта.
- Имя VLAN.
- IP-адрес управления.
- Возможности системы (коммутация, маршрутизация и т. д.).
- Информация о MAC/PHY.
- Питание по MDI (Power over Ethernet).

- Агрегация каналов (Link aggregation).

Примечание:

LLDP не использует шифрование и работает на канальном уровне. Он не может использоваться в публичных сетях и должен быть отключён для интерфейсов, на которых он не используется.

15.7.1 Общие настройки LLDP

Основные настройки

Для настройки сервиса LLDP используются следующие команды конфигурационного режима:

1. Отключить сервис LLDP:

```
set service lldp disable
```

2. Задать интерфейс для работы сервиса:

```
set service lldp interface <interface-name>
```

где **<interface-name>** – имя интерфейса. Допускается использование всех доступных интерфейсов с помощью указания значения **«all»**.

3. Задать протоколы, которые будут использоваться при работе сервиса:

```
set service lldp legacy-protocols <protocol>
```

где **<protocol>** – имя протокола. Возможно указание следующих протоколов:

- **«cdp»** – Cisco Discovery;
- **«edp»** – Extreme Discovery;
- **«fdp»** – Foundry Discovery;
- **«sonmp»** – Nortel/SynOptics Network Management.

4. Указать IP-адрес для удалённого управления устройством, передаваемый через LLDP:

```
set service lldp management-address <IPv4 | IPv6>
```

где **<IPv4 | IPv6>** – IPv4 или IPv6 адрес в формате **<x.x.x.x>** или **<h:h:h:h:h:h:h>** соответственно.

5. Разрешить доступ к информации LLDP с помощью SNMP-запросов:

```
set service lldp snmp
```

6. Задать интервал для отправки LLDP-пакетов:

```
set service lldp transmit-interval <interval>
```

где **<interval>** – интервал отправки пакетов в секундах. Возможно указание значения в диапазоне от «**30**» до «**300**». По умолчанию используется значение «**30**».

Пример настройки

```
set service lldp interface all
set service lldp legacy-protocols cdp
set service lldp legacy-protocols edp
set service lldp legacy-protocols fdp
set service lldp transmit-interval 100
commit
save
```

Проверка работы LLDP

Для проверки работы сервиса LLDP можно выполнить в эксплуатационном режиме команду для отображения списка соседей:

```
admin@ngfwos:~$ show lldp neighbours
Capability Codes: R - Router, B - Bridge, W - Wlan r - Repeater, S - Station
                  D - Docsis, T - Telephone, O - Other
```

Device	Local Port	Port	Protocol	Capability	Platform
Remote Port	RID	Age	ID	Value	Mgmt IP
TTL					
ngfwos	eth0		LLDP	R	NGFWOS 4.7.0
eth0	2	0 day, 00:01:31	00:50:56:bd:8c:53	192.168.1.10,	
fe80::200:ff:fe00:0	120				
ngfwos	eth1		LLDP	R	NGFWOS 4.7.0
eth1	2	0 day, 00:01:31	00:50:56:bd:83:0c	192.168.1.10,	
fe80::200:ff:fe00:0	120				
ngfwos	eth2		LLDP	R	NGFWOS 4.7.0
eth2	2	0 day, 00:01:31	00:50:56:bd:63:bc	192.168.1.10,	
fe80::200:ff:fe00:0	120				

15.8 Interface State Sender

Сервис Interface State Sender (ISS) используется для проверки состояния интерфейсов **ARMA Стена** при работе со сторонними системами диспетчерского управления и сбора данных (SCADA). Во время работы сервис проверяет статус интерфейса и передает его посредством изменения состояния TCP соединения.

Сервис имеет два режима работы – клиент и сервер. В режиме клиента сервис подключается к серверу, который развёрнут на SCADA системе. В режиме сервера позволяет выполнить подключение к себе клиентом, который используется SCADA системой. Во время работы сервис выполняет логирование в rsyslog.

15.8.1 Общие настройки ISS

Основные настройки

Для настройки сервиса Interface State Sender используются следующие команды конфигурационного режима:

1. Включить сервис Interface State Sender:

```
set service interface-state-sender enabled yes
```

2. Задать режим работы сервиса для указанного интерфейса:

```
set service interface-state-sender interface <interface-name> <client-mode |  
server-mode>
```

где:

- **<interface-name>** – имя интерфейса;
- **«client-mode»** – работа в режиме клиента;
- **«server-mode»** – работа в режиме сервера.

Примечание:

Сервис может использоваться как в роли сервера или клиента, так и быть сервером и клиентом одновременно.

3. Указать IP-адрес, к которому будет выполняться подключение при работе сервиса в режиме клиента:

```
set service interface-state-sender interface <interface-name> client-mode  
address <IP-address>
```

где **<IP-address>** – IPv4 адрес в формате **<x.x.x.x>**.

4. Указать порт, по которому будет выполняться подключение при работе сервиса в режиме клиента:

```
set service interface-state-sender interface <interface-name> client-mode port  
<port>
```

где **<port>** – порт в диапазоне от «1» до «65535».

5. Указать IP-адрес который будет прослушиваться сервисом при работе в режиме сервера:

```
set service interface-state-sender interface <interface-name> server-mode  
address <IP-address>
```

где **<IP-address>** - IPv4 адрес в формате **<x.x.x.x>**. По умолчанию используется значение **«0.0.0.0»**.

6. Указать порт, который будет использоваться сервисом при работе в режиме сервера:

```
set service interface-state-sender interface <interface-name> server-mode port  
<port>
```

где **<port>** - порт в диапазоне от «1» до «65535».

7. Задать интервал проверки состояния интерфейсов:

```
set service interface-state-sender check-timeout <timeout>
```

где **<timeout>** - интервал проверки состояния в секундах. По умолчанию используется значение **«5»**.

8. Указать интервал для отправки проверочных пакетов:

```
set service interface-state-sender keepalive-interval <interval>
```

где **<interval>** - временной интервал в секундах между проверочными пакетами. По умолчанию используется значение **«75»**.

Пример настройки

В качестве примера представлена настройка сервиса ISS для интерфейсов eth1 и eth2 **ARMA Стена**:

```
set service interface-state-sender enable  
set service interface-state-sender interface eth1 client-mode address 192.168.102.13  
set service interface-state-sender interface eth1 client-mode port 50101  
set service interface-state-sender interface eth1 server-mode address 192.168.102.14  
set service interface-state-sender interface eth1 server-mode port 50102  
set service interface-state-sender interface eth2 client-mode address 192.168.101.13  
set service interface-state-sender interface eth2 client-mode port 50101  
set service interface-state-sender interface eth2 server-mode address 192.168.101.16  
set service interface-state-sender interface eth2 server-mode port 50104  
commit  
save
```

Проверка работы ISS

При корректной работе сервиса ISS в rsyslog **ARMA Стена** появятся следующие записи:

```
Nov 12 11:31:25 ngfwos systemd[1]: Started interface-state-sender.service - Service
to send network interfaces status.
Nov 12 11:31:25 ngfwos interface-state-sender[10666]: interface-state-sender
started
Nov 12 11:31:25 ngfwos interface-state-sender[10666]: [supervisor] Started
server:eth1 for 192.168.102.14:50102
Nov 12 11:31:25 ngfwos interface-state-sender[10666]: [supervisor] Started
client:eth1 for 192.168.102.13:50101
Nov 12 11:31:25 ngfwos interface-state-sender[10666]: [supervisor] Started
server:eth2 for 192.168.101.16:50104
Nov 12 11:31:25 ngfwos interface-state-sender[10666]: [supervisor] Started
client:eth2 for 192.168.101.13:50101
Nov 12 11:31:27 ngfwos interface-state-sender[10666]: [server:eth1] Accepted
connection from ('192.168.102.14', 49716)
Nov 12 11:31:27 ngfwos interface-state-sender[10666]: [client:eth1] Connected to
192.168.102.13:50101
```

16 ПРОКСИ-СЕРВЕР

Прокси-сервер обеспечивает контролируемый доступ хостов локальной сети в сеть Интернет, а также защиту локальной сети от внешнего доступа.

Примечание:

В случае установки блокировки всего входящего и/или исходящего трафика по протоколу IPv4 и/или IPv6 в МЭ, для корректной работы прокси-сервера необходимо добавить разрешающие правила, обеспечивающие обработку трафика через loopback:

Для IPv4-трафика:

```
# Для входящего трафика:
set firewall ipv4 input filter rule 5 action accept
set firewall ipv4 input filter rule 5 destination address 127.0.0.1
set firewall ipv4 input filter rule 5 description "Allow IPv4 loopback"

# Для исходящего трафика:
set firewall ipv4 output filter rule 5 action accept
set firewall ipv4 output filter rule 5 source address 127.0.0.1
set firewall ipv4 output filter rule 5 description "Allow IPv4 loopback"
```

Для IPv6-трафика:

```
# Для входящего трафика:
set firewall ipv6 input filter rule 5 action accept
set firewall ipv6 input filter rule 5 destination address ::1/128
set firewall ipv6 input filter rule 5 description "Allow IPv6 loopback"

# Для исходящего трафика:
set firewall ipv6 output filter rule 5 action accept
set firewall ipv6 output filter rule 5 source address ::1/128
set firewall ipv6 output filter rule 5 description "Allow IPv6 loopback"
```

16.1 Основные настройки прокси-сервера

1. Для указания порта по умолчанию, на котором прокси-сервер будет прослушивать запросы, необходимо ввести следующую команду:

```
set service webproxy default-port <portnumber>
```

где **<portnumber>** – номер порта. Возможно указание значения в диапазоне от «1025» до «65535». По умолчанию используется порт «3128».

2. Задать IPv4-адрес сетевого интерфейса, на котором прокси-сервер будет прослушивать запросы пользователей:

```
set service webproxy listen-address <x.x.x.x>
```

где **<x.x.x.x>** – IPv4-адрес. В целях обеспечения безопасности адрес прослушивания должен использоваться только в локальных/защищённых сетях.

3. Указать порт, на котором прокси-сервер будет прослушивать запросы:

```
set service webproxy listen-address <x.x.x.x> port <portnumber>
```

где **<portnumber>** – номер порта. Возможно указание значения в диапазоне от «1025» до «65535». По умолчанию применяется значение, заданное параметром **«default-port»**.

В режиме прозрачного прокси данная команда определяет порт прослушивания HTTP-трафика для указанного IPv4-адреса. В непрозрачном режиме указанный порт используется для прослушивания как HTTP-, так и HTTPS-трафика на соответствующем IPv4-адресе.

4. Установить отличный от значения по умолчанию номер порта для указанного IPv4-адреса прокси, используемого для HTTPS трафика в прозрачном режиме работы прокси-сервер:

```
set service webproxy listen-address <x.x.x.x> https-port <portnumber>
```

где **<portnumber>** – номер TCP-порта, на котором прокси-сервер будет ожидать соединение. Возможно указание значения в диапазоне от «1025» до «65535». По умолчанию используется значение «3129».

Данная команда предназначена для перенастройки прокси-сервера на ожидание соединений по другому порту, отличному от используемого по умолчанию для HTTPS трафика. Перенастройка выполняется только для сетевого интерфейса, связанного с указанным IP-адресом.

5. Отключить прозрачный режим работы прокси-сервер на прослушиваемом адресе:

```
set service webproxy listen-address <x.x.x.x> disable-transparent
```

Данная команда предназначена для отключения прозрачного режима работы прокси-сервера для запросов, поступающих на сетевой интерфейс системы **ARMA Стена**, связанный с указанным IP-адресом. В случае отключения прозрачного прокси-сервера на клиентских машинах необходимо указать настройки прокси-сервера.

6. Запретить доступ к указанному домену:

```
set service webproxy domain-block <domain>
```


где **<domain>** – домен, доступ к которому нужно закрыть. Например, указание «facebook.com» в качестве аргумента закрывает весь доступ к домену facebook.com и его поддоменам, а указание «.cn» закрывает доступ ко всем сайтам доменной зоны Китая.

7. Запретить доступ к веб-содержимому указанного типа:

```
set service webproxy reply-block-mime <тип_mime>
```

где **<тип_mime>** – тип mime, доступ к которому будет закрыт. Типы mime задаются в виде «тип/подтип». К примеру, тип mime видео в формате Quicktime выглядит как «video/quicktime», тип mime для файлов в формате PDF – как «application/pdf», а тип mime для файлов .wav – как «audio/wav».

Поддерживается блокирование следующих типов mime:

- application/andrew-inset;
- application/mac-binhex40;
- application/mac-compactpro;
- application/macbinary;
- application/macwriteii;
- application/msword;
- application/octet-stream;
- application/oda;
- application/pdf;
- application/pict;
- application/postscript;
- application/smil;
- application/vnd.lotus-1-2-3;
- application/vnd.mif;
- application/vnd.ms-excel;
- application/vnd.ms-powerpoint;
- application/vnd.wap.wbxml;
- application/vnd.wap.wmlc;
- application/vnd.wap.wmlscript;
- application/vnd.wap.wmlscriptc;
- application/x-arj-compressed;

- application/x-bcpio;
- application/x-cdlink;
- application/x-chess-pgn;
- application/x-cpio;
- application/x-csh;
- application/x-deflate;
- application/x-director;
- application/x-dvi;
- application/x-futuresplash;
- application/x-gtar;
- application/x-hdf;
- application/x-javascript;
- application/x-koan;
- application/x-latex;
- application/x-lha-compressed;
- application/x-netcdf;
- application/x-rpm;
- application/x-sh;
- application/x-shar;
- application/x-shockwave-flash;
- application/x-stuffit;
- application/x-sv4cpio;
- application/x-sv4crc;
- application/x-tar;
- application/x-tcl;
- application/x-tex;
- application/x-texinfo;
- application/x-troff;
- application/x-troff-man;
- application/x-troff-me;
- application/x-troff-ms;

- application/x-ustar;
- application/x-wais-source;
- application/x-xpinstall;
- application/xhtml;
- application/zip;
- audio/basic;
- audio/midi;
- audio/mpeg;
- audio/x-aiff;
- audio/x-pn-realaudio;
- audio/x-realaudio;
- audio/x-wav;
- chemical/x-pdb;
- chemical/x-xyz;
- image/bmp;
- image/gif;
- image/ief;
- image/jpeg;
- image/png;
- image/tiff;
- image/vnd.djvu;
- image/vnd.wap.wbmp;
- image/x-cmu-raster;
- image/x-portable-anymap;
- image/x-portable-bitmap;
- image/x-portable-graymap;
- image/x-portable-pixmap;
- image/x-rgb;
- image/x-xbitmap;
- image/x-xpixmap;
- image/x-xwindowdump;

- model/iges;
- model/mesh;
- model/vrml;
- text/css;
- text/html;
- text/plain;
- text/richtext;
- text/rtf;
- text/sgml;
- text/tab-separated-values;
- text/x-setext;
- text/xml;
- video/mpeg;
- video/quicktime;
- video/vnd.mpegurl;
- video/x-msvideo;
- video/x-sgi-movie;
- www/mime;
- x-conference/x-cooltalk.

8. Включить аутентификацию пользователей в прокси:

```
set service webproxy authentication enable
```

9. Указать используемый метод аутентификации пользователей прокси:

```
set service webproxy authentication <method>
```

где **<method>** – метод аутентификации.

ARMA Стена поддерживает следующие методы аутентификации:

- **«kerberos»** – аутентификация на основе протокола Kerberos;
- **«ldap»** – аутентификация на основе протокола LDAP;
- **«ntlm»** – аутентификация на основе протокола NTLM.

10. Указать максимальное количество запускаемых процессов аутентификации:

```
set service webproxy authentication children <number>
```

где **<number>** – количество процессов аутентификации. По умолчанию используется значение «5».

11. Указать временной интервал между запросами учётных данных пользователя:

```
set service webproxy authentication credentials-ttl <number>
```

где **<number>** – интервал, исчисляемый в минутах. По умолчанию используется значение «60».

12. Указать текст, который должен быть сообщён клиенту в схеме аутентификации:

```
set service webproxy authentication realm "ARMA proxy auth"
```

где **«ARMA proxy auth»** – текст, который будет отображаться пользователю при запросе имени пользователя и пароля.

13. Выключить кэширование данных, полученных с указанного домена в ответ на запросы пользователей:

```
set service webproxy domain-noncache <domain>
```

где **<domain>** – имя домена, данные с которого в кэш помещаться не будут. Если домен в команде не указан, то в кэш помещается всё содержимое, не противоречащее другим ограничениям.

14. Указать доменное имя, которое будет присоединяться к каждому URL, доменная часть которого не содержит точек, перед его дальнейшей обработкой:

```
set service webproxy append-domain <domain>
```

где **<domain>** – имя домена, которое будет присоединяться к доменной части URL. Например, если в рассматриваемой команде указано доменное имя «infowatch.ru», а запрос пользователя обращается по URL «www/abc.html», то в результате присоединения в дальнейшую обработку пойдёт URL «www.infowatch.ru/abc.html».

15. Указать размера кэша - хранилища для временного хранения содержимого:

```
set service webproxy cache-size <num>
```

где **<num>** – объём дискового пространства, указываемый в мегабайтах. Возможно указать значение в диапазоне от «0» до «4294967295». По умолчанию используется значение «0», т.е. кэширование не производится.

16. Ограничение входящей скорости передачи данных для определённых IP-адресов:

16.1 Команда создания списка контроля доступа:

```
set service webproxy limit <name>
```

где **<name>** – имя списка контроля доступа.

16.2 Команда установки максимальной входящей скорости передачи данных для указанного списка контроля доступа:

```
set service webproxy limit <name> speed <1-10000000>
```

где **<1-10000000>** – значение максимальной скорости передачи данных в Кбит/сек.

16.3 Команда добавления IP-адреса в указанный список контроля доступа:

```
set service webproxy limit <name> ip-address <ip>
```

где **<ip>** – IP-адрес в форматах <x.x.x.x>, <x.x.x.x/x> для IPv4 или <h:h:h:h:h:h:h> для IPv6.

Примечание:

Если в качестве значения параметра **<ip>** указан IP-адрес в формате <x.x.x.x/24>, то ограничение скорости будет действовать только для одного хоста. Если задан адрес <x.x.x.0/24>, то ограничение будет использоваться для всех хостов подсети.

Например, необходимо ограничить входящую скорость до 100 Мбит/сек для IP-адресов 10.0.0.1 и 10.0.0.2:

```
set service webproxy limit limit_100mbit speed 102400
set service webproxy limit limit_100mbit ip-address 10.0.0.1
set service webproxy limit limit_100mbit ip-address 10.0.0.2
commit
save
```

17. Включение режима симметричной многопроцессорной обработки (SMP) в прокси-сервере:

```
set service webproxy workers <n>
```

где **<n>** – количество рабочих процессов прокси-сервера. Возможно указать значение в диапазоне от «1» до «256». По умолчанию используется значение «1» – режим без SMP, запуск одного основного демона процесса Squid.

Рекомендуется устанавливать значение параметра **«workers»** не выше количества доступных процессорных ядер в системе. Превышение этого значения приводит к избыточной конкуренции за ресурсы ЦПУ, увеличению накладных расходов на переключение контекстов и снижению общей производительности.

Кроме того, не рекомендуется выделять все ядра процессора исключительно под прокси-сервер, поскольку это может негативно сказаться на работе других системных служб и фоновых процессов, необходимых для стабильной и безопасной эксплуатации устройства.

Примечание:

При использовании более одного рабочего процесса (`workers > 1`) функция кэширования должна быть отключена. Для этого необходимо выполнить следующую команду:

```
set service webproxy cache-size 0
```

Примечание:

Настройки параметра **«workers»** вступают в силу после перезапуска службы прокси-сервера. Перезапуск службы выполняется автоматически при сохранении настроек (выполнении команд **«commit»** и **«save»**) с измененным значением параметра `workers`. Вручную перезапустить сервис возможно с помощью следующей команды, используя УЗ **admin**:

```
admin@ngfwos:~$ sudo -i
root@ngfwos:~# systemctl restart squid
root@ngfwos:~# exit
admin@ngfwos:~$
```

18. Отключить запись событий службы прокси-сервера.

```
set service webproxy disable-access-log
```

Команда отключает ведение журнала событий в глобальный журнал для службы прокси-сервера.

Примечание:

Для повторного включения записи событий необходимо удалить соответствующую настройку с помощью следующей команды:

```
delete service webproxy disable-access-log
```

19. Для просмотра параметров конфигурации прокси-сервера необходимо в режиме конфигурации ввести следующую команду:

```
show service webproxy
```

Пример просмотра параметров конфигурации прокси-сервера:

```
admin@ngfwos# show service webproxy
icap-client {
    enable
    remote-address 127.0.0.1
    remote-port 1344
    request {
        location reqmod
    }
    response {
        location respmod
    }
}
listen-address 192.168.38.1 {
    https-port 3129
    tls-bump {
        ca-certificate ARMA
        enable
    }
}
[edit]
admin@ngfwos#
```

16.2 URL-фильтрация

Фильтрация веб-запросов в системе **ARMA Стена** осуществляется с использованием URL-фильтров. По умолчанию функция URL-фильтрации отключена и все запросы пропускаются без ограничений.

Существуют два типа URL-фильтров:

- **Глобальные фильтры** – применяются ко всему трафику, источник которого не принадлежит ни одной группе пользователей;
- **Правила фильтрации, привязанные к группам пользователей** – применяются только к трафику от пользователей, включённых в соответствующую группу.

Порядок обработки запросов

Система определяет принадлежность IP-адреса источника к какой-либо группе пользователей, для которой установлены правила фильтрации.

- Если принадлежность установлена, к трафику применяются только правила указанной группы в порядке возрастания их номеров (от «1» до «1024»). При первом совпадении с правилом выполняется предписанное действие, после чего дальнейшая обработка запроса прекращается. Глобальные

фильтры при этом не учитываются, даже если ни одно из правил группы не было применено.

- Если IP-адрес не принадлежит ни одной группе или в привязанной группе отсутствуют правила, применяются глобальные фильтры.
- Если ни один фильтр (ни глобальный, ни в правилах групп) не сработал, применяется действие, указанное в параметре **«default-action»**.

Порядок проверки глобальных фильтров определяется приоритетом: фильтр с более высоким приоритетом обрабатывается первым. Приоритеты фильтров (1 – наивысший):

1. **«local-ok»** – разрешает доступ к указанному IP-адресу;
2. **«local-block»** – запрещает доступ к указанному IP-адресу;
3. **«allow-ipaddr-url»** – разрешает запросы, в URL которых вместо доменного имени сайта указан IP-адрес;
4. **«block-category»** – запрещает доступ по адресам из указанной категории;
5. **«allow-category»** – разрешает доступ по адресам из указанной категории;
6. **«local-block-keyword»** – блокирует запросы к содержимому, URL которого содержит указанный набор символов;
7. **«local-block-url»** – блокирует доступ к указанному URL;
8. **«local-ok-url»** – разрешает доступ к указанному URL;
9. **«default-action»** – задаёт действие, которое будет применяться ко всем запросам, не попавшим под имеющиеся фильтры.

Правила фильтрации могут включать дополнительные условия – например, привязку к временным интервалам или к источникам трафика. Фильтрация применяется только при выполнении всех условий, заданных в правиле.

Примечание:

При создании правила фильтрации обязательно требуется его привязка к существующей группе пользователей. Правило, не привязанное ни к одной группе, приводит к нарушению корректной работы службы **SquidGuard**: в этом случае отключается вся URL-фильтрация – как глобальная, так и привязанная к группам, – и весь веб-трафик пропускается без ограничений.

Примечание:

Поскольку **SquidGuard** работает на уровне HTTP-запросов (а не IP-пакетов), он не может автоматически сопоставлять IP-адреса с доменными именами в HTTPS-трафике. Следовательно, блокировка по IP-адресу не гарантирует запрета доступа к соответствующему веб-ресурсу

через HTTPS. Для полноценной блокировки доступа необходимо также настроить запрет на URL-адрес ресурса.

Альтернативный подход заключается в настройке правил межсетевого экрана для блокировки IP-адреса, связанного с данным ресурсом.

16.2.1 Настройки глобальных URL-фильтров

1. Разрешить доступ к ресурсам из указанной категории:

```
set service webproxy url-filtering squidguard allow-category <категория>
```

где **<категория>** – имя категории. Возможно указать следующие категории:

- ads;
- adult;
- aggressive;
- agressif;
- arjel;
- associations_religieuses;
- astrology;
- audio-video;
- bank;
- bitcoin;
- blog;
- celebrity;
- chat;
- child;
- cleaning;
- cooking;
- cryptojacking;
- dangerous_material;
- dating;
- ddos;
- dialer;
- doh;
- download;

- drogue;
- drugs;
- dynamic-dns;
- educational_games;
- examen_pix;
- exceptions_liste_bu;
- fakenews;
- filehosting;
- financial;
- forums;
- gambling;
- games;
- hacking;
- jobsearch;
- lingerie;
- liste_blanche;
- liste_bu;
- local-block-default;
- local-block-url-default;
- mail;
- malware;
- manga;
- marketingware;
- mixed_adult;
- mobile-phone;
- phishing;
- porn;
- press;
- proxy;
- publicite;
- radio;

- reaffected;
- redirector;
- remote-control;
- residential-proxies;
- sect;
- sexual_education;
- shopping;
- shortener;
- social_networks;
- special;
- sports;
- stalkerware;
- strict_redirector;
- strong_redirector;
- translation;
- tricheur;
- tricheur_pix;
- update;
- violence;
- vpn;
- warez;
- webhosting;
- webmail.

2. Запретить доступ к ресурсам из указанной категории:

```
set service webproxy url-filtering squidguard block-category <категория>
```

3. Разрешить запросы, в URL которых указан IP-адрес, а не доменное имя:

```
set service webproxy url-filtering squidguard allow-ipaddr-url
```

4. Задать действие, которое будет применяться ко всем запросам, не попавшим под имеющиеся фильтры:

```
set service webproxy url-filtering squidguard default-action <действие>
```

где **<действие>** – действие над запросами по умолчанию. Допустимые значения: **«allow»** – пропустить, **«block»** – блокировать. По умолчанию используется значение **«allow»**.

5. Включить режим безопасного поиска на популярных поисковых системах:

```
set service webproxy url-filtering squidguard enable-safe-search
```

В настоящее время поддерживаются следующие поисковые системы: «Google», «Yahoo» и «Bing». По умолчанию режим безопасного поиска выключен.

6. Заблокировать доступ к указанному IPv4-адресу:

```
set service webproxy url-filtering squidguard local-block <x.x.x.x>
```

где **<x.x.x.x>** – IP-адрес, доступ к которому надо запретить.

7. Заблокировать запросы, URL которых содержит указанный в качестве ключа набор символов:

```
set service webproxy url-filtering squidguard local-block-keyword <ключ>
```

где **<ключ>** – простая строка символов или регулярное выражение, совпадение которых с чем-либо в URL вызовет блокировку содержащего URL-запроса.

8. Заблокировать доступ к указанному URL:

```
set service webproxy url-filtering squidguard local-block-url <адрес>
```

где **<адрес>** – URL, доступ к которому требуется закрыть. Вводить значение необходимо без «http://».

9. Разрешить доступ к указанному IP-адресу:

```
set service webproxy url-filtering squidguard local-ok <x.x.x.x>
```

где **<x.x.x.x>** – IP-адрес, доступ к которому необходимо разрешить.

10. Разрешить доступ к указанному URL:

```
set service webproxy url-filtering squidguard local-ok-url <адрес>
```

где **<адрес>** – URL, доступ к которому требуется разрешить. Вводить значение необходимо без «http://».

11. Включить журналирование URL-запросов:

```
set service webproxy url-filtering squidguard log [all | <категория>]
```

где:

- **«all»** – включить журналирование всех URL-запросов;

- **<категория>** – только запросы, относящиеся к указанной категории.

12. Указать URL, возвращаемый при попытке доступа к заблокированному ресурсу:

```
set service webproxy url-filtering squidguard redirect-url <адрес>
```

где **<адрес>** – URL, который будет возвращён в ответ на запросы по URL из «чёрного» списка. По умолчанию используется значение «block.ngfwos.net».

Примечание:

При значении default-action **block** указанный **<адрес>** должен быть внесён в список исключений (например, через local-ok-url), иначе пользователь не получит страницу перенаправления.

13. Определить временной периода, в течение которого будет действовать URL-фильтрация:

```
set service webproxy url-filtering squidguard time-period <имя_периода>
```

где **<имя_периода>** – имя временного периода.

13.1. Указать дни и временные интервалы действия периода:

```
set service webproxy url-filtering squidguard time-period <имя_периода> days  
<день> time <hh:mm-hh:mm>
```

где:

- **<день>** – день, по наступлении которого указанный временной период приобретает актуальность. Поддерживаются следующие значения: «Sun» – по воскресеньям, «Mon» – по понедельникам, «Tue» – по вторникам, «Wed» – по средам, «Thu» – по четвергам, «Fri» – по пятницам, «Sat» – по субботам, «weekdays» – по будням, «weekend» – по выходным (не праздничным) дням, «all» – во все дни;
- **<hh:mm-hh:mm>** – время, в течение которого актуален указанный временной период. Представление времени 24-часовое, формат диапазона «чч:мм-чч:мм» без пробелов. Если не указан временной период, то правило действует весь день «00:00-24:00».

13.2. Установить описание временного периода:

```
set service webproxy url-filtering squidguard time-period <имя_периода>  
description <описание>
```

где **<описание>** – краткое описание. Если описание содержит пробелы, то его необходимо заключить в двойные кавычки. Максимальная длина значения – «255» символов.

14. Отключить URL-фильтрацию без удаления конфигурации:

```
set service webproxy url-filtering disable
```

16.2.2 Настройка групп пользователей для URL-фильтрации

Для индивидуальной обработки трафика от различных пользователей используется механизм группирования по IP-адресам, подсетям, доменам или именам аутентифицированных пользователей.

Команды управления группами пользователей:

1. Создать группу пользователей:

```
set service webproxy url-filtering squidguard source-group <имя_группы>
```

где **<имя_группы>** – имя группы. Имя группы пользователей должно соответствовать следующим требованиям:

- не должно начинаться с цифры;
- первый символ должен быть латинской буквой (a–z, A–Z) или символом подчёркивания (_);
- второй символ должен быть латинской буквой или символом подчёркивания (_);
- третий символ должен быть латинской буквой или цифрой (0–9);
- последующие символы (начиная с четвёртого, если есть) могут включать латинские буквы, цифры, символы подчёркивания (_), дефисы (-) и точки (.);
- минимальная длина имени – три символа.

2. Добавить IPv4-адрес, подсеть или диапазон адресов в группу:

```
set service webproxy url-filtering squidguard source-group <имя_группы> address  
<адрес>
```

где **<адрес>** – IP-адрес в формате <x.x.x.x> или адрес IPv4-подсети в формате <x.x.x.x/x>. Также возможно указать диапазон IPv4-адресов в формате <x.x.x.x>-<x.x.x.x>.

3. Установить описание группы:

```
set service webproxy url-filtering squidguard source-group <имя_группы>  
description <описание>
```

где **<описание>** – краткое описание группы. Если описание содержит пробелы, то его необходимо заключить в двойные кавычки. Максимальная длина значения – «255» символов.

4. Добавить домен в группу:

```
set service webproxy url-filtering squidguard source-group <имя_группы> domain  
<домен>
```

где **<домен>** – название домена, который нужно включить в члены группы (например, infowatch.ru).

IP-адреса систем или подсетей пользователей должны успешно разрешаться по обратной зоне DNS в указанное доменное имя.

5. Добавить пользователя, успешно прошедшего аутентификацию, в члены группы:

```
set service webproxy url-filtering squidguard source-group <имя_группы> user  
<имя_пользователя>
```

где **<имя_пользователя>** – имя аутентифицированного пользователя, которого нужно включить в члены группы.

6. Создать правило фильтрации для группы пользователей:

```
set service webproxy url-filtering squidguard rule <номер> source-group  
<имя_группы>
```

где **<номер>** – уникальный номер правила. Возможно указать значение в диапазоне от «1» до «1024».

Для правил фильтрации групп пользователей доступны все параметры глобальной фильтрации.

Синтаксис написания параметров настроек правил фильтрации групп пользователей:

#Разрешить доступ к веб-содержимому по адресам из указанной категории в пределах правила:

```
set service webproxy url-filtering squidguard rule <номер> allow-category  
<категория>
```

#Запретить доступ к веб-содержимому по адресам из указанной категории в пределах правила:

```
set service webproxy url-filtering squidguard rule <номер> block-category  
<категория>
```

#Разрешить запросы в указанном правиле, у которых в URL указан IP-адрес, а не доменное имя:

```
set service webproxy url-filtering squidguard rule <номер> allow-ipaddr-url
```

#Задать действие по умолчанию для указанного правила:


```
set service webproxy url-filtering squidguard rule <номер> default-action  
<действие>
```

#Включить режим безопасного поиска на популярных поисковых системах для указанного правила:

```
set service webproxy url-filtering squidguard rule <номер> enable-safe-search
```

#Запретить доступ к указанному адресу IP или URL в пределах правила:

```
set service webproxy url-filtering squidguard rule <номер> local-block <x.x.x.x>
```

#Блокировать запросы к URL, если в нем содержится указанное ключевое значение в данном правиле:

```
set service webproxy url-filtering squidguard rule <номер> local-block-url  
<адрес>
```

#Блокировать в рамках правила запросы к содержимому, URL которого содержит указанный набор символов:

```
set service webproxy url-filtering squidguard rule <номер> local-block-  
keyword <ключ>
```

#Разрешить доступ к указанному адресу IP или URL в пределах правила:

```
set service webproxy url-filtering squidguard rule <номер> local-ok <x.x.x.x>
```

#Разрешить доступ по указанному IP или URL в пределах правила:

```
set service webproxy url-filtering squidguard rule <номер> local-ok-url  
<адрес>
```

#Включить в пределах указанного правила протоколирование запросов пользователей к адресам из определенной категории:

```
set service webproxy url-filtering squidguard rule <номер> log [all |  
<категория>]
```

#Изменить URL, содержимое которого возвращается вместо запрошенного при обращении к адресам из "чёрного" списка в указанном правиле:

```
set service webproxy url-filtering squidguard rule <номер> redirect-url  
<адрес>
```

#Задать промежуток времени, в течение которого указанное правило будет действовать:

```
set service webproxy url-filtering squidguard rule <номер> time-period  
<имя_периода>
```

Примечание:

Минимально необходимый набор команд для корректной работы правила:

```
set service webproxy url-filtering squidguard source-group <имя_группы>  
set service webproxy url-filtering squidguard source-group <имя_группы>  
address <адрес>  
set service webproxy url-filtering squidguard rule <номер> source-group  
<имя_группы>
```

Интеграция с LDAP

Squidguard может осуществлять поиск в LDAP, используя заданные URL-адреса, если имя пользователя или IP-адрес не были найдены в существующем списке пользователей. Для этого применяются следующие команды:

1. Указать URL-адрес LDAP для поиска IP-адреса источника и добавить его в группы пользователей:

```
set service webproxy url-filtering squidguard source-group tests ldap-ip-search  
<ldap-ip>
```

где **<ldap-ip>** – URL-адрес LDAP для поиска IP-адреса источника. Возможно указать несколько LDAP URL. В LDAP URL необходимо использовать «%s» для ссылки на IP-адреса источника. Если поиск возвращает запись, то IP-адрес считается найденным, в противном случае выполняется попытка поиска следующего URL.

2. Указать URL-адрес LDAP для поиска имени пользователя и добавить его в члены группы:

```
set service webproxy url-filtering squidguard source-group tests ldap-user-search  
<ldap-user>
```

где **<ldap-user>** – URL-адрес LDAP для поиска неизвестного имени пользователя. Возможно указать несколько LDAP URL. В LDAP URL необходимо использовать «%s» для ссылки на имя пользователя. Если поиск возвращает запись, то пользователь считается найденным, в противном случае выполняется попытка поиска следующего URL.

16.3 Кэширующий прокси-сервер

В качестве примера настройки кэширующего прокси-сервера будет использоваться схема стенда, представленная на рисунке (см. [Рисунок – Схема стенда для настройки прокси-сервера](#)).

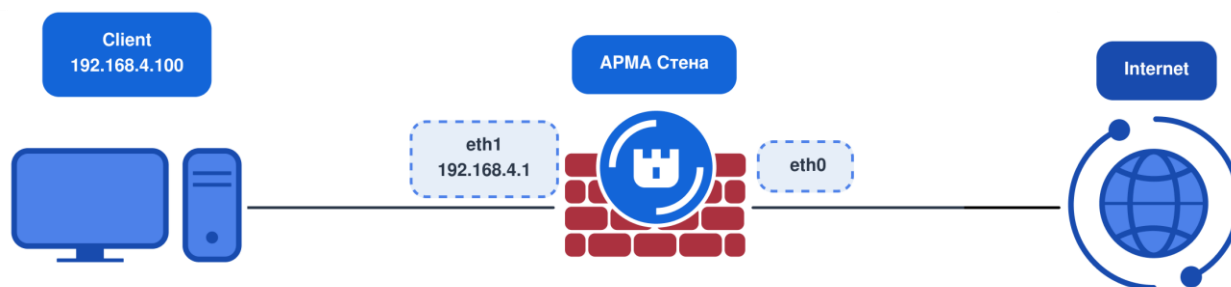


Рисунок – Схема стенда для настройки прокси-сервера

Предварительно система **ARMA Стена** настроена следующим образом:

1. Настроена переадресация DNS:

```

set system name-server 8.8.8.8
set service dns forwarding cache-size 500
set service dns forwarding listen-address 192.168.4.1
set service dns forwarding allow-from 192.168.4.0/24
set service dns forwarding name-server 8.8.8.8
commit
save
  
```

2. Настроены правила NAT:

```

set nat source rule 10 outbound-interface name eth0
set nat source rule 10 source address 192.168.4.0/24
set nat source rule 10 translation address masquerade
commit
save
  
```

где:

- «eth0» – интерфейс с доступом к сети интернет;
- «192.168.4.0/24» – адрес сети интерфейса «eth1», который будет подменяться IP-адресом интерфейса «eth0».

3. Включена отправка ответов на локальные ICMP-запросы:

```

set firewall global-options all-ping enable
commit
save
  
```

4. В системе **ARMA Стена** по умолчанию транзитный трафик блокируется. Для разрешения такого трафика необходимо создать соответствующие правила в **МЭ** или изменить действие по умолчанию для транзитного трафика с «drop» на «accept» с помощью команды «**set firewall <ipv4 | ipv6 | bridge> forward filter default-action accept**».

На ПК «**Client**» после перезапуска сетевого интерфейса обеспечен доступ к сети Интернет.

16.3.1 Настройка прокси-сервера

Для настройки прокси-сервера необходимо ввести следующие команды:

```
set service webproxy listen-address 192.168.4.1 port 3128
set service webproxy listen-address 192.168.4.1 disable-transparent
commit
save
```

16.3.2 Обновление чёрного списка

Для обновления чёрного списка необходимо ввести следующую команду:

```
admin@ngfwos:~$ update webproxy blacklists
```

% Total	% Received	% Xferd	Average Speed		Time	Time	Time
Current			Dload	Upload	Total	Spent	Left
Speed							
100 22.0M	100 22.0M	0	0	3622k	0	0:00:06	0:00:06 --:--:--
4505k							
Uncompressing blacklist...							
Processing	file	and	database		/opt/vyatta/etc/config/url-		
filtering/squidguard/db/warez/domains							
[=====]							
100 % done							
Processing	file	and	database		/opt/vyatta/etc/config/url-		
filtering/squidguard/db/warez/urls							
[=====]							
100 % done							
...							
Processing	file	and	database		/opt/vyatta/etc/config/url-		
filtering/squidguard/db/chat/urls							
[=====]							
100 % done							
admin@ngfwos:~\$							

После завершения процесса обновления необходимо перезапустить службу прокси:

```
admin@ngfwos:~$ restart webproxy
```

16.3.3 Настройка ПК «Client»

На ПК «**Client**» необходимо указать вручную следующие настройки прокси:

- «**HTTP прокси**» – «192.168.4.1»;
- «**порт**» – «3128»;
- «**HTTPS прокси**» – «192.168.4.1»;
- «**порт**» – «3128»;
- «**Не использовать прокси для**» – «localhost 127.0.0.0/8; ::1».

16.3.4 Настройка политик блокировки

Для настройки политик блокировки какого-либо ресурса необходимо ввести следующую команду:

```
set service webproxy url-filtering squidguard local-block-url youtube.com
set service webproxy url-filtering squidguard local-block-url rutube.ru
commit
save
```

В результате с ПК «**Client**» после перезапуска веб-браузера доступ к ресурсам «youtube.com» и «rutube.ru» будет запрещён.

16.4 Прозрачный режим прокси-сервер

В качестве примера настройки прокси-сервера в прозрачном режиме работы будет использоваться схема стенда, представленная на рисунке (см. [Рисунок – Схема стенда для настройки прокси-сервера](#)).

В приведённой схеме видно, что **ARMA Стена** будет использоваться на границе сети, поэтому необходимо настроить двунаправленное преобразование сетевых адресов (NAT masquerade). Для работы прокси в прозрачном режиме необходимо будет настроить перенаправление портов (DNAT) http и https на порты прокси 3128 и 3129, соответственно. Для работы прокси в непрозрачном режиме использование DNAT не требуется.

16.4.1 Настройка NAT для перенаправления HTTPS и HTTP трафика на прокси-сервер:

```
set nat destination rule 10 destination port 'https'
set nat destination rule 10 inbound-interface name 'eth1'
set nat destination rule 10 protocol 'tcp'
set nat destination rule 10 translation address '192.168.4.1'
set nat destination rule 10 translation port '3129'
set nat destination rule 20 destination port 'http'
set nat destination rule 20 inbound-interface name 'eth1'
set nat destination rule 20 protocol 'tcp'
set nat destination rule 20 translation address '192.168.4.1'
set nat destination rule 20 translation port '3128'
commit
save
```

Правило с приоритетом «10» определяет настройки NAT для перенаправления HTTPS-трафика на прокси-сервер. Правило с приоритетом «20» предназначено для перенаправления HTTP-трафика.

Просмотр настроенных правил для NAT:

```
admin@ngfwos# show nat destination
rule 10 {
    destination {
        port https
    }
    inbound-interface {
        name eth1
    }
    protocol tcp
    translation {
        address 192.168.4.1
        port 3129
    }
}
rule 20 {
    destination {
        port http
    }
    inbound-interface {
        name eth1
    }
    protocol tcp
```

```
translation {  
    address 192.168.4.1  
    port 3128  
}  
}  
[edit]  
admin@ngfwos#
```

16.4.2 Настройка NAT для маскировки адресов локальной сети:

```
set nat source rule 30 outbound-interface name eth0  
set nat source rule 30 source address 192.168.4.0/24  
set nat source rule 30 translation address masquerade  
commit  
save
```

Просмотр настроек правила «30» для NAT:

```
admin@ngfwos# show nat source rule 30  
outbound-interface {  
    name eth0  
}  
source {  
    address 192.168.4.0/24  
}  
translation {  
    address masquerade  
}  
[edit]  
admin@ngfwos#
```

16.4.3 Настройка системного DNS-сервера:

```
set service dns forwarding allow-from 192.168.4.0/24  
set service dns forwarding listen-address 192.168.4.1  
set service dns forwarding name-server 8.8.8.8  
commit  
save
```

Просмотр настроек системного DNS-сервера:

```
admin@ngfwos# show service dns
forwarding {
    allow-from 192.168.4.0/24
    listen-address 192.168.4.1
    name-server 8.8.8.8 {
    }
}
[edit]
admin@ngfwos#
```

16.4.4 Сгенерировать сертификат УЦ:

```
admin@ngfwos# run generate pki ca install test
Enter private key type: [rsa, dsa, ec] (Default: rsa)
Enter private key bits: (Default: 2048)
Enter country code: (Default: GB)
Enter state: (Default: Some-State)
Enter locality: (Default: Some-City)
Enter organization name: (Default: NGFWOS)
Enter common name: (Default: ngfwos.net)
Enter how many days certificate will be valid: (Default: 1825)
Note: If you plan to use the generated key on this router, do not encrypt the private
key.
Do you want to encrypt the private key with a passphrase? [y/N]
2 value(s) installed. Use "compare" to see the pending changes, and "commit" to
apply.
[edit]

commit
save
```

В данном случае при создании сертификата все параметры были оставлены без изменений.

Просмотр сгенерированного сертификата УЦ:


```
admin@ngfwos# show pki
Must specify config path
ca test {
    certificate MIIDpzCC.....
    private {
        key MIIEvAIBADAN..... ==
    }
}
[edit]
admin@ngfwos#
```

16.4.5 Настройки прокси-сервера:

```
set service webproxy listen-address 192.168.4.1 https-port 3129
set service webproxy listen-address 192.168.4.1 tls-bump ca-certificate test
set service webproxy listen-address 192.168.4.1 tls-bump enable
set service webproxy url-filtering squidguard allow-ipaddr-url
set service webproxy url-filtering squidguard local-block-url ya.ru
commit
```

DEPRECATION WARNING: URL filtering with SquidGuard is deprecated and will be removed in the future NGFWOS versions.

```
save
```

В данном примере реализована блокировка доступа к сайту «ya.ru», при этом разрешены запросы, в URL которых вместо доменного имени сайта указан IP-адрес.

Просмотр настроек прокси-сервера:

```
admin@ngfwos# show service webproxy
authentication {
    ldap {
        base-dn ru
    }
}
listen-address 192.168.4.1 {
    https-port 3129
    tls-bump {
        ca-certificate test
        enable
    }
}
url-filtering {
```

```
squidguard {  
    allow-ipaddr-url  
    local-block-url ya.ru  
}  
}  
[edit]  
admin@ngfwos#
```

QUIC-трафик

Примечание:

При разрешённом по умолчанию входящем и исходящем трафике в системе **ARMA Стена** прокси-сервер в прозрачном режиме обрабатывает соединения на портах 80/TCP и 443/TCP, перехватывая TCP-трафик, но не перенаправляя UDP-трафик на порту 443, вследствие чего QUIC-трафик передаётся напрямую от клиента к серверу, минуя прокси.

Блокировка QUIC-трафика может быть реализована с использованием правил межсетевого экрана (**МЭ**) или посредством службы контроля приложений (App Control).

Для фильтрации QUIC-трафика с использованием службы контроля приложений необходимо добавить правило фильтрации протокола **quic** и активировать службу COV в режиме **IPS** на интерфейсе, через который проходит интернет-трафик:

```
set app-control category protocols app quic  
set suricata netmap interface <iname> copy-mode ips  
set suricata enable yes  
commit  
save
```

При использовании межсетевого экрана для блокировки QUIC-трафика необходимо настроить правило, запрещающее UDP-трафик на порту 443. Ниже приведён пример конфигурации правила фильтрации для IPv4 в рамках стандартной политики обработки трафика:

```
set firewall ipv4 forward filter rule 10 action drop  
set firewall ipv4 forward filter rule 10 destination port 443  
set firewall ipv4 forward filter rule 10 protocol udp
```

16.4.6 Настройка ПК «Client»:

Прозрачный режим не предполагает какой-либо дополнительной настройки ПО пользователей. Однако для корректной работы системы необходимо, чтобы на клиентских устройствах в качестве основного шлюза и DNS-сервера был указан IP-адрес **ARMA Стена** - 192.168.4.1. Если используется настройка подмены сертификата

TLS-Bump, как показано в примере, то на компьютере пользователя необходимо установить сгенерированный сертификат УЦ (см. [Настройки подмены сертификата TLS-Bump](#)).

16.4.7 Проверка:

Для проверки работоспособности фильтра на компьютере «Client» необходимо открыть веб-браузер и перейти на сайт «ya.ru». В результате сайт будет заблокирован, и происходит перенаправление на страницу «block.ngfwos.net». При этом доступ ко всем остальным интернет-ресурсам открыт.

16.5 Технология единого входа

В качестве примера настройки SSO для прокси-сервера будет использоваться схема стенда, представленная на рисунке (см. [Рисунок – Схема стенда для настройки SSO](#)), со следующими параметрами:

- домен Active Directory – «example.com»;
- FQDN контроллера домена – «dc.example.com»;
- контроллер домена является DNS-сервером сети «LAN»;
- ПК «**Client**» введён в домен «example.com»;
- FQDN **ARMA Стена** – «ngfwos.example.com».

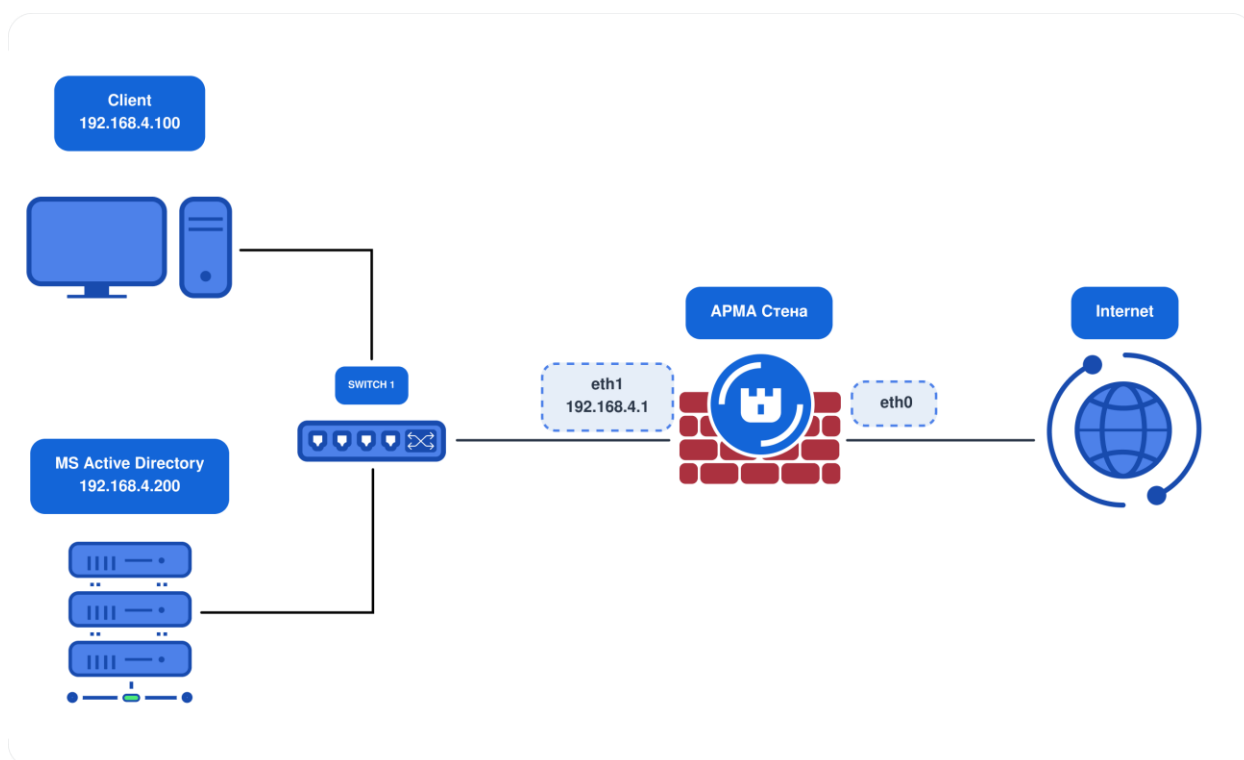


Рисунок – Схема стенда для настройки SSO

16.5.1 Аутентификация по протоколу Kerberos

В качестве примера настройки SSO по протоколу Kerberos для прокси-сервера будет использоваться схема стенда, представленная на рисунке (см. [Рисунок – Схема стенда для настройки SSO](#)).

Сервер AD предварительно настроен следующим образом:

- добавлены пользователи «ngfwos» и «user1»;
- создан домен «example.com»;
- сгенерирован файл «ngfwos.keytab» с помощью ввода в Powershell следующей команды:

```
ktpass -princ HTTP/ngfwos.example.com@EXAMPLE.COM -mapuser  
ngfwos@EXAMPLE.COM -pass examplePsw123 -crypto RC4-HMAC-NT -ptype  
KRB5_NT_PRINCIPAL -out C:\ngfwos.keytab
```

Полученный файл «ngfwos.keytab» перенесён на **ARMA Стена** и расположен по пути «/home/admin/ngfwos.keytab».

Для использования SSO на настроенном прокси-сервере необходимо выполнить следующие шаги:

1. Добавить DNS-записи на DNS-сервере.
2. Настроить **ARMA Стена** для работы с Active Directory.
3. Настроить прокси на ПК «Client».

16.5.1.1 Добавление DNS-записей

На DNS-сервере необходимо создать записи:

- **Запись 1:**
 - «Имя» – «ngfwos»;
 - «Полное доменное имя» – «ngfwos.example.com»;
 - «IP-адрес» – «192.168.4.1»;
- **Запись 2:**
 - «Имя» – «user1»;
 - «Полное доменное имя» – «user1.example.com»;
 - «IP-адрес» – «192.168.4.100»;
- **Запись 3:**
 - «Имя» – «dc»;
 - «Полное доменное имя» – «dc.example.com»;
 - «IP-адрес» – «192.168.4.200».

Записи создаются в соответствии с руководством пользователя используемого DNS-сервера.

На ПК «**Client**» необходимо войти в домен «example.com» под пользователем «user1». В качестве DNS-сервера указать «192.168.4.200».

16.5.1.2 Настройка ARMA Стена для работы с Active Directory

Для настройки **ARMA Стена** необходимо в режиме конфигурирования ввести следующие команды:

```
set service webproxy authentication kerberos domain example.com
```

где «**example.com**» – имя домена;

```
set service webproxy authentication kerberos domain-controller dc.example.com
```

где «**dc.example.com**» – FQDN контроллера домена;

```
set service webproxy authentication kerberos host ngfwos.example.com
```

где «**ngfwos.example.com**» – FQDN текущего хоста;

```
set service webproxy authentication kerberos kdc dc.example.com
```

где «**dc.example.com**» – FQDN сервера распространения ключей;

```
set service webproxy authentication kerberos keytab ngfwos.keytab
```

где «**ngfwos.keytab**» – имя keytab-файла, расположенного в каталоге «/config/files/configuration/service/webproxy/authentication/kerberos/keytab»;

```
set service webproxy authentication kerberos realm EXAMPLE.COM
```

где «**EXAMPLE.COM**» – realm;

```
set service webproxy listen-address 192.168.4.1 port 2000
set service webproxy listen-address 192.168.4.1 disable-transparent
set service webproxy authentication enable
```

где:

- «**192.168.4.1**» – IP-адрес **ARMA Стена**;
- «**2000**» – номер порта;

```
set system name-server 192.168.4.200
```

где «**192.168.4.200**» – IP-адрес сервера AD.

Зафиксировать изменения с помощью ввода команд «**commit**» и «**save**».

16.5.1.3 Настройка прокси на ПК «Client»

На ПК «**Client**» указать настройки прокси для следующих параметров:

- «**HTTP прокси**» – «ngfwos.example.com»;
- «**Порт**» – «2000»;
- «**Также использовать этот прокси для HTTPS**» – флажок установлен.

16.5.1.4 Проверка

На ПК «**Client**» с помощью утилиты «Wireshark» выполнить захват трафика при подключении к какому-либо ресурсу сети Интернет.

В поле информации захваченного пакета «Proxy Authentication Required» будет присутствовать строка следующего вида: «Proxy-Authenticate: Negotiate\r\n».

16.5.2 Аутентификация пользователей по протоколу NTLMv2

В качестве примера настройки SSO по протоколу NTLMv2 для прокси-сервера будет использоваться схема стенда, представленная на рисунке (см. [Рисунок – Схема стенда для настройки SSO](#)).

Сервер AD предварительно настроен следующим образом:

- добавлен пользователь «**ngfwos**»;
- создан домен «**example.com**».

Примечание:

Пользователь «**ngfwos**» должен обладать правами на добавления рабочих станций к домену.

Для использования SSO на настроенном прокси-сервере необходимо выполнить следующие шаги:

1. Добавить DNS-записи на DNS-сервере (см. [Добавление DNS-записей](#)).
2. Настроить **ARMA Стена** для работы с Active Directory.
3. Настроить прокси на ПК «**Client**» (см. [Настройка прокси на ПК «Client»](#)).

16.5.2.1 Настройка ARMA Стена для работы с Active Directory

Для настройки **ARMA Стена** необходимо в режиме конфигурирования ввести следующие команды:

```
set service webproxy authentication ntlm netbios-name NGFWOS
```

где «**NGFWOS**» – NetBIOS-имя устройства в верхнем регистре;

```
set service webproxy authentication ntlm username ngfwos
```

где «**ngfwos**» – логин пользователя **ARMA Стена** в AD;

```
set service webproxy authentication ntlm password examplePsw123
```

где «**examplePsw123**» – пароль пользователя **ARMA Стена** в AD, приведён в качестве примера;

```
set service webproxy authentication ntlm realm EXAMPLE.COM
```

где «**EXAMPLE.COM**» – realm;

```
set service webproxy authentication ntlm workgroup EXAMPLE
```

где «**EXAMPLE**» – NetBIOS-имя домена AD, в верхнем регистре;

```
set service webproxy listen-address 192.168.4.1 port 2000
set service webproxy listen-address 192.168.4.1 disable-transparent
set service webproxy authentication enable
```

где:

- «**192.168.4.1**» – IP-адрес **ARMA Стена**;
- «**2000**» – номер порта;

```
set system name-server 192.168.4.200
```

где «**192.168.4.200**» – IP-адрес сервера AD.

Зафиксировать изменения с помощью ввода команд «**commit**» и «**save**».

Примечание:

При включении аутентификации NTLMv2 **ARMA Стена** не предлагает себя в качестве Master Browser (local master = no, preferred master = no, domain master = no, os level = 0).

Дополнительно возможно ограничить область действия службы NTLM-аутентификации, настроив её на прослушивание только определённого сетевого интерфейса. Конфигурирование осуществляется с использованием следующих команд:

- Указание сетевого интерфейса, на котором веб-прокси будет ожидать входящие запросы с использованием NTLM-аутентификации:

```
set service webproxy authentication ntlm interface <iname>
```

где **<iname>** - имя физического или логического сетевого интерфейса, на котором разрешено принимать клиентские подключения, требующие NTLM-аутентификации.

- Указание IPv4-адреса, привязанного к интерфейсу, на котором будет приниматься трафик для NTLM-аутентификации:

```
set service webproxy authentication ntlm interface-address <ip_address>
```

где **<ip_address>** – IPv4-адрес сетевого интерфейса.

Команда обязательна, если указан интерфейс прослушивания.

16.5.2.2 Проверка

На ПК «**Client**» с помощью утилиты «Wireshark» выполнить захват трафика при подключении к какому-либо ресурсу сети Интернет.

В поле информации захваченного пакета «Proxy Authentication Required» будет присутствовать строка следующего вида: «Proxy-Authenticate: Negotiate\r\n».

16.5.3 Аутентификация пользователей LDAP

В качестве примера настройки SSO по протоколу LDAP для прокси-сервера будет использоваться схема стенда, представленная на рисунке (см. [Рисунок – Схема стенда для настройки SSO](#)).

Сервер AD предварительно настроен следующим образом:

- добавлены пользователи «**ngfwos**» и «**user1**»;
- создан домен «**example.com**».

Для использования SSO на настроенном прокси-сервере необходимо выполнить следующие шаги:

1. Добавить DNS-записи на DNS-сервере (см. [Добавление DNS-записей](#)).
2. Настроить **ARMA Стена** для работы с Active Directory.
3. Настроить прокси на ПК «**Client**» (см. [Настройка прокси на ПК «Client»](#)).

16.5.3.1 Настройка ARMA Стена для работы с Active Directory

Для настройки **ARMA Стена** необходимо в режиме конфигурирования ввести следующие команды:

```
set service webproxy authentication children 15
set service webproxy authentication ldap base-dn CN=имя_группы,
DC=example,DC=com
set service webproxy authentication ldap bind-dn CN=admin, DC=example,DC=com
set service webproxy authentication ldap filter-expression cn=%s
set service webproxy authentication ldap password <examplePsw123>
```

Описание параметров:

- **children** – задаёт количество дочерних процессов аутентификации, обрабатывающих LDAP-запросы.

- **base-dn** – определяет базовый DN каталога LDAP, с которого начинается поиск пользователей. В примере указан корневой домен «example.com».
- **bind-dn** – задаёт учётную запись с правами на чтение LDAP-каталога. В примере используется учётная запись admin.
- **filter-expression** – устанавливает фильтр поиска пользователя в каталоге. Выражение «**cn=%s**» означает, что поиск выполняется по полному имени, где «**%s**» заменяется на введённое имя пользователя.
- **password** – указывает пароль для учётной записи, заданной в параметре «bind-dn».

Примечание:

При наличии пробелов в значениях параметров DN указанное значение должно быть заключено в двойные кавычки (").

```
set service webproxy authentication ldap server 192.168.4.200
```

где «**192.168.4.200**» – IP-адрес сервера AD.

```
set service webproxy authentication ldap port <portnumber>
```

где **<portnumber>** – порт.

```
set service webproxy authentication ldap username-attribute CN
```

где «**CN**» – имя атрибута DN.

```
set service webproxy authentication ldap version 3
```

где «**3**» – версия протокола LDAP.

```
set service webproxy listen-address 192.168.4.1 port 2000
set service webproxy listen-address 192.168.4.1 disable-transparent
set service webproxy authentication enable
```

где:

- «**192.168.4.1**» – IP-адрес **ARMA Стена**;
- «**2000**» – номер порта.

```
set system name-server 192.168.4.200
```

где «**192.168.4.200**» – IP-адрес сервера AD.

Зафиксировать изменения с помощью ввода команд «**commit**» и «**save**».

16.5.3.2 Проверка

Для проверки на ПК «**Client**» необходимо в веб-браузере инициировать подключение к какому-либо сайту и ввести учётные данные пользователя.

16.5.4 Настройки подмены сертификата TLS-Bump

В качестве примера настройки подмены сертификата TLS-Bump будет использоваться схема стенда, представленная на рисунке (см. [Рисунок – Схема стенда для настройки SSO](#)).

Предварительно настроена аутентификация пользователей по протоколу NTLM (см. [Аутентификация пользователей по протоколу NTLMv2](#)).

Для настройки подмены сертификата TLS-Bump необходимо выполнить следующие действия:

1. Сгенерировать сертификат УЦ с помощью следующей команды:

```
admin@ngfwos# run generate pki ca install test

Enter private key type: [rsa, dsa, ec] (Default: rsa)
Enter private key bits: (Default: 2048)
Enter country code: (Default: GB)
Enter state: (Default: Some-State)
Enter locality: (Default: Some-City)
Enter organization name: (Default: NGFWOS)
Enter common name: (Default: ngfwos.net)
Enter how many days certificate will be valid: (Default: 1825)
Note: If you plan to use the generated key on this router, do not encrypt the
private key.
Do you want to encrypt the private key with a passphrase? [y/N]
2 value(s) installed. Use "compare" to see the pending changes, and "commit"
to apply.
[edit]

commit
save
```

В данном случае при создании сертификата все параметры были оставлены без изменений.

Просмотр сгенерированного сертификата УЦ:

```
admin@ngfwos# show pki
Must specify config path
ca test {
    certificate MIIDpzCC.....
    private {
        key MIIEvAIBADAN..... =
    }
}
[edit]
admin@ngfwos#
```

2. Настроить функциональность TLS-Bump, введя следующие команды:

```
set service webproxy listen-address 192.168.4.1 tls-bump ca-certificate test
set service webproxy listen-address 192.168.4.1 tls-bump enable
commit
save
```

где «**192.168.4.1**» – IP-адрес **ARMA Стена**.

Примечание:

Сертификат УЦ сохраняется в каталог «**/etc/squid/certs/test.pem**».

3. На ПК «**Client**» импортировать сгенерированный сертификат в веб-браузер.

Например, в браузере Firefox необходимо открыть меню «Сертификаты», выбрать пункт «Просмотр сертификатов», а затем «Центры сертификации». После этого следует нажать кнопку «Импортировать» и выбрать файл «test.pem». В открывшемся окне необходимо установить все флажки и нажать кнопку «ОК».

Примечание:

В случае перевыпуска сертификата УЦ в системе **ARMA Стена**, необходимо удалить старый сертификат и установить новый на компьютере пользователя. Рекомендуются также очистить историю браузера на данном компьютере.

Отключение подмены сертификата TLS-Bump для определённых доменов.

Система **ARMA Стена** предоставляет возможность управления механизмом подмены сертификатов TLS-Bump путём создания списка исключений. Поддерживаются два метода добавления доменов в список исключений:

- ручное добавление отдельных доменов;
- загрузка списка доменов из внешнего файла.

1. Добавление отдельных доменов.

Для добавления конкретного домена в список исключений используется следующая команда в конфигурационном режиме:

```
set service webproxy nobump-site <domain>
```

где **<domain>** – полное доменное имя, для которого требуется отключить подмену сертификата TLS-Bump.

2. Добавление списка доменов.

Для массового добавления доменов используется команда:

```
set service webproxy nobump-sites-file sites.txt
```

где **sites.txt** – имя файла, расположенного в каталоге «/config/files/configuration/service/webproxy/nobump-sites-file/», содержащего список доменных имён, для которых отключается подмена сертификата TLS-Bump. В случае использования файла, расположенного в другом каталоге, необходимо указать полный путь к нему. Пример: «set service webproxy nobump-sites-file /config/sites.txt».

Пример структуры файла с доменами:

```
aliexpress.ru  
youtube.com
```

Допускается одновременное использование обоих методов добавления исключений. При использовании обоих методов система формирует объединённый список исключений.

16.5.4.1 Проверка

На ПК «**Client**» запустить веб-браузер и открыть любой сайт, использующий протокол HTTPS. В адресной строке нажать по иконке в форме замка и выбрать опцию защищённого соединения. Веб-браузер преобразует это соединение в защищённое.

16.6 Группы пользователей

Для управления группами необходимо наличие конфигурации SSO по протоколу «Kerberos» или «NTLM».

Для запрета доступа пользователям какой-либо группы AD необходимо ввести следующую команду:

```
set service webproxy user-group <groupname> access <groupname>
```

где **<groupname>** – имя группы пользователей. Приведено в качестве примера.

Для блокирования доступа пользователей группы к определённым доменам необходимо ввести следующие команды:

```
set service webproxy user-group <groupname> access permit
set service webproxy user-group <groupname> block-domain .youtube.com
```

где «**.youtube.com**» – доменное имя.

16.7 Параметры ICAP-клиента

Для настройки отправки расшифрованного HTTP-трафика на ICAP-сервер необходимо выполнить следующие команды:

```
set service webproxy icap-client enable
set service webproxy icap-client remote-address <address>
set service webproxy icap-client remote-port <port>
set service webproxy icap-client request location <service_name>
set service webproxy icap-client response location <service_name>
```

где

- **<address>** - IP-адрес ICAP-сервера в формате <x.x.x.x> для IPv4 или <h:h:h:h:h:h:h> для IPv6;
- **<port>** - порт ICAP-сервера. Возможно указать значение в диапазоне от «1» до «65535»;
- **<service_name>** - имя ICAP-сервер.

Дополнительные настройки:

- в случае возникновения ошибки при отправке на ICAP-сервер, пропускать трафик дальше:

```
set service webproxy icap-client request bypass
```

- установить поле в заголовке HTTP с отправкой имени пользователя прокси:

```
set service webproxy icap-client username-header <header>
```

где **<header>** - заголовок имени пользователя.

16.8 Прокси-сервер ActiveSync

Команды для настройки хранилища сертификатов:

```
set pki certificate <cert_name> certificate <bas64 data>
set pki certificate <cert_name> private key <bas64 data>
set pki ca <ca_cert_name> certificate <bas64 data>
```

где:

- **<cert_name>** – имя сертификата;
- **<bas64 data>** – сертификат в формате PEM;
- **<ca_cert_name>** – название узла конфигурации определяемого удостоверяющего центра.

Команды для настройки прокси-сервера Active Sync:

```
set service active-sync-proxy service <name> backend-address <hostname>
set service active-sync-proxy service <name> port <port>
set service active-sync-proxy service <name> certificate <cert_name>
set service active-sync-proxy service <name> ca-certificate <ca_cert_name>
set service active-sync-proxy kerberos domain <domain.xx>
set service active-sync-proxy kerberos domain-controller <domain-controller>
set service active-sync-proxy kerberos host <proxy-test>
set service active-sync-proxy kerberos kdc <x.x.x.x>
set service active-sync-proxy kerberos keytab <proxy-test.keytab>
set service active-sync-proxy kerberos realm <TEST.RU>
```

где:

- **<name>** – имя прокси-сервер ActiveSync;
- **<hostname>** – доменное имя или IPv4-адрес почтового сервера;
- **<port>** – порт почтового сервера. Возможно указать значение в диапазоне от «1» до «65535». По умолчанию используется значение «443»;
- **<domain.xx>** – имя домена, в котором находится **ARMA Стена**;
- **<domain-controller>** – доменное имя или IPv4-адрес контроллера домена;
- **<proxy-test>** – имя хоста **ARMA Стена** в Active Directory;
- **<x.x.x.x>** – IP-адрес или доменное имя центра распределения ключей. Обычно IP-адрес совпадает с адресом контроллера домена;
- **<proxy-test.keytab>** – имя keytab-файла, сгенерированного для текущего хоста (указано в качестве примера) и расположенного в каталоге **«/config/files/configuration/service/active-sync-proxy/kerberos/keytab/»**;
- **<TEST.RU>** – realm в Active Directory.

Для поиска записей, связанных с прокси-сервером Active Sync, в глобальном журнале возможно применить следующий фильтр:

```
admin@ngfwos:~$ show logging all | match nginx
```

Выводимые записи содержат следующую информацию:

- IP-адрес клиента;
- имя клиента;
- сведения о сертификате, который используется клиентом;
- порт, по которому было инициализировано соединение.

17 DR.WEB

Сервис Dr.Web позволяет с помощью веб-прокси осуществлять захват и сканирование проксируемого трафика HTTP и HTTPS на предмет наличия вирусов, вредоносного программного обеспечения и других угроз. Дополнительно сервис обеспечивает фильтрацию трафика в соответствии с базами данных нежелательных вредоносных ресурсов и тематических категорий, а также в соответствии с пользовательскими правилами, реализуемыми посредством модуля ICAPD.

Примечание:

Для функционирования сервиса Dr.Web требуется ключ активации лицензии.

Сервис Dr.Web интегрирован в систему **ARMA Стена**. Конфигурирование параметров сервиса осуществляется через интерфейс командной строки (CLI) в разделе **«set third-party service drweb gss icapd»**.

17.1 Лицензирование Dr.Web

Примечание:

Перед активацией продукта **Dr.Web Gateway Security Suite** необходимо включить службу Dr.Web – *«set third-party service drweb gss enable yes»*.

Права пользователя на использование копии **Dr.Web Gateway Security Suite** подтверждаются и регулируются лицензией, приобретённой пользователем у компании «Доктор Веб» или её партнёров. Параметры лицензии, регулирующие права пользователя, установлены в соответствии с Лицензионным соглашением (см. <https://license.drweb.com/agreement/>), условия которого принимаются пользователем при активации **Dr.Web Gateway Security Suite** в системе **ARMA Стена**.

Имеется также возможность активировать для приобретённой копии **Dr.Web Gateway Security Suite** демонстрационный период. В этом случае, если не нарушены условия активации демонстрационного периода, пользователь получает право на полноценное использование **Dr.Web Gateway Security Suite** в течение демонстрационного периода.

Каждой лицензии на использование программных продуктов компании «Доктор Веб» сопоставлен уникальный серийный номер, а в системе **ARMA Стена** с лицензией связывается специальный файл, регулирующий работу компонентов в соответствии с параметрами лицензии. Он называется лицензионным ключевым файлом. При активации демонстрационного периода также автоматически формируется специальный ключевой файл, называемый демонстрационным.

В случае отсутствия у пользователя действующей лицензии или активированного демонстрационного периода, антивирусные функции компонентов **Dr.Web**

Gateway Security Suite блокируются, кроме того, недоступен сервис регулярных обновлений вирусных баз с серверов обновлений компании «Доктор Веб».

После получения лицензионного ключевого файла для продукта **Dr.Web Gateway Security Suite** необходимо скопировать его в каталог «`/config/files/configuration/third-party/service/drweb/gss/license/`» системы **ARMA Стена**.

Для выполнения данной операции возможно использовать программное обеспечение, поддерживающее передачу файлов по протоколам SFTP или SCP (например, WinSCP для операционной системы Windows), либо воспользоваться командой «`scp`» через интерфейс командной строки. Возможны также альтернативные способы передачи данных.

Пример использования команды «`scp`»:

```
«C:\Users\test> scp c:\Users\test\Desktop\151473289.key  
admin@172.16.20.76:/config/files/configuration/third-  
party/service/drweb/gss/license»
```

Команда выполнит копирование лицензионного ключевого файла «151473289.key» в каталог «`/config/files/configuration/third-party/service/drweb/gss/license/`» на системе **ARMA Стена**, доступной по IP-адресу 172.16.20.76.

Для активации продукта **Dr.Web Gateway Security Suite** необходимо ввести следующую команду в конфигурационном режиме:

```
set third-party service drweb gss license 151473289.key  
  
# Применить и сохранить настройку:  
commit  
save
```

Для просмотра информации о текущей лицензии продукта **Dr.Web Gateway Security Suite** необходимо в эксплуатационном режиме ввести следующую команду:

```
admin@ngfwos:~$ show third-party service drweb gss license  
  
License number 151473289, expires 2025-May-29 14:53:29 (35 days left)
```

17.2 Принципы работы Dr.Web

Компонент **Dr.Web ICAPD** использует протокол ICAP (Internet Content Adaptation Protocol, RFC 3507) для взаимодействия с внешним по отношению к **Dr.Web Gateway Security Suite** прокси-сервером, обслуживающим соединения узлов локальной сети с веб-серверами по протоколу HTTP/HTTPS.

Протокол ICAP представляет собой легковесный HTTP-подобный протокол. Клиент отправляет на ICAP-сервер запрос, в состав которого входят заголовки, а также инкапсулированный HTTP-запрос, который необходимо проверить. В ответе ICAP-сервер возвращает модифицированный HTTP-запрос в инкапсулированном виде, а также один или несколько заголовков.

Для взаимодействия по протоколу ICAP используются следующие типы запросов (методы):

- REQMOD – для проверки и модификации запросов;
- RESPMOD – для проверки и модификации ответов;
- OPTIONS – для получения информации о параметрах соединения с ICAP-сервером.

В запросах REQMOD и RESPMOD используются заголовки:

- X-Client-IP – IP-адрес, с которого поступил проверяемый HTTP-запрос;
- X-Server-IP – IP-адрес, на который направлен проверяемый HTTP-запрос;
- X-Client-Username – имя клиента, прошедшего аутентификацию на прокси-сервере (в формате user или user@domain).

В ответах REQMOD и RESPMOD используются заголовки:

- X-Response-Info – присутствует в ответе, если запрашиваемый ресурс принадлежит к категории нежелательных или потенциально опасных. Всегда имеет значение Blocked.
- X-Infection-Found – содержит информацию о наличии вирусов и других нежелательных или потенциально опасных объектов.
- X-Virus-ID – содержит имя обнаруженной угрозы.
- X-Violations-Found – содержит информацию об ошибках, произошедших во время проверки.

В запросе OPTIONS может использоваться заголовок DrWeb-Get-Scan-Status. Если этот заголовок имеет значение Yes, то в ответе будет возвращена информация об используемых версиях антивирусного ядра Dr.Web Virus-Finding Engine, сканирующего ядра Dr.Web Scanning Engine и вирусных баз (см. ниже).

В ответе OPTIONS используются заголовки:

- X-Allow-Out – содержит список полей заголовков, которые Dr.Web ICAPD может включать в ответы;
- X-Include – значения заголовков, полученные из выполненного ранее запроса;
- DrWeb-Core-Engine – версия антивирусного ядра Dr.Web Virus-Finding Engine;

- DrWeb-Scan-Engine – версия сканирующего ядра Dr.Web Scanning Engine;
- DrWeb-Scan-Status – информация о статусе текущей операции сканирования;
- DrWeb-Database-Timestamp – метка времени вирусной базы;
- DrWeb-Virus-Records – количество записей в базе.

Dr.Web ICAPD также может фильтровать веб-контент и блокировать доступ к нежелательным и потенциально опасным веб-ресурсам. Если пользователь запросит доступ к такому ресурсу, ему будет возвращена страница блокировки, сформированная на основе шаблона. На странице содержится сообщение о запрете доступа с кратким объяснением причины. Такая же страница будет возвращена, если Dr.Web ICAPD обнаружит угрозу или если при проверке передаваемых данных произошла ошибка.

Для проверки URL на предмет принадлежности к нежелательным или потенциально опасным категориям **Dr.Web ICAPD** использует как базу категорий веб-ресурсов, регулярно обновляемую с серверов обновлений компании «Доктор Веб», так и опрашивает облачный сервис **Dr.Web Cloud**.

Потенциально опасные категории:

- InfectionSource – сайты, содержащие вредоносное ПО («источники распространения угроз»);
- NotRecommended – сайты, используемые для мошенничества («социальной инженерии») и не рекомендованные к посещению;
- AdultContent – сайты, содержащие материалы порнографического или эротического содержания, сайты знакомств и т. д.;
- Violence – сайты, содержащие призывы к насилию, материалы о различных происшествиях с человеческими жертвами и т. д.;
- Weapons – сайты, посвященные оружию и взрывчатым веществам, а также материалы с описанием их изготовления и т. д.;
- Gambling – сайты, на которых размещены онлайн-игры на деньги, интернет-казино, аукционы, а также принимающие ставки и т. д.;
- Drugs – сайты, пропагандирующие употребление, изготовление или распространение наркотиков и т. д.;
- ObsceneLanguage – сайты, на которых содержится нецензурная лексика (в названиях разделов, статьях и пр.);
- Chats – сайты для обмена сообщениями в режиме реального времени;
- Terrorism – сайты, содержащие материалы агрессивно-агитационного характера, описания терактов и т. д.;

- FreeEmail – сайты, предоставляющие возможность бесплатной регистрации электронного почтового ящика;
- SocialNetworks – социальные сети общего характера, деловые, корпоративные и тематические социальные сети, а также тематические сайты знакомств;
- DueToCopyrightNotice – сайты, ссылки на которые указаны правообладателями произведений, защищенных авторскими правами (кинофильмы, музыкальные произведения и т. д.);
- OnlineGames – сайты, на которых размещены игры, использующие постоянное соединение с интернет-сетью;
- Anonymizers – сайты, позволяющие пользователю скрывать свою личную информацию и предоставляющие доступ к заблокированным сайтам;
- CryptocurrencyMiningPool – сайты, предоставляющие доступ к сервисам, объединяющим пользователей с целью добычи (майнинга) криптовалют;
- Jobs – сайты, предназначенные для поиска работы.

В настройках компонента системный администратор может определять нежелательные категории веб-ресурсов, а также формировать черные и белые списки (см. раздел [Настройки блокировок](#)). При запросе ресурсов, включенных в черный список, пользователю возвращается страница блокировки. Если же ресурс включен в белый список, то доступ к нему будет всегда разрешен, даже если он относится к одной из нежелательных категорий.

Примечание:

Один сайт может принадлежать к нескольким категориям. Если одна из этих категорий отнесена к нежелательным, доступ к сайту будет заблокирован.

Примечание:

Даже если сайт включен в белый список, отправляемые и загружаемые с него данные все равно проверяются на наличие угроз.

Примечание:

В силу особенностей протокола ICAP, проверка данных большого объема (образы «.iso», большие архивы, файлы видео и т. п.) может занимать продолжительное время. Рекомендуется настроить ограничения по MIME-типу данных, подлежащих проверке, а также ограничить в настройках прокси-сервера HTTP максимальный размер данных, проверяемых по протоколу ICAP (см. пример для прокси-сервера Squid).

Для более подробного ознакомления с функциональными возможностями и особенностями продукта **Dr.Web Gateway Security Suite** рекомендуется обратиться к официальной документации, доступной по адресу – https://download.geo.drweb.com/pub/drweb/unix/gateway/11.1/documentation/html/ru/index.html?dw_8_intro.htm.

17.3 Включение Dr.Web

Для включения сервиса Dr.Web необходимо выполнить следующие действия:

1. Настроить прокси-сервера в любой из доступных режимов (см. «[Прокси-сервер](#)»).
2. Выполнить настройку ICAP:

```
set service webproxy icap-client enable
set service webproxy icap-client remote-address 127.0.0.1
set service webproxy icap-client remote-port 1344
set service webproxy icap-client request location reqmod
set service webproxy icap-client response location respmod

# Применить и сохранить конфигурацию:
commit
save
```

Значения указаны в качестве примера.

3. Включить сервис Dr.Web:

```
set third-party service drweb gss enable yes
```

4. Включить компонент Dr.Web ICAP:

```
set third-party service drweb gss icapd enable yes
```

5. Применить и сохранить конфигурацию командами «**commit**» и «**save**».

17.4 Конфигурация Dr.Web ICAPD

Компонент Dr.Web ICAPD использует протокол ICAP (Internet Content Adaptation Protocol, RFC 3507) для взаимодействия с внешним по отношению к **Dr.Web Gateway Security Suite** прокси-сервером, обслуживающим соединения узлов локальной сети с веб-серверами по протоколу HTTP/HTTPS.

Для запуска компонента Dr.Web ICAPD необходимо ввести следующую команду в конфигурационном режиме:

```
set third-party service drweb gss icapd enable yes
```

Значение «**no**» отключает компонент Dr.Web ICAPD (установлено по умолчанию).

17.4.1 Общие настройки

1. Уровень подробности ведения журнала компонента:

```
set third-party service drweb gss icapd log-level <text>
```

где **<text>** – значение уровня подробности записи в журнал для компонента Dr.Web ICAPD. Возможно указать следующие значение:

- **debug** – самый подробный (отладочный) уровень. Выводятся все сообщения, а также отладочная информация.
- **info** – выводятся все сообщения.
- **notice** – выводятся сообщения об ошибках, предупреждения, уведомления. Используется по умолчанию.
- **warning** – выводятся сообщения об ошибках и предупреждения.
- **error** – выводятся только сообщения об ошибках.

2. Сохранять или не сохранять в журнал содержимое сообщений, передаваемых по протоколу ICAP, если уровень подробности ведения журнала – отладочный (при LogLevel = DEBUG):

```
set third-party service drweb gss icapd debug-dump-icap <yes | no>
```

где:

- **yes** – сохранять в журнал содержимое сообщений;
- **no** – не сохранять в журнал содержимое сообщений. Значение используется по умолчанию.

3. Использовать или не использовать эвристический анализ для поиска неизвестных угроз:

```
set third-party service drweb gss icapd heuristic-analysis <off | on>
```

где:

- **on** – использовать эвристический анализ при проверке. Значение используется по умолчанию;
- **off** – не использовать эвристический анализ.

Эвристический анализ повышает надёжность проверки, но увеличивает её длительность.

4. Включить или отключить режим ICAP preview (предварительный просмотр) для Dr.Web ICAPD:

```
set third-party service drweb gss icapd use-preview <yes | no>
```

где:

- **yes** – включить режим ICAP preview. Значение используется по умолчанию;
- **no** – отключить режим ICAP preview.

Определяет, будет ли антивирус использовать предварительный просмотр содержимого файла перед его полной проверкой. Предварительный просмотр позволяет антивирусу быстро оценить содержимое файла без выполнения полного анализа. Основная цель – оптимизация производительности. Если файл явно безопасен или не представляет интереса для детального анализа, антивирус может пропустить его полную проверку.

Примечание:

Не изменять значение этого параметра без необходимости.

5. Возвращать код ответа «204» не только в режиме ICAP preview:

```
set third-party service drweb gss icapd use-204 <yes | no>
```

где:

- **yes** – возвращать код ответа «204». Значение используется по умолчанию;
- **no** – не возвращать код ответа «204».

Параметр «**use-204**» определяет, будет ли Dr.Web ICAPD использовать HTTP-статус 204 No Content для ответов на запросы от прокси-сервера. Параметр позволяет оптимизировать взаимодействие между прокси-сервером и Dr.Web ICAPD, избегая ненужной передачи данных, если файл или трафик признан безопасным.

Примечание:

Рекомендуется не изменять значение этого параметра без необходимости.

6. Разрешить или запретить Dr.Web ICAPD использовать режим «раннего» ответа ICAP, т. е. начинать отправлять ответ клиенту, не прочитав до конца запрос от прокси-сервера HTTP:

```
set third-party service drweb gss icapd allow-early-response <yes | no>
```

где:

- **yes** – разрешить использовать режим «раннего» ответа ICAP. Значение используется по умолчанию;
- **no** – запретить Dr.Web ICAPD использовать режим «раннего» ответа ICAP.

Примечание:

Рекомендуется не изменять значение этого параметра без необходимости.

7. IP-адрес, прослушиваемый Dr.Web ICAPD в ожидании подключений от прокси-серверов HTTP:

```
set third-party service drweb gss icapd listen-address <x.x.x.x>
```

где **<x.x.x.x>** - IP-адрес, который Dr.Web ICAPD будет прослушивать в ожидании подключений от прокси-сервера. По умолчанию используется IP-адрес «127.0.0.1».

8. Порт, прослушиваемый Dr.Web ICAPD в ожидании подключений от прокси-серверов HTTP:

```
set third-party service drweb gss icapd listen-port <1-65535>
```

где **<1-65535>** - порт IP-адреса, который Dr.Web ICAPD будет прослушивать в ожидании подключений от прокси-сервера. Возможно указать значение в диапазоне от «1» до «65535». По умолчанию используется порт «1344».

9. Тайм-аут на проверку одного файла по запросу Dr.Web ICAPD:

```
set third-party service drweb gss icapd scan-timeout <1-3600>
```

где **<1-3600>** - значение тайм-аута в секундах. Возможно указать значение в диапазоне от «1» до «3600». По умолчанию используется значение «30».

10. Максимальный уровень вложенности для запакованных объектов:

```
set third-party service drweb gss icapd packer-max-level <0-1000>
```

где **<0-1000>** - значение максимального уровня вложенности для запакованных объектов. Возможно указать значение в диапазоне от «0» до «1000». По умолчанию используется значение «8». Значение «0» указывает, что вложенные объекты не проверяются.

Под запакованным объектом понимается исполняемый код, сжатый при помощи специализированных инструментов (UPX, PELock, PECompact, Petite, ASPack, Morphine и др.). Такие объекты могут включать другие запакованные объекты, в состав которых также могут входить другие запакованные объекты,

и т. д. Значение этого параметра устанавливает предельный уровень иерархии вложенности, после которого объекты внутри объектов не будут проверяться.

11. Максимальный уровень вложенности для архивов (.zip, .rar и др.):

```
set third-party service drweb gss icapd archive-max-level <0-1000>
```

где **<0-1000>** - значение максимального уровня вложенности для архивов. Возможно указать значение в диапазоне от «0» до «1000». По умолчанию используется значение «0». Значение этого параметра устанавливает предельный уровень иерархии вложенности, после которого архивы внутри архивов не будут проверяться.

Примечание:

При значении параметра **«archive-max-level»** равном **«0»** содержимое архивов не проверяется.

12. Максимальный уровень вложенности для файлов почтовых программ (.pst, .tbb и др.):

```
set third-party service drweb gss icapd mail-max-level <0-1000>
```

где **<0-1000>** - значение максимального уровня вложенности для файлов почтовых программ. Возможно указать значение в диапазоне от «0» до «1000». По умолчанию используется значение «0».

13. Максимальный уровень вложенности для других типов объектов с вложениями (например, страницы HTML, файлы .jar и др.):

```
set third-party service drweb gss icapd container-max-level <0-1000>
```

где **<0-1000>** - значение максимального уровня вложенности для других типов объектов с вложениями. Возможно указать значение в диапазоне от «0» до «1000». По умолчанию используется значение «8».

14. Максимальная допустимая степень сжатия запакованных объектов (отношение сжатого объёма к несжатому):

```
set third-party service drweb gss icapd max-compression-ratio <2-10000>
```

где **<2-10000>** - значение степени сжатия запакованных объектов. Возможно указать значение в диапазоне от «2» до «10000». По умолчанию используется значение «500». Если степень сжатия объекта превысит указанную величину, он будет пропущен при проверке данных, инициированной по запросу Dr.Web ICAPD.

17.4.2 Настройки блокировок

Примечание:

В случае исключения ресурса из списка блокируемых **Dr.Web**, при котором доступ к указанному ресурсу не восстанавливается, требуется выполнить перезапуск компонента **DrWeb ICAPD**. Для этого необходимо вручную отключить, а затем вновь включить компонент **DrWeb ICAPD**. Только после завершения данного действия обеспечивается корректное применение изменений в политике фильтрации и восстановление доступа к ресурсу.

1. Блокировать получение и передачу данных, если они содержат неизвестную угрозу, обнаруженную эвристическим анализатором:

```
set third-party service drweb gss icapd block-suspicious <yes | no>
```

где:

- **yes** – включить блокировку. Значение используется по умолчанию;
- **no** – отключить блокировку.

2. Блокировать получение и передачу данных, если они содержат известную угрозу:

```
set third-party service drweb gss icapd block-known-virus <yes | no>
```

Значение по умолчанию: «yes».

3. Блокировать попытки подключения к веб-сайтам, содержащим вредоносное ПО (входящим в категорию InfectionSource):

```
set third-party service drweb gss icapd block-infection-source <yes | no>
```

Значение по умолчанию: «yes».

4. Блокировать попытки подключения к нерекомендуемым веб-сайтам (входящим в категорию NotRecommended):

```
set third-party service drweb gss icapd block-not-recommended <yes | no>
```

Значение по умолчанию: «yes».

5. Блокировать получение и передачу данных, если они содержат рекламную программу:

```
set third-party service drweb gss icapd block-adware <yes | no>
```

Значение по умолчанию: «yes».

6. Блокировать получение и передачу данных, если они содержат программу дозвона:

```
set third-party service drweb gss icapd block-dialers <yes | no>
```

Значение по умолчанию: «yes».

7. Блокировать попытки подключения к веб-сайтам онлайн-игр (входящим в категорию OnlineGames):

```
set third-party service drweb gss icapd block-online-games <yes | no>
```

Значение по умолчанию: «yes».

8. Блокировать попытки подключения к веб-сайтам анонимайзеров (входящим в категорию Anonymizers):

```
set third-party service drweb gss icapd block-anonymizers <yes | no>
```

Значение по умолчанию: «yes».

9. Блокировать попытки подключения к веб-сайтам, объединяющим пользователей с целью добычи (майнинга) криптовалют (входящим в категорию CryptocurrencyMiningPool):

```
set third-party service drweb gss icapd block-cryptocurrency-mining-pools <yes | no>
```

Значение по умолчанию: «yes».

10. Блокировать попытки подключения к веб-сайтам, содержащим материалы для взрослых (входящим в категорию AdultContent):

```
set third-party service drweb gss icapd block-adult-content <yes | no>
```

Значение по умолчанию: «no».

11. Блокировать попытки подключения к веб-сайтам, содержащим сцены насилия (входящим в категорию Violence):

```
set third-party service drweb gss icapd block-violence <yes | no>
```

Значение по умолчанию: «no».

12. Блокировать попытки подключения к веб-сайтам, посвящённым оружию (входящим в категорию Weapons):

```
set third-party service drweb gss icapd block-weapons <yes | no>
```

Значение по умолчанию: «no».

13. Блокировать попытки подключения к веб-сайтам, посвящённым азартным играм и играм на деньги (входящим в категорию Gambling):

```
set third-party service drweb gss icapd block-gambling <yes | no>
```

Значение по умолчанию: «но».

14. Блокировать попытки подключения к веб-сайтам, посвящённым наркотикам (входящим в категорию Drugs):

```
set third-party service drweb gss icapd block-drugs <yes | no>
```

Значение по умолчанию: «но».

15. Блокировать попытки подключения к веб-сайтам, содержащим нецензурную лексику (входящим в категорию ObsceneLanguage):

```
set third-party service drweb gss icapd block-obscene-language <yes | no>
```

Значение по умолчанию: «но».

16. Блокировать попытки подключения к веб-сайтам чатов (входящим в категорию Chats):

```
set third-party service drweb gss icapd block-chats <yes | no>
```

Значение по умолчанию: «но».

17. Блокировать попытки подключения к веб-сайтам, посвящённым терроризму (входящим в категорию Terrorism):

```
set third-party service drweb gss icapd block-terrorism <yes | no>
```

Значение по умолчанию: «но».

18. Блокировать попытки подключения к веб-сайтам бесплатных почтовых служб (входящим в категорию FreeEmail):

```
set third-party service drweb gss icapd block-free-email <yes | no>
```

Значение по умолчанию: «но».

19. Блокировать попытки подключения к веб-сайтам социальных сетей (входящим в категорию SocialNetworks):

```
set third-party service drweb gss icapd block-social-networks <yes | no>
```

Значение по умолчанию: «но».

20. Блокировать попытки подключения к веб-сайтам, ссылки на которые были добавлены по обращению правообладателей (входящим в категорию DueToCopyrightNotice):

```
set third-party service drweb gss icapd block-due-to-copyright-notice <yes | no>
```

Значение по умолчанию: «yes».

21. Блокировать получение и передачу данных, если они содержат программу-шутку:

```
set third-party service drweb gss icapd block-jokes <yes | no>
```

Значение по умолчанию: «no».

22. Блокировать получение и передачу данных, если они содержат потенциально опасную программу:

```
set third-party service drweb gss icapd block-riskware <yes | no>
```

Значение по умолчанию: «no».

23. Блокировать получение и передачу данных, если они содержат программу взлома:

```
set third-party service drweb gss icapd block-hacktools <yes | no>
```

Значение по умолчанию: «no».

24. Блокировать получение и передачу данных, если они не могут быть проверены:

```
set third-party service drweb gss icapd block-unchecked <yes | no>
```

Значение по умолчанию: «no».

25. Блокировать попытки подключения к веб-сайтам для поиска работы (входящим в категорию Jobs):

```
set third-party service drweb gss icapd block-jobs <yes | no>
```

Значение по умолчанию: «no».

Примечание:

Для блокировки необходимо, чтобы в настройках присутствовали правила проверки трафика.

17.4.3 Белый список

Все домены, включённые в белый список, будут доступны пользователям, даже если они отнесены к нежелательным категориям веб-ресурсов. Доступ ко всем поддоменам этих доменов также будет открыт.

Для добавления домена в белый список необходимо ввести следующую команду в конфигурационном режиме:

```
set third-party service drweb gss icapd whitelist <url>
```

где **<url>** – URL-адрес или путь. URL-адрес может содержать символы кириллического и латинского алфавитов, а также цифры. В пути допускается использование следующих символов: & - = ! " № ; % : ? * () _ + < > [] { } / \ | , . ' @ # \$ ^ ~ `.

Пример:

```
set third-party service drweb gss icapd whitelist example.com
set      third-party      service      drweb      gss      icapd      whitelist
infowatch.ru/pages/viewpage.actionpageId=239930185
```

Просмотр белого списка:

```
admin@ngfwos# show third-party service drweb gss icapd whitelist
whitelist example.com
whitelist wiki.infowatch.ru/pages/viewpage.actionpageId=239930185
[edit]
admin@ngfwos#
```

Примечание:

Реальное использование списка доменов, указанного в данном параметре, определяется правилами управления доступом к веб-ресурсам, настроенными для Dr.Web ICAPD.

В правилах, заданных по умолчанию (см. «[Конфигурация Dr.Web ICAPD](#)»), гарантируется предоставление доступа к доменам и их поддоменам из данного списка, даже если там будут находиться домены из блокируемых категорий веб-ресурсов указанных в разделе «Настройки блокировок». Кроме того, правила по умолчанию обеспечивают проверку данных, загружаемых с доменов из белого списка, на наличие потенциальных угроз.

17.4.4 Чёрный список

Все домены, включённые в чёрный список, не будут доступны пользователям, даже если они не отнесены к категориям нежелательных веб-ресурсов. Доступ ко всем поддоменам этих доменов также будет заблокирован.

Для добавления домена в чёрный список необходимо ввести следующую команду в конфигурационном режиме:

```
set third-party service drweb gss icapd blacklist <url>
```

где **<url>** – URL-адрес или путь. URL-адрес может содержать символы кириллического и латинского алфавитов, а также цифры. В пути допускается

использование следующих символов: & - = ! " № ; % : ? * () _ + < > [] { } / \ | , . ' @ # \$ ^ ~ `.

Пример:

```
set third-party service drweb gss icapd blacklist example.net
set      third-party      service      drweb      gss      icapd      blacklist
infowatch.ru/pages/viewpage.actionpageId=239930185
```

Просмотр чёрного списка:

```
admin@ngfwos# show third-party service drweb gss icapd blacklist
blacklist example.net
blacklist wiki.infowatch.ru/pages/viewpage.actionpageId=239930185
[edit]
admin@ngfwos#
```

Примечание:

Реальное использование списка доменов, указанного в данном параметре, определяется правилами управления доступом к веб-ресурсам, настроенными для Dr.Web ICAPD.

В правилах, заданных по умолчанию (см. «[Конфигурация Dr.Web ICAPD](#)»), гарантируется запрет доступа ко всем доменам и их поддоменам, включённым в этот список. Если домен одновременно присутствует в белом и чёрном списке, приоритет будет отдан правилу запрета, и доступ к нему будет заблокирован.

17.4.5 Список реклам

Список регулярных выражений для описания веб-сайтов. URL, соответствующий любому из приведённых в этом списке регулярных выражений, считается рекламным.

Для добавления регулярных выражений в список реклам необходимо ввести следующую команду в конфигурационном режиме:

```
set third-party service drweb gss icapd adlist <text>
```

где **<text>** - значение регулярного выражения.

Пример:

```
set third-party service drweb gss icapd adlist .*ads.+
set third-party service drweb gss icapd adlist .*/ad/.*\.gif$
```

Просмотр списка реклам:

```
admin@ngfwos# show third-party service drweb gss icapd adlist
adlist .*ads.+
adlist .*/ad/*\gif$
[edit]
admin@ngfwos#
```

Примечание:

Реальное использование списка выражений, указанного в данном параметре, определяется правилами управления доступом к веб-ресурсам, настроенными для Dr.Web ICAPD.

В правилах, заданных по умолчанию (см. [«Конфигурация Dr.Web ICAPD»](#)), доступ к URL из данного списка запрещается только в том случае, если домены, на которые ссылаются эти URL, не включены в белый список.

17.5 Правила проверки трафика Dr.Web ICAPD

Помимо вышеперечисленных параметров, в Dr.Web ICAPD предусмотрено семь наборов правил **«rule-set*»** (**«rule-set0», ..., «rule-set6»**), предназначенных для управления проверкой трафика и контроля доступа пользователей к веб-ресурсам, а также загрузке контента из интернета. Каждый набор может содержать неограниченное количество правил. Правила внутри набора обрабатываются последовательно, сверху вниз, до достижения конечного результата. Пропуски в списке правил, если встречаются, игнорируются.

Правила представляют собой конструкции вида: **ЕСЛИ <условная часть> ТО <часть действий>**, где:

- *Условная часть* включает проверки следующих типов:
 - переменная (не) имеет заданное значение;
 - значение переменной (не) входит в указанное множество.
- *Часть действий* содержит одно или несколько действий, которые могут быть:
 - конечной резолюцией: пропустить или заблокировать проверяемый объект;
 - модифицирующим действием, например:
 - изменить свойства проверяемого объекта;
 - присвоить указанной переменной заданное значение;
 - добавить заданное значение к множеству значений переменной.

Действия правила выполняются только если его условная часть *истинна*. Если условие *ложно*, правило пропускается, и обработка продолжается со следующего правила. Правила обрабатываются последовательно, сверху вниз, до достижения конечной резолюции. После её срабатывания все последующие правила игнорируются.

Примечание:

Действия в части действий правила выполняются последовательно, слева направо. Если в цепочке действий встречается конечная резолюция, прерывающая обработку, все последующие действия в этом правиле игнорируются.

Для создание нового правила необходимо в конфигурационном режиме ввести следующей команду:

```
set third-party service drweb gss icapd rule-set rule <N> action "<text>"
```

где:

- **<N>** - номер набора правил. Возможно указать значение от «0» до «6».
- **<text>** - правило в формате «[<условие>[, <условие>[, ...]]] : <действие>[, <действие>[, ...]]» (см. «[Настройки блокировок](#)»).

В записи правил не предусмотрено дизъюнкции (логическое «ИЛИ») условий в условной части, для реализации логического «ИЛИ» необходимо записывать цепочку правил, указав в условии каждого единственное условие-дизъюнкт. Например, следующие два правила эквивалентны правилу «Осуществить блокировку, если обнаружен вредоносный объект типа KnownVirus или URL из категории Terrorism»:

```
set third-party service drweb gss icapd rule-set rule 0 action "threat_category in (KnownVirus) : BLOCK as _match"
set third-party service drweb gss icapd rule-set rule 0 action "url_category in (Terrorism) : BLOCK as _match"
```

17.5.1 Набор правил по умолчанию

По умолчанию задан следующий набор правил, управляющих блокировкой:

```
rule-set0 =  
rule-set1 = direction request, url_host in "ICAPD.Blacklist" : BLOCK as BlackList  
rule-set1 = direction request, url_host not in "ICAPD.Whitelist", url match  
"ICAPD.Adlist" : BLOCK as BlackList  
rule-set2 =  
rule-set3 = direction request, url_host not in "ICAPD.Whitelist", url_category in  
"ICAPD.BlockCategory" : BLOCK as _match  
rule-set4 =  
rule-set5 = threat_category in "ICAPD.BlockThreat" : BLOCK as _match  
rule-set6 =
```

Первые два правила регламентируют обработку исходящих HTTP-соединений: если узел (или URL), с которым производится попытка установить соединение, включён в чёрный список, соединение блокируется по причине попадания в чёрный список, дальнейшие проверки не производятся. Если же узел (URL) не находится в белом списке и относится к любой из категорий веб-сайтов, отмеченной как нежелательные для посещения, или соответствует списку регулярных выражений, описывающих рекламные веб-сайты, то соединение блокируется по причине попадания URL в запрещённую к посещению категорию.

Правило, указанное в «**rule-set5**», проверяет, не содержатся ли в теле проверяемого HTTP-запроса или HTTP-ответа угрозы, относящиеся к категориям, которые следует блокировать, и если да, то соединение блокируется по причине обнаружения угрозы.

Примечание:

По умолчанию проверяются как запросы клиентов (request), так и ответы серверов (response).

Примечание:

В системе **ARMA Стена** запрещено удалять или редактировать правила по умолчанию, заданные для Dr.Web ICAPD.

17.5.2 Формат правил

Правила имеют формат:

```
[<условие>[, <условие>[, ...]]] : <действие>[, <действие>[, ...]]
```

Условная часть правила (перед символом «:») может отсутствовать, в этом случае часть действий выполняется безусловно. Если условная часть правила отсутствует, то разделитель «:» может быть опущен. Запятая между условиями в условной части и действиями в части действий играет роль конъюнкции (т. е. логического «И»): условная часть считается истинной, только если истинны все перечисленные в ней условия, а все действия, указанные в части действий, выполняются в порядке их перечисления слева направо до момента встречи конечной резолюции,

прерывающей обработку правил. Ключевые слова, имена переменных и параметров конфигурации в правилах не чувствительны к регистру.

17.5.2.1 Условия

В правилах используются следующие условия:

- **<переменная> <значение>**

Значение указанной переменной совпадает с заданным. Может быть использовано только для переменных, которые не могут принимать множество значений.

- **<переменная> [not] in <множество значений>**

Значение переменной содержится в указанном множестве значений (для not – не совпадает ни с одним из значений указанного множества).

- **<переменная> [not] match <множество значений>**

Значение переменной соответствует регулярному выражению из указанного набора (для not – не соответствует ни одному из выражений в указанном наборе). Регулярные выражения записываются с использованием синтаксиса POSIX (BRE, ERE) или Perl (PCRE, PCRE2).

- **<переменная> [not] gt <значение>**

Значение указанной переменной (не) больше заданного. Может быть использовано только для переменных, которые принимают единственное числовое значение.

- **<переменная> [not] lt <значение>**

Значение указанной переменной (не) меньше заданного. Может быть использовано только для переменных, которые принимают единственное числовое значение.

Часть <множество значений>, с которым сравнивается переменная, может быть указана следующими способами:

- **(<значение 1>[, <значение 2>[, ...]])**

В скобках перечисляется непосредственно множество проверяемых значений (не менее одного). Для случая с одним значением и использованием условия in скобки можно опустить (получится случай <переменная> <значение>).

- **«<секция>.<параметр>»**

Множество параметров конфигурации, где в кавычках указывается имя параметра из конфигурации (с указанием содержащей его секции), значение (или набор значений) которого проверяется.

Перечни параметров, которые можно использовать в условии, зависят от компонента, для которого заданы правила, и приведены ниже.

- **file(<<имя файла>>)**

Перечень значений считывается из текстового файла <имя файла> (одна строка файла – один элемент списка, ведущие и завершающие пробелы в строках не учитываются). Путь к файлу должен быть абсолютным. Кавычки и апострофы, если они встречаются в <имя файла>, должны быть экранированы символом косой черты «\».

Размер файла не должен быть больше 64 МБ.

Содержимое файла считывается и подставляется в правила один раз – при загрузке файла конфигурации. Если указанный файл отсутствует или его размер слишком велик, при загрузке настроек возвращается ошибка x102.

Если были внесены изменения в файл, для применения внесённых изменений необходимо выключить и снова включить сервис Dr.Web.

Если переменная имеет множественное значение, то условие <переменная> in <множество значений> истинно, если пересечение множества текущих значений указанной переменной <переменная> с указанным множеством <множество значений> не пусто. Условие not in истинно в противоположном случае.

Например, пусть X – переменная, текущее значение которой – множество, содержащее значения a, b, c. Тогда:

- X in (a, b) – истинно, так как значения a и b встречаются в обоих множествах;
- X in (a, d, e) – истинно, так как значение a встречается в обоих множествах;
- X in (d, e) – ложно, так как ни одно из значений переменной (a, b, c) не встречается в множестве (d, e);
- X in () – ложно, так как множество значений переменной не пусто;
- X not in () – истинно, так как множество значений переменной не пусто;
- X not in (d, e) – истинно, так как ни одно из значений переменной (a, b, c) не встречается в множестве (d, e);
- X not in (a, d, e) – ложно, так как значение a встречается в обоих множествах.

17.5.2.2 Действия

Действия делятся на конечные резолюции, определяющие запрет или разрешение на пропуск объекта, и действия, изменяющие значения переменных, что может быть использовано при проверке условий в последующих правилах.

Конечные резолюции

Общие резолюции:

- **PASS**

Пропустить трафик (разрешить создание соединения, передать объект получателю). Последующие правила (если имеются) не используются.

- **BLOCK as <reason>**

Заблокировать трафик (отказать в создании соединения, передаче объекта получателю). Последующие правила (если имеются) не используются.

В журнале фиксируется факт блокировки с указанием причины <reason>. Эта же причина используется для определения, какую страницу с уведомлением показать пользователю в браузере.

В качестве <reason> для BLOCK могут быть использованы две стандартные причины:

- **BlackList** – данные заблокированы по причине попадания в чёрный список пользователя.
- **_match** – причиной блокировки является попадание веб-ресурса или файла с угрозой в категорию, из-за которой сработало правило (для условий *_category in (...)). Переменная _match хранит список блокируемых категорий, для которых сработало соответствие.

Особенности обработки конечных резолюций:

- BLOCK as BlackList всегда отрабатывает как «попал в чёрный список» (вне зависимости от того, что за условие указано в правиле с данной резолюцией).
- BLOCK as _match, если в _match не пусто, отрабатывает как «попал в категорию(и) _match».
- BLOCK as _match, если в _match пусто, отрабатывает как «попал в чёрный список» (вне зависимости от того, что за условие указано в правиле с данной резолюцией).
- Если были просмотрены все правила, но ни одно правило с резолюцией не сработало (или резолюции отсутствуют в правилах), то это равносильно применению к соединению действия PASS.

Изменение значения переменной

Для изменения значения переменной используется инструкция:

SET <переменная> = ([<значение 1>[, <значение 2>[, ...]])

Если в скобках ничего не указано, список значений переменных будет очищен:

SET <переменная> = ()

Если переменная имеет только одно значение, скобки не используются:

SET <переменная> = <значение>

17.5.2.3 Переменные, используемые в правилах

При указании переменных в правилах регистр символов не учитывается. Переменные, название которых состоит из нескольких слов, могут быть записаны с использованием подчёркивания для разделения слов или записаны без подчёркивания. Таким образом, имя переменной может быть указано как `variable_name`, `VariableName` или `variablename`. В данном разделе все переменные записаны с использованием подчёркивания (т. е. используется вариант написания `variable_name`).

Переменные, используемые в правилах:

1. **protocol**

Тип сетевого протокола, используемого соединением. В правилах для Dr.Web ICAPD может быть указано только одно значение – HTTP.

Возможно использовать в:

- условия - *да*
- действия - *нет*

Пример:

- `protocol in (HTTP)`

2. **url**

URL, запрошенный клиентом. Может быть сравнен со строкой или регулярным выражением. Может быть использована в паре с переменной `proc`.

Возможно использовать в:

- условия - *да*
- действия - *нет*

Пример:

- `url match («drweb.com», «example..*», «aaa.ru/»)`

3. **url_host**

URL или узел, с которым устанавливается соединение.

Значение переменной определено, только если не используется SSL/TLS или проверка SSL была разрешена.

Возможно использовать в:

- условия - *да*
- действия - *нет*

Пример:

- `url_host in („vk.com“, „ya.ru“)`

4. **url_category**

Список категорий, к которым (по базам категорий веб-ресурсов) относится URL или узел, с которым установлено соединение.

Особенности использования:

- Значение переменной определено, только если не используется SSL/TLS или проверка SSL разрешена.
- Для правил, используемых Dr.Web ICAPD, условие с `not in` будет истинным, даже если по результатам проверки URL или узел не принадлежит никакой из предопределённых категорий («безопасный» URL или узел).
- Если базы данных категорий веб-ресурсов не установлены, то переменную нельзя использовать в правилах (попытка проверить истинность условия в правиле будет приводить к ошибке x112).

Возможно использовать в:

- условия - *да*
- действия - *нет*

Категории нежелательных веб-сайтов для переменной «url_category»:

- **InfectionSource** - веб-сайты, содержащие вредоносное ПО («источники распространения угроз»).
- **NotRecommended** - веб-сайты, используемые для мошенничества («социальной инженерии») и не рекомендованные к посещению.
- **AdultContent** - веб-сайты, содержащие материалы порнографического или эротического содержания, веб-сайты знакомств и т. д.
- **Violence** - веб-сайты, содержащие призывы к насилию, материалы о различных происшествиях с человеческими жертвами и т. д.
- **Weapons** - веб-сайты, посвященные оружию и взрывчатым веществам, а также материалы с описанием их изготовления и т. д.
- **Gambling** - веб-сайты, на которых размещены онлайн-игры на деньги, интернет-казино, аукционы, а также принимающие ставки и т. д.

- **Drugs** - веб-сайты, пропагандирующие употребление, изготовление или распространение наркотиков и т. д.
- **ObsceneLanguage** - веб-сайты, на которых содержится нецензурная лексика (в названиях разделов, статьях и пр.).
- **Chats** - веб-сайты для обмена сообщениями в режиме реального времени.
- **Terrorism** - веб-сайты, содержащие материалы агрессивно-агитационного характера, описания терактов и т. д.
- **FreeEmail** - веб-сайты, предоставляющие возможность бесплатной регистрации электронного почтового ящика.
- **SocialNetworks** - социальные сети общего характера, деловые, корпоративные и тематические социальные сети, а также тематические веб-сайты знакомств.
- **DueToCopyrightNotice** - веб-сайты, ссылки на которые указаны правообладателями некоторого произведения, защищённого авторскими правами (кинофильмы, музыкальные произведения и т. д.).
- **OnlineGames** - веб-сайты, на которых размещены игры, использующие постоянное интернет-соединение.
- **Anonymizers** - веб-сайты, позволяющие пользователю скрывать свою личную информацию и предоставляющие доступ к заблокированным веб-сайтам.
- **CryptocurrencyMiningPool** - веб-сайты, предоставляющие доступ к сервисам, объединяющим пользователей с целью добычи (майнинга) криптовалют.
- **Jobs** - веб-сайты, предназначенные для поиска работы.

Примеры:

- url_category not in (AdultContent, Chats)
- url_category in «LinuxFirewall.BlockCategory»
- url_category in (FreeEmail)

5. **threat_category**

Список категорий, к которым по информации из вирусных баз относится угроза, обнаруженная в передаваемых данных. Переменная может принимать множество значений.

Особенности использования:

- Значение переменной определено, только если не используется SSL/TLS или проверка SSL разрешена.
- Для правил, используемых Dr.Web ICAPD, условие с `not in` будет истинным, даже если по результатам проверки объект не содержит угроз ни из одной из predetermined категорий («безопасный» объект).

Возможно использовать в:

- условия - *да*
- действия - *нет*

Категории угроз для переменной `threat_category`:

- **KnownVirus** - известная угроза;
- **VirusModification** - модификация известной угрозы;
- **UnknownVirus** - неизвестная угроза, подозрительный объект;
- **Adware** - рекламная программа;
- **Dialer** - программа дозвона;
- **Joke** - программа-шутка;
- **Riskware** - потенциально опасная программа;
- **Hacktool** - программа взлома.

Пример:

- `threat_category not in (Joke)`

6. **src_ip**

IP-адрес узла, со стороны которого следует соединение.

Возможно использовать в:

- условия - *да*
- действия - *нет*

Пример:

- `src_ip not in (127.0.0.1, 10.20.30.41, 198.126.10.0/24)`

7. **direction**

Тип трафика, идущего по соединению.

Возможные значения: «request» (клиентский запрос), «response» (ответ сервера). Переменная не может иметь множества значений, условия типа `match` и `in` неприменимы.

Возможно использовать в:

- условия - *да*
- действия - *нет*

Примеры:

- direction request
- direction not response

8. **divert**

Направление соединения.

Возможные значения: «input» (входящее – создано или инициировано извне локального узла), «output» (исходящее – создано или инициировано на локальном узле). Переменная не может иметь множества значений, условия типа match и in неприменимы.

Возможно использовать в:

- условия - *да*
- действия - *нет*

Примеры:

- divert input
- divert not output

9. **content_type**

MIME-тип данных, передаваемых по соединению.

Особенности использования:

- Может быть определён, только если не используется SSL/TLS или проверка SSL разрешена.
- Выражению «/» соответствуют данные любого MIME-типа, а также HTTP-ответы без заголовка Content-Type.

Возможно использовать в:

- условия - *да*
- действия - *нет*

Примеры:

- content_type in («multipart/byteranges», «application/octet-stream»)
- content_type not in ("text/*", "image/*")
- content_type not in ("audio/*")
- content_type in ("*/*")

17.5.3 Примеры правил проверки трафика и блокировки доступа

1. Разрешить для пользователей с диапазоном IP-адресов 10.10.0.0–10.10.0.254 доступ к веб-сайтам любых категорий, кроме категории Chats:

```
set third-party service drweb gss icapd rule-set rule 2 action "src_ip in (10.10.0.0/24),  
url_category not in (Chats) : PASS"
```

Примечание:

Если создаваемое правило размещено в наборе, расположенном ниже «**rule-set1**», где присутствует правило по умолчанию «url_host in «ICAPD.Blacklist» : BLOCK as BlackList», то доступ к доменам из чёрного списка (указанным в параметре ICAPD.Blacklist) будет заблокирован и для пользователей с IP-диапазоном 10.10.0.0–10.10.0.254. Если же это правило разместить выше (в наборе «**rule-set0**»), то пользователям с указанным диапазоном IP-адресов будет разрешён доступ и к сайтам из чёрного списка. Это связано с тем, что резолюция PASS является конечной – дальнейшая обработка правил прекращается, и проверка загружаемого контента на наличие угроз выполняться не будет.

Для предоставления пользователям с диапазоном IP-адресов 10.10.0.0–10.10.0.254 доступа ко всем веб-сайтам, кроме относящихся к категории Chats (если они не находятся в чёрном списке), с одновременной проверкой загружаемого контента на наличие угроз, используйте следующее правило:

```
set third-party service drweb gss icapd rule-set rule 0 action "url_category not in  
(Chats), url_host not in "ICAPD.Blacklist", threat_category not in  
"ICAPD.BlockCategory" : PASS"
```

2. Не выполнять проверку содержимого видео-файлов (т. е. данных с типом MIME video/*, где «*» соответствует любому типу MIME-класса video):

```
set third-party service drweb gss icapd rule-set rule 0 action "content_type in  
("video/*") : PASS"
```

17.6 Обновление Dr.Web

Компонент обновлений Dr.Web предназначен для получения обновлений вирусных баз и антивирусного ядра Dr.Web Virus-Finding Engine, базы категорий веб-ресурсов, а также компонентов **Dr.Web Gateway Security Suite** с серверов обновлений компании «Доктор Веб».

В зависимости от наличия подключения к сети Интернет доступны следующие методы обновления:

- *обновление через сеть Интернет* – автоматическое получение и установка актуальных версий компонентов Dr.Web с использованием интернет-соединения;
- *ручное обновление без доступа к сети Интернет* – выполнение обновления путём импорта предварительно загруженных в систему **ARMA Стена** архива обновлений.

Для вывода информации о версии компонента Dr.Web необходимо ввести следующую команду в эксплуатационном режиме:

```
admin@ngfwos:~$ show third-party drweb gss version  
  
drweb-ctl 11.1.16.2406170954
```

Для отключения компонента обновления Dr.Web необходимо ввести следующую команду в конфигурационном режиме:

```
set third-party service drweb gss update enable no  
  
# Применить и сохранить настройку:  
commit  
save
```

По умолчанию используется значение «yes» – обновление включено.

17.6.1 Обновление Dr.Web через сеть Интернет

По умолчанию в системе **ARMA Стена** автоматическое обновление компонентов Dr.Web включено и выполняется каждые 30 минут. Указанную периодичность возможно изменить с помощью команды «**set third-party service drweb gss update update-interval <0-100>**».

Примечание:

Для отключения автоматического обновления компонентов Dr.Web необходимо установить значение параметра частоты проверки обновлений в ноль:

```
set third-party service drweb gss update update-interval 0
```

При наличии на серверах обновлений доступных обновлений, они загружаются в каталог «/var/opt/drweb.com/cache/», после чего размещаются в рабочих каталогах **Dr.Web Gateway Security Suite** – «/var/opt/drweb.com/dws/».

Для получения данных о времени последнего успешного обновления и расписании следующего обновления Dr.Web необходимо ввести следующую команду в эксплуатационном режиме:

```
admin@ngfwos:~$ show third-party drweb gss update
```

```
Core engine version: 7.00.67.02170
```

```
Virus database timestamp: 2025-Apr-25 05:42:36
```

```
Virus database fingerprint: 2266ED0D630ED79A3BE9599A852ADD17
```

```
Virus databases loaded: 116
```

```
Virus records: 12516258
```

```
Anti-spam core is not loaded
```

```
Last successful update: 2025-Apr-25 06:56:13
```

```
Next scheduled update: 2025-Apr-25 07:26:13
```

```
admin@ngfwos:~$
```

Дополнительные параметры настройки автоматического обновления компонентов Dr.Web через сеть Интернет:

1. Частота проверки наличия обновлений на серверах обновления Dr.Web:

```
set third-party service drweb gss update update-interval <0-100>
```

где **<0-100>** – значение частоты проверки наличия обновлений в минутах, т. е. период времени, который должен пройти от предыдущей успешной попытки подключения к серверам обновления до следующей попытки выполнить обновление. Возможно указание значения в диапазоне от «0» до «100». По умолчанию используется значение «30».

Примечание:

При установке значения «0» автоматическое обновление компонентов службы Dr.Web через интернет отключается.

2. Частота повторных попыток выполнить обновление с серверов обновления, если очередная попытка выполнить обновление завершилась неудачей:

```
set third-party service drweb gss update retry-interval <1-30>
```

где **<1-30>** – значение частоты повторных попыток выполнить обновление в минутах. Возможно указание значения в диапазоне от «1» до «30». По умолчанию используется значение «3».

3. Количество повторных попыток выполнить обновление с серверов обновления Dr.Web (предпринимаемых через промежутки времени, указанные в параметре `retry-interval`), если предыдущая попытка обновления закончилась неудачей:

```
set third-party service drweb gss update max-retries <0-9>
```

где **<0-9>** – количество повторных попыток выполнить обновление. Возможно указание значения в диапазоне от «0» до «9». Если значение параметра – «0», то повторные попытки выполнить неудавшееся обновление не производятся (следующее обновление будет производиться через период времени, указанный в параметре «update-interval»). По умолчанию используется значение «3».

4. Тайм-аут на сетевые операции компонента при выполнении обновлений с серверов Dr.Web:

```
set third-party service drweb gss update network-timeout <5-75>
```

где **<5-75>** – значение тайм-аута в секундах. Возможно указание значения в диапазоне от «5» до «75». Используется для ожидания продолжения обновления в случае временного обрыва соединения. Если оборванное сетевое соединение будет восстановлено до истечения тайм-аута, то обновление будет продолжено. По умолчанию используется значение «60».

5. Параметры подключения к прокси-серверу, который используется компонентом обновлений Dr.Web Updater для подключения к серверам обновлений Dr.Web (например, если непосредственное подключение к внешним серверам запрещено политиками безопасности сети):

```
set third-party service drweb gss update proxy <url>
```

URL подключение к прокси-серверу имеет следующий формат:

[<протокол>://][<пользователь>:<пароль>@]<хост>:<порт>

где:

- **<протокол>** – тип используемого протокола (в текущей версии доступен только http);
- **<пользователь>** – имя пользователя для подключения к прокси-серверу;
- **<пароль>** – пароль для подключения к прокси-серверу;
- **<хост>** – адрес узла, на котором работает прокси-сервер (IP-адрес или имя домена, т. е. FQDN);
- **<порт>** – используемый порт.

Части URL **<протокол>** и **<пользователь>:<пароль>** могут отсутствовать. Адрес прокси-сервера **<хост>:<порт>** является обязательным. Если имя пользователя или пароль содержат символы «@», «%» или «:», то их следует заменить на соответствующие HEX-коды: «@» – «%40», «%» – «%25» и «:» – «%3A».

Если значение параметра не задано, то прокси-сервер не используется.

Пример:

Настройка подключения к прокси-серверу, расположенному по адресу `10.26.127.0:3336`, с использованием учётной записи «`user@company.com`» и пароля «`passw%123:`»:

```
set third-party service drweb gss update proxy  
user%40company.com:passw%25123%3A@10.26.127.0:3336
```

Примечание:

Для исключения возникновения ошибок в работе компонента обновлений, необходимо указать только один прокси-сервер для подключения к серверам обновлений Dr.Web.

17.6.2 Ручное обновление Dr.Web без доступа к сети Интернет

В случае недоступности подключения к сети Интернет обновление антивирусных компонентов Dr.Web возможно выполнить вручную с использованием архивного файла обновлений. Для этого необходимо выполнить следующие действия:

1. Скопировать предварительно подготовленный архив обновлений компонентов Dr.Web в каталог «**/config/third-party/drweb/gss/**» системы **ARMA Стена**.

Примечание:

Поддерживаются только архивы форматов «**tar**» и «**zip**».

2. Включить компонент обновления Dr.Web в случае, если он был ранее отключён:

```
set third-party service drweb gss update enable yes  
  
# Применить и сохранить настройку:  
commit  
save
```

3. Выполнить команду ручного обновления компонентов Dr.Web в эксплуатационном режиме:

```
admin@ngfwos:~$ third-party drweb gss update file backup.tar
```

где **backup.tar** – имя файла архива обновлений, предварительно скопированного в каталог «**/config/third-party/drweb/gss/**». Указанное имя архива приведено в качестве примера.

4. По завершении процесса обновления система выведет информационное сообщение:

```
Success: Update completed successfully.
```

5. Проверка применения обновлений:

```
admin@ngfwos:~$ show logging third-party service drweb gss update
```

17.6.3 Параметры конфигурации компонента обновления Dr.Web

1. Разрешить или запретить обновление вирусных баз и антивирусного ядра:

```
set third-party service drweb gss update base-update-enabled <yes | no>
```

где:

- **yes** – обновление разрешено и будет производиться. Значение используется по умолчанию;
- **no** – обновление не разрешено и не будет производиться.

2. Разрешить или запретить обновление базы категорий веб-ресурсов:

```
set third-party service drweb gss update dws-update-enabled <yes | no>
```

где:

- **yes** – обновление разрешено и будет производиться. Значение используется по умолчанию;
- **no** – обновление не разрешено и не будет производиться.

3. Разрешить или запретить обновление версий компонентов Dr.Web Gateway Security Suite:

```
set third-party service drweb gss update version-update-enabled <yes | no>
```

где:

- **yes** – обновление разрешено и будет производиться. Значение используется по умолчанию;
- **no** – обновление не разрешено и не будет производиться.

4. Указать файл, который не будет обновляться компонентом обновлений Dr.Web Updater:

```
set third-party service drweb gss update excluded-files <filename>
```

где **<filename>** – имя файла, который не будет обновляться.

5. Максимальное количество сохраняемых предыдущих версий обновляемых файлов:


```
set third-party service drweb gss update max-backups <0-9>
```

где **<0-9>** – количество сохраняемых предыдущих версий обновляемых файлов. Возможно указание значения в диапазоне от «0» до «9». При превышении этой величины самая старая копия удаляется при очередном обновлении. Если значение параметра – «0», то предыдущие версии файлов для восстановления не сохраняются. По умолчанию используется значение «0».

6. Уровень подробности ведения журнала компонента обновления Dr.Web:

```
set third-party service drweb gss update log-level <text>
```

где **<text>** – значение уровня подробности записи в журнал для компонента обновления Dr.Web. Возможно указать следующие значение:

- **debug** – самый подробный (отладочный) уровень. Выводятся все сообщения, а также отладочная информация;
- **info** – выводятся все сообщения;
- **notice** – выводятся сообщения об ошибках, предупреждения, уведомления;
- **warning** – выводятся сообщения об ошибках и предупреждения;
- **error** – выводятся только сообщения об ошибках.

По умолчанию используется значение – «**notice**».

17.7 Журналирование Dr.Web

Для журнала событий Dr.Web возможно настроить уровень детализации записей (**<level>**), сохраняемых в журнал.

Возможные значения уровня детализации записей:

- **debug** – самый подробный (отладочный) уровень. Выводятся все сообщения, а также отладочная информация;
- **info** – выводятся все сообщения;
- **notice** – выводятся сообщения об ошибках, предупреждения, уведомления;
- **warning** – выводятся сообщения об ошибках и предупреждения;
- **error** – выводятся только сообщения об ошибках.

Команды настройки уровня детализации записей:

1. Глобальная настройка общего журналирования, которая определяет, насколько подробно будут записываться события для всех компонентов Dr.Web, если для конкретного компонента не указан собственный уровень журналирования:

```
set third-party service drweb gss log-level <level>
```

По умолчанию используется значение – «**notice**».

2. Установить, насколько подробно будут записываться события, связанные с работой компонента ICAPD (например, проверка трафика, блокировка доступа к сайтам, обработка запросов):

```
set third-party service drweb gss icapd log-level <level>
```

По умолчанию используется значение – «**notice**».

3. Установить, насколько подробно будут записываться события, связанные с работой компонента Network Checker:

```
set third-party service drweb gss netcheck log-level <level>
```

По умолчанию используется значение – «**notice**».

Журнал Network Checker в Dr.Web предназначен для записи событий, связанных с проверкой сетевых подключений и трафика. Этот компонент отвечает за мониторинг сетевой активности, выявление подозрительных или потенциально опасных соединений и блокировку доступа к небезопасным ресурсам.

4. Установить, насколько подробно будут записываться события, связанные с работой компонента обновлений Dr.Web:

```
set third-party service drweb gss update log-level <level>
```

По умолчанию используется значение – «**notice**».

Для просмотра журнала событий Dr.Web необходимо ввести в эксплуатационном режиме следующую команду:

```
admin@ngfwos:~$ show logging third-party service drweb gss [<filter>]
```

где **<filter>** – дополнительный фильтр событий журнала Dr.Web. Возможно указать следующие значения:

- **config** – события, связанные с конфигурацией Dr.Web;
- **http** – события, связанные с обработкой HTTP-запросов/ответов через Dr.Web;
- **icapd** – события компонента Dr.Web ICAPD;
- **netcheck** – события сетевых проверок, например, соединений с серверами обновлений;
- **scan-engine** – события о работе сканирующего движка Dr.Web;

- **update** – события, связанные с обновлением Dr.Web;
- **url-check** – события проверки URL-адресов на предмет вредоносного содержимого.

Пример вывода журнала событий Dr.Web:

```
admin@ngfwos:~$ show logging third-party service drweb gss
24.04.2025 07:12:00 1745478720649176 ngfwos drweb-configd[35989]: ConfigD
11.1.25.2411271404
24.04.2025 07:12:00 1745478720792893 ngfwos drweb-configd[35989]:
RELOAD_REQUEST received, config will be reloaded
24.04.2025 07:12:01 1745478721146274 ngfwos drweb-icapd[37116]: ICAPD
11.1.9.2205231640
24.04.2025 07:12:01 1745478721153857 ngfwos drweb-icapd[37116]: ICAP Server
started: 127.0.0.1:1344
24.04.2025 07:12:01 1745478721170562 ngfwos drweb-httpd[37114]: HTTPD
11.1.12.2410251812
24.04.2025 07:12:01 1745478721221837 ngfwos drweb-update[37094]: Update
11.1.10.2404121438: Ready for service
24.04.2025 07:12:01 1745478721247928 ngfwos drweb-update[37094]: Couldn't
recognize Linux distribution. Assuming it is Unknown
24.04.2025 07:12:41 1745478761115525 ngfwos drweb-update[37094]: Downloaded
timestamp (10 bytes)
24.04.2025 07:12:42 1745478762395328 ngfwos drweb-update[37094]: Downloaded
drw11000.vdb (18796765 bytes)
24.04.2025 07:12:44 1745478764118794 ngfwos drweb-update[37094]: Downloaded
drw11001.vdb (20665362 bytes)
24.04.2025 07:12:45 1745478765031279 ngfwos drweb-update[37094]: Downloaded
drw11002.vdb (11416493 bytes)
```

18 ЛОГИРОВАНИЕ

Логирование сервисов настраивается в подсистеме **system logging**. Существует возможность экспортировать логи в файл, терминал и на удалённый хост.

18.1 Настройки глобального журнала

В **ARMA Стена** все логи хранятся в бинарном виде. Это необходимо для локального просмотра логов в интерфейсе CLI. По умолчанию для глобальных логов отведено место на диске в размере **10 Гб**. После заполнения отведённого места старые логи будут перезаписываться.

Для изменения максимального размера локального хранилища всех журналов необходимо ввести следующую команду:

```
set system logging global max-size <size>
```

где **<size>** – размер хранилища в гигабайтах. Возможно указание значения в диапазоне от «1» до «100».

Для просмотра фактического объёма, занимаемого всеми журналами, необходимо ввести следующую команду:

```
admin@ngfwos:~$ show logging global size
```

Для очистки всех журналов необходимо ввести следующую команду:

```
admin@ngfwos:~$ clear logging
```

18.2 Просмотр глобального журнала

Для вывода всех событий системы **ARMA Стена** в локальном консольном интерфейсе используется команда:

```
admin@ngfwos:~$ show logging all [| <filter>]
```

где **<filter>** - дополнительный фильтр для уточнения и обработки выводимых данных. Возможно применить следующие фильтры:

- **count** - подсчитывает количество строк, соответствующих текущему запросу, и выводит это число на экран. Позволяет быстро определить объем данных без необходимости их просмотра.
- **json** - преобразует вывод в формате JSON. Используется при интеграции с внешними системами мониторинга или автоматизации.
- **match <pattern>** - отображает только те строки, которые содержат заданный текстовый шаблон **<pattern>**. Позволяет выполнять точечный поиск событий по ключевым словам или кодам ошибок.

- **no-match <pattern>** - исключает из вывода строки, содержащие указанный текстовый шаблон <pattern>. Позволяет скрывать информационные сообщения или другие несущественные записи.
- **more** - активирует постраничный вывод результатов. Удобен при работе с длинными списками записей в консоли.
- **no-more** - отключает постраничный вывод, обеспечивая немедленное отображение всего результата. Используется при необходимости получить полный вывод без пауз.
- **strip-private** - маскирует или удаляет частную информацию из записей журнала, такую как IP-адреса, имена пользователей, идентификаторы сессий и т. д. Используется при подготовке журналов для внешней отправки, например, службе поддержки, с соблюдением требований конфиденциальности.

Примечание:

Некоторые дополнительные фильтры **<filter>** могут быть недоступны для использования в отдельных командах просмотра событий. В случае, если выбранная команда не поддерживает применение указанного фильтра, система отображает соответствующее информационное сообщение.

Для просмотра событий всех служб системы **ARMA Стена** в локальном консольном интерфейсе необходимо ввести команду:

```
admin@ngfwos:~$ show logging [| <filter>]
```

Для просмотра всех системных логов ядра (kernel logs) в локальном консольном интерфейсе необходимо ввести команду:

```
admin@ngfwos:~$ show logging kernel [| <filter>]
```

Для вывода событий, отфильтрованных по сервису, следует ввести команду:

```
admin@ngfwos:~$ show logging <service-name> [| <filter>]
```

где **<service-name>** – имя сервиса, по которому выполняется фильтрация событий. Список допустимых имён сервисов приведён в [таблице «Сервисы»](#).

Таблица «Сервисы»

Сервис	Описание
all	Отображение всех журналов событий, генерируемых системой.
arma-endpoint	События службы контроля целостности.

Сервис	Описание
commit-commands	События операций применения (commit) конфигурационных изменений, включая информацию о УЗ, времени и содержании внесённых изменений.
conntrack	События модуля отслеживания сетевых соединений.
conntrack-sync	События службы синхронизации таблицы отслеживания соединений (conntrack) между узлами кластера.
console-server	События, связанные с локальным доступом к командной строке через консольный интерфейс устройства.
dhcp	События DHCP-сервера и DHCP-клиента для протокола IPv4.
dhcpv6	События DHCP-сервера и DHCP-клиента для протокола IPv6.
dns	События встроенного DNS-резолвера, DNS-прокси или DNS-сервера.
firewall	События межсетевого экрана.
http-api	События, связанные с обработкой запросов к API системы: действия пользователей в веб-интерфейсе, служба синхронизации конфигурации.
https	События службы nginx.
idps	События системы обнаружения и предотвращения вторжений (COB).
interface-state-sender	События отправки уведомлений о состоянии сетевых интерфейсов внешним системам мониторинга или другим узлам.
ipoe-server	События сервера IP over Ethernet (IPoE).
kernel	Системные события ядра ОС.
lldp	События протокола LLDP (Link Layer Discovery Protocol).
login	События подсистемы аутентификации и авторизации.
nat	События трансляции сетевых адресов и портов (NAT/PAT).

Сервис	Описание
ntp	События синхронизации времени по NTP.
pppoe	События PPPoE-клиента.
pppoe-server	События PPPoE-сервера.
snmp	События протокола SNMP.
ssh	События SSH-сервера.
systemd	События менеджера системных служб systemd.
third-party service drweb gss	События компонента Dr.Web Gateway Security Suite.
users	События действий пользователей системы в интерфейсе командной строки.
vpn	События подсистемы VPN.
vrp	События протокола VRRP.
webproxy	События модуля веб-прокси.

Для сервисов «**commit-commands**» и «**users**» фильтрация событий выполняется с учётом прав доступа пользователя. Выводятся только те записи, которые соответствуют действиям пользователей, принадлежащих к тому же классу доступа, что и текущий пользователь. События, связанные с действиями пользователей других классов, недоступны для просмотра.

Дополнительно возможно выполнить фильтрацию сервисов, за исключением «**kernel**», «**nat**» и «**firewall**», по действиям пользователей, указав класс, имя пользователя, дату и время событий:

```
admin@ngfwos:~$ show logging <service-name|all> class <class-name|all> [user  
<user-name|all>] [date <date|all>] [time <time|all>] [| <filter>]
```

где:

- **<service-name|all>** - имя сервиса. Список сервисов, используемых для фильтрации событий, указан в [таблице «Сервисы»](#). Если указано значение «**all**», фильтрация по сервису не осуществляется;
- **<class-name|all>** - имя класса. Если указано значение «**all**», фильтрация по классу не осуществляется. Для инвертирования значения используется знак «**!**»;
- **<user-name|all>** - имя пользователя. Если указано значение «**all**», фильтрация по имени пользователя не осуществляется. Для инвертирования значения используется знак «**!**»;

- **<date|all>** - дата события. Возможно указать значение в формате:
 - **«yyyy-mm-dd»** - выводятся записи лога, строго соответствующие указанной дате;
 - **«yyyy-mm»** - выводятся записи лога за каждый день указанного месяца и года;
 - **«yyyy-mm-dd/yyyy-mm-dd»** - выводятся записи лога с первой по вторую даты включительно;
 - **«all»** - фильтрация по дате не осуществляется;
- **<time|all>** - время события. Возможно указать значение в формате:
 - **«hh24:mm:ss»** - выводятся записи лога, строго соответствующие указанному времени;
 - **«hh24:mm»** - выводятся записи лога, соответствующие указанному часу и минуте;
 - **«hh»** - выводятся записи лога, соответствующие указанному часу;
 - **«hh24:mm:ss/hh24:mm:ss»** - выводятся записи лога в указанный промежуток времени, включая пограничные метки времени;
 - **«all»** - фильтрация по времени не осуществляется.

Для всех сервисов, кроме **«firewall»**, **«commit-commands»**, **«kernel»**, **«nat»** и **«users»**, возможно дополнительно указать уровень события:

```
admin@ngfwos:~$ show logging <service-name> level <event_levels> [| <filter>]
```

где **<event_levels>** - имя уровня события. Возможно указать значения, представленные в [таблице «Уровни событий»](#).

Таблица «Уровни событий»

Уровень событий	Уровень событий
alert	critical
debug	emergency
error	informational
notice	warning

В случае фильтрации событий по сервису **NAT** возможно дополнительно указать направление трафика:

```
admin@ngfwos:~$ show logging nat <source|static|destination> [| <filter>]
```


Для сервиса **VPN** допустимо указать дополнительные фильтры:

```
admin@ngfwos:~$ show logging vpn [<filter>] [level <event_levels>] [| <filter>]
```

где:

- **<filter>** - имя фильтра. Возможно указать следующие значения:
 - **«ipsec»**;
 - **«l2tp»**;
 - **«openconnect»**;
 - **«openvpn»**;
 - **«pptp»**;
 - **«sstp»**;
 - **«wireguard»**;
- **<event_levels>** - уровень события. Возможно ввести значение указанное в [таблице «Уровни событий»](#).

Для сервиса **DNS** предусмотрены дополнительные фильтры **«dynamic»** и **«forwarding»**, которые возможно классифицировать по уровням событий, приведённых в [таблице «Уровни событий»](#):

```
admin@ngfwos:~$ show logging dns <dynamic|forwarding> [level <event_levels>]  
[| <filter>]
```

Для сервиса **third-party service drweb gss** допустимо указать дополнительные фильтры:

```
admin@ngfwos:~$ show logging third-party service drweb gss [<filter>] [| <filter>]
```

где **<filter>** - дополнительный фильтр событий журнала Dr.Web. Возможно указать следующие значения:

- **config** - события, связанные с конфигурацией Dr.Web;
- **http** - события, связанные с обработкой HTTP-запросов/ответов через Dr.Web;
- **icapd** - события компонента Dr.Web ICAPD;
- **netcheck** - события сетевых проверок, например, соединений с серверами обновлений;
- **scan-engine** - события о работе сканирующего движка Dr.Web;
- **update** - события, связанные с обновлением Dr.Web;

- **url-check** - события проверки URL-адресов на предмет вредоносного содержимого.

События сервиса **idps** возможно отфильтровать с помощью дополнительных фильтров:

- **engine** - вывод событий запуска Suricata:

```
admin@ngfwos:~$ show logging idps engine [class <> | level <>] [| <filter>]
```

- **rules** - вывод событий срабатывания правил Suricata согласно настройкам ведения журнала (по умолчанию используется уровень «notice»):

```
admin@ngfwos:~$ show logging idps rules [class <> | level <>] [| <filter>]
```

- **server** - вывод событий, связанных с настройками Suricata:

```
admin@ngfwos:~$ show logging idps server [class <> | level <>] [| <filter>]
```

- **update-rules** - вывод событий, связанных с обновлением правил Suricata:

```
admin@ngfwos:~$ show logging idps update_rules [class <> | level <>] [| <filter>]
```

Для отслеживания актуальных событий системы в локальном консольном интерфейсе необходимо ввести команду:

```
admin@ngfwos:~$ monitor log [<filter_name>]
```

где **<filter_name>** – фильтр событий глобального журнала. Список фильтров указан в [таблице «Фильтры глобального журнала»](#).

Таблица «Фильтры глобального журнала»

Фильтр	Фильтр	Фильтр	Фильтр
certbot	conntrack-sync	console-server	container
dhcp	dhcprv6	dns	flow-accounting
frr	haproxy	idps	ipoe-server
ipsec	kernel	l2tp	macsec
mdns	ndp-proxy	nhrp	ntp
openconnect	openvpn	pppoe	pppoe-server
pptp	protocol	router-advert	snmp
ssh	sstp	sstpc	systemd
vpn	vrrp	webproxy	wireless

18.3 Экспорт журнала

18.3.1 Экспорт журнала в файл

Для экспорта журналов в файл необходимо ввести следующую команду:

```
set system logging file <name> log <service-name>
```

где:

- **<name>** – имя целевого файла журнала;
- **<service-name>** – идентификатор сервиса, по которому выполняется фильтрация событий (см. [Таблица «Экспортируемые сервисы»](#)).

Примечание:

Log-файлы сохраняются в каталоге «**/var/log/user/**».

Таблица «Экспортируемые сервисы»

Сервис	Сервис	Сервис	Сервис
arma-endpoint	commit-commands	conntrack	conntrack-sync
console-server	dhcp	dhcpv6	dns
firewall	https-api	https	idps
ipoe-server	kernel	lldp	login
nat	ntp	pppoe	pppoe-server
snmp	ssh	systemd	users
vpn	vrrp	webproxy	

Уровень логирования

Для всех сервисов, кроме «**firewall**», «**kernel**», «**nat**» и «**users**», допускается указание одного или нескольких уровней событий в соответствии с [таблицей «Уровни событий»](#). **В файл экспортируются только те события, уровень которых соответствует указанному.**

Примечание:

Сервис **webproxy** использует собственную классификацию уровней логирования, включающую 10 уровней (в отличие от 8 уровней syslog). По умолчанию применяется первый уровень, приблизительно соответствующий уровню **informational** в syslog. При экспорте событий **webproxy** не рекомендуется указывать уровень **debug**, поскольку события данного уровня в журнале отсутствуют.

В случае отсутствия явного указания уровня логирования при выполнении команды настройки экспорта, файл будет содержать все события, относящиеся к данному

сервису, в соответствии с текущими системными настройками уровня логирования. Уровни логирования по умолчанию для различных сервисов приведены в [таблице «Уровни логирования по умолчанию для сервисов»](#).

Таблица «Уровни логирования по умолчанию для сервисов»

Сервис	Уровень логирования по умолчанию
arma-endpoint	informational
conntrack	informational
conntrack-sync	informational
console-server	informational
dhcp: client	informational
dhcp: server	informational
dhcpv6: client	informational
dhcpv6: server	informational
dns: dynamic	informational
dns: forwarding	informational
http-api	informational
https	notice
idps: engine	notice
idps: rules	notice
idps: server	notice
idps: update-rules	notice
ipoe-server	informational
lldp	informational
login	informational
ntp	informational
pppoe	debug
pppoe-server	informational
snmp	warning
ssh	debug
systemd	informational
third-party: service drweb gss config	notice

Сервис	Уровень логирования по умолчанию
third-party: service drweb gss http	notice
third-party: service drweb gss icapd	notice
third-party: service drweb gss netcheck	notice
third-party: service drweb gss scan-engine	notice
third-party: service drweb gss update	notice
third-party: service drweb gss url-check	notice
vpn: ipsec	informational
vpn: l2tp	informational
vpn: openconnect	informational
vpn: openvpn	informational
vpn: pptp	informational
vpn: sstp	informational
vpn: wireguard	informational
vrrp	informational
webproxy	informational

Пример

Экспорта журнала в файл «LogSSH» с фильтрацией событий сервиса «ssh» по уровню «alert»:

```
set system logging file LogSSH log ssh level alert
```

Спецификация фильтрации по пользователям (сервис «users»)

При настройке экспорта журнала действий пользователей (users) допускается указание класса пользователей или имени определенного пользователя:

```
set system logging file <name> log users class <name_class>
set system logging file <name> log users name <user>
```

где:

- **<name_class>** – класс пользователей;
- **<user>** – имя пользователя.

В параметрах **<name_class>** и **<user>** допустимо указать несколько значений, разделенных запятыми без пробелов. Для инвертирования значения или значений необходимо использовать знак «!».

Спецификация фильтрации для NAT

При экспорте журнала **NAT** возможно указание направления трафика:

```
set system logging file <name> log nat destination
set system logging file <name> log nat source
set system logging file <name> log nat static
```

Примечание:

В случае настройки по направлениям «destination» и «static», будет выполняться логирование только первого пакета.

Спецификация фильтрации для VPN

Для журнала **VPN** доступны дополнительные фильтры по протоколам: «ipsec», «12tp», «openconnect», «openvpn», «pptp», «sstp», «wireguard». Фильтрация может быть дополнена указанием уровня события из [таблицы «Уровни событий»](#), например:

```
set system logging file ipsec_alert log vpn sstp level alert
```

где:

- «**ipsec_alert**» – имя файла, в который будут записываться все события, соответствующие уровню alert протокола sstp;
- «**vpn sstp**» – применённый фильтр событий;
- «**alert**» – уровень логирования.

Спецификация фильтрации для DNS

Для журнала **DNS** предусмотрены дополнительные фильтры «**dynamic**» и «**forwarding**», которые возможно классифицировать по уровням событий, указанным в [таблице «Уровни событий»](#).

```
set system logging file <name> log dns [<dynamic | forwarding> level  
<event_levels>]
```

Спецификация фильтрации для Dr.Web

Для сервиса third-party service drweb gss допускается указание дополнительного фильтра событий:

```
set system logging file <name> log third-party service drweb gss [<filter>]
```

где **<filter>** - дополнительный фильтр событий журнала Dr.Web. Возможно указать следующие значения:

- **config** - события, связанные с конфигурацией Dr.Web;
- **http** - события, связанные с обработкой HTTP-запросов/ответов через Dr.Web;
- **icapd** - события компонента Dr.Web ICAPD;
- **netcheck** - события сетевых проверок, например, соединений с серверами обновлений;
- **scan-engine** - события о работе сканирующего движка Dr.Web;
- **update** - события, связанные с обновлением Dr.Web;
- **url-check** - события проверки URL-адресов на предмет вредоносного содержимого.

18.3.1.1 Ротация журналов

Ротация журналов возможна по количеству и размеру файлов.

Для настройки ротации по количеству файлов необходимо ввести следующую команду:

```
set system logging file <name> rotation file <number>
```

где **<number>** – количество файлов. Возможно указать значение в диапазоне от «1» до «100». По умолчанию используется значение «5».

Примечание:

Возможно создать не более 64 файлов логирования.

Для настройки ротации по размеру файлов необходимо ввести следующую команду:

```
set system logging file <name> rotation size <number>
```

где **<number>** – размер файлов в мегабайтах. Возможно указать значение в диапазоне от «1» до «1024». По умолчанию используется значение «5».

18.3.2 Экспорт на удалённый сервер по протоколу Syslog (RFC3164)

ARMA Стена позволяет выполнять экспорт событий на удалённый сервер, в том числе сервер **Syslog**.

Для передачи событий на удалённый сервер необходимо в режиме конфигурирования ввести следующую команду:

```
set system logging host <hostname> log <service-name>
```

где:

- **<hostname>** – доменное имя (FQDN) или IPv4-адрес удалённого сервера;
- **<service-name>** – сервис для отправки (см. [Таблица «Экспортируемые сервисы»](#)).

Все дополнительные фильтры сервисов, которые возможно использовать при экспорте журналов на удалённый сервер, описаны в разделе «[Экспорт журнала в файл](#)».

Команды для настройки дополнительных параметров отправки событий на удалённый сервер:

```
set system logging host <hostname> protocol <protocol>
set system logging host <hostname> port <portnumber>
set system logging host <hostname> format <rfc3164|cef>
```

где:

- **<protocol>** – тип транспортного протокола. Возможно указание значения «**tcp**» или «**udp**». По умолчанию используется протокол «**tcp**»;
- **<portnumber>** – порт удалённого сервера. По умолчанию используется порт «**514**».
- **<rfc3164|cef>** – формат отправки событий на удалённый сервер. Возможно указать значение «**rfc3164**» или «**cef**».

18.3.2.1 Экспорт на удалённый сервер по протоколу Syslog (RFC3164) с шифрованием TLS (RFC5425) без проверки сертификатов

Для экспорта событий на удалённый сервер с шифрованием TLS (RFC5425) без проверки сертификатов необходимо в режиме конфигурирования ввести следующие команды:

```
set system logging host <hostname> encryption yes
set system logging host <hostname> protocol tcp
set system logging host <hostname> port 6514
set system logging host <hostname> format cef
```

В режиме шифрования рекомендуется использовать порт «6514».

Примечание:

Шифрование трафика осуществляется исключительно по протоколу «**tcp**».

Для версий rsyslog младше 8.19.0, возможно, потребуется импортировать корневой сертификат (CA) в **ARMA Стена**. Для этого необходимо выполнить следующие действия:

1. Скопировать корневой сертификат (CA) rsyslog в каталог «/config/» файловой системы **ARMA Стена** (каталог указан в качестве примера).
2. Ввести следующую команду в режиме эксплуатации:

```
admin@ngfwos:~$ import pki ca <ca_name> file </config/ca.pem>
```

где:

- **<ca_name>** - имя корневого сертификата;
 - **</config/ca.pem>** - место расположения скопированного корневого сертификата.
3. После выполнения команды система сгенерирует команду, которую необходимо ввести в режиме конфигурации, а затем применить и сохранить изменения:

```
You are not in configure mode, commands to install manually from configure mode:
```

```
set pki ca <ca_name> certificate 'MIIEELzCCApegAwIBAg.....o=='
```

```
# Перейти в конфигурационный режим работы:
```

```
admin@ngfwos:~$ conf
```

```
# Ввести ранее сгенерированную команду:
```

```
admin@ngfwos# set pki ca <ca_name> certificate  
'MIIEELzCCApegAwIBAg.....o=='
```

```
# Применить и сохранить изменения в конфигурации:
```

```
admin@ngfwos# commit
```

```
admin@ngfwos# save
```

4. Ввести команду для сохранения корневого сертификата в конфигурационный файл:

```
set system logging global ssl ca-certificate <ca_name>
```

```
# Применить и сохранить изменения в конфигурации:
```

```
admin@ngfwos# commit
```

```
admin@ngfwos# save
```

Настройки сервера rsyslog

На сервере rsyslog требуется установить пакет «**rsyslog-gnutls**». Проверить наличие пакета возможно с помощью команды:

```
dpkg -l | grep rsyslog-gnutls
```

Если пакет не установлен, его возможно установить с помощью команды:

```
sudo apt-get install rsyslog-gnutls
```

Необходимо настроить сервер rsyslog для приёма зашифрованного трафика от **ARMA Стена**:

```
...
global(
    DefaultNetstreamDriver="gtls"
    DefaultNetstreamDriverCAFile="/path/to/contrib/gnutls/ca.pem"
    DefaultNetstreamDriverCertFile="/path/to/contrib/gnutls/cert.pem"
    DefaultNetstreamDriverKeyFile="/path/to/contrib/gnutls/key.pem"
)

module(
    load="imtcp"
    StreamDriver.Name="gtls"
    StreamDriver.Mode="1"
    StreamDriver.Authmode="anon"
)

input(
    type="imtcp"
    port="6514"
)
...
```

18.3.2.2 Экспорт на удалённый сервер по протоколу Syslog (RFC3164) с шифрованием TLS (RFC5425) и проверкой сертификатов

Настройка экспорта событий на удалённый сервер с использованием шифрования протокола TLS (в соответствии с RFC 5425) и проверкой подлинности сертификатов рассматривается на примере, в котором система **ARMA Стена** выступает в качестве источника генерации необходимых криптографических сертификатов.

Для реализации указанного режима передачи данных необходимо выполнить следующую последовательность действий:

1. Сгенерировать и установить корневой сертификат:

```
# Команда вводится в конфигурационном режиме:
run generate pki ca install ca_test

# Параметры создания сертификата указаны по умолчанию:
Enter private key type: [rsa, dsa, ec] (Default: rsa)
Enter private key bits: (Default: 2048)
Enter country code: (Default: GB)
Enter state: (Default: Some-State)
Enter locality: (Default: Some-City)
Enter organization name: (Default: NGFWOS)
Enter common name: (Default: ngfwos.net)
Enter how many days certificate will be valid: (Default: 1825)
Note: If you plan to use the generated key on this router, do not encrypt the
private key.
Do you want to encrypt the private key with a passphrase? [y/N]
2 value(s) installed. Use "compare" to see the pending changes, and "commit"
to apply
```

где **ca_test** – имя корневого сертификата, используемого в качестве примера.

Зафиксировать изменения с помощью ввода команд «commit» и «save».

2. Сгенерировать и установить клиентский сертификат:

```
# Команда вводится в конфигурационном режиме:
run generate pki certificate sign ca_test install client_test

# Параметры создания сертификата указаны по умолчанию, за
исключением следующих
  полей: «common name» - 192.168.1.33 и «certificate type» - client:
Do you already have a certificate request? [y/N]
Enter private key type: [rsa, dsa, ec] (Default: rsa)
Enter private key bits: (Default: 2048)
Enter country code: (Default: GB)
Enter state: (Default: Some-State)
Enter locality: (Default: Some-City)
Enter organization name: (Default: NGFWOS)
Enter common name: (Default: ngfwos.net) 192.168.1.33
Do you want to configure Subject Alternative Names? [y/N]
Enter how many days certificate will be valid: (Default: 365)
Enter certificate type: (client, server) (Default: server) client
Note: If you plan to use the generated key on this router, do not encrypt the
private key.
Do you want to encrypt the private key with a passphrase? [y/N]
2 value(s) installed. Use "compare" to see the pending changes, and "commit"
to apply.
```

где:

- **client_test** - имя клиентский сертификата, используемого в качестве примера;
- **192.168.1.33** - IP-адрес системы **ARMA Стена**, используемый для сетевого взаимодействия с сервером rsyslog.

Зафиксировать изменения с помощью ввода команд «commit» и «save».

3. Сгенерировать и сохранить в файл сертификат для сервера rsyslog:

```
# Команда вводится в конфигурационном режиме:
run generate pki certificate sign ca_test file /home/admin/

# Параметры создания сертификата указаны по умолчанию, за
исключением следующих
  полей: «common name» - 192.168.1.27 и «certificate type» - server:
Do you already have a certificate request? [y/N]
Enter private key type: [rsa, dsa, ec] (Default: rsa)
Enter private key bits: (Default: 2048)
Enter country code: (Default: GB)
```

```
Enter state: (Default: Some-State)
Enter locality: (Default: Some-City)
Enter organization name: (Default: NGFWOS)
Enter common name: (Default: ngfwos.net) 192.168.1.27
Do you want to configure Subject Alternative Names? [y/N]
Enter how many days certificate will be valid: (Default: 365)
Enter certificate type: (client, server) (Default: server) server
Note: If you plan to use the generated key on this router, do not encrypt the
private key.
Do you want to encrypt the private key with a passphrase? [y/N]
File written to /home/admin/.pem
File written to /home/admin/.key
```

где **192.168.1.27** – IP-адрес сервера rsyslog.

Зафиксировать изменения с помощью ввода команд «commit» и «save».

После выполнения команды в указанном каталоге /home/admin/ будут созданы два файла без явно заданных имён:

- **/home/admin/.pem** – файл, содержащий сертификат;
- **/home/admin/.key** – файл, содержащий приватный ключ.

Необходимо скопировать эти файлы на сервер rsyslog и разместить их в соответствующих директориях, используемых для хранения SSL-сертификатов и ключей.

4. Скопировать корневой сертификат на сервер rsyslog. Для этого необходимо ввести команду в эксплуатационном режиме:

```
admin@ngfwos:~$ show pki ca ca_test pem

-----BEGIN CERTIFICATE-----
MIIDPzCCAo+gAwIBAgIUXX4OYrhzXEOCTvdmS/aHNEYfN+QwDQYJKoZIhvcNAQEL
QEL
BQAwwXDELMAkGA1UEBhMCRC0lxEzARBgNVBAgMCINvbWUtU3RhdGUxEjAQBg
NVBAcM
CVNvbWUtQ2l0eTEPMA0GA1UECgwGTkdGV09TMRMwEQYDVQQDDApuZ2Z3
b3MubmV0
MB4XDTI1MDYwNDEyMzEzMFoXDTE1MDYwNDEyMzEzMFowXDELMAkGA1UE
BhMCRC0lxEzARBgNVBAgMCINvbWUtU3RhdGUxEjAQBgNVBAcMCVNvbWUtQ2l0eTEPMA
0GA1UE
CgwGTkdGV09TMRMwEQYDVQQDDApuZ2Z3b3MubmV0MIIBIjANBgkqhkiG9w
0BAQEF
```

```
AAOCAQ8AMIIBCgKCAQEAq5ggnKHa7II0/PoSne+wc2d0YO4a3wM7dycB4Ovv
k0Dy
FfSUgxRou+agKJQFYlo11c/54nzz90yWEz1uGalAKTCaLf07zJ1DhufvEtLnsFVP
j6GTqlX9GdV5RifTAN5OPuBmBr9n/BpGz7iQhGJnTRNzhaqqkfl284oiREUR4rx+
TTFvQ5lydVGJWDliSzPZ6Zx/rnom6hKFR2MOEvHZJLuvSrjdl6dASP4KL6nPg6hZ
CkH8eh8VMx5FReJg2wrfAQn+h844eWqZ8YEbEKJNSGjgeSfVhBf5F5n6Rsw4ioS
E
a/IESAHO2iMJT5vaep8SdKeNo7LYD45QzPoBsJo7mQIDAQABo2EwXzAPBgNVH
RMB
Af8EBTADAQH/MA4GA1UdDwEB/wQEAwIBhjAdBgNVHSUEFjAUBggrBgEFBQc
DAgYI
KwYBBQUHAWAwHQYDVR0OBBYEF0GzMguk8LcRc5j+KKHHYYwxJDgWMA0GC
SqGSIb3
DQEBChUAA4IBAQBVwrNOC9PpssxxhLRNAd9OBjxwOVnySVXHT9lr7g4Uf4AwI
ZyK
pw30X0D9bvijXNskQXJga01mMy1DNclD6ZarVcH6lvSZE/YDNncCKeBRZptfgP7
a
BDyVKFf8uDxKjWfJITYpsGnRk5JdnEqXsiFBx/mkAsXiQEOhIV2zspDGM8wRidE6
26RXMI0RB5GSeCg2hm+ZocHzNhAlnIVz08qzqxZ9BkcU/ONMDN4pCOXjWjh5
DKIn
mp8CJQJjULTN3ifYV0PzGoetHWig/unGlq0JfK3atlZs8bzA8tBjfuj4yNexOi3e
bnCtMkqg+IT2X3W9dn1l0JB4Oc3kwarjiZOB
-----END CERTIFICATE-----
```

Необходимо скопировать сертификат и сохранить его в новый текстовый файл. Затем изменить расширение файла с «.txt» на «.pem» и перенести его на сервер rsyslog.

5. Настроить систему **ARMA Стена** на экспорт событий на сервер rsyslog:

```
# Сохранить корневой и клиентский сертификаты в конфигурационный
# файл:
set system logging global ssl ca-certificate ca_test
set system logging global ssl certificate client_test

# Установить отправку событий сервиса ssh на сервер rsyslog:
set system logging host 192.168.1.27 log ssh

set system logging host 192.168.1.27 format cef
set system logging host 192.168.1.27 protocol tcp
set system logging host 192.168.1.27 encryption yes
set system logging host 192.168.1.27 port 6514

# Установить отправку событий на сервер rsyslog по адресу 192.168.1.27
# с аутентификацией через X.509-сертификат клиента:
set system logging host 192.168.1.27 authentication x509-name
```

Зафиксировать изменения с помощью ввода команд «commit» и «save».

18.3.3 Экспорт в ARMA Management Console

В системе **ARMA Стена** необходимо создать и установить API ключ для выполнения HTTP-запросов. API-ключ – это отдельный пароль для локальных УЗ в системе **ARMA Стена**, использующийся для выполнения HTTP-запросов. Данный ключ предоставляет доступ к системе **ARMA Стена** посредством **ARMA Management Console (MC)** начиная с версии **1.8 и выше**.

Для создания и установки API ключа необходимо ввести следующую команду в конфигурационном режиме:

```
set service https api keys user <УЗ> key <key>
```

где:

- **<УЗ>** - имя локальной учётной записи в системе **ARMA Стена**;
- **<key>** - пользовательский пароль (API-ключ) для локальной учётной записи **<УЗ>**. Данные параметры будут использоваться для взаимодействия с **ARMA MC**.

Применить настройки командой **commit**:

```
admin@ngfwos# commit
```

WARNING: No certificate specified, using build-in self-signed certificates. Do not use them in a production environment!

```
[ service https ]
```

WARNING: No certificate specified, using build-in self-signed certificates. Do not use them in a production environment!

Сохранить конфигурацию командой «**save**»:

```
admin@ngfwos# save
```

Примечание:

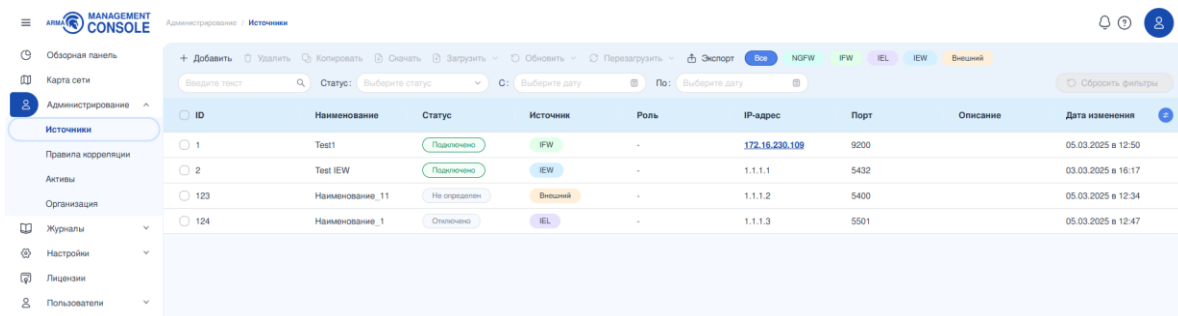
При использовании API-ключа, созданного для учётной записи с ограниченными привилегиями в системе **ARMA Стена** (см. раздел «[Права доступа](#)» руководство по настройке **ARMA Стена** в веб-интерфейсе), доступ к функциональным возможностям веб-интерфейса **ARMA Стена** в **ARMA MC** будет предоставлен в соответствии с уровнем прав, назначенных данной учётной записи. В случаях, когда доступ к определённому разделу отсутствует, в нижнем левом углу экрана будет отображаться сообщение об ошибке: «**Request failed with status code 500**».

Рекомендуется создать API-ключ для учётной записи, относящейся к классу «**NGFW_Administrators**».

18.3.3.1 Настройка ARMA Management Console

Для подключения устройства **ARMA Стена** к программному обеспечению **ARMA MC** необходимо выполнить следующую последовательность действий:

1. Выполнить аутентификацию в веб-интерфейсе **ARMA MC**.
2. Выбрать раздел меню «**Администрирование**», затем – подраздел «**Источники**» (см. [Рисунок – Источники](#)).



ID	Наименование	Статус	Источник	Роль	IP-адрес	Порт	Описание	Дата изменения
1	Test1	Подключено	IFW	-	172.16.230.109	9200		05.03.2025 в 12:50
2	Test IEW	Подключено	IEW	-	1.1.1.1	5432		03.03.2025 в 16:17
123	Наименование_11	Не определен	Внешний	-	1.1.1.2	5400		05.03.2025 в 12:34
124	Наименование_1	Отключено	IEL	-	1.1.1.3	5501		05.03.2025 в 12:47

Рисунок – Источники

3. В панели инструментов нажать **кнопку «+ Добавить»**.
4. В открывшейся карточке **«Добавление источника»** выбрать тип источника **«NGFW»** и указать значения следующих параметров (см. [Рисунок – Добавление нового источника событий «NGFW»](#)):

- **«Наименование»** – отображаемое в **ARMA MC** имя устройства. Параметр может содержать только латинские и кириллические буквы, пробел, спецсимволы («.», «_», «-») и не может превышать 128 символов.
- **«IP-адрес»** – IP-адрес подключаемого устройства **ARMA Стена**.
- **«Логин пользователя»** – имя учётной записи (**<УЗ>**), для которой сформирован API-ключ в системе **ARMA Стена**.
- **«API-Ключ»** – пароль (**<key>**), указанный при создании API-ключа для учётной записи (**<УЗ>**) в **ARMA Стена**.

Примечание:

Если добавить источник **«NGFW»** с неверными реквизитами для подключения, **ARMA Стена** со своей стороны заблокирует дальнейшие попытки подключения на 10 минут. При этом в **ARMA MC** этот источник сначала перейдёт в состояние **«Неавторизован»**, а затем в **«Отключен»**. Если это произошло, необходимо исправить данные и сохранить изменения. Подключение произойдёт через 10 минут.

- **«Порт»** – номер порта для приёма незашифрованных событий. Указываются порты в диапазоне от **«1500»** до **«65535»**. Значение должно быть уникальным среди всех настроенных источников в **ARMA MC**.
- **«Передача зашифрованных событий»** – переключатель, определяющий режим приёма событий:
 - *если активирован* – события принимаются по протоколу **TCP** на порт **6514** в зашифрованном виде;
 - *если отключён* – события принимаются по протоколу **UDP** на порт, указанный в поле **«Порт»**, в незашифрованном виде.

При необходимости заполнить поле **«Описание»** дополнительной информацией об устройстве. Поле может содержать не более 250 символов.

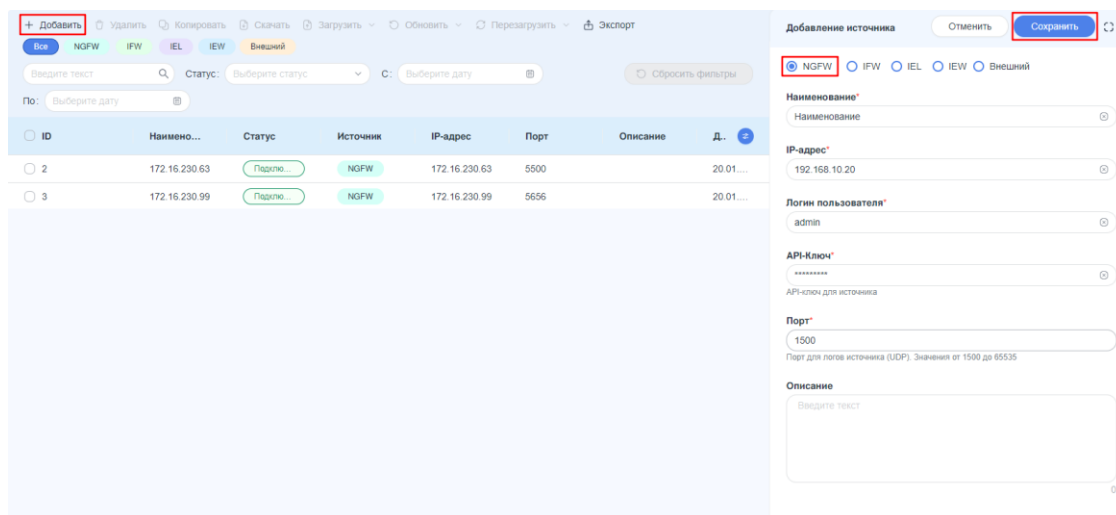


Рисунок – Добавление нового источника событий «NGFW»

После сохранения настроек в столбе «**Статус**» таблицы «**Источники**» отобразится значение «**Подключено**». При указании неверных учётных данных **МС** отобразит статус «**Не авторизован**». Статус «**Ошибка**» отображается, если произошла ошибка, которая может быть связана с аппаратным или программным обеспечением источника «NGFW», а также при использовании данных несуществующей локальной учётной записи в **ARMA Стена**.

18.3.3.2 Настройка ARMA Стена

Передача событий в незашифрованном виде

Для настройки передачи событий в **ARMA МС** в незашифрованном виде требуется выполнение следующих команд в конфигурационном режиме:

1. Указать IP-адрес и порт **ARMA МС**:

```
set system logging host <address> port <portnumber>
```

где:

- **<address>** – IPv4-адрес **ARMA МС**;
- **<portnumber>** – заданный при добавлении источника «NGFW» в **ARMA МС**.

2. Установить формат передачи событий **CEF**:

```
set system logging host <address> format cef
```

3. Задать протокол передачи **UDP**:

```
set system logging host <address> protocol udp
```

4. Указать сервисы, события которых подлежат экспорту:

```
set system logging host <address> log <service-name>
```

где **<service-name>** – идентификатор сервиса из перечня, события которого будут передаваться в **ARMA MC**. Возможно указать следующие сервисы (см. [Таблица «Сервисы»](#)).

Таблица «Сервисы»

Сервис	Сервис	Сервис	Сервис
arma-endpoint	commit-commands	conntrack	conntrack-sync
console-server	dhcp	dhcpv6	dns
firewall	https-api	https	idps
ipoe-server	kernel	lldp	login
nat	ntp	pppoe	pppoe-server
snmp	ssh	systemd	users
vpn	vrrp	webproxy	

Дополнительные фильтры, применимые к экспорту журналов, описаны в разделе «[Экспорт журнала в файл](#)».

5. Применить конфигурацию командой **«commit»** и сохранить её командой **«save»**.

Передача событий в зашифрованном виде

Для настройки передачи событий в **ARMA MC** в зашифрованном виде требуется выполнение следующих команд в конфигурационном режиме:

1. Указать IPv4-адрес **ARMA MC** и порт 6514:

```
set system logging host <address> port 6514
```

где **<address>** – IPv4-адрес **ARMA MC**;

2. Установить формат передачи событий **CEF**:

```
set system logging host <address> format cef
```

3. Задать протокол передачи **TCP**:

```
set system logging host <address> protocol tcp
```

4. Активировать шифрование:

```
set system logging host <address> encryption yes
```

5. Указать сервисы, события которых подлежат экспорту:

```
set system logging host <address> log <service-name>
```

где **<service-name>** – идентификатор сервиса из перечня в [таблице «Сервисы»](#).

Дополнительные фильтры описаны в разделе «[Экспорт журнала в файл](#)».

6. Применить конфигурацию командой «**commit**» и её командой «**save**».

18.3.4 Экспорт в терминал пользователя

Для настройки экспорта журналов в терминал пользователя необходимо выполнить команду:

```
set system logging user-terminal <user-name> log <service-name>
```

где:

- **<user-name>** – имя пользователя, подключённого через CLI;
- **<service-name>** – идентификатор сервиса из перечня, приведённого в [таблице «Сервисы»](#)

Дополнительные фильтры, применимые к экспорту журналов в терминал пользователя, описаны в разделе «[Экспорт журнала в файл](#)».