Утвержден

НВЦС.465651.001И3-ЛУ

ПРОГРАММНО-АППАРАТНЫЙ КОМПЛЕКС «ФОРТИКС»

Руководство администратора

НВЦС.465651.001И3

Инв. № подл. | Подп. и дата | Взам. инв. № | Инв. № дубл. | Подп. дата

Предисловие

Настоящий документ является руководством администратора программно-аппаратного комплекса «Фортикс» (далее по тексту – ПАК «Фортикс», ПАК) и входит в состав эксплуатационной документации ПАК «Фортикс».

В руководстве администратора содержится описание функциональных возможностей, условий и порядка функционирования ПАК «Фортикс», а также действий по эксплуатации ПАК «Фортикс».

Оглавление

Обозначения и сокращения ... 16

1 Введение ... 17

1.1 Область применения ... 17

1.2 Краткое описание возможностей ... 17

1.2.1 Маршрутизатор ... 17

1.2.2 Зонный межсетевой экран ... 19

1.2.3 Основной межсетевой экран ... 20

1.2.4 Прозрачный межсетевой экран ... 21

1.2.5 Трансляция пакетов SNAT, DNAT ... 22

1.2.6 Фильтрация WEB-контента (WCF) ... 23

1.2.7 Криптографическая защита ... 23

1.2.8 Обеспечение высокой доступности сервиса ... 24

1.2.9 Обеспечение качества сервиса (QoS) ... 24

1.2.10 Обеспечение мониторинга ... 25

1.2.11 Сетевые сервисы ... 25

1.2.12 Управление ... 26

1.3 Уровень подготовки администратора ... 26

1.4 Перечень эксплуатационной документации, с которой необходимо ознакомиться администратору ... 26

2 Основы работы ... 28

2.1 Основы работы с интерфейсом командной строки ... 28

2.2 Режим администрирования ... 29

2.2.1 Процесс администрирования ... 29

2.2.2 Команды режима администрирования ... 30

2.3 Режим конфигурации ... 33

2.3.1 Процесс конфигурирования ... 34

2.3.2 Процесс управления деревом конфигурации ... 35

2.4 Ошибки соответствия YANG-схеме ... 38
3 Ввод в эксплуатацию ... 40
3.1 Ввод в эксплуатацию нового изделия ... 40
3.1.1 Подключение к изделию ... 40
3.1.2 Проверка работоспособности ... 41
3.1.3 Смена пароля учётной записи администратора root ... 41
3.1.4 Смена нумерации интерфейсов ... 42
3.1.5 Настройка времени системы ... 42
3.1.6 Настройка имени хоста ... 43
3.1.7 Настройка учётных записей ... 43
3.1.8 Настройка сетевых интерфейсов ... 43
3.1.9 Настройка межсетевого экрана ... 46
3.1.10 Настройка маршрутизации ... 46
3.1.11 Настройка SSL-сертификатов и ключей ... 47
3.2 Ввод в эксплуатацию отремонтированного изделия ... 50
4 Вывод из эксплуатации и утилизация ... 52
4.1 Вывод из эксплуатации ... 52
4.2 Утилизация ... 53
5 Ролевая модель ... 55
5.1 Управление учётными записями ... 55
5.1.1 Создание и удаление учётных записей ... 55
5.1.2 Создание пароля учётной записи ... 55
5.1.3 Настройка ключевой информации для учётной записи ... 56
5.1.4 Настройка времени активности сессии ... 59
5.1.5 Блокировка учётных записей ... 59
5.1.6 Автоматическая блокировка учётных записей ... 60
5.2 Ролевая модель в механизме NACM ... 61
5.2.1 Предустановленные ролевые группы ... 61

5.2.2 Управление членством учётных записей в группах 62
5.2.3 Механизм NACM 63
5.2.4 Удалённая аутентификация учётных записей по протоколу RADIUS 74
6 Сетевые интерфейсы 77
6.1 Общая настройка 77
6.2 Просмотр состояния интерфейсов 79
6.3 Конфигурирование интерфейсов 80
6.4 Интерфейс default 81
6.5 Интерфейсы типа bond 82
6.6 Интерфейсы типа bridge 83
6.7 Интерфейсы типа dummy 84
6.8 Интерфейсы типа fortun 85
6.9 Интерфейсы типа gre 86
6.10 Интерфейсы типа ifb 87
6.11 Интерфейс типа loopback 87
6.12 Интерфейсы типа vlan 87
6.13 Интерфейсы типа vxlan 88
6.14 Интерфейсы типа wg 89
7 Межсетевой экран 91
7.1 Зонный межсетевой экран 91
7.1.1 Зоны 91
7.1.2 Фильтры 93
7.1.3 Счётчики 99
7.1.4 Алгоритм отбора трафика 102
7.1.5 Пример настройки зонного межсетевого экрана 102
7.2 Трансляция адресов (NAT) 104
7.2.1 SNAT (замена адреса источника) 105
7.2.2 DNAT (замена адреса назначения) 107

7.3 Основной межсетевой экран (Netfilter) ... 110
7.3.1 Фильтры ... 112
7.3.2 nDPI ... 118
7.4 Модули conntrack (helper) ... 120
7.5 Bridge firewall ... 121
7.6 Схема работы firewall ... 126
7.7 Журналирование пакетов ... 126
7.7.1 Настройки журналирования ... 128
7.8 Трассировка пакетов ... 129
8 Качество обслуживания (QoS) ... 131
8.1 Величины скорости полос пропускания ... 131
8.2 Классификация ... 131
8.3 Дисциплины исходящего трафика ... 133
8.4 Дисциплина HTB ... 134
8.5 Дисциплина для входящего трафика ... 137
8.6 Интерфейс типа ifb ... 137
8.7 Диагностика ... 138
9 Служба dhcp ... 139
9.1 Служба dhcp в режиме IPv4 ... 140
9.1.1 Настройки принятия запросов ... 140
9.1.2 Настройки тайм-аутов ... 141
9.1.3 Настройка статического назначения ... 142
9.1.4 Настройка динамического назначения ... 143
9.1.5 Настройка разделяемых сетей для динамического назначения ... 144
9.1.6 Настройки разделяемых сетей ... 145
9.1.7 Сетевые DHCP-опции ... 146
9.1.8 Пользовательские DHCP-опции ... 148
9.1.9 Прочие настройки ... 149

9.1.10 Динамическое обновление зон DNS ... 149
9.2 Служба dhcp в режиме IPv6 ... 150
9.2.1 Настройки принятия запросов ... 151
9.2.2 Настройка статического назначения ... 151
9.2.3 Настройка динамического назначения ... 152
9.2.4 Сетевые DHCP-опции ... 152
9.2.5 Пользовательские DHCP-опции ... 153
9.2.6 Связь с DNS (динамическое обновление) ... 154
9.3 Команды режима администрирования ... 154
9.3.1 Команды удаления данных ... 154
10 Служба dhcprelay ... 155
10.1 Служба dhcprelay в режиме IPv4 ... 155
10.1.1 Основные настройки ... 155
10.1.2 Дополнительные настройки ... 156
10.2 Служба dhcprelay в режиме IPv6 ... 157
10.2.1 Основные настройки ... 157
10.2.2 Дополнительные настройки ... 157
10.3 Примеры ... 158
11 Служба dns ... 159
11.1 Общие сведения ... 159
11.2 Базовые настройки службы ... 159
11.2.1 Глобальные настройки службы ... 159
11.2.2 Настройки представления view ... 160
11.2.3 Настройки зоны zone ... 161
11.2.4 Пример конфигурации службы dns ... 162
11.2.5 Команды режима администрирования ... 162
11.3 DNSSEC ... 162
11.3.1 Глобальные настройки службы ... 162

12 Служба conntrack 163
12.1 Общие настройки 163
12.2 Протоколы синхронизации 165
12.2.1 Настройки режима FTFW 165
12.2.2 Настройки режима ALARM 166
12.2.3 Настройки режима NOTRACK 167
12.3 Транспортные протоколы 167
12.3.1 Настройки протокола Multicast 168
12.3.2 Настройки протоколов TCP и UDP 169
12.4 Фильтрация 171
12.5 Команды для просмотра информации 172
13 Служба iperf 173
13.1 Настройка серверной части 173
13.2 Настройка клиентской части 174
14 Служба ntp 176
14.1 Настройка сервера времени 176
14.2 Настройка синхронизации 177
14.3 Диагностика 178
15 Служба snmp 180
15.1 Базовая настройка 180
15.1.1 Настройка информации о системе 181
15.1.2 Настройка SNMPv3 182
15.2 Настройка правил доступа 185
15.3 Настройка уведомлений 186
16 Служба ssh 189
16.1 Настройка серверной части 189
16.1.1 Настройка контроля доступа 190
16.1.2 Списки доступа 192

16.1.3 Настройка алгоритмов 194
16.2 Команды клиентской части 197
17 Служба telnet 200
17.1 Настройка серверной части 200
17.2 Команды клиентской части 202
18 Служба wcf 203
18.1 Общие сведения 203
18.2 Глобальный MITM и фильтр mitm 203
18.2.1 Настройки глобального MITM 203
18.2.2 Настройки фильтра mitm 204
18.3 Служба wcf как ICAP-клиент 205
18.4 Фильтры 206
18.4.1 Правила составления списков 206
18.4.2 Фильтр url 209
18.4.3 Фильтр ban 210
18.4.4 Фильтр file-type 210
18.4.5 Фильтр phrase 211
18.4.6 Фильтр search 212
18.4.7 Фильтр modify 214
18.4.8 Объединение списков 214
18.5 Фильтр main-filter 215
18.6 Политики 216
18.6.1 Настройки группы 216
18.6.2 Аутентификация пользователей 217
18.6.3 Группа default 218
18.7 Алгоритм анализа http(s) трафика службой 219
18.8 Настройки журнала службы 222
18.9 Настройка портов и адресов службы 222

18.10 Настройка страницы блокировки ... 223
19 Служба captive-portal ... 224
19.1 Общие сведения ... 224
19.2 Базовые настройки ... 225
19.3 Настройка web-страницы портала ... 226
19.4 Настройка фильтрации трафика ... 226
19.5 Настройка аутентификации ... 228
19.6 Настройка лимитов и тайм-аутов ... 228
19.7 Настройка квот трафика ... 230
19.8 Прочие настройки ... 231
19.9 Управление службой ... 231
20 Служба journal ... 232
20.1 Общие сведения ... 232
20.2 Настройка размера системного журнала на диске ... 232
20.3 Уведомления о критичных событиях в интерфейсе командной строки ... 233
20.4 События в журнале и их обработка ... 234
20.4.1 Правила написания регулярных выражений для фильтра message-regex ... 235
20.4.2 Пересылка сообщения на удалённый сервер ... 236
20.4.3 Выполнение скрипта ... 237
20.4.4 Дублирование сообщения в журнал событий СКЗИ ... 239
20.5 Просмотр журнала ... 241
20.6 Очистка журнала ... 242
20.7 Проверка целостности журнала ... 243
21 Служба scheduler ... 245
21.1 Общие сведения ... 245
21.2 Настройка пользователя ... 245
21.3 Настройка события ... 245
21.4 Особенности работы ... 246

22 Служба vrrp 247
22.1 Базовая настройка 247
22.2 Настройка виртуальных IP-адресов 249
22.3 Группы синхронизации 250
22.4 Настройка режима отслеживания 251
22.5 Диагностика 251
23 Служба netconf 252
23.1 Краткое описание настроек службы netconf 252
23.1.1 Настройка режима listen 252
23.1.2 Настройка режима call-home 255
23.1.3 Настройка глобального хранилища секретных ключей (keystore) 258
23.2 Пример минимальной настройки службы netconf в режиме listen 259
23.3 Минимальная настройка службы netconf в режиме call-home 263
23.4 RPC-процедуры 264
23.4.1 Стандартные RPC 264
23.4.2 RPC-процедуры, специфические для ПАК «Фортикс» 265
24 Стандартная статическая маршрутизация 269
24.1 Основные настройки 269
24.2 Статический маршрут с несколькими переходами 270
24.3 Просмотр информации о маршрутах 271
25 Статическая маршрутизация на основе политик (pbr) 273
25.1 Группы маршрутизации 273
25.2 Правила маршрутизации 273
25.3 Качество канала связи (sla) 275
25.4 Диагностика 277
26 Динамическая маршрутизация 278
26.1 NHT (Nexthop Tracking) 278
26.2 Фильтрация 279

26.2.1 Списки доступа (access-list) 279
26.2.2 Списки префиксов (prefix-list) 281
26.2.3 Карты маршрутов (route-map) 283
26.3 RIP 285
26.3.1 Введение 285
26.3.2 Настройка 285
26.3.3 26.3.3 Диагностика 293
26.4 RIPNG 293
26.4.1 Введение 293
26.4.2 Настройка 293
26.4.3 Диагностика 296
26.5 OSPFv2 296
26.5.1 Введение 296
26.5.2 Основные настройки маршрутизации 298
26.5.3 Настройка зон 303
26.5.4 Команды для настройки интерфейсов 305
26.5.5 Диагностика 307
26.6 OSPFv3 308
26.6.1 Введение 308
26.6.2 26.6.2 Настройка 308
26.6.3 Диагностика 311
26.7 BGP 312
26.7.1 Основные понятия 313
26.7.2 Настройка 315
26.7.3 Диагностика 341
26.8 ISIS 342
26.8.1 Введение 342
26.8.2 Настройка 344

26.8.3 Диагностика ... 351
26.8.4 Пример конфигурации ... 352
26.9 BFD ... 354
26.9.1 Введение ... 354
26.9.2 Настройка ... 355
26.9.3 Диагностика ... 360
27 Виртуальная маршрутизация (VRF) ... 362
28 Мультикаст маршрутизация ... 366
28.1 Статическая мультикаст маршрутизация ... 367
28.2 Настройка IGMP ... 368
28.3 Настройка PIM ... 369
28.4 Диагностика ... 372
29 Обслуживание ... 374
29.1 Общие сведения ... 374
29.2 Управление прошивками и системами ... 375
29.3 Управление слотами данных ... 377
29.4 Информационные команды ... 377
29.5 Лицензия системы ... 378
29.6 Контроль целостности ... 381
30 Скрипты ... 382
30.1 Дескрипторы ... 383
30.2 Функции ... 384
30.2.1 Функции set_config() и del_config() ... 385
30.2.2 Функция load_config() ... 386
30.2.3 Функция commit() ... 386
30.2.4 Функция revert() ... 387
30.2.5 Функция exit() ... 387
30.2.6 Функция command() ... 387

30.2.7 Функция file() ... 388
30.2.8 Функция sleep() ... 388
30.2.9 Функция getenv() ... 388
30.2.10 Функция stop_on_error() ... 389
30.2.11 Функция noerror() ... 389
30.2.12 Функция check_error() ... 390
30.2.13 Функции time() и date() ... 390
30.2.14 Функция send_smtp ... 390
30.2.15 Функция send_snmp ... 391
30.2.16 Функция journal ... 393
30.2.17 Функции get, get_data, get_xpath ... 394
30.3 Библиотеки ... 394
30.4 Расширение стандартных библиотек ... 395
30.4.1 Расширение библиотеки string ... 395
30.4.2 Расширение библиотеки table ... 395
30.5 Пример скрипта ... 396
31 Средства криптографической защиты информации (СКЗИ) ... 397
31.1 Ключ доступа (КД) ... 397
31.1.1 Правила работы с КД ... 397
31.1.2 Инициализация нового КД ... 398
31.1.3 Сохранение КД ... 398
31.1.4 Загрузка КД ... 399
31.1.5 Состояние КД ... 400
31.1.6 Экспорт КД ... 401
31.1.7 Импорт КД ... 401
31.1.8 Плановая замена КД ... 402
31.1.9 Удаление КД ... 402
31.2 Ключи forsec-key ... 403

31.2.1 Импорт forsec-key 403
31.2.2 Просмотр информации о ключах forsec-key 403
31.2.3 Удаление ключей forsec-key и блокировка абонента 405
31.3 Ключи forsec-keypair 405
31.3.1 Генерация ключей forsec-keypair 406
31.3.2 Экспорт и импорт ключей forsec-keypair 406
31.3.3 Просмотр информации о ключах forsec-keypair 407
31.3.4 Удаление ключей forsec-keypair 409
31.3.5 Электронная подпись с использованием ключей forsec-keypair 409
31.4 Интерфейсы fortun 410
31.4.1 Минимальные настройки 411
31.4.2 Настройка шифрования в интерефейсе fortun 412
31.4.3 Сетевые настройки туннелей fortun 416
31.5 Генератор ключевых документов (ГКД) 418
31.5.1 Генерация ключей 419
31.5.2 Создание ключевых документов абонентов 422
31.5.3 Диагностика 425
31.6 Контейнер парольной защиты 425
31.6.1 Создание контейнера парольной защиты 425
31.6.2 Расшифрование контейнера парольной защиты 426
31.7 Журнал событий СКЗИ 426
31.8 Динамический и регламентный контроль ФДСЧ 430
31.9 Блокировка СКЗИ 430
Ссылочные нормативные документы 432
Ссылочные документы 433

Обозначения и сокращения

В настоящем руководстве применяются следующие обозначения и сокращения:

ГКД – генератор ключевых документов

КД – ключ доступа

ПАК – программно-аппаратный комплекс

ПДСЧ – программный датчик случайных чисел

ПО – программное обеспечение

СКЗИ – средство криптографической защиты информации

ФДСЧ – физический датчик случайных чисел

1 Введение

Программно-аппаратный комплекс (далее по тексту – ПАК) «Фортикс» представляет собой программно-техническое средство, реализующее функции контроля и фильтрации в соответствии с заданными правилами проходящих через него информационных потоков и используемое в целях обеспечения защиты информации ограниченного доступа, в том числе криптографическими методами.

В ПАК «Фортикс» встроено программно-аппаратное средство криптографической защиты информации (далее по тексту – СКЗИ) «Фортикс».

1.1 Область применения

ПАК «Фортикс» может использоваться в государственных и коммерческих структурах для обработки и обмена персональными данными, конфиденциальной, служебной, коммерческой и другой информацией, не содержащей сведений, составляющих государственную тайну.

1.2 Краткое описание возможностей

ПАК «Фортикс» предоставляет функциональные возможности маршрутизатора, СКЗИ и средства межсетевого экранирования, реализованные в программном обеспечении (далее по тексту – ПО) ПАК «Фортикс».

1.2.1 Маршрутизатор

ПАК «Фортикс» поддерживает следующие типы сетевых интерфейсов:

– ether:
  – Ethernet интерфейсы;
  – USB-модемы 3G/4G/LTE;
– vlan:
  – 802.1Q;
  – IEEE 802.1ad (QinQ);
– bond – интерфейс для агрегирования сетевых интерфейсов в следующих режимах:
  – поочерёдное циклическое использование (round robin);
  – резервирование (active-backup);

– распределение по хэш-функции (balance-xor);

– одновременная передача (broadcast);

– по стандарту IEEE 802.3ad (LACP);

– адаптивная балансировка передачи (balance-tlb);

– адаптивная балансировка, в том числе на приёме (balance-alb);

– контроль состояния несущей сетевого порта (MII);

– контроль доступности заданного хоста (ARP);

– bridge – интерфейс для работы в режиме сетевого моста с поддержкой протоколов STP, IGMP-snooping и IGMP-routing;

– fortun – туннельный интерфейс с обеспечением криптозащиты трафика по алгоритмам ГОСТ, поддержкой ICMP-проб, автоопределением параметров (работа через NAT), инкапсуляцией трафика в UDP, работающий в режимах L3VPN (IP over IP) и L2VPN (Ethernet over IP);

– gre – туннельный интерфейс, работающий по протоколу GRE;

– loopback – интерфейс-петля;

– dummy – интерфейс-заглушка;

– ifb – виртуальный интерфейс для обеспечения QoS на приёме для всего трафика, проходящего через ПАК «Фортикс»;

– wireguard – интерфейс для клиентской и серверной поддержки Wireguard VPN.

Перечисленные интерфейсы поддерживают:

– произвольный набор адресов IPv4 (в т.ч. по DHCP) и IPv6;

– режим link-detect;

– L2 адрес;

– mtu/multicast/arp и другие свойства.

В ПАК «Фортикс» поддерживаются следующие типы маршрутизации:

– статическая маршрутизация IPv4 и IPv6 с метриками и управлением маршрутами в зависимости от состояния интерфейса (link-detect);

– маршрутизация на основе политик (PBR) со следующими критериями выборки:

– адрес источника и/или адрес назначения;

– порты назначения и/или источника;

– интерфейс, на который принят сетевой пакет;

– динамическая маршрутизация по протоколам:

– OSPFv2/v3;

– BGPv4, v4+, v4-;

– ISIS;

– RIP/RIP2/RIPNG;

– маршрутизация мультикаст-трафика:

– статическая;

– по протоколу IGMP;

– по протоколу PIM SM.

Маршрутизация PBR поддерживает механизм использования ping-проб (keepalive) для обнаружения недоступности шлюза и механизм контроля SLA для обнаружения недоступности шлюза по следующим критериям:

– процент потерь;

– значение задержки;

– значение джиттера.

Поддерживается протокол BFD, реализующий быстрое обнаружение сбоев для статической, PBR и динамической маршрутизации.

Поддерживается технология VRF.

1.2.2 Зонный межсетевой экран

Для обеспечения функциональных возможностей зонного межсетевого экрана ПАК «Фортикс» поддерживает:

– фильтрацию с контролем состояния соединений (Stateful);

– зоны, объединяющие интерфейсы;

– политику блокировки трафика для зоны;

– политику блокировки трафика между зонами при помощи фильтров;

– фильтры, содержащие правила фильтрации;

– следующие критерии отбора трафика для фильтрации:

– IP-адрес;

– TCP/UDP-порт;

– тип ICMP сообщений;

– тип сетевого интерфейса (принимающий/отправляющий);

– номер протокола;

– следующие действия для отобранного трафика:

– пропустить;

– заблокировать с уведомлением;

– заблокировать без уведомления;

– вложенные списки TCP/UDP-портов;

– вложенные списки IP-адресов;

– счётчики и журналирование срабатывания правил.

1.2.3 Основной межсетевой экран

Для обеспечения функциональных возможностей основного межсетевого экрана ПАК «Фортикс» поддерживает:

– фильтрацию каждого пакета (Stateless);

– фильтрацию с контролем состояния соединений (Stateful);

– фильтры, содержащие правила фильтрации и модификации трафика;

– фильтры по определённому приложению (DPI);

– фильтры по расписанию;

– следующие критерии отбора трафика:

– IP-адрес;

– TCP/UDP-порт;

– тип ICMP сообщений;

– тип сетевого интерфейса (принимающий/отправляющий);

– номер протокола;

– количество байт/пакетов за единицу времени;

– состояние соединения;

– значения определённых байт в пакете;

– следующие действия для отобранного трафика:

– пропустить;

– заблокировать с уведомлением;

– заблокировать без уведомления;

– модификацию трафика:

– установка MSS;

– установка TTL;

– установка DSCP;

– вложенные списки TCP/UDP-портов;

– вложенные списки IP-адресов;

– следующие цепочки обработки трафика для применения фильтров:

– prerouting;

– local-in;

– forward;

– local-out;

– postrouting;

– следующие области в цепочках обработки трафика для применения фильтров:

– fragged;

– raw;

– mangle;

– after-nat;

– after-zone;

– счётчики и журналирование срабатывания правил.

1.2.4 Прозрачный межсетевой экран

Для обеспечения функциональных возможностей прозрачного межсетевого экрана ПАК «Фортикс» поддерживает:

– фильтрацию каждого пакета (Stateless);

– фильтры, содержащие правила фильтрации и модификации трафика;

– фильтры по расписанию;

– следующие критерии отбора трафика:

– MAC-адрес;

– ARP пакет;

– VLAN-тег;

– IP-адрес;

– TCP/UDP-порт;

– тип ICMP сообщений;

– имя принимающего/отправляющего интерфейса;

– номер протокола;

– количество байт/пакетов за единицу времени;

– значения определённых байт в пакете;

– следующие действия для отобранного трафика:

– пропустить;

– заблокировать с уведомлением;

– заблокировать без уведомления;

– модификацию трафика:

– установка MAC-адресов отправителя/получателя;

– вложенные списки TCP/UDP-портов;

– счётчики и журналирование срабатывания правил.

1.2.5 Трансляция пакетов SNAT, DNAT

Для обеспечения трансляции пакетов SNAT, DNAT ПАК «Фортикс» поддерживает:

– трансляцию следующих типов:

– адресов и портов входящих пакетов, DNAT;

– адресов и портов исходящих пакетов, SNAT;

– в статический адрес;

– подсеть в подсеть;

– в адрес выходного интерфейса;

– следующие критерии отбора трафика:

– IP-адрес;

– TCP/UDP-порт;

– тип сетевого интерфейса (принимающий/отправляющий);

– ICMP по типу сообщения;

– тип зоны межсетевого экрана (входная/выходная);

– списки сетей и сервисов межсетевого экрана;

– счётчики и журналирование срабатывания правил;

– перенаправление трафика на адрес или порт (redirect);

– отслеживание и трансляция зависимых соединений по следующим протоколам: SIP, H.323 (H.245, Q.931, RAS), AMANDA, IRC, NETBIOS, PPTP, SANE, SNMP, FTP, TFTP.

1.2.6 Фильтрация WEB-контента (WCF)

Для обеспечения фильтрации WEB-контента ПАК «Фортикс» поддерживает:

– следующие типы списков фильтрации:

  – белый (пропустить);

  – чёрный (блокировать);

  – полусерый (проверить контент и чёрный список);

  – серый (проверить контент и пропустить);

– следующие области применения фильтрация:

  – URL;

  – заголовок WEB-страницы;

  – содержимое WEB-страницы;

– следующие критерии фильтрации:

  – слова;

  – регулярные выражения;

  – команды протокола HTTP;

  – MIME-типы микрокода;

  – расширения файлов;

– проксирование HTTP/HTTPS, в том числе прозрачное;

– SSL инспекция HTTPS-трафика.

1.2.7 Криптографическая защита

Для обеспечения криптографической защиты ПАК «Фортикс» поддерживает:

– средства криптографической защиты информации по ГОСТ Р 34.12-2018 [1], 34.13-2018 [2] для VPN-туннелей Fortun;

– два варианта ключей: симметричные ключи и ключевые пары (открытый и закрытый ключи Диффи-Хелманна);

– использование физического датчика случайных чисел на устройстве «Фортикс-стена» для выработки ключей.

1.2.8 Обеспечение высокой доступности сервиса

Для обеспечения высокой доступности сервиса ПАК «Фортикс» поддерживает:

– организацию отказоустойчивого кластера из нескольких изделий по протоколу VRRP в режимах активный/резервный и активный/активный;

– выделенный интерфейс для работы кластера;

– виртуальный MAC-адрес;

– технологию синхронизации состояния соединений между нодами VRRP-кластера.

1.2.9 Обеспечение качества сервиса (QoS)

Для обеспечения качества сервиса ПАК «Фортикс» поддерживает:

– классификацию трафика по следующим критериям:

  – IP-адреса;

  – TCP/UDP-порты;

  – ToS/DSCP;

  – номер протокола;

– следующие дисциплины обработки трафика:

  – noqueue;

  – pfifo_fast;

  – fqcodel;

  – RED;

  – SFQ;

  – HTB;

– шейпер HTB со следующими возможностями:

  – использование иерархической структуры управления полосами пропускания;

  – установка гарантированной полосы;

  – установка предельной полосы;

  – установка дисциплины для полосы;

– политики отбора классифицированного трафика в полосы шейпера HTB;

– установку дисциплин на интерфейсы;

– виртуальный интерфейс IFB, позволяющий обработать весь трафик системы с использованием шейпера HTB;

– перенаправление/зеркалирование трафика на любой интерфейс (в том числе IFB);

– наследование поля ToS/DSCP для туннельного трафика;

– SLA-контроль в PBR.

1.2.10 Обеспечение мониторинга

Для обеспечения мониторинга ПАК «Фортикс» поддерживает:

– протокол SNMP v2/v3;

– трапы SNMP:

  – неуспешная попытка получения информации по snmp;

  – изменение статуса сетевого интерфейса;

– протокол NetFlow v5/v9/ipfix;

– протокол Syslog;

– запись дампов пакетов (tcpdump).

1.2.11 Сетевые сервисы

Для обеспечения функциональных возможностей сетевых сервисов ПАК «Фортикс» поддерживает:

– утилиты для диагностики сети (ping, arping, traceroute);

– утилиты для работы с DNS;

– DHCP-сервер/клиент;

– DHCP Relay;

– DNS-сервер;

– DNS resolver;

– DNS redirect;

– SSH-сервер/клиент;

– NTP-сервер/клиент;

– IPERF-сервер/клиент;

– TELNET-сервер/клиент;

– CURL-клиент (протоколы FTP, HTTP(s), TFTP и др.).

1.2.12 Управление

Для управления ПАК «Фортикс» предусмотрены:

– интерфейс командной строки;

– технология применения конфигурации (точки возврата к предыдущей успешно применённой конфигурации);

– импорт/экспорт и копирование конфигураций в виде файлов;

– доступ к командной строке по протоколу SSH;

– приём/отправка файлов по протоколу SCP;

– работа с конфигурацией по протоколу Netconf;

– ролевая модель (NACM);

– аутентификация учётных записей администраторов ПАК «Фортикс» по протоколу Radius;

– обновление системы средствами командной строки;

– установка нескольких версий ПО на одном ПАК;

– пробная загрузка при обновлении с возможностью автоматического возврата на резервную копию ПО;

– возврат на стабильную конфигурацию (временный коммит).

1.3 Уровень подготовки администратора

К администрированию ПАК «Фортикс» рекомендуется допуск лиц, прошедших специализированное обучение по его безопасной эксплуатации.

1.4 Перечень эксплуатационной документации, с которой необходимо ознакомиться администратору

Для обеспечения безопасной установки, настройки и работы ПАК «Фортикс» администратору необходимо ознакомиться с эксплуатационной документацией согласно следующему перечню:

– ПАК «Фортикс» Руководство администратора НВЦС.465651.001И3 (настоящий документ) (далее по тексту – руководство, руководство администратора);

– ПАК «Фортикс» Формуляр НВЦС.465651.001ФО (далее по тексту – формуляр);

– ПАК «Фортикс» Формуляр. Приложение А Спецификация поставки НВЦС.465651.001ФО1 (далее по тексту – спецификация поставки);

– СКЗИ «Фортикс» Формуляр ПБЦР.468269.003ФО (далее по тексту – формуляр СКЗИ);

– СКЗИ «Фортикс» Правила пользования ПБЦР.468269.003ПП (далее по тексту – правила пользования СКЗИ).

2 Основы работы

В ПАК «Фортикс» предусмотрены следующие режимы работы:

– **режим администрирования:** позволяет осуществлять первичную настройку, диагностические функции, работу с ключевой информацией и другие функции по обслуживанию устройства;

– **режим конфигурации:** позволяет изменять конфигурацию устройства.

Для описания процесса конфигурирования устройства применяются следующие понятия:

– *running* – действующая конфигурация;

– *candidate* – конфигурация-копия действующей конфигурации *running*, используемая для внесения изменений;

– *startup* – сохранённая на внутренний носитель конфигурация (по умолчанию запись *running* сохраняется в *startup*), используемая при запуске системы;

– *commit* – успешно применённая конфигурация-точка восстановления, используемая для сохранения состояния конфигурации.

Конфигурации *commit* хранятся в виде списка точек восстановления, который «сдвигается вниз» при добавлении новой точки восстановления (в случае переполнения списка последняя (наиболее старая) запись удаляется). Список точек восстановления может содержать не более 50 элементов.

Конфигурация устройства представлена в виде древовидной схемы на языке YANG (см. RFC 7950).

2.1 Основы работы с интерфейсом командной строки

Для управления системой используется Juniper-подобный интерфейс, команды в котором применяются следующим образом:

```
> command parameters
```

где

– `command` – команда;

– `parameters` – параметры команды (если параметров несколько, они указываются через пробел).

Каждый параметр команды может быть:

– опциональным (необязательным);

– имеющим аргумент;

– не имеющим аргумент.

Далее по тексту обязательный параметр команды обозначается в <>, необязательный – [].

Для удобства взаимодействия с командной строкой ПАК «Фортикс» доступно использование следующих горячих клавиш:

– <Tab> – автодополнение команды/параметра или вывод возможных вариантов команд/параметров;

– <?> – вывод списка доступных на текущем уровне конфигурации команд или параметров.

2.2 Режим администрирования

2.2.1 Процесс администрирования

Непосредственно после запуска системы используется режим администрирования, который обозначается символом > в начале командной строки:

```
> command
```

Пример применения команды режима администрирования для просмотра действующей конфигурации *running*:

```
> show running
```

Для преобразования вывода команды command-1 с помощью команды command-2 применяется конструкция:

```
> command-1 | command-2
```

Важно! Данная конструкция применима не для всех команд.

По умолчанию для многих команд применяется опция pager для постраничного преобразования вывода.

Для подавления опции pager применяется конструкция:

```
> command | no-pager
```

Пример подавления опции pager в выводе команды для просмотра действующей конфигурации *running*:

```
> show running | no-pager
```

Для преобразования вывода с использованием n-ого количества команд применяется конструкция:

```
> command-1 | command-2 | ... | command-n
```

Пример преобразования вывода с использованием n-ого количества команд для записи информации о версии ядра в файл:

```
> show version | grep Kernel | write <file-name>
```

где <file-name> – полное имя файла или имя файла относительно домашней директории пользователя.

Список некоторых команд для преобразования ввода:

– grep – найти (выбрать);

– sort – отсортировать;

– compare – сравнить;

– silent – подавить интерактивность (не спрашивать);

– write – записать.

2.2.2 Команды режима администрирования

В режиме администрирования в интерфейсе командной строки ПАК «Фортикс» возможно использование следующих команд:

1) Команды для работы с файлами:

– edit <file-name> – редактировать файл, где <file-name> – полное имя файла или имя файла относительно домашней директории пользователя;

– archive [gzip|tar|zip] create <archive-name> <source-name> – создать архив, где gzip|tar|zip – тип создаваемого архива, по умолчанию – tar, <archive-name> – полное имя создаваемого архива или имя архива относительно домашней директории пользователя, <source-name> – полное имя архивируемого файла/директории или имя файла/директории относительно домашней директории пользователя;

– archive [gzip] extract <archive-name> <destination-name> – извлечь архив, где <archive-name> – полное имя извлекаемого архива или имя архива относительно домашней директории пользователя, <destination-name> – полное имя директории для извлечённых из архива данных или имя директории относительно домашней директории пользователя (архивы типа tar|zip извлекаются автоматически);

– `archive list <archive-name>` – вывести содержимое архива, где `<archive-name>` – полное имя существующего архива или имя архива относительно домашней директории пользователя;

– `cat <file-name>` – вывести на экран содержимое файла типа `tar|zip`, где `<file-name>` – полное имя файла или имя файла относительно домашней директории пользователя;

– `compare <file-name-1> <file-name-2>` – сравнить содержимое файлов, где `<file-name-1>`, `<file-name-2>` – полные имена сравниваемых файлов или имена файлов относительно домашней директории пользователя, на экран выводится сообщение при наличии отличий;

– `copy <name-1> <name-2>` – скопировать содержимое файла/директории `<name-1>` в файл/папку `<name-2>`, где `<name-1>`, `<name-2>` – полные имена файлов/директорий или имена файлов относительно домашней директории пользователя;

– `echo <message>` – вывести сообщение в терминал, где `<message>` – строка;

– `ls <file-name>` – вывести размер в байтах, дату и время последнего изменения и имя файла, где`<file-name>` – полное имя файла или имя файла относительно домашней директории пользователя;

– `mkdir <directory-name>` – создать директорию, где ` – полное имя директории или имя директории относительно домашней директории пользователя;

– `mv <file-name-1> <file-name-2>` – перенести содержимое файла `<file-name-1>` в файл `<file-name-2>`, где `<file-name-1>`, `<file-name-2>` – полные имена файлов или имена файлов относительно домашней директории пользователя;

– `rm <file-name>` – удалить файл, где `<file-name>` – полное имя существующего файла или имя файла относительно домашней директории пользователя;

– `tail <file-name> [follow|lines]` – вывести конец содержимого файла, где `<file-name>` – полное имя существующего файла или имя файла относительно домашней директории пользователя, `follow` – режим отслеживания содержимого, `lines` – количество последних выводимых строк;

– `who ami` – вывести имя текущей учётной записи (пользовтаеля).

2) Команды для сетевого взаимодействия:

– `ping <domain-name>|<address>` – проверить доступность сетевого узла, где `<domain-name>|<address>` – имя или IPv4/IPv6-адрес существующего узла;

– `traceroute <domain-name>|<address>` – выполнить трассировку маршрута до сетевого узла, где `<domain-name>|<address>` – имя или IPv4/IPv6-адрес существующего узла;

– arping <domain-name>|<address> – проверить доступность сетевого узла, где <domain-name>|<address> – имя или IPv4/IPv6-адрес существующего узла;

– curl <url> – загрузить/выгрузить файл с/на указанный URL, где <url> – строка;

– nslookup <domain-name>|<address> – получить доменную информации о сетевом узле , где <domain-name>|<address> – имя или IPv4/IPv6-адрес существующего узла;

– ssh connect – подключиться к сетевому узлу по протоколу SSH (см. подраздел «Команды клиентской части»);

– ssh get|put – получить/отправить файл по протоколу SSH с/на сетевой узел (см. подраздел «Команды клиентской части»);

– ssh key generate – сгенерировать ключевую пару для аутентификации на SSH-сервере (см. подраздел «Настройка ключевой информации для учётной записи»);

– tcpdump [interface <interface-name>] [pcap <filter>] – выполнить анализ сетевого трафика, где <interface-name> – имя существующего интерфейса (см. раздел «Сетевые интерфейсы»), <filter> – pcap-фильтр;

– telnet <domain-name>|<address> – подключиться к сетевому узлу по протоколу Telnet, где <domain-name>|<address> – имя или IPv4/IPv6-адрес существующего узла (см. подраздел «Команды клиентской части»);

– whois <domain-name> – получить регистрационную информацию о сетевом узле, где <domain-name> – имя существующего узла.

3) Прочие команды:

– poweroff – выключить ПАК «Фортикс»;

– reboot – перезагрузить ПАК «Фортикс»;

– clear conntrack [<filters>] – удалить запись из таблицы отслеживания соединений, где<filter> – строка (см. ниже).

В качестве параметра <filter> возможно указание одного или нескольких из следующих фильтров:

– dnat – DNAT-соединения;

– dport <dport-number> – соединения с заданным DNAT-портом, где <dport-number> – число от 1 до 65535;

– dst <dst-address> – соединения с заданным адресом назначения, где <dst-address> – IPv4/IPv6-адрес;

– ipv4|ipv6 – соединения заданного семейства адресов;

– proto <proto-name> – соединения заданного протокола, где <proto-name> – строка;

– snat – SNAT-соединения;

– sport <sport-number> – соединения с заданным SNAT-портом, где <sport-number> – число от 1 до 65535;

– src <src-address> – соединения с заданным адресом источника, где <dst-address> – IPv4/IPv6-адрес.

2.3 Режим конфигурации

Для перехода в режим конфигурации применяется команда:

```
> configure
#
```

Режим конфигурации обозначается символом # в начале командной строки.

Для применения команд из режима администрирования в режиме конфигурации перед командой режима администрирования используется префикс do:

```
# do command
```

Пример применения команд из режима администрирования в режиме конфигурации для просмотра версии ПО:

```
# do show version
```

В режиме конфигурации доступны следующие основные команды:

– commit – применить конфигурацию-копию *candidate* в качестве действующей конфигурации *running*;

– del <path-to-element> – удалить элемент конфигурации, где <path-to-element> – строка в формате интерфейса командной строки;

– diff – просмотреть разницу между действующей конфигурацией *running* и конфигурацией-копией *candidate*;

– edit <configuration-level> – перейти на уровень дерева конфигурации, где <configuration-level> – строка в формате интерфейса командной строки;

– up – подняться на уровень выше в дереве конфигурации;

– end – выйти из режима конфигурации;

– exit – в зависимости от текущего уровня в дереве конфигурации подняться на уровень выше (аналогично up) или выйти из режима конфигурации (аналогично end);

– `insert <path-to-element> first|last` – вставить элемент в начало/в конец списка на его уровне конфигурации, где `<element-path>` – строка в формате интерфейса командной строки;

– `insert <path-to-element> after|before <path-to-element>` – вставить элемент до/после другого элемента, где `<path-to-element>` – строка в формате интерфейса командной строки;

– `rollback <commit-date>` – заменить конфигурацию-копию *candidate* на указанную конфигурацию-точку восстановления *commit*, где `<commit-date>` – строка в формате `commit-yyyy-mm-dd-hh:mm:ss-<account-login>`, в которой `<account-login>` – имя учётной записи, выполнившей команду `commit` для сохранения данной конфигурации-точки восстановления (например, `commit-2025-10-10-20:10:10-root`);

– `set <path-to-element>` – установить элемент, где `<path-to-element>` – строка в формате интерфейса командной строки;

– `show` – просмотреть конфигурацию-копию *candidate*;

– `top` – подняться на корневой уровень в дереве конфигурации.

Преобразование вывода в режиме конфигурации осуществляется аналогично преобразованию в режиме администрирования.

2.3.1 Процесс конфигурирования

Процесс конфигурирования осуществляется по следующему алгоритму:

1) При внесении изменений администратор автоматически работает с конфигурацией-копией *candidate*, накапливая все необходимые модификации в ней.

2) После формирования конфигурации-копии *candidate* согласно всем необходимым изменениям применяется команда `commit` для замены действующей конфигурации *running* на *candidate*. При этом конфигурация, сохраняемая на внутренний носитель, *startup* обновляется автоматически.

3) После применения изменений сохраняется новая точка восстановления *commit*, равнозначная новой текущей конфигурации *running*.

Такой процесс управления конфигурацией позволяет администратору постоянно контролировать логическую атомарность и консистентность вносимых изменений, например, при изменении маршрутизации и правил фильтрации одновременно.

2.3.2 Процесс управления деревом конфигурации

Для модификации дерева конфигурации используются следующие основные команды:

– `set` – установить элемент;

– `del` – удалить элемент;

– `insert` – вставить/переместить элемент.

Параметры данных команд см. выше.

Путь к элементу дерева конфигурации в формате интерфейса командной строки вводится как последовательность «слов», разделённых пробелами.

Пример команды для установления значения «`main interface`» для элемента `description` (описание) интерфейса `en0` типа `ether`:

```
# set interface ether en0 description «main interface»
```

Для настройки сразу нескольких элементов, находящихся на одном уровне конфигурации, используется конструкция one-liner: в команде указываются сразу несколько элементов через пробел на их уровне конфигурации.

Пример применения one-liner для перевода интерфейса из примера выше в рабочий режим и настройки получения IPv4-адреса по протоколу DHCP:

```
# set interface ether en0 description «main interface» enable ipv4 dhcp
```

2.3.2.1 Способы изменения, импорта и экспорта конфигурации

Команда `show` позволяет просматривать конфигурацию в текстовом формате и задавать в качестве её параметра путь к просматриваемому уровню конфигурации.

Пример применения команды `show` для просмотра конфигурации всех интерфейсов типа `ether`:

```
# show interface ether
```

Для добавления конфигурации в текстовом формате используется команда `merge`, позволяющая дополнять конфигурацию (не замещать её).

Возможны следующие варианты применения команды `merge`:

– дополнить конфигурацию из терминала (командной строки);

– дополнить конфигурацию из файла.

Так как команда merge позволяет вносить изменения на текущем уровне конфигурации (при применении команды edit), дополнение конфигурации из терминала с помощью данной команды применимо при копировании фрагментов конфигурации.

Пример применения команды merge для переноса конфигурации интерфейса en0 в конфигурацию интерфейса en1:

1) Вывести конфигурацию интерфейса en0:

```
# show interface ether en0
description «main interface»
enable
ipv4 dhcp
[edit]
```

2) Выделить и скопировать в буфер обмена вывод команды.

3) Перейти на уровень конфигурации интерфейса en1 и применить команду merge для дополнения конфигурации из терминала:

```
# edit interface ether en1
[edit interface ether en1]
# merge terminal
Paste config and press C-d to ccc, C-c to abort.
enable
ipv4 dhcp
[edit interface ether en1]
```

4) Вставить содержимое буфера обмена и воспользоваться комбинацией клавиш <Ctrl> + <D> для применения изменений к конфигурации-копии *candidate*.

5) При необходимости выполнить команду diff для просмотра разницы между текущей конфигурацией *running* и конфигурацией-копией *candidate*. Выполнить команду commit для применения изменений к текущей конфигурации *running*:

```
# diff
interface {
ether en1 {
-    no-link-detect
    ipv4 {
+      dhcp
-      address 192.168.101.1/24
    }
  }
}
[edit interface ether en1]
# commit
```

Важно! Не все настройки конфигурации возможно дополнить с помощью вышеописанного метода из-за особенностей вывода команды show. Например, пароли администраторов при применении команды show выводятся следующим образом:

```
# show system login account admin
uid 1001
passwd-hash <hidden>
```

Подобные настройки перенести через буфер обмена невозможно.

Для экспорта конфигурации-копии *candidate* в заданном формате применяется команда:

```
# export json|xml [component]
```

где

– `json|xml` – формат экспортируемой конфигурации;

– `component` – импортируемый уровень конфигурации в формате интерфейса командной строки.

По данной команде выводится вся конфигурация или настройки указанного уровня конфигурации при наличии параметра `[component]`. Для записи конфигурации в файл используется преобразование вывода с помощью команды `write` (см. подраздел «Режим администрирования»).

Для импорта конфигурации в заданном формате применяется команда:

```
# import json|xml <file-name>
```

где

– `json|xml` – формат файла с импортируемой конфигурации;

– `<file-name>` – полное имя файла с импортируемой конфигурацией или имя файла относительно домашней директории пользователя.

Для импорта конфигурации-точки восстановления заданной версии (даты) применяется команда:

```
# import commit <commit-date>
```

где `<commit-date>` – строка в формате `commit-yyyy-mm-dd-hh:mm:ss-<account-login>`, в которой `<account-login>` – имя учётной записи, выполнившей команду `commit` для сохранения данной конфигурации-точки восстановления (например, `commit-2025-10-10-20:10:10-root`).

Для импорта заводской конфигурации применяется команда:

```
# import factory-default
```

Сброс к заводской конфигурации возможен только через применение заводской конфигурации *factory-default* посредством команды `commit`. Никакие комбинации клавиш на корпусе изделия не приведут к сбросу до заводских настроек.

Сохранённая конфигурация *startup* хранится в формате xml.

Важно! Команды `import`, `export`, `merge` не вносят изменения в текущую конфигурацию *running*, данные команды изменяют конфигурацию-копию *candidate*. Для применения изменений к текущей конфигурации *running* используется команда `commit`.

2.4 Ошибки соответствия YANG-схеме

Схема конфигурации ПАК «Фортикс» описана на языке YANG (см. RFC 7950). При применении команды `commit` перед внесением изменений в текущую конфигурацию *running*, сформированных в конфигурации-копии *candidate*, осуществляется проверка конфигурации-копии *candidate* на соответствие YANG-схеме. Если конфигурация-копия *candidate* не проходит проверку, выводится информация об ошибке в виде текстового сообщения, содержащего информацию о проблемном участке конфигурации в виде пути XPath к YANG-схеме или пути к элементу конфигурации.

Пример сообщения об ошибке соответствия YANG-схеме:

```
# diff
qos {
  qdisc {
+    htb a
  }
}
# commit
Error: Mandatory node «ceil» instance does not exist. (Data location «/fx-qo
s:qos/qdisc/htb[name='a']».)
Error: Invalid candidate configuration
```

Команда `commit` не выполнена, так как не создан обязательный элемент `ceil` на участке `/fx-qos:qos/qdisc/htb[name='a']` (данный путь соответствует пути `qos qdisc htb a` в формате интерфейса командной строки).

Сообщения об ошибке имеют следующий формат:

Error: Содержание ошибки (местоположение ошибки).

Значения, принимаемые полем *Содержание ошибки* представлены в таблице 1.

Т а б л и ц а 1 – Возможные значения поля *Содержание ошибки*

Сообщение	Значение
Too few <path> instances.	Недостаточное число элементов на участке <path>.
Too many <path> instances.	Избыточное число элементов на участке <path>.
Mandatory choice <choice-name> data do not exist.	Обязательная ветка <choice-name> не задана.
Mandatory node <node-name> instance does not exist.	Обязательный элемент <node-name> не задан.
When condition <expression> not satisfied.	Не выполнено условие <expression> в конструкции when.
Unique data leaf(s) <leaf-name> not satisfied in <path-1> and <path-2>.	Нарушено требование уникальности элемента(ов) <leaf-name> на участках <path-1> и <path-2>.
Must condition <expression> not satisfied.	Не выполнено условие <expression> в конструкции must.

Значения, принимаемые полем *Местоположение ошибки*, представлены в таблице 2.

Т а б л и ц а 2 – Возможные значения поля *Местоположение ошибки*

Сообщение	Значение
Data location	Путь к элементу конфигурации в формате XPath
Schema location	Путь к схеме конфигурации в формате XPath
Path	Путь в формате XPath, который не соответствует ни элементу, ни схеме

Для просмотра информации о YANG-схеме ПАК «Фортикс» применяется группа команд `show system yang` в режиме администрирования.

Пример применения группы команд `show system yang`:

```
> show system yang xpath interface ether en0
/fx-interface:interface/fx-interface-ether:ether[name=«en0»]

> show system yang scheme /fx-interface:interface/fx-interface-ether:ether
fx-interface-ether:ether[name]/
 description
 enable
 mtu
 no-multicast
...
..
.
> show system yang package fx-interface
```

3 Ввод в эксплуатацию

3.1 Ввод в эксплуатацию нового изделия

При наличии СКЗИ в системе для ввода в эксплуатацию нового изделия следует руководствоваться правилами пользования СКЗИ.

Ввод в эксплуатацию ПАК «Фортикс» должны осуществлять лица, допущенные к управлению ПАК «Фортикс» в качестве администратора. Для ввода в эксплуатацию ПАК «Фортикс» необходимо выполнить:

1) подключение к изделию;
2) проверку работоспособности;
3) смену пароля администратора root;
4) смену нумерации интерфейсов (опционально);
5) настройку времени системы;
6) настройку имени хоста;
7) настройку учётных записей;
8) настройку сетевых интерфейсов;
9) настройку межсетевого экрана;
10) настройку маршрутизации;
11) настройку SSL-сертификатов и ключей (опционально).

3.1.1 Подключение к изделию

Предусмотрено два способа подключения к ПАК «Фортикс»:

– удалённо по протоколу SSH посредством SSH-клиента (в заводской конфигурации ПАК «Фортикс» на интерфейсе 0 сконфигурирован IPv4-адрес 192.168.0.1/24 и включён SSH-сервер);

– локально через консольный порт (нумерация портов для каждого изделия и реквизиты подключения указаны в спецификации поставки), по умолчанию скорость подключения 9600 б/с.

3.1.2 Проверка работоспособности

Для проверки работоспособности изделия необходимо выполнить расчёт и сравнение контрольных сумм в соответствии с разделом «Контрольные суммы» формуляра.

3.1.3 Смена пароля учётной записи администратора root

В ПАК «Фортикс» по умолчанию зарегистрирована учётная запись администратора root, которая обладает полным набором полномочий и не доступна для удаления. При первичной настройке **необходимо** сменить пароль по умолчанию «root» данной учётной записи.

Для смены пароля учётной записи администратора root после входа в систему (логин: `root`, пароль: `root`) применяются команды:

```
> configure
# setup login root password
Change password for root
Password: <new-password>
Retype password: <new-password>
# commit
```

где `<new-password>` – строка, длиной не менее 8 буквенно-цифровых символов латинского алфавита и специальных знаков (# $ % ^ & *).

При изменении пароля указанным способом осуществляется проверка его стойкости, основанная на сравнении значения пароля со словами из словаря. Данный механизм позволяет предотвратить использование слабых или легко угадываемых паролей, повышая безопасность системы.

3.1.3.1 Сброс забытого пароля учётной записи администратора root

Сброс забытого пароля учётной записи администратора root может быть выполнен только со вскрытием корпуса изделия. Сброс пароля выполняется только специалистом компании Изготовителя с последующим опечатыванием корпуса наклейкой-пломбой. Сброс пароля может быть осуществлён на месте эксплуатации изделия или на территории компании Изготовителя. Сброс пароля не является гарантийным случаем и может предоставляется как отдельная услуга или в рамках договора технической поддержки.

При сбросе пароля устанавливается новый пароль, заданный заказчиком услуги. При необходимости конфигурация и ключи шифрования сохраняются.

3.1.4 Смена нумерации интерфейсов

В заводской конфигурации ПАК «Фортикс» реализована нумерация интерфейсов Ethernet по умолчанию (имена соответствуют конструкции `en<номер_порта>`, например, `en0`).

Для изменения заводской нумерации применяется команда:

```
> interface ether enumerate
```

После применения изменений с помощью команды `commit` для фактической смены нумерации интерфейсов необходимо перезагрузить устройство.

Для перезагрузки устройства применяется команда:

```
> reboot
```

3.1.5 Настройка времени системы

Для настройки временной зоны применяется команда:

```
# set system timezone <timezone-value>
```

где `<timezone-value>` – временная зона.

Пример применения команды для настройки временной зоны МСК+0 (UDC+3):

```
> configure
# set system timezone Europe/Moscow
# commit
```

Для настройки даты и времени применяется команда:

```
> clock <date>
```

где `<date>` – строка в формате `hh:mm:ss yyyy-mm-dd`.

Пример применения команды для настройки времени 10 часов 6 минут 40 секунд и даты 2 апреля 2024 года:

```
> clock 10:06:40 2024-04-02
```

3.1.6 Настройка имени хоста

В начале командной строки при вводе команд отображается имя хоста, которое можно использовать для идентификации системы. В заводской конфигурации ПАК «Фортикс» используется имя хоста `Fortics`.

Для изменения имени хоста применяется команда:

```
# set system hostname <hostname>
```

где `<hostname>` – строка.

Пример применения команды для изменения имени хоста на `gw1`:

```
# set system hostname gw1
# commit
```

3.1.7 Настройка учётных записей

В ПАК «Фортикс» по умолчанию создана учётная запись администратора root, имеющая доступ к полному набору действий по управлению конфигурацией и обслуживанию. Для усиления мер безопасности и удобства управления правами доступа в ПАК «Фортикс» реализована возможность создания учётных записей администраторов с ограниченными полномочиями. Для удобства управления учётными записями администраторов с однотипным набором полномочий реализована возможность создания ролевых групп.

П р и м е ч а н и е – Не рекомендуется использовать учётную запись администратора root для удалённого управления изделием. Для этого возможно создание отдельной учётной записи администратора или использование учётных записей, аутентифицируемых по протоколу RADIUS. Для учётной записи администратора root не рекомендуется разрешать сетевой доступ.

Подробнее см. раздел «Ролевая модель».

3.1.8 Настройка сетевых интерфейсов

Для успешного ввода ПАК «Фортикс» в эксплуатацию необходимо выполнить настройку сетевых интерфейсов на устройстве (персональном компьютере) администратора:

1) Если сетевые кабели не были подключены ранее, следует подключить сетевые кабели.

2) Проверить индикацию на портах изделия.

3) Проверить состояние линии связи.

Для проверки состояния линии связи на интерфейсе применяется команда:

```
> show interface <interface-type> <interface-name> link
```

где

– <interface-type> – тип интерфейса (подробнее см. раздел «Сетевые интерфейсы»);

– <interface-name> – имя интерфейса (подробнее см. раздел «Сетевые интерфейсы»).

Пример применения и вывода команды для проверки состояния линии связи на интерфейсе en0 типа ether:

```
> show interface ether en0 link
en0 [ether]: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state
UP group default qlen 1000
Settings for en0:
        Supported ports: [ TP ]
        Supported link modes:   10baseT/Half 10baseT/Full
                                100baseT/Half 100baseT/Full
                                1000baseT/Full
        Supported pause frame use: No
        Supports auto-negotiation: Yes
        Supported FEC modes: Not reported
        Advertised link modes:  10baseT/Half 10baseT/Full
                                100baseT/Half 100baseT/Full
                                1000baseT/Full
        Advertised pause frame use: No
        Advertised auto-negotiation: Yes
        Advertised FEC modes: Not reported
        Speed: 1000Mb/s
        Duplex: Full
        Auto-negotiation: on
        Port: Twisted Pair
        PHYAD: 0
        Transceiver: internal
        MDI-X: off (auto)
        Supports Wake-on: d
        Wake-on: d
        Current message level: 0x00000007 (7)
                               drv probe link
        Link detected: yes
```

4) Проверить доступность сетевого оборудования (посредством ping-проб).

5) В случае неуспеха на шаге 4) проверить ARP-таблицу.

Для проверки соседства применяется команда:

```
> show neighbor
```

Пример вывода команды для проверки соседства:

```
192.168.174.1 dev en0 lladdr 00:50:56:c0:00:08 DELAY
192.168.174.2 dev en0 lladdr 00:50:56:eb:87:3c STALE
192.168.174.254 dev en0 lladdr 00:50:56:ea:d9:b7 STALE
```

Примечание – В заводской конфигурации ПАК «Фортикс» маршрутизация отключена в целях безопасности. Включение маршрутизации необходимо выполнять на последнем этапе ввода устройства в эксплуатацию после настройки средств защиты информации (в случае их наличия в системе).

6) Если при вводе в эксплуатацию подключение к изделию осуществляется по протоколу SSH, следует настроить реквизиты для удалённого подключения и подключиться удалённо на настроенный IP-адрес.

Для указания дополнительного IP-адреса на интерфейсе применяется команда:

```
# set interface <interface-type> <interface-name> ipv4|ipv6 address <address
>
```

где

– `<interface-type>` – тип интерфейса (подробнее см. раздел «Сетевые интерфейсы»);

– `<interface-name>` – имя интерфейса (подробнее см. раздел «Сетевые интерфейсы»);

– `ipv4|ipv6` – уровень конфигурации IPv4/IPv6;

– `<address>` – IPv4-адрес в формате `A.B.C.D/mask` или IPv6-адрес в формате `A:B:...:H/mask` в зависимости от уровня конфигурации.

Пример применения команды для указания дополнительного IP-адреса `10.0.0.7/24` на интерфейсе `en0` типа `ether` (в заводской конфигурации ПАК «Фортикс» на данном интерфейсе настроен IP-адрес 192.168.0.1/24):

```
# edit interface ether en0
[edit interface ether en0]
# set ipv4 address 10.0.0.7/24
# commit
```

Для просмотра установленных IP-адресов на интерфейсе и его состояния применяется команда:

```
> show interface <interface-type> <interface-name>
```

где

– `<interface-type>` – тип интерфейса (подробнее см. раздел «Сетевые интерфейсы»);

– `<interface-name>` – имя интерфейса (подробнее см. раздел «Сетевые интерфейсы»).

Пример применения и вывода команды для просмотра состояния интерфейса `en0` типа `ether`:

```
> show interface ether en0
en0 [ether]: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state
UP group default qlen 1000
    link/ether 00:0c:29:4f:7b:f2 brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.1/24 brd 192.168.0.255 scope global en0
       valid_lft forever preferred_lft forever
    inet 192.168.174.130/24 brd 192.168.174.255 scope global en0
       valid_lft forever preferred_lft forever
```

7) Для завершения этапа настройки сетевых интерфейсов необходимо удалить заводскую настройку IP-адреса `192.168.0.1` с интерфейса `en0`.

Для удаления заводской настройки IP-адреса `192.168.0.1` с интерфейса `en0` применяется команда:

```
# edit interface ether en0
[edit interface ether en0]
# del ipv4 address 192.168.0.1/24
# commit
```

3.1.9 Настройка межсетевого экрана

Необходимо выполнить настройку фильтрации, исключающую несанкционированный доступ к ПАК «Фортикс» и защищаемым сетям. ПАК «Фортикс» не имеет скрытых открытых TCP/UDP-портов, которые бы следовало защищать отдельно.

Подробнее см. раздел «Межсетевой экран».

3.1.10 Настройка маршрутизации

Необходимо выполнить настройку маршрутизации и проверить доступность сетевого оборудования.

Подробнее см. разделы «Стандартная статическая маршрутизация», «Статическая маршрутизация на основе политик (pbr)», «Динамическая маршрутизация», «Виртуальная маршрутизация (VRF)», «Мультикаст маршрутизация».

3.1.11 Настройка SSL-сертификатов и ключей

Некоторые подсистемы ПАК «Фортикс» требуют наличия специальных криптографических материалов: закрытых и открытых ключей, подписанных и самоподписанных X.509-сертификатов. Все операции с данными ключами и сертификатами не требуют наличия ключа доступа. Для удобства работы в системе предустановлен ряд сертификатов, а также корневой самоподписанный сертификат (`fx-cert.pem`) и соответствующий ему закрытый ключ (`fx-key.pem`). Все предустановленные сертификаты расположены в хранилище сертификатов в каталоге `/system/ssl/certs/`. Ключ расположен в каталоге `/system/ssl/private/`. Если файл с самоподписанным сертификатом или закрытым ключом отсутствует, оба файла `fx-cert.pem` и `fx-key.pem` автоматически пересоздаются. Некоторые службы используют не сам сертификат, а его отпечаток (хэш-файл). Хэш-файлы также расположены в хранилище сертификатов, их создание и удаление осуществляется автоматически при добавлении или удалении сертификатов в хранилище.

3.1.11.1 Команды для работы с сертификатами и ключами в ПАК «Фотикс»

Важно! При генерации ssl-сертификатов/ключей время генерации учитывается относительно таймзоны, настроенной на устройстве, выполняющем команду. Таким образом, при условии переноса сертификата на устройство, таймзона которого сдвинута на `n` часов вперёд, он будет валиден только спустя `n` часов относительно времени генерации сертификата.

Например: если на устройстве генерации ключа выставлена таймзона UTC и сертификат сгенерирован в 12:00, при этом сертификат переносится на устройство в таймзоне UTC+3, данный сертификат будет валиден только с 15:00.

Для генерации закрытого ключа применяется команда:

```
> ssl key generate rsa|dsa [bits <bits-number>] [pubexp <pubexp-value>] <path-to-public-key-file>
```

где

– `rsa|dsa` – криптографический алгоритм для формирования ключа (RSA или DSA);

– `<bits-number>` – размер ключа (число);

– `<pubexp-value>` – значение публичной экспоненты (число);

– `<path-to-public-key-file>` – полное имя файла с закрытым ключом или имя файла относительно домашней директории пользователя.

Для проверки закрытого ключа применяется команда:

```
> ssl key check <path-to-key-file>
```

где <path-to-key-file> – полное имя файла с закрытым ключом или имя файла относительно домашней директории пользователя.

Для генерации самоподписанного сертификата применяется команда:

```
> ssl cert generate <path-to-private-key-file> <day-number> <path-to-cert-fi
le>
```

где

– <path-to-private-key-file> – полное имя файла с закрытым ключом или имя файла относительно домашней директории пользователя;

– <day-number> – срок действия сертификата (число дней);

– <path-to-cert-file> – полное имя файла самоподписанного сертификата или имя файла относительно домашней директории пользователя.

Для генерации подписанного сертификата применяется команда:

```
> ssl cert generate <path-to-key-file> <day-number> <path-to-cert-file> sign
<path-to-ca-cert-file> <path-to-ca-private-key-file> cn <cn-value> sn <sn-nu
mber>
```

где

– <path-to-private-key-file> – полное имя файла с закрытым ключом или имя файла относительно домашней директории пользователя;

– <day-number> – срок действия сертификата (число дней);

– <path-to-cert-file> – полное имя файла подписанного сертификата или имя файла относительно домашней директории пользователя;

– <path-to-ca-cert-file> – полное имя файла корневого сертификата или имя файла относительно домашней директории пользователя;

– <path-to-ca-private-key-file> – полное имя файла с закрытым ключом корневого сертификата или имя файла относительно домашней директории пользователя;

– <cn-value> – поле Common Name (CN) подписанного сертификата;

– <sn-number> – серийный номер (Serial Number) подписанного сертификата.

Для проверки соответствия сертификата закрытому ключу применяется команда:

```
> ssl cert check <path-to-cert-file> <path-to-key-file>
```

где

– <path-to-cert-file> – полное имя файла сертификата или имя файла относительно домашней директории пользователя;

– <path-to-private-key-file> – полное имя файла с закрытым ключом или имя файла относительно домашней директории пользователя.

Для преобразования формата сертификата применяется команда:

```
> ssl cert convert <path-to-cert-file> der|pem <path-to-new-cert-file>
```

где

– <path-to-cert-file> – полное имя файла преобразуемого сертификата или имя файла относительно домашней директории пользователя;

– der|pem – формат нового сертификата (DER или PEM);

– <path-to-new-cert-file> – полное имя файла преобразованного сертификата или имя файла относительно домашней директории пользователя.

Для восстановления хранилища сертификатов применяется команда:

```
> ssl cert restore
```

Для проверки подписанного сертификата применяется команда:

```
> ssl cert signed-check <path-to-cert-file> <path-to-ca-cert-file>
```

где

– <path-to-cert-file> – полное имя файла подписанного сертификата или имя файла относительно домашней директории пользователя;

– <path-to-ca-cert-file> – полное имя файла корневого сертификата или имя файла относительно домашней директории пользователя.

Для генерации закрытого ключа WireGuard-туннеля применяется команда:

```
ssl wg gen key <path-to-private-key-file>
```

где <path-to-private-key-file> – полное имя файла с закрытым ключом или имя файла относительно домашней директории пользователя.

Для генерации открытого ключа WireGuard-туннеля применяется команда:

```
ssl wg gen pubkey <path-to-public-key-file>
```

где <path-to-public-key-file> – полное имя файла с открытым ключом или имя файла относительно домашней директории пользователя.

Для генерации дополнительного ключа шифрования WireGuard-туннеля применяется команда:

```
ssl wg gen psk <path-to-psk-key-file>
```

где `<path-to-psk-key-file>` – полное имя файла с дополнительным ключом шифрования или имя файла относительно домашней директории пользователя.

3.2 Ввод в эксплуатацию отремонтированного изделия

При наличии СКЗИ в системе для ввода в эксплуатацию отремонтированного изделия следует руководствоваться правилами пользования СКЗИ.

Ввод в эксплуатацию отремонтированного изделия предполагает наличие у администратора резервной копии информации, подлежащей восстановлению на отремонтированном изделии. В случае отсутствия резервной копии или необходимости восстановления информации следует вводить изделие в эксплуатацию как новое.

Порядок ввода в эксплуатацию отремонтированного изделия:

1) Подключиться к изделию.

Подключение к изделию возможно локально через консольный порт или удалённо по протоколу SSH. Нумерация портов каждого изделия и реквизиты подключения указаны в спецификации поставки.

2) Проверить работоспособность.

Необходимо убедиться в работоспособности изделия, для этого следует выполнить расчёт и сравнение контрольных сумм в соответствии с разделом «Контрольные суммы» формуляра.

3) Восстановить резервную копию пользовательских файлов (опционально).

При наличии копий пользовательских файлов (например, скриптов) необходимо скопировать их на внутренний накопитель изделия с помощью команды:

```
> copy <source-name> <destination-name>
```

где

– `<source-name>` – полное имя файла/директории, откуда копируются данные, или имя файла/директории относительно домашней директории пользователя;

– `<destination-name>` – полное имя файла/директории, куда копируются данные, или имя файла/директории относительно домашней директории пользователя.

4) Восстановить резервную копию конфигурации.

Для восстановления конфигурации необходимо:

4.1) Выполнить импорт конфигурации (см. пункт «Способы изменения, импорта и экспорта конфигурации»).

4.2) Применить импортированную конфигурацию с помощью команды:

```
# commit
```

После применения конфигурации пароли администраторов, в том числе администратора root, устанавливаются согласно заданным в импортированной конфигурации.

5) Повторно проверить работоспособность (см. подраздел «Проверка работоспособности»).

При проверке работоспособности на заключительном этапе необходимо:

– перезагрузить изделие;

– проверить доступность сетевого оборудования.

4 Вывод из эксплуатации и утилизация

4.1 Вывод из эксплуатации

При выводе из эксплуатации изделия, используемого в качестве СКЗИ, следует руководствоваться правилами пользования СКЗИ.

Порядок вывода изделия из эксплуатации:

1) Подключиться к изделию.

Подключение к изделию следует выполнять локально через консольный порт. Удалённое подключение невозможно, так как в процессе вывода из эксплуатации сетевые настройки удаляются.

2) Создать резервную копию пользовательских файлов (опционально).

Для переноса настроек на новое или отремонтированное изделие необходимо предварительно создать резервную копию конфигурации на USB-флеш-накопителе и, если необходимо, копию пользовательских файлов (например, скриптов).

Для создания копии пользовательских файлов применяется команда:

```
> copy <source-name> <destination-name>
```

где

– `<source-name>` – полное имя файла/директории с копируемыми данными или имя файла/директории относительно домашней директории пользователя;

– `<destination-name>` – полное имя файла/папки для сохранения копируемых данных или имя файла/директории относительно домашней директории пользователя.

3) Создать резервную копию конфигурации (опционально).

Для создания копии конфигурации необходимо воспользоваться командой для экспорта конфигурации (см. подраздел «Способы изменения, импорта и экспорта конфигурации»).

4) Удалить настройки.

Для удаления настроек требуется удалить старый слот данных (см. раздел «Обслуживание»). Порядок удаления настроек:

4.1) создать новый пустой слот данных;

4.2) привязать к системе новый пустой слот данных (при этом пароль учётной записи администратора root примет значение root);

4.3) войти в систему и удалить старый слот данных.

5) Выключение изделия.

Для выключения изделия применяется команда:

```
> poweroff
```

или используется кнопка включения/выключения питания.

4.2 Утилизация

При использовании СКЗИ в составе ПАК «Фортикс» для утилизации изделия следует руководствоваться правилами пользования СКЗИ.

Утилизация ПАК «Фортикс» должна выполняться в соответствии с действующей нормативной документацией и законодательством Российской Федерации.

Утилизация должна выполняться для изделий, прошедших процедуру вывода из эксплуатации в соответствии с подразделом «Вывод из эксплуатации».

Перед утилизацией необходимо удалить ПО ПАК «Фортикс».

Для удаления ПО ПАК «Фортикс» применяется команда:

```
> system software destroy
```

При выполнении вышеуказанной команды выводится предупреждающее сообщение на экран и запрашивается подтверждение действия:

```
> system software destroy
Warning! The system will de destroyed.
To confirm, type <yes>:
```

После успешного подтверждения осуществляется удаление с отображением прогресса.

Пример вывода при успешном выполнении команды для удаления ПО:

```
Disk 1: [ ==================== ] 100%
The system was destroyed and going to be halted.
[ 7216.527155] reboot: System halted
```

Запрещается утилизация изделий, содержащих ПО ПАК «Фортикс». В случае аппаратной неисправности, не позволяющей загрузить изделие и/или выполнить команду для удаления ПО, следует вскрыть корпус, изъять внутренний накопитель и стереть с него информацию

(отформатировать) с помощью сторонних средств. За подробной инструкцией к каждой аппаратной платформе следует обращаться к Изготовителю.

Порядок утилизации определяет эксплуатирующая изделие организация в соответствии с собственными принятыми правилами утилизации серверного или телекоммуникационного оборудования.

5 Ролевая модель

5.1 Управление учётными записями

Все действия, связанные с использованием учётных записей администраторов, записываются в системный журнал.

5.1.1 Создание и удаление учётных записей

Для создания учётной записи применяется команда:

```
# set system login account <account-name> uid <uid>
```

где

– <account-name> – строка длиной от 1 до 64 символов;

– <uid> – число от 1001 до 64000.

Если значение уникального числового идентификатора (<uid>) учётной записи в данной системе не имеет значения, вместо вышеуказанной команды применяется следующая:

```
# setup login <account-name>
```

где <account-name> – строка длиной от 1 до 64 символов.

При использовании данной команды формируется элемент на уровне конфигурации [edit system login account <account-name>] с использованием незанятого числового идентификатора.

Для удаления учётной записи применяется команда:

```
# del system login account <account-name>
```

где <account-name> – имя существующей учётной записи.

Удаление учётной записи администратора root невозможно.

5.1.2 Создание пароля учётной записи

В ПАК «Фортикс» предусмотрено два способа установки пароля учётной записи:

– в интерактивном режиме;

– в виде хэшированного пароля.

В ПАК «Фортикс» принимается хэш пароля, вычисленный с помощью функции PBKDF2, описанной в рекомендациях Р 1323565.1.040-2022 с использованием хэш-функции, описанной в ГОСТ Р 34.11-2012 [3].

Для указания пароля в интерактивном режиме применяется команда:

```
# setup login <account-name> password
```

где <account-name> – имя существующей учётной записи.

Пример установки пароля данным способ подробно описан в подразделе «Смена пароля администратора root».

Для установки хэшированного пароля учётной записи, отличной от учётной записи администратора root, применяется команда:

```
# set system login account <account-name> passwd-hash <hash>
```

где

– <account-name> – имя существующей учётной записи;

– <hash> – строка в формате crypt(5).

Для установки хэшированного пароля учётной записи администратора root применяется команда:

```
# set system login root passwd-hash <hash>
```

где <hash> – строка в формате crypt(5).

5.1.3 Настройка ключевой информации для учётной записи

В ПАК «Фортикс» реализована возможность аутентификации учётной записи с использованием ключевой информации (без пароля) при использовании протокола SSH для подключения к системе. Для аутентификации по SSH-ключам создаётся пара криптографических ключей: закрытый ключ, хранящийся на устройстве администратора, и открытый ключ для проверки подлинности, размещаемый на удалённом устройстве, к которому необходим доступ.

Для генерации ключевой пары в ПАК «Фортикс» используется команда:

```
> ssh key generate [ecdsa|rsa] [comment <key-id>]
```

где

– ecdsa|rsa – криптографический алгоритм формирования ключа, по умолчанию – RSA;

– <key-id> – слово.

По умолчанию в качестве идентификатора используется имя администратора.

Полученные ключи хранятся в домашнем каталоге администратора в директории ssh/.

Пример применения команд для генерации и просмотра ключевой пары в ПАК «Фотрикс»:

```
> ssh key generate rsa comment ident
The rsa key was successfully created
> ls /home/root/ssh
03.09.2025 20:15:57  ../
04.09.2025 00:37:08  id_rsa                2.5K
04.09.2025 00:37:08  id_rsa.pub            558
```

В данном примере для администратора root создана ключевая пара с закрытым ключом id_rsa и открытым ключом id_rsa.pub.

Для просмотра содержимого файла с открытым ключом применяется команда:

```
> cat <path-to-public-key-file>
```

где <path-to-public-key-file> – полное имя файла с открытым ключом или имя файла относительно домашней директории пользователя.

Пример применения команды для просмотра содержимого файла с открытым ключом:

```
> cat /home/root/ssh/id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQC5AsjWL3H8aEzykgV2hHutYg6PNTQ/z+oL8jMi
/OaFXpyyNjZIqKt3cOMij5zBJ8My8uy6J/X/NONjGsZ5A+QJ28kUrHCa5Tjdb2X9PfNgddtFWbH/
yuha67qieOy0Tnr1LDI7J66K9f7Lmhaal5pMoJd7N93PQvqAJJtq1ksO9e125o+hRr1PnH2bq/Jz
UExluL8SPJMBshcbFA5UbRwGVggRb5JaG8WLNLb/exVi+nItAoPUcXydgFck3ymdkFOFRmp/efby
n3Ab17RyLyfOfRWRSXFLXkelcabBML88rGXRhQCG9EsInz85opnruBVUOeh/BSP/iB/lCFffW7ed
0PAcNAU1DxhR781heX6JsEAx3+UkFDpBLaE/t9NyBByo3NjXLkAORV3+zR1QqmyMm+hDlm9FlV8I
5Y1KvOhHUrYpYSP6WpFyhALZ9wvLQmhNN/n6whaPBuobnZHnK/qRsTr+BoLxmJMUyJd9F+wupdVG
bOdzFXHClj0ofvnbLp8= ident
```

Файл, содержащий открытый ключ, состоит из трёх значений: алгоритм формирования ключа (в данном примере ssh-rsa), сам ключ (AAAAB3N ... vnbLp8=) и идентификатор ключа (ident).

После создания ключевой пары необходимо добавить открытый SSH-ключ на удалённое устройство, к которому настраивается беспарольный доступ. Настройка доступа к устройству без пароля зависит от учётной записи и осуществляется одной из следующих команд:

1.1) Для настройки аутентификации учётной записи администратора root применяется команда:

```
# set system login root ssh-pubkey <ssh-pubkey-id> key <ssh-key-value>
```

где

– <ssh-pubkey-id> – слово;

– <ssh-key-value> – строка в формате алгоритм_формирования_ключа значение_ключа, где указываются алгоритм формирования ключа и значение ключа в одну строку подряд через один пробел.

Например:

```
# set system login root ssh-pubkey ident key «ssh-rsa AAAAB3NzaC1yc2EAAAADAQ
ABAAABgQC5AsjWL3H8aEzykgV2hHutYg6PNTQ/z+oL8jMi/OaFXpyyNjZIqKt3cOMij5zBJ8My8u
y6J/X/NONjGsZ5A+QJ28kUrHCa5Tjdb2X9PfNgddtFWbH/yuha67qieOy0Tnr1LDI7J66K9f7Lmh
aal5pMoJd7N93PQvqAJJtq1ksO9e125o+hRr1PnH2bq/JzUExluL8SPJMBshcbFA5UbRwGVggRb5
JaG8WLNLb/exVi+nItAoPUcXydgFck3ymdkFOFRmp/efbyn3Ab17RyLyfOfRWRSXFLXkelcabBML
88rGXRhQCG9EsInz85opnruBVUOeh/BSP/iB/lCFffW7ed0PAcNAU1DxhR781heX6JsEAx3+UkFD
pBLaE/t9NyBByo3NjXLkAORV3+zR1QqmyMm+hDlm9FlV8I5Y1KvOhHUrYpYSP6WpFyhALZ9wvLQm
hNN/n6whaPBuobnZHnK/qRsTr+BoLxmJMUyJd9F+wupdVGbOdzFXHClj0ofvnbLp8=«
```

1.2) Для настройки аутентификации учётной записи, отличной от администратора root, применяется команда:

```
# set system login account <account-name> ssh-pubkey <ssh-pubkey-id> key <ss
h-key-value>
```

где

– <account-name> – имя существующей учётной записи;

– <ssh-pubkey-id> – слово;

– <ssh-key-value> – строка в формате алгоритм_формирования_ключа значение_ключа, где указываются алгоритм формирования ключа и значение ключа в одну строку подряд через один пробел.

2) Настройка ключевой информации учётной записи с помощью команды setup и значений открытого ключа:

```
# setup login <account-name> ssh-pubkey text <ssh-pubkey-text>
# commit
```

где

– <account-name> – имя существующей учётной записи;

– <ssh-pubkey-text> – строка в формате алгоритм_формирования_ключа значение_ключа идентификатор_ключа, где указываются алгоритм формирования ключа, значение ключа и идентификатор ключа в одну строку подряд через один пробел.

3) Настройка ключевой информации учётной записи с помощью команды setup и файла, содержащего значение открытого ключа:

```
# setup login <account-name> ssh-pubkey file <path-to-sshpubkey-file>
```

где

– <account-name> – имя существующей учётной записи;

– <path-to-sshpubkey-file> – полное имя файла с открытым ключом или имя файла относительно домашней директории пользователя.

5.1.4 Настройка времени активности сессии

Для настройки тайм-аута активности сессии, по истечении которого при отсутствии каких-либо действий администратора в системе сессия его учётной записи автоматически завершается, применяется команда:

```
# set system login session-timeout <session-timeout>
```

где <session-timeout> – число секунд от 0 до 4294967295, по умолчанию – 0.

Для удаления тайм-аута активности сессии применяется одна из следующих команд:

```
# del system login session-timeout
```

или

```
# set system login session-timeout 0
```

5.1.5 Блокировка учётных записей

Блокировка учётной записи позволяет запретить доступ учётной записи к системе.

Для блокировки учётной записи применяется команда:

```
# set system login account <account-name> locked
```

где <account-name> – имя существующей учётной записи.

Блокировка учётной записи администратора root невозможна.

Для снятия блокировки учётной записи применяется команда:

```
# del system login account <account-name> locked
```

где <account-name> – имя существующей учётной записи.

5.1.6 Автоматическая блокировка учётных записей

Для предотвращения несанкционированного доступа посредством подбора пароля к учётной записи администратора в ПАК «Фортикс» реализована временная блокировка учётной записи, которая осуществляется по следующему сценарию: если за определённый промежуток времени (по умолчанию – 15 минут) последовательно осуществляется несколько (по умолчанию – 3) неудачных попыток аутентификации учётной записи, данная учётная запись временно блокируется (отключается). Время блокировки по умолчанию составляет 10 минут. По истечении указанного промежутка времени учётная запись становится доступной. При перезагрузке системы блокировка учётных записей снимается.

Для снятия блокировки всех учётных записей без перезагрузки системы применяется команда:

```
> clear system auth faillock
```

Данная команда снимает блокировку всех ранее заблокированных учётных записей.

Для разблокировки заданной учётной записи применяется команда:

```
> clear system auth faillock account <account-name>
```

где <account-name> – имя существующей учётной записи.

Для просмотра информации о попытках аутентификации применяется команда:

```
> show system auth faillock [brief]
```

где [brief] – параметр, при указании которого информация отображается в сжатом виде.

5.1.6.1 Команды настройки автоматической блокировки

Для изменения количества допустимых последовательно неудачных попыток аутентификации учётной записи применяется команда:

```
# set system auth faillock deny <faillock-deny-number>
```

где <faillock-deny-number> – число от 0 до 100, по умолчанию – 3.

Для изменения времени блокировки учётной записи по истечение допустимого количества неудачных попыток аутентификации применяется команда:

```
# set system auth faillock unlock-time <faillock-unlock-time>
```

где `<faillock-unlock-time>` – число секунд от 0 до 65535, по умолчанию – 600.

При использовании значения 0 указанной настройки автоматическая разблокировка учётной записи отключается. При этом активация учётной записи осуществляется только по команде `clear system auth faillock` или после перезагрузки системы.

Для изменения интервала времени, за который учитываются попытки аутентификации, применяется команда:

```
# set system auth faillock fail-interval <faillock-fail-interval>
```

где `<faillock-fail-interval>` – число секунд от 0 до 65535, по умолчанию – 900.

5.2 Ролевая модель в механизме NACM

5.2.1 Предустановленные ролевые группы

В заводской конфигурации ПАК «Фортикс» определены следующие ролевые группы:

– группа adm;

– группа netadm;

– группа oper.

Учётные записи, добавленные в одну из данных ролевых групп, наделяются соответствующими полномочиями. Если созданная учётная запись не добавлена ни в одну из групп, при включённом механизме NACM (см. подраздел «Механизм NACM») данная учётная запись не имеет никаких полномочий.

5.2.1.1 Группа adm

Группа adm представляет собой группу учётных записей администраторов, обладающих следующими ограничениями полномочий относительно учётной записи администратора root:

– не могут просматривать/администрировать настройки NACM (права доступа);

– не могут просматривать/администрировать учётные записи (настройки уровня конфигурации `system login` и `system auth`, команды уровня `clear system auth`);

– не могут администрировать установленные образы (команды уровней `system software` и `system data-slot`);

– не могут обращаться к директории `/config`.

5.2.1.2 Группа netadm

Группа netadm представляет собой группу учётных записей администраторов, обладающих следующими ограничениями полномочий относительно учётных записей администраторов группы adm:

– не могут выполнять команды и администрировать настройки СКЗИ (команды и настройки уровня `crypto`);

– не могут выполнять команды диагностики СКЗИ, в том числе просматривать журнал событий СКЗИ (команды уровня `show crypto`);

– не могут обращаться к директориям `/share`, `/system`, `/crypto`.

5.2.1.3 Группа oper

Группа oper представляет собой группу учётных записей администраторов, обладающих следующими ограничениями полномочий относительно учётных записей администраторов группы netadm:

– не могут менять конфигурацию системы;

– не могут выполнять действия, меняющие состояние узла;

– не могут менять состояние системы, в том числе:

  – не могут перезагружать/выключать систему;

  – не могут выключать сигнал на события уровня ALERT;

– не имеют доступа к внешним носителям (директория `/media`).

5.2.2 Управление членством учётных записей в группах

Для добавление учётной записи в существующую группу применяется команда:

```
# set nacm groups group <group-name> user-name <user-name>
```

где

– `<group-name>` – имя существующей группы;

– `<user-name>` – имя существующей учётной записи.

Для удаления учётной записи из группы применяется команда:

```
# del nacm groups group <group-name> user-name <user-name>
```

где

– <group-name> – имя существующей группы;

– <user-name> – имя существующей учётной записи.

Для удаления всех учётных записей из группы применяется команда:

```
# del nacm groups group <group-name> user-name
```

где <group-name> – имя существующей группы.

Пример применения команд для создания учётной записи администратора группы adm с именем alex:

```
> configure
# setup login alex
# setup login alex password
Change password for alex
Password:
Retype password:
# set nacm groups group adm user-name alex
# commit
```

После добавления учётной записи администратора в группу adm целесообразно отключить удалённый доступ по протоколу SSH для учётной записи администратора root.

Для отключения удалённого доступа по протоколу SSH учётной записи администратора root применяется команда:

```
# del service ssh access root-login
```

5.2.3 Механизм NACM

В ПАК «Фортикс» контроль доступа и полномочий учётных записей основан на механизме NACM (Network Configuration Access Control Model), который представляет собой модель управления доступом к элементам конфигурации и операциям системы (см. RFC 8341). В настройки механизма NACM ПАК «Фортикс» добавлены дополнительные опции, обеспечивающие управление доступом к командам режима администрирования.

Включённый механизм NACM позволяет контролировать каждую попытку администратора изменить конфигурацию через консоль, сессию SSH или протокол NETCONF: для каждого действия администратора осуществляется проверка на наличие прав у его учётной

записи на изменения (создание, удаление, модификацию). Механизм NACM используется в системе по умолчанию.

Для отключения механизма NACM применяется команда:

```
# set nacm enable-nacm false
```

Важно! Не рекомендуется отключать механизм NACM, так как при отключённом механизме NACM все учётные записи получают полный доступ ко всей конфигурации и RPC-операциям протокола NETCONF.

Для включения механизма NACM применяется одна из следующих команд:

```
# del nacm enable-nacm
```

или

```
# set nacm enable-nacm true
```

Учётная запись администратора root обладает полным набором полномочий, механизм NACM на неё не влияет.

Предусмотрена возможность редактирования настроек механизма NACM для существующих ролевых групп или создание новых групп со специфическими наборами полномочий. Изменение/просмотр настроек механизма NACM доступны учётной записи администратора root и учётным записям администраторов группы adm.

В настоящем руководстве приводится краткое описание стандартных настроек механизма NACM. Далее по тексту пометка (`Фортикс`) соответствует настройкам, специфичным для механизма NACM ПАК «Фортикс».

5.2.3.1 Глобальные настройки механизма NACM

Настройка механизма NACM осуществляется на следующем уровне конфигурации:

```
[edit nacm]
```

На данном уровне конфигурации доступны следующие настройки:

– `enable-nacm true|false` – включить/выключить использование механизма NACM, по умолчанию – `true`;

– `read-default permit|deny <leaf-path>` – разрешить/запретить чтение узла конфигурации, если для него не найдено иных правил, где `<leaf-path>` – строка в формате интерфейса командной строки;

– write-default permit|deny <leaf-path> – разрешить/запретить изменение узла конфигурации, если для него не найдено иных правил, где <leaf-path> – строка в формате интерфейса командной строки;

– exec-default permit|deny <leaf-path> – разрешить/запретить выполнение RPC-операций над узлом конфигурации, если для него не найдено иных правил, где <leaf-path> – строка в формате интерфейса командной строки;

– groups – перейти на уровень конфигурации ролевых групп (см. ниже);

– rule-list – перейти на уровень конфигурации именованных наборов правил (см. ниже).

Для редактирования настроек механизма NACM применяется команда:

```
[edit nacm]
# set <setting>
```

где <setting> – строка.

5.2.3.2 Настройки групп

Настройка групп осуществляется на следующем уровне конфигурации:

```
[edit nacm groups]
```

На данном уровне конфигурации доступны настройки именованных списков правил match/exclude и настройки групп.

Настройка именованных списков правил match/exclude осуществляется на следующем уровне конфигурации:

```
[edit nacm groups match-list <match-list-name>]
```

где <match-list-name> – строка.

На данном уровне конфигурации доступны следующие настройки:

– match *|<pattern> (Фортикс) – указать шаблон команд режима администрирования, разрешённых данной группе (* – все команды, <pattern> – шаблон команд (строка)), возможно определение нескольких настроек данного уровня конфигурации;

– exclude <pattern> (Фортикс) – указать шаблон команд, попадающих в шаблон настройки match, но подлежащих запрету (<pattern> – шаблон команд (строка)), возможно определение нескольких настроек данного уровня конфигурации.

Настройка групп осуществляется на следующем уровне конфигурации:

```
[edit nacm groups group <group-name>]
```

где <group-name> – строка.

На данном уровне конфигурации доступны следующие настройки:

– user-name <user-name> – указать имя учётной записи, входящей в группу, где <user-name> – имя существующей учётной записи, возможно определение нескольких настроек данного уровня конфигурации;

– match *|<pattern> (Фортикс) – указать шаблон команд режима администрирования, разрешённых данной группе, где * – любые команды, <pattern> – строка, возможно определение нескольких настроек данного уровня конфигурации;

– exclude <pattern> (Фортикс) – указать шаблон команд, попадающих в шаблон настройки match, но подлежащих запрету, где <pattern> – строка, возможно определение нескольких настроек данного уровня конфигурации;

– match-list <match-list-name> (Фортикс) – указать именованный список правил match/exclude, применяемый к данной группе, где <match-list-name> – имя существующего списка правил, возможно определение нескольких настроек данного уровня конфигурации;

– fs-crypto-access (Фортикс) – разрешить группе доступ к области /crypto;

– fs-media-access (Фортикс) – разрешить группе доступ к внешним носителям /media;

– fs-system-access (Фортикс) – разрешить группе доступ к директории /system;

– fs-config-access (Фортикс) – разрешить группе доступ к директории /config;

– fs-share-access (Фортикс) – разрешить группе доступ к директории /share.

Настройки групп позволяют определять полномочия данной группы только в режиме администрирования. Полномочия группы в режиме конфигурации определяются с помощью других настроек механизма.

Шаблоны команд режима администрирования представляют собой указанный в кавычках набор слов, с которых начинаются команды. Шаблону соответствуют все команды, начинающиеся с указанного набора слов. Символ * подразумевает множество всех команд.

По умолчанию для учётной записи, созданной вне предустановленных групп, все команды режима администрирования запрещены.

Команда считается разрешённой, если она соответствует хотя бы одному шаблону настройки `match` хотя бы одной группы, в которую входит данная учётная запись, при этом не соответствует ни одному шаблону настройки `exclude` данной группы.

Примеры применения шаблонов:

– `match *` – разрешить все команды;

– `match «crypto matrix»` – разрешить все команды, начинающиеся с `crypto matrix`;

– `exclude «crypto matrix operate»` – запретить команды, начинающиеся с `crypto matrix operate`.

5.2.3.3 Настройки наборов правил

Настройка наборов правил осуществляется на следующем уровне конфигурации:

```
[edit nacm rule-list <rule-list-name>]
```

где `<rule-list-name>` – строка.

На данном уровне конфигурации доступны следующие настройки:

– `group <group-name>` – указать имя группы, для которой применяется данный набор правил, где `<group-name>` – имя существующей группы, возможно определение нескольких настроек данного уровня конфигурации;

– `rule <rule-name>` – указать имя правила, входящего в данных набор правил, где `<rule-name>` – имя существующего правила, возможно определение нескольких настроек данного уровня конфигурации.

Порядок указания наборов правил при настройке определяет их приоритет (см. подпункт «Алгоритм работы механизма NACM»).

Настройка именованных правил осуществляется на следующем уровне конфигурации:

```
[edit nacm rule-list <rule-list-name> rule <rule-name>]
```

где

– `<rule-list-name>` – имя существующего набора правил;

– `<rule-name>` – строка.

На данном уровне конфигурации доступны следующие настройки:

– `comment <description>` – указать описание правила, где `<description>` – строка;

– path <leaf-xpath> – указать путь к узлу конфигурации, к ветвям и элементам которого применимо правило, где <leaf-xpath> – строка в формате XPath;

– module-name <module-name> – указать имя YANG-модуля, к членам которого применимо правило, где <module-name> – строка;

– rpc-name *|<rpc-name> – указать имя RPC-операции, к которой применимо правило, где * – любые операции, <rpc-name> – строка;

– access-operations *|<list> – указать список действий над элементом/RPC-операций, к которым применимо правило, где * – любые действия/операции, <list> – строка в формате списка действий/операций;

– action permit|deny – разрешить/запретить запрашиваемое действие в случае срабатывания правила.

В качестве параметра <list> настройки access-operations *|<list> указывается строка, содержащая перечисление через пробел каких-либо из следующих операций:

– read;

– create;

– update;

– delete;

– exec.

Порядок указания именованных правил при настройке определяет их приоритет (см. подпункт «Алгоритм работы механизма NACM»).

5.2.3.4 Алгоритм работы механизма NACM

При поступлении исходящей от учётной записи попытки изменения конфигурации или выполнения RPC-операции через протокол NETCONF (при включённом механизме NACM) выполняется следующий алгоритм их обработки:

1) Формируется список групп, членом которых является данная учётная запись, согласно настройкам уровня конфигурации [edit nacm groups].

2) Осуществляется обработка наборов правил (rule-list) в том порядке, в котором они объявлены в конфигурации.

3) Если набор правил неприменим к группе(ам) учётной записи (то есть нет пересечения с группами настройки nacm rule-list <rule-list> group), набор правил пропускается.

4) Если набор правил применим к группе(ам) учётной записи, рассматриваются правила (`rule`) одно за другим в порядке их определения в конфигурации.

5) Проверяется применимость правила согласно установленным критериям по принципу логического «И».

6) Если все критерии выполняются, применяется действие, установленное в настройке `action` (то есть операция либо разрешается, либо запрещается). В случае применимости дальнейшие правила и наборы не рассматриваются.

7) Если не сработало ни одно правило в текущем наборе правил, осуществляется переход к следующему набору правил (п. 3).

8) Если не сработало ни одно правило ни в одном наборе правил, действие применяется согласно глобальным настройкам `read-default`, `write-default`, `exec-default`.чё В случае наличия настройки `read-default true` при операции чтения узла конфигурации с установленным YANG-атрибутом `nacm:default-deny-all` операция запрещается.

5.2.3.5 Предустановленные настройки механизма NACM

В заводской конфигурации ПАК «Фортикс» определены следующие настройки механизма NACM:

```
nacm {
  enable-nacm true
  read-default permit
  write-default deny
  exec-default deny
  groups {
    group adm {
      match *
      exclude «clear system auth»
      exclude «system data-slot»
      exclude «system software»
      fs-crypto-access
      fs-media-access
      fs-system-access
      fs-share-access
    }
    group netadm {
      match-list adm-common
      match-list oper-common
      match-list show-common
      match «clear conntrack»
      match «clear firewall»
      match «clear neighbor»
      match «clear router»
```

```
    match «clear vrf»
    match dnssec
    match firewall
    match interface
    match «service captive-portal»
    match «service conntrack»
    match «service dhcp»
    match «service dns»
    match «service wcf»
    match ssl
    fs-media-access
  }
  group oper {
    match-list oper-common
    match-list show-common
  }
  match-list adm-common {
    match «clear alert»
    match «clear ssh known-hosts»
    match clock
    match configure
    match poweroff
    match reboot
    match «service journal»
  }
  match-list oper-common {
    match @
    match archive
    match arping
    match cat
    match compare
    match copy
    match curl
    match echo
    match edit
    match exit
    match gosthash
    match iftop
    match iperf
    match ls
    match mkdir
    match mv
    match nslookup
    match ping
    match rm
    match scp
    match «service journal verify»
    match ssh
    match sysmon
    match tail
```

```
      match tcpdump
      match telnet
      match traceroute
      match who
      match whois
      match write
    }
    match-list show-common {
      exclude «show crypto»
      match show
    }
  }
  rule-list deny-account-mgmt-rules {
    group adm
    group netadm
    group oper
    rule deny-account-mgmt {
      path /fx-system:system/fx-login:login
      access-operations *
      action deny
    }
    rule deny-auth-mgmt {
      path /fx-system:system/fx-auth:auth
      access-operations *
      action deny
    }
    rule deny-nacm {
      path /ietf-netconf-acm:nacm
      access-operations *
      action deny
    }
  }
  rule-list adm-rules {
    group adm
    rule allow-all {
      access-operations *
      action permit
    }
  }
  rule-list netadm-rules {
    group netadm
    rule deny-crypto {
      path /fx-crypto:crypto
      access-operations «create update delete exec»
      action deny
    }
    rule allow-rest {
      access-operations «create update delete»
      action permit
    }
```

```
    rule allow-keystore-rpc {
      module-name ietf-keystore
      rpc-name *
      action permit
    }
  }
  rule-list netconf-rpc-admins-rules {
    group netadm
    rule allow-commit {
      module-name ietf-netconf
      rpc-name commit
      action permit
    }
    rule allow-edit-config {
      module-name ietf-netconf
      rpc-name edit-config
      action permit
    }
    rule allow-copy-config {
      module-name ietf-netconf
      rpc-name copy-config
      action permit
    }
    rule deny-delete-config {
      module-name ietf-netconf
      rpc-name delete-config
      action deny
    }
    rule allow-lock {
      module-name ietf-netconf
      rpc-name lock
      action permit
    }
    rule allow-unlock {
      module-name ietf-netconf
      rpc-name unlock
      action permit
    }
    rule deny-kill-session {
      module-name ietf-netconf
      rpc-name kill-session
      action deny
    }
    rule allow-discard-changes {
      module-name ietf-netconf
      rpc-name discard-changes
      action permit
    }
    rule allow-cancel-commit {
      module-name ietf-netconf
```

```
      rpc-name cancel-commit
      action permit
    }
    rule allow-validate {
      module-name ietf-netconf
      rpc-name validate
      action permit
    }
    rule allow-get-schema {
      module-name ietf-netconf-monitoring
      rpc-name get-schema
      action permit
    }
    rule allow-edit-data {
      module-name ietf-netconf-nmda
      rpc-name edit-data
      action permit
    }
    rule allow-establish-subscription {
      module-name ietf-subscribed-notifications
      rpc-name establish-subscription
      action permit
    }
    rule allow-modify-subscription {
      module-name ietf-subscribed-notifications
      rpc-name modify-subscription
      action permit
    }
    rule allow-delete-subscription {
      module-name ietf-subscribed-notifications
      rpc-name delete-subscription
      action permit
    }
    rule deny-kill-subscription {
      module-name ietf-subscribed-notifications
      rpc-name kill-subscription
      action deny
    }
    rule allow-resync-subscription {
      module-name ietf-yang-push
      rpc-name resync-subscription
      action permit
    }
    rule allow-create-subscription {
      module-name notifications
      rpc-name create-subscription
      action permit
    }
  }
  rule-list oper-rpc-rules {
```

```
    group netadm
    group oper
    rule allow-exec-script {
      module-name fx-system
      rpc-name exec-script
      access-operations exec
      action permit
    }
    rule allow-get-uptime {
      module-name fx-system
      rpc-name get-uptime
      access-operations exec
      action permit
    }
    rule allow-get-interface-info {
      module-name fx-interface
      rpc-name get-interface-info
      access-operations exec
      action permit
    }
  }
}
```

5.2.4 Удалённая аутентификация учётных записей по протоколу RADIUS

ПАК «Фортикс» поддерживает механизм аутентификации через удалённый сервер по протоколу RADIUS, который позволяет централизованно настраивать и администрировать множество учётных записей для различных систем в одном месте на удалённом сервере.

Для подключения удалённой аутентификации учётной записи по протоколу RADIUS необходимо:

1) Активировать механизм удалённой аутентификации учётных записей с помощью команды:

```
# set system auth radius enable
# commit
```

2) Выполнить настройку механизма удалённой аутентификации по протоколу RADIUS.

Обязательной настройкой является определение IP-адреса RADIUS-сервера и установка пароля для подключения к данному серверу. Данные настройки осуществляются с помощью команды:

```
# set system auth radius server <server-ip> secret <password>
# commit
```

где

– <server-ip> – IP-адрес или DNS-имя, которое автоматически трансформируется в IP-адрес;

– <password> – строка.

Для указания нескольких RADIUS-серверов, имеющих различные адреса, необходимо выполнить данную команду несколько раз с указанием адреса и пароля для каждого сервера (при удалённой аутентификации осуществляются поочередные попытки подключения ко всем указанным серверам).

При необходимости для указания номера порта подключения сервера применяется команда:

```
# set system auth radius server <server-ip> port <port-number>
# commit
```

где

– <server-ip> – IP-адрес или DNS-имя, которое автоматически трансформируется в IP-адрес;

– <port-number> – число от 1 до 65535, по умолчанию – 1812.

При необходимости для настройки тайм-аута подключения применяется команда:

```
# set system auth radius server <server-ip> timeout <timeout>
# commit
```

где

– <server-ip> – IP-адрес или DNS-имя, которое автоматически трансформируется в IP-адрес;

– <timeout> – число секунд, по умолчанию – 60.

3) Создать учётную запись (достаточно без пароля) и добавить её в список учётных записей, которым разрешена удалённая аутентификации по протоколу RADIUS, с помощью команд:

```
# setup login <account-name>
# set system auth radius allow-login <account-name>
# commit
```

где <account-name> – имя существующей учётной записи.

После выполнения вышеописанных настроек на RADIUS-сервере возможно определение неограниченного количества пользователей и ассоциирование с ними атрибута `Juniper-Local-User-Name` (26.2636.1), содержащего имя учётной записи на узле.

Пользователь, успешно аутентифицированный на RADIUS-сервере, получает доступ к ПАК «Фортикс» со всеми полномочиями согласно настройкам его учётной записи.

Данный механизм работает как при входе с консоли, так и при соединении по протоколам SSH, Telnet и NETCONF.

6 Сетевые интерфейсы

В ПАК «Фортикс» поддерживаются следующие типы сетевых интерфейсов:

– `ether` – интерфейс Ethernet;

– `bond` – интерфейс, объединяющий интерфейсы в один логический;

– `bridge` – интерфейс-сетевой мост;

– `dummy` – интерфейс-»заглушка»;

– `fortun` – туннельный криптографический интерфейс fortun;

– `gre` – туннельный интерфейс gre;

– `ifb` – интерфейс для выполнения QoS;

– `loopback` – интерфейс «петля»;

– `vlan` – интерфейс 802.1Q;

– `vxlan` – туннельный интерфейс VxLAN;

– `wg` – туннельный интерфейс WireGuard.

6.1 Общая настройка

Для определения интерфейса в конфигурации необходимо указать его уникальное имя (строка длиной от 1 до 15 символов), которое выбирается произвольно (исключение: интерфейсы типа `ether`, `loopback`), и тип. Для интерфейсов типа `ether` предусмотрено автоматическое присвоение имени в формате `en<n>`, где `<n>` – число, соответствующее номеру порта маршрутизатора ПАК «Фортикс».

В заводской конфигурации ПАК «Фортикс» настроен один интерфейс `en0` типа `ether` и один интерфейс типа `loopback`:

```
interface {
  ether en0 {
    enable
    ipv4 address 192.168.0.1/24
  }
  loopback lo enable
}
```

Для изменения IP-адреса интерфейса применяются следующие команды:

```
# del interface <interface-type> <interface-name> ipv4|ipv6 address
# set interface <interface-type> <interface-name> ipv4|ipv6 address <address
>
# commit
```

где

– <interface-type> – тип интерфейса;

– <interface-name> – имя интерфейса;

– ipv4|ipv6 – уровень конфигурации IPv4/IPv6;

– <address> – IPv4-адрес в формате A.B.C.D/mask или IPv6-адрес в формате A:B:...:H/mask в зависимости от уровня конфигурации.

Пример применения команд для изменения IP-адреса интерфейса en0 типа ether с 192.168.0.1/24 на 192.168.122.184/24:

```
> configure

# del interface ether en0 ipv4 address
# set interface ether en0 ipv4 address 192.168.122.184/24
# commit
```

Для настройки получения IP-адреса по протоколу DHCP применяются команды:

```
# del interface <interface-type> <interface-name> ipv4|ipv6
# set interface <interface-type> <interface-name> ipv4|ipv6 dhcp
# commit
```

где

– <interface-type> – тип интерфейса;

– <interface-name> – имя интерфейса;

– ipv4|ipv6 – уровень конфигурации IPv4/IPv6.

Пример применения команд для настройки получения IP-адреса интерфейса en0 типа ether по протоколу DHCP:

```
# del interface ether en0 ipv4
# set interface ether en0 ipv4 dhcp
# commit
```

Настройка интерфейсов осуществляется на следующем уровне конфигурации:

```
[edit interface <interface-type> <interface-name>]
```

где

– <interface-type> – тип интерфейса;

– <interface-name> – имя интерфейса.

На данном уровне конфигурации доступны следующие основные настройки интерфейсов (общие для всех типов):

– `description <description>` – задать текстовое описание интерфейса, где`<description>` – строка;

– `enable` – перевести интерфейс в состояние UP (сделать доступным);

– `egress` – перейти на уровень конфигурации выходной дисциплины;

– `ingress` – перейти на уровень конфигурации входной дисциплины;

– `ipv4` – перейти на уровень конфигурации IPv4;

– `ipv6` – перейти на уровень конфигурации IPv6;

– `mac-addr <mac-address>` – задать MAC-адрес, где `<mac-address>` – MAC-адрес в формате `xx:xx:xx:xx:xx:xx`;

– `mtu <mtu-value>` – задать размер MTU, где `<mtu-value>` – число от 1 до 65535;

– `no-arp` – отключить ARP;

– `no-link-detect` – отключить детектирование несущей для управления маршрутами;

– `no-multicast` – отключить мультикаст;

– `promisc` – использовать режим promisc;

– `rps` – использовать принудительное распределение по ядрам процессора на приёме.

6.2 Просмотр состояния интерфейсов

Для просмотра текущего состояния интерфейса и его статистики применяется команда:

```
> show interface <interface-type> <interface-name>
```

где

– `<interface-type>` – тип интерфейса;

– `<interface-name>` – имя интерфейса.

В качестве типа и имени возможно использование символа *, при указании которого подразумеваются все типы или все имена соответственно, например:

– `show interface` (`show interface * *`) – вывести информацию о всех интерфейсах;

– `show interface * en0` – вывести информацию об интерфейсе с именем `en0`;

– `show interface ether *` – вывести информацию о всех интерфейсах типа `ether`;

– `show interface ether en0` – вывести информацию об интерфейсе `en0` типа `ether`.

Для изменения формата вывода или детализации в команде `show` указываются следующие уточняющие параметры:

– `brief` – параметр, при указании которого информация представляется в краткой табличной форме;

– `detail` – параметр, при указании которого информация представляется детализированно;

– `long` – параметр, при указании которого информация представляется в развернутом виде;

– `device` – параметр, при указании которого представляется информация об устройстве;

– `link` – параметр, при указании которого представляется информация о подключении (carrier);

– `qdisc` – параметр, при указании которого представляется информация о дисциплинах обслуживания трафика;

– `stat` – параметр, при указании которого представляется информация о статистике;

– `stat reset` – параметр, при указании которого информация о статистике сбрасывается.

Пример применения команды для просмотра информации о всех интерфейсах в краткой табличной форме:

```
> show interface * * brief
Interface        Status  VRF             Addresses
----------       ------  ---             ---------
en0:             up      default         192.168.122.184/24
lo:              up      default
tun0:            up      default         10.0.0.2/24
```

6.3 Конфигурирование интерфейсов

При выполнении команды `commit` (применении конфигурации-копии *candidate* как текущей конфигурации *running*) осуществляется проверка консистентности конфигурации. В случае проблем консистентности команда `commit` не выполняется и на экран выводится диагностическое сообщение.

П р и м е ч а н и е – Конфигурирование интерфейсов, в общем случае, осуществляется не в момент выполнения команды `commit`, а в фоновом режиме. Например, при настройке интерфейса `bond` указываются подчинённые интерфейсы, которые на момент выполнения команды `commit` могут быть не полностью настроены. В этом случае модуль конфигурации ожидает выполнения всех необходимых условий для применения желаемой конфигурации и только после этого выполняет настройку интерфейса `bond`.

Для просмотра журнала модуля конфигурации применяется команда:

```
> show journal service config
```

Для просмотра ошибок модуля конфигурации применяется команда:

```
> show journal service config priority err
```

6.4 Интерфейс default

В схеме конфигурирования ПАК «Фортикс» определён специальный безымянный интерфейс `default`, который не соответствует никакому реальному или виртуальному интерфейсу. Данный интерфейс предназначен для определения настроек по умолчанию для всех интерфейсов: если какие-либо настройки некоторого интерфейса не заданы явно, используются настройки интерфейса `default`.

Настройка интерфейса `default` осуществляется на следующем уровне конфигурации:

```
[edit interface default]
```

На данном уровне конфигурации доступны следующие настройки:

– `ipv4 accept-local on|off` – разрешить/запретить приём пакетов с адресом отправителя текущей системы;

– `ipv4 accept-redirects on|off` – разрешить/запретить приём (обработку) ICMP-redirect сообщений;

– `ipv4 arp-filter on|off` – разрешить/запретить ответ на ARP-запросы от других интерфейсов;

– `ipv4 proxy-arp on|off` – включить/выключить механизм проксирования ARP-запросов;

– `ipv4 rp-filter loose|none|strict` – использовать механизм проверки адреса источника, где `loose` – параметр, при указании которого адрес источника каждого входящего пакета проверяется на соответствие FIB, и, если адрес источника недоступен через какой-либо интерфейс, пакет отбрасывается, `none` – параметр, при указании которого проверка адреса источника не осуществляется, `strict` – параметр, при указании которого адрес источника каждого входящего пакета проверяется на соответствие FIB, и, если интерфейс не является наилучшим обратным путём, пакет отбрасывается (см. RFC 3704);

– `ipv4 send-redirects on|off` – разрешить/запретить отправку ICMP-redirect сообщений IPv4;

– ipv6 accept-redirects on|off – разрешить/запретить приём (обработку) redirect сообщений IPv6 ;

– ipv6 hop-limit <hop-limit-value> – задать hop-limit для IPv6, где <hop-limit-value> – число от 0 до 255, по умолчанию – 64;

– ipv6 ra – перейти на уровень конфигурации IPv6 RA (объявления маршрутизатора) клиента;

– ipv6 mtu <mtu-value> – задать MTU для IPv6, где <mtu-value> – число от 0 до 65535, по умолчанию – 1280.

Все вышеуказанные настройки могут быть переопределены на каждом интерфейсе и/или заданы на интерфейсе default. При этом больший приоритет имеют явно заданные в конфигурации настройки интерфейса относительно настроек интерфейса default.

Пример применения команды для настройки интерфейса default:

```
# set interface default ipv4 rp-filter none
```

6.5 Интерфейсы типа bond

Настройка интерфейсов типа bond осуществляется на следующем уровне конфигурации:

```
[edit interface bond <bond-name>]
```

где <bond-name> – строка длиной от 1 до 15 символов.

На данном уровне конфигурации доступны следующие обязательные настройки:

– slave <interface-name> – задать подчинённый интерфейс, где <interface-name> – имя существующего интерфейса, возможно определение нескольких настроек данного уровня конфигурации;

– mode <mode-name> – задать режим работы, где <mode-name> принимает одно из значений active-backup, balance-alb, balance-rr, balance-tlb, balance-xor, broadcast, ieee-802.3ad.

На данном уровне конфигурации доступны следующие необязательные настройки:

– monitor <monitor-name> – задать режим мониторинга состояния подчинённых интерфейсов, где <monitor-name> принимает одно из значений arp, mii;

– primary <interface-name> – задать основной подчинённый интерфейс, где <interface-name> – имя существующего интерфейса;

– primary-reselect <primary-reselect-name> – задать режим выбора основного подчинённого интерфейса, где <primary-reselect-name> принимает одно из значений always, better, failure;

– xmit-hash-policy <xmit-hash-policy-name> – задать функцию распределения на подчинённые интерфейсы, где <xmit-hash-policy-name> принимает одно из значений encap2+3, encap3+4, layer2, layer2+3, layer3+4, vlan+srcmac;

– all-slaves-active – использовать режим приёма с неактивных портов.

Пример применения команд для настройки интерфейса типа bond:

```
# edit interface bond bond0
[edit interface bond bond0]
# set slave en0
# set slave en1
# set mode balance-rr
# set enable
# commit
# top
```

6.6 Интерфейсы типа bridge

Настройка интерфейсов типа bridge осуществляется на следующем уровне конфигурации:

```
[edit interface bridge <bridge-name>]
```

где <bridge-name> – строка длиной от 1 до 15 символов.

На данном уровне конфигурации доступны следующие обязательные настройки:

– port <interface-name> – задать порт интерфейса, объединяемого в мост, где <interface-name> – имя существующего интерфейса, возможно определение нескольких настроек данного уровня конфигурации, для каждой из которых указывается:

– cost <cost-value> – «стоимость» порта, где <cost-value> – число от 1 до 65535;

– prio <priority-value> – приоритет порта, где <priority-value> – число от 0 до 63.

На данном уровне конфигурации доступны следующие необязательные настройки:

– stp – использовать STP;

– ageing-time <ageing-time-value> – задать время жизни MAC-адресов в таблицах, где <ageing-time-value> – число секунд от 0.00 до 600.00, по умолчанию – 300;

– forward-delay <forward-delay-value> – задать задержку перед переходом в новое состояние после изменения сетевой топологии, где <forward-delay-value> – число секунд от 0.00 до 60.00, по умолчанию – 15;

– group-fwd lldp|lacp|stp – использовать пересылку LLDP/LACP/STP-кадров;

– hello-time <hello-time-value> – задать интервал между рассылками сообщений Hello протокола STP, где <hello-time-value> – число секунд от 0.00 до 60.00, по умолчанию – 2;

– max-age <max-age-value> – задать максимальное время жизни сообщений протокола STP, где <max-age-value> – число секунд от 0.00 до 120.00, по умолчанию – 20;

– no-conntrack – отключить отслеживание соединений TCP/IP.

Пример применения команд для настройки интерфейса типа bridge:

```
# edit interface bridge br0
[edit interface bridge br0]
# set port en0
# set port en1
# set enable
# commit
# top
```

6.7 Интерфейсы типа dummy

Настройка интерфейсов типа dummy осуществляется на следующем уровне конфигурации:

```
[edit interface dummy <dummy-name>]
```

где <dummy-name> – строка длиной от 1 до 15 символов.

Интерфейсы типа dummy (интерфейсы-заглушки) не имеют специфичных обязательных настроек. В ПАК «Фортикс» возможно создание нескольких интерфейсов данного типа.

6.8 Интерфейсы типа fortun

Использование интерфейсов типа `fortun` (туннелей) в режиме шифрования описано в разделе «СКЗИ». В настоящем подразделе описаны настройки для использования интерфейса данного типа без криптографической защиты.

Настройка интерфейсов типа `fortun` осуществляется на следующем уровне конфигурации:

```
[edit interface fortun <fortun-name>]
```

где `<fortun-name>` – строка длиной от 1 до 15 символов.

На данном уровне конфигурации доступны следующие обязательные настройки:

– `ipv4|ipv6 local <address>` – задать локальный IP-адрес туннеля, где `ipv4|ipv6` – уровень конфигурации IPv4/IPv6, `<address>` – IPv4-адрес в формате `A.B.C.D` или IPv6-адрес в формате `A:B:...:H` в зависимости от уровня конфигурации;

– `ipv4|ipv6 remote <address>` – задать удалённый IP-адрес туннеля, где `ipv4|ipv6` – уровень конфигурации IPv4/IPv6, `<address>` – IPv4-адрес в формате `A.B.C.D` или IPv6-адрес в формате `A:B:...:H` в зависимости от уровня конфигурации;

– `mode tun|tap` – задать режим работы;

– `id <id-value>` – задать идентификатор туннеля, где `<id-value>` – число от 0 до 65535.

На данном уровне конфигурации доступны следующие необязательные настройки:

– `ttl <ttl-value>` – задать TTL, где `<ttl-value>` – число от 0 до 255;

– `tos <hex-value>` – задать TOS, где `<hex-value>` – тип TOS;

– `keepalive` – перейти на уровень конфигурации режима пинг-проб.

Пример применения команд для настройки интерфейса типа `fortun` для использования без криптографической защиты:

```
# edit interface fortun ft0
[edit interface fortun ft0]
# set mode tun
# set id 1
# set ipv4 local 192.168.0.1
# set ipv4 remote 192.168.0.2
# set ipv4 address 10.0.0.1/24
# set enable
# commit
# top
```

6.9 Интерфейсы типа gre

Настройка интерфейсов типа `gre` осуществляется на следующем уровне конфигурации:

```
[edit interface gre <gre-name>]
```

где `<gre-name>` – строка длиной от 1 до 15 символов.

Примечание – Имя интерфейса `gre0` зарезервировано системой и не может быть использовано.

На данном уровне конфигурации доступны следующие обязательные настройки:

– `ipv4|ipv6 local <address>` – задать локальный IP-адрес туннеля, где `ipv4|ipv6` – уровень конфигурации IPv4/IPv6, `<address>` – IPv4-адрес в формате `A.B.C.D` или IPv6-адрес в формате `A:B:...:H` в зависимости от уровня конфигурации;

– `ipv4|ipv6 remote <address>` – задать удалённый IP-адрес туннеля , где `ipv4|ipv6` – уровень конфигурации IPv4/IPv6, `<address>` – IPv4-адрес в формате `A.B.C.D` или IPv6-адрес в формате `A:B:...:H` в зависимости от уровня конфигурации;

– `mode tun|tap` – задать режим работы.

На данном уровне конфигурации доступны следующие необязательные настройки:

– `key <key-value>` – задать ключ, где `<key-value>` – число от 0 до 4294967295;

– `seq` – использовать номера пакетов;

– `csum` – использовать контрольные суммы;

– `ttl <ttl-value>` – задать TTL, где `<ttl-value>` – число от 0 до 255;

– `tos <hex-value>` – задать TOS, где `<hex-value>` – тип TOS;

– `keepalive` – использовать режим пинг-проб.

Пример применения команд для настройки интерфейса типа `gre`:

```
# edit interface gre gre1
[edit interface gre gre1]
# set mode tun
# set ipv4 local 192.168.0.1
# set ipv4 remote 192.168.0.2
# set ipv4 address 10.0.0.1/24
# set enable
# commit
# top
```

6.10 Интерфейсы типа ifb

Настройка интерфейсов типа `ifb` осуществляется на следующем уровне конфигурации:

```
[edit interface ifb <ifb-name>]
```

где `<ifb-name>` – строка длиной от 1 до 15 символов.

Интерфейсы типа `ifb` используются для применения дисциплин QoS (качества обслуживания) на входе. Интерфейсы данного типа не имеют специфичных обязательных настроек. Использование интерфейсов типа `ifb` подробно описано в разделе «Качество обслуживания (QoS)».

6.11 Интерфейс типа loopback

Настройка интерфейсов типа `loopback` осуществляется на следующем уровне конфигурации:

```
[edit interface loopback lo]
```

В ПАК «Фортикс» допустимо создание только одного интерфейса типа `loopback` (с именем `lo`). Интерфейс данного типа имеет предустановленный адрес, даже если он не задан в конфигурации устройства, при этом возможно добавление других адресов.

При назначении интерфейсу данного типа IP-адреса с маской, отличной от `/32`, интерфейс будет отвечать на все адреса из указанной подсети. Например, если для интерфейса типа `loopback` задать IP-адрес 10.0.0.1/24, он будет отвечать на команду `ping` со всех адресов из диапазона с 10.0.0.1 по 10.0.0.254.

П р и м е ч а н и е – Рекомендуется использовать интерфейс типа `dummy` вместо интерфейса типа `loopback`.

6.12 Интерфейсы типа vlan

Настройка интерфейсов типа `vlan` осуществляется на следующем уровне конфигурации:

```
[edit interface vlan <vlan-name>]
```

где `<vlan-name>` – строка длиной от 1 до 15 символов.

На данном уровне конфигурации доступны следующие обязательные настройки:

– `vlan-id <vlan-id-value>` – задать идентификатор VLAN, где `<vlan-id-value>` – число от 1 до 4096;

– `master <master-name>` – задать родительский интерфейс, на основе которого создаётся VLAN, где `<master-name>` – имя существующего интерфейса;

– `proto 802.1Q|802.1ad` – задать протокол поддержки VLAN.

Пример применения команд для настройки интерфейса типа `vlan`:

```
# edit interface vlan vlan0
[edit interface vlan vlan0]
# set vlan-id 1
# set master en0
# set proto 802.1Q
# set enable
# commit
# top
```

6.13 Интерфейсы типа vxlan

Настройка интерфейсов типа `vxlan` осуществляется на следующем уровне конфигурации:

```
[edit interface vxlan <vxlan-name>]
```

где `<vxlan-name>` – строка длиной от 1 до 15 символов.

На данном уровне конфигурации доступны следующие обязательные настройки:

– `vxlan-id <vxlan-id-value>` – задать идентификатор VxLAN, где `<vxlan-id-value>` – число от 0 до 16777215;

– `interface <interface-name>` – задать связанный интерфейс, где `<interface-name>` – имя существующего интерфейса;

– `ipv4|ipv6 remote <address>` – задать удалённый адрес туннеля или мультикаст-группу, где `ipv4|ipv6` – уровень конфигурации IPv4/IPv6, `<address>` – IPv4-адрес в формате `A.B.C.D` или IPv6-адрес в формате `A:B:...:H` в зависимости от уровня конфигурации;

– `encap` – перейти на уровень конфигурации параметров инкапсуляции;

– `ipv4|ipv6 local <address>` – задать локальный адрес туннеля, где `ipv4|ipv6` – уровень конфигурации IPv4/IPv6, `<address>` – IPv4-адрес в формате `A.B.C.D` или IPv6-адрес в формате `A:B:...:H` в зависимости от уровня конфигурации.

На данном уровне конфигурации доступны следующие необязательные настройки:

– dont-fragment – использовать DF-бит;

– ageing-time <ageing-time-value> – задать время жизни записей FDB, где <ageing-time-value> – число секунд от 0 до 600;

– no-learning – не добавлять в FDB неизвестные адреса;

– max-address <max-address-number> – задать максимальное число FDB, где <max-address-number> – число от 0 до 4294967295;

– ttl <ttl-value> – задать TTL, где <ttl-value> – число от 0 до 255;

– tos <hex-value> – задать TOS, где <hex-value> – тип TOS.

Пример применения команд для настройки интерфейса типа vxlan:

```
# edit interface vxlan vx1000
[edit interface vxlan vx1000]
# set ipv4 remote 225.0.0.1
# set interface en0
# set vxlan-id 1000
# set encap dport 4789
# set ipv4 local 192.168.1.1
# set enable
# commit
# top
```

6.14 Интерфейсы типа wg

Интерфейсы типа wg реализуют технологию WireGuard для создания зашифрованных каналов связи. При определении интерфейса данного типа включается настройка локального конца туннеля и одного или более удалённых (peers).

Настройка интерфейсов типа wg осуществляется на следующем уровне конфигурации:

```
[edit interface wg <wg-name>]
```

где <wg-name> – строка длиной от 1 до 15 символов.

На данном уровне конфигурации доступны следующие обязательные настройки:

– key <private-key> – задать закрытый ключ соединения, где <private-key> – значение закрытого ключа/полное имя файла с закрытым ключом или имя файла относительно домашней директории пользователя;

– port <port-number> – задать порт соединения, где <port-number> – число от 1 до 65535.

Настройка удалённого конца туннеля осуществляется на следующем уровне конфигурации:

```
[edit interface wg <wg-name> peer <peer-name>]
```

где

– `<wg-name>` – строка длиной от 1 до 15 символов;

– `<peer-name>` – имя удалённого конца туннеля.

На данном уровне конфигурации доступны следующие настройки:

– `pubkey <public-key>` – задать открытый ключ соединения, где `<public-key>` – значение открытого ключа/полное имя файла с открытым ключом удалённого конца туннеля или имя файла относительно домашней директории пользователя;

– `allowed-ip <network>` – задать подсеть, которой предназначается трафик, где `<network>` – IPv4-адрес в формате `A.B.C.D[/mask]` или IPv6-адрес в формате `A:B:...:H[/mask]`;

– `endpoint addr <address>` – задать IP-адрес, с которого ожидается подключение, где `<address>` – IPv4-адрес в формате `A.B.C.D[/mask]` или IPv6-адрес в формате `A:B:...:H[/mask]`;

– `endpoint port <port-number>` – задать порт, с которого ожидается подключение, где `<port-number>` – число от 1 до 65535;

– `psk <public-key>` – задать дополнительный ключ шифрования для усиления защиты соединения, где `<public-key>` – значение ключа/полное имя файла с ключом или имя файла относительно домашней директории пользователя;

– `keepalive interval <interval-value>` – задать интервал отправки пакетов для проверки активности канала, где `<interval-value>` – число секунд от 0 до 65535.

Пример конфигурации интерфейса типа `wg`:

```
wg wg1 {
  enable
  ipv4 addr 192.168.0.1/24
  peer user {
    allowed-ip 192.168.0.100
    pubkey de1/bde5Yrfv1rtQ3z5QjbaKqetcT+qa5VU+1zLs2qr=
  }
  key ../priv.key
  port 33225
}
```

7 Межсетевой экран

В ПАК «Фортикс» межсетевой экран (далее по тексту МЭ, firewall) обеспечивает фильтрацию трафика, модификацию пакетов и трансляцию адресов (NAT). Все настройки МЭ осуществляются на следующем уровне конфигурации:

```
[edit firewall]
```

7.1 Зонный межсетевой экран

7.1.1 Зоны

Основная единица защиты в зонном firewall — зона, формирование которой осуществляется по следующему принципу: интерфейсы со схожими назначениями объединяются в зоны, и, в зависимости от уровня доверия между ними, выстраиваются соответствующие правила доступа для них. При этом один интерфейс может принадлежать только одной зоне или не принадлежать никакой. Самый простой пример — две зоны, одна из которых для «внешних» интерфейсов, трафику с которых нельзя доверять, вторая — для «внутренних». Кроме того, возможно добавление зоны DMZ для серверов, компрометация которых не должна привести к проникновению во «внутреннюю» зону.

Настройка зон осуществляется на следующем уровне конфигурации:

```
[edit firewall zone <zone-name>]
```

где `<zone-name>` – строка длиной от 1 до 128 символов.

На данном уровне конфигурации доступны следующие настройки:

– `drop-policy to-zone|from-zone|both` – указать блокируемые соединения, где `to-zone` – входящие соединения от других зон или интерфейсов, не принадлежащих ни одной зоне, `from-zone` – исходящие соединения, `both` – входящие и исходящие соединения;

– `interface <interface-name>` – указать интерфейс, водящий в зону, где `<interface-name>` – имя существующего интерфейса.

Настройка `drop-policy` применяется для базовой настройки доступа в зонах и обладает наименьшими привилегиями. Данная настройка не оказывает никакого влияния на трафик, проходящий внутри зоны.

Пример конфигурации зон:

```
firewall {
  zone lan {
    interface en2
    interface en3
    drop-policy to-zone
  }
  zone wan {
    interface en0
    drop-policy from-zone
  }
  zone dmz {
    interface en1
    drop-policy from-zone
  }
}
```

В данном примере заданы три зоны (`lan`, `wan`, `dmz`), между которыми распределены интерфейсы `en0`,`en1`,`en2`,`en3`, определены базовые ограничения настройкой `drop-policy`. Таблица 3 отображает, какие соединения разрешены в зонах, а какие запрещены (в строках указаны интерфейсы, на которые приходит первый пакет соединения, в столбцах — через которые он отсылается согласно таблице маршрутизации).

Т а б л и ц а 3 – Пример настройки зон

Интерфейс	en0	en1	en2	en3	local
en0	+ (self)	- (from wan)	- (from wan, to lan)	- (from wan, to lan)	- (from wan)
en1	- (from dmz)	+ (self)	- (from dmz, to lan)	- (from dmz, to lan)	- (from dmz)
en2	+	+	+ (self)	+ (self)	+
en3	+	+	+ (self)	+ (self)	+
local	+	+	- (to lan)	- (to lan)	+ (self)

Символом «+» отмечен трафик, который пропускается настройками `drop-policy` (в скобках указано `self`, если трафик проходит внутри одной зоны и не может быть ограничен настройками `drop-policy`). Символом «-» отмечен трафик, который блокируется (в скобках указано, каким именно правилом: например, запись `from wan` означает, что трафик заблокирован настройкой `drop-policy from-zone` зоны `wan`, `to lan` — `drop-policy to-zone` зоны `lan`).

Для управления трафиком, источником или получателем которого является ПАК «Фортикс», применяется специальная псевдозона `local` (в таблице обозначена как интерфейс

local). К трафику данной зоны неприменимы настройки drop-policy, для его фильтрации применяются политики (см. подпункт «Политики»).

7.1.2 Фильтры

Для более точного отбора трафика в зонном firewall используются фильтры, которые объединяются в политики (см. подпункт «Политики»). Фильтр зонного firewall состоит из списка правил (rule), по которым осуществляется отбор трафика. Каждое правило из списка состоит из критериев отбора и действия action, которое применяется в случае выполнения критериев. При формировании списка правил важен порядок их указания в конфигурации: чем раньше указано правило в конфигурации (чем выше правило в списке), тем оно приоритетнее. Первый пакет соединения проходит по очереди через все правила до тех пор, пока не попадёт в первое, соответствующее ему и имеющее действие action, отличное от отключающего применение правила (disabled). Фильтры применяются отдельно к IPv4- и IPv6-трафику.

Настройка фильтров осуществляется на следующем уровне конфигурации:

```
[edit firewall ipv4|ipv6 filter <filter-name>]
```

где

– ipv4|ipv6 – уровень конфигурации IPv4/IPv6;

– <filter-name> – строка длиной от 1 до 128 символов.

На данном уровне конфигурации доступны следующие настройки:

– description <description> – указать описание фильтра, где <description> – строка;

– rule <rule-name> – указать правило, соответствующее данному фильтру, где <rule-name> – имя правила (см. ниже).

Настройка правил фильтра осуществляется на следующем уровне конфигурации:

```
[edit firewall ipv4|ipv6 filter <filter-name> rule <rule-name>]
```

где

– ipv4|ipv6 – уровень конфигурации IPv4/IPv6;

– <filter-name> – строка длиной от 1 до 128 символов;

– <rule-name> – строка длиной от 1 до 128 символов.

На данном уровне конфигурации доступны следующие настройки:

– `description <description>` – указать описание правила, где `<description>` – строка;

– `from address <address>|file-list <file-list-name>|network <network-name>` – (критерий отбора) указать адрес(а) источника, по которому(ым) осуществляется отбор трафика, где `<address>` – IPv4-адрес в формате `A.B.C.D[/mask]` или IPv6-адрес в формате `A:B:..:H[/mask]` в зависимости от уровня конфигурации, `<network-name>` – имя существующего списка сетей, `<file-list-name>` – имя существующего файла списка сетей (см. подпункт «Списки сетей и сервисы»);

– `to address <address>|file-list <file-list-name>|network <network-name>` – (критерий отбора) указать адрес(а) назначения, по которому(ым) осуществляется отбор трафика, где `<address>` – IPv4-адрес в формате `A.B.C.D[/mask]` или IPv6-адрес в формате `A:B:..:H[/mask]` в зависимости от уровня конфигурации, `<network-name>` – имя существующего списка сетей, `<file-list-name>` – имя файла существующего списка сетей (см. подпункт «Списки сетей и сервисы»);

– `from-port <port>` – (критерий отбора) указать исходящий порт, по которому осуществляется отбор трафика, где `<port>` – строка в формате `tcp|udp n[-m]` (`n`, `m` – числа от 1 до 65535) или имя существующего списка портов (см. подпункт «Списки сетей и сервисы»);

– `to-port <port>` – (критерий отбора) указать входящий порт, по которому осуществляется отбор трафика, где `<port>` – строка в формате `tcp|udp n[-m]` (`n`, `m` – числа от 1 до 65535) или имя существующего списка портов (см. подпункт «Списки сетей и сервисы»);

– `from-interface <interface-name>` – (критерий отбора) указать интерфейс источника, по которому осуществляется отбор трафика, где `<interface-name>` – имя существующего интерфейса;

– `to-interface <interface-name>` – (критерий отбора) указать интерфейс назначения, по которому осуществляется отбор трафика, где `<interface-name>` – имя существующего интерфейса;

– `dscp [value <value-dscp>] [mask <mask-dscp>]` – (критерий отбора) указать значения поля dscp, по которым осуществляется отбор трафика, где `<value-dscp>` – hex-значение `0x00..0x3f` или одно из представленных в командной строке стандартных значений, `<mask-dscp>` – hex-значение `0x00..0x3f` или одно из представленных в командной строке стандартных значений;

– protonum <protocol-number> – (критерий отбора) указать номер протокола, по которому осуществляется отбор трафика, где <protocol-number> – число от 0 до 255;

– tcp|udp|icmp (для IPv4-трафика) – (критерий отбора) указать протокол, по которому осуществляется отбор трафика, и перейти на уровень конфигурации протокола (не может быть задано вместе с настройкой protonum);

– tcp|udp|icmpv6 (для IPv6-трафика) – (критерий отбора) указать протокол, по которому осуществляется отбор трафика, и перейти на уровень конфигурации протокола (не может быть задано вместе с настройкой protonum);

– timestart <timestart-value> – (критерий отбора) указать начальное время выполнения правила, где <timestart-value> – строка в формате HH:MM[:SS];

– timestop <timestop-value> – (критерий отбора) указать конечное время выполнения правила, где <timestop-value> – строка в формате HH:MM[:SS];

– datestart <datestart-value> – (критерий отбора) указать начальную дату (и время) выполнения правила, где <datestart-value> – строка в формате YYYY-MM-DD[THH:MM[:SS]], по умолчанию – 00:00:00;

– datestop <datestop-value> – (критерий отбора) указать конечную дату (и время) выполнения правила, где <datestop-value> – строка в формате YYYY-MM-DD[THH:MM[:SS]], по умолчанию – 00:00:00);

– connlimit <limit> – (критерий отбора) указать максимальное число активных соединений, попадающих под критерии отбора, для которых выполняется правило, где <limit> – число от 0 до 4294967295;

– log – перейти на уровень конфигурации журналирования пакетов (см. подраздел «Журналирование пакетов»);

– counter <counter-name> – указать счётчик срабатывания правила, где <counter-name> – имя счётчика (см. пункт «Счётчики»);

– action <action> – указать действие, применяемое при выполнении критериев отбора, где <action> – строка (см. ниже).

Предусмотрены следующие действия для настройки action:

– disabled — отключить применение правила (применяется для временного отключения правила, например, если необходимо временно предоставить доступ к некоторому ресурсу);

– accept — разрешить соединение и прекратить его дальнейшую проверку зонным firewall;

– drop — запретить соединение без отправки ICMP-уведомления;

– `reject` — запретить соединение с отправкой источнику ICMP-уведомления (ICMPv6-уведомления для IPv6) `port-unreachable`;

– `return` — прекратить обработку пакета в данном фильтре (в таком случае соединение обрабатывается настройкой `default-action` политики (см. подпункт «Политики») или настройкой `drop-policy`).

7.1.2.1 Списки сетей и сервисы

Для указания нескольких адресов источника или назначения возможно использование списков сетей.

Настройка списков сетей осуществляется на следующем уровне конфигурации:

```
[edit firewall ipv4|ipv6 network <network-name>]
```

где

– `ipv4|ipv6` – уровень конфигурации IPv4/IPv6;

– `<network-name>` – строка длиной от 1 до 128 символов.

На данном уровне конфигурации доступны следующие настройки:

– `description <description>` – указать описание списка сетей, где `<description>` – строка;

– `address <address>` – указать адрес, входящий в данный список сетей, где `<address>` – IPv4-адрес в формате `A.B.C.D[/mask]` или IPv6-адрес в формате `A:B:..:H[/mask]` в зависимости от уровня конфигурации;

– `network <network-name>` – указать существующий список сетей, содержимое которого включается в данный список, где `<network-name>` – имя существующего списка сетей.

Пример конфигурации списка сетей:

```
firewall {
  ipv4 {
    network blocklist-common {
      address 1.1.1.0/24
      address 3.3.0.0/16
      address 7.8.1.2
    }
    network blocklist-lan {
      network blocklist-common
      address 4.4.4.4
    }
```

```
  }
}
```

Возможно хранение списка сетей в файле. Настройка файла списка сетей осуществляется на следующем уровне конфигурации:

```
[edit firewall ipv4|ipv6 file-list <file-list-name>]
```

где

– ipv4|ipv6 – уровень конфигурации IPv4/IPv6;

– <file-list-name> – строка длиной от 1 до 128 символов.

На данном уровне конфигурации доступны следующие настройки:

– description <description> – указать описание файла списка сетей, где <description> – строка;

– path <file-path> – указать путь к файлу списка сетей, где <file-path> – полное имя файла.

Каждая запись файла списка сетей начинается с новой строки и может являться:

– IP-адресом (например, 192.168.1.1);

– сетью (например, 192.168.0.0/24);

– диапазоном (например, 192.168.0.100-192.168.0.200).

Пример конфигурации файла списка сетей:

```
firewall {
  ipv4 {
    file-list geoip-RU path /share/list-RU.nft
  }
}
```

При выполнении команды commit после настройки файла списка сетей его содержимое считывается и преобразовывается в список сетей geoip-RU.

Для обновления списка сетей, полученного из файла списка сетей, без перезагрузки подсистемы firewall применяется команда:

```
> firewall update file-list ipv4|ipv6 <file-list-name>
```

где

– ipv4|ipv6 – уровень конфигурации IPv4/IPv6;

– <file-list-name> – псевдоним файла списка сетей в конфигурации.

Пример применения команды для обновления списка сетей, полученного из файла /share/list-RU.nft:

```
> firewall update file-list ipv4 geoip-RU
```

Для указания нескольких входящих и исходящих портов возможно использование списков портов (сервисов).

Настройка сервисов осуществляется на следующем уровне конфигурации:

```
[edit firewall service <service-name>]
```

где <service-name> – строка длиной от 1 до 128 символов.

На данном уровне конфигурации доступны следующие настройки:

– description <description> – указать описание сервиса, где <description> – строка;

– tcp <port-number> – указать TCP-порт(ы), входящий(ие) в данный сервис, где <port-number> – строка в формате n[-m] (n, m – числа от 1 до 65535);

– udp <port-number> – указать UDP-порт(ы), входящий(ие) в данный сервис, где <port-number> – строка в формате n[-m] (n, m – числа от 1 до 65535);

– service <service-name> – указать существующий сервис, содержимое которого включается в данный сервис, где <service-name> – имя существующего сервиса.

Пример конфигурации сервиса:

```
firewall {
  service http {
    tcp 80
    tcp 443
  }
}
```

7.1.2.2 Пример

Пример конфигурации фильтров:

```
firewall {
  ipv4 {
    filter allow-http {
      rule 1 {
        to-port service http
        to address 192.168.130.4
        action accept
      }
```

```
    }
    filter blocklist-common {
      rule 1 {
        to network blocklist-common
        action drop
      }
    }
    filter blocklist-lan {
      rule 1 {
        to network blocklist-lan
        action drop
      }
    }
    filter allow-admin {
      rule 1 {
        from address 192.168.2.87
        action accept
      }
    }
  }
}
```

7.1.3 Счётчики

Для отслеживания количества срабатываний правила фильтра используются счётчики `counter`.

Важно! В случае зонного firewall счётчик увеличивается только при срабатывания на первые пакеты соединений, т.к. зонный firewall применим только для них.

Для создания счётчика применяется команда:

```
[edit firewall ipv4|ipv6 filter <filter-name> rule <rule-name>]
# set counter <counter-name>
```

где

– `ipv4|ipv6` – уровень конфигурации IPv4/IPv6;

– `<filter-name>` – строка длиной от й ;

– `<rule-name>` – строка длиной от 1 до 128 символов;

– `<counter-name>` – строка длиной от 1 до 128 символов.

Пример конфигурации счётчиков:

```
firewall {
  ipv4 {
    filter blocklist-common {
```

```
      rule 1 {
        counter cnt-blocklist
      }
    }
    filter blocklist-lan {
      rule 1 {
        counter cnt-blocklist
      }
    }
    filter allow-admin {
      rule 1 {
        counter cnt-allow-admin
      }
    }
  }
}
```

Для просмотра значения счётчиков применяется команда:

```
> show firewall counter ipv4|ipv6 <counter-name>
```

где

– `ipv4|ipv6` – уровень конфигурации IPv4/IPv6;

– `<counter-name>` – имя существующего счётчика.

Пример применения команды для просмотра значения счётчика:

```
> show firewall counter ipv4 cnt-blocklist
```

Для просмотра всех загруженных в ядро правил применяется команда:

```
> show firewall raw
```

Важно!

1) Если в нескольких правилах задано одно и то же имя счётчика, создаётся один счётчик, который вычисляет сумму всех срабатываний правил, в которых он используется.

2) Счётчики с одинаковыми именами, заданные в разных подсистемах (ipv4/ipv6/bridge), различны. Каждый счётчик относится только к одной подсистеме.

3) После выполнения команды `commit` счётчики сбрасываются.

7.1.3.1 Политики

Политики зонного firewall определяют настройки доступа для соединений одного направления между двумя зонами. Каждая политика содержит фильтры (см. пункт «Фильтры») и (опционально) действие по умолчанию `default-action`, которое выполняется в случае

неприменимости фильтров. Возможно определение политики для соединения из зоны в саму себя, применяемой для трафика между интерфейсами одной зоны.

Настройка политик осуществляется на следующем уровне конфигурации:

```
[edit firewall ipv4|ipv6 policy <from-zone-name> to <to-zone-name>]
```

где

– `ipv4|ipv6` – уровень конфигурации IPv4/IPv6;

– `<from-zone-name>` – имя существующей зоны, из которой осуществляется соединение;

– `<to-zone-name>` – имя существующей зоны, в которую осуществляется соединение.

На данном уровне конфигурации доступны следующие настройки:

– `filter <filter-name>` – указать имя фильтра, относящегося к данной политике, где `<filter-name>` – имя существующего фильтра, возможно указание нескольких настроек данного уровня конфигурации;

– `default-action <action>` – указать действие по умолчанию для политики, если ни один фильтр политики неприменим, где `<action>` – строка (см. ниже).

Предусмотрены следующие действия по умолчанию `<action>` для настройки `default-action <action>`:

– `accept` – разрешить соединение и прекратить его дальнейшую проверку зонным firewall;

– `disabled` – отключить применение политики;

– `drop` – запретить соединение без отправки ICMP-уведомления;

– `reject` – запретить соединение с отправкой источнику ICMP-уведомления (ICMPv6-уведомления для IPv6) `port-unreachable`.

Пример конфигурации политик:

```
firewall {
  ipv4 {
    policy dmz to wan {
      default-action accept
      filter blocklist-common
    }
    policy wan to dmz filter allow-http
    policy lan to dmz filter allow-http
    policy lan to wan {
      filter blocklist-lan
    }
    policy local to wan {
      filter blocklist-common
```

```
    }
    policy lan to local {
      default-action drop
      filter allow-admin
    }
  }
}
```

7.1.4 Алгоритм отбора трафика

1) Если к соединению применимы правила фильтров, выполняется действие `action` первого из применимых правила фильтра. Дальнейший отбор трафика не осуществляется.

2) Если к соединению не применим ни один фильтр, но применимы политики, применяется `default-action` первой из применимых политики. Дальнейший отбор трафика не осуществляется.

3) Если к соединению не применимы ни фильтры, ни политики, применяются настройки `drop-policy`.

7.1.5 Пример настройки зонного межсетевого экрана

Объединённая из примеров выше конфигурация зонного firewall:

```
firewall {
  service http {
    tcp 80
    tcp 443
  }
  zone lan {
    interface en2
    interface en3
    drop-policy to-zone
  }
  zone wan {
    interface en0
    drop-policy from-zone
  }
  zone dmz {
    interface en1
    drop-policy from-zone
  }
  ipv4 {
    network blocklist-common {
      address 1.1.1.0/24
      address 3.3.0.0/16
      address 7.8.1.2
```

```
}
network blocklist-lan {
  network blocklist-common
  address 4.4.4.4
}
policy dmz to wan {
  default-action accept
  filter blocklist-common
}
policy wan to dmz filter allow-http
policy lan to dmz filter allow-http
policy lan to wan {
  filter blocklist-lan
}
policy local to wan {
  filter blocklist-common
}
policy lan to local {
  default-action drop
  filter allow-admin
}
filter allow-http {
  rule 1 {
    to-port service http
    to address 192.168.130.4
    action accept
  }
}
filter blocklist-common {
  rule 1 {
    counter cnt-blocklist
    to network blocklist-common
    action drop
  }
}
filter blocklist-lan {
  rule 1 {
    counter cnt-blocklist
    to network blocklist-lan
    action drop
  }
}
filter allow-admin {
  rule 1 {
    counter cnt-allow-admin
    from address 192.168.2.87
    action accept
  }
}
```

```
    }
}
```

В данном примере:

– созданы четыре фильтра, каждый из которых состоит из одного правила:

– фильтры `blocklist-common` и `blocklist-lan` блокируют соединения к сетям из списков сетей;

– фильтр `allow-http` разрешает соединения к web-серверу;

– фильтр `allow-admit` разрешает соединения от источника с адресом 192.168.2.87;

– разрешён трафик из зоны `dmz` в зону `wan`;

– разрешён доступ к web-серверу, расположенному в зоне `dmz`, из остальных зон;

– добавлены два списка блокировки трафика в зоне `wan`:

– для зоны `lan`;

– для зон `lan`, `dmz` и псевдозоны `local`;

– разрешён доступ к самому маршрутизатору только для администратора из зоны `lan`.

Настройки `drop-policy` данного примера подробно описаны в Таблице 3.

7.2 Трансляция адресов (NAT)

Механизм NAT применяется для преобразования адресов и портов проходящих пакетов. Предусмотрены замены двух типов:

– SNAT (замена адреса источника);

– DNAT (замена адреса назначения).

При этом замена осуществляется только в первом пакете соединения. После прохождения первого пакета для соединения создаётся специальная ассоциация, которая, в зависимости от направления, заменяет адрес назначения или источника. Например, если у первого пакета заменён адрес назначения при помощи механизма DNAT, у ответного пакета заменяется адрес источника.

Настройка NAT осуществляется на следующем уровне конфигурации:

```
[edit firewall ipv4|ipv6 nat]
```

где `ipv4|ipv6` – уровень конфигурации IPv4/IPv6.

7.2.1 SNAT (замена адреса источника)

Механизм SNAT представляет собой набор правил, который применяется к трафику из выходного интерфейса или выходной зоны.

Настройка механизма SNAT осуществляется на следующем уровне конфигурации:

```
[edit firewall ipv4|ipv6 nat source]
```

где ipv4|ipv6 – уровень конфигурации IPv4/IPv6.

На данном уровне конфигурации доступны следующие настройки:

– ruleset <ruleset-name> – указать набор правил, применяемый к механизму SNAT, где <ruleset-name> – имя набора правил (см. ниже).

Настройка наборов правил осуществляется на следующем уровне конфигурации:

```
[edit firewall ipv4|ipv6 nat source ruleset <ruleset-name>]
```

где

– ipv4|ipv6 – уровень конфигурации IPv4/IPv6;

– <ruleset-name> – строка длиной от 1 до 128 символов.

На данном уровне конфигурации доступны следующие настройки:

– to-interface <to-interface-name> – указать выходной интерфейс, к которому применяется набор правил, где <to-interface-name> – имя существующего интерфейса;

– to-zone <to-zone-name> – указать выходную зону, к которой применяется набор правил, где <to-zone-name> – имя существующей зоны;

– rule <rule-name> – указать правило, входящее в набор правил, где <rule-name> – имя правила (см. ниже).

Настройка правил осуществляется на следующем уровне конфигурации:

```
[edit firewall ipv4|ipv6 nat source ruleset <ruleset-name> rule <rule-name>]
```

где

– ipv4|ipv6 – уровень конфигурации IPv4/IPv6;

– <ruleset-name> – строка длиной от 1 до 128 символов;

– <rule-name> – строка длиной от 1 до 128 символов.

На данном уровне конфигурации доступны следующие настройки:

– `log` – перейти на уровень конфигурации журналирования пакетов (см. подраздел «Журналирование пакетов»);

– `from address <address>|file-list <file-list-name>|network <network-name>` – (критерий отбора) указать адрес(а) источника, по которому(ым) осуществляется отбор трафика, где `<address>` – IPv4-адрес в формате `A.B.C.D[/mask]` или IPv6-адрес в формате `A:B:..:H[/mask]` в зависимости от уровня конфигурации, `<network-name>` – имя существующего списка сетей, `<file-list-name>` – имя существующего файла списка сетей (см. подпункт «Списки сетей и сервисы»);

– `to address <address>|file-list <file-list-name>|network <network-name>` – (критерий отбора) указать адрес(а) назначения, по которому(ым) осуществляется отбор трафика, где `<address>` – IPv4-адрес в формате `A.B.C.D[/mask]` или IPv6-адрес в формате `A:B:..:H[/mask]` в зависимости от уровня конфигурации, `<network-name>` – имя существующего списка сетей, `<file-list-name>` – имя существующего файла списка сетей (см. подпункт «Списки сетей и сервисы»);

– `from-port <port>` – (критерий отбора) указать исходящий порт, по которому осуществляется отбор трафика, где `<port>` – строка в формате `tcp|udp n[-m]` (`n`, `m` – число от 1 до 65535) или имя существующего списка портов (см. подпункт «Списки сетей и сервисы»);

– `to-port <port>` – (критерий отбора) указать входящий порт, по которому осуществляется отбор трафика, где `<port>` – строка в формате `tcp|udp n[-m]` (`n`, `m` – число от 1 до 65535) или имя существующего списка портов (см. подпункт «Списки сетей и сервисы»);

– `from-interface <interface-name>` – (критерий отбора) указать интерфейс источника, по которому осуществляется отбор трафика, где `<interface-name>` – имя существующего интерфейса;

– `to-interface <interface-name>` – (критерий отбора) указать интерфейс назначения, по которому осуществляется отбор трафика, где `<interface-name>` – имя существующего интерфейса;

– `snat-ip <address>` – изменить адрес источника на известный заранее, где `<address>` – IPv4-адрес в формате `A.B.C.D[/mask]` или IPv6-адрес в формате `A:B:..:H[/mask]` в зависимости от уровня конфигурации;

– `snat-netmap <address>` – отобразить в указанную подсеть, причём младшая часть адреса остается неизменной (например, настройка `snat-natmap 10.3.0.0/16` приведёт к замене адреса `192.168.85.132` на `10.3.85.132`), где `<address>` – IPv4-адрес в формате

A.B.C.D[/mask] или IPv6-адрес в формате A:B:..:H[/mask] в зависимости от уровня конфигурации;

– snat-masquerade – изменить адрес источника на адрес выходного интерфейса;

– snat-port <port-number> – (в комбинации с snat-ip, snat-masquerade или snat-netmap) изменить порт источника, где <port-number> – число от 1 до 65535;

– return — прекратить обработку пакета в данном фильтре (в данном случае соединение обрабатывается настройкой default-action политики (см. подпункт «Политики») или настройкой drop-policy).

Пример конфигурации механизма SNAT для дополнения примера подраздела «Зонный межсетевой экран»:

```
firewall {
  ipv4 {
    nat {
      source {
        ruleset out {
          to-zone wan
          rule 1 {
            snat-masquerade
          }
        }
      }
    }
  }
}
```

В данном примере для доступа в зону wan отображаются адреса источника пакетов на адрес выходного интерфейса.

7.2.2 DNAT (замена адреса назначения)

Механизм DNAT аналогичен SNAT, но заменяет адрес назначения, а не источника.

Настройка механизма DNAT осуществляется на следующем уровне конфигурации:

```
[edit firewall ipv4|ipv6 nat destination]
```

где ipv4|ipv6 – уровень конфигурации IPv4/IPv6.

На данном уровне конфигурации доступны следующие настройки:

– ruleset <ruleset-name> – указать набор правил, применяемый к механизму DNAT, где <ruleset-name> – имя набора правил (см. ниже).

Настройка набора правил осуществляется на следующем уровне конфигурации:

```
[edit firewall ipv4|ipv6 nat destination ruleset <ruleset-name>]
```

где

– ipv4|ipv6 – уровень конфигурации IPv4/IPv6;

– <ruleset-name> – строка длиной от 1 до 128 символов.

На данном уровне конфигурации доступны следующие настройки:

– from-interface <from-interface-name> – указать входной интерфейс, к которому относится набор правил, где <from-interface-name> – имя существующего интерфейса;

– from-zone <from-zone-name> – указать входную зону, к которой относится набор правил, где <from-zone-name> – имя существующей зоны;

– rule <rule-name> – указать правило, входящее в набор, где <rule-name> – имя правила (см. ниже).

Настройка правил осуществляется на следующем уровне конфигурации:

```
[edit firewall ipv4|ipv6 nat source ruleset <ruleset-name> rule <rule-name>]
```

где

– ipv4|ipv6 – уровень конфигурации IPv4/IPv6;

– <ruleset-name> – имя набора правил (строка длиной от 1 до 128 символов);

– <rule-name> – имя правила (строка длиной от 1 до 128 символов).

На данном уровне конфигурации доступны следующие настройки:

– log – перейти на уровень конфигурации журналирования пакетов;

– from address <address>|file-list <file-list-name>|network <network-name> – (критерий отбора) указать адрес(а) источника, по которому(ым) осуществляется отбор трафика, где <address> – IPv4-адрес в формате A.B.C.D[/mask] или IPv6-адрес в формате A:B::..:H[/mask] в зависимости от уровня конфигурации, <network-name> – имя существующего списка сетей, <file-list-name> – имя существующего файла списка сетей (см. подпункт «Списки сетей и сервисы»);

– to address <address>|file-list <file-list-name>|network <network-name> – (критерий отбора) указать адрес(а) назначения, по которому(ым) осуществляется отбор трафика, где <address> – IPv4-адрес в формате A.B.C.D[/mask] или IPv6-адрес в формате A:B::..:H[/mask] в зависимости от уровня конфигурации, <network-name> – имя

существующего списка сетей, <file-list-name> – имя существующего файла списка сетей (см. подпункт «Списки сетей и сервисы»);

– from-port <port> – (критерий отбора) указать исходящий порт, по которому осуществляется отбор трафика, где <port> – строка в формате tcp|udp n[-m] (n, m – число от 1 до 65535) или имя существующего списка портов (см. подпункт «Списки сетей и сервисы»);

– to-port <port> – (критерий отбора) указать входящий порт, по которому осуществляется отбор трафика, где <port> – строка в формате tcp|udp n[-m] (n, m – число от 1 до 65535) или имя существующего списка портов (см. подпункт «Списки сетей и сервисы»);

– from-interface <interface-name> – (критерий отбора) указать интерфейс источника, по которому осуществляется отбор трафика, где <interface-name> – имя существующего интерфейса;

– to-interface <interface-name> – (критерий отбора) указать интерфейс назначения, по которому осуществляется отбор трафика, где <interface-name> – имя существующего интерфейса;

– dnat-ip <address> – изменить адрес назначения на известный заранее, где <address> – IPv4-адрес в формате A.B.C.D[/mask] или IPv6-адрес в формате A:B:..:H[/mask] в зависимости от уровня конфигурации;

– dnat-netmap <address> – отобразить в указанную подсеть, причём младшая часть адреса остаётся неизменной (например, настройка dnat-natmap 10.3.0.0/16 приведёт к замене адреса 192.168.85.132 на 10.3.85.132), где <address> – IPv4-адрес в формате A.B.C.D[/mask] или IPv6-адрес в формате A:B:..:H[/mask] в зависимости от уровня конфигурации;

– dnat-masquerade – изменить адрес назначения на адрес входного интерфейса (перенаправить трафик в зону local);

– dnat-port <port-number> – (в комбинации с dnat-ip, dnat-masquerade или dnat-netmap) изменить порт назначения, где <port-number> – число от 1 до 65535;

– return — прекратить обработку пакета в данном фильтре (в данном случае соединение обрабатывается настройкой default-action политики (см. подпункт «Политики») или настройкой drop-policy).

Пример конфигурации DNAT:

```
firewall {
  ipv4 {
    nat {
      destination {
```

```
        ruleset in {
          from-zone wan
          rule 1 {
            to-port service http
            dnat-ip 192.168.130.4
          }
        }
      }
    }
  }
}
```

В примере подраздела «Зонный межсетевой экран» адрес HTTP-сервера — `192.168.130.4`, при этом по данному адресу сервер не доступен из зоны `wan`. После применения данной конфигурации все соединения на порты 80 и 443 (см. `service http` в подпункте «Списки сетей и сервисы») перенаправляются на HTTP-сервер.

7.3 Основной межсетевой экран (Netfilter)

Основной межсетевой экран `netfilter` позволяет работать попакетно и модифицировать пакеты. Подсистема `netfilter` работает независимо от зонного firewall, то есть, если пакет принят в одном из firewall, он может быть отброшен в другом.

Настройка основного МЭ осуществляется на следующем уровне конфигурации:

```
[edit firewall ipv4|ipv6 netfilter]
```

где `ipv4|ipv6` – уровень конфигурации IPv4/IPv6.

На данном уровне конфигурации доступны следующие настройки:

– `application <application-name>` – задать имя списка приложений, где `<application-name>` – строка длиной от 1 до 128 символов (см. пункт «nDPI»);

– `filter <filter-name>` – перейти на уровень конфигурации фильтра основного МЭ, где `<filter-name>` – строка длиной от 1 до 128 символов (см. ниже);

– `forward` – (цепочка применения фильтра) применить фильтр к пакетам, передаваемым от одного интерфейса к другому;

– `local-in` – (цепочка применения фильтра) применить фильтр к пакетам, передаваемым на ПАК «Фортикс»;

– `local-out` – (цепочка применения фильтра) применить фильтр к пакетам, передаваемым с ПАК «Фортикс»;

– prerouting – (цепочка применения фильтра) применить фильтр к входящим пакетам до их маршрутизации;

– postrouting – (цепочка применения фильтра) применить фильтр к выходящим пакетам.

Для каждой цепочки указывается точка перехвата (хук) согласно следующему списку:

– fragged — точка перехвата до дефрагментации пакета;

– raw — точка перехвата до работы conntrack;

– mangle — основная точка перехвата, в которой предполагается большая часть работы с пакетами;

– after-zone — точка перехвата после работы зонного firewall;

– after-nat — точка перехвата после работы NAT.

При этом точка перехвата fragged доступна только в цепочке prerouting, raw — только в цепочках prerouting и local-out. Критерий отбора state недоступен на данных точках перехвата, так как на этапе применения точек перехвата модуль conntrack ещё не соотнёс пакеты с какими-либо соединениями.

Для применения фильтра к точке перехвата используется команда:

```
[edit firewall ipv4|ipv6 netfilter]
# set <chain-name> <hook-name> filter <filter-name>
```

где

– ipv4|ipv6 – уровень конфигурации IPv4/IPv6;

– <chain-name> – цепочка применения фильтра (см. выше);

– <hook-name> – точка перехвата (см. выше);

– <filter-name> – имя существующего фильтра.

Данная настройка является обязательной для использования фильтра основного firewall. Фильтр проходит через все точки перехвата, к которым данный фильтр применен.

Пример конфигурации применённого к точке перехвата фильтра:

```
firewall {
  ipv4 {
    netfilter {
      prerouting mangle filter in-filter
    }
  }
}
```

7.3.1 Фильтры

Настройка фильтров основного МЭ осуществляется на следующем уровне конфигурации:

```
[edit firewall ipv4|ipv6 netfilter filter <filter-name>]
```

где

– `ipv4|ipv6` – уровень конфигурации IPv4/IPv6;

– `<filter-name>` – строка длиной от 1 до 128 символов.

На данном уровне конфигурации доступны следующие настройки:

– `description <description>` – указать описание фильтра, где `<description>` – строка;

– `limit <limit-name>` – перейти на уровень конфигурации ограничений на число срабатываний правила, где `<limit-name>` – имя существующего ограничения (см. подпункт «Ограничения на количество срабатываний»);

– `rule <rule-name>` – указать правило, принадлежащее данному фильтру, где `<rule-name>` – имя правила (см. ниже).

7.3.1.1 Правила фильтра основного межсетевого экрана

Настройка правил фильтров основного межсетевого экрана `netfilter` осуществляется на следующем уровне конфигурации:

```
[edit firewall ipv4|ipv6 netfilter filter <filter-name> rule <rule-name>]
```

где

– `ipv4|ipv6` – уровень конфигурации IPv4/IPv6;

– `<filter-name>` – строка длиной от 1 до 128 символов;

– `<rule-name>` – строка длиной от 1 до 128 символов.

Критерии отбора зонного межсетевого экрана также применимы для основного МЭ. Предусмотрены следующие дополнительные критерии отбора для основного МЭ (по сравнению с зонным МЭ):

– `content <layer> offset <offset>` – перейти на уровень конфигурации критерия отбора по содержимому (см. подпункт «Фильтрация по содержимому»);

– `dont-fragment true|false` (только для ipv4) – указать значение флага don't fragment, по которому осуществляется отбор, где `true` – флаг установлен, `false` – флаг не установлен;

– more-fragment true|false (только для ipv4) – указать значение флага more fragment, по которому осуществляется отбор, где true – флаг установлен, false – флаг не установлен;

– length [min <length-value>] [max <length-value>] – указать ограничения на длину пакетов, по которым осуществляется отбор, где <length-value> – число от 20 до 65535;

– limit <limit-name> – указать ограничение на количество срабатываний правила, где <limit-name> – имя существующего ограничения;

– ndpi (только ipv4) – перейти на уровень конфигурации глубокого исследования пакетов (см. пункт «nDPI»);

– state <state-value> – указать состояние conntrack, по которому осуществляется отбор (см. ниже);

– ttl [min <ttl-value>] [max <ttl-value>] (только ipv4) – указать значение поля TTL, по которому осуществляется отбор, где <ttl-value> – число от 0 до 255;

– hop-limit [min <hl>] [max <hl>] (только ipv6) – указать значение поля Hop Limit, по которому осуществляется отбор, где <hl> – число от 0 до 255;

– encrypted true|false – указать, для каких пакетов (зашифрованных/незашифрованных) осуществляется отбор, где true – зашифрованные, false – незашифрованные.

Настройки правил фильтров основного МЭ аналогичны настройкам правил фильтров зонного МЭ. Для правил фильтров основного МЭ возможно указание следующих состояний conntrack:

– new – состояние соединения при отправке начального пакета;

– established – состояние установленного соединения (после прохождения хотя бы по одному пакету в обе стороны);

– related – состояние для expected-соединений (ожидаемые ответные соединения), которое принимается до established (подробнее см. подраздел «Модули conntrack»);

– invalid – состояние соединения для пакетов, не соответствующих требованиям протокола.

Для указания состояния, по которому осуществляется отбор, применяется команда:

```
[edit firewall ipv4|ipv6 netfilter filter <filter-name> rule <rule-name>]
# set state <state-value>
```

где

– ipv4|ipv6 – уровень конфигурации IPv4/IPv6;

– <filter-name> – имя существующего фильтра;

– <rule-name> – имя существующего правила;

– <state-value> – состояние conntrack.

Пример конфигурации с указанием состояния соединения:

```
firewall {
  ipv4 {
    netfilter {
      filter in-filter {
        rule 1 {
          state invalid
          drop
        }
        rule 2 {
          state established
          state related
          accept
        }
      }
    }
  }
}
```

Применение данной конфигурации позволяет:

– запретить пакеты, которые не относятся к существующим соединениям, при этом не начинают нового (например новый tcp-пакет без флага SYN);

– разрешить пакеты, относящиеся к уже установленным соединениям (как в зонном firewall).

Для основного МЭ, в отличие от зонного МЭ, отсутствует настройка action, так как действия указываются непосредственно в правиле, при этом возможно указание только одного действия в одном правиле. Кроме действий зонного МЭ для основного МЭ доступны следующие:

– goto <filter-name> – прекратить обработку пакета в текущем фильтре и перейти к указанному, где <filter-name> – имя существующего фильтра;

– call <filter-name> – обработать пакет в другом фильтре (если в другом фильтре для пакета не будет применимо действие, завершающее обработку пакета (т.е. accept, drop или reject), он продолжит прохождение текущего фильтра), где <filter-name> – имя существующего фильтра;

– set-dscp <dscp-value> – указать DSCP пакета, где <dscp-value> – значение DSCP в формате 0x<hex-value>;

– set-ttl <ttl-value> – указать TTL пакета, где <ttl-value> – число от 0 до 255;

– adjust-mss <mss-value> – настроить MSS TCP-пакета, где <mss-value> – число от 0 до 65535.

Пример конфигурации для вызова фильтра из другого:

```
firewall {
  ipv4 {
    netfilter {
      filter in-filter {
        rule 3 {
          to address 192.168.130.4
          to-port service http
          call http-filter
        }
      }
    }
  }
}
```

Применение конфигурации из данного примера позволяет вызвать фильтр http-filter из фильтра in-filter.

7.3.1.2 Ограничения на количество срабатываний

Настройка ограничений на количество срабатываний правила осуществляется на следующем уровне конфигурации:

```
[edit firewall ipv4|ipv6 netfilter filter <filter-name> limit <limit-name>]
```

где

– ipv4|ipv6 – уровень конфигурации IPv4/IPv6;

– <filter-name> – строка длиной от 1 до 128 символов;

– <limit-name> – строка длиной от 1 до 128 символов.

На данном уровне конфигурации доступны следующие настройки:

– bytes – перейти к уровню конфигурации ограничения на количество байт за единицу времени;

– packets – перейти к уровню конфигурации ограничения на количество пакетов за единицу времени;

– per day|hour|minute|second|week – указать единицу времени для ограничения, где day – за день, hour – за час, minute – за минуту, second – за секунду, week – за неделю.

Для настройки bytes предусмотрены следующие параметры:

– count <count-value> – указать максимальное количество байт, для которых возможно срабатывание правила, за единицу времени, где <count-value> – строка в формате <number>(kbytes,mbytes,gbytes,kbit,mbit,gbit);

– burst <burst-value> – указать запас для увеличения максимального количества байт, для которых возможно срабатывание правила, за единицу времени при пиковых нагрузках, где <burst-value> – строка в формате <number>(kbytes,mbytes,gbytes,kbit,mbit,gbit).

Для настройки packets предусмотрены следующие параметры:

– count <count-value> – указать максимальное количество пакетов, для которых возможно срабатывание правила, за единицу времени, где <count-value> – число от 0 до 4294967295;

– burst <burst-value> – указать запас для увеличения максимального количества пакетов, для которых возможно срабатывание правила, за единицу времени при пиковых нагрузках, где <burst-value> – число от 0 до 4294967295.

Пример конфигурации ограничения на количество срабатываний правила:

```
firewall {
  ipv4 {
    netfilter {
      filter http-filter {
        limit lim-http {
          packets count 5
          per second
        }
        rule 1 {
          limit lim-http
          accept
        }
        rule 2 {
          drop
        }
      }
    }
  }
}
```

Применение данной конфигурации позволяет разрешить только 5 соединений в секунду к http-серверу.

7.3.1.3 Фильтрация по содержимому

Настройка фильтрации по содержимому пакета осуществляется на следующем уровне конфигурации:

```
[edit firewall ipv4|ipv6 netfilter filter <filter-name> rule <rule-name> con
tent <layer> offset <offset>]
```

где

– ipv4|ipv6 – уровень конфигурации IPv4/IPv6;

– <filter-name> – строка длиной от 1 до 128 символов;

– <rule-name> – строка длиной от 1 до 128 символов;

– <layer> – уровень заголовка, от которого считается отступ (link-layer, network-header, transport-header);

– <offset> – число байт от 0 до 65535.

Так как в шестнадцатеричном представлении заголовка одному байту соответствует два символа, отступ в символах равен удвоенному значению <offset>.

Возможные значения уровня заголовка layer:

– link-layer – отступ считается от начала заголовка канального уровня (например, Ethernet);

– network-header – отступ считается от начала заголовка сетевого уровня (например, IPv4 или IPv6);

– transport-header – отступ считается от начала заголовка транспортного уровня (например, TCP или UDP).

На данном уровне конфигурации доступны следующие настройки:

– length <length-value> – указать длину проверяемого фрагмента в байтах, где <length-value> – число байт от 1 до 16;

– value <value-string> – указать значение, с которым сравнивается фрагмент, где <value-string> – строка в формате 0xHEX;

– mask <mask-value> – указать маску, применяемую к фрагменту перед сравнением, где <mask-value> – строка в формате 0xHEX, по умолчанию – 0xFFFF...

В значениях настроек mask <mask-value> и value <value-string> подстрока HEX – подряд идущие значения байтов, указанные в шестнадцатеричной системе счисления, где одному

байту соответствует два символа (например, возможно значение настройки `0x0102`, где 01 – значение первого байта, 02 – значение второго байта). Длина подстроки `HEX` соответствует значению настройки `length <length-value>`, то есть равна удвоенному значению настройки `length <length-value>`.

Перед сравнением в проверяемом фрагменте обнуляются биты, не установленные в значении настройки `mask`, а затем полученное значение сравнивается со значением настройки `value`. Если значения не совпадают, правило не применяется.

Пример конфигурации фильрации по содержимому:

```
firewall {
  ipv4 {
    netfilter {
      filter nofrag {
        rule 1 {
          content network-header offset 6 {
            length 1
            value 0x00
            mask 0x40
          }
          drop
        }
      }
    }
  }
}
```

В данном примере проверяется второй бит седьмого байта IP-заголовка, то есть флаг Don’t Fragment. Если он не установлен, пакет отбрасывается.

7.3.2 nDPI

nDPI – подсистема Deep Packet Inspection (глубокое исследование пакета), позволяющая через исследование содержимого пакета соотнести его с одним из L7-протоколов («приложений»). Для работы данной подсистемы необходимо указать список приложений.

Настройка списка приложений осуществляется на следующем уровне конфигурации:

```
[edit firewall ipv4 netfilter application <application-name>]
```

где `<application-name>` – строка длиной от 1 до 128 символов.

На данном уровне конфигурации доступны следующие настройки:

– protocol <protocol-name> – указать протокол, где <protocol-name> – строка.

Пример конфигурации списка приложений:

```
firewall {
  ipv4 {
    netfilter {
      application A {
        protocol instagram
        protocol twitter
        protocol whatsapp
        protocol youtube
      }
    }
  }
}
```

Настройка применения списка приложений осуществляется на следующем уровне конфигурации:

```
[edit firewall ipv4 netfilter filter <filter-name> rule <rule-name> ndpi]
```

где

– <filter-name> – строка длиной от 1 до 128 символов;

– <rule-name> – строка длиной от 1 до 128 символов.

На данном уровне конфигурации доступны следующие настройки:

– proto <application-name> – применить список приложений, где <application-name> – имя существующего списка приложений;

– in-progress <application-name> – применить список не полностью обнаруженных приложений, где <application-name> – имя существующего списка приложений.

Пример конфигурации механизма nDPI в фильтре netfilter:

```
firewall {
  ipv4 {
    netfilter {
      filter web-filter {
        rule 1 {
          ndpi proto A
          drop
        }
        rule 2 {
          ndpi in-progress A
          log {
            prefix «Forbidden app?»
            snaplen 1500
```

```
            }
          }
        }
      }
    }
}
```

7.4 Модули conntrack (helper)

Некоторых протоколы (например, FTP) используют несколько соединений в рамках одной сессии. Для корректной работы firewall на таких протоколах (например, чтобы соединение, устанавливаемое ответной стороной, не заблокировалось зонным firewall и правильно обработалось NAT) используются специальные модули conntrack (так называемые – helper).

Настройки helper осуществляются на следующем уровне конфигурации:

```
[edit firewall ipv4|ipv6 helper <helper-name>]
```

где

– `ipv4|ipv6` – уровень конфигурации IPv4/IPv6;

– `<helper-name>` – строка длиной от 1 до 128 символов.

На данном уровне конфигурации доступны следующие настройки:

– `description <description>` – указать описание helper, где `<description>` – строка;

– `log` – перейти на уровень конфигурации журналирования пакетов;

– `protocol tcp|udp` – указать протокол;

– `to address <address>|file-list <file-list-name>|network <network-name>` – (критерий отбора) указать адрес(а) назначения, по которому(ым) осуществляется отбор трафика, где `<address>` – IPv4-адрес в формате `A.B.C.D[/mask]` или IPv6-адрес в формате `A:B:..:H[/mask]` в зависимости от уровня конфигурации, `<network-name>` – имя существующего списка сетей, `<file-list-name>` – имя существующего файла списка сетей (см. подпункт «Списки сетей и сервисы»);

– `to-port <port-number>` – (критерий отбора) указать входящий порт, по которому осуществляется отбор трафика, где `<port-number>` – строка в формате `n[-m]` (`n`, `m` – числа от 1 до 65535);

– `type` – указать тип helper (`H.245`, `Q.931`, `RAS`, `amanda`, `ftp`, `irc`, `netbios-ns`, `pptp`, `sane`, `sip`, `snmp`, `tftp`).

Пример конфигурации helper:

```
firewall {
  ipv4 {
    helper hlp-ftp {
      protocol tcp
      to-port 21
      type ftp
      to address 192.168.130.4
    }
  }
}
```

7.5 Bridge firewall

Для фильтрации трафика, проходящего через bridge-интерфейсы, используется bridge firewall. Трафик, проходящий в рамках одного интерфейса типа `bridge`, не попадает в другие firewall'ы, поэтому bridge firewall – единственный способ фильтрации такого трафика.

Настройка bridge firewall осуществляется на следующем уровне конфигурации:

```
[edit firewall bridge]
```

На данном уровне конфигурации доступны следующие настройки:

– `filter <filter-name>` – перейти на уровень конфигурации фильтра bridge firewall, где `<filter-name>` – имя фильтра (см. ниже);

– `forward` – (цепочка применения фильтра) применить фильтр к кадрам, передаваемым от одного интерфейса к другому;

– `local-in` – (цепочка применения фильтра) применить фильтр к кадрам, передаваемым на ПАК «Фортикс»;

– `local-out` – (цепочка применения фильтра) применить фильтр к кадрам, передаваемым с ПАК «Фортикс»;

– `prerouting` – (цепочка применения фильтра) применить фильтр к входящим кадрам до их маршрутизации;

– `postrouting` – (цепочка применения фильтра) применить фильтр к выходящим кадрам.

Настройка фильтров bridge firewall осуществляется на следующем уровне конфигурации:

```
[edit firewall bridge filter <filter-name>]
```

где `<filter-name>` – строка длиной от 1 до 128 символов.

На данном уровне конфигурации доступны следующие настройки:

– `description <description>` – указать описание фильтра, где `<description>` – строка;

– `limit <limit-name>` – перейти на уровень конфигурации ограничений на число срабатываний правила, где `<limit-name>` – имя существующего ограничения (см. подпункт «Ограничения на количество срабатываний»);

– `rule <rule-name>` – указать правило, соответствующее данному фильтру, где `<rule-name>` – имя правила (см. ниже).

Настройка правил фильтров bridge firewall осуществляется на следующем уровне конфигурации:

```
[edit firewall bridge filter <filter-name> rule <rule-name>]
```

где

– `<filter-name>` – строка длиной от 1 до 128 символов;

– `<rule-name>` – строка длиной от 1 до 128 символов.

На данном уровне конфигурации доступны следующие настройки:

– `description <description>` – указать описание правила, где `<description>` – строка;

– `from-interface <interface-name>` – (критерий отбора) указать интерфейс источника, по которому осуществляется отбор трафика, где `<interface-name>` – имя существующего интерфейса;

– `to-interface <interface-name>` – (критерий отбора) указать интерфейс назначения, по которому осуществляется отбор трафика, где `<interface-name>` – имя существующего интерфейса;

– `timestart <timestart-value>` – (критерий отбора) указать начальное время выполнения правила, где `<timestart-value>` – строка в формате `HH:MM[:SS]`;

– `timestop <timestop-value>` – (критерий отбора) указать конечное время выполнения правила, где `<timestop-value>` – строка в формате `HH:MM[:SS]`;

– `datestart <datestart-value>` – (критерий отбора) указать начальную дату (и время) выполнения правила, где `<datestart-value>` – строка в формате `YYYY-MM-DD[THH:MM[:SS]]`, по умолчанию – 00:00:00;

– datestop <datestop-value> – (критерий отбора) указать конечную дату (и время) выполнения правила, где <datestop-value> – строка в формате YYYY-MM-DD[THH:MM[:SS]], по умолчанию – 00:00:00;

– content <layer> offset <offset> – перейти на уровень конфигурации критерия отбора по содержимому (см. подпункт «Фильтрация по содержимому»);

– encrypted true|false – указать, для каких пакетов (зашифрованных/незашифрованных) осуществляется отбор, где true – зашифрованные, false – незашифрованные;

– log – перейти на уровень конфигурации журналирования кадров;

– counter <counter-name> – указать счётчик срабатывания правила, где <counter-name> – имя счётчика (см. пункт «Счётчики»);

– trace – применить трассировку кадров.

– from-mac <mac> – (критерий отбора) указать адрес источника, по которому осуществляется отбор трафика, где <mac> – MAC-адрес в формате xx:xx:xx:xx:xx:xx;

– to-mac <mac> – (критерий отбора) указать адрес назначения, по которому осуществляется отбор трафика, где <mac> – MAC-адрес в формате xx:xx:xx:xx:xx:xx;

– vlan – (критерий отбора) использовать виртуальную локальную сеть (VLAN) и перейти на уровень её конфигурации:

– id <id> – (критерий отбора) указать идентификатор виртуальной локальной сети (VLAN Identifier), где <id> – число от 0 до 4095;

– pcp [value <value-pcp>] [mask <mask-pcp>] – (критерий отбора) указать приоритет трафика в VLAN (Priority Code Point), где <value-pcp> – hex-значение в формате 0x00..0x3f, <mask-pcp> – hex-значение в формате 0x00..0x3f;

– dei – (критерий отбора) указать индикатор допустимости удаления (Drop Eligible Indicator);

– ipv4|ipv6|arp – (критерий отбора) указать протокол и перейти на уровень его конфигурации (см. ниже).

На уровне конфигурации протоколов IPv4 и IPv6 доступны следующие критерии отбора:

– from address <address>|file-list <file-list-name>|network <network-name> – (критерий отбора) указать адрес(а) источника, по которому(ым) осуществляется отбор трафика, где <address> – IPv4-адрес в формате A.B.C.D[/mask] или IPv6-адрес в формате A:B:..:H[/mask] в зависимости от уровня конфигурации, <network-name> – имя

существующего списка сетей, <file-list-name> – имя существующего файла списка сетей (см. подпункт «Списки сетей и сервисы»);

– to address <address>|file-list <file-list-name>|network <network-name> – (критерий отбора) указать адрес(а) назначения, по которому(ым) осуществляется отбор трафика, где <address> – IPv4-адрес в формате A.B.C.D[/mask] или IPv6-адрес в формате A:B:..:H[/mask] в зависимости от уровня конфигурации, <network-name> – имя существующего списка сетей, <file-list-name> – имя существующего файла списка сетей (см. подпункт «Списки сетей и сервисы»);

– from-port <port> – (критерий отбора) указать исходящий порт, по которому осуществляется отбор трафика, где <port> – строка в формате tcp|udp n[-m] (n, m – число от 1 до 65535) или имя существующего списка портов (см. подпункт «Списки сетей и сервисы»);

– to-port <port> – (критерий отбора) указать входящий порт, по которому осуществляется отбор трафика, где <port> – строка в формате tcp|udp n[-m] (n, m – число от 1 до 65535) или имя существующего списка портов (см. подпункт «Списки сетей и сервисы»);

– protonum <protocol-number> – (критерий отбора) указать номер протокола, где <protocol-number> – число от 0 до 255;

– tcp|udp|icmp (для ipv4) – (критерий отбора) указать протокол и перейти на уровень конфигурации протокола (не может быть задано вместе с protonum);

– tcp|udp|icmpv6 (для ipv6) – (критерий отбора) указать протокол и перейти на уровень конфигурации протокола (не может быть задано вместе с protonum).

На уровне конфигурации протокола ARP доступны следующие критерии отбора:

– arp-operation inreply|inrequest|nak|reply|request|rreply|rrequest – указать код операции ARP;

– from-mac <mac> – указать mac-адрес источника в ARP-пакете, где <mac> – MAC-адрес в формате xx:xx:xx:xx:xx:xx;

– to-mac <mac> – указать mac-адрес назначения в ARP-пакете, где <mac> – MAC-адрес в формате xx:xx:xx:xx:xx:xx;

– from <address> – указать IPv4-адрес источника в ARP-пакете, где <address> – IPv4-адрес в формате A.B.C.D[/mask];

– to <address> – указать IPv4-адрес назначения в ARP-пакете, где <address> – IPv4-адрес в формате A.B.C.D[/mask].

Действия в bridge firewall указываются непосредственно в правиле, как и в основном МЭ. Доступны следующие действия:

– `accept` — разрешить соединение и прекратить дальнейшую его проверку зонным firewall;

– `drop` — запретить соединение без отправки ICMP-уведомления;

– `reject` — запретить соединение с отправкой источнику ICMP-уведомление (ICMPv6-уведомление для IPv6) `port-unreachable`;

– `return` — прекратить обработку кадра в данном фильтре (в данном случае соединение обрабатывается `default-action` политики (см. подпункт «Политики») или `drop-policy`).

– `goto <filter-name>` – прекратить обработку кадра в текущем фильтре и перейти к указанному, где `<filter-name>` – имя существующего фильтра;

– `call <filter-name>` – обработать кадр в другом фильтре (если в другом фильтре для кадра не будет применимо действие, завершающее обработку кадра (т.е. `accept`, `drop` или `reject`), он продолжит прохождение текущего фильтра), где `<filter-name>` – имя существующего фильтра;

– `set-src-mac <mac-value>` – изменить адрес источника кадра, где `<mac-value>` – MAC-адрес в формате `xx:xx:xx:xx:xx:xx`;

– `set-dst-mac <mac-value>` – изменить адрес назначения кадра, где `<mac-value>` – MAC-адрес в формате `xx:xx:xx:xx:xx:xx`.

Последние два действия позволяют задать трансляцию MAC-адресов. В отличие от NAT данная трансляция выполняется не для некоторого соединения, а покадрово, в частности при замене адреса источника у ответного кадра не заменяется адрес назначения.

7.6 Схема работы firewall

Схема прохождения пакета через все компоненты firewall представлена на рисунке 1.

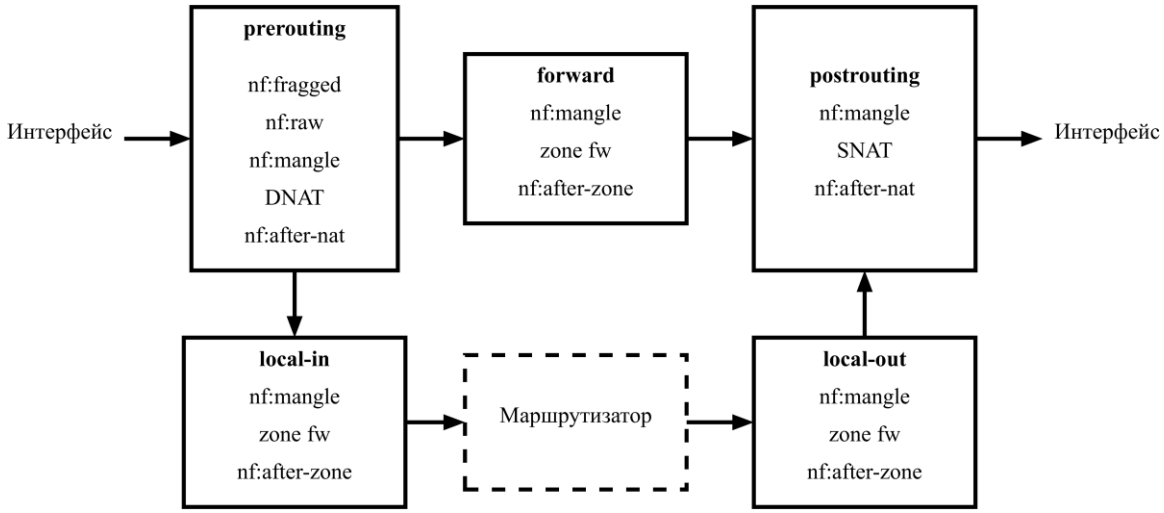

Рисунок 1 – Схема работы firewall.

7.7 Журналирование пакетов

Запись пакетов в ПАК «Фортикс» осуществляется в журнал МЭ (см. ниже). Для журналирования пакетов в правиле (`rule`) фильтра firewall возможно применение настройки `log`.

Настройка журналирования пакетов осуществляется на следующем уровне конфигурации:

```
[edit firewall ... rule <rule-name> log]
```

где `<rule-name>` – строка длиной от 1 до 128 символов.

На данном уровне конфигурации доступны следующие настройки:

– `prefix <prefix-text>` – указать описание, по которому идентифицируется журналируемое правило, где `<prefix-text>` – строка в двойных кавычках, допустимо указание одного слова без кавычек;

– `snaplen <snaplen-value>` – указать длину записываемого фрагмента пакета, где `<snaplen-value>` – число байт от 0 до 65535, по умолчанию записывается весь пакет;

– `journal alert|info` – указать уровень события для записи пакета в системный журнал, без указания данной настройки в системный журнал пакеты не записываются.

Пример конфигурации журналирования правила фильтра:

```
firewall {
  ipv4 {
```

```
    netfilter {
      filter in-filter {
        rule 3 {
          to address 192.168.130.4
          to-port service http
          log {
            prefix «http catched»
            snaplen 1500
          }
          call http-filter
        }
      }
    }
  }
}
```

Для просмотра журнала МЭ применяется команда:

```
> show firewall journal
```

Для изменения формата выводимой по данной команде информации используются следующие параметры:

Т а б л и ц а 4 – Параметры команды для просмотра журнала

Настройка	Описание
verbose	вывести журнал в режиме подробного отображения
since <date-time>	вывести пакеты, пришедшие после указанного времени
until <date-time>	вывести пакеты, пришедшие до указанного времени
count <record-count>	вывести первые <record-count> записей
tail <record-count>	вывести последние <record-count> записей
ascii|hex|hex-ascii	применить режим вывода содержимого пакета
follow	вывести пакеты в режиме реального времени
resolve	вывести IP-адреса, преобразованные при помощи DNS
alert	вывести только пакеты с флагом `alert`
write <file-path>	экспортировать пакеты в файл в формате tcpdump
archive <file-path>	вывести содержимое указанного файла журнала МЭ (см. ниже)
forward	вывести пакеты только из цепочки `forward`
local-in	вывести пакеты только из цепочки `local-in`
local-out	вывести пакеты только из цепочки `local-out`

Настройка	Описание
postrouting	вывести пакеты только из цепочки `postrouting`
prerouting	вывести пакеты только из цепочки `prerouting`
in <interface-name>	вывести пакеты, пришедшие на указанный интерфейс
out <interface-name>	вывести пакеты, выходящие через указанный интерфейс
ipv4	вывести только IPv4-пакеты
ipv6	вывести только IPv6-пакеты
pcap <pcap-filter>	вывести только пакеты, отобранные по pcap-фильтру

Дата/время <date-time> в параметрах могут быть заданы в одном из следующих форматов:

– `YYYY-mm-dd`;

– `HH:MM`;

– `HH:MM:SS`;

– `YYYY-mm-ddTHH:MM:SS`;

– `YYYY-mm-ddTHH:MM:SS`.

где

– YYYY – год (четырёхзначное число);

– mm – месяц (число от 1 до 12);

– dd – день (число от 1 до 31);

– HH – часы (от 0 до 23);

– MM – минуты (от 0 до 59);

– SS – секунды (от 0 до 59).

7.7.1 Настройки журналирования

Настройка журналирования МЭ осуществляется на следующем уровне конфигурации:

```
[edit firewall journal]
```

На данном уровне конфигурации доступны следующие настройки:

– `file-count <max-file-count>` – указать максимальное число файлов журнала МЭ, где `<max-file-count>` – число от 1 до 65535;

– `file-size <max-file-size>` – указать максимальный размер одного файла журнала МЭ, где `<max-file-size>` – число Мбит от 1 до 4294967295;

– kernel-size <max-kernel-size> – указать максимальный размер буфера для передачи сообщений из ядра, где <max-kernel-size> – число Кбит от 128 до 4294967295.

Пример конфигурации журналирования:

```
firewall journal {
  file-size 20
  file-count 5
  kernel-size 2048
}
```

При превышении максимального размера одного файла журнала создаётся новый файл журнала. При превышении максимального числа файлов журнала удаляются наиболее старые файлы журнала. При переполнении буфера (как правило из-за ограничения скорости записи журнала на носитель) пакеты отбрасываются без записи в журнал.

Полное имя файла журнала МЭ, в который осуществляется текущая запись – /log/kernel.fwlog. При его переполнении создаётся файл /log/kernel.fwlog-YYYY-mm-ddTHH:MM:SS, в который помещаются записи файла /log/kernel.fwlog, файл /log/kernel.fwlog очищается.

7.8 Трассировка пакетов

Трассировка пакетов применяется для отладки прохождения пакетов через firewall в правилах фильтров firewall netfilter или firewall bridge.

Для использования трассировки пакетов применяется команда:

```
[edit firewall ... rule <rule-name>]
# set trace
```

где <rule-name> – строка длиной от 1 до 128 символов.

Пример конфигурации трассировки пакетов:

```
firewall ipv4 netfilter {
  filter trace rule 1 {
    icmp {
      icmp-type echo-reply
      icmp-type echo-request
    }
    trace
  }
  prerouting fragged filter trace
}
```

В данной конфигурации трассировка применяется ко всем входящим в ПАК «Фортикс» и проходящим через него ping-пробам, причём признак трассировки устанавливается в самом раннем месте из возможных.

Для просмотра трассировки пакетов применяется команда:

```
> show firewall trace
```

П р и м е ч а н и е – Трассировка пакетов не сохраняется во внешнюю среду, её просмотр доступен только в конфигурации.

8 Качество обслуживания (QoS)

Механизмы QoS ПАК «Фортикс» позволяют назначать различные дисциплины обслуживания входящего и исходящего трафика. В зависимости от применённых политик дисциплин для выбранных классов трафика механизмы QoS позволяют:

– управлять гарантированной полосой пропускания;

– задавать предельную полосу пропускания;

– приоритизировать трафик;

– управлять контролируемой перегрузкой.

8.1 Величины скорости полос пропускания

При настройке полос пропускания используются величины скорости, которые задаются в виде числа и необязательного постфикса для выбора единицы измерения согласно таблице 5.

Т а б л и ц а 5 – Величины скорости полосы пропускания

Постфикс	Единица измерения
нет	бит в секунду
kbps	килобайт в секунду
mbps	мегабайт в секунду
kbit	килобит в секунду
mbit	мегабит в секунду
bps	байт в секунду

Если постфикс не указан, скорость полосы пропускания измеряется в битах в секунду.

8.2 Классификация

Классификация трафика в ПАК «Фортикс» осуществляется непосредственно перед его отправкой на интерфейс (для дисциплин обслуживания исходящего трафика) или сразу после его получении (для дисциплин обслуживания входящего трафика).

Для создания и настройки классов применяется команда:

```
# set qos class <class-name>
```

где `<class-name>` – слово.

Пример применения команды для создания и настройки классов:

```
# set qos class voip
```

По умолчанию создан пустой класс `all`, который относится к любому IPv4/IPv6-трафику. Если в классе не указаны никакие правила отбора, он считается применимым для любого трафика. Если в классе задано хотя бы одно правило, оно «ограничивает» действие класса согласно заданному правилу.

Настройка классов осуществляется на следующем уровне конфигурации:

```
[edit qos class <class-name>]
```

где `<class-name>` – слово.

На данном уровне конфигурации доступны следующие настройки:

– `description <description>` – описание класса, где `<description>` – строка;

– `ether` – применить класс к Ethernet-трафику и перейти на уровень конфигурации Ethernet-трафика:

– `from address <address>` – указать адрес источника , где `<address>` – MAC-адрес в формате `xx:xx:xx:xx:xx:xx`;

– `to address <address>` – указать адрес назначения, где `<address>` – MAC-адрес в формате `xx:xx:xx:xx:xx:xx`;

– `ipv4|ipv6` – применить класс к IPv4/IPv6-трафику и перейти на уровень конфигурации IPv4/IPv6-трафика:

– `fragment df|first|mf|no` (только для ipv4) – указать флаг фрагментации, где `df` – установлен флаг DF, `first` – первый фрагмент, `mf` – установлен флаг MF, `no` – не фрагментированный пакет;

– `from address <address>` – указать адрес источника, где `<address>` – IPv4-адрес в формате `A.B.C.D[/mask]` или IPv6-адрес в формате `A:B:..:H[/mask]` в зависимости от уровня конфигурации;

– `to address <address>` – указать адрес назначения, где `<address>` – IPv4-адрес в формате `A.B.C.D[/mask]` или IPv6-адрес в формате `A:B:..:H[/mask]` в зависимости от уровня конфигурации;

– `from port high|low <port-number>` – указать верхнюю/нижнюю границу значения номера порта источника, где `high` – верхняя граница, `low` – нижняя граница, `<port-number>` – число от 1 до 65535;

– `to port high|low <port-number>` – указать верхнюю/нижнюю границу значения номера порта назначения, где `high` – верхняя граница, `low` – нижняя граница, `<port-number>` – число от 1 до 65535;

– `tos <hex-value>` – задать ToS, где `<hex-value>` – тип ToS.

Пример применения правила в классе:

```
# set qos class voip ipv4 from address 192.168.1.133
```

8.3 Дисциплины исходящего трафика

Настройка дисциплин для исходящего трафика осуществляется на следующем уровне конфигурации:

```
[edit qos qdisc]
```

ПАК «Фортикс» поддерживает дисциплины обслуживания следующих типов:

– `htb` – иерархическая дисциплина, позволяющая создавать древовидные структуры очередей;

– `codel` – политика борьбы с перегрузками, в которой ограничивается не размер очереди, а максимальное время нахождения пакета в очереди;

– `fq-codel` – политика борьбы с перегрузками (в отличие от `codel` пакеты разделяются на некоторое количество очередей на основе соединения);

– `pfifo-fast` – простая очередь;

– `red` – Random Early Detection (произвольное раннее обнаружение);

– `sfq` – Stochastic Fairness Queueing);

– `noqueue` – нет очереди.

Дисциплина типа `htb` позволяет классифицировать трафик и направлять его в различные очереди, дисциплины других типов могут быть использованы в качестве дочерних. Дисциплина данного типа выступает в роли основного «связующего» средства механизма QoS.

Настройка механизма QoS в общем случае осуществляется следующим образом:

1) При использовании дисциплины типа `htb` создаются классы трафика с помощью команды:

```
set qos class <class-name>
```

где `<class-name>` – слово.

2) Создаются и настраиваются политики дисциплин требуемого типа с помощью команды:

```
set qos qdisc <discipline-type> <discipline-name>
```

где

– <discipline-type> – тип дисциплины (см. выше);

– <discipline-name> – слово.

3) Присоединяются дисциплины к выходам интерфейсов с помощью команды:

```
set interface <interface-type> <interface-name> egress qdisc <qos-discipline
-name>
```

где

– <interface-type> – тип существующего интерфейса;

– <interface-name> – имя существующего интерфейса;

– <qos-discipline-name> – имя существующей дисциплины QoS.

8.4 Дисциплина HTB

Дисциплина HTB позволяет контролировать полосу пропускания для иерархии классов. Для настройки иерархии необходимо задать несколько полос (band) и, при необходимости, объединить их в дерево.

Для определения полос пропускания применяется команда:

```
[edit qos qdisc htb main]
# set band <band-name> rate <rate-value>
```

где

– <band-name> – слово;

– <rate-value> – строка в формате <number>(kbit, mbit, bps..), <number> – число, после которого указывается единица измерения.

Пример применения команды для определения полос пропускания:

```
# edit qos qdisc htb main
# set band voip rate 100mbit
# set band route rate 900mbit
```

Для указания ограничения всей полосы пропускания применяется команда:

```
[edit qos qdisc htb main]
# set ceil <ceil-value>
```

где <ceil-value> – строка в формате <number>(kbit, mbit, bps..), <number> – число, после которого указывается единица измерения.

Пример применения команды для указания ограничения всей полосы пропускания:

```
[edit qos qdisc htb main]
# set ceil 10000mbit
```

В данных примерах не создаётся иерархия полос, полоса в 1000mbit делится между полосами `voip` и `route` линейно. При этом полосе `voip` гарантируется предоставление 1000mbit, а полосе route – 900mbit.

П р и м е ч а н и е – Сумма `voip rate` и `route rate` не может превышать ограничение `ceil` политики в 1000mbit.

Для направления трафика в полосы пропускания применяется команда:

```
# set policy <class-name> band <band-name>
```

где

– `<class-name>` – имя существующего класса;

– `<band-name>` – имя существующей полосы.

Пример применения команды для направления трафика в полосы пропускания:

```
[edit qos qdisc htb main]
# set policy voip band voip
# set policy
# set default route
```

В данном примере трафик класса `voip` направляется в полосу `voip`, а весь остальной трафик в полосу `route`.

Для маркировки поля `tos` у пакетов заданного класса применяется команда:

```
# set policy <class-name> set ipv4|ipv6 tos <tos-mark>
```

где

– `<class-name>` – имя существующего класса;

– `ipv4|ipv6` – тип трафика;

– `<band-name>` – имя существующей полосы.

Пример применения команды для маркировки поля `tos`:

```
[edit qos qdisc htb main]
# set policy voip set ipv4 tos 0x46
```

Для создания иерархии распределения общей полосы выполняется следующий алгоритм:

1) создать несколько полос, на которые делится общая полоса;

2) преобразовать полосы в дочерние для общей полосы.

Пример применения команд для разделения полосы route на две полосы a и b:

1) Создание полос a и b:

```
[edit qos qdisc htb main]
# set band a rate 200mbit
# set band b rate 700mbit
```

2) Преобразование полос a и b в дочерние для полосы route:

```
[edit qos qdisc htb main]
# set band a parent route
# set band b parent route
```

При выполнении вышеуказанных настроек полосы a и b суммарно не смогут использовать полосу больше 900mbit родительской полосы.

Классы трафика могут быть направлены только на те полосы, которые не имеют дочерних. Для этого создаются соответствующие классы для распределения трафика по конечным полосам (не имеющим дочерних полос).

В продолжении примера выше создание классов для распределения трафика по полосам a и b:

```
[edit qos qdisc htb main]
# top
# set qos class route-a ipv4 to address 192.168.0y.0/24
# set qos class route-b ipv4 to address 192.168.1.0/24
# edit qos qdisc htb main
# set policy route-a band a
# set policy route-b band b
# del default
```

В данном примере полосы a, b и voip являются конечными. С конечными полосами возможно связать любую ранее настроенную дисциплину, обеспечив тем самым требуемое качество обслуживания.

Пример настройки qos:

```
[edit qos qdisc htb main]
# top
# set qos qdisc sfq sfq
# set qos qdisc htb main set band a qdisc sfq
# set qos qdisc htb main set band b qdisc sfq
# set qos qdisc htb main set band voip qdisc sfq
```

8.5 Дисциплина для входящего трафика

Дисциплина для входящего трафика `ingress` позволяет использовать следующие политики:

– `mirror` – для перенаправления/зеркалирования трафика в другой интерфейс;

– `rate` – для ограничения полосы пропускания на вход;

– `set` – для задания поля dscp/tos.

Политика работает с выбранным классом трафика, в связи с чем первоначально необходимо создать требуемые классы или использовать класс `all`, например:

```
# set interface ether en0 ingress policy all rate ceil 1000mbit
# set interface ether en0 ingress policy voip set ipv4 tos 0x46
```

8.6 Интерфейс типа ifb

Дисциплины исходящего трафика позволяют управлять трафиком перед непосредственной отправкой. Для управления трафиком на приёме (например, при шифровании трафика для выделения гарантированной полосы для класса, который отправляется в туннель на зашифрование) используется виртуальный интерфейс типа `ifb`.

Настройка QoS для управления трафиком на приёме в общем случае осуществляется следующим образом:

1) создаётся интерфейс ifb;

2) к интерфейсу привязывается необходимая дисциплина;

3) для всех интерфейсов, попадающих в `ingress` и разделяющих общую дисциплину на интерфейсе ifb, настраивается перенаправление трафика на интерфейс типа `ifb`.

Пример настройки QoS для управления трафиком на приёме:

```
# set interface ifb ifb0 enable
# set interface ifb ifb0 egress qdisc main
# set interface ether en0 ingress mirror all interface ifb0 redirect
# set interface ether en1 ingress mirror all interface ifb0 redirect
```

При применении данных настроек весь трафик, приходящий на интерфейсы `en0` и `en1`, обслуживается дисциплиной `main`.

Важно! При зеркалировании на интерфейс трафик отправляется сразу на исходящую дисциплину, не попадая в дисциплину `ingress` интерфейса, на который осуществляется

перенаправление. Таким образом, дисциплина `ingress` политики на интерфейсе `ifb` не действует для зеркалируемого трафика.

8.7 Диагностика

Для просмотра информации о применённых входящих и выходящих дисциплинах для указанного интерфейса применяется команда:

```
> show interface <interface-type> <interface-name> qdisc
```

где

– `<interface-type>` – тип существующего интерфейса;

– `<interface-name>` – имя существующего интерфейса.

Пример применения команды для просмотра информации о входящих и исходящих дисциплинах для указанного интерфейса:

```
> show interface ether en0 qdisc
```

9 Служба dhcp

Служба dhcp в ПАК «Фортикс» реализует серверную часть протокола DHCP (Dynamic Host Configuration Protocol). Данная служба применяется для динамической конфигурации узла.

Протокол DHCP позволяет сетевому узлу автоматически получать IP-адрес и другие параметры, необходимые для работы в сети. Данный протокол работает по модели «клиент-сервер». Для автоматической конфигурации клиент обращается к серверу DHCP и получает от него необходимые параметры на этапе конфигурации сетевого устройства.

Основная концепция настройки службы dhcp ПАК «Фортикс» – иерархичность и наследуемость конфигурационных пространств.

Предусмотрена следующая иерархия конфигурации:

– `[edit service dhcp]`, `[edit service dhcp ipv4]`, `[edit service dhcp ipv6]` – уровень глобальной конфигурации службы, глобальной конфигурации службы в режиме IPv4 или IPv6 (уровень А);

– `[edit service dhcp ipv4|ipv6 subnet]`, `[edit service dhcp ipv4|ipv6 shnet]` или `[edit service dhcp ipv4|ipv6 host]` – уровень динамической конфигурации для подсети, разделяемой сети или статической конфигурации для хоста (уровень Б).

В ПАК «Фортикс» предусмотрен следующий принцип наследуемости конфигурации:

– заданное значение настройки уровня А неявно определяет такое же значение для той же настройки на уровне Б, в случае если последняя не задана;

– часть настроек уровня А может быть задана и на уровне Б: в этом случае настройка уровня Б переопределяет глобальную настройку, заданную на уровне А, или настройку по умолчанию (если аналогичной настройки на уровне А не задано).

Настройка службы dhcp осуществляется на следующем уровне конфигурации:

```
[edit service dhcp]
```

Служба может работать в режиме IPv4, в режиме IPv6 или в обоих одновременно.

9.1 Служба dhcp в режиме IPv4

Служба считается настроенной и включённой для работы в режиме IPv4 по настройке `enable`, в случае если выполнено любое условие из следующих:

– не задано ни одной команды `listen ipv4` и `listen ipv6`: служба принимает запросы на всех подходящих интерфейсах;

– задана одна или более `listen ipv4`-команд: служба принимает запросы на указанных интерфейсах.

9.1.1 Настройки принятия запросов

Для указания интерфейса, на котором служба ожидает DHCP-запросы от клиентов, применяется команда:

```
# set listen ipv4 interface <interface-name>
```

где `<interface-name>` – имя существующего интерфейса.

По умолчанию служба ожидает запросы на всех широковещательных Ethernet-интерфейсах.

Для указания порта, на котором ожидаются DHCP-запросы, применяется команда:

```
# set listen ipv4 port <port-number>
```

где `<port-number>` – число от 1 до 65535, по умолчанию – 67.

Для указания IP-адреса, на котором принимаются нешироковещательные DHCP-запросы, применяется команда:

```
# set listen ipv4 address <address>
```

где `<address>` – IPv4-адрес в формате `A.B.C.D`.

Широковещательные при этом запросы не принимаются.

П р и м е ч а н и е – Данная команда полезна при применении службы dhcp в связке со службой dhcprelay (на другом узле).

9.1.2 Настройки тайм-аутов

Для настройки максимального срока аренды адреса применяется команда:

```
# set ipv4 timeout lease max <lease-max-value>
```

где `<lease-max-value>` – число секунд, по умолчанию – 86400.

Данную настройку можно указать глобально, в настройках хоста и подсети.

Сетевое устройство, взаимодействующее с ПАК «Фортикс» по сети TCP/IP (далее по тексту клиент), в запросе может прислать желаемое максимальное значение срока аренды адреса. При указании максимального срока аренды адреса в конфигурации клиент не может получить в аренду адрес на время, большее заданного в настройке.

Для настройки минимального срока аренды применяется команда:

```
# set ipv4 timeout lease min <lease-min-value>
```

где `<lease-min-value>` – число секунд, по умолчанию – 300.

Данную настройку можно указывать глобально, в настройках хоста и подсети.

Клиент в запросе может прислать желаемое минимальное значение срока аренды адреса. При указании минимального срока аренды адреса в конфигурации клиент не может получить в аренду адрес на время, меньшее заданного.

Для настройки срока аренды адреса по умолчанию применяется команда:

```
# set ipv4 timeout lease default <lease-default-value>
```

где `<lease-default-value>` – число секунд, по умолчанию – 43200.

Данную настройку можно указать глобально, в настройках хоста и подсети.

Срок аренды адреса назначается клиенту в случае, если он не прислал в запросе желаемое значение.

Для настройки промежутка времени, в течение которого служба ожидает перед ответом на запрос клиента, применяется команда:

```
# set ipv4 timeout respond-delay <respond-delay-value>
```

где `<respond-delay-value>` – число секунд от 0 до 255, по умолчанию – 0.

Настройка применима для организации дублирующего DHCP-сервера на основе данной службы (если основной сервер DHCP не ответил в течение указанного периода времени, клиенту ответит дублирующая служба dhcp).

Для настройки значения TTL динамических записей применяется команда:

```
# set ipv4 timeout ddns-ttl <ddns-ttl-value>
```

где `<ddns-ttl-value>` – число секунд, по умолчанию – определяется клиентом.

Данная настройка применима при использовании динамических DNS-обновлений.

9.1.3 Настройка статического назначения

Статическое назначение адреса применимо в случае существенных хостов сети (например, серверов), для рабочих станций используется динамическое назначение адреса (см. пункт «Настройка динамического назначения»).

Важно! Статический диапазон адресов для назначения не может пересекаться с динамическим.

Настройка статического назначения IP-адреса для клиентов осуществляется на следующем уровне конфигурации (далее по тексту host-секция):

```
[edit service dhcp ipv4 host <host-name>]
```

где `<host-name>` –строка длиной от 1 до 253 символов.

Аргумент `<host-name>` существенен только при включённой настройке `send-hostname` (см. пункт «Прочие настройки»): в этом случае оно передаётся клиенту в качестве имени его хоста. При выключенной настройке `send-hostname` имя хоста несущественно.

Для переопределения имени хоста клиента применяется команда:

```
# set hostname <hostname>
```

где `<hostname>` – строка длиной от 1 до 253 символов.

В службе dhcp предусмотрены настройки признаков, по которым служба определяет принадлежность входящего DHCP-запроса host-секции.

Для указания MAC-адреса клиента в качестве привязки к host-секции применяется команда:

```
# set mac <mac-address>
```

где `<mac-address>` – MAC-адрес в формате `xx:xx:xx:xx:xx:xx`.

Для указания идентификатора клиента в качестве привязки host-секции применяется команда:

```
# set client-id <client-id-value>
```

где `<client-id-value>` – строка длиной от 1 до 253 символов.

В качестве аргумента `<client-id-value>` принимается значение поля dhcp-client-identifier DHCP-запроса.

Таким образом, для поиска host-секции, соответствующей клиенту, от которого поступил запрос, выполняется алгоритм:

1) Осуществляется поиск идентификатора клиента, указанного в настройке `client-id <client-id-value>`, совпадающего с dhcp-client-identifier клиента.

2) Если искомый идентификатора клиента `client-id` не найден, осуществляется поиск MAC-адреса, указанного в настройке `mac <mac-address>`, совпадающего с MAC-адресом клиента.

Для указания статического IP-адреса клиента, который назначается ему в случае соответствия host-секции по указанным в ней настройкам привязки (`mac <mac-address>` или `client-id <client-id-value>`), применяется команда:

```
# set ip <address>
```

где `<address>` – IPv4-адрес в формате `A.B.C.D`.

9.1.4 Настройка динамического назначения

Динамическое назначение адресов рекомендуется для обычных рабочих станций и других узлов, для которых не требуется постоянный IP-адрес.

Важно! Статический диапазон адресов для назначения не должен пересекаться с динамическим диапазоном.

Настройка динамического назначения IP-адреса клиентов осуществляется на следующем уровне конфигурации (далее по тексту subnet-секция):

```
[edit service dhcp ipv4 subnet <subnet-address>]
```

где `<subnet-address>` – IPv4-адрес в формате `A.B.C.D/mask`.

Для настройки динамического назначения адресов необходимо определить диапазоны адресов, из которых назначаются IP-адреса для сетей.

Для указания диапазона адресов сети применяется команда:

```
# set range <from-address> to <to-address>
```

где

– `<from-address>` –IPv4-адрес в формате `A.B.C.D`;

– `<to-address>` – IPv4-адрес в формате `A.B.C.D`.

IP-адреса в диапазоне должны принадлежать подсети, настройка которой осуществляется.

9.1.5 Настройка разделяемых сетей для динамического назначения

На уровне конфигурации `[edit service dhcp ipv4 subnet <subnet-address>]` описывается сеть, обслуживаемая одним из интерфейсов системы. Для присвоения адресов клиентам из сетей, не обслуживаемых интерфейсами системы (например, в случае использования DHCP-Relay), используется группировка сетей в разделяемые сети.

Для включения подсети в разделяемую сеть внутри subnet-секции применяется команда:

```
# set shnet <shnet-name>
```

где `<shnet-name>` – слово.

Данная команда применяется минимум в двух subnet-секциях, так как невозможно сгруппировать одну сеть в разделяемую сеть.

Пример применения команд для включения подсети в разделяемую сеть:

```
[edit service dhcp ipv4]
# edit subnet 10.0.10.0/24
[edit service dhcp ipv4 subnet 10.0.10.0/24]
# set shnet shnet1
# set range 10.0.10.2 to 10.0.10.100

[edit service dhcp ipv4]
```

```
# edit subnet 10.0.0.0/24
[edit service dhcp ipv4 subnet 10.0.0.0/24]
# set shnet shnet1
```

По умолчанию в системе настроен интерфейс en0 с адресом 10.0.0.1/24, на котором необходимо принимать запросы от клиентов из другого сегмента сети через службу dhcprelay и раздавать им адреса из сети 10.0.10.0/24. Настройки из примера выше позволяют объединить две сети в одну разделяемую и обеспечить попадание запросов, приходящих на интерфейс сети 10.0.0.0/24, в shnet1. Так как интервал адресов задан только для сети 10.0.10.0/24, адреса выделяются клиентам из этого диапазона.

Важно! Разделяемые сети создаются автоматически службой dhcp для ненастроенных в конфигурации сетей, если они принадлежат интерфейсам, обслуживающим несколько сетей. Для присоединения сети к автоматической разделяемой сети используется следующий формат именования автоматических разделяемых сетей:

```
shnet_<interface-name>
```

где `interface-name` – имя существующего интерфейса.

Например, для многосетевого интерфейса en0, если его сети не описаны в конфигурации службы и не задана их принадлежность к разделяемой сети, создается автоматическая разделяемая сеть с именем shnet_en0.

9.1.6 Настройки разделяемых сетей

Настройка разделяемой сети осуществляется на следующем уровне конфигурации (далее по тексту – разделяемо-сетевая секция):

```
[edit service dhcp ipv4 shnet <shnet-name>]
```

где `<shnet-name>` – слово.

Настройки host- или subnet-секций аналогичны настройкам разделяемой сети. Настройки разделяемой сети являются общими для всех subnet-секций, которые выходят в указанную разделяемую сеть (задаётся настройкой `shnet <shnet-name>` subnet-секции).

9.1.7 Сетевые DHCP-опции

Служба dhcp ПАК «Фортикс» позволяет передавать клиентам конфигурационную сетевую информацию (например, сетевые DHCP-опции). Настройки данного механизма указываются на любом из уровней службы: как глобально, так и в host-, сетевой- или разделяемо-сетевой секции.

Для указания IP-адреса для широковещательных запросов применяется команда:

```
# set broadcast <address>
```

где `<address>` – IPv4-адрес в формате `A.B.C.D`.

Для указания имени домена для трансляции имён через DNS применяется команда:

```
# set domain-name <domain-name>
```

где `<domain-name>` – строка длиной от 1 до 253 символов.

По данной настройке возможно указание только одного домена.

Для указания доменных имён для трансляции имён через DNS применяется команда:

```
# set search <domain-name>
```

где `<domain-name>` – строка длиной от 1 до 253 символов.

По данной настройке возможно указание нескольких доменов.

Для указания IP-адреса шлюза по умолчанию применяется команда:

```
# set gateway <address>
```

где `<address>` – IPv4-адрес в формате `A.B.C.D`.

По данной настройке возможно указание нескольких шлюзов по умолчанию.

Для указания маски подсети применяется команда:

```
# set subnet-mask <subnet-mask-address>
```

где `<subnet-mask-address>` – IPv4-адрес в формате `A.B.C.D/mask`.

Если маска подсети не указана, значение маски берётся из настройки имени сети `<subnet-address>` subnet-секции, в которую попадает запрос.

Для указания IP-адреса сервера имён применяется команда:

```
# set server dns <address>
```

где <address> – IPv4-адрес в формате A.B.C.D.

Для указания IP-адреса сервера времени применяется команда:

```
# set server ntp <address>
```

где <address> – IPv4-адрес в формате A.B.C.D.

Для указания IP-адреса WINS (NetBios) сервера применяется команда:

```
# set server wins <address>
```

где <address> – IPv4-адрес в формате A.B.C.D.

Для указания IP-адреса почтового SMTP-сервера применяется команда:

```
# set server smtp <address>
```

где <address> – IPv4-адрес в формате A.B.C.D.

Для указания IP-адреса TFTP-сервера применяется команда:

```
# set server tftp <address>
```

где <address> – IPv4-адрес в формате A.B.C.D.

Для указания доменного имени TFTP-сервера применяется команда:

```
# set server tftp-name <address>
```

где <address> – IPv4-адрес в формате A.B.C.D.

Для указания предлагаемого BOOTP-клиентам имени bootstrap-файла на BOOTP-сервере применяется команда:

```
# set boot file <boot-file-name>
```

где <boot-file-name> – слово.

Для указания размера загрузочного образа для BOOTP-клиентов применяется команда:

```
# set boot size <size-value>
```

где <size-value> – число 512-секторов.

9.1.8 Пользовательские DHCP-опции

ПАК «Фортикс» позволяет создавать пользовательские сетевые DHCP-опции, передаваемые клиентам как стандартные сетевые DHCP-опции.

Использование пользовательской опции возможно после её определения, которое осуществляется на глобальном уровне службы; использование (присвоение ей какого-либо значения) – на любых уровнях.

Для определения новой опции применяется команда:

```
[edit service dhcp ipv4]
# set user-option-def <option-name> code <option-code> type <option-type>
```

где

– `<option-name>` – слово;

– `<option-code>` – число от 128 до 254;

– `<option-type>` – тип опции (см. ниже).

П р и м е ч а н и е – Код опции принимает значения из интервала 128-254, т.к. все коды меньше 128 зарезервированы под стандартные DHCP-опции. В стандарте RFC интервал от 128 до 224 также зарезервирован под стандартные DHCP-опции, при этом не все клиенты поддерживают данный стандарт и могут использовать интервал 128-224 как пользовательский интервал опций. Рекомендуется использовать интервал кодов 224-254. Значения из интервала 128-224 допустимы для совместимости.

Предусмотрены следующие типы опции:

– `bool` – булевый тип значения опции (on, off);

– `string` – строковый тип значения опции (любая текстовая строка);

– `bytes` – бинарный тип значения опции (последовательность байт длиной до 128, байты разделяются символом «:»);

– `uint32` – целочисленный тип значения опции (любое 32-битное число);

– `ip` – тип значения опции в виде IP-адреса.

Для указания значения раннее определённой опции применяется команда:

```
# set user-option <option-name> value <option-value>
```

где

– `<option-name>` – имя существующей опции;

– `<option-value>` – строка (см. выше).

9.1.9 Прочие настройки

Для присвоения имени хоста BOOTP-клиентам (бездисковым рабочим станциям) применяется команда:

```
# set ipv4 send-hostname on|off
```

где

– `on` – включить;

– `off` – отключить (по умолчанию – `off`).

При включённой настройке для каждого объявления хоста, находящегося в зоне действия настройки, имя `<host-name>`, заданное в host-секции (см. пункт «Настройка статического назначения») передаётся клиенту в качестве его имени хоста.

Настройка определяется глобально или на уровне конфигурации хоста.

Для указания IP-адреса BOOTP-сервера (сервера, откуда загружается файл начальной загрузки – bootstrap-файл) применяется команда:

```
# set server boot address <address>
```

где `<address>` – IPv4-адрес в формате `A.B.C.D`.

Для указания bootstrap-файла на BOOTP-сервере применяется команда:

```
# set server boot file <boot-file-name>
```

где `<boot-file-name>` – слово.

9.1.10 Динамическое обновление зон DNS

Служба dhcp может обновлять динамические ресурсные записи службы dns или некоторого DNS-сервера.

Для разрешения динамического обновления зон в службе dns необходимо задать настройку `update` в DNS-зоне и, если необходимо, с помощью настройки `allow-update` указать, кому именно разрешено обновлять зону DNS (подробнее см. раздел «Служба dns»). В случае обновления зон локальной службы dns никакой дополнительной настройки в службе dhcp не требуется.

Для включения динамического обновления зон удалённого сервера DNS на стороне службы dhcp применяется команда:

```
[edit service dhcp ipv4]
# set update <dns-server-ip> zone <zone-name> [password]
```

где

– `<dns-server-ip>` – IPv4-адрес в формате `A.B.C.D`;

– `<zone-name>` – строка длиной от 1 до 253 символов в формате FQDN;

– `[password]` – строка.

Пароль для обновления зоны задаётся также и на удалённом DNS-сервере.

9.2 Служба dhcp в режиме IPv6

Протокол DHCPv6 использует понятия префикс сети и длина префикса сети:

– префиксом сети называется часть IPv6-адреса, которая задаёт адрес сети;

– длина префикса сети обозначает, какая часть IPv6-адреса является адресом сети, причём отсчёт сетевого адреса начинается слева направо (длина префикса сети может быть от 0 до 128).

В DHCPv6 также используются понятия *делегирующий роутер*, раздающий префиксы, и *запрашивающий роутер*, получающий и использующий их для назначения внутри префиксов адресов для собственных клиентов.

Служба считается настроенной и включённой для работы в режиме IPv6 по настройке `enable` в случае, если выполнено любое из следующих условий:

– не задано ни одной настройки `listen ipv4` и `listen ipv6`: служба принимает запросы на всех подходящих интерфейсах;

– задана одна или более настроек `listen ipv6`: служба принимает запросы на указанных интерфейсах.

9.2.1 Настройки принятия запросов

Аналогично настройкам службы в режиме IPv4, при этом IP-адреса указываются в формате IPv6.

9.2.2 Настройка статического назначения

Важно! Статический диапазон адресов для назначения не должен пересекаться с динамическим диапазоном.

Настройка статического назначения осуществляется на следующем уровне конфигурации (далее по тексту host-секция):

```
[edit service dhcp ipv6 host <host-name>]
```

где `<host-name>` – строка длиной от 1 до 253 символов.

Для привязки host-секции к идентификатору клиента `<client-id>` применяется команда:

```
# set host-id <client-id>
```

где `<client-id>` – строка.

Клиент использует уникальный идентификатор DHCP (DUID) для получения IP-адреса и других настроек от сервера DHCPv6. Фактическая длина DUID зависит от его типа. Первые 16 бит DUID содержат один из следующих типов DUID (см. RFC 3315):

– адрес уровня ссылки и время;

– присвоенный поставщиками уникальный идентификатор;

– адрес уровня ссылки.

Значение оставшихся бит зависит от типа.

Для указания статического IPv6-адреса клиента применяется команда:

```
# set ip <address>
```

где `<address>` – IPv6-адрес в формате `A:B:..:H`.

Для использования делегирования префикса применяется команда:

```
# set prefix <net-address>
```

где `<net-address>` – IPv6-адрес в формате `A:B:..:H/mask`.

9.2.3 Настройка динамического назначения

Важно! Статический диапазон адресов для назначения не должен пересекаться с динамическим диапазоном.

Аналогично настройкам службы в режиме IPv4, при этом IP-адреса указываются в формате IPv6.

Для настройки делегирования префиксов в subnet-секции применяется команда:

```
# set prefix <start-prefix> end <end-prefix> len <prefix-length>
```

где

– `<start-prefix>` – IPv6-адрес в формате `A:B:..:H`;

– `<end-prefix>` – IPv6-адрес в формате `A:B:..:H`;

– `<prefix-length>` – IPv6-адрес в формате `A:B:..:H`.

В команде задаётся начальный `<start-prefix>` и конечный `<end-prefix>` IPv6-адрес внутри сети subnet-секции, а также длина префикса `<prefix-length>` для данного интервала адресов.

9.2.4 Сетевые DHCP-опции

Для указания IP-адреса сервера имён применяется команда:

```
# set server dns <address>
```

где `<address>` – IPv6-адрес в формате `A:B:..:H`.

Для указания IP-адреса сервера времени NTP применяется команда:

```
# set server ntp <address>
```

где `<address>` – IPv6-адрес в формате `A:B:..:H`.

Для указания домена для трансляции имён через DNS применяется команда:

```
# set search <domain-name>
```

где `<domain-name>` – строка.

По данной настройке возможно указание нескольких доменов.

Некоторые DHCP-клиенты отправляют DHCP-сообщения, например, RELEASE, методом Unicast. Для разрешения обработки службой Unicast-сообщений от локального DHCP-клиента при динамических обновлениях локального DNS-сервера применяется команда:

```
# set unicast
```

Данная настройка по-умолчанию включена для службы. Если включить настройку для некоторой секции службы (например, subnet), действие настройки ограничивается данной секцией. Таким образом, можно избирательно включать разрешение Unicast-сообщений только для определённых секций службы dhcp. Для других секций в таком случае запрещаются принятие и обработка Unicast-сообщений клиентов.

Для указания длины префикса в процессе делегирования префиксов службой применяется команда:

```
# set ia-prefix <ia-prefix-length>
```

где `<ia-prefix-length>` – число от 0 до 128.

Примечание – Данная настройка задаётся службой автоматически и не требует явного указания администратором.

Для указания FQDN клиента в процессе динамического DNS-обновления зон применяется команда:

```
# set fqdn <fqdn-name>
```

где `<fqdn-name>` – строка длиной от 1 до 253 символов.

Примечание – Данная настройка задаётся службой автоматически и не требует явного указания администратором.

Для определения значения промежутка времени, сообщаемого клиентам, использующим Information-request сообщения, через которое им следует снова запросить у сервера сетевые параметры (настройки), применяется команда:

```
# set timeout info-refresh <timeout-info-refresh-value>
```

где `<timeout-info-refresh-value>` – число секунд.

9.2.5 Пользовательские DHCP-опции

Аналогично настройкам службы в режиме IPv4.

9.2.6 Связь с DNS (динамическое обновление)

Аналогично настройкам службы в режиме IPv4.

9.3 Команды режима администрирования

Для просмотра текущего статуса службы dhcp (корректность внутренней конфигурации, состояние сервиса и корректность базы данных аренды) для режимов IPv4 и IPv6 применяется команда:

```
> show service dhcp status
```

Для просмотра информации по выбранным адресам (все – `all`, действующие – `active`, свободные – `free`, указанный адрес – `<address>`) применяется команда:

```
> show service dhcp lease ipv4|ipv6 [all|active|free|<address>]
```

Формат выходных данных:

```
HOST:<host-name> (<status>)
IP:<address> MAC:<mac> <start-date>-<end-date>
```

где

– `<host-name>` – имя хоста клиента, полученное из его DHCP-запроса (может отсутствовать, т.к. протокол DHCP не требует его передачи);

– `<status>` – статус адресной информации: `free` – свободная, `active` – занятая;

– `<address>` – арендованный IP-адрес;

– `<mac>` – MAC-адрес клиента;

– `<start-date>` – время начала срока аренды адреса в формате `YYYY/MM/DD/HH:MM:SS`;

– `<end-date>` – время окончания срока аренды адреса в формате `YYYY/MM/DD/HH:MM:SS`.

9.3.1 Команды удаления данных

Для прекращения аренды указанного IP-адреса (всех адресов, если адрес не указан) применяется команда:

```
> service dhcp ipv4|ipv6 lease remove [<address>]
```

где `<address>` – IP-адрес.

10 Служба dhcprelay

Служба dhcprelay ПАК «Фортикс» является ретранслятором DHCP-сообщений.

Настройка службы dhcprelay осуществляется на следующем уровне конфигурации:

```
[edit service dhcprelay]
```

Служба работает в режиме IPv4, IPv6 или в обоих одновременно.

10.1 Служба dhcprelay в режиме IPv4

Служба считается настроенной и включённой по настройке `enable`, в случае если выполнена команда:

```
# set listen ipv4 server
```

10.1.1 Основные настройки

Для определения интерфейса, на котором ожидаются запросы DHCP-клиентов или DHCP-агентов, применяется команда:

```
# set listen ipv4 from interface <interface-name>
```

где `<interface-name>` – имя существующего интерфейса.

Для определения интерфейса, на котором ожидаются ответы DHCP-серверов или DHCP-агентов, применяется команда:

```
# set listen ipv4 to interface <interface-name>
```

где `<interface-name>` – имя существующего интерфейса.

По умолчанию – все широковещательные интерфейсы.

Для определения IP-адреса сервера DHCP применяется команда:

```
# set ipv4 server <address>
```

где `<address>` – IPv4-адрес в формате `A.B.C.D`.

10.1.2 Дополнительные настройки

Для добавления к DHCP-запросу идентификатора службы, состоящего из Circuit ID (имя аппаратного порта получения запроса) и Remote ID (MAC-адрес интерфейса получения запроса), применяется команда:

```
# set ipv4 send-relay-options
```

Данная настройка является DHCP Опцией 82 (настройка протокола DHCP, применимая для информирования DHCP-сервера о DHCP-ретрансляторе и номере порта, через которые был получен запрос; применяется при решении задач привязки IP-адреса к порту коммутатора и для защиты от атак с использованием протокола DHCP).

Для отбрасывания ответов DHCP-серверов, содержащих чужую Опцию 82 (идентификаторы в Опции 82, несоответствующие идентификаторам службы) применяется команда:

```
# set ipv4 drop-alien-replies
```

Для настройки максимального числа узлов, через которые может пройти DHCP-пакет до отбрасывания службой, применяется команда:

```
# set ipv4 max-hops <max-hops>
```

где `<max-hops>` – число от 0 до 255, по умолчанию – 10.

Для настройки максимального размера DHCP-пакета (вместе с Опцией 82), который служба может ретранслировать, применяется команда:

```
# set ipv4 max-packet-size <max-packet-size>
```

где `<max-packet-size>` – число байт, по умолчанию – 576.

Для определения действий по отношению к входящим DHCP-пакетам, которые уже содержат Опцию 82 (т.е. пришли от других relay-агентов), применяется команда:

```
# set ipv4 alien-opts append|replace|forward|discard
```

где

– `append` – добавить свои идентификаторы к Опции 82;

– `replace` – заменить своими идентификаторами уже имеющиеся в Опции 82 (по умолчанию);

– `forward` – отправить Опцию 82 без изменений;

– `discard` – отбросить чужую Опцию 82.

10.2 Служба dhcprelay в режиме IPv6

Служба считается настроенной и включённой по настройке `enable`, в случае если выполнены команды:

```
# set listen ipv6 from interface
```

и

```
# set listen ipv6 to interface
```

10.2.1 Основные настройки

Для определения интерфейса (и его адреса), на котором служба ожидает запросы клиентов или других ретрансляторов DHCPv6, применяется команда:

```
# set listen ipv6 from interface <interface-name> [ip <address>]
```

где

– `<interface-name>` – имя существующего интерфейса;

– `<address>` – IPv6-адрес в формате `A:B:..:H`.

Если IP-адрес в команде не задан, используется первый найденный не Link-local адрес интерфейса.

Для определения интерфейса (и его адреса), на который служба перенаправляет запросы клиентов или других ретрансляторов DHCPv6, применяется команда:

```
# set listen ipv6 to interface <interface-name> [ip <address>]
```

где

– `<interface-name>` – имя существующего интерфейса;

– `<address>` – IPv6-адрес в формате `A:B:..:H`.

Если IP-адрес в команде не задан, используется адрес FF02::1:2 (All_DHCP_Relay_Agents_and_Servers).

10.2.2 Дополнительные настройки

Для отправки DHCPv6-опции Interface-Id (идентификация интерфейса) применяется команда:

```
# set send-iface-id
```

Настройка по данной команде применяется также при наличии нескольких интерфейсов, на которых было получено сообщение от клиента.

Для определения максимального числа узлов, через которые может пройти DHCPv6-пакет до отбрасывания службой, применяется команда:

```
# set max-hops <max-hops-number>
```

где <max-hops-number> – число от 0 до 255, по умолчанию – 10.

10.3 Примеры

В данном подразделе приведён пример настройки сети, указанной на рисунке 2.

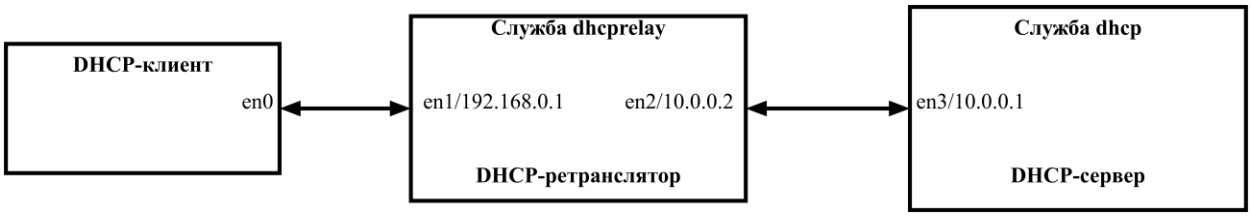

Рисунок 2 – Пример настройки dhcprelay.

Интерфейсы en0,en1 - обслуживают клиентскую сеть.

Интерфейсы en2,en3 - обслуживают сеть сервера.

Минимальная настройка службы dhcp-relay на узле «DHCP-ретранслятор»:

```
# [edit service dhcp-relay]
# set ipv4 server 10.0.0.1
# set listen ipv4 from interface en1
# set listen ipv4 to interface en2
# set enable
```

Минимальная настройка службы dhcp на узле «DHCP-сервер»:

```
# [edit service dhcp]
# set listen ipv4 address 10.0.0.1
# set ipv4 shnet relay
# set ipv4 subnet 10.0.0.0/24 shnet relay
# set ipv4 subnet 192.168.0.0/24 shnet relay range 192.168.0.10 to 192.168.0
.100
# set enable
# [edit] router unicast ipv4 to 192.168.0.0/24 via gw 10.0.0.2
```

Последней командой задаётся маршрут в клиентскую сеть через узел DHCP-ретранслятора.

11 Служба dns

11.1 Общие сведения

Служба dns – иерархическая и распределённая служба имён, которая обеспечивает систему именования компьютеров, служб и других ресурсов в сети Интернет или других сетях Интернет-протокола (IP). В ПАК «Фортикс» служба dns обеспечивает функциональность узла службы DNS.

11.2 Базовые настройки службы

Настройка службы dns ПАК «Фортикс» осуществляется по иерархическому принципу: верхний уровень является обязательными для вложенных уровней ниже.

Всего таких уровня три:

1) глобальный уровень конфигурации службы;

2) уровень конфигурации представления – `view`;

3) уровень конфигурации зоны – `zone`.

Абстракция `view` введена для «виртуализации» функциональности сервиса DNS в рамках одного процесса. С практической точки зрения каждое представление `view` работает как отдельный экземпляр службы dns. Таким образом, возможно, например, описать одну и ту же зону в зависимости от сети, из которой был сделан запрос.

11.2.1 Глобальные настройки службы

Глобальная настройка службы dns осуществляется на следующем уровне конфигурации:

```
[edit service dns]
```

На данном уровне конфигурации доступны следующие настройки:

– `enable` – включить службу;

– `acl <acl-name> address <address>` – задать именованный список IP-адресов и сетей для использования в других настройках в качестве подстановки, где `<acl-name>` – строка, `<address>` – IPv4-адрес в формате `A.B.C.D[/mask]` или IPv6-адрес в формате `A:B:..:H[/mask]`;

– `listen <address>|<acl-name>` – задать список IP-адресов или список `acl`, по которым служба принимает запросы, где `<address>` – IPv4-адрес в формате `A.B.C.D` или IPv6-адрес в формате `A:B:..:H`, `<acl-name>` – имя существующего списка IP-адресов и сетей;

– `dnssec-validation yes|no|auto` – включить/выключить проверку dnssec;

– `allow-query <address>|<acl-name>` – задать список IP-адресов или список `acl` узлов сети, с которых разрешено получение DNS-запросов, где `<address>` – IPv4-адрес в формате `A.B.C.D` или IPv6-адрес в формате `A:B:..:H`, `<acl-name>` – строка;

– `allow-transfer <address>|<acl-name>` – задать список IP-адресов или список `acl`, которым доступны зоны с сервера, где `<address>` – IPv4-адрес в формате `A.B.C.D` или IPv6-адрес в формате `A:B:..:H`, `<acl-name>` – строка;

– `allow-recursion <address>|<acl-name>` – задать список IP-адресов или список `acl`, для которых разрешены рекурсивные запросы (для остальных – итеративные), где `<address>` – IPv4-адрес в формате `A.B.C.D` или IPv6-адрес в формате `A:B:..:H`, `<acl-name>` – имя существующего списка IP-адресов и сетей, по умолчанию сервер выполняет рекурсивные запросы для всех сетей;

– `allow-notify <address>|<acl-name>` – задать список IP-адресов или список `acl` первичных серверов зоны, от которых служба, как вторичный уполномоченный сервер, принимает извещения об изменениях зоны, где `<address>` – IPv4-адрес в формате `A.B.C.D` или IPv6-адрес в формате `A:B:..:H`, `<acl-name>` – имя существующего списка IP-адресов и сетей;

– `allow-update <address>|<acl-name>` – задать список IP-адресов или список `acl`, определяющий системы, которым разрешено динамически обновлять primary-зону, где `<address>` – IPv4-адрес в формате `A.B.C.D` или IPv6-адрес в формате `A:B:..:H`, `<acl-name>` – имя существующего списка IP-адресов и сетей;

– `forwarder <address>|<acl-name>` – задать список IP-адресов или список `acl`, которые обслуживают перенаправленные запросы, где `<address>` – IPv4-адрес в формате `A.B.C.D` или IPv6-адрес в формате `A:B:..:H`, `<acl-name>` – имя существующего списка IP-адресов и сетей.

11.2.2 Настройки представления view

Настройка представления осуществляется на следующем уровне конфигурации:

```
[edit service dns view <view-name>]
```

где `<view-name>` – строка.

На данном уровне конфигурации доступны следующие настройки:

– `match-client <address>|<acl-name>` – определить представление пространства имён DNS для заданного подмножества IP-адресов клиента, где `<address>` – IPv4-адрес в формате `A.B.C.D` или IPv6-адрес в формате `A:B:..:H`, `<acl-name>` – имя существующего списка IP-адресов и сетей;

– `match-destination <address>|<acl-name>` – определить представление пространства имён DNS для заданного подмножества IP-адресов назначения, где `<address>` – IPv4-адрес в формате `A.B.C.D` или IPv6-адрес в формате `A:B:..:H`, `<acl-name>` – имя существующего списка IP-адресов и сетей;

– `match-recursive-only true|false` – определить, обслуживает ли представление только рекурсивные запросы.

Настройки `allow-notify`, `allow-query`, `allow-recursion`, `allow-transfer`, `allow-update`, `forwarder` данного уровня конфигурации аналогичны глобальному уровню конфигурации службы.

11.2.3 Настройки зоны zone

Настройка зоны осуществляется на следующем уровне конфигурации:

```
[edit service dns view <view-name> zone <zone-name>]
```

где

– `<view-name>` – имя существующего представления;

– `<zone-name>` – строка-доменное имя, оканчивающаяся на «.».

На данном уровне конфигурации доступны следующие настройки:

– `type <zone-type>` – задать один из типов зоны: `primary`, `secondary`, `forward`;

– `origin <domain-name>` – задать доменное имя, которое добавляется к любым неквалифицированным записям, где `<domain-name>` – строка, оканчивающаяся на «.»;

– `ttl <ttl-value>` – определить TTL по умолчанию для всех записей в текущей зоне, где `<ttl-value>` – число 0 до 4294967295;

– `sign` – подписать зону;

– `update` – разрешить обновление зоны DHCP-сервером.

Настройки `allow-notify`, `allow-query`, `allow-transfer`, `allow-update`, `forwarder` аналогичны уровню конфигурации представления.

11.2.4 Пример конфигурации службы dns

Пример минимальной конфигурации службы dns:

```
dns {
  enable
  dnssec-validation no
  forwarder 1.1.1.1
  view default {
    zone 100.168.192.in-addr.arpa. {
      type primary
      soa {
        domain 100.168.192.in-addr.arpa.
        master gw.example.com.
        admin admin.gw.example.com.
        serial 1
      }
      ns 100.168.192.in-addr.arpa. server gw.example.com.
      ptr 10 host foo.example.com.
    }
    zone example.com. {
      type primary
      origin example.com.
      soa {
        domain example.com.
        master gw.example.com.
        admin admin.gw.example.com.
        serial 1
      }
      ns example.com. server gw.example.com.
      a foo address 192.168.100.10
      a gw address 192.168.100.254
    }
  }
  allow-query 192.168.100.0/24
}
```

11.2.5 Команды режима администрирования

Для просмотра текущего статуса службы dns применяется команда:

```
> show service dns status
```

11.3 DNSSEC

11.3.1 Глобальные настройки службы

– `dnssec-validation` – включить/выключить проверку dnssec;

12 Служба conntrack

Служба conntrack предназначена для отслеживания и передачи информации о сетевых соединениях между узлами.

Настройка службы conntrack осуществляется на следующем уровне конфигурации:

```
[edit service conntrack]
```

12.1 Общие настройки

Для определения размера хэш-таблицы, используемой для хранения информации о соединениях, применяется команда:

```
# set hash-size <hash-size-value>
```

где `<hash-size-value>` – число от 1 до 4294967295.

Примечание – Увеличение размера хэш-таблицы позволяет улучшить производительность при значительном количестве соединений и увеличивает объём используемой памяти.

Для ограничения количества записей в хэш-таблице применяется команда:

```
# set hash-limit <hash-limit-number>
```

где `<hash-limit-number>` – число от 1 до 4294967295.

Если количество записей превышает параметр-значение настройки `hash-limit`, новые соединения отбрасываются, что позволяет предотвратить переполнение памяти в системах со значительным количеством соединений.

Для определения размера буфера, используемого при отправке сообщений через Netlink, применяется команда:

```
# set netlink-buff-size <netlink-buff-size-value>
```

где `<netlink-buff-size-value>` – число байт от 1 до 4294967295.

Примечание – Увеличение размера буфера позволяет улучшить производительность и увеличивает объём используемой памяти.

При обнаружении службой потери netlink-сообщений размер буфера удваивается автоматически.

Для определения максимального размера буфера, до которого он может быть увеличен, применяется команда:

```
# set netlink-buff-size-max-growth <netlink-buff-size-max-growth-value>
```

где <netlink-buff-size-max-growth-value> – число байт от 1 до 4294967295.

Для настройки перезапуска процесса синхронизации при переполнении буфера применяется команда:

```
# set netlink-overrun-resync <netlink-overrun-resync-value>|off|on
```

где

– on – процесс синхронизации перезапустится автоматически при переполнении буфера;

– off – процесс синхронизации продолжит работу, что может привести к снижению производительности из-за невозможности обработки некоторых сообщений;

– <netlink-overrun-resync-value> – процесс синхронизации перезапускается с указанным интервалом (число секунд от 1 до 4294967295).

Для использования надёжной доставки событий Netlink применяется команда:

```
# set netlink-events-reliable
```

Если настройка задана, события отправляются надёжно, что может увеличить задержку, но уменьшит вероятность потери событий. Если команда не задана, события отправляются без гарантий доставки, что может уменьшить задержку, но увеличит вероятность потери событий.

Для определения частоты опрашивания соединения на предмет изменений применяется команда:

```
# set poll-secs <poll-secs-value>
```

где <poll-secs-value> – число секунд от 1 до 4294967295.

Данная настройка применима для оптимизации производительности при уменьшении количества опрашиваемых соединений.

Для ограничения количества итераций при обработке событий применяется команда:

```
# set event-iteration-limit <event-iteration-limit-number>
```

где <event-iteration-limit-number> – число от 1 до 4294967295.

Если количество итераций превышает заданное ограничение, обработка событий прекращается. Данная настройка применима для предотвращения зацикливания при обработке определённых типов событий.

12.2 Протоколы синхронизации

Служба conntrack поддерживает 3 протокола (режима) синхронизации:

– FTFW (Fast Track Forward) – режим, основанный на надёжном протоколе, отслеживающем сообщения, данный протокол может восстанавливать состояние таблицы отслеживания соединений после потери, изменения порядка и повреждения сообщений;

– ALARM – режим, использующийся для оповещения о новых соединениях или изменениях в существующих соединениях (применим для мониторинга сетевой активности или обнаружения подозрительной деятельности), данный протокол потребляет много трафика, при этом быстро решает проблемы синхронизации;

– NOTRACK – режим, при котором новые соединения не отслеживаются (применим при необходимости снизить нагрузку на систему или при отсутствии необходимости в отслеживании всех соединений), данный протокол основан на постоянной репликации сообщений (отправляет и получает информацию о состоянии таблицы соединений без выполнения какой-либо специальной проверки).

Для работы службы необходимо выбрать и, при необходимости, настроить один из них.

Для активации режима синхронизации применяется команда:

```
# set mode ftfw|alarm|notrack
```

где `ftfw|alarm|notrack` – режим работы (см. выше).

12.2.1 Настройки режима FTFW

Настройка протокола FTFW осуществляется на следующем уровне конфигурации:

```
[edit service conntrack ftfw-setting]
```

Для определения количества подтверждений, которое может быть потеряно до того, как служба начнёт отправлять повторные подтверждения, применяется команда:

```
# set ack-window-size <ack-window-size-number>
```

где `<ack-window-size-number>` – число от 1 до 4294967295.

Для определения промежутка времени, в течение которого служба ожидает подтверждения успешного восстановления сессий, применяется команда:

```
# set commit-timeout <commit-timeout-value>
```

где `<commit-timeout-value>` – число секунд от 1 до 4294967295.

Если подтверждение не получено в течение заданного времени, сессии удаляются.

Для отключения использования внешнего кэш применяется команда:

```
# set disable-external-cache
```

Для настройки времени очистки кэш таблицы соединений при переходе узла из основного состояния в резервное применяется команда:

```
# set purge-timeout <purge-timeout-value>
```

где `<purge-timeout-value>` – число секунд от 1 до 4294967295.

Данная настройка применима для очистки таблицы отслеживания соединений от неактивных записей и предотвращения конфликтов со старыми записями.

При полном заполнении очереди отправки новые события ставятся в очередь повторной отправки до тех пор, пока для их отправки не появится достаточно места. Такой механизм предотвращает потерю событий в случае проблем с сетью или других сбоев.

Для определения максимальной длины очереди повторной отправки применяется команда:

```
# set resend-queue-size <resend-queue-size-value>
```

где `<resend-queue-size-value>` – число от 1 до 4294967295.

Для включения синхронизации данных при запуске службы применяется команда:

```
# set startup-resync
```

12.2.2 Настройки режима ALARM

Настройка протокола ALARM осуществляется на следующем уровне конфигурации:

```
[edit service conntrack alarm-setting]
```

Для настройки периода времени, в течение которого служба сохраняет информацию о сетевом подключении в своем кэш, применяется команда:

```
# set cache-timeout <cache-timeout-value>
```

где `<cache-timeout-value>` – число секунд от 1 до 4294967295.

По истечении указанного в настройке периода времени информация удаляется из кэша для освобождения места для новых подключений. Данный механизм позволяет поддерживать управляемый размер кэша и повышать эффективность процесса отслеживания соединений.

Для настройки временного интервала, через который служба проверяет и обновляет информацию о соединениях, применяется команда:

```
# set refresh-time <refresh-time-value>
```

где `<refresh-time-value>` – число секунд от 1 до 4294967295.

Настройки `commit-timeout` и `purge-timeout` аналогичны настройкам режима FTFW.

12.2.3 Настройки режима NOTRACK

Настройка протокола NOTRACK осуществляется на следующем уровне конфигурации:

```
[edit service conntrack notrack-setting]
```

Для отключения использования внутреннего кэш применяется команда:

```
# set disable-internal-cache
```

Настройки `commit-timeout`, `disable-external-cache`, `purge-timeout` и `startup-resync` аналогичны настройкам режима FTFW.

12.3 Транспортные протоколы

Служба conntrack поддерживает 3 транспортных протокола:

– Multicast – передача информации о сетевых сессиях с помощью multicast-пакетов;

– TCP – передача информации о сетевых сессиях с помощью tcp-пакетов;

– UDP – передача информации о сетевых сессиях с помощью udp-пакетов.

Для работы службы необходимо выбрать и настроить один из них.

Для выбора протокола применяется команда:

```
# set proto multicast|tcp|udp
```

Настройка протокола осуществляется на следующем уровне конфигурации:

```
[edit service conntrack <protocol-name>-settings]
```

где `<protocol-name>` – один из транспортных протоколов: `multicast`, `tcp`, `udp`.

На уровне конфигурации протокола указываются параметры соединения для передачи информации на удалённый узел. Кроме настройки основного соединения возможно указание до трёх резервных каналов связи. Если пересылка по основному каналу невозможна, служба поочерёдно переключается на резервные каналы.

Настройка резервных каналов осуществляется на следующем уровне конфигурации:

```
[edit service conntrack <protocol-name>-settings backup-link <backup-link-name>]
```

где

– <protocol-name> – один из транспортных протоколов: multicast, tcp, udp;

– <backup-link-name> – строка.

12.3.1 Настройки протокола Multicast

Настройка протокола Multicast осуществляется на следующем уровне конфигурации:

```
[edit service conntrack multicast-setting]
```

Для включения проверки контрольных сумм сообщений применяется команда:

```
# set checksum
```

Для настройки размера буфера входящих пакетов с информацией о состояниях сессий применяется команда:

```
# set rcv-socket-buffer <rcv-socket-buffer-size>
```

где <rcv-socket-buffer-size> – число байт от 1 до 4294967295.

П р и м е ч а н и е – При малом размере буфера существует вероятность потери пакетов.

Для настройки размера буфера исходящих пакетов с информацией о состояниях сессий применяется команда:

```
# set snd-socket-buffer <snd-socket-buffer-size>
```

где <snd-socket-buffer-size> – число байт от 1 до 4294967295.

П р и м е ч а н и е – При малом размере буфера существует вероятность потери пакетов.

Для настройки номера мультикаст-группы применяется команда:

```
# set group <group-number>
```

где <group-number> – число от 1 до 4294967295.

Для настройки мультикаст-адреса группы получателей применяется команда:

```
# set destination address ipv4 <address>
```

где <address> – IPv4-адрес в формате A.B.C.D.

Для настройки имени локального интерфейса системы для отправки мультикаст-сообщений применяется команда:

```
# set source interface <interface-name>
```

где <interface-name> – имя существующего интерфейса.

Для указания локального IP-адреса системы, с которого осуществляется отправка мультикаст-сообщений, применяется команда:

```
# set source address <address>
```

где <address> – IPv4-адрес в формате A.B.C.D.

12.3.2 Настройки протоколов TCP и UDP

Настройка протокола TCP осуществляется на следующем уровне конфигурации:

```
[edit service conntrack tcp-setting]
```

Настройка протокола UDP осуществляется на следующем уровне конфигурации:

```
[edit service conntrack udp-setting]
```

На данных уровнях конфигурации настройки, описанные ниже, идентичны.

Для использования проверки контрольных сумм сообщений применяется команда:

```
# set checksum
```

Для настройки размера буфера входящих пакетов с информацией о состояниях сессий применяется команда:

```
# set rcv-socket-buffer <rcv-socket-buffer-size>
```

где <rcv-socket-buffer-size> – число байт от 1 до 4294967295.

П р и м е ч а н и е – При малом размере буфера существует вероятность потери пакетов.

Для настройки размера буфера исходящих пакетов с информацией о состояниях сессий применяется команда:

```
# set snd-socket-buffer <snd-socket-buffer-size>
```

где <snd-socket-buffer-size> – число байт от 1 до 4294967295.

П р и м е ч а н и е – При малом размере буфера существует вероятность потери пакетов.

Для настройки IP-адреса получателя пакетов с информацией о состояниях сессий применяется команда:

```
# set destination address ipv4|ipv6 <address>
```

где

– `ipv4|ipv6` – уровень конфигурации IPv4/IPv6;

– `<address>` – IPv4-адрес в формате `A.B.C.D` или IPv6-адрес в формате `A:B:..:H` в зависимости от уровня конфигурации.

Для настройки IP-адреса приёма пакетов с информацией о состояниях сессий применяется команда:

```
# set listen address ipv4|ipv6 <address>
```

где

– `ipv4|ipv6` – уровень конфигурации IPv4/IPv6;

– `<address>` – IPv4-адрес в формате `A.B.C.D` или IPv6-адрес в формате `A:B:..:H` в зависимости от уровня конфигурации.

Для настройки номера порта протокола применяется команда:

```
# set port <port-number>
```

где `<port-number>` – число от 1 до 65535.

Для определения локального интерфейса системы для отправки сообщений применяется команда:

```
# set source interface <interface-name>
```

где `<interface-name>` – имя существующего интерфейса.

12.4 Фильтрация

Служба conntrack поддерживает фильтрацию пакетов с информацией о состояниях сессий. Фильтры доступны как для административного пространства (user-space), так и для пространства ядра (kernel-space).

Настройка фильтров осуществляется на следующем уровне конфигурации:

```
[edit service conntrack filter kernel|user]
```

где

– `kernel` – пространство ядра;

– `user` – административное пространство.

Предусмотрены следующие виды правил фильтрации:

– `accept` – принять информацию о сессии;

– `ignore` – игнорировать информацию о сессии.

Для фильтрации трафика для набора IP-адресов применяется команда:

```
# set accept|ignore address ipv4|ipv6 <address>
```

где

– `accept|ignore` – вид правила фильтрации;

– `ipv4|ipv6` – уровень конфигурации IPv4/IPv6;

– `<address>` – IPv4-адрес в формате `A.B.C.D[/mask]` или IPv6-адрес в формате `A:B:..:H[/mask]` в зависимости от уровня конфигурации.

Для фильтрации трафика по протоколу применяется команда:

```
# set accept|ignore proto dccp|icmp|ipv6-icmp|sctp|tcp|udp
```

где

– `accept|ignore` – вид правила фильтрации;

– `dccp|icmp|ipv6-icmp|sctp|tcp|udp` – протокол.

Для фильтрации по состоянию сессии применяется команда:

```
# set accept|ignore state close-wait|closed|established|fin-wait|last-ack|li
sten|syn-recv|syn-sent|time-wait
```

где

– `accept|ignore` – вид правила фильтрации;

– close-wait|closed|established|fin-wait|last-ack|listen|syn-recv|syn-sent|time-wait – состояние трафика.

12.5 Команды для просмотра информации

Для просмотра информации о состоянии внешнего кэш применяется команда:

```
> show service conntrack cache external
```

Для просмотра информации о состоянии внутреннего кэш применяется команда:

```
> show service conntrack cache internal
```

Для просмотра общей статистики применяется команда:

```
> show service conntrack statistics
```

Для просмотра сетевой статистики применяется команда:

```
> show service conntrack statistics network
```

Для просмотра расширенной статистики о состоянии внешнего и внутреннего кэш применяется команда:

```
> show service conntrack statistics cache
```

Для просмотра статистики о состоянии очереди применяется команда:

```
> show service conntrack statistics queue
```

Для просмотра статистики ожидания применяется команда:

```
> show service conntrack statistics expect
```

Для просмотра статистики времени выполнения применяется команда:

```
> show service conntrack statistics runtime
```

13 Служба iperf

Служба iperf предназначена для измерения производительности сети и представляет собой генератор сетевого трафика. Данная служба применима для оценки максимальной пропускной способности и задержки сетевых соединений.

Основные функции службы:

– измерение пропускной способности: служба позволяет измерить пропускную способность сети в обоих направлениях (от источника к месту назначения и наоборот);

– измерения задержки: служба позволяет измерить задержку сети для определения качества соединения;

– тестирование двунаправленной передачи: служба позволяет тестировать двунаправленную передачу данных между двумя узлами, что применимо для определения производительности в реальных сценариях;

– поддержка нескольких протоколов: служба поддерживает несколько сетевых протоколов, таких как TCP и UDP, что позволяет тестировать различные типы приложений.

Служба состоит из клиентской и серверной части.

Для измерения пропускной способности сети между двумя узлами ПАК «Фортикс» необходимо на одном узле в режиме конфигурации настроить серверную часть службы, а на другом – в режиме администрирования запустить клиентскую часть.

13.1 Настройка серверной части

Для запуска службы используется применяется команда:

```
# set service iperf enable
```

По указанной команде запущенная служба по умолчанию прослушивает 5001 порт и ожидает TCP-соединение на всех доступных IPv4-адресах.

Для прекращения работы службы применяется команда:

```
# del service iperf enable
```

Служба поддерживает следующие типы тестов:

– TCP;

– UDP;

– UDP-single.

Для выбора типа теста по умолчанию применяется команда:

```
# set service iperf listen proto tcp|udp|udp-single
```

где tcp|udp|udp-single – тип теста.

Для выбора порта по умолчанию применяется команда:

```
# set service iperf listen port <port-number>
```

где <port-number> – число от 1 до 65535.

Для определения IPv4- или IPv6-адреса, на котором запускается служба, и типа теста и/или порта для данного адреса применяется команда:

```
# set service iperf listen ipv4|ipv6 address <address> [port <port-number>]
[proto tcp|udp|udp-single]
```

где

– ipv4|ipv6 – уровень конфигурации IPv4/IPv6;

– <address> – IPv4-адрес в формате A.B.C.D или IPv6-адрес в формате A:B:...:H;

– <port-number> – число от 1 до 65535;

– tcp|udp|udp-single – тип теста.

13.2 Настройка клиентской части

Для запуска тестирования пропускной способности сети применяется команда:

```
> iperf addr <address> [port <port-number>] [tcp|udp] [<options>]
```

где

– <address> – IPv4-адрес в формате A.B.C.D или IPv6-адрес в формате A:B:...:H;

– <port-number> – число от 1 до 65535;

– tcp|udp – тип теста, по умолчанию – tcp;

– <options> – дополнительные параметры тестирования (см. ниже).

Предусмотрены следующие дополнительные параметры тестирования <options>:

– bandwidth <bandwidth-value> – указать пропускную способность, где <bandwidth-value> – целое число бит в секунду;

– buffer <buffer-size> – указать размер буфера сокета, где <buffer-size> – целое число байт;

– duplex-port <duplex-port-number> – указать номер локального порта для двунаправленного тестирования, где <duplex-port-number> – число от 1 до 65535;

– interval <interval-value> – указать интервал между повторной передачей пакетов, где <interval-value> – целое число секунд;

– mss <mss-max-size> – указать максимальный размер сегмента TCP, где <mss-max-size> – целое число байт;

– reverse – применить обратный тест (сервер выступает как передатчик, а клиентская сторона – как приёмник);

– source <address> – указать локальный IP-адрес сокета для соединения с удалённым узлом, где <address> – IPv4-адрес в формате A.B.C.D или IPv6-адрес в формате A:B:...:H;

– threads <threads-number> – указать количество потоков, где <threads-number> – целое число;

– time <time-value> – указать продолжительность одного цикла тестирования, где <time-value> – целое число секунд;

– tos <tos-type> – указать тип ToS;

– verbose – применить расширенный формат отчёта;

– window <window-size> – указать размер TCP-окна, где <window-size> – целое число байт.

14 Служба ntp

Служба ntp предназначена для обеспечения высокоточного времени на сетевых устройствах. В ПАК «Фортикс» служба применима для синхронизации локального системного времени с удалёнными NTP-серверами и в качестве сервера времени для других устройств.

Настройка службы ntp осуществляется на следующем уровне конфигурации:

```
[edit service ntp]
```

Для запуска службы применяется команда:

```
[edit service ntp]
# set enable
```

14.1 Настройка сервера времени

Для настройки службы в качестве сервера времени указывается(ются) IP-адрес(а), на котором(ых) открывается слушающий сокет.

Для указания IP-адреса для прослушивания применяется команда:

```
[edit service ntp]
# set listen ipv4|ipv6 address <address>
```

где

– `ipv4|ipv6` – уровень конфигурации IPv4/IPv6;

– `<address>` – IPv4-адрес в формате `A.B.C.D` или IPv6-адрес в формате `A:B:...:H` в зависимости от уровня конфигурации.

Для указания нескольких адресов для прослушивания команда применяется для каждого адреса отдельно.

Одним из ключевых понятий в работе серверов времени является стратум (stratum) – уровень в иерархической структуре сетевого времени NTP. Уровень присваивается каждому NTP-серверу и указывает на его расстояние от первичных источников времени: чем ниже значение уровня, тем выше точность времени, предоставляемого сервером (NTP-серверы уровня 1 имеют самую высокую точность).

Для изменения уровня сервера времени используется команда:

```
[edit service ntp]
# set stratum <stratum-value>
```

где `<stratum-value>` – число от 1 до 15, по умолчанию – 1.

14.2 Настройка синхронизации

Для синхронизации времени необходимо указать NTP-сервера, к которым осуществляется подключение.

Для указания NTP-сервера применяется команда:

```
[edit service ntp]
# set server <server-address>
```

где `<server-address>` – IPv4-адрес в формате `A.B.C.D` или IPv6-адрес в формате `A:B:...:H`.

Для указания в качестве адреса сервера FQDN-имени применяется команда:

```
[edit service ntp]
# set server <FQDN> [multi]
```

где `<FQDN>` – строка длиной от 1 до 253 символов.

Параметр `multi` указывается для осуществления попытки синхронизации со всеми адресами из пула, в несколько IP-адресов которого транслируется FQDN-имя сервера. Настройка `server` может быть задана несколько раз.

Для указания конкретного IP-адреса интерфейса, с которого осуществляется отправка исходящих запросов, применяется команда:

```
[edit service ntp]
# set query-from ipv4|ipv6 address <address>
```

где

– `ipv4|ipv6` – уровень конфигурации IPv4/IPv6;

– `<address>` – IPv4-адрес в формате `A.B.C.D` или IPv6-адрес в формате `A:B:...:H` в зависимости от уровня конфигурации.

Для обеспечения безопасности

Для определения максимально допустимого отклонения во времени, полученном от сервера, применяется команда:

```
[edit service ntp]
# set max-offset <max-offset-value>
```

где `<max-offset-value>` – число секунд от 1 до 999999.

Таким образом, если отклонение во времени на сервере превышает значение настройки, синхронизация не осуществляется.

По умолчанию при активации службы осуществляется попытка синхронизации с NTP-серверами немедленно, что может вызывать задержки.

Для отключения немедленной синхронизации и использования синхронизации в фоновом режиме применяется команда:

```
[edit service ntp]
# set no-sync
```

14.3 Диагностика

Для просмотра информации о состоянии службы применяется команда:

```
> show service ntp status
```

Пример отображения информации по команде для просмотра информации о состоянии службы:

```
> show service ntp status
1/2 peers valid, clock synced, stratum 3

peer
   wt tl st  next  poll          offset       delay      jitter
193.192.36.3
 *  1 10  2   20s   34s         0.452ms    22.330ms     1.637ms
1.1.11.1 from pool 1.1.11.1
    1  2  -    0s    0s             ---- peer not valid ----
```

Команда отображает следующую информацию о каждом NTP-сервере:

– `wt` – вес;

– `tl` – уровень доверия;

– `st` – стратум;

– `next` – количество секунд до следующего опроса;

– `pool` – интервал опроса в секундах;

– `offset` – смещение в миллисекундах;

– `delay` – задержка сети в миллисекундах;

– `jitter` – джиттер сети в миллисекундах.

В начале строки с информацией о сервере, с которым синхронизированы системные часы, отображается символ *.

15 Служба snmp

SNMP (Simple Network Management Protocol) – протокол для взаимодействия с сетевыми устройствами.

В ПАК «Фортикс» служба snmp предназначена для удаленного мониторинга состояния системы. Данная служба позволяет другим узлам сети получать информацию об устройстве и автоматически отправляет уведомления о некоторых событиях на другие устройства.

Поддерживаются следующие версии протоколов:

– SNMPv1;

– SNMPv2;

– SNMPv2c;

– SNMPv3.

15.1 Базовая настройка

Настройка службы snmp осуществляется на следующем уровне конфигурации:

```
[edit service snmp]
```

Для активации службы применяется команда:

```
[edit service snmp]
# set enable
```

По указанной команде запущенная служба по умолчанию прослушивает 161 порт и ожидает UDP-соединение на всех доступных IPv4-адресах.

Для прекращения работы службы применяется команда:

```
[edit service snmp]
# del enable
```

Служба поддерживает несколько типов протоколов: TCP, UDP, DTLSUDP и TLSTCP. DTLSUDP (Datagram Transport Layer Security/User Datagram Protocol) и TLSTCP (Transport Layer Security/Transmission Control Protocol) используются для безопасной передачи данных и обеспечивают конфиденциальность, целостность и подлинность сообщений SNMP, защищая от перехвата, изменения и подмены данных. Данные протоколы используются при настройке службы с поддержкой SNMPv3. Информация о работе службы доступна в системном журнале.

Для увеличения количества записываемых в журнал сообщений применяется команда:

```
[edit service snmp]
# set log dump
```

Для определения IPv4- или IPv6-адреса, на котором запускается служба, и типа протокола и/или порта для данного адреса применяется команда:

```
[edit service snmp]
# set listen ipv4|ipv6 address <address> [port <port-number>] [proto udp|tcp
|dtlsudp|tlstcp]
```

где

– `ipv4|ipv6` – уровень конфигурации IPv4/IPv6;

– `<address>` – IPv4-адрес в формате `A.B.C.D` или IPv6-адрес в формате `A:B:...:H` в зависимости от уровня конфигурации;

– `<port-number>` – число от 1 до 65535;

– `udp|tcp|dtlsudp|tlstcp` – тип протокола.

15.1.1 Настройка информации о системе

Для указания контакта администратора системы применяется команда:

```
[edit service snmp]
# set system contact <contact>
```

где `<contact>` – произвольная строка.

Для указания краткого описания системы применяется команда:

```
[edit service snmp]
# set system description <system-description>
```

где `<system-description>` – произвольная строка.

Для указания местоположения системы применяется команда:

```
[edit service snmp]
# set system location <system-location>
```

где `<system-location>` – произвольная строка.

Для указания имени системы применяется команда:

```
[edit service snmp]
# set system name <system-name>
```

где `<system-name>` – произвольная строка.

15.1.2 Настройка SNMPv3

В архитектуре SNMPv3 ПАК «Фортикс» для защиты сообщений используется модель защиты на основе SNMPv3-пользователей (USM). В USM применяется концепция общего SNMPv3-пользователя, для которого в системах агента и менеджера настраиваются параметры защиты (уровни защиты, протоколы идентификации и защиты данных, ключи). Для сообщений, отправляемых с использованием USM, обеспечивается более высокий уровень защиты по сравнению с сообщениями, отправляемыми с использованием модели защиты на основе сообществ, которая предполагает передачу незашифрованных паролей с возможностью их просмотра.

Важно! Имя SNMPv3-пользователя никак не связано с именем учётной записи администратора, поэтому для работы SNMPv3 необходимо выполнить отдельные настройки для SNMPv3-пользователей.

15.1.2.1 Настройка SNMPv3 engineID

Для ответа на запросы SNMPv3 необходимо определить уникальный идентификатор (`engineID`). В случае рекомендуемого подхода данный идентификатор определяется автоматически с использованием двух достаточно непредсказуемых значений — случайного числа и текущего времени в секундах. В ПАК «Фортикс» также возможно определить `engineID` другими способами.

Для определения значения `engineID` на основе первого IPv4-адреса применяется команда:

```
[edit service snmp]
# set system engine-id ipv4
```

Для определения значения `engineID` на основе первого IPv6-адреса применяется команда:

```
[edit service snmp]
# set system engine-id ipv6
```

Для определения значения `engineID` на основе мак-адреса указанного интерфейса применяется команда:

```
[edit service snmp]
# set system engine-id mac <interface-name>
```

где `<interface-name>` – имя существующего интерфейса.

Для определения значения engineID вручную применяется команда:

```
[edit service snmp]
# set system engine-id id <engine-id>
```

где <engine-id> – строка от 5 до 32 октетов в шестнадцатеричном формате, начинающаяся с 0x (например, 0x11223344AA).

15.1.2.2 Настройка SNMPv3-пользователей

В ПАК «Фортикс» для работы SNMPv3 используется модель безопасности USM (User Security Model, на основе пользователей), обеспечивающая защиту данных на нескольких этапах:

– аутентификация: обеспечивает проверку подлинности отправителя и получателя данных (поддерживаются алгоритмы аутентификации HMAC-MD5 и HMAC-SHA);

– шифрование: обеспечивает конфиденциальность передаваемых данных (поддерживаются алгоритмы шифрования: AES и DES);

– управление ключами: обеспечивает генерацию и распределение ключей для аутентификации и шифрования.

USM предусматривает 3 уровня безопасности:

– без аутентификации и шифрования;

– с использованием только аутентификации;

– с использованием аутентификации и шифрования.

Таким образом, для применения пользователей SNMPv3 на основе USM необходимо их создание и, при необходимости, настройка аутентификации и шифрования. Данные пользователи в дальнейшем применимы при настройках правил доступа и нотификаций для версии SNMPv3.

Для создания пользователя применяется команда:

```
[edit service snmp]
# set user <user-name>
```

где <user-name> – строка.

По данной команде создаётся пользователь с указанным именем без настроек аутентификации и шифрования.

Для настройки аутентификации пользователя необходимо указать алгоритм и ключ аутентификации с помощью команды:

```
[edit service snmp]
# set user <user-name> auth md5|sha key <auth-key>
```

где

– `<user-name>` – имя существующего пользователя;

– `md5|sha` – алгоритм аутентификации;

– `<auth-key>` – строка.

Для настройки аутентификации и шифрования пользователя необходимо дополнительно к настройкам аутентификации указать алгоритм и ключ шифрования с помощью команды:

```
[edit service snmp]
# set user <user-name> priv aes|des key <priv-key>
```

где

– `<user-name>` – имя существующего пользователя;

– `aes|des` – алгоритм шифрования;

– `<priv-key>` – строка.

Дополнительно, для идентификации SNMPv3-пользователя возможно указание его собственного `engineID` с помощью команды:

```
[edit service snmp]
# set user <user-name> engine-id <user-engine-id>
```

где

– `<user-name>` – имя существующего пользователя;

– `<user-engine-id>` – строка от 5 до 32 октетов в шестнадцатеричном формате, начинающаяся с 0x (например, 0x11223344AA).

Указанное в команде значение используется для отправки SNMPv3-уведомлений.

15.2 Настройка правил доступа

Для определения сообщества правила доступа, агентам и менеджерам которого настраивается полный доступ к информации о системе по протоколу SNMPv1/SNMPv2, применяется команда:

```
[edit service snmp]
# set access community <community-name> [address <address>]
```

где

– `<community-name>` – строка;

– `<address>` – диапазон IPv4- или IPv6-адресов в формате `A.B.C.D/mask` или `A:B:...:H/mask`.

По умолчания данная команда обеспечивает доступ к полному дереву OID для указанных сообществ независимо от того, откуда были отправлены запросы. Параметр `address` используется для настройки доступа конкретных источников запросов.

Для определения пользователя правила доступа, для которого настраивается полный доступ к информации о системе по протоколу SNMPv3, применяется команда:

```
[edit service snmp]
# set access user <user-name>
```

где `<user-name>` – имя существующего SNMPv3-пользователя.

Данная команда обеспечивает доступ к полному дереву OID для указанных пользователей независимо от того, откуда были отправлены запросы.

Для ограничения доступа к некоторой информации возможно расширение правил доступа при их настройке с помощью модели на основе видов VACM (View Access Control Model). В ПАК «Фортикс» VACM представляет собой списки (представления), содержащие информацию, доступ к которой разрешён или запрещён при запросе к узлу. Для настройки доступа с помощью VACM необходимо создать именованный список, содержащий необходимую информацию, а затем применить список к правилу доступа.

Для создания списка (представления) и добавления необходимой информации в него применяется команда:

```
[edit service snmp]
# set view <view-name> excluded|included <oid>
```

где

– `<view-name>` – строка;

– `excluded|included` – политика доступа к информации;

– `<oid>` – поддерево OID, содержащее информацию для указанной политики (строка).

Для применения списка к сообществу правила доступа, агентам и менеджерам которого настраивается доступ к информации о системе по протоколу SNMPv1,SNMPv2, применяется команда:

```
[edit service snmp]
# set access community <community-name> address <address> view <view-name>
```

где

– `<community-name>` – строка;

– `<address>` – диапазон IPv4- или IPv6-адресов в формате `A.B.C.D/mask` или `A:B:...:H/mask`;

– `<view-name>` – имя существующего списка (представления).

Для применения списка к пользователю правилу доступа, для которого настраивается доступ к информации о системе по протоколу SNMPv3, используется команда:

```
[edit service snmp]
# set access user <user-name> view <view-name>
```

где

– `<user-name>` – имя существующего SNMPv3-пользователя;

– `<view-name>` – имя существующего списка (представления).

15.3 Настройка уведомлений

Служба snmp поддерживает отправку уведомлений (нотификаций) другим узлам об изменениях состояния системы.

Для настройки отправки уведомлений версии SNMPv1 или SNMPv2 необходимо указать имя сообщества и адрес для отправки уведомлений, при этом по умолчанию используется порт

162, транспортный протокол UDP и версия уведомлений v2c. Для изменения параметров по умолчанию при настройке уведомления дополнительно указываются номер порта, тип (версия) уведомления и транспортный протокол.

Для настройки уведомлений версии SNMPv1/SNMPv2 применяется команда:

```
[edit service snmp]
# set notify community <community-name> [type v1|v2|v2c port <port-number> p
roto tcp|udp] address <address>
```

где

– `<community-name>` – имя существующего сообщества;

– `<address>` – IPv4-адрес в формате `A.B.C.D` или IPv6-адрес в формате `A:B:...:H`;

– `<port-number>` – число от 1 до 65535;

– `tcp|udp` – тип транспортного протокола;

– `v1|v2|v2c` – тип (версия) уведомления.

Для настройки SNMPv3-уведомлений необходимо указать имя настроенного SNMPv3-пользователя и адрес для отправки, при этом по умолчанию используется порт 162, транспортный протокол UDP и версия нотификаций inform. Для изменения параметров по умолчанию при настройке уведомлений указывается номер порта, тип уведомления и транспортный протокол.

Для настройки SNMPv3-уведомлений применяется команда:

```
[edit service snmp]
# set notify user <user-name> [type trap|inform port <port-number> proto tcp
|udp] address <address>
```

где

– `<user-name>` – имя существующего SNMPv3-пользователя;

– `<address>` – IPv4-адрес в формате `A.B.C.D` или IPv6-адрес в формате `A:B:...:H`;

– `<port-number>` – число от 1 до 65535;

– `tcp|udp` – тип транспортного протокола;

– `trap|inform` – тип уведомления.

Некоторые уведомления (такие как запуск, остановка службы) отправляются автоматически.

Для настройки отправки уведомлений о включении/отключении интерфейса (с указанной частотой опроса интерфейсов для отслеживания состояния) применяется команда:

```
[edit service snmp]
# set trap iface [freq <freq-value>]
```

где <freq-value> – число секунд от 1 до 3600.

Для настройки отправки уведомлений при неудачной аутентификации SNMP-клиента применяется команда:

```
[edit service snmp]
# set trap auth
```

16 Служба ssh

Служба ssh предназначена для поддержки сетевого протокола SSH, который обеспечивает аутентификацию и шифрование данных для удалённого доступа и управления, что позволяет исключить подслушивание трафика, перехват соединения и другие атаки.

Данная служба применима для предоставления безопасного доступа к узлам через защищённые каналы. По умолчанию служба использует TCP-порт 22 для связи между клиентом и сервером. Кроме того, служба предоставляет большой набор возможностей безопасного соединения, несколько методов аутентификации и широкие параметры конфигурации.

Служба состоит из серверной части, которая служит для предоставления удалённого доступа другим узлам в сети, и клиентской части, которая предоставляет инструменты для подключения к удалённым узлам, операций с файлами на этих узлах.

Для идентификации узла, на котором запущена служба у других клиентов, необходимо присутствие асимметричной ключевой пары на нём. Данная пара генерируется автоматически и не требует настройки администратором.

Настройка службы ssh осуществляется на следующем уровне конфигурации:

```
[edit service ssh]
```

16.1 Настройка серверной части

Для активации службы и обеспечения возможности удалённого подключения к узлу необходимо запустить службу.

Для запуска службы применяется команда:

```
[edit service ssh]
# set enable
```

По данной команде служба настраивается на приём SSH-соединений на всех интерфейсах через TCP-порт 22.

Для изменения номера порта прослушивания по умолчанию применяется команда:

```
[edit service ssh]
# set listen port <port-number>
```

где `<port-number>` – число от 1 до 65535.

Для настройки прослушивания соединений на указанных IP-адресах (и портах) интерфейсов применяется команда:

```
[edit service ssh]
# set listen ipv4|ipv6 address <address> [port <port-number>]
```

где

– ipv4|ipv6 – уровень конфигурации IPv4/IPv6;

– <address> – IPv4-адрес в формате A.B.C.D или IPv6-адрес в формате A:B:...:H в зависимости от уровня конфигурации;

– <port-number> – число от 1 до 65535.

Параметр port является необязательным. Если в команде параметр не задан, используется значение номера порта по умолчанию.

Для настройки прослушивания соединений на всех IPv4-адресах применяется команда:

```
[edit service ssh]
# set listen ipv4 address 0.0.0.0 [port <port-number>]
```

где <port-number> – число от 1 до 65535.

Параметр port является необязательным. Если в команде параметр не задан, используется значение номера порта по умолчанию.

Для настройки прослушивания соединений на всех IPv6-адресах применяется команда:

```
[edit service ssh]
# set listen ipv6 address :: [port <port-number>]
```

где <port-number> – число от 1 до 65535.

Параметр port является необязательным. Если в команде параметр не задан, используется значение номера порта по умолчанию.

16.1.1 Настройка контроля доступа

По умолчанию служба предоставляет доступ извне ко всем учётным записям администраторов, за исключением учётной записи администратора root, которая является служебной. Для предоставления удалённого доступа к учётной записи root применяется команда:

```
[edit service ssh]
# set access root-login
```

В службе ssh предусмотрены несколько режимов аутентификации: с использованием пароля и с использованием ключевой информации (без пароля). По умолчанию активированы оба режима работы. Для отключения аутентификации с использованием паролей и применения только аутентификации по ключам применяется команда:

```
[edit service ssh]
# set access no-password
```

В службе реализованы различные настройки для обеспечения контроля доступа: возможно указание учётных записей и IP-адресов, с которых разрешено или запрещено удалённое управление. Кроме того, при определении имени учётной записи поддерживаются шаблоны, по которым осуществляется проверка на соответствие правилу доступа. Шаблон может содержать символ «*» для обозначения набора символов любой длины, в том числе нулевой, и символ «?» для обозначения одного символа. При отсутствии IP-адреса в настройке правило применяется для любого адреса.

Для разрешения доступа с указанной учётной записи (и IP-адреса) применяется команда:

```
[edit service ssh]
# set access allow login <user-name> [address <address>]
```

где

– `<user-name>` – строка;

– `<address>` – IPv4-адрес в формате `A.B.C.D[/mask]` или IPv6-адрес в формате `A:B:...:H[/mask]`.

По данной команде предоставляется доступ для указанных учётных записей. Если указан IP-адрес (диапазон адресов, указанный с помощью маски), он также проверяется на соответствие правилу. Подключение учётных записей, которые не соответствуют правилу, отклоняется.

Для запрета доступа с указанной учётной записи (и IP-адреса) применяется команда:

```
[edit service ssh]
# set access deny login <user-name> [address <address>]
```

где

– `<user-name>` – строка;

– `<address>` – IPv4-адрес в формате `A.B.C.D[/mask]` или IPv6-адрес в формате `A:B:...:H[/mask]`.

По данной команде предоставляется доступ для всех учётных записей, за исключением указанных в команде.

Важно! Приоритет команды `deny` выше приоритета команды `allow`. Если используется команда `allow`, доступ предоставляется только указанным учётным записям (и адресам).

Важно! Команды `allow` и `deny` являются наиболее приоритетными при настройке контроля доступа, поэтому для предоставления доступа с учётной записи администратора `root` необходимо использовать команду `access root-login` совместно с указанными командами – добавить разрешающее правило для учётной записи администратора `root` с помощью команд:

```
[edit service ssh]
# set access root-login
# set access allow login root
```

16.1.2 Списки доступа

Для осуществления контроля доступа также применимы списки соответствий (доступа). Список может содержать шаблоны имён учётных записей или IP-адресов, для которых разрешён доступ. Для списков возможно отключение аутентификации с использованием паролей. Имена списков используются исключительно для удобства администрирования.

Настройка списков доступа осуществляется на следующем уровне конфигурации:

```
[edit service ssh access match-list <match-list-name>]
```

где `<match-list-name>` – строка.

Для добавления шаблона имени учётной записи в список применяется команда:

```
[edit service ssh access match-list <match-list-name>]
# set user <pattern>
```

где `<pattern>` – строка.

Для добавления шаблона адреса удалённого узла в список применяется команда:

```
[edit service ssh access match-list <match-list-name>]
# set host <pattern>
```

где `<pattern>` – строка.

Для отключения аутентификации с использованием пароля для подключений, соответствующих списку, применяется команда:

```
[edit service ssh access match-list <match-list-name>]
# set no-password
```

16.1.2.1 Настройка параметров соединения

Служба ssh позволяет контролировать некоторые параметры уже установленного соединения.

Для определения тайм-аута ожидания сервером (службой ssh) сигнала от клиента применяется команда:

```
[edit service ssh]
# set access alive-interval <alive-interval-value>
```

где <alive-interval-value> – число секунд от 0 до 4294967295.

Если в течение указанного времени клиент не отправляет сигнал, служба закрывает соединение.

Для определения максимального количества попыток повторной передачи данных применяется команда:

```
[edit service ssh]
# set access alive-count <alive-count-value>
```

где <alive-count-value> – число от 0 до 4294967295.

16.1.2.2 Настройка параметров беспарольного доступа

Для настройки беспарольного доступа используются открытые ключи. Для предоставления доступа без пароля к ПАК «Фортикс» необходимо добавить открытый ключ удалённого узла в настройки учётной записи в системе.

Настройка беспарольного доступа осуществляется в режиме конфигурации системы. Возможно указание как значения открытого ключа удалённого узла, с которого осуществляется подключение, так и файла, содержащего открытый ключ.

Для добавления значения ключа в настройки учётной записи применяется команда:

```
# setup login <user-name> ssh-pubkey text <ssh-pubkey-text>
```

где

– <user-name> – имя существующей учётной записи;

– <ssh-pubkey-text> – строка.

Для добавления файла, содержащего открытый ключ удалённого узла, в настройки учётной записи применяется команда:

```
# setup login <user-name> ssh-pubkey file <ssh-pubkey-file-path>
```

где

– `<user-name>` – имя существующей учётной записи;

– `<ssh-pubkey-file-path>` – полное имя файла или имя файла относительно домашней директории пользователя.

Для предоставления ПАК «Фортикс» беспарольного доступа к удалённому узлу необходимо сгенерировать на ПАК «Фортикс» ключевую пару (открытый и закрытый ключ), а затем добавить на удалённый узел полученный открытый ключ.

Для генерации ключевой пары применяется команда:

```
> ssh key generate [dsa|rsa|ecdsa] [comment <comment-text>]
```

где

– `dsa|rsa|ecdsa` – алгоритм шифрования (по умолчанию – `rsa`);

– `<comment-text>` – строка.

Необязательный параметр `comment` указывается для записи описания в файл открытого ключа.

16.1.3 Настройка алгоритмов

Служба поддерживает настройку алгоритмов шифрования, аутентификации (MAC), обмена ключей (KEX) и алгоритмов ключей хоста.

Для настройки использования указанного алгоритма шифрования в режиме конфигурации службы применяется команда:

```
[edit service ssh]
# set algo cipher <algorithm-cipher> true|false
```

где `<algorithm-cipher>` – алгоритм шифрования (см. ниже).

Доступные алгоритмы шифрования:

– `des3-cbc` – по умолчанию отключён;

– `aes128-cbc` – по умолчанию отключён;

– `aes192-cbc` – по умолчанию отключён;

– aes256-cbc – по умолчанию отключён;

– aes128-ctr – по умолчанию включён;

– aes192-ctr – по умолчанию включён;

– aes256-ctr – по умолчанию включён;

– aes128-gcm-openssh.com – по умолчанию включён;

– aes256-gcm-openssh.com – по умолчанию включён;

– chacha20-poly1305-openssh.com – по умолчанию включён.

Для настройки использования указанного алгоритма аутентификации применяется команда:

```
[edit service ssh]
# set algo mac <algorithm-mac> true|false
```

где <algorithm-mac> – алгоритм аутентификации (см. ниже).

Доступные алгоритмы аутентификации:

– hmac-sha1 – по умолчанию включён;

– hmac-sha1-96 – по умолчанию отключён;

– hmac-sha2-256 – по умолчанию включён;

– hmac-sha2-512 – по умолчанию включён;

– hmac-md5 – по умолчанию отключён;

– hmac-md5-96 – по умолчанию отключён;

– umac-64-openssh.com – по умолчанию включён;

– umac-128-openssh.com – по умолчанию включён;

– hmac-sha1-etm-openssh.com – по умолчанию включён;

– hmac-sha1-96-etm-openssh.com – по умолчанию отключён;

– hmac-sha2-256-etm-openssh.com – по умолчанию включён;

– hmac-sha2-512-etm-openssh.com – по умолчанию включён;

– hmac-md5-etm-openssh.com – по умолчанию отключён;

– hmac-md5-96-etm-openssh.com – по умолчанию отключён;

– umac-64-etm-openssh.com – по умолчанию включён;

– umac-128-etm-openssh.com – по умолчанию включён.

Для настройки использования указанного алгоритма обмена ключей применяется команда:

```
[edit service ssh]
# set algo kex <algorithm-kex> true|false
```

где <algorithm-kex> – алгоритм обмена ключей (см. ниже).

Доступные алгоритмы обмена ключей:

– curve25519-sha256 – по умолчанию включён;

– curve25519-sha256-libssh.org – по умолчанию включён;

– diffie-hellman-group1-sha1 – по умолчанию отключён;

– diffie-hellman-group14-sha1 – по умолчанию отключён;

– diffie-hellman-group14-sha256 – по умолчанию включён;

– diffie-hellman-group16-sha512 – по умолчанию включён;

– diffie-hellman-group18-sha512 – по умолчанию включён;

– diffie-hellman-group-exchange-sha1 – по умолчанию отключён;

– diffie-hellman-group-exchange-sha256 – по умолчанию включён;

– ecdh-sha2-nistp256 – по умолчанию включён;

– ecdh-sha2-nistp384 – по умолчанию включён;

– ecdh-sha2-nistp521 – по умолчанию включён;

– sntrup761x25519-sha512-openssh.com – по умолчанию отключён.

Для настройки использования указанного алгоритма формирования ключей хоста применяется команда:

```
[edit service ssh]
# set algo host-key <algorithm-host-key> true|false
```

где <algorithm-host-key> – алгоритм формирования ключей хоста.

Доступные алгоритмы формирования ключей хоста:

– ssh-ed25519 – по умолчанию включён;

– ssh-ed25519-cert-v01-openssh.com – по умолчанию включён;

– sk-ssh-ed25519-openssh.com – по умолчанию включён;

– sk-ssh-ed25519-cert-v01-openssh.com – по умолчанию включён;

– ssh-rsa – по умолчанию отключён;

– rsa-sha2-256 – по умолчанию включён;

– rsa-sha2-512 – по умолчанию включён;

– ssh-dss – по умолчанию отключён;

– ecdsa-sha2-nistp256 – по умолчанию включён;

– ecdsa-sha2-nistp384 – по умолчанию включён;

– ecdsa-sha2-nistp521 – по умолчанию включён;

– sk-ecdsa-sha2-nistp256-openssh.com – по умолчанию включён;

– ssh-rsa-cert-v01-openssh.com – по умолчанию отключён;

– rsa-sha2-256-cert-v01-openssh.com – по умолчанию включён;

– rsa-sha2-512-cert-v01-openssh.com – по умолчанию включён;

– ssh-dss-cert-v01-openssh.com – по умолчанию отключён;

– ecdsa-sha2-nistp256-cert-v01-openssh.com – по умолчанию включён;

– ecdsa-sha2-nistp384-cert-v01-openssh.com – по умолчанию включён;

– ecdsa-sha2-nistp521-cert-v01-openssh.com – по умолчанию включён;

– sk-ecdsa-sha2-nistp256-cert-v01-openssh.com – по умолчанию включён.

16.2 Команды клиентской части

Для подключения к удалённому узлу применяется команда:

```
> ssh connect <user-name> <address> [port <port-number>] [source <source-add
ress>] [vrf <vrf-name>]
```

где

– <user-name> – учётная запись удалённого узла;

– <address> – IPv4-адрес в формате A.B.C.D или IPv6-адрес в формате A:B:...:H или хост SSH-сервера удалённого узла;

– <port-number> – номер порта от 1 до 65535 SSH-сервера удалённого узла;

– <source-address> – локальный IPv4-адрес в формате A.B.C.D или IPv6-адрес в формате A:B:...:H системы, с которого осуществляется подключение;

– <vrf-name> – имя виртуальной таблицы маршрутизации (имя интерфейса).

Для копирования файлов с ПАК «Фортикс» на удалённый узел применяется команда:

```
> ssh put <local-path> <user-name> <address> [port <port-number>] [source <s
ource-address>] [vrf <vrf-name>] [<remote-path>]
```

где

– <local-path> – полное имя файла или имя файла относительно домашней директории пользователя в локальной файловой системе ПАК «Фортикс»;

– <user-name> – учётная запись удалённого узла;

– <address> – IPv4-адрес в формате A.B.C.D или IPv6-адрес в формате A:B:...:H или хост SSH-сервера удалённого узла;

– <port-number> – номер порта от 1 до 65535 SSH-сервера удалённого узла;

– <source-address> – локальный IPv4-адрес в формате A.B.C.D или IPv6-адрес в формате A:B:...:H системы, с которого осуществляется подключение;

– <vrf-name> – имя виртуальной таблицы маршрутизации (имя интерфейса);

– <remote-path> – имя файла на удалённом узле.

Для копирования файлов на ПАК «Фортикс» с удалённого узла применяется команда:

```
> ssh get <user-name> <address> <remote-path> [port <port-number>] [source <
source-address>] [vrf <vrf-name>] [<local-path>]
```

где

– <user-name> – учётная запись удалённого узла;

– <address> – IPv4-адрес в формате A.B.C.D или IPv6-адрес в формате A:B:...:H или хост SSH-сервера удалённого узла;

– <remote-path> – имя файла на удалённом узле;

– <port-number> – номер порта от 1 до 65535 SSH-сервера удалённого узла;

– <source-address> – локальный IPv4-адрес в формате A.B.C.D или IPv6-адрес в формате A:B:...:H системы, с которого осуществляется подключение;

– <vrf-name> – имя виртуальной таблицы маршрутизации (имя интерфейса);

– <local-path> – полное имя файла или имя файла относительно домашней директории пользователя в локальной файловой системе ПАК «Фортикс».

Для хранения списка известных SSH-ключей серверов в системе используется файл known_hosts, который расположен в каталоге ssh/ домашней директории администратора:

```
> ls ssh/
22.03.2024 01:16:36  known_hosts
```

Файл known_hosts используется для предотвращения атак, связанных с подменой IP-адресов. Файл содержит имя хоста, IP-адрес или ключ сервера и дату последнего обновления информации о сервере. При попытке администратора подключиться к серверу по протоколу SSH служба проверяет наличие записи для данного сервера в файле known_hosts. Если запись присутствует и устарела, служба сообщает о необходимости обновления информации о сервере.

Если запись для сервера отсутствует, служба добавляет новую запись и подключается к серверу. Для редактирования файла `known_hosts` доступны стандартные средства системы.

17 Служба telnet

Служба telnet предназначена для поддержки сетевого протокола Telnet, который предоставляет текстовый терминальный интерфейс по сети. В протоколе не предусмотрено использование шифрования или проверки подлинности данных, в связи с чем не рекомендуется его использование в сетях, не являющихся полностью контролируемыми и безопасными от перехвата трафика, для таких сетей предпочтительней протокол SSH. Таким образом, использование службы telnet, из соображений безопасности, рекомендуется только в доверенной и безопасной локальной сети, в остальных случаях для удалённого доступа следует использовать службу ssh.

По умолчанию служба telnet использует TCP-порт 23 для связи между клиентом и сервером.

Служба состоит из серверной части, которая служит для предоставления удалённого доступа другим узлам в сети, и клиентской части, которая предоставляет инструменты для подключения к удалённым узлам.

Настройка службы telnet осуществляется на следующем уровне конфигурации:

```
[edit service telnet]
```

17.1 Настройка серверной части

Для активации службы и обеспечения возможности удалённого подключения к узлу необходимо запустить службу.

Для запуска службы применяется команда:

```
[edit service telnet]
# set enable
```

По данной команде служба настраивается на приём Telnet-соединений на всех интерфейсах через TCP-порт 22.

Для изменения номера порта прослушивания по умолчанию применяется команда:

```
[edit service telnet]
# set listen port <port-number>
```

где `<port-number>` – число от 1 до 65535.

Для настройки прослушивания соединений на указанных IP-адресах интерфейсов применяется команда:

```
[edit service telnet]
# set listen ipv4|ipv6 address <address> [port <port-number>]
```

где

– ipv4|ipv6 – уровень конфигурации IPv4/IPv6;

– <address> – IPv4-адрес в формате A.B.C.D или IPv6-адрес в формате A:B:...:H в зависимости от уровня конфигурации;

– <port-number> – число от 1 до 65535.

Параметр port является необязательным. Если в команде параметр не задан, используется значение номера порта по умолчанию.

Для прослушивания соединений на всех IPv4-адресах применяется команда:

```
[edit service telnet]
# set listen ipv4 address 0.0.0.0 [port <port-number>]
```

где <port-number> – число от 1 до 65535.

Параметр port является необязательным. Если в команде параметр не задан, используется значение номера порта по умолчанию.

Для прослушивания соединений на всех IPv6-адресах применяется команда:

```
[edit service telnet]
# set listen ipv6 address :: [port  <port-number>]
```

где <port-number> – число от 1 до 65535.

Параметр port является необязательным. Если в команде параметр не задан, используется значение номера порта по умолчанию.

По умолчанию при отсутствии настройки listen служба ожидает запросы на всех адресах IPv4 и IPv6.

17.2 Команды клиентской части

Для подключения к удалённому узлу применяется команда:

```
> telnet <host-name>|<address> [port <port-number>] [source <source-address>
] [vrf <vrf-name>]
```

где

– `<host-name>` – имя удалённого узла;

– `<address>` – IPv4-адрес в формате `A.B.C.D` или IPv6-адрес в формате `A:B:...:H` Telnet-сервера удалённого узла;

– `<port-number>` – номер порта от 1 до 65535 Telnet-сервера удалённого узла;

– `<vrf-name>` – имя виртуальной таблицы маршрутизации (имя интерфейса).

18 Служба wcf

18.1 Общие сведения

Служба wcf – это HTTP(S) прокси-сервер, позволяющий фильтровать содержимое веб-ресурсов на основе списков-ограничений для различных групп пользователей сети.

Настройка данной службы осуществляется на следующем уровне конфигурации:

```
[edit service wcf]
```

На данном уровне конфигурации осуществляются настройки групп пользователей, политик, журнала службы, MITM и сетевые настройки.

18.2 Глобальный MITM и фильтр mitm

По умолчанию MITM в службе wcf отключён. Настройка MITM осуществляется двумя способами:

– через глобальный MITM;

– через фильтр mitm, применяемый к группе.

18.2.1 Настройки глобального MITM

Настройки глобального MITM позволяют включить MITM, выбрать политику проверки сертификатов сайтов на ПАК «Фортикс», указать сертификаты и ключи, используемые для MITM, указать сайты-исключения, для которых MITM не применяется.

Настройка глобального MITM осуществляется на следующем уровне конфигурации:

```
[edit service wcf mitm]
```

На данном уровне конфигурации доступны следующие настройки:

– `enable` – включить глобальный MITM;

– `root-path <file-path>` – задать путь к файлу, содержащему корневой сертификат, устанавливаемый как корневой в цепочке доверия MITM-сертификата, где `<file-path>` – полное имя файла или имя файла относительно директории `/system/wcf`;

– `root-key-path <file-path>` – задать путь к файлу, содержащему закрытый ключ корневого сертификата, указанного в настройке `root-path`, где `<file-path>` – полное имя файла или имя файла относительно директории `/system/wcf`;

– cert-keypair <file-path> – задать путь к файлу, содержащему ключевую пару, используемую в сертификатах сайтов при включённом MITM, где <file-path> – полное имя файла или имя файла относительно директории /system/wcf;

– no-mitm <file-path> – задать путь к файлу(ам) со списком(ами) сайтов/IP-адресов, для которых MITM не применяется, где <file-path> – полное имя файла или имя файла относительно директории /system/wcf, формат определения списков приведён в пункте «Правила составления списков»;

– process-site-cert check on|off – включить/отключить проверку сертификатов сайта;

– process-site-cert check-exception <file-path> – задать путь к файлу с IP-адресами/сайтами, для которых проверка сертификатов сайта не осуществляется , где <file-path> – полное имя файла или имя файла относительно директории /system/wcf.

Если для настройки process-site-cert check указан параметр off, настройка process-site-cert check-exception игнорируется.

18.2.2 Настройки фильтра mitm

Настройки фильтра mitm позволяют включить MITM для определённых групп (см. ниже) и указать сайты, для которых применяется MITM.

Настройка фильтра mitm осуществляется на следующем уровне конфигурации:

```
[edit service wcf filter mitm <filter-mitm-name>]
```

где <filter-mitm> – строка длиной от 1 до 128 символов.

На данном уровне конфигурации доступны следующие настройки:

– enable – включить фильтр mitm;

– grey-ssl-list <address>|<host-name> – указать сайт/IP-адрес, для которого применяется MITM, где <address> – IPv4-адрес в формате A.B.C.D[/mask] или IPv6-адрес в формате A:B:...:H[/mask], <host-name> – доменное имя сайта, возможно определение нескольких настроек данного уровня конфигурации.

При определении настройки grey-ssl-list и ассоциации фильтра с политикой (при условии, что глобальный MITM и фильтр mitm включены), MITM применяется **исключительно** к сайтам/IP-адресам, содержащимся в наборе пользователей группы политики.

18.3 Служба wcf как ICAP-клиент

В ПАК «Фортикс» возможно использование службы wcf как ICAP-клиента посредством режима icap. Настройка данного режима осуществляется на следующем уровне конфигурации:

```
[edit service wcf icap]
```

На данном уровне конфигурации доступны следующие настройки:

– `enable` – включить режим icap;

– `url <url-address>` – задать URL-адрес ICAP-сервера RESPMODE, где `<url-address>` – строка в формате `icap://<IP>:<PORT><optional path>`;

– `max-content-scan-size <max-content-scan-size-value>` – задать максимальный размер файлов/страниц, которые могут быть обработаны с помощью ICAP, где `<max-content-scan-size-value>` – число килобайт от 0 до 4294967295, по умолчанию – 2048.

Пример конфигурации службы wcf в режиме icap:

```
# edit service wcf
# edit icap
# set enable
# set url «icap://192.168.56.1:1344/respmod»
# diff
service {
  wcf {
+   icap {
+     enable
+     url icap://192.168.56.1:1344/respmod
+   }
  }
}
```

Если размер загружаемого на ICAP-сервер файла/страницы превышает значение аргумента настройки `max-content-scan-size`, он обрезается с конца до размера, указанного в настройке. Параметр настройки `max-content-scan-size` влияет на быстродействие, так как содержимое файла/страницы заданного размера хранится в RAM ПАК «Фортикс».

ICAP-сервер получает оригинальный IP-адрес клиента (заголовок X-Client-IP) и имя группы, к которой принадлежит клиент (заголовок X-Client-Username).

При блокировке URL-адреса или файла ICAP-сервер отправляет причину блокировки со следующими заголовками:

– X-Infection-Found – время, когда файл был заражен;

– X-Response-Info – время, когда файл/URL-адрес был заблокирован из-за локальных правил ICAP-сервера.

Если данные HTTP-заголовки не отправлены ICAP-сервером, в качестве причины блокировки указывается «Unknown».

18.4 Фильтры

В службе wcf фильтром (filter) является набор списков для фильтрации или изменения содержимого HTTP-запросов. Каждый фильтр имеет имя, по которому он может быть ассоциирован с политикой (policy, см. подраздел «Политики»). С одной политикой возможно ассоциировать несколько фильтров (исключение: фильтр mitm). В этом случае содержимое фильтров объединяется и обрабатывается в том порядке, в котором они были ассоциированы с политикой в конфигурации. Подробная механика работы фильтров описана в подразделе «Алгоритм анализа http(s) трафика службой».

18.4.1 Правила составления списков

Предусмотрены следующие типы списков:

1) список IP-адресов/сайтов/URL-адресов;

2) список фраз;

3) список регулярных выражений.

18.4.1.1 Списки IP-адресов/сайтов/URL-адресов

Списки IP-адресов/сайтов/URL-адресов формируются в файлах, где каждый из IP-адресов/сайтов/URL-адресов записывается с новой строки без указания протокола (HTTP(S)).

Для группировки IP-адресов/сайтов/URL-адресов в категорию перед группируемым набором применяется конструкция:

```
#listcategory: «Category»
```

Пример группировки IP-адресов/сайтов/URL-адресов в категории:

```
#listcategory: «Category 1»
website1.com
website2.ru
we.b.ru/s/i/te
22.11.22.11
```

```
#listcategory: «Category 2»
website3.ru
website4.ru
web.com/site
```

Важно! При формировании и объединении списков необходимо учитывать механизм их объединения (см. пункт «Объединение списков»).

18.4.1.2 Списки фраз

Списки фраз формируются в файлах, где каждая фраза записывается с новой строки и ограничивается <>. Категории формируются аналогично категориям в подпункте «Списки IP-адресов/сайтов/URL-адресов».

Поиск совпадений осуществляется без учёта регистра, все знаки препинания заменяются на пробелы (или игнорируются во избежание двойных пробелов).

При указании нескольких фраз в одной строке через запятую проверяется наличие всех фраз из набора на странице/в запросе.

Для применения фильтров относительно количества вхождений искомых фраз на странице/в запросе используются накопленный и предельный веса фразы: при обнаружении фразы на странице/в запросе её накопленный вес увеличивается (отрицательное значение веса уменьшает накопленный вес); если накопленный вес превышает предельный вес фразы, страница/запрос с данной фразой блокируется. Вес указывается в <> после фразы. В случае указания нескольких фраз через запятую вес применяется ко всему набору фраз, при этом учитывается вхождение всего набора (см. пункты «Фильтр phrase» и «Фильтр search»).

Пример составления списков фраз без весов:

```
#listcategory: «Category 1»
<phrase 1>
<phrase with white space in the end >
<phrase 2>,<phrase 3>

#listcategory: «Category 2»
<phrase 4>
< Phrase with white space in the begin>
```

Пример составления списков фраз с весами:

```
#listcategory: «Category 1»
<phrase 1><80>
<phrase with white space in the end ><100>
```

```
<phrase 2><-100>
<phrase 3>,<phrase 4>,<phrase 5><200>

#listcategory: «Category 2»
<phrase 6><40>
< Phrase with white space in the begin><100>
<phrase 7><-80>
```

Важно! При формировании и объединении списков необходимо учитывать механизм их объединения (см. пункт «Объединение списков»).

18.4.1.3 Списки регулярных выражений

Списки регулярных выражений формируются в файлах, где каждое регулярное выражение начинается с новой строки и указывается в ««. Категории формируются аналогично категориям в подпункте «Списки IP-адресов/сайтов/URL-адресов».

При работе с регулярными выражениями применяется синтаксис PCRE-библиотеки (и синтаксис yang, в случае указания регулярного выражения непосредственно в конфигурации: например, для экранирования PCRE с помощью символа \ необходимо данный символ дополнительно экранировать для yang (тоже с помощью \)). При этом символ / экранировать необязательно.

Например:

```
«google.com/search\\\?client=firefox»
```

Для применения регулярных выражений с заменой применяется конструкция:

```
<regex-1>-><regex-2>
```

где

– `<regex-1>` – заменяемое регулярное выражение;

– `<regex-2>` – регулярное выражение-замена.

Пример применения регулярного выражения для отключения safe-поиска в поиске по картинкам google:

```
«(^http://[0-9a-z]+\\.google\\.[a-z]+[-/%.0-9a-z]*/images\\\?)(.*)(&?)(safe=[^&]*)->\\1\\2\\3»
```

18.4.2 Фильтр url

Фильтр url позволяет осуществлять различные действия над запросами в зависимости от хоста запроса. Настройка данного фильтра осуществляется на следующем уровне конфигурации:

```
[edit service wcf filter url <filter-url-name>]
```

где `<filter-url-name>` – строка длиной от 1 до 128 символов.

На данном уровне конфигурации доступны следующие настройки:

– `banned-list <file-path>` – указать файл со списком IP-адресов/URL-адресов/сайтов, которые блокируются без последующих проверок, где `<file-path>` – полное имя файла или имя файла относительно директории `/system/wcf`;

– `exception-list <file-path>` – указать файл со списком IP-адресов/URL-адресов/сайтов, которые пропускаются без последующих проверок, где `<file-path>` – полное имя файла или имя файла относительно директории `/system/wcf`;

– `grey-list <file-path>` – указать файл со списком IP-адресов/URL-адресов/сайтов, содержимое при запросе к которым проверяется, где `<file-path>` – полное имя файла или имя файла относительно директории `/system/wcf`;

– `semi-exception-list <file-path>` – указать файл со списком IP-адресов/сайтов, которые пропускаются без последующих проверок, если они не содержатся в списке настройки `banned-list`, где `<file-path>` – полное имя файла или имя файла относительно директории `/system/wcf`.

Пример конфигурации фильтра url:

```
# edit service wcf
# edit filter url test
# set banned-list ban1
# set banned-list /system/wcf/ban2
# set exception-list good_sites
# diff
service {
  wcf {
    filter {
+       url test {
+         exception-list good_sites
+         banned-list /system/wcf/ban2
+         banned-list ban1
+       }
    }
  }
}
```

18.4.3 Фильтр ban

Фильтр ban позволяет блокировать HTTP-запросы на основе регулярных выражений. Настройка данного фильтра осуществляется на следующем уровне конфигурации:

```
[edit service wcf filter ban <filter-ban-name>]
```

где <filter-ban-name> – строка длиной от 1 до 128 символов.

Для применения фильтра ban применяется команда:

```
# set <http-method> <regex-name> regex <regex-value>
```

где

– <http-method> – один из методов HTTP-запроса: delete, get, head, options, patch, post, put, trace;

– <regex-name> – строка длиной от 1 до 128 символов;

– <regex-value> – строка в кавычках, допустимо указание одного слова без кавычек.

Пример настройки фильтра ban:

```
[edit]
# set service wcf filter ban test get 1 regex «google.com/search\\\?client=firefox»
```

Метод connect в фильтре не предусмотрен. Для фильтрации с помощью данного метода применима настройка banned-list фильтра url.

Важно! Регулярные выражения в данном фильтре указываются без протокола HTTP(S).

18.4.4 Фильтр file-type

Фильтр file-type позволяет блокировать скачивание файлов с определённым расширением или MIME-типом. Настройка данного фильтра осуществляется на следующем уровне конфигурации:

```
[edit service wcf filter file-type <filter-file-type-name>]
```

где <filter-file-type-name> – строка длиной от 1 до 128 символов.

На данном уровне конфигурации доступны следующие настройки:

– banned-extensions <extension> – указать расширение, файлы с которым блокируются, где <extension> – строка с точкой в начале, возможно определение нескольких настроек данного уровня конфигурации;

– banned-mime <mime> – указать MIME-тип, файлы с которым блокируются, где <mime> – MIME-тип, указанный полностью (регулярные выражения, например text/*, не поддерживаются);

– trusted-download-sites <site> – указать URL-адрес/сайт/IP-адрес, для которого блокировка согласно параметрам настроек banned-mime/banned-extensions не применяется, где <site> – URL-адрес/сайт/IP-адрес, возможно определение нескольких настроек данного уровня конфигурации.

Пример конфигурации фильтра file-type:

```
# edit service wcf
# edit filter file-type test
# set banned-extensions .rar
# set banned-extensions .zip
# set banned-mime image/webp
# set trusted-download-sites web.com
# diff
service {
  wcf {
    filter {
+      file-type test {
+        banned-extensions .rar
+        banned-extensions .zip
+        banned-mime image/webp
+        trusted-download-sites web.com
+      }
    }
  }
}
```

18.4.5 Фильтр phrase

Фильтр phrase позволяет блокировать страницы по их содержимому. Настройка фильтра осуществляется на следующем уровне конфигурации:

```
[edit service wcf filter phrase <filter-phrase-name>]
```

где <filter-phrase-name> – строка длиной от 1 до 128 символов.

На данном уровне конфигурации доступны следующие настройки:

– banned-list <file-path> – указать файл со списком фраз (без веса), наличие которых приведёт к блокировке страницы, где <file-path> – полное имя файла или имя файла относительно директории /system/wcf;

– exception-list <file-path> – указать файл со списком фраз-исключений (без веса) для списка из параметра настройки banned-list (т.е. если страница блокируется по настройке banned-list, но в ней содержится фраза из списка данной настройки, блокировка к странице не применяется), где <file-path> – полное имя файла или имя файла относительно директории /system/wcf;

– weighted-list <file-path> – указать файл со списком фраз (с весами), где <file-path> – полное имя файла или имя файла относительно директории /system/wcf.

При ассоциации с одной политикой фильтров, содержащих списки фраз с весами и без, или при указании в фильтре списков, содержащих фразы с весами и без, необходимо учитывать, что фразы из списка настройки banned-list имеют положительный «бесконечный» вес, а фразы из списка настройки exception-list – отрицательный «бесконечный» вес (но больший, чем вес фраз из списка в banned-list). Таким образом, при единовременном использовании списков с весами и без, списки с весами приоритетнее.

18.4.6 Фильтр search

Фильтр search позволяет блокировать поисковый запрос по содержимому (словам). Настройка фильтра осуществляется на следующем уровне конфигурации:

```
[edit service wcf filter search <filter-search-name>]
```

где <filter-search-name> – строка длиной от 1 до 128 символов.

На данном уровне конфигурации доступны следующие настройки:

– banned-list <file-path> – указать файл со списком фраз (без веса), наличие которых приведёт к блокировке поискового запроса, где <file-path> – полное имя файла или имя файла относительно директории /system/wcf;

– exception-list <file-path> – указать файл со списком фраз-исключений (без веса) для списка из параметра настройки banned-list (т.е. если запрос блокируется по настройке banned-list, но в нём содержится фраза из списка данной настройки, блокировка к запросу не применяется), где <file-path> – полное имя файла или имя файла относительно директории /system/wcf;

– weighted-list <file-path> – указать файл со списком фраз (с весами), где <file-path> – полное имя файла или имя файла относительно директории /system/wcf;

– engine-regex <search-engine> regex <regex> – указать регулярное выражение для определения части запроса в указанной поисковой системе, к которой применяется фильтр, где <search-engine> – по умолчанию в ПАК «Фортикс» поддерживаются системы yandex, google, mail, rambler, duckduckgo, youtube, yahoo, bing, kiddle, <regex> – регулярное выражение, протокол в котором, в случае его указания, должен быть HTTP.

При ассоциации с одной политикой фильтров, содержащих списки фраз с весами и без, или при указании в фильтре списков, содержащих фразы с весами и без, необходимо учитывать, что фразы из списка в banned-list имеют положительный «бесконечный» вес, а фразы из списка в exception-list – отрицательный «бесконечный» вес (но больший, чем вес фраз из списка в banned-list). Таким образом, при единовременном использовании списков с весами и без, списки с весами приоритетнее.

Пример конфигурации фильтра search:

```
#edit service wcf
#edit filter search test
#set banned-list bad_search_words_1
#set banned-list catchy_search
#set exception-list legal_search
#set weighted-list w_search
#set engine-regex mail regex «^http://mail\\.ru/(.*?)\\&text=([^&]*)->\\2»
#diff
service {
  wcf {
    filter {
      search test {
+        banned-list bad_search_words_1
+        banned-list catchy_search
+        exception-list legal_search
+        weighted-list w_search
+        engine-regex mail {
+          regex ^http://mail\\.ru/(.*?)\\&text=([^&]*)->\\2
+        }
      }
    }
  }
}
```

18.4.7 Фильтр modify

Фильтр modify позволяет изменять запрос клиента в режиме реального времени. Настройка данного фильтра осуществляется на следующем уровне конфигурации:

```
[edit service wcf filter modify <filter-modify-name>]
```

где `<filter-modify-name>` – строка длиной от 1 до 128 символов.

На данном уровне конфигурации доступны следующие настройки:

– `redirect <regex-name> regex <regex-value>` – перенаправить клиента на другой URL-адрес согласно регулярному выражению, где `<regex-name>` – строка длиной от 1 до 128 символов, `<regex-value>` – регулярное выражение, в котором после «->« указан URL-адрес;

– `regex-replace <regex-name> regex <regex-value>` – изменить HTTP-запрос с помощью регулярного выражения, где `<regex-name>` – строка длиной от 1 до 128 символов, `<regex-value>` – регулярное выражение.

Пример конфигурации фильтра modify:

```
# edit service wcf
# edit filter modify test
# set redirect sport regex «championat.com->sports.ru»
# set regex-replace 1 «(^http://[0-9a-z]+\\.google\\.[a-z]+[-/%.0-9a-z]*/ima
ges\\?)(.*)(&?)(safe=[^&]*)->\\1\\2\\3»
```

18.4.8 Объединение списков

Объединение списков осуществляется в порядке их определения в конфигурации. Пример 1 конфигурации объединения двух списков:

```
service {
  wcf {
    filter {
       url test {
         banned-list ban2
         banned-list ban1
    }
```

Содержимое списков примера 1:

```
ban1:

#listcategory: «Category 1»
web1.com
web2.com
```

```
ban2:

site1.com
site2.ru
```

Содержимое объединения данных списков в том порядке, в котором они объявлены в конфигурации:

```
ban2 + ban1:

site1.com
site2.ru
#listcategory: «Category 1»
web1.com
web2.com
```

При данном порядке объединения списков сайты site1.com и site2.ru категории не имеют.

Пример 2 конфигурации объединения списков:

```
service {
  wcf {
    filter {
       url test {
         banned-list ban1
         banned-list ban2
    }
```

Содержимое объединения списков примера 2 в том порядке, в котором они объявлены в конфигурации:

```
ban1 + ban2:

#listcategory: «Category 1»
web1.com
web2.com
site1.com
site2.ru
```

При данном порядке объединения списков сайты site1.com и site2.ru имеют категорию «Category 1».

Данные примеры демонстрируют особенности механизма объединения списков.

18.5 Фильтр main-filter

Настройка фильтра main-filter осуществляется на следующем уровне конфигурации:

```
[edit service wcf main-filter]
```

Настройки данного уровня конфигурации повторяют настройки уровня конфигурации фильтра url со следующими дополнениями:

– `banned-regex-list <file-path>` – указать файл со списком регулярных выражений для сайтов/URL-адресов/IP-адресов, которые блокируются без последующих проверок, где `<file-path>` – полное имя файла или имя файла относительно директории `/system/wcf`;

– `exception-regex-list <file-path>` – указать файл со списком регулярных выражений для сайтов/URL-адресов/IP-адресов, которые пропускаются без последующих проверок, где `<file-path>` – полное имя файла или имя файла относительно директории `/system/wcf`.

Назначение данного фильтра см. в подразделе «Алгоритм анализа http(s) трафика службой».

18.6 Политики

Политики позволяют создавать группы пользователей и назначать им фильтры. При этом одной политике соответствует одна группа пользователей.

18.6.1 Настройки группы

Настройка группы осуществляется на следующем уровне конфигурации:

```
[edit service wcf policy group <group-name>]
```

где `<group-name>` – строка длиной от 1 до 128 символов.

По умолчанию предусмотрена группа «default», особенности настройки и назначение которой описаны в пункте «Группа default».

На данном уровне конфигурации доступны следующие настройки:

– `ban <filter-ban-name>` – указать имя(ена) фильтра(ов) ban, который(ые) должен(ы) применятся к пользователям группы, где `<filter-ban-name>` – имя существующего фильтра ban;

– `modify <filter-modify-name>` – указать имя(ена) фильтра(ов) modify, который(ые) должен(ы) применятся к пользователям группы, где `<filter-modify-name>` – имя существующего фильтра modify;

– file-type <filter-file-type-name> – указать имя(ена) фильтра(ов) file-type, который(ые) должен(ы) применятся к пользователям группы, где <filter-file-type-name> – имя существующего фильтра file-type;

– search <filter-search-name> – указать имя(ена) фильтра(ов) search, который(ые) должен(ы) применятся к пользователям группы, где <filter-search-name> – имя существующего фильтра search;

– phrase <filter-phrase-name> – указать имя(ена) фильтра(ов) phrase, который(ые) должен(ы) применятся к пользователям группы, где <filter-phrase-name> – имя существующего фильтра phrase;

– url <filter-url-name> – указать имя(ена) фильтра(ов) url, который(ые) должен(ы) применятся к пользователям группы, где <filter-url-name> – имя существующего фильтра url;

– mitm <filter-mitm-name> – указать имя фильтра mitm, который должен применятся к пользователям группы, где <filter-mitm-name> – имя существующего фильтра mitm;

– search-weight-limit <search-weight-limit-value> – указать предельный вес поискового запроса, при достижении которого запрос блокируется, где <search-weight-limit-value> – число от 0 до 65535, по умолчанию – 50;

– phrase-weight-limit <phrase-weight-limit-value> – указать предельный вес содержимого страницы, при достижении которого страница блокируется, где <weight> – число от 0 до 65535, по умолчанию – 150;

– user ip <ip> – указать IP-адрес, подсеть или диапазон IP-адресов, который принадлежит группе, где <ip> – IPv4-адрес в формате A.B.C.D/[mask] или диапазон IP-адресов в формате A.B.C.D-A.B.C.D, возможно определение нескольких настроек данного уровня конфигурации.

В аргументе настройки user ip указываются уникальные адреса/подсети/диапазоны адресов для каждой группы.

18.6.2 Аутентификация пользователей

Аутентификация пользователей осуществляется по их IP-адресам при присоединении к службе (как автоматически с помощью прозрачного режима, так и напрямую): пользователь

ассоциируется с группой, которая содержит его IP-адрес, или с группой default, если ни одна группа не содержит его IP-адрес.

18.6.3 Группа default

По умолчанию с группой default ассоциируется только фильтр main-filter. Для ассоциации других фильтров с данной группой применяются настройки следующего уровня конфигурации:

```
[edit service wcf policy group default]
```

Настройки данного уровня конфигурации повторяют настройки уровня конфигурации группы, при этом настройка `user ip` неприменима.

18.7 Алгоритм анализа http(s) трафика службой

Схема работы службы wcf с входящим трафиком (от пользователя) представлена на рисунке 3.

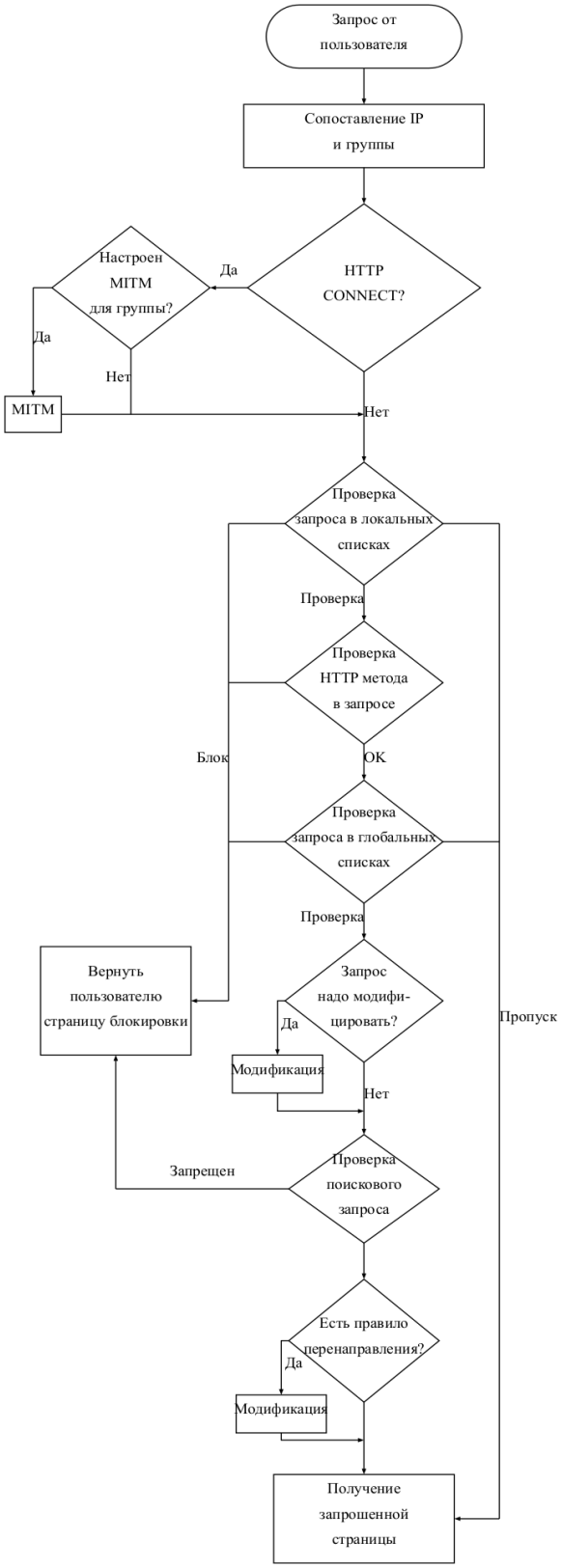

Рисунок 3 – Схема работы службы wcf с входящим трафиком от пользователя.

Схема работы службы wcf с входящим трафиком (от сайта) представлена на рисунке 4.

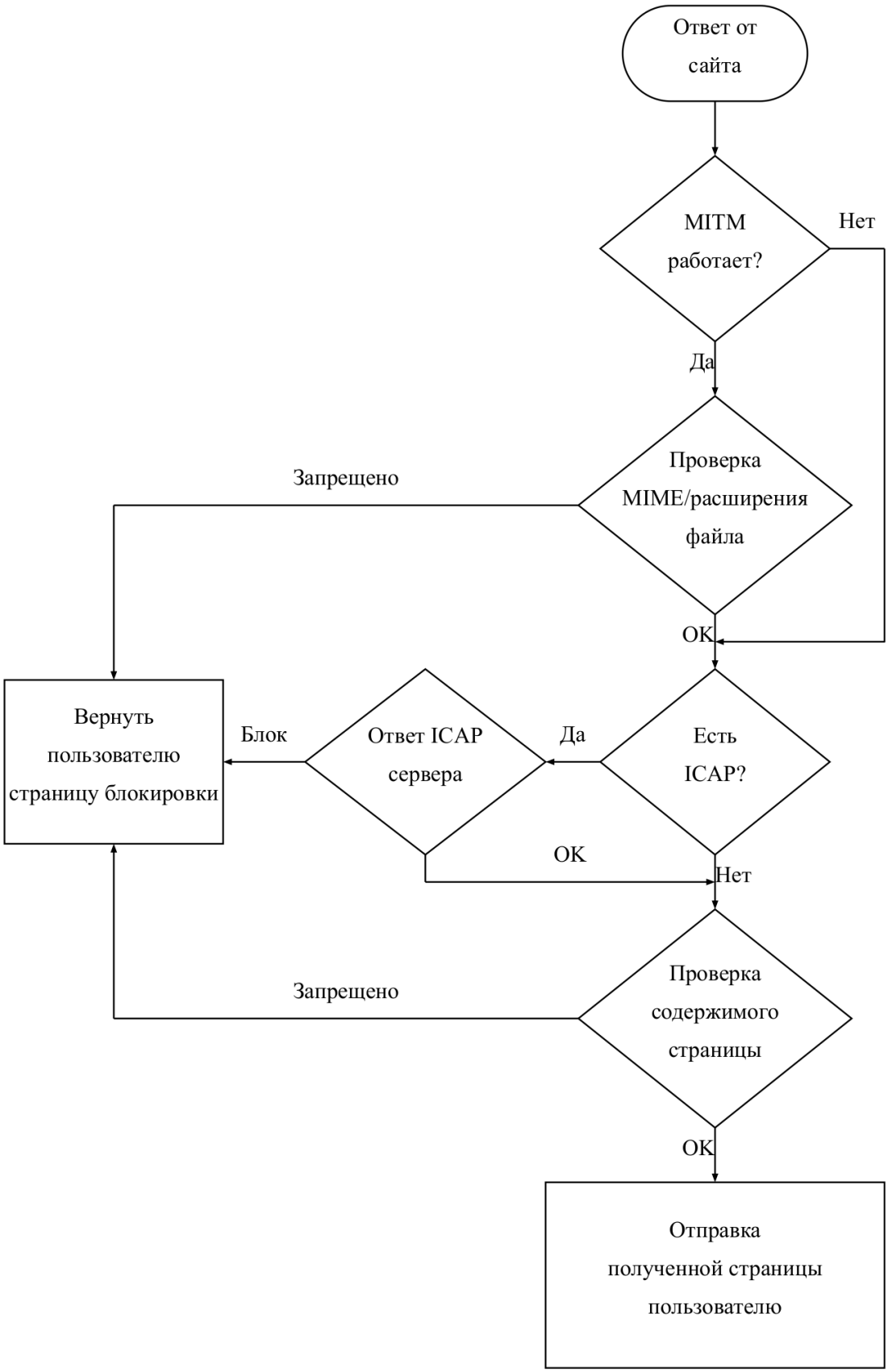

Рисунок 4 – Схема работы службы wcf с входящим трафиком от сайта.

Далее по тексту в данном подразделе HTTP-трафик и HTTPS-трафик (с включённым MITM для сайта, на который посылается запрос, у данного пользователя) называются открытым трафиком, остальные – закрытым; все фильтры url данного пользователя обозначаются одним фильтром local.

Алгоритм прохождения трафика с вышеуказанными обозначениями:

1) Если хост запроса содержится в списке semi-exception фильтра local, этапы 2, 3 пропускаются.

2) Если хост запроса содержится в списке exception фильтра local, запрос проходит без последующей проверки.

3) Если хост запроса содержится в списке grey фильтра local, страница запроса загружается и проверяется её содержимое (этапы 5 и 11).

4) Если хост запроса содержится в списке banned фильтра local, запрос блокируется без последующей проверки.

5) Запрос проверяется по фильтру(ам) ban, ассоциированным(и) с данным пользователем.

6) Если хост запроса содержится в списке semi-exception фильтра main-filter, этапы 7, 8, 9 пропускаются.

7) Если хост запроса содержится в списке exception фильтра main-filter, запрос проходит без последующей проверки.

8) Если хост запроса содержится в списке exception-regex фильтра main-filter, страница запроса проходит без последующей проверки.

9) Если хост запроса содержится в списке grey фильтра main-filter, страница запроса загружается и проверяется её содержимое (этап 12).

10) Если хост запроса содержится в списке banned фильтра main-filter, запрос блокируется без последующей проверки.

11) Если хост запроса содержится в списке banned-regex фильтра main-filter, страница запроса блокируется без последующей проверки.

12) Страница запроса загружается, и проверяется её содержимое фильтрами phrase, file-type, search, modify.

Этап, фильтр или содержимое фильтра которого не задан, пропускается.

URL-адреса из списков фильтров local и main-filter в случае закрытого трафика службе не видны.

Фильтры ban, file-type, search, modify, phrase применяются исключительно для открытого трафика.

18.8 Настройки журнала службы

Настройка журнала службы осуществляется на следующем уровне конфигурации:

```
[edit service wcf log]
```

На данном уровне конфигурации доступны следующие настройки:

– `format <format-value>` – задать формат журнала, где `<format-value>` – число от 1 до 8, по умолчанию – 7;

– `verbosity <verbosity-value>` – указать, какие сообщения от службы записываются в журнал, где `<verbosity-value>` – число от 0 до 3, по умолчанию – 1;

– `level info|warning` – указать уровень события, по умолчанию – info.

Для передачи информации об инцидентах на удалённый сервер указываются значение `warning` аргумента настройки `level` и значение `1` аргумента настройки `verbosity` в комбинации с настройками service journal.

18.9 Настройка портов и адресов службы

По умолчанию служба ожидает трафик на всех IP-адресах и на порте 8080 на данных адресах.

Настройка портов и адресов службы осуществляется на следующем уровне конфигурации:

```
[edit service wcf listen]
```

На данном уровне конфигурации доступны следующие настройки:

– `http-port <port-number>` – указать порт(ы) для приёма HTTP(S)-трафика, где `<port-number>` – число от 1 до 65535;

– `thttps-port <port>` – указать порт(ы) для приёма HTTP(S)-трафика при работе в прозрачном режиме, где `<port-number>` – число от 1 до 65535;

– `ipv4 address <address>` – указать IP-адрес(а), на которых служба ожидает трафик, где `<address>` – IPv4-адрес в формате `A.B.C.D`.

Все IP-адреса и порты, указанные в аргументах данных настроек, должны быть доступны.

Пример конфигурации портов и адресов службы:

```
# edit service wcf
# edit listen
# set http-port 8082
# set thttps-port 8143
# set ipv4 address 192.168.56.101
# diff
service {
  wcf {
+    listen {
+      ipv4 {
+        address 192.168.56.101
+      }
+      http-port 8082
+      thttps-port 8143
+    }
  }
}
```

Служба wcf работает как в прозрачном, так и в непрозрачном режиме. Для настройки прозрачного режима HTTP(S)-порты перенаправляются на порты, на которых принимает трафик служба wcf. Для HTTP-трафика (80 порт) возможно перенаправление трафика на порт, указанный в настройке `http-port <port-number>`, для HTTPS-трафика рекомендуется перенаправление на порт, указанный в настройке `thttps-port <port-number>`.

18.10 Настройка страницы блокировки

Для изменения страницы, демонстрируемой пользователям при их попытке получения доступа к нежелательной информации, в директорию `/system/wcf/ban-page/` помещается файл `template.html`, содержащий необходимую для демонстрации пользователям страницу (размер файла не может превышать 1 МБ).

На данной странице возможно указание некоторых переменных окружения, полученных из причины блокировки:

– URL – полный URL-адрес, который пользователь пытался получить;

– REASONGIVEN – краткая причина блокировки;

– REASONLOGGED – причина блокировки с детализацией;

– FILTERGROUP – имя группы пользователя;

– IP – IP-адрес пользователя;

– CATEGORIES – категория заблокированного ресурса (#listcategory).

19 Служба captive-portal

19.1 Общие сведения

Служба captive-portal (далее по тексту – портал захвата, портал) обеспечивает пограничный контроль между общедоступной локальной сетью и сетью Интернет. Данная служба поддерживает два метода обнаружения портала клиентом:

– CPD – Captive Portal Detection, обнаружение портала захвата, управляемое клиентом;

– CPI – Captive Portal Identification (см. RFC 8910), обнаружение портала захвата, управляемое службой.

Служба поддерживает следующие возможности:

– аутентификация клиентов через Radius-сервер;

– квоты использования трафика;

– правила контроля доступа.

Для настройки портала захвата предлагается следующий пример тестового стенда:

– интерфейс en0 с адресом 10.0.0.1/24 – в клиентскую сеть;

– интерфейс en1 – в сеть WAN/Интернет.

Для настройки портала захвата необходимо:

– настроить и включить службу dns, ожидающую запросы на интерфейсе `en0`;

– настроить службу dhcp с обслуживанием сети `10.0.0.0/24`, адресом DNS `10.0.0.1` и шлюзом по умолчанию `10.0.0.1`;

– настроить firewall для клиентской сети, обеспечивающий доступ в Интернет через интерфейс `en1` (например, с помощью настройки `snat masquarade`);

– настроить службу captive-portal, указав в ней интерфейс портала `en0`;

– опционально: указать FQDN портала с помощью настройки `portal-fqdn` службы captive-portal (в этом случае клиент должен уметь транслировать данное имя в IP-адрес).

При определении данных настроек запросы клиента на порт 80 (HTTP) проходят через портал, при этом клиент перенаправляется на web-страницу портала. Все остальные сетевые запросы клиента, за исключением DHCP- и DNS-запросов, блокируются до момента регистрации (с аутентификацией или без) клиента в портале.

19.2 Базовые настройки

Настройки службы captive-portal осуществляются на следующем уровне конфигурации:

```
[edit service captive-portal]
```

Для запуска службы применяется команда:

```
[edit service captive-portal]
# set enable
```

Для прекращения работы службы применяется команда:

```
[edit service captive-portal]
# del enable
```

Для указания интерфейса портала в клиентскую сеть применяется команда:

```
# set listen interface <interface-name>
```

где `<interface-name>` – имя существующего интерфейса.

На указанном интерфейсе служба ожидает входящие HTTP-запросы клиентов. Данная настройка является обязательной.

Для определения IP-адреса, принадлежащего интерфейсу портала, применяется команда:

```
# set listen ipv4 <address>
```

где `<address>` – IPv4-адрес в формате `A.B.C.D`.

По умолчанию используется IP-адрес, принадлежащий интерфейсу, указанному в настройке `listen interface`. Если у интерфейса потрала несколько адресов, указанный IP-адрес используется в качестве адреса портала.

Для определения номера порта, на котором ожидается соединение с клиентом, применяется команда:

```
# set listen port <port-number>
```

где `<port-number>` – число от 0 до 65535, по умолчанию – 2050.

Для определения полного доменного имени портала применяется команда:

```
# set portal-fqdn <domain>
```

где `<domain>` – строка длиной от 1 до 253 символов.

По умолчанию перенаправление осуществляется на IP-адрес интерфейса портала.

Данное доменное имя предлагается клиенту для перенаправления его HTTP-запросов, при этом клиент должен уметь транслировать указанное доменное имя в IP-адрес, например, через службу dns.

19.3 Настройка web-страницы портала

Для настройки внешнего вида (темы) web-страницы портала применяется команда:

```
# set theme default|none|external
```

где

– `default` – тема по умолчанию;

– `external` – внешняя тема, задаваемая администратором;

– `none` – служебная тема (применима для справочной информации при указании параметра `external`).

Для настройки внешней темы (по параметру `external`) необходимо:

– скопировать желаемые текстовые фрагменты (в виде текста или HTML-разметки) в файлы, имена которых оканчиваются на `_text`, директории `/system/captive-portal/text/`;

– скопировать желаемые файлы картинок в файлы, имена которых оканчиваются на `_image`, директории `/system/captive-portal/images/`.

Имена файлов, оканчивающиеся на `_image` и `_text`, доступны администратору на web-странице портала. Для их получения необходимо запустить портал с темой `none` или `external` (при отсутствии соответствующего файла в директории `/system/captive-portal/`)

19.4 Настройка фильтрации трафика

Для регулирования трафика, приходящего на IP-адрес портала или проходящего через портал от ещё незарегистрированных на портале клиентов, используются действия для трафика в соответсвии с правилами отбора. Предусмотрены следующие действия:

– `allow` – разрешить;

– `block` – заблокировать.

При этом в правиле отбора так же указываются:

– протокол: tcp или udp;

– номер порта;

– (опционально) IP-адрес сети назначения трафика.

По умолчанию на IP-адрес портала принимаются пакеты со следующими номерами портов:

– порт 2050 (tcp) – номер порта портала по умолчанию (или заданный по настройке `listen`);

– порт 53 (udp) – DNS-запросы на интерфейс портала, на котором может быть настроена служба dns (опционально);

– порт 67 (udp) – DHCP-запросы на интерфейс портала, на котором должна быть настроена служба dhcp.

Для обеспечения работоспособности портала указанные номера портов должны быть разрешены.

Для указания других номеров (диапазонов) портов, например для доступа по протоколу SSH на интерфейс портала, применяется команда:

```
# set acl user-to-portal allow|block protocol tcp|udp|any <port-number-1>[-port-number-2]
```

где

– `allow|block` – действие для трафика;

– `tcp|udp|any` – протокол;

– `<port-number-1>` – число от 1 до 65535;

– `[-port-number-2]` – число от 1 до 65535.

По умолчанию разрешён трафик с UDP-портов 53 и 67 и TCP-порта 2050.

Настройка портов не по умолчанию по данной команде применима только при наличии разрешающих правил для UDP-портов 53 и 67.

Для указания действия, применеяемого к проходящему через портал трафику от неаутентифицированных клиентов, применяется команда:

```
# set acl preauth-user allow|block protocol tcp|udp|any <port-1>[-port-2] [to <net>]
```

где

– `allow|block` – действие для трафика;

– `tcp|udp|any` – протокол;

– `<port-1>` – число от 1 до 65535;

– [-port-2] – число от 1 до 65535;

– <net> – IPv4-адрес в формате A.B.C.D[/mask].

Важно! Предоставление доступа к внешним DNS-серверам с помощью данной команды может привести к снижению уровня безопасности.

Создание правил для клиентов, прошедших регистрацию и аутентификацию на портале, осуществляется посредством службы firewall.

Для добавления MAC-адреса в список доверенных применяется команда:

```
# set acl trusted-mac <trusted-mac-address>
```

где <trusted-mac-address> – строка в формате xx:xx:xx:xx:xx:xx.

При выполнии данной команды клиенту с указанным в настрйоке MAC-адресом разрешается доступ к сети без аутентификации.

19.5 Настройка аутентификации

Для определения IP-адреса Radius-сервера, используемого для аутентификации клиентов портала, применяется команда:

```
# set auth radius <address> secret <secret-string>
```

где

– <address> – IPv4-адрес в формате A.B.C.D;

– <secret-string> – секретная строка для получения доступа к Radius-серверу.

Для аутентификации клиент вводит свой логин и пароль в полях web-формы портала при подключении к сети на своём устройстве. Логин и пароль должны содержаться в базе Radius-сервера.

19.6 Настройка лимитов и тайм-аутов

Для определения максимального числа клиентов портала применяется команда:

```
# set limit max-clients <limit-max-clients-number>
```

где <limit-max-clients-number> – число от 1 до 65535, по умолчанию – 250.

Для настройки интервала проверки различных ограничений службы (например, квот и тайм-аутов) применяется команда:

```
# set timeout check <timeout-check-value>
```

где `<timeout-check-value>` – число секунд, по умолчанию – 15.

Для определения тайм-аута неактивного соединения неаутентифицированных клиентов применяется команда:

```
# set timeout idle-preauth <timeout-idle-preauth-value>
```

где `<timeout-idle-preauth-value>` – число секунд, по умолчанию – 1800.

Если клиент не осуществляет попытку аутентификации в течение указанного промежутка времени, он отключается от сети.

Для определения тайм-аута неактивного соединения аутентифицированных клиентов применяется команда:

```
# set timeout idle-auth <timeout-idle-auth-value>
```

где `<timeout-idle-auth-value>` – число секунд, по умолчанию – 7200.

Если клиент не использует сеть после успешной аутентификации в течение указанного промежутка времени, он отключается от сети.

Для определения тайм-аута сессии аутентифицированных клиентов применяется команда:

```
# set timeout session <timeout-session-value>
```

где `<timeout-session-value>` – число секунд, по умолчанию – 86400.

Клиент отключается от сети по истечении указанного промежутка времени. Для настройки неограниченного времени сессии устанавливается значение 0.

19.7 Настройка квот трафика

Предусмотрена настройка квот для загрузки (download) из Интернета клиентам и для выгрузки (upload) в Интернет от клиентов.

Для определения максимальной средней скорости загрузки клиентам применяется команда:

```
# set quota download rate <download-rate-value>
```

где `<download-rate-value>` – число KB/s, по умолчанию – 0 (не ограничено).

Для определения максимального объёма данных, разрешённых для загрузки клиентам, применяется команда:

```
# set quota download size <download-size-value>
```

где `<download-size-value>` – число KB, по умолчанию – 0 (не ограничено).

Для разрешения единоличного захвата полосы пропускания канала до тех пор, пока средняя скорость загрузки не превысит значение настройки `quota download rate`, применяется команда:

```
# set quota download bursting
```

По умолчанию настройка отключена.

Для настройки значения мультипликатора для расчёта интервала проверки квот трафика применяется команда:

```
# set quota rate-check-mul <rate-check-mul-value>
```

где `<rate-check-mul-value>` – число от 1 до 255, по умолчанию – 2.

Интервал проверки квот вычисляется по формуле:

```
<timeout-check-value> * <rate-check-mul-value>
```

где

– `<timeout-check-value>` – значение аргумента настройки `timeout check`;

– `<rate-check-mul-value>` – значение аргумента настройки `quota rate-check-mul`.

Команды для настройки выгрузки в Интернет от клиентов аналогичны вышеуказанным и указываются на уровне конфигурации `quota upload` (вместо `quota download`).

19.8 Прочие настройки

Для настройки уровня журналирования службы применяется команда:

```
# set log level low|middle|high|debug
```

где `low|middle|high|debug` – уровень журналирования, по умолчанию – `middle`.

19.9 Управление службой

Для просмотра клиентов службы применяется команда:

```
> show service captive-portal clients
```

Для закрытия сессии клиента службы применяется команда:

```
> service captive-portal client logout <ip>|<mac>|<account>
```

где `<ip>|<mac>|<account>` – IP-адрес, MAC-адрес или имя пользователя, с которым клиент аутентифицирован на портале.

20 Служба journal

20.1 Общие сведения

Служба journal позволяет отслеживать и обрабатывать события в системном журнале и настраивать размер журнала на диске.

Настройка данной службы осуществляется на следующем уровне конфигурации:

```
[edit service journal]
```

20.2 Настройка размера системного журнала на диске

Журналы хранятся на диске в виде набора файлов. Для определения максимального размера всех файлов журналов на диске в совокупности применяется команда:

```
# set limits max-disk-usage <max-disk-usage-value>
```

где `<max-disk-usage-value>` – число Мбайт, по умолчанию – 10% от размера диска, но не более 4G.

Для определения максимального размера каждого файла журнала по отдельности применяется команда:

```
# set limits max-file-size <max-file-size-value>
```

где `<max-file-size-value>` – число МБайт, по умолчанию – 1/8 от значения настройки `max-disk-usage`.

Для определения максимального количества файлов журналов на диске применяется команда:

```
# set limits max-journal-files <max-journal-files-value>
```

где `<max-journal-files-value>` – число, по умолчанию – 100.

Пример настройки размера системного журнала на диске:

```
# edit service journal limits
# set max-disk-usage 4096
# set max-file-size 1
# set max-journal-files 50
```

В данном примере максимальное количество файлов журналов – 100, каждый из которых не превышает по размеру 1 МБ (т.е., если текущий журнал заполняется до 1 МБ, он ротируется; если общее количество файлов журналов превышает 100, самый старый файл журнала удаляется).

20.3 Уведомления о критичных событиях в интерфейсе командной строки

При возникновении событий уровня CRIT и выше в интерфейсе командной строки выводится уведомление в виде:

```
>

[CRIT] Lorem ipsum dolor sit amet
>
```

Для отключения данных уведомлений применяется команда:

```
# del service journal console-log-level
```

Для включения уведомлений или смены уровня событий, о которых приходит уведомление, применяется команда:

```
# set service journal console-log-level [emerg|alert|crit|err|warning|notice
|info|debug]
```

где `emerg|alert|crit|err|warning|notice|info|debug` – уровень событий.

П р и м е ч а н и е – Рекомендуется использовать уровень событий не ниже `crit`.

Для уведомлений о событиях уровня ALERT и выше:

– включается звуковой сигнал;

– в режиме конфигурации вместо знака # в командной строке отображается знак !;

– в режиме администрирования вместо знака > – >!.

Для выключения звукового сигнала применяется команда:

```
# del service journal alert-beep
```

По умолчанию настройка включена.

Для включения звукового сигнала применяется команда:

```
# set service journal alert-beep
```

Для просмотра уведомлений о событиях уровня ALERT и выше применяется команда:

```
> show alert
```

Для удаления уведомлений о событиях уровня ALERT и выше применяется команда:

```
> clear alert
```

После выполнения команд `show alert` и `clear alert` знак `!` в командной строке режима администрирования и конфигурации перестаёт отображаться и отключается звуковой сигнал, если он включён.

20.4 События в журнале и их обработка

Служба journal позволяет определять события, отслеживаемые в журнале, и действия, предпринимаемые при их возникновении.

Предусмотрены действия трёх типов:

– пересылка сообщения на удалённый сервер (`syslog-server <syslog-server-name>`);

– вызов скрипта (`script <script-name>`);

– дублирование сообщения в журнал событий СКЗИ (`crypto-log`).

Настройка событий осуществляется на следующем уровне конфигурации

```
[edit service journal event <event-name>]
```

где `<event-name>` – строка длиной от 1 до 128 символов.

На данном уровне конфигурации доступны следующие настройки:

– `facility <facility-name>` – указать категорию журнала, сообщения которого отслеживаются, где `<facility-name>` – имя syslog facility;

– `max-priority <max-priority-name>` – указать максимальный уровень приоритета журнала, сообщения которого отслеживаются, где `<max-priority-name>` – имя syslog priority;

– `min-priority <min-priority-name>` – указать минимальный уровень приоритета журнала, сообщения которого отслеживаются, где `<min-priority-name>` – имя syslog priority;

– `message-regex <regex-value>` – указать регулярное выражение для отслеживаемых сообщений, где`<regex-value>` – строка длиной от 1 до 128 символов по стандарту POSIX ERE;

– `syslogtag <syslogtag-name>` – указать тэг журнала, сообщения от которого отслеживаются, где `<syslogtag-name>` – значение поля syslog tag;

– `action <action-name>` – указать действие(я), которое(ые) предпринимаются при возникновении события, где `<action-name>` – `syslog-server <syslog-server-name>`, `script <script-name>` или `crypto-log`.

При отслеживании сообщений применяется следующее правило: между различными настройками (критериями отбора) событий действует логическое ‘И’, для настроек событий одного типа действует логическое ‘ИЛИ’.

При указании настройки `syslogtag <syslogtag-name>` отслеживаются все сообщения, начинающиеся указанного в аргументе настройки значения. Например, при указании `systemd` в качестве тэга журнала в настройке `syslogtag <syslogtag-name>` отслеживаются все `systemd*` сервисы.

Пример настройки события (без настройки `action`):

```
# edit service journal
# edit event alert_fortun
# set syslogtag fxconf
# set min-priority 5
# set regex test regex «fortun»
# exit
# diff
service {
  journal {
+    event alert_fortun {
+      min-priority 5
+      syslogtag fxconfd
+      message-regex test {
+        regex fortun
+      }
+    }
  }
}
```

20.4.1 Правила написания регулярных выражений для фильтра message-regex

При написании регулярных выражений для фильтра message-regex необходимо соблюдать следующие правила:

1) Все сообщения начинаются с пробела.

2) Символ « следует дополнительно экранировать символом \ (в этом случае при установке (`set`) настройки `regex` в регулятронном выражении перед символом « указываются три символа \).

3) Если с помощью регулярного выражения фильтруются сообщения со спецсимволами |.()[]+*$^, их следует экранировать с помощью символов \ (в этом случае при выставлении (set) regex перед спецсимволами |.()[]+*$^ указываются четыре символа \).

Примеры команд с экранированием:

```
# set message-regex test regex «^ found \\\» at the start of message»
# set message-regex test2 regex «\\\\(in brackets\\\\) i want to find (this|or_this)»
```

20.4.2 Пересылка сообщения на удалённый сервер

Настройка удалённых серверов, на которые пересылаются сообщения по настройке `action syslog-server`, осуществляется на следующем уровне конфигурации:

```
[edit service journal syslog-server <syslog-server-name>]
```

где `<syslog-server-name>` – строка длиной от 1 до 128 символов.

На данном уровне конфигурации доступны следующие настройки:

– `address ip <ip>|<host>` – указать IP-адрес удалённого сервера, где `<ip>|<host>` – IP-адрес или имя хоста;

– `address port <port-number>` – указать порт удалённого сервера, где `<port-number>` – число от 1 до 65535;

– `address protocol udp|tcp` – указать протокол передачи, где `udp|tcp` – протокол, по умолчанию – `udp`.

– `prefix <prefix-value>` – указать префикс для сообщения при пересылке, где `<prefix-value>` – строка;

– `source ip <ip-address>|<host>` – указать IP-адрес, с которого отправляются сообщения при пересылке, где `<ip>|<host>` – IPv4/IPv6-адрес или имя хоста;

– `source interface <interface-name>` – указать имя интерфейса, с которого отправляются сообщения при пересылке, где `<interface-name>` – имя существующего интерфейса.

Настройка `source ip` может быть определена только при указании настройки `address protocol udp`.

Настройка `prefix` не является обязательной. Если данная настройка не указана, сообщения пересылаются на удалённый syslog-сервер без изменений. Если данная настройка указана, записи пересылаются в следующем виде:

```
<prefix-str>: <orig-message>
```

После настройки удалённого сервера, его имя можно указывать в качестве действия `action` при настройке события `event`.

Пример настройки события (продолжение примера настройки события):

```
# edit service journal
# set syslog-server server1 address ip 192.168.56.101
# set syslog-server server1 address port 1234
# set event alert_fortun action syslog-server server 1
# diff
service {
  journal {
+    syslog-server server1 {
+      address {
+        ip 192.168.56.101
+        port 1234
+      }
+    }
+    event alert_fortun {
+      min-priority 5
+      syslogtag fxconfd
+      message-regex test {
+        regex fortun
+      }
+      action {
+        syslog-server server1
+      }
+    }
  }
}
```

20.4.3 Выполнение скрипта

Настройка скриптов, вызываемых по настройке `action script`, осуществляется на следующем уровне конфигурации:

```
[edit service journal event <event-name> action script <script-name>]
```

где

– `<event-name>` – имя существующего события `event`;

– `<script-name>` – строка длиной от 1 до 128 символов.

На данном уровне конфигурации доступны следующие настройки:

– `path <path-to-script>` – указать выполняемый скрипт, где `<path-to-script>` – полное имя файла;

– `args <args>` – аргументы скрипта, где `<args>` – слова, указанные через пробел.

Экранирование пробелов при указании аргументов осуществляется с помощью символа \ (при этом символ \ внутри yang также подлежит экранированию).

В скрипт в качестве переменной окружения передаются следующие параметры:

– JOURNAL_EVENT_COUNT – число запусков события с момента его появления после последнего выполнения скрипта и до текущего вызова;

– JOURNAL_EVENT_MESSAGE – сообщение, вызвавшее событие.

При использовании неспецифичных правил под критерии отбора может попадать большое количество сообщений, для каждого из которых вызывается скрипт. Так как скрипты могут быть различными по времени выполнения, размер очереди выполнения ограничен 32 событиями, вызванными различными сообщениями. При этом параметр JOURNAL_EVENT_COUNT увеличивается до тех пор, пока событие находится в очереди.

Для использования скриптов необходимо указать пользователя, от имени которого выполняется скрипт, с помощью команды:

```
[edit service journal]
# set script-user <account>
```

где <account> – имя существующей учетной записи.

Пример настройки скриптов (при условии существования интерфейса типа fortun):

```
# edit service journal
# set script-user admin
# set event key_exp message-regex catch regex «ifaces: Warning: private key»
# edit event key_exp
# set action script job path /system/scripts/snmp_send.lua
# set action script job args «one two three\\ four»
# commit
# show
event key_exp {
  message-regex catch regex «ifaces: Warning: private key»
  action script job path /system/scripts/snmp_send.lua
  action script job args «one two three\\ four»
}
script-user admin
# exit
# exit
# edit interface fortun test
# show
ipv4 {
  local 192.168.66.123
  remote 192.168.66.125
}
id 5
forsec-keypair {
  local-key pair1
```

```
  remote-key pair2
}
encryption
```

Содержимое скрипта, находящегося в /system/scripts/snmp_send.lua:

```
local conf1 = {
  snmptype = «trap»,
  version = «3»,
  addr = «192.168.56.1:12345»,
  sec_engine_id = «0x8000123acd1ab43abbfff000fa»,
  user = «test»,
  auth_alg = «MD5»,
  auth_key = «testsnmp»,
  privacy_alg = «DES»,
  privacy_key = «testSNMP»,
}
local message = getenv(«JOURNAL_EVENT_MESSAGE»)
local key_name = string.match(message,»'%b'«)
if ARGS[1] then
  journal(«info», ARGS[1]) -- напишется только one
end
if ARGS[3] then
  journal(«info», ARGS[3]) -- напишется three four
end
send_snmp(conf1, {«1.1.1.1.1.2.2.3.4.5»}, {«iso.3.6.1.6.3.1.1.6.2», key_name
})
```

Пример события в журнале, подходящего под критерии отбора из примера выше:

```
апр 19 10:53:45 Fortics fxconf[3544]: ifaces: Warning: private key 'pair1' i
s expired!
```

После выполнения указанного скрипта на сервер поступает следующий сигнал SNMP-trap (ниже указан вывод snmptrapd):

```
2024-04-19 13:53:47 <UNKNOWN> [UDP: [192.168.56.101]:35686->[192.168.56.1]:1
2345]:
iso.3.6.1.6.3.1.1.4.1.0 = OID: iso.1.1.1.1.2.2.3.4.5    iso.3.6.1.6.3.1.1.6.
2 = STRING: «'pair1'«
```

20.4.4 Дублирование сообщения в журнал событий СКЗИ

Настройка дублирования осуществляется на следующем уровне конфигурации:

```
[edit service journal event <name-event> action crypto-log]
```

где <name-event> – имя существующего события event.

На данном уровне конфигурации доступна следующая настройка:

– `prefix <prefix-value>` – указать префикс для сообщения при дублировании в журнал событий СКЗИ, где `<prefix-value>` – строка.

Настройка не является обязательной. Если данная настройка не указана, сообщения дублируются в журнал событий СКЗИ без изменений. Если данная настройка указана, записи дублируются в виде:

```
<prefix-str>: <orig-message>
```

где

– `<prefix-str>` – префикс длч сообщения;

– `<orig-message>` – дублируемое сообщение.

Для сообщений из категории журнала `local7` дублирование сообщений в журнал СКЗИ неприменимо.

Пример настройки дублирования:

```
# edit service journal event test
# set message-regex catch regex «.*»
# set facility authpriv
# set action crypto-log prefix «Prefix»
# commit
# show
facility authpriv
message-regex catch regex .*
action crypto-log prefix Prefix
```

Пример события в журнале, подходящего под критерии отбора из примера выше:

```
фев 07 13:53:15 Fortics sshd-session[5581]: pam_unix(sshd:session): session
opened for user root(uid=0) by (uid=0)
```

Пример дублированного сообщения в журнале событий СКЗИ по указанным выше настройкам:

```
root@Fortics> show crypto log
2025-02-07 13:53:15 : Prefix:  pam_unix(sshd:session): session opened for us
er root(uid=0) by (uid=0)
```

Пример удаления настройки `prefix`:

```
# edit service journal event test
# del action crypto-log prefix
# commit
# show
facility authpriv
```

```
message-regex catch regex .*
action crypto-log
```

Пример события в журнале, подходящего под критерии отбора из примера выше:

```
фев 07 13:58:48 Fortics sshd-session[5581]: pam_unix(sshd:session): session
closed for user root
```

Пример дублированного сообщения в журнале событий СКЗИ при удалённой настройке `prefix`:

```
root@Fortics> show crypto log
2025-02-07 13:58:48 :  pam_unix(sshd:session): session closed for user root
```

20.5 Просмотр журнала

Для просмотра журнала применяется команда:

```
> show journal
```

Для фильтрации вывода указываются следующие опции:

– `boot 0|<negative-number>|<positive-number>` – вывести указанную загрузку, где `0` – текущая загрузка, `<negative-number>` – отрицательное число (прошлые загрузки, например `-1` – предыдущая), где `<positive-number>` – положительное число (начальные загрузки, присутствующие в журнале, например `1` – самая первая загрузка);

– `service <service-name>` – вывести сообщения указанной службы, где `<service-name>` – имя службы;

– `facility <facility-name>` – вывести сообщения указанной категории журнала, где `<facility>` – имя syslog facility;

– `priority <priority-name>` – вывести сообщения указанной уровня приоритета, где `<priority>` – имя syslog priority;

– `format <format-name>` – указать формат вывода журнала, где `<format-name>` – json, plain, режим выводимого времени;

– `lines <lines-number>` – вывести указанное количество последних строк журнала, где `<lines-number>` – число;

– `search <search-string>` – выделить в выводе команды сообщения, содержащие указанную строку, где `<search-string>` – строка;

– `list-boots` – вывести информацию о загрузках устройства;

– `kernel` – вывести сообщения ядра;

– `reverse` – вывести сообщения в обратном порядке (сверху – новые, снизу – старые);

– since <yyyy-mm-dd hh:mm:ss> – вывести сообщения начиная с указанной даты;

– until <yyyy-mm-dd hh:mm:ss> – вывести сообщения до указанной даты;

– size – вывести размер журнала (текущего и архивированных);

– utc – вывести время в формате UTC;

– follow – вывести журнал в интерактивном режиме.

Доступно единовременное использование нескольких опций из вышеуказанных.

Пример вывода команды для просмотра журнала:

```
> show journal service wcf lines 10
Jun 19 07:15:35 Fortics e2guardian[907]: Check the group that e2guardian run
s as (wcf)
Jun 19 07:15:35 Fortics systemd[1]: Started WCF service.
Jun 19 07:15:35 Fortics e2guardian[914]: master: Started successfully.
Jun 20 08:29:17 Fortics systemd[1]: Starting WCF service...
Jun 20 08:29:17 Fortics e2guardian[909]: Unable to getgrnam(): Success
Jun 20 08:29:17 Fortics e2guardian[909]: Unable to getgrnam(): Success
Jun 20 08:29:17 Fortics e2guardian[909]: Check the group that e2guardian run
s as (wcf)
Jun 20 08:29:17 Fortics e2guardian[909]: Check the group that e2guardian run
s as (wcf)
Jun 20 08:29:17 Fortics systemd[1]: Started WCF service.
Jun 20 08:29:17 Fortics e2guardian[919]: master: Started successfully.
```

20.6 Очистка журнала

Для очистки журнала в режиме администрирования применяется команда:

```
> service journal clear
```

Для данной команды возможно указание следующих опций:

– time <time-value> – удаление событий, произошедших ранее указанного периода, где <time-value> – строка в формате n(s|m|h|days|weeks|years|months), где n – число, s – секунды, m – минуты, h – часы, days – дни, weeks – недели, years – годы, months – месяцы;

– size <size-value> – очистка журнала до указанного размера, где <size-value> – строка в формате n(K|M|G), где n – число, K – Кбайты, M – Мбайты, G – Гбайты.

Если никакие опции в команде не указаны, очищается весь журнал.

Пример применения команд для очистки журнала:

```
> service journal clear time 2days

> service journal clear size 100M
```

20.7 Проверка целостности журнала

В ПАК «Фортикс» реализована возможность проверки целостности журнала за счёт проверки корректности структуры двоичных файлов журнала и свёрки хэшей. В случае, если в журналах обнаружены ошибки, администратор может игнорировать их или очистить данные журналы.

Для проверки целостности файлов журнала применяется команда:

```
> service journal verify
```

Перед файлами журнала, успешно прошедшими проверку, выводится `PASS:`.

Пример вывода команды для проверки целостности файлов журнала в случае успешного прохождения проверки всеми файлами:

```
> service journal verify
PASS: /log/journal/8768c0a72e9b479ba5beb45880f8e9f3/system@d1b49a459bfb4a8da
0721025bcc44ca7-000000000000075c-00062c491ba6919e.journal
PASS: /log/journal/8768c0a72e9b479ba5beb45880f8e9f3/system@d1b49a459bfb4a8da
0721025bcc44ca7-0000000000000001-00062c49195cb2ec.journal
PASS: /log/journal/8768c0a72e9b479ba5beb45880f8e9f3/system@00062bee841167e0-
3832fd4329d459c9.journal~
PASS: /log/journal/8768c0a72e9b479ba5beb45880f8e9f3/system.journal
PASS: /log/journal/8768c0a72e9b479ba5beb45880f8e9f3/system@00062c4919679642-
f6fba473abdc3043.journal~
```

В случае неуспешного прохождения проверки выводится причина ошибки и перед повреждённым файлом выводится `FAIL:`.

Пример вывода команды для проверки целостности файлов журнала в случае неуспешного прохождения проверки:

```
> service journal verify
0015e0: Invalid data hash table hash table item (49369/178318): head_hash_of
fset=000000 tail_hash_offset=220000
0015e0: Invalid object contents: Bad message
File corruption detected at /log/journal/ea96a9058961432fab9c25ae20da5e6a/sy
stem@f3fa1fe5da904a39b55e64da94b7d5f2-0000000000006ffa-00062c4903c8d5ec.jour
nal:0015e0 (of 5175480 bytes, 0%).
FAIL: /log/journal/ea96a9058961432fab9c25ae20da5e6a/system@f3fa1fe5da904a39b
55e64da94b7d5f2-0000000000006ffa-00062c4903c8d5ec.journal (Bad message)
PASS: /log/journal/ea96a9058961432fab9c25ae20da5e6a/system@f3fa1fe5da904a39b
55e64da94b7d5f2-0000000000006a39-00062c48ea69c34f.journal
PASS: /log/journal/ea96a9058961432fab9c25ae20da5e6a/system@f3fa1fe5da904a39b
55e64da94b7d5f2-00000000000003a6-00062be3a82af550.journal
PASS: /log/journal/ea96a9058961432fab9c25ae20da5e6a/system@f3fa1fe5da904a39b
55e64da94b7d5f2-0000000000000001-00062be3a7c77551.journal
```

```
PASS: /log/journal/ea96a9058961432fab9c25ae20da5e6a/system.journal
PASS: /log/journal/ea96a9058961432fab9c25ae20da5e6a/system@f3fa1fe5da904a39b
55e64da94b7d5f2-0000000000000abb-00062be4c96dfdd4.journal
```

21 Служба scheduler

21.1 Общие сведения

Служба scheduler позволяет планировать выполнение скриптов через равные промежутки времени.

Настройки данной службы осуществляются на следующем уровне конфигурации:

```
[edit service scheduler]
```

21.2 Настройка пользователя

Для указания учетной записи, от имени которой выполняются скрипты, применяется команда:

```
# set script-user <script-user-name>
```

где `<account>` – имя существующей учётной записи.

21.3 Настройка события

Настройки событий осуществляются на следующем уровне конфигурации:

```
[edit service scheduler event <event-name>]
```

где `<event-name>` – строка длиной от 1 до 128 символов.

На данном уровне конфигурации доступны следующие настройки:

– `timer <w:m:h:d:M>` – указать периодичность выполнения скрипта, где `w` – день недели в числовом формате (1 – понедельник, 2 – вторник, и т.д.), `m` – число минут от 0 до 59, `h` – число часов от 0 до 23, `d` – число дней от 1 до 31, `M` – число месяцев от 1 до 12, применимы значение `*`, означающее «любой», перечисления, диапазоны;

– `script path <path-to-script>` – указать скрипт, `<path>` – полное имя файла;

– `script args <args-value>` – указать аргументы скрипта, где `<args>` – слова, указанные через пробел.

Экранирование пробелов при указании аргументов осуществляется с помощью символа \ (при этом символ \ внутри yang также подлежит экранированию).

Примеры настройки периодичности выполнения скрипта:

– *:15:10:10,15-17:11 – 10,15,16,17 ноября в 10:15;

– 3:*:*:*:* – каждую среду в 00:00;

– 2:*:12,17:19:9 – 19 августа в 12 и 17 часов, если указанные даты – вторник.

Пример настройки события:

```
# edit service scheduler
# set script-user adm
# edit event test
# set timer 4:*:*:*:*
# set script path /system/scripts/test
# set script args «a\\ b»
# diff
+service {
+  scheduler {
+    event test {
+      timer 4:*:*:*:*
+      script {
+        path /system/scripts/test
+        args «a\\ b»
+      }
+    }
+  }
+}
```

Указан единственный аргумент к скрипту – «a b».

21.4 Особенности работы

1) Время в настройке `timer` указывается по стандарту UTC.

2) При указании в настройке `timer` несуществующей даты (например, 31 февраля) скрипт никогда не будет выполнен.

3) Если в период выполнения скрипта систем была отключена, скрипт выполняется на следующем тике таймера.

22 Служба vrrp

Служба vrrp предназначена для применения протокола VRRP в ПАК «Фортикс». VRRP (Virtual Router Redundancy Protocol) — сетевой протокол, предназначенный для обеспечения отказоустойчивости маршрутизаторов, которая обеспечивается путём объединения нескольких маршрутизаторов в одну группу, обслуживающую общие виртуальные IP-адреса. Объединение нескольких ПАК «Фортикс» называется кластером, внутри кластера каждый ПАК «Фортикс» называется нодой. На каждой ноде настраиваются экземпляры службы vrrp, позволяющие отнести ноду к некоторому кластеру.

22.1 Базовая настройка

Настройка службы vrrp осуществляется на следующем уровне конфигурации:

```
[edit service vrrp]
```

Для заупска службы VRRP применяется команда:

```
[edit service vrrp]
# set enable
```

Для функционирования службы vrrp необходимо создание хотя бы одного экземпляра (`instance`). Для создания экземпляра применяется команда:

```
[edit service vrrp]
# set instance <instance-name>
```

где `<instance-name>` – слово.

Настройка экземпляров осуществляется на следующем уровне конфигурации:

```
[edit service vrrp instance <instance-name>]
```

где `<instance-name>` – слово.

На данном уровне конфигурации доступны следующие обязательные настройки:

– `router-id <router-id>` – задать идентификатор экземпляра, где `<router-id>` – число от 1 до 255 (на каждой ноде одного кластера настраиваются экземпляры с одинаковыми идентификаторами);

– `state master|backup` – задать первоначальную роль (состояние) ноды (одна нода кластера настраивается как `master`, остальные – `backup`);

– `interface <interface-name>` – указать имя первичного интерфейса, используемого для VRRP-оповещений, где `<interface-name>` – имя существующего интерфейса.

На данном уровне конфигурации доступны следующие дополнительные настройки:

– ipv4 – перейти на уровень конфигурации IPv4 для настройки виртуальных IP-адресов;

– ipv6 – перейти на уровень конфигурации IPv6 для настройки виртуальных IP-адресов;

– adv-interval <adv-interval-value> – указать интервал времени, с которым осуществляются VRRP-оповещения, где <adv-interval-value> – число секунд от 0.00 до 3600.00;

– auth <password> – задать пароль для аутентификации, где <password> – строка;

– garp – перейти на уровень конфигурации и настроить Gratuitous ARP-оповещений для перехода в состояние master;

– no-preempt – отключить перехват состояния у ноды с более низким приоритетом;

– no-track-primary – отключить отслеживание состояния первичного интерфейса;

– preempt-delay <preempt-delay-value> – задать задержку для перехвата состояния, где <preempt-delay-value> – число секунд от 0 до 3600;

– priority <priority-value> – задать приоритет ноды в кластере, где <priority-value> – число от 0 до 255 (чем больше число, тем выше приоритет);

– src-ip <address> – задать IP-адрес источника для мультикаст-пакетов, где <address> – IPv4-адрес в формате A.B.C.D или IPv6-адрес в формате A:B:..:H;

– track – перейти на уровень конфигурации параметров отслеживания состояния интерфейса;

– unicast – перейти на уровень конфигурации параметров unicast-оповещений, используемых вместо multicast-оповещений;

– vmac – включить режим подмены MAC-адреса.

Пример обязательной настройки экземпляра для основной ноды:

```
[edit service vrrp]
# set instance main router-id 1 state master interface en0
```

Пример обязательной настройки экземпляра для резервной ноды:

```
[edit service vrrp]
# set instance main router-id 1 state backup interface en0
```

При наличии хотя бы двух нод с настроенными на них экземплярами, кластер может функционировать в режиме основной/резервный.

Если нода кластера с ролью backup перестаёт получать сообщения от ноды с ролью master, она принимает на себя роль master и начинает поддерживать настроенные виртуальные

IP-адреса. Если первичный интерфейс или интерфейс, настроенный на уровне конфигурации `track`, переходит в выключенное состояние, нода не может исполнять роль `master`.

22.2 Настройка виртуальных IP-адресов

У экземпляра может быть несколько виртуальных IPv4- или IPv6-адресов.

Для настройки виртуальных IP-адресов применяется команда:

```
[edit service vrrp instance <instance-name> ipv4|ipv6]
# set address <address> interface <interface-name>
```

где

– `<instance-name>` – имя существующего экземпляра;

– `ipv4|ipv6` – уровень конфигурации IPv4/IPv6;

– `<address>` – IPv4-адрес в формате `A.B.C.D/M` или IPv6-адрес в формате `A:B:..:H/M` в зависимости от уровня конфигурации;

– `<interface-name>` – имя существующего интерфейса.

Если в команде указан несуществующий интерфейс, виртуальный IP-адрес устанавливается на первичный интерфейс.

Для включения режима подмены MAC-адреса применяется команда:

```
[edit service vrrp instance <instance-name> ipv4|ipv6]
# set address <address> vmac
```

где

– `<instance-name>` – имя существующего экземпляра;

– `ipv4|ipv6` – уровень конфигурации IPv4/IPv6;

– `<address>` – IPv4-адрес в формате `A.B.C.D/M` или IPv6-адрес в формате `A:B:..:H/M` в зависимости от уровня конфигурации.

Для отключения смены роли экземпляра при отказе интерфейса с виртуальным IP-адресом применяется команда:

```
[edit service vrrp instance <instance-name> ipv4|ipv6]
# set address <address> no-track
```

где

– `<instance-name>` – имя существующего экземпляра;

– `ipv4|ipv6` – уровень конфигурации IPv4/IPv6;

– <address> – IPv4-адрес в формате A.B.C.D/M или IPv6-адрес в формате A:B:..:H/M в зависимости от уровня конфигурации.

Для указания broadcast-адреса для виртуального IPv4-адреса применяется команда:

```
[edit service vrrp instance <instance-name> ipv4]
# set address <address> brd <brd-address>
```

где

– <instance-name> – имя существующего экземпляра;

– <address> – IPv4-адрес в формате A.B.C.D/M;

– <brd-address> – broadcast-адрес в формате A.B.C.D.

Для отключения режима обнаружения повторяющихся адресов для виртуального IPv6-адреса применяется команда:

```
[edit service vrrp instance <instance-name> ipv6]
# set address <address> no-dad
```

где

– <instance-name> – имя существующего экземпляра;

– <address> – IPv6-адрес в формате A:B:..:H/M.

22.3 Группы синхронизации

Для объединения нескольких экземпляров в общую группу на одной ноде применяется команда:

```
[edit service vrrp]
# set group <group-name> instance <instance-name-1> instance <instance-name-2>
```

где

– <group-name> – имя слово;

– <instance-name-1> – имя существующего экземпляра;

– <instance-name-2> – имя существующего экземпляра.

При изменении состояния любого экземпляра в группе, состояние остальных экземпляров в группе также изменяется.

22.4 Настройка режима отслеживания

Служба VRRP может отслеживать состояния сетевых интерфейсов и, в зависимости от него, изменять приоритет экземпляра или группы на указанное значение.

Настройка параметров отслеживания состояния интерфейсов для экземпляра осуществляется на следующем уровне конфигурации:

```
[edit service vrrp instance <instance-name> track]
```

где `<instance-name>` – имя существующего экземпляра.

Для настройки отслеживания состояния интерфейса применяется команда:

```
[edit service vrrp instance <instance-name> track]
# set interface <interface-name> [weight <weight-value>] [reverse]
```

где

– `<instance-name>` – имя существующего экземпляра;

– `<interface-name>` – имя существующего интерфейса;

– `<weight-value>` – значение приоритета от -253 до 253;

– `reverse` – увеличение приоритета для неработающего интерфейса.

Настройка параметров отслеживания состояния интерфейсов для группы осуществляется на следующем уровне конфигурации:

```
[edit service vrrp group <group-name> track]
```

где `<group-name>` – имя существующей группы.

Настройки данного уровня конфигурации аналогичны настройкам уровня конфигурации отслеживания для экземпляра.

22.5 Диагностика

Для просмотра статистики службы vrrp применяется команда:

```
> show service vrrp stat
```

Для просмотра журнала службы vrrp применяется команда:

```
> show journal service vrrp
```

23 Служба netconf

В ПАК «Фортикс» реализована возможность удалённого управления узлом по протоколу NETCONF (Network Configuration Protocol) (см. RFC 6241). Протокол NETCONF реализует обмен управляющими XML-сообщениями и работает по принципу «клиент-сервер». ПАК «Фортикс» выступает в роли сервера. Аавторизованные клиенты NETCONF имеют возможность запрашивать/изменять конфигурацию ПАК «Фортикс» и инициировать выполнение определённых RPC-процедур (Remote Procedure Call) на ПАК.

В ПАК «Фортикс» в качестве транспорта протокола NETCONF используется протокол SSH (см. RFC 6242).

Протокол NETCONF работает в двух режимах: `listen` и `call-home`.

Режим `listen` – стандартный режим сервера. ПАК «Фортикс» ожидает на сокете и принимает SSH-соединения от клиентов. По умолчанию используется TCP-порт 830. В случае успешной идентификации и аутентификации пользователя SSH, ему разрешаются операции с конфигурацией и RPC-процедуры согласно его ролевой группе, то есть (при включённом NACM) к операциям NETCONF применяются ограничения согласно настройкам ролевой модели (см. раздел «Ролевая модель»).

Режим `call-home` (см. RFC 8071) применим в случае, если IP-адрес узла заранее неизвестен или ПАК «Фортикс» находится за областью NAT. В режиме `call-home` ПАК «Фортикс» первый инициирует TCP-соединение с клиентом (с периодичностью, согласно собственным настройкам). Далее клиент по данному TCP-соединению инициирует транспортную сессию (например, SSH) с идентификацией/аутентификацией и начинает обмен NETCONF-процедурами. Таким образом, ПАК «Фортикс» самостоятельно «звонит домой» (от названия режима) клиенту NETCONF для получения от него команд управления.

23.1 Краткое описание настроек службы netconf

23.1.1 Настройка режима listen

Настройка режима `listen` осуществляются на следующем уровне конфигурации:

```
[edit netconf-server listen]
```

На данном уровне конфигурации доступны следующие настройки:

– `idle-timeout <idle-timeout-value>` – указать тайм-аут автоматического закрытия сессии NETCONF при отсутствии запросов от клиента, где `<idle-timeout-value>` – число секунд, по умолчанию – 180;

– `endpoints endpoint <endpoint-name> ssh` – перейти на уровень конфигурации именованной группы настроек одного слушающего сокета протокола NETCONF/SSH, где `<endpoint-name>` – строка, возможно определение нескольких именованных групп на данном уровне конфигурации:

– `tcp-server-parameters` – перейти на уровень конфигурации TCP-соединений для ожидающего и принимающего сокета:

– `local-address <address>` – указать IP-адрес, на котором ожидаются и принимаются входящие соединения, где `<address>` – IPv4-адрес в формате `A.B.C.D`;

– `local-port <port-number>` – указать TCP-порт, на котором ожидаются и принимаются входящие соединения, где `<port-number>` – число от 1 до 65535, по умолчанию – 830;

– `keepalives` – перейти на уровень конфигурации политики пересылки пакетов, поддерживающих соединение (см. RFC 9293, п. 3.8.4):

– `idle-time <idle-time-value>` – указать период отсутствия трафика по TCP-соединению, по истечении которого начинается передача пакетов «TCP keep-alive», где `<idle-time-value>` – число секунд, по умолчанию – 7200;

– `max-probe <max-probe-value>` – указать максимальное количество переданных подряд пакетов «keep-alive», оставленных без ответа, до определения TCP-соединения как потерянного, где `<max-probe-value>` – число от 1 до 65535, по умолчанию – 9;

– `probe-interval <probe-interval-value>` – указать интервал между передачей пакетов «keep-alive», оставленных без ответа, где `<probe-interval-value>` – число секунд, по умолчанию – 75;

– `ssh-server-parameters` – перейти на уровень конфигурации SSH-сервера для слушающего сокета:

– `server-identity host-key <host-key-name> public-key` – перейти на уровень конфигурации именованной ассоциации ключевой пары,

использующейся для аутентификации сервера SSH, где <host-key-name> – строка, возможно определение нескольких именованных ассоциаций на данном уровне конфигурации:

– central-keystore-reference <key-name> – указать ссылку на ключевую пару, хранящуюся на глобальном уровне конфигурации [edit keystore], где <key-name> – строка (см. ниже);

– inline-definition – перейти на уровень конфигурации непосредственного хранения ключевой пары, без ссылок на другие хранилища (см. ниже);

– client-authentication – перейти на уровень конфигурации аутентификации клиентов NETCONF/SSH:

– auth-timeout <auth-timeout-value> – указать тайм-аут аутентификации, где <auth-timeout-value> – число секунд, по умолчанию – 30;

– endpoint-reference <endpoint-name> – использовать помимо собственных методы аутентификации клиентов из другой именованной группы настроек endpoint, где <endpoint-name> – имя существующей именованной группы настроек endpoint;

– transport-params – перейти на уровень конфигурации транспортного уровня SSH:

– encryption encryption-alg <algorithm> – указать приоритетный список алгоритмов шифрования, где <algorithm> – алгоритм(ы) из предложенного в командной строке списка (если настройка не задана, используются алгоритмы по умолчанию);

– host-key host-key-alg <algorithm> – указать приоритетный список алгоритмов подписи, где <algorithm> – алгоритм(ы) из предложенного в командной строке списка;

– key-exchange key-exchange-alg <algorithm> – указать приоритетный список алгоритмов выработки общего секрета, где <algorithm> – алгоритм(ы) из предложенного в командной строке списка;

– mac mac-alg <algorithm> – указать приоритетный список алгоритмов имитозащиты, где <algorithm> – алгоритм(ы) из предложенного в командной строке списка.

На уровне конфигурации [edit netconf-server listen endpoints endpoint <endpoint-name> ssh ssh-server-parameters server-identity host-key <host-key-name> public-key inline-definition] доступны следующие настройки:

– public-key-format – перейти на уровень конфигурации формата открытого ключа:

– ssh-public-key-format – использовать формат открытого ключа SSH (см. RFC 4253, п.6);

– subject-public-key-info-format – использовать ASN.1-кодировку структуры SubjectPublicKeyInfo (см. RFC 5280);

– public-key <public-key-value> – определить значение открытого ключа, где <public-key-value> – строка в представлении BASE64;

– private-key-format – перейти на уровень конфигурации формата закрытого ключа:

– ec-private-key-format – использовать ASN.1-кодировку структуры ECPrivateKey (см. RFC 5915);

– one-asymmetric-key-format – использовать ASN.1-кодировку структуры OneAsymmetricKey (см. RFC 5958);

– openssh-private-key-format – использовать формат закрытого ключа OpenSSH;

– private-key-info-format – использовать ASN.1-кодировку структуры PrivateKeyInfo (#8);

– rsa-private-key-format – использовать ASN.1-кодировку структуры RSAPrivateKey (см. RFC 3447);

– cleartext-private-key <private-key-value> – определить значение закрытого ключа, где <private-key-value> – строка в представлении BASE64.

23.1.2 Настройка режима call-home

Настройка режима call-home осуществляется на следующем уровне конфигурации:

```
[edit netconf-server call-home]
```

На данном уровне конфигурации доступны следующие настройки:

– netconf-client <netconf-client-name> – перейти на уровень конфигурации именованной группы настроек, относящейся к одному клиенту NETCONF, где <netconf-client-name> – строка, возможно определение нескольких именованных групп на данном уроне конфигурации:

– connection-type – перейти на уровень конфигурации политики соединения:

– persistent – использовать постоянное соединение (в случае отсутствия, закрытия или потери соединения сервер повторяет попытку соединения с периодичностью, указанной в настройке max-wait);

– periodic – перейти на уровень конфигурации периодичного соединения (настройки данного уровня конфигурации применяются совместно с настройками уровня конфигурации reconnect-strategy):

– period <period-value> – указать период повторного соединения от начала инициации предыдущего соединения, где <period-value> – число минут, по умолчанию – 60, если соединение закрыто аварийно (без использования процедуры close-session), новое соединение инициируется немедленно;

– idle-timeout <idle-timeout-value> – указать период, по истечении которого при отсутствии трафика соединение автоматически закрывается, где <idle-timeout-value> – число секунд, по умолчанию – 180;

– anchor-time <yyyy-mm-ddThh:mm:00(Z|+-hh:mm)> – указать точку отсчёта времени для периодов соединений, как в будущее, так и в прошлое, где <yyyy-mm-ddTHH:MM:00(Z|+-HH:MM)> – время, кратное минуте (если настройка не задана, периоды отсчитываются от момента применения конфигурации);

– reconnect-strategy – перейти на уровень конфигурации политики повторного соединения:

– max-attempts <max-attempts-value> – указать количество неудачных произведённых подряд попыток соединения, после которых осуществляется переход к следующей группе настроек endpoint, если она имеется, и соединение принимается неудачным, где <max-attempts-value> – число, по умолчанию – 3;

– max-wait <max-wait-value> – указать период ожидания ответа на соединение, по истечении которого осуществляется переход к следующей попытке, где <max-wait-value> – число секунд, по умолчанию – 5;

– start-with first-listed – испозовать первую группу настроек endpoint при следующем запланированном соединении (настройка установлена по умолчанию);

– start-with last-connected – испозовать последнюю удачно применённую группу настроек endpoint при следующем запланированном соединении;

– start-with random-selection – испозовать случайную группу настроек endpoint при следующем запланированном соединении;

– endpoints endpoint <endpoint-name> ssh – перейти на уровень конфигурации именованной группы настроек одного клиента NETCONF/SSH, где <endpoint-name> – строка, возможно определение нескольких именнованных групп на данном уровне конфигурации:

– tcp-client-parameters – перейти на уровень конфигурации TCP-соединения с клиентом:

– remote-address <address>|<host> – указать IP-адрес/имя хоста NETCONF-клиента, ожидающего и принимающего в режиме call-home, где <address> – IPv4-адрес в формате A.B.C.D[/mask], <host> – имя хоста;

– remote-port <port-number> – указать порт NETCONF-клиента, ожидающего и принимающего в режиме call-home, где <port-number> – число от 1 до 65535, по умолчанию – 4334;

– local-address <address> – указать локальный IP-адрес, через который инициируется TCP-соединение call-home, где <address> – IPv4-адрес в формате A.B.C.D[/mask], по умолчанию – 0.0.0.0/:: (первый подходящий);

– local-port <port-number> – указать локальный порт, от которого инициируется TCP-соединение call-home, где <port-number> – число от 1 до 65535, по умолчанию – 0 (первый свободный);

– keepalives – перейти на уровень конфигурации политики пересылки пакетов, поддерживающих соединение (аналогично уровню конфигурации [edit netconf-server listen ... tcp-server-parameters keepalives]);

– ssh-server-parameters – перейти на уровень конфигурации SSH-сервера:

– server-identity host-key <host-key-name> public-key – указать имя ассоциации ключевой пары для аутентификации SSH-сервера (аналогично режиму listen), где <host-key-name> – строка;

– client-authentication – перейти на уровень конфигурации аутентификации клиентов NETCONF/SSH (аналогично режиму listen);

– transport-params – перейти на уровень конфигурации транспортного уровня SSH (аналогично режиму listen).

23.1.3 Настройка глобального хранилища секретных ключей (keystore)

Настройка глобального хранилища секретных ключей осуществляется на следующем уровне конфигурации:

```
[edit keystore]
```

На данном уровне конфигурации доступны следующие настройки (далее перечислены только настройки, относящиеся к хранению закрытых ключей, использующихся в секции [edit ... server-identity] настроек сервера NETCONF):

– asymmetric-keys asymmetric-key <asymmetric-key-name> – перейти на уровень конфигурации именованной пары асимметричных ключей, которая используется в настройках netconf-server ... ssh-server-parameters server-identity ... central-keystore-reference, где <asymmetric-key-name> – строка, возможно определение нескольких именованных пар на данном уровне конфигурации:

– public-key-format – перейти на уровень конфигурации формата открытого ключа:

– ssh-public-key-format – использовать формат открытого ключа SSH (см. RFC 4253, п.6);

– subject-public-key-info-format – использовать ASN.1-кодировку структуры SubjectPublicKeyInfo (см. RFC 5280);

– public-key <public-key-value> – определить значение открытого ключа, где <public-key-value> – строка в представлении BASE64;

– private-key-format – перейти на уровень конфигурации формата закрытого ключа:

– ec-private-key-format – использовать ASN.1-кодировку структуры ECPrivateKey (см. RFC 5915);

– one-asymmetric-key-format – использовать ASN.1-кодировку структуры OneAsymmetricKey (см. RFC 5958);

– openssh-private-key-format – использовать формат закрытого ключа OpenSSH;

– private-key-info-format – использовать ASN.1-кодировку структуры PrivateKeyInfo (#8);

– rsa-private-key-format – использовать ASN.1-кодировку структуры RSAPrivateKey (см. RFC 3447);

– cleartext-private-key <cleartext-private-key-value> – определить значение закрытого ключа, где <cleartext-private-key-value> – строка в представлении BASE64.

23.2 Пример минимальной настройки службы netconf в режиме listen

В данном подразделе рассматривается пример настройки доступа по протоколу NETCONF для двух учётных записей:

– сетевой администратор netadmin с аутентификацией по паролю;

– администратор admin с аутентификацией по открытому ключу.

Для создания учётных записей применяются команды:

```
# setup login netadmin
# setup login netadmin password
Change password for netadmin
Password:****
Retype password:****
# setup login admin
# commit
```

Примечание – Пароль для учётной записи admin не задан, так как аутентификация осуществляется только по открытому ключу.

Для добавления созданных учётных записей в соответствующие ролевые группы применяются команды:

```
# set nacm groups group netadm user-name netadmin
# set nacm groups group adm user-name admin
# commit
```

Для добавления разрешённых методов аутентификации по протоколу NETCONF к учётным записям применяются команды:

```
# set system auth netconf allow-login netadmin method keyboard-interactive
# set system auth netconf allow-login admin method public-key
# commit
```

Для работы ПАК «Фортикс» в качестве сервера SSH необходимо указание пары асимметричных ключей для подтверждения подлинности. Для создания закрытого асимметричного ключа применяется команда:

```
# setup netconf-identity <key-name> [<algorithm>]
```

где

– <key-name> – произвольный текстовый идентификатор, используемый в дальнейшем для ссылки на ключ;

– <algorithm> – алгоритм из предложенного в командной строке списка, по умолчанию – rsa2048 (рекомендуется).

Для генерации ключевой пары применяется команда:

```
# setup netconf-identity idkey
# commit
```

Конфигурация после выполнения указанной команды:

```
keystore asymmetric-keys asymmetric-key idkey {
  public-key-format ssh-public-key-format
  private-key-format rsa-private-key-format
  cleartext-private-key <private-key-base64>
}
```

Примечания

1) Настройка cleartext-private-key имеет атрибут nacm:default-deny-all, поэтому отображается для учетной записи администратора root. Для других учётных записей (предустановленной ролевой модели) данное поле скрыто.

2) Открытый ключ в поле public-key указывать необязательно, так как он автоматически генерируется NETCONF-сервером из закрытого ключа.

Настройка одного сокета, ожидающего соединение по протоколу SSH, осуществляется на следующем уровне конфигурации:

```
[edit netconf-server listen endpoints endpoint p1 ssh]
```

где p1 – имя группы настроек одного сокета.

Для указания локального IP-адреса, на котором служба ожидает NETCONF-соединения, применяется команда:

```
[edit netconf-server listen endpoints endpoint p1 ssh]
# set tcp-server-parameters local-address 0.0.0.0
```

Для предоставления службе возможности ожидать соединения на всех интерфейсах указан адрес `0.0.0.0`.

П р и м е ч а н и е – На данном этапе настройки команда `commit` не применима из-за ошибки целостности конфигурации.

Настройка SSH-сервера осуществляется на следующем уровне конфигурации:

```
[edit netconf-server listen endpoints endpoint p1 ssh ssh-server-parameters]
```

Для указания ссылки на ключ ПАК «Фортикс», используемого в протоколе SSH для подтверждения подлинности, применяется команда:

```
[edit netconf-server listen endpoints endpoint p1 ssh ssh-server-parameters]
# set server-identity host-key key1 public-key central-keystore-reference id
key
```

где

– `key1` – имя ассоциации ключевой пары;

– `idkey` – имя ассиметричного ключа.

Для аутентификации учётных записей при подключении по протоколу NETCONF поддерживаются режимы `publickey` (для авторизации по SSH-ключу) и `keyboard-interactive` (для авторизации по паролю или по протоколу RADIUS).

Для просмотра конфигурации применяются команды:

```
# top
<Ctrl>+<Backspace>
```

Конфигурация NETCONF-сервера согласно указанным настройкам:

```
netconf-server listen endpoints endpoint p1 ssh {
  tcp-server-parameters local-address 0.0.0.0
  ssh-server-parameters server-identity host-key key1 public-key central-key
store-reference idkey
}
```

Для проверки работоспособности вышеуказанных настроек применим клиент NETCONF. В качестве клиента возможно использование утилиты `netopeer2-cli` на сторонней Linux-машине. При этом на данной машине должен присутствовать сгенерированный закрытый ключ для учётной записи `admin` в файле ~/.ssh/id_rsa.

Для использования утилиты `netopeer2-cli` необходимо последовательно собрать и установить следующие пакеты:

– libyang – https://github.com/CESNET/libyang;

– sysrepo – https://github.com/sysrepo/sysrepo.git;

– libnetconf2 – https://github.com/CESNET/libnetconf2;

– netopeer2 – https://github.com/CESNET/netopeer2.git.

Для запуска утилиты применяется команда:

```
$ netopeer2-cli
> _
```

Для определения приоритетов методов аутентификации применяются команды:

```
> auth pref publickey 1
> auth pref interactive 2
> auth pref password -1
> auth pref
The SSH authentication method preferences:
    'publickey':   1
    'password':    disabled
    'interactive': 2
```

Для соединения с ПАК «Фортикс» по протоколу NETCONF/SSH от имени учётной записи `netadmin` применяется команда:

```
> connect --host <ip> --login netadmin
Keyboard-Interactive Authentication
Please enter your authentication token
Password: ********
> _
```

где `<ip>` – IP-адрес ПАК «Фортикс».

При отсутствии сообщений об ошибках полагается, что аутентификация прошла успешно.

Для проверки NETCONF-соединения применяется команда:

```
> get-config --source running
```

В случае успеха выводится конфигурация узла ПАК «Фортикс» в формате XML.

Для закрытия соединения учётной записи `netadmin` применяется команда:

```
> disconnect
```

Для регистрации ключевой пары учётной записи `admin` используются команды:

```
> auth keys add /home/user-name/.ssh/id_rsa.pub /home/user-name/.ssh/id_rsa
> auth keys
```

```
The keys used for SSH authentication:
#0: /home/user-name/.ssh/id_rsa.pub (private /home/user-name/.ssh/id_rsa)
```

Для инициализации соединения от имени учётной записи администратора admin применяется команда:

```
> connect --host <ip> --login admin
> _
```

где <ip> – IP-адрес ПАК «Фортикс».

При отсутствии запроса на введение пароля полагается, что выполнена аутентификация по ключу.

Для проверки работоспособности NETCONF-соединения применяется команда:

```
> get-config --source running
```

Для выхода из утилиты применяется команда:

```
> exit
```

23.3 Минимальная настройка службы netconf в режиме call-home

Минимальная настройка службы в режиме call-home аналогична настройкам режима listen, за исключением настройки tcp-client-parameters remote-address, где для режима call-home указывается адрес клиента, с которым ПАК «Фортикс» устанавливает TCP-соединение. Кроме того, указывается тип подключения (настройка connection-type) – постоянное или периодическое. В примере используется постоянное (persistent) подключение, то есть на ПАК «Фортикс» (в случае отсутствия соединения) постоянно осуществляется попытка подключения к клиенту (по умолчанию – каждые 5 секунд на порт 4334).

Пример конфигурации минимальной настроки режима call-home:

```
netconf-server {
  call-home netconf-client client1 {
    endpoints endpoint p2 ssh {
      tcp-client-parameters remote-address <client_IP_address>
      ssh-server-parameters server-identity host-key key1 public-key central
-keystore-reference idkey
    }
    connection-type persistent
  }
}
```

Для проверки работоспособности с помощью утилиты `netopeer2-cli` (полагается, что выполнены настройки `auth pref` и `auth keys` из примера подраздела «Пример минимальной настройки службы netconf в режиме listen») применяются команды:

```
$ netopeer2-cli
> listen --login netadmin
Waiting 60s for an SSH Call Home connection on port 4334...
Keyboard-Interactive Authentication
Please enter your authentication token
Password: ********
> get-config --source running
... Конфигурация в формате XML
> disconnect

> listen --login admin
Waiting 60s for an SSH Call Home connection on port 4334...
> get-config --source running
... Конфигурация в формате XML
> exit
```

23.4 RPC-процедуры

23.4.1 Стандартные RPC

В ПАК «Фортикс» поддерживаются представленные в таблице 6 стандартные RPC-процедуры протокола NETCONF.

Т а б л и ц а 6 – Стандартные RPC-процедуры протокола NETCONF в ПАК «Фортикс»

RPC	Стандарт
cancel-commit	RFC 6241, 8.4.4.1
close-session	RFC 6241, 7.8
commit	RFC 6241, 8.3.4.1
copy-config	RFC 6241, 7.3; RFC 6243, 4.5.1
create-subscription	RFC 5277, 2.1.1
delete-config	RFC 6241, 7.4
delete-subscription	RFC 8639, 2.4.4
discard-changes	RFC 6241, 8.3.4.2
edit-config	RFC 6241, 7.2
edit-data	RFC 8526, 3.1.2

RPC	Стандарт
establish-subscription	RFC 8639, 2.4.2
factory-reset	RFC 8808, 2
get	RFC 6241, 7.7
get-config	RFC 6241, 7.1; RFC 6243, 4.5.1
get-data	RFC 8526, 3.1.1
get-schema	RFC 6022, 3.1
kill-session	RFC 6241, 7.9
kill-subscription	RFC 8639, 2.4.5
lock	RFC 6241, 7.5; RFC 8526, 3.2
modify-subscription	RFC 8639, 2.4.3
resync-subscription	RFC 8641, 4.4.4
unlock	RFC 6241, 7.6; RFC 8526, 3.2
validate	RFC 6241, 8.6.4.1; RFC 8526, 3.2

23.4.2 RPC-процедуры, специфические для ПАК «Фортикс»

23.4.2.1 exec-script

Процедура `exec-script` позволяет выполнять скрипты на ПАК «Фортикс» и получать результаты его выполнения по протоколу NETCONF (см. раздел «Скрипты»).

YANG-схема RPC-процедуры `exec-script`:

```
module fx-system {
  yang-version «1.1»;
  namespace «http://zts.ru/fx/yang/system»;
  prefix «system»;

  rpc exec-script {
    description «Execute FX script»;
    input {
      leaf script {
        description «Path or @[script...]»;
        type string;
        mandatory true;
      }
      leaf-list args {
```

```
        description «Arguments»;
        type string;
      }
    }
    output {
      leaf status {
        description «Status»;
        type boolean;
      }
      leaf retval {
        description «Return value»;
        type int32;
      }
      leaf stdout {
        description «Stdout»;
        type string;
      }
      leaf stderr {
        description «Stderr»;
        type string;
      }
    }
  }
}
```

Пример:

На ПАК «Фортикс» используется учётная запись `netadmin` (см. выше).

Для создания скрипта `hello.lua` в домашней директории пользователя применяется команда:

```
> edit /home/netadmin/hello.lua
```

Скрипт:

```
--@help Simple hello-world script
--@arg a1:string Argument 1
--@arg a2:string Argument 2

print(«Hello from Fortics!»)
print(«Arg1=« .. ARGS.a1)
print(«Arg2=« .. ARGS.a2)
command(«no-command»)
```

Для сохранения файла и выхода из редактора используются следующие сочетания клавиш: <Ctrl> + <O>, <Ctrl> + <X>.

П р и м е ч а н и е – В последней строке вызывается несуществующая команда для получения ошибочного вывода в стандартном потоке вывода ошибок (`stderr`).

Для вызова RPC-процедуры на сторонней Linux-машине используется утилита `netopeer2-cli` (полагается, что выполнены необходимые настройки из примеров выше).

Предварительно создаётся файл с RPC-процедурой следующего содержания:

```
$ vim rpc.xml

<exec-script xmlns=«http://zts.ru/fx/yang/system»>
  <script>/home/netadmin/hello.lua</script>
  <args>some argument number one</args>
  <args>some argument number two</args>
</exec-script>
```

Для получения результата выполнения скрипта вызывается RPC-процедура с использованием утилиты `netopeer2-cli`:

```
$ netopeer2-cli

> connect --host <ip> --login netadmin
Keyboard-Interactive Authentication
Please enter your authentication token
Password: ********

> user-rpc --content rpc.xml
DATA
<status xmlns=«http://zts.ru/fx/yang/system»>false</status>
<retval xmlns=«http://zts.ru/fx/yang/system»>1</retval>
<stdout xmlns=«http://zts.ru/fx/yang/system»>Hello from Fortics!
Arg1=some argument number one
Arg2=some argument number two</stdout>
<stderr xmlns=«http://zts.ru/fx/yang/system»>&lt;3&gt;core: Error: Illegal c
ommand
&lt;3&gt;system: exit code 1</stderr>
```

где `<ip>` – IP-адрес ПАК «Фортикс».

Предусмотрена возможность передачи скрипта непосредственно в теле RPC-процедуры (без создания файла скрипта на ПАК «Фортикс»). Для этого в начале тела тэга `<script>` указывается символ `@`.

Содержимое файла `rpc.xml`:

```
<exec-script xmlns=«http://zts.ru/fx/yang/system»>
  <script>@
    print(«\n\nHello, World! Counting to 5...»)
    for i=1,5 do
      print(i)
    end
    command(«show version», true)
```

```
    print(«\n»)
  </script>
</exec-script>
```

Вызов RPC-процедуры через утилиту `netopeer2-cli`:

```
> user-rpc --content rpc.xml
DATA
<status xmlns=«http://zts.ru/fx/yang/system»>true</status>
<retval xmlns=«http://zts.ru/fx/yang/system»>0</retval>
<stdout xmlns=«http://zts.ru/fx/yang/system»>

Hello, World! Counting to 5...
1
2
3
4
5
Software: Fortics 1.0-0d-240625 (Resurrection)
Version: 1.0
Release: 0d
Revision: r0.f3858b6dfa
Date: 2024.06.25 01:19:56
Kernel: 5.10.208 x86_64
Status: dev r0 debug
License: Full
HWID: 3cba-8fc7-fdb7-0014-92af
Hash (kernel): 35b0fbfe5be498758fa42a1dae3140970cf6061dae260ca7325e6c53805e8
069
Hash (rootfs): a1904fdb1cc2dec51ae550007d4653e84fd6d7b7042836e2737c0bdf6bb17
f5f
Hash (loader): e34300f7b5fc767f565ffbf09bda715541f51ff843deb62f2698726a71de8
648

</stdout>
<stderr xmlns=«http://zts.ru/fx/yang/system»/>
```

24 Стандартная статическая маршрутизация

24.1 Основные настройки

Статическая маршрутизация является фундаментальной особенностью технологии маршрутизации. Для предоставления ПАК «Фортикс» возможности выполнения функции маршрутизатора, необходимо разрешить передачу транзитных пакетов между сетевыми интерфейсами.

Для включения функции маршрутизации в режиме конфигурации применяется следующая команда для соответствующего протокола:

```
# set system ipv4|ipv6 forwarding
```

где `ipv4|ipv6` – уровень конфигурации IPv4/IPv6.

Настройка одноадресных маршрутов осуществляется на следующем уровне конфигурации:

```
[edit router unicast]
```

На данном уровне конфигурации предусмотрены следующие настройки:

– `ipv4|ipv6` – перейти на уровень конфигурации IPv4/IPv6:

– `to <network> via` – указать префикс назначения, где `<network>` – IPv4-адрес в формате `A.B.C.D/mask` или IPv6-адрес в формате `A:B:...:H/mask` в зависимости от уровня конфигурации, и перейти на уровень конфигурации правил перенаправления пакета:

– `gw <gateway>` – указать IP-адрес, определяющий направление маршрута, где `<gateway>` – IPv4-адрес в формате `A.B.C.D` или IPv6-адрес в формате `A:B:..:H` в зависимости от уровня конфигурации;

– `interface <interface-name>` – указать интерфейс, используемый в качестве следующего перехода, где `<interface-name>` – имя существующего интерфейса;

– `blackhole drop|reject` – указать «тупиковый» маршрут, весь трафик которого отклоняется, а пакеты – удаляются, где `drop` – пакеты отбрасываются без уведомления, `reject` – пакеты отбрасываются с ICMP-сообщением `destination host unreachable`;

– `dist <distance>` – (опционально) указать административное состояние, где `<distance>` – число от 1 до 255;

– nexthop-vrf <vrf-name> – (опционально) задать маршрутизацию в другую виртуальную таблицу из текущей, где <vrf-name> – имя существующей виртуальной таблицы маршрутизации;

– bfd <profile> – (опционально) указать протокол BFD, где <profile> – профиль протокола BFD.

Таким образом, для определения статических маршрутов применяются команды:

```
set ipv4|ipv6 to <network> via gw <gateway> [dist <distance>] [nexthop-vrf <
vrf-name>] [bfd <profile>]
set ipv4|ipv6 to <network> via interface <interface-name> [dist <distance>]
[nexthop-vrf <vrf-name>] [bfd <profile>]
set ipv4|ipv6 to <network> via gw <gateway> interface <interface-name> [dist
<distance>] [nexthop-vrf <vrf-name>] [bfd <profile>]
set ipv4|ipv6 to <network> via blackhole null|drop|reject [dist <distance>]
[nexthop-vrf <vrf-name>] [bfd <profile>]
```

При использовании нескольких маршрутов с пересекающимися адресами назначения <network> приоритетным является маршрут с большей маской.

Пример настройки IPv4-маршрута по умолчанию:

```
# set ipv4 to 0.0.0.0/0 via gw 10.0.0.1
```

По данной команде все пакеты, проходящие через маршрутизатор и не попадающие под действия других правил маршрутизации, перенаправляются на адрес 10.0.0.1.

Для удаления статических маршрутов вместо команды set применяется команда del.

24.2 Статический маршрут с несколькими переходами

Для настройки нескольких правил перехода для одной и той же сети <network> необходимо добавить несколько маршрутов с одним и тем же адресом назначения <network> и указать различные адреса перенаправления пакета.

Пример применения команд для создания нескольких следующих переходов к одной и той же сети <network>:

```
# set ipv4 to 10.0.0.100/32 via gw 20.0.0.1
# set ipv4 to 10.0.0.100/32 via gw 30.0.0.1
```

Пример конфигурации статического маршрута с несколькими переходами:

```
> show router unicast ipv4
S>* 10.0.0.100/32 [1/0] via 20.0.0.1
                        via 30.0.0.1
```

24.3 Просмотр информации о маршрутах

Для просмотра всех одноадресных маршрутов применяется команда:

```
> show router unicast ipv4|ipv6
```

где `ipv4|ipv6` – уровень конфигурации IPv4/IPv6.

ПАК «Фортикс» поддерживает следующие типы маршрутов:

– `connected` – маршруты с прямым подключением (при назначении IP-адресов сетевым интерфейсам);

– `kernel` – маршруты ядра;

– `static` – статические маршруты, настроенные администратором;

– `rip`, `ospf`, `isis`, `bgp` – маршруты, полученные от протоколов динамической маршрутизации.

Для просмотра маршрутов указанного типа применяется команда:

```
> show router unicast ipv4|ipv6 <type>
```

где

– `ipv4|ipv6` – уровень конфигурации IPv4/IPv6;

– `<type>` – тип маршрута (см. выше).

Для просмотра маршрутов указанной подсети применяется команда:

```
> show router unicast ipv4|ipv6 <network>
```

где

– `ipv4|ipv6` – уровень конфигурации IPv4/IPv6;

– `<network>` – IPv4-адрес в формате `A.B.C.D` или IPv6-адрес в формате `A:B:..:H` в зависимости от уровня конфигурации.

Для просмотра информации о количестве маршрутов разных типов применяется команда:

```
> show router unicast ipv4|ipv6 summary
```

где `ipv4|ipv6` – уровень конфигурации IPv4/IPv6.

Для просмотра точного маршрута до указанного адреса назначения применяется команда:

```
> show [vrf <vrf-name>] router route ipv4|ipv6 <destination-address> [opt1 o
pt2 ... optN]
```

где

– `<vrf-name>` – имя существующей виртуальной таблицы маршрутизации;

– `ipv4|ipv6` – уровень конфигурации IPv4/IPv6;

– `<destination-address>` – IPv4-адрес в формате `A.B.C.D` или IPv6-адрес в формате `A:B:..:H`;

– `opt1 opt2 ... optN` – критерии отбора.

По данной команде выводится маршрут, по которому проходит пакет, с учётом различных критериев отбора:

– `dport <destination-port-number>` – порт назначения, где ` – число от 0 до 65535;

– `sport <source-port-number>` – порт источника, где `<source-port-number>` – число от 0 до 65535;

– `iif <input-interface>` – входящий интерфейс, где `<input-interface>` – строка длиной от 1 до 15 символов;

– `oif <output-interface>` – исходящий интерфейс, где `<output-interface>` – строка длиной от 1 до 15 символов;

– `from <source-address>` – адрес источника, где `<source-address>` – IPv4-адрес в формате `A.B.C.D` или IPv6-адрес в формате `A:B:..:H`;

– `fibmatch` – параметр для отображения полного маршрута в соответствии с FIB-таблицей;

– `tos <VAL>` – значения поля TOS, где `<VAL>` – шестнадцатеричное значение в диапазоне от 0x00 до 0xFF.

25 Статическая маршрутизация на основе политик (pbr)

В ПАК «Фортикс» реализована расширенная статическая маршрутизация на основе политик (Policy Based Routing – pbr), настройки которой осуществляются на следующем уровне конфигурации:

```
# edit router pbr ipv4|ipv6
```

где `ipv4|ipv6` – уровень конфигурации IPv4/IPv6.

25.1 Группы маршрутизации

Для настройки расширенной статической маршрутизации создаётся группа маршрутизации, которая представляет собой отдельную таблицу маршрутизации, выделенную для некоторого трафика. Доступно создание нескольких таблиц, каждая из который идентифицируется уникальным именем. При этом настройки расширенной статической маршрутизации повторяют настройки стандартной.

Для создания группы маршрутизации применяется команда:

```
[edit router pbr ipv4|ipv6]
# set group <group-name>
```

где

– `ipv4|ipv6` – уровень конфигурации IPv4/IPv6;

– `<group-name>` – строка.

Пример применения команд для создания и настройки групп:

```
[edit router pbr ipv4]
# set group gw1 to 0.0.0.0/0 via gw 192.168.0.1
# set group gw2 to 0.0.0.0/0 via gw 192.168.1.1
```

В данном примере создаются две группы `gw1` и `gw2`, каждая из которых содержит по одному правилу маршрутизации.

25.2 Правила маршрутизации

Для направления трафика в группу используются следующие типы правил:

– `pre` – правила, выполняющиеся до стандартной статической маршрутизации;

– `post` – правила, выполняющиеся после стандартной статической маршрутизации.

Настройка правил осуществляется на следующем уровне конфигурации:

```
[edit router pbr ipv4|ipv6 <rule-type> rule <rule-name>]
```

где

– ipv4|ipv6 – уровень конфигурации IPv4/IPv6;

– <rule-type> – тип правила;

– <rule-name> – строка.

На данном уровне конфигурации доступны следующие настройки:

– from <address> – применить проверку на соответствие адресу источника, где <address> – IPv4-адрес в формате A.B.C.D или IPv6-адрес в формате A:B:..:H;

– to <address> – применить проверку на соответствие адресу назначения, где <address> – IPv4-адрес в формате A.B.C.D или IPv6-адрес в формате `A:;

– interface <interface-name> – применить проверку на соответствие входному интерфейсу, где <interface-name> – имя существующего интерфейса;

– proto <protocol> – применить проверку на соответствие IP-протоколу, где <protocol> – число от 1 до 255 или строка из предложенного в командной строке списка;

– sport-range low <low-port-number> high <high-port-number> – применить проверку на соответствие указанному диапазону портов источника, где <low-port-number>, <high-port-number> – число от 1 до 65535;

– dport-range low <low-port-number> high <high-port-number> – применить проверку на соответствие указанному диапазону портов назначения, где <low-port-number>, <high-port-number> – число от 1 до 65535;

– group <group-name> – указать группу, к которой применяется правило, где <group-name> – имя существующей группы.

Все правила выстраиваются в упорядоченный список и выполняются последовательно. При этом, если правило срабатывает для пакета и находится маршрут в соответствующей группе, дальнейший анализ правил прекращается, иначе – продолжается согласно списку.

Пример настройки правила для направления трафика в группу gw1 или gw2.

```
[edit router pbr ipv4]
# set post rule to-gw1 from 192.168.0.0/24 group gw1
# set post rule to-gw2 from 192.168.1.0/24 group gw2
```

П р и м е ч а н и е – В рассматриваемом примере создаются два правила с критериями post, которые срабатывают после стандартной статической маршрутизации. Если в конфигурации присутствует шлюз по

умолчанию, правила статической маршрутизации pbr никогда не выполнятся, так как решение о маршрутизации принимается на этапе стандартной маршрутизации. Таким образом, если используются правила типа post необходимо удалить маршрут по умолчанию и создать его как последнее правило статической маршрутизации pbr типа post. Для этого применяются команды:

```
[edit router pbr ipv4]
# top
# del router unicast ipv4 to 0.0.0.0/0
# edit router pbr ipv4
[edit router pbr ipv4]
# set post rule default to 0.0.0.0/0 group gw1
# insert post rule default last
```

В данном примере весь трафик, не попадающий под правила to-gw1 и to-gw2, перенаправляется в группу gw1.

25.3 Качество канала связи (sla)

Для проверки соответствия качества канала связи в правилах статической маршрутизации на основе политик в ПАК «Фортикс» реализованы следующие механизмы:

– keepalive – механизм простых ping-проб;

– sla – расширенный механизм оценки канала связи.

Важно: Каждое правило может использовать только один механизм проб.

Механизм ping-проб позволяет задавать мониторинг удалённого узла с помощью ICMP-пакетов (если узел перестаёт отвечать на запросы, правило перестаёт действовать).

Настройка механизма ping-проб осуществляется на следующем уровне конфигурации:

```
[edit router pbr ipv4|ipv6 <rule-type> rule <rule-name> keepalive]
```

где

– ipv4|ipv6 – уровень конфигурации IPv4/IPv6;

– <rule-type> – тип правила;

– <rule-name> – строка.

На данном уровне конфигурации доступны следующие настройки:

– peer <address> – указать узел назначения для проб, где <address> – IPv4-адрес в формате A.B.C.D или IPv6-адрес в формате A:B:..:H;

– interval <interval-value> – указать интервал отправки ping-проб, где <interval-value> – число секунд, по умолчанию – 1;

– retries <retries-value> – указать количество попыток, где <retries-value> – число, по умолчанию – 3;

– interface <interface-name> – указать интерфейс для отправки, где <interface-name> – имя существующего интерфейса.

Пример настройки ping-проб:

```
[edit router pbr ipv4]
# set post rule to-gw1 keepalive peer 192.168.0.1
```

Настройка механизма sla осуществляется на следующем уровне конфигурации:

```
[edit router pbr ipv4|ipv6 <rule-type> rule <rule-name> sla]
```

где

– ipv4|ipv6 – уровень конфигурации IPv4/IPv6;

– <rule-type> – тип правила;

– <rule-name> – строка.

На данном уровне конфигурации доступны следующие настройки:

– count <count> – определить количество последних проб, для которых рассчитываются параметры качества, где <count> – число от 0 до 65535, по умолчанию – 100;

– interface <interface-name> – указать интерфейс для отправки, где <interface-name> – имя существующего интерфейса;

– peer <address> – указать узел назначения проб, где <address> – IPv4-адрес в формате A.B.C.D или IPv6-адрес в формате A:B:..:H;

– max-jitter <max-jitter-value> – указать максимальную задержку в доставке пакетов, где <max-jitter-value> – число миллисекунд от 0 до 65535;

– max-rtt-avg <max-rtt-avg-value> – указать общее время, необходимое для передачи и возврата ответа, где <max-rtt-avg-value> – число миллисекунд от 0 до 65535;

– max-packet-loss <max-packet-loss-value> – определить процент потерь, где <max-packet-loss-value> – число процентов от 1 до 100.

При превышении значений, заданных данными настройками, правило перестаёт действовать.

Пример настройки механизма sla:

```
[edit router pbr ipv4]
# set post rule to-gw1 sla peer 192.168.0.1 max-rtt-avg 10 count 10
```

25.4 Диагностика

Для просмотра действующих правил маршрутизации применяется команда:

```
> show router pbr ipv4|ipv6
```

где `ipv4|ipv6` – уровень конфигурации IPv4/IPv6.

Для просмотра групп маршрутизации применяется команда:

```
> show router pbr ipv4|ipv6 group <group-name>
```

где

– `ipv4|ipv6` – уровень конфигурации IPv4/IPv6;

– `<group-name>` – имя существующей группы.

26 Динамическая маршрутизация

26.1 NHT (Nexthop Tracking)

ПАК «Фортикс» поддерживает механизм определения следующего перехода (далее по тексту – nexthop) с помощью маршрута по умолчанию: при наличии маршрута по умолчанию для маршрута, следующий переход в котором не определяется с помощью таблицы маршрутизации, nexthop извлекается из маршрута по умолчанию. Данная функция требует отдельной активации для IPv4- и IPv6-маршрутов для каждой виртуальной таблицы маршрутизации (VRF).

Для включения механизма определения следующего перехода с помощью маршрута по умолчанию для основной таблицы маршрутизации применяется команда:

```
# set router nht ipv4|ipv6 resolve-via-default
```

где `ipv4|ipv6` – уровень конфигурации IPv4/IPv6.

Для включения данного механизма для указанной виртуальной таблицы маршрутизации применяется команда:

```
# set vrf <vrf-name> router nht ipv4|ipv6 resolve-via-default
```

где

– `ipv4|ipv6` – уровень конфигурации IPv4/IPv6;

– `<vrf-name>` – имя существующей виртуальной таблицы маршрутизации.

Для просмотра текущего состояния механизма определения следующего перехода применяется команда:

```
> show [ vrf <vrf-name> ] router nht ipv4|ipv6
```

где

– `ipv4|ipv6` – уровень конфигурации IPv4/IPv6;

– `<vrf-name>` – имя существующей виртуальной таблицы маршрутизации.

26.2 Фильтрация

В ПАК «Фортикс» для динамической маршрутной информации предусмотрена фильтрация на основе списков, применимая для любого направления трафика.

26.2.1 Списки доступа (access-list)

Списки доступа (далее по тексту – access-list) – инструмент, позволяющий контролировать и фильтровать сетевой трафик на основе различных критериев, таких как IP-адрес источника и назначения, протокол, порт и т.д. Данные критерии формируют правила фильтрации трафика, прохождение которого через маршрутизатор разрешено или запрещено. Списки доступа применимы для управления трафиком и ограничения доступа к указанным ресурсам и сервисам.

Использование access-list позволяет существенно улучшить безопасность и контроль над сетью за счёт ограничения доступа к некоторым ресурсам и сервисам. Кроме того, данные списки могут быть использованы для управления трафиком, например, для ограничения полосы пропускания.

Для создания разрешающего IPv4-списка доступа применяется команда:

```
# set router access-list ipv4 list <list-name> [description <description>] s
eq <seq> action permit prefix <network>
```

где

– `<list-name>` – строка длиной от 1 до 128 символов;

– `<seq>` – порядковый номер списка от 1 до 4294967295;

– `<description>` – описание списка;

– `<network>` – IPv4-адрес в формате `A.B.C.D/mask`.

Для создания запрещающего IPv4-списка доступа применяется команда:

```
# set router access-list ipv4 list <list-name> [description <description>] s
eq <seq> action deny prefix <network>
```

где

– `<list-name>` – строка длиной от 1 до 128 символов;

– `<seq>` – порядковый номер списка от 1 до 4294967295;

– `<description>` – описание списка;

– `<network>` – IPv4-адрес в формате `A.B.C.D/mask`.

Для создания разрешающего IPv6-списка доступа применяется команда:

```
# set router access-list ipv6 list <list-name> [description <description>] s
eq <seq> action permit prefix <network>
```

где

– `<list-name>` – строка длиной от 1 до 128 символов;

– `<seq>` – порядковый номер списка от 1 до 4294967295;

– `<description>` – описание списка;

– `<network>` – IPv6-адрес `A:B:..:H/mask`.

Для создания запрещающего IPv6-списка доступа применяется команда:

```
# set router access-list ipv6 list <list-name> [description <description>] s
eq <seq> action deny prefix <network>
```

где

– `<list-name>` – строка длиной от 1 до 128 символов;

– `<seq>` – порядковый номер списка от 1 до 4294967295;

– `<description>` – описание списка;

– `<network>` – IPv6-адрес `A:B:..:H/mask`.

Для просмотра информации о всех доступных списках применяется команда:

```
> show router access-list ipv4|ipv6
```

где `ipv4|ipv6` – уровень конфигурации IPv4/IPv6.

26.2.1.1 Списки доступа на основе AS-path (as-path access-list)

Списки доступа на основе AS-path (далее по тексту – as-path access-list, as-path ACL) – механизм, используемый в протоколе BGP для фильтрации маршрутов на основе атрибутов автономной системы (AS). Данный механизм позволяет контролировать трафик, проходящий через указанные автономные системы (автономные системы, содержащие указанные префиксы), и управлять им.

П р и м е ч а н и е – Списки доступа на основе AS-path предоставляют возможность блокировать или разрешать трафик на основе происхождения маршрута, что применимо для обеспечения безопасности сети или для контроля за политиками маршрутизации.

Списки доступа на основе AS-path используются для реализации следующих политик маршрутизации:

– фильтрация маршрутов по автономным системам, через которые они проходят (например, заблокировать маршруты, проходящие через указанные страны или регионы);

– контроль за взаимодействием с указанными автономными системами (например, разрешить только маршруты, не проходящие через указанные автономные системы).

Для создания разрешающего списка доступа на основе AS-path применяется команда:

```
# set router as-path access-list <list-name> seq <seq> action permit as-path <as-path>
```

где

– `<list-name>` – строка длиной от 1 до 128 символов;

– `<seq>` – порядковый номер списка от 1 до 4294967295;

– `<as-path>` – путь к автономной системе в формате регулярного выражения, содержащего числа и символы _^|[,{}()]$*+.?-.

Для создания запрещающего списка доступа на основе AS-path применяется команда:

```
# set router as-path access-list <list-name> seq <seq> action deny as-path <as-path>
```

где

– `<list-name>` – строка длиной от 1 до 128 символов;

– `<seq>` – порядковый номер списка от 1 до 4294967295;

– `<as-path>` – путь к автономной системе в формате регулярного выражения, содержащего числа и символы _^|[,{}()]$*+.?-.

Для просмотра всех актуальных списков доступа на основе AS-path применяется команда:

```
> show router as-path <as-path>
```

где `<as-path>` – путь к автономной системе в формате регулярного выражения, содержащего числа и символы _^|[,{}()]$*+.?-.

26.2.2 Списки префиксов (prefix-list)

Списки префиксов (далее по тексту – prefix-list) используются для фильтрации маршрутов на основе их префикса. Данные списки применимы для управления доступом к указанным сетям или ресурсам, а также для обеспечения безопасности, так как контроль трафика на основе

префикса позволяет предотвращать атаки с подменой адресов (ARP-spoofing) и другие виды атак. Например, с помощью списка префиксов возможно обеспечить доступ к некоторым подсетям, при этом ограничить ко всем остальным.

Списки префиксов применимы для управления трафиком и оптимизации пропускной способности, так как позволяет уменьшить количество трафика, проходящего через сеть, за счёт чего улучшается её производительность. Например, для сети с большим количеством подсетей возможно создание prefix-list, разрешающего трафик только к некоторым подсетям.

Списки префиксов являются удобным инструментом для управления сетевым трафиком и обеспечения безопасности в сети.

Для создания разрешающего IPv4-списка префиксов применяется команда:

```
# set router prefix-list ipv4 list <list-name> seq <seq> action permit prefi
x <prefix> [le <len>] [ge <len>]
```

где

– `<list-name>` – строка длиной от 1 до 128 символов;

– `<seq>` – порядковый номер списка от 1 до 4294967295;

– `<prefix>` – IPv4-адрес адрес в формате `A.B.C.D/mask`;

– `<len>` – длина префикса от 0 до 32.

Для создания запрещающего IPv4-списка префиксов применяется команда:

```
# set router prefix-list ipv4 list <list-name> seq <seq> action deny prefix
<prefix> [le <len>] [ge <len>]
```

где

– `<list-name>` – строка длиной от 1 до 128 символов;

– `<seq>` – порядковый номер списка от 1 до 4294967295;

– `<prefix>` – IPv4-адрес адрес в формате `A.B.C.D/mask`;

– `<len>` – длина префикса от 0 до 32.

Для создания разрешающего IPv6-списка префиксов применяется команда:

```
# set router prefix-list ipv6 list <list-name> seq <seq> action permit prefi
x <prefix> [le <len>] [ge <len>]
```

где

– `<list-name>` – строка длиной от 1 до 128 символов;

– `<seq>` – порядковый номер списка от 1 до 4294967295;

– <prefix> – IPv6-адрес адрес в формате A:B:...:H/mask;

– <len> – длина префикса от 0 до 128.

Для создания запрещающего IPv6-списка префиксов применяется команда:

```
# set router prefix-list ipv6 list <list-name> seq <seq> action deny prefix
<prefix> [le <len>] [ge <len>]
```

где

– <list-name> – строка длиной от 1 до 128 символов;

– <seq> – порядковый номер списка от 1 до 4294967295;

– <prefix> – IPv6-адрес адрес в формате A:B:...:H/mask;

– <len> – длина префикса от 0 до 128.

При указании параметра le в командах выше список применяется, если длина префикса меньше или равна заданному значению, ge – больше или равна.

Для просмотра информации о всех доступных списках префиксов применяется команда:

```
> show router prefix-list ipv4|ipv6 [detail|summary]
```

где

– ipv4|ipv6 – уровень конфигурации IPv4/IPv6;

– detail – параметр, при указании которого выводится подробная информация;

– summary – параметр, при указании которого выводится краткая информация.

26.2.3 Карты маршрутов (route-map)

Карты маршрутов (route-map) предоставляют средства для фильтрации и/или применения действий к маршруту, что позволяет использовать различные политики для маршрутов. Карты маршрутов состоят из упорядоченного списка правил, для каждого из которых возможно указание:

1) типа правила: разрешающее или запрещающее;

2) критериев отбора маршрутов: условия, по которым отбираются маршруты для применения правила;

3) действия для маршрутов: действие, применяемое к отобранным в соответствии с критериями маршрутам;

4) вызываемой карты маршрутов: карта маршрутов, к которой осуществляется переход, если правило применимо.

Действием по умолчанию, если ни одно правило из списка карты маршрутов не соответствует рассматриваемому маршруту, является запрет (т.е. карта маршрутов имеет в качестве последней записи запрещающее правило без остальных элементов описания, что соответствует всем маршрутам). Для изменения действия по умолчанию указывается разрешающее правило без остальных элементов описания в качестве последней записи в карте маршрутов.

Для указания типа правила карты маршрутов применяется команда:

```
# set router route-map <route-map-name> seq <seq> action permit|deny
```

где

– <route-map-name> – строка длиной от 1 до 128 символов;

– <seq> – порядковый номер правила в карте от 1 до 4294967295;

– permit|deny – тип правила.

Для указания критерия отбора маршрута в правиле карты маршрутов применяется команда:

```
# set router route-map <route-map-name> seq <seq> match <match-option>
```

где

– <route-map-name> – строка длиной от 1 до 128 символов;

– <seq> – порядковый номер записи в карте от 1 до 4294967295;

– <match-option> – критерий соответствия из предложенного в командной строке списка.

Для определения действия для маршрута в правиле карты маршрутов применяется команда:

```
# set router route-map <route-map-name> seq <seq> set <set-option>
```

где

– <route-map-name> – строка длиной от 1 до 128 символов;

– <seq> – порядковый номер правила в карте от 1 до 4294967295;

– <set-option> – действие из предложенного в командной строке списка.

Для определения вызываемой карты маршрутов в правиле карты маршрутов применяется команда:

```
# set router route-map <route-map-name> seq <seq> call <call-route-map-name>
```

где

– <route-map-name> – строка длиной от 1 до 128 символов;

– <seq> – порядковый номер правила в карте от 1 до 4294967295;

– <call-route-map-name> – имя существующей карты маршрутов.

Для просмотра информации о всех доступных картах маршрутов применяется команда:

```
> show router route-map
```

26.3 RIP

26.3.1 Введение

Routing Information Protocol – протокол дистанционно-векторной маршрутизации для семейства IPv4-адресов. Маршрутизаторы, работающие по данному протоколу, отправляют всю свою таблицу маршрутизации или её часть соседним маршрутизаторам в сообщениях с обновлениями. Протокол RIP позволяет настраивать хосты в качестве узлов сети RIP. Данный протокол использует UDP-порт 520 для отправки и получения пакетов RIP.

26.3.2 Настройка

Для включения маршрутизатора RIP применяется команда:

```
# set router rip ipv4
```

Для выключения маршрутизатора RIP и удаления всех его настроек применяется команда:

```
# del router rip ipv4
```

Настройка RIP осуществляется на следующем уровне конфигурации:

```
[edit router rip ipv4]
```

Настройка сетевых интерфейсов RIP осуществляется на следующем уровне конфигурации:

```
[edit router rip ipv4 interface]
```

26.3.2.1 Настройка интерфейсов маршрутизатора

Для включения RIP на всех интерфейсах, адреса которых относятся к указанному префиксу, применяется команда:

```
[edit router rip ipv4]
# set network prefix <network>
```

где `<network>` – IPv4-адрес в формате `A.B.C.D/mask`.

Данная команда включает интерфейсы RIP на всех адресах указанного префикса. Например, если в сети 10.0.0.0/24 включён RIP, все интерфейсы с адресами от 10.0.0.0 до 10.0.0.255 задействуются для RIP.

Для отключения RIP на всех интерфейсах, адреса которых относятся к указанному префиксу, применяется команда:

```
[edit router rip ipv4]
# del network prefix <network>
```

где `<network>` – IPv4-адрес в формате `A.B.C.D/mask`.

Для включения маршрутизации RIP на указанном интерфейсе применяется команда:

```
[edit router rip ipv4]
# set network interface <interface-name>
```

где `<interface-name>` – имя существующего интерфейса.

Для отключения маршрутизации RIP на указанном интерфейсе применяется команда:

```
[edit router rip ipv4]
# del network interface <interface-name>
```

где `<interface-name>` – имя существующего интерфейса.

26.3.2.2 Настройка соседства

Для определения IP-адреса соседнего маршрутизатора RIP, которому отправляются обновления, применяется команда:

```
[edit router rip ipv4]
# set neighbor <address>
```

где `<address>` – IPv4-адрес в формате `A.B.C.D`.

Данная настройка используется при подключении соседнего маршрутизатора RIP через сеть, не поддерживающую многоадресную рассылку, или при необходимости статического определения соседнего маршрутизатора RIP. При этом обновления RIP отправляются посредством одноадресной рассылки каждому соседнему маршрутизатору. Обновления соседних маршрутизаторов RIP дополняют любые многоадресные обновления, если интерфейс не находится в пассивном режиме. Обрабатываются все обновления RIP, полученные как от соседнего маршрутизатора RIP, так и через многоадресную рассылку.

26.3.2.3 Настройка пассивного интерфейса

Для перевода интерфейса в пассивный режим применяется команда:

```
[edit router rip ipv4]
# set passive-interface <interface-name>
```

где `<interface-name>` – имя существующего интерфейса.

По данной команде все принимаемые пакеты обрабатываются как обычно, но маршрутизатор не отправляет ни многоадресные, ни одноадресные пакеты RIP. Отправка пакетов осуществляется только маршрутизаторам, для которых явно указаны настройки соседства.

26.3.2.4 Настройка избежания петель

По умолчанию настройка предотвращения петель (split-horizon) включена для каждого интерфейса, который участвует в маршрутизации RIP.

Для отключения данной настройки на указанном интерфейсе применяется команда:

```
[edit router rip ipv4]
# set interface <interface-name> split-horizon disabled
```

где `<interface-name>` – имя существующего интерфейса.

Для включения настройки, по которой маршрутизатор отправляет полученные маршруты с наивысшей метрикой (недостижимый маршрут) обратно на отправляющий маршрутизатор, применяется команда:

```
[edit router rip ipv4]
# set interface <interface-name> split-horizon poison-reverse
```

где `<interface-name>` – имя существующего интерфейса.

26.3.2.5 Настройка ECMP

Для разрешения балансировки между маршрутами с одинаковой стоимостью применяется команда:

```
[edit router rip ipv4]
# set allow-ecmp
```

26.3.2.6 Контроль версий

Маршрутизатор RIP настраивается для отправки пакетов Версии 1 (RIPv1) или Версии 2 (RIPv2). По умолчанию отправляются пакеты RIPv2, а принимаются – как RIPv1, так и RIPv2.

Для определения версии получаемых и отправляемых пакетов применяется команда:

```
[edit router rip ipv4]
# set version 1|2
```

где `1|2` – версия пакетов.

Для определения версии отправляемых пакетов на указанном интерфейсе применяется команда:

```
[edit router rip ipv4]
# set interface <interface-name> version send 1|2|1-2
```

где

– `<interface-name>` – имя существующего интерфейса;

– `1|2|1-2` – версия пакетов.

Для определения версии получаемых пакетов на указанном интерфейсе применяется команда:

```
[edit router rip ipv4]
# set interface <interface-name> version receive 1|2|1-2
```

где

– `<interface-name>` – имя существующего интерфейса;

– `1|2|1-2` – версия пакетов.

26.3.2.7 Анонсирование маршрутов

Для настройки перераспределения маршрутов между протоколами маршрутизации применяется команда:

```
[edit router rip ipv4]
# set redistribute <redistribute-protocol> [metric <metric>] [route-map <rou
te-map-name>]
```

где

– `<redistribute-protocol>` – протокол маршрутизации;

– `<metric>` – значение метрики от 1 до 16;

– `<route-map-name>` – имя существующей карты маршрутов.

Для настройки анонсирования статических маршрутов без добавления в таблицу маршрутизации (только внутри процесса RIP) применяется команда:

```
[edit router rip ipv4]
# set route <network>
```

где `<network>` – IPv4-адрес в формате `A.B.C.D/mask`.

26.3.2.8 Фильтрация маршрутов

Для фильтрации маршрутов RIP применяется команда:

```
[edit router rip ipv4]
# set distribute-list <interface-name> direction in|out access-list|prefix-l
ist <list-name>
```

где

– `<interface-name>` – имя существующего интерфейса;

– `in|out` – тип пакетов;

– `access-list|prefix-list` – уровень конфигурации списка доступа или префиксов;

– `<list-name>` – имя существующего списка доступа или префиксов в зависимости от уровня конфигурации.

26.3.2.9 Управление метрикой маршрутов

По умолчанию маршрутизатор RIP присваивает перераспределённым маршрутам метрику 1.

Для изменения значения по умолчанию метрики перераспределённых маршрутов применяется команда:

```
[edit router rip ipv4]
# set default-metric <default-metric-value>
```

где <default-metric-value> – число от 1 до 16.

По данной команде метрики для connected маршрутов не изменяются. Для изменения метрики таких маршрутов применяется команда для настройки перераспределения маршрутов, карта маршрутов route-map или специальная настройка для изменения метрики offset-list.

Для настройки значения метрики перераспределённых маршрутов применяется команда:

```
[edit router rip ipv4]
# set redistribute <redistribute-protocol> metric <metric-value>
```

где

– <redistribute-protocol> – протокол маршрутизации;

– <metric-value> – число от 0 до 16.

Для настройки значения метрики с помощью offset-list применяется команда:

```
[edit router rip ipv4]
# set offset-list <interface-name> direction in|out metric <metric-value>
```

где

– <metric-value> – число от 1 до 16;

– <interface-name> – имя существующего интерфейса;

– in|out – тип пакетов.

26.3.2.10 Административная дистанция

Административная дистанция применяется для изменения приоритета маршрутов, полученных от разных протоколов. По умолчанию значение административной дистанции для маршрутов RIP равно 120.

Для изменения значения административной дистанции по умолчанию применяется команда:

```
[edit router rip ipv4]
# set distance default <distance-value>
```

где `<distance-value>` – число от 1 до 255.

Для изменения значения административной дистанции для указанных маршрутов применяется команда:

```
[edit router rip ipv4]
# set distance source <network> [access-list <access-list-name>] distance <d
istance-value>
```

где

– `<network>` – IPv4-адрес в формате `A.B.C.D/mask`;

– `<access-list-name>` – имя существующего списка доступа;

– `<distance-value>` – число от 1 до 255.

26.3.2.11 Настройка аутентификации

Аутентификация доступна только для протокола версии 2 (RIPv2). Маршрутизация RIPv2 позволяет аутентифицировать пакеты с помощью незащищённого текстового пароля, содержащегося в пакете, или через более безопасный HMAC на основе MD5. Так как RIPv1 не может быть аутентифицирован, при настроенной аутентификации маршрутизатор отбрасывает все обновления, полученные через пакеты RIPv1.

Если приём RIPv1 не отключён полностью, полученные пакеты RIP Version Control и RIPv1 REQUEST, запрашивающие информацию о маршрутизации, учитываются, при этом маршрутизатор отвечает на такие пакеты. Данный механизм позволяет маршрутизатору учитывать такие запросы (которые иногда используются старым оборудованием), обеспечивая при этом безопасность получаемых обновлений маршрутов.

Использование аутентификации предотвращает обновление маршрутов неаутентифицированными удалёнными маршрутизаторами, при этом разрешает удалённый запрос информации о маршрутах через RIPv1. Для изменения данного поведения необходимо отключить RIPv1.

Для настройки аутентификации с помощью указанного незащищённого текстового пароля для указанного интерфейса применяются команды:

```
[edit router rip ipv4]
# set interface <interface-name> authentication mode text
# set interface <interface-name> authentication string <password>
```

где

– `<interface-name>` – имя существующего интерфейса;

– `<password>` – строка длиной от 1 до 16 символов.

26.3.2.12 Настройка таймеров

Маршрутизация RIP позволяет использовать несколько типов таймеров, каждый из которых настраивается с помощью основной команды `timers`.

Для настройки значения таймера обновления применяется команда:

```
[edit router rip ipv4]
# set timers update <timer-update-value>
```

где `<timer-update-value>` – число секунд от 5 до 2147483647, по умолчанию – 30.

По истечении указанного времени процесс RIP активируется для отправки незапрошенного ответного сообщения с полной таблицей маршрутизации всем соседним маршрутизаторам RIP.

Для настройки значения таймера тайм-аута применяется команда:

```
[edit router rip ipv4]
# set timers timeout <timer-timeout-value>
```

где `<timer-timeout-value>` – число секунд от 5 до 2147483647, по умолчанию – 180.

По истечении указанного времени маршрут становится недействительным. При этом он сохраняется в таблице маршрутизации в течение некоторого малого промежутка времени для уведомления соседних маршрутизаторов об удалении маршрута.

Для настройки значения таймера сбора мусора применяется команда:

```
[edit router rip ipv4]
# set timers garbage-collection <timer-garbage-collection-value>
```

где `<timer-garbage-collection-value>` – число секунд от 5 до 2147483647, по умолчанию – 120.

По истечении указанного времени маршрут окончательно удаляется из таблицы маршрутизации.

26.3.3 26.3.3 Диагностика

Для просмотра информации о маршрутах применяется команда:

```
> show router rip ipv4
```

Для просмотра текущего статуса маршрутизатора RIP применяется команда:

```
> show router rip ipv4 status
```

Вывод команды содержит значения таймеров, настройки фильтрации, версию протокола, информацию об интерфейсах с поддержкой маршрутизации RIP и узлах RIP.

Для просмотра всех маршрутов, полученных с помощью маршрутизации RIP, применяется команда:

```
> show router unicast ipv4 rip
```

26.4 RIPNG

26.4.1 Введение

ПАК «Фортикс» поддерживает протокол RIPng – развитие протокола RIP для семейства IPv6-адресов.

26.4.2 Настройка

Для включения RIPng-маршрутизатора применяется команда:

```
# set router rip ipv6
```

Для выключения RIPng-маршрутизатора и удаления всех его настроек применяется команда:

```
# del router rip ipv6
```

Настройка RIPng-маршрутизатора осуществляется на следующем уровне конфигурации:

```
[edit router rip ipv6]
```

Настройка сетевых интерфейсов RIPng осуществляется на следующем уровне конфигурации:

```
[edit router rip ipv6 interface]
```

Настройки маршрутизатора RIPng аналогичны настройкам маршрутизатора RIP, за исключением формата адреса, который менятся с IPv4 на IPv6.

Для настройки агрегации маршрутов применяется команда:

```
[edit router rip ipv6]
# set aggregate-address <address>
```

где `<address>` – IPv6-адрес в формате `A:B:...:H/mask`.

Для настройки анонсирования маршрута по умолчанию применяется команда:

```
[edit router rip ipv6]
# set default-information originate
```

Для настройки значения метрики по умолчанию применяется команда:

```
[edit router rip ipv6]
# set default-metric <default-metric-value>
```

где `<default-metric-value>` – число от 1 до 16.

Для включения маршрутизации RIPng на указанном интерфейсе применяется команда:

```
[edit router rip ipv6]
# set network interface <interface-name>
```

где `<interface-name>` – имя существующего интерфейса.

Для включения RIPng на всех интерфейсах, адреса которых относятся к указанному префиксу сети, применяется команда:

```
[edit router rip ipv6]
# set network prefix <network>
```

где `<network>` – префикс сети.

Для настройки значения метрики применяются команды:

```
[edit router rip ipv6]
# set offset-list <interface-name> direction in|out metric <metric-value>
# set offset-list <interface-name> direction in|out access-list <access-list
-name>
```

где

– <interface-name> – имя существующего интерфейса;

– in|out – тип пакетов;

– <metric-value> – число от 1 до 16;

– <access-list-name> – имя существующего списка доступа access-list.

В данной команде список access-list указывается для обеспечения контроля сети, для которой настраивается метрика.

Для перевода интерфейса в пассивный режим применяется команда:

```
[edit router rip ipv6]
# set passive-interface <interface-name>
```

где <interface-name> – имя существующего интерфейса.

Для настройки перераспределения маршрутов между протоколами маршрутизации применяется команда:

```
[edit router rip ipv6]
# set redistribute <redistribute-protocol> [metric <metric-value>] [route-ma
p <route-map-name>]
```

где

– <redistribute-protocol> – протокол маршрутизации;

– <metric-value> – число от 1 до 16;

– <route-map-name> – имя существующей карты маршрутов.

Для настройки анонсирования статического маршрута без добавления в таблицу маршрутизации (только внутри процесса RIPng) применяется команда:

```
[edit router rip ipv6]
# set route <network>
```

где <network> – IPv6-адрес в формате A:B:...:H/mask.

Для настройки значения таймера обновления применяется команда:

```
[edit router rip ipv6]
# set timers update <timer-update-value>
```

где <timer-update-value> – число секунд от 5 до 2147483647, по умолчанию – 30.

Для настройки значения таймера тайм-аута применяется команда:

```
[edit router rip ipv6]
# set timers timeout <timer-timeout-value>
```

где <timer-timeout-value> – число секунд от 5 до 2147483647, по умолчанию – 180.

Для настройки значения таймера сбора мусора применяется команда:

```
[edit router rip ipv6]
# set timers garbage-collection <timer-garbage-collection-value>
```

где <timer-garbage-collection-value> – число секунд от 5 до 2147483647, по умолчанию – 120.

26.4.3 Диагностика

Для отображения информации о маршрутах применяется команда:

```
> show router rip ipv6
```

Для отображения текущего статуса маршрутизатора RIPng применяется команда:

```
> show router rip ipv6 status
```

Вывод команды содержаит значения таймеров, настройки фильтрации, версию протокола, информацию об интерфейсах с поддержкой RIPng и узлах RIPng.

Для отображения всех маршрутов, полученных по протоколу RIPng, применяется команда:

```
> show router unicast ipv6 rip
```

26.5 OSPFv2

26.5.1 Введение

Протокол OSPF (Open Shortest Path First) версии 2 является протоколом динамической маршрутизации, используемым, в основном, в сетях IPv4, и входит в семейство протоколов OSPF.

OSPF — протокол маршрутизации, работа которого основана на состоянии канала. В отличие от протоколов дистанционно-векторной маршрутизации, таких как RIP или BGP, где маршрутизаторы описывают доступные пути (маршруты) друг к другу, в протоколах состояния канала маршрутизаторы описывают состояние своих каналов с непосредственно соседними маршрутизаторами.

Каждый маршрутизатор описывает информацию о состоянии своего канала связи в сообщении LSA (link-state advertisement – объявление о состоянии канала), которое распространяется на все остальные маршрутизаторы в домене маршрутизации с помощью процесса, называемого лавинной рассылкой (flooding). Для работы OSPF требуется иерархическая структура сети, которая делится на области OSPF, каждая из которых имеет свою базу данных состояния каналов (Link State Database, LSDB). Каждый маршрутизатор создаёт LSDB всех сообщений о состоянии канала в своей области. Из этого набора LSA в LSDB каждый маршрутизатор может вычислить кратчайший путь к любому другому маршрутизатору на основе общей метрики с помощью алгоритма Дейкстры (алгоритм кратчайшего пути/SPF-алгоритм).

Описывая связность сети с точки зрения состояния каналов между маршрутизаторами, а не с точки зрения путей через сеть, протокол OSPF использует меньшую полосу пропускания и сходиться быстрее, чем другие протоколы. Когда канал на любом отдельном маршрутизаторе меняет состояние, рассматриваемый протокол распространяет только одно сообщение о состоянии этого канала по всему домену.

Недостаток данного протокола заключается в том, что процесс вычисления наилучших путей может быть относительно интенсивным по сравнению с протоколами дистанционно-векторной маршрутизации, в которых практически не требуется никаких вычислений, кроме выбора между несколькими маршрутами.

Основными компонентами OSPFv2 являются:

– маршрутизаторы, которые обрабатывают информацию и принимают решение о выборе маршрутов;

– область OSPF – логическая структура, объединяющая несколько сетей и маршрутизаторов;

– таблица маршрутизации (Routing Table), которая хранит информацию о всех доступных сетях.

Основными особенностями протокола являются:

– быстрая сходимость: изменения топологии сети распространяются только между соседними маршрутизаторами, что позволяет быстрее адаптироваться к ним;

– избыточность: OSPFv2 поддерживает избыточность связей, что повышает отказоустойчивость сети;

– масштабируемость: протокол может работать в крупных сетях с большим количеством устройств и соединений;

– безопасность: OSPFv2 поддерживает механизмы аутентификации и шифрования.

Одними из основных компонентов протокола являются ABR-маршрутизаторы (Area Border Router, далее по тексту – ABR), которые играют ключевую роль в процессе обмена информацией и маршрутизации между областями. ABR – это маршрутизатор, который служит пограничным узлом между различными областями в протоколе динамической маршрутизации. OSPF разбивает сеть на несколько областей, которые соединяются через ABR.

26.5.2 Основные настройки маршрутизации

Для включение OSPF-маршрутизатора применяется команда:

```
# set router ospf ipv4
```

Для выключения OSPF-маршрутизатора и удаления всех его настроек применяется команда:

```
# del router ospf ipv4
```

Настройка OSPF-маршрутизатора осуществляется на следующем уровне конфигурации:

```
[edit router ospf ipv4]
```

Настройка сетевых интерфейсов OSPF осуществляется на следующем уровне конфигурации:

```
[edit router ospf ipv4 interface]
```

26.5.2.1 Идентификатор маршрутизатора

Для определения идентификатора маршрутизатора процесса OSPF применяется команда:

```
[edit router ospf ipv4]
# set ospf router-id <router-id>
```

где `<router-id>` – IPv4-адрес в формате `A.B.C.D`.

Идентификатор должен быть уникальным во всём домене OSPF. Если идентификатор не указан явно, маршрутизатор OSPF создаст его автоматически на основании одного из IP-адресов интерфейсов в системе.

26.5.2.2 Тип ABR

OSPF не позволяет ABR (Area Border Router) рассматривать маршруты через немагистральные области, если его каналы с магистральной сетью не работают, даже если в

присоединённых немагистральных областях есть другие ABR, которые могут достичь магистральной сети. Данное ограничение накладывается во избежание петель маршрутизации.

Для настройки типа ABR применяется команда:

```
[edit router ospf ipv4]
# set ospf abr-type cisco|ibm|shortcut|standard
```

где

– `cisco` – тип, при указании которого маршрутизатор считает себя ABR, если он имеет несколько каналов к сетям различных областей и хотя бы одна из этих областей является магистральной, при этом канал к магистральной области активен;

– `ibm` – аналогичен типу `cisco`, но канал к магистрали может быть неактивным;

– `standard` – тип, при указании которого маршрутизатор имеет несколько активных каналов к различным областям;

– `shortcut` – аналогичен типу `standard`, при этом маршрутизатору разрешается использовать топологию не магистральных подключенных к нему областей для построения межобластных маршрутов, пролегающих через такие области.

Использование типа `cisco` или `ibm` позволяет ABR учитывать сводные данные, полученные от других ABR через немагистральные области, и маршрутизировать через немагистральные области только в случае, если магистральные каналы не работают.

26.5.2.3 Совместимость с RFC 2328

В RFC 2328 предлагается изменить алгоритм выбора предпочтительного пути для предотвращения возможных петель маршрутизации, допустимые в старой версии OSPFv2. Такое изменение требует, чтобы межобластные пути и внутриобластные магистральные пути имели одинаковое предпочтение, но по-прежнему были предпочтительнее внешних путей.

Для настройки совместимости с RFC 2328 применяется команда:

```
[edit router ospf ipv4]
# set ospf rfc1583compatibility
```

26.5.2.4 Таймеры

Для определения начальной задержки между расчётом SPF и событием, инициировавшим расчёт, применяется команда:

```
[edit router ospf ipv4]
# set timers throttle spf delay <timer-throttle-spf-delay-value>
```

где `<timer-throttle-spf-delay-value>` – число миллисекунд от 0 до 600 000.

Данная команда определяет минимальное время задержки расчёта SPF.

Для определения периода удержания между расчётом SPF и событием, которое инициировало расчёт, применяется команда:

```
[edit router ospf ipv4]
# set timers throttle spf initial-hold-time <timer-throttle-spf-initial-hold
-time-value>
```

где `<timer-throttle-spf-initial-hold-time-value>` – число миллисекунд от 0 до 600 000.

Данная настройка задаёт интервал удержания, которым разделяются вычисления SPF. Период удержания является адаптивным и изначально устанавливается равным значению начальной задержки в настройке `timers throttle spf delay`.

Для определения максимального периода удержания между расчётом SPF и событием, которое инициировало расчёт, применяется команда:

```
[edit router ospf ipv4]
# set timers throttle spf max-hold-time <timer-throttle-spf-max-hold-time-va
lue>
```

где `<timer-throttle-spf-max-hold-time-value>` – число миллисекунд от 0 до 600 000.

События, возникающие в течение периода удержания предыдущего расчёта SPF, приводят к увеличению значения периода удержания на значение начальной задержки, ограниченное значением максимального периода удержания (max-hold-time). Если время адаптивного удержания истекает без какого-либо события, запускающего SPF, текущее время удержания сбрасывается до начального времени удержания.

26.5.2.5 Совместимость с RFC 3137

В ПАК «Фортикс» обеспечивается поддержка RFC 3137, где процесс OSPF описывает свои транзитные каналы в LSA-маршрутизаторе как имеющие бесконечное расстояние, в связи с чем

другие маршрутизаторы не рассчитывают транзитные пути через маршрутизатор, но при этом могут подключаться к сетям через данный маршрутизатор.

Для включения поддержки RFC 3137 на неопределенный срок применяется команда:

```
[edit router ospf ipv4]
# set max-metric router-lsa administrative
```

Административное включение данной функции допускает вмешательство в расчёты по любой причине на неопределенный период времени.

Для включения поддержки RFC 3137 после запуска на указанный промежуток времени применяется команда:

```
[edit router ospf ipv4]
# set max-metric router-lsa on-startup <timer-on-startup-value>
```

где `<timer-on-startup-value>` – число секунд от 5 до 86400.

Включение данной функции на некоторое время после запуска позволяет OSPF полностью сходиться, не затрагивая существующие маршруты, используемые другими маршрутизаторами, и при этом обеспечивать доступность любых подключенных тупиковых каналов и/или перераспределённых маршрутов.

Для включения поддержки перед выключением на указанный промежуток времени применяется команда:

```
[edit router ospf ipv4]
# set max-metric router-lsa on-shutdown <timer-on-shutdown-value>
```

где `<timer-on-shutdown-value>` – период перед выключением (число секунд от 5 до 100).

Включение данной функции на некоторый промежуток времени перед выключением позволяет маршрутизатору корректно выйти из домена OSPF.

26.5.2.6 Настройка полосы пропускания

Для определения эталонной полосы пропускания для расчёта стоимости маршрута применяется команда:

```
[edit router ospf ipv4]
# set auto-cost-reference-bandwidth <auto-cost-reference-bandwidth-value>
```

где `<auto-cost-reference-bandwidth-value>` – число Мбит/с от 1 до 4294967, по умолчанию – 100.

По умолчанию канал с пропускной способностью 100 Мбит/с или выше имеет стоимость 1, стоимость каналов с более низкой пропускной способностью масштабируется с учётом установленного эталонного значения.

Значение должно быть одинаковым на всех OSPF-маршрутизаторах домена.

26.5.2.7 Включение интерфейсов

Для работы маршрутизатора OSPF необходимо указать интерфейсы, участвующие в работе протокола, и их принадлежность к областям OSPF.

Для соотнесения интерфейсов, IP-адреса которых включены в указанный диапазон, с областью применяется команда:

```
[edit router ospf ipv4]
# set network <network> area <area-id>
```

где

– `<network>` – IPv4-адрес в формате `A.B.C.D/mask`;

– `<area-id>` – идентификатор существующей области OSPF.

На указанных интерфейсах применяется маршрутизация OSPF, при этом их IP-сети анонсируются соседним маршрутизаторам.

Для включения маршрутизации OSPF на указанном интерфейсе применяется команда:

```
[edit router ospf ipv4]
# set interface <interface-name> area <area-id> [address <address>]
```

где

– `<interface-name>` – имя существующего интерфейса;

– `<area-id>` – идентификатор существующей области OSPF;

– `<address>` – (если интерфейс имеет несколько адресов) IPv4-адрес в формате `A.B.C.D/mask` интерфейса, который должен участвовать в маршрутизации.

Важно! Совместное использование команд `set network <network> ...` и `set interface <interface-name> area <area-id>` недопустимо.

26.5.3 Настройка зон

26.5.3.1 Обобщение маршрутов

Для объединения путей внутри области в одно Summary-LSA (Тип-3), объявляемое другим областям, применяется команда:

```
[edit router ospf ipv4]
# set area <area-id> ranges range <range>
```

где

– `<area-id>` – идентификатор существующей области OSPF;

– `<range>` – IPv4-адрес в формате `A.B.C.D/mask`.

Примечание – Данная команда применима только в ABR и только для Router-LSA (Тип 1) и Network-LSA (Тип 2). AS-external-LSA (Тип 5) суммировать нельзя, так как их область действия — AS.

Для отключения анонсирования внутренних путей зоны из указанного диапазона в другие области применяется команда:

```
[edit router ospf ipv4]
# set area <area-id> ranges range <range> not-advertise
```

где

– `<area-id>` – идентификатор существующей области OSPF;

– `<range>` – IPv4-адрес в формате `A.B.C.D/mask`.

Примечание – Данная команда имеет смысл только в ABR-маршрутизаторах.

26.5.3.2 Поддержка виртуальных каналов

Для включения поддержки виртуальных каналов необходимо указать значение `shortcut` в качестве параметра настройки `abr-type`.

Для настройки поддержки виртуальных каналов (см. RFC 3509) применяется команда:

```
[edit router ospf ipv4]
# set area <area-id> virtual-link <router-id>
# set area <area-id> shortcut enable
```

где

– `<area-id>` – идентификатор существующей области OSPF;

– `<router-id>` – идентификатор существующего маршрутизатора.

26.5.3.3 Настройка параметров зон

Тупиковой называется область, в которой ни один маршрутизатор не создаёт внешние по отношению к домену OSPF маршруты.

Для определения тупиковой зоны применяется команда:

```
[edit router ospf ipv4]
# set area <area-id> stub
```

где `<area-id>` – идентификатор существующей области OSPF.

NNSA-зоной (Not-So-Stubby Area – не совсем тупиковая область) называется область, позволяющая OSPF импортировать внешние маршруты в тупиковую область посредством LSA типа 7. Граничный маршрутизатор автономной системы NSSA (ASBR – Autonomous System Boundary Router) генерирует LSA данного типа. Граничный маршрутизатор области (ABR) преобразует LSA типа 7 в LSA типа 5, который распространяется в домен OSPF.

Для определения NSSA-зоны применяется команда:

```
[edit router ospf ipv4]
# set area <area-id> nssa
```

где `<area-id>` – идентификатор существующей области OSPF.

26.5.3.4 Настройка аутентификации

Для применения простой аутентификации с помощью пароля для указанной области применяется команда:

```
[edit router ospf ipv4]
# set area <area-id> authentication
```

где `<area-id>` – идентификатор существующей области OSPF.

Для применения аутентификации пакетов OSPF с помощью MD5 HMAC в пределах указанной области применяется команда:

```
[edit router ospf ipv4]
# set area <area-id> authentication message-digest
```

где `<area-id>` – идентификатор существующей области OSPF.

26.5.4 Команды для настройки интерфейсов

26.5.4.1 Включение OSPF на интерфейсе

Для включения OSPF на указанном интерфейсе применяется команда:

```
[edit router ospf ipv4]
# set interface <interface-name> area <area-id> [address <address>]
```

где

– `<interface-name>` – имя существующего интерфейса;

– `<area-id>` – идентификатор существующей области OSPF;

– `<address>` – IPv4-адрес в формате `A.B.C.D`.

26.5.4.2 Настройка аутентификации

Для настройки указанного простого пароля в качестве ключа аутентификации OSPF на указанном интерфейсе применяется команда:

```
[edit router ospf ipv4]
# set interface <interface-name> authentication-key <key-value>
```

где

– `<interface-name>` – имя существующего интерфейса;

– `<key-value>` – строка длиной от 1 до 8 символов.

По данной команде все пакеты OSPF аутентифицируются.

Для настройки аутентификации MD5 HMAC на указанном интерфейсе применяется команда:

```
[edit router ospf ipv4]
# set interface <interface-name> authentication message-digest
```

где `<interface-name>` – имя существующего интерфейса.

Для настройки указанного криптографического пароля в качестве ключа аутентификации OSPF на указанном интерфейсе применяется команда:

```
[edit router ospf ipv4]
# set interface <interface-name> message-digest-key <key-id> mds-key <mds-key>
```

где

– `<interface-name>` – имя существующего интерфейса;

– <key-id> – идентификатор от 1 до 255 секретного ключа, используемый для создания дайджеста сообщения;

– <mds-key> – фактический ключ дайджеста сообщения в формате строки длиной от 1 до 16 символов.

Для данной настройки используется криптографический алгоритм — MD5. Идентификатор <key-id> является частью протокола и должен быть одинаковым для всех маршрутизаторов в канале, при этом ключ <mds-key> связан с данным идентификатором.

26.5.4.3 Настройка приоритета маршрутизатора

Для настройки приоритета маршрутизации применяется команда:

```
[edit router ospf ipv4]
# set interface <interface-name> priority <priority-value>
```

где

– <interface-name> – имя существующего интерфейса;

– <priority-value> – число от 1 до 65535, по умолчанию – 1.

От значения приоритета напрямую зависит вероятность того, что маршрутизатор станет DR-маршрутизатором. Значение 0 лишает маршрутизатор права стать DR-маршрутизатором.

26.5.4.4 Настройка таймеров

Для настройки значения таймера Router Dead Interval, используемого в качестве таймера ожидания и таймера бездействия, применяется команда:

```
[edit router ospf ipv4]
# set interface <interface-name> dead-interval interval <interval-value>
```

где

– <interface-name> – имя существующего интерфейса;

– <interval-value> – число секунд от 1 до 65535, по умолчанию – 40.

Для настройки интервала отправки Hello-пакетов применяется команда:

```
[edit router ospf ipv4]
# set interface <interface-name> hello-interval <hello-interval-value>
```

где

– <interface-name> – имя существующего интерфейса;

– <hello-interval-value> – число от 1 до 65535, по умолчанию – 10.

Определение интервала отправки Hello-пакетов также возможно через настройку значения таймера Router Dead Interval равного 1 секунде и указание количества Hello-пакетов, отправляемых за 1 секунду, с помощью команды:

```
[edit router ospf ipv4]
# set interface <interface-name> dead-interval minimal hello-multiplier <hel
lo-multiplier-value>
```

где

– <interface-name> – имя существующего интерфейса;

– <hello-multiplier-value> – число от 2 до 20, 2 – отправка осуществляется каждые 500 мс, 20 – 50 мс.

С помощью данной команды можно получить время сходимости протокола равное 1 секунде.

Важно! При использовании данной команды настройка интервала отправки Hello-пакетов не учитывается.

26.5.5 Диагностика

Для просмотра общей информации об OSPF, состоянии области и конфигурации применяется команда:

```
> show router ospf ipv4
```

Для просмотра информации о состоянии и конфигурации OSPF-интерфейсов (указанного интерфейса) применяется команда:

```
> show router ospf ipv4 interface [<interface-name>]
```

где <interface-name> – имя существующего интерфейса.

Для просмотра информации LSA для LSDB применяется команда:

```
> show router ospf ipv4 neighbor [<interface-name>|all|detail]
```

где

– <interface-name> – имя существующего интерфейса;

– all – параметр, при указании которого отображается статус соседнего маршрутизатора;

– `detail` – параметр, при указании которого отображается информация о всех соседних маршрутизаторах.

Для просмотра таблиц маршрутизации OSPF, определённой на основе последнего расчёта SPF, применяется команда:

```
> show router ospf ipv4 route
```

Для просмотра всех маршрутов, полученных по протоколу OSPFv2, применяется команда:

```
> show router unicast ipv4 ospf
```

26.6 OSPFv3

26.6.1 Введение

ПАК «Фортикс» поддерживает протокол OSPF версии 3 для IPv6 сетей.

26.6.2 26.6.2 Настройка

Для включения OSPFv3-маршрутизатора применяется команда:

```
# set router ospf ipv6
```

Для выключения OSPFv3-маршрутизатора и удаления всех его настроек применяется команда:

```
# del router ospf ipv6
```

Настройка OSPFv3-маршрутизатора осуществляется на следующем уровне конфигурации:

```
[edit router ospf ipv6]
```

Настройка сетевых интерфейсов OSPF осуществляется на следующем уровне конфигурации:

```
[edit router ospf ipv6 interface]
```

Настройки уровня конфигурации OSPFv3-маршрутизатора аналогичны настройкам уровня конфигурации OSPFv2-маршрутизатора, за исключением формата адреса, который меняется с IPv4 на IPv6.

26.6.2.1 Таймер суммирования маршрутов

Для указания таймера агрегации, по завершении которого начинает работать суммирование маршрутов, применяется команда:

```
[edit router ospf ipv6]
# set aggregation timer <aggregation-timer-value>
```

где <aggregation-timer-value> – число секунд от 5 до 1800, по умолчанию – 5.

По данной команде изменяется период времени, по истечении которого отправляются внешние LSA.

26.6.2.2 Настройка зон

Для объединения путей внутри области в одно Summary-LSA (Тип-3), объявляемое другим областям, применяется команда:

```
[edit router ospf ipv6]
# set area <area-id> range <network> [not-advertise]
```

где

– <area-id> – идентификатор существующей области OSPFv3;

– <network> – IPv6-адрес в формате A:B:...:H/mask;

– [not-advertise] – параметр, при указании которого предотвращается анонсирование суммарных маршрутов.

26.6.2.3 Настройка полосы пропускания

Для определения эталонной полосы пропускания для расчёта стоимости маршрута применяется команда:

```
[edit router ospf ipv6]
# set auto-cost-reference-bandwidth <bandwidth-value>
```

где <bandwidth-value> – число Мбит/с от 1 до 4294967.

26.6.2.4 Настройка количества параллельных маршрутов

Для определения максимального количества параллельных маршрутов, поддерживаемых OSPFv3-маршрутизатором, применяется команда:

```
# set maximum-paths <maximum-paths-number>
```

где `<maximum-paths-number>` – число от 1 до 64, по умолчанию – 64.

26.6.2.5 Таймеры

Для определения начальной задержки между расчётом SPF и событием, инициировавшим расчёт, применяется команда:

```
[edit router ospf ipv6]
# set timers throttle spf delay <timer-throttle-spf-delay-value>
```

где `<timer-throttle-spf-delay-value>` – число миллисекунд от 0 до 600000.

Для определения периода удержания между расчётом SPF и событием, которое инициировало расчёт, применяется команда:

```
[edit router ospf ipv6]
# set timers throttle spf initial-hold-time <timer-throttle-spf-initial-hold
-time-value>
```

где `<timer-throttle-spf-initial-hold-time-value>` – число миллисекунд от 0 до 600000.

Для определения максимального периода удержания между расчётом SPF и событием, которое инициировало расчёт, применяется команда:

```
[edit router ospf ipv6]
# set timers throttle spf max-hold-time <timer-throttle-spf-initial-max-time
-value>
```

где `<timer-throttle-spf-initial-max-time-value>` – число миллисекунд от 0 до 600000.

26.6.2.6 Идентификатор маршрутизатора

Для определения идентификатора OSPFv3-маршрутизатора применяется команда:

```
[edit router ospf ipv6]
# set router-id <router-id>
```

где `<router-id>` – IPv4-адрес в формате `A.B.C.D`.

26.6.2.7 Протоколирование информации

Для добавления в журнал работы более подробной информации об изменениях в отношениях смежности между маршрутизаторами применяется команда:

```
[edit router ospf ipv6]
set log-adjacency-changes [detail]
```

где [detail] – параметр, при указании которого в журнал добавляются все изменения состояний.

26.6.2.8 Анонсирование маршрутов

Для настройки перераспределения маршрутов между протоколами маршрутизации применяется команда:

```
[edit router ospf ipv6]
# set redistribute <redistribute-setting> [metric <metric-value>] [route-map <route-map-name>]
```

где

– <redistribute-setting> – протокол маршрутизации;

– <metric-value> – значение метрики от 0 до 16;

– <route-map-name> – имя существующей карты маршрутов.

26.6.2.9 Настройка тупикового маршрутизатора

Для отключения режима транзитного маршрутизатора применяется команда:

```
[edit router ospf ipv6]
# set stub-router administrative
```

26.6.3 Диагностика

Для просмотра общей информации об OSPFv3, состоянии области и конфигурации применяется команда:

```
> show router ospf ipv6
```

Для просмотра информации о состоянии и конфигурации OSPFv3-интерфейсов применяется команда:

```
> show router ospf ipv6 interface [<interface-name>]
```

где <interface-name> – имя существующего интерфейса.

Для просмотра информации LSA для LSDB применяется команда:

```
> show router ospf ipv6 neighbor [<interface-name>|all|detail]
```

где

– `<interface-name>` – имя существующего интерфейса;

– `all` – параметр, при указании которого отображается статус соседнего маршрутизатора;

– `detail` – параметр, при указании которого отображается информация о всех соседних маршрутизаторах.

Для отображения таблицы маршрутизации OSPFv3, определённой на основе последнего расчёта SPF, применяется команда:

```
> show router ospf ipv6 route
```

Для отображения всех маршрутов, полученных по протоколу OSPFv3, применяется команда:

```
> show router unicast ipv6 ospf
```

26.7 BGP

Border Gateway Protocol (BGP) – протокол динамической маршрутизации, используемый для обмена информацией о достижимости различных IP-сетей и маршрутизации трафика между ними. Данный протокол является одним из стандартных протоколов междоменной маршрутизации.

Каждый маршрутизатор, работающий по протоколу BGP, имеет свою собственную таблицу маршрутизации, содержащую информацию о доступных через различные интерфейсы сетях. При обмене маршрутной информацией между двумя маршрутизаторами через BGP осуществляется обновление их таблиц маршрутизации на основе полученной информации, что позволяет выбирать наиболее оптимальный маршрут для каждого IP-пакета.

Важной особенностью BGP является его способность выбора маршрута на основе различных критериев, таких как стоимость, задержка, надёжность и т.д. Данная особенность позволяет протоколам маршрутизации выбирать оптимальный маршрут в зависимости от требований к качеству обслуживания и условий сети. Протокол BGP обеспечивает безопасность и конфиденциальность маршрутной информации, передаваемой между маршрутизаторами.

26.7.1 Основные понятия

26.7.1.1 Автономная система

Автономная система (далее по тексту – AS) – группа маршрутизаторов и сетей, которые совместно используют общую политику маршрутизации и соглашения о технических аспектах маршрутизации. В протоколе BGP автономные системы используются для разделения сетей на логические области, в которых осуществляется обмен маршрутной информацией и управление данными областями. Каждая автономная система имеет свой уникальный номер (далее по тексту – ASN), который используется для идентификации и маршрутизации трафика. Автономные системы взаимодействуют друг с другом по протоколу BGP, обмениваясь маршрутной информацией, выбирая оптимальные маршруты и обновляя свои таблицы маршрутизации.

26.7.1.2 Внутренний BGP (Internal BGP) и Внешний BGP (External BGP)

Внешний BGP (далее по тексту – External BGP, eBGP) — BGP-маршрутизатор, работающий между автономными системами. По умолчанию соседние eBGP-маршрутизаторы должны быть непосредственно соединены друг с другом.

При работе iBGP-маршрутизаторов в нетранзитной AS соединение между ними должно быть полносвязным: маршрутизатор, находящийся на границе AS и получивший обновление, передаёт его всем соседним маршрутизаторам. Соседние маршрутизаторы, находящиеся внутри автономной системы, перестают распространять это обновление, так как считают, что все соседние маршрутизаторы внутри AS уже его получили.

26.7.1.3 Семейство адресов

Расширение MP-BGP (Multiprotocol BGP) – расширение протокола BGP, которое позволяет маршрутизаторам поддерживать несколько протоколов маршрутизации в BGP-процессе, таких как IPv4, IPv6 и другие. MP-BGP позволяет более эффективно использовать ресурсы маршрутизатора и упрощает настройку и управление маршрутизацией.

26.7.1.4 Выбор маршрута

Процесс выбора маршрута в ПАК «Фортикс» осуществляется согласно следующим критериям принятия решения (начиная с верхней части списка и продвигаясь вниз до тех пор, пока не выполнится какой-либо критерий):

1) Проверка веса маршрута: предпочтительнее локальный маршрут с наибольшим весом;

2) Проверка приоритета: предпочтительнее локальный маршрут с наибольшим приоритетом;

3) Проверка типа маршрута: локальный маршрут (статический, перераспределённый) предпочтительнее полученного;

4) Проверка длины пути: предпочтительнее наиболее короткий маршрут (с меньшим числом переходов);

5) Проверка происхождения: предпочтительнее IGP-маршрут;

6) Проверка MED (Multi-Exit Discriminator): если маршруты с MED были получены от одной и той же AS, предпочтительнее маршрут с наименьшим MED;

7) Проверка источника: маршрут, полученный от внешнего узла eBGP, предпочтительнее маршрута, полученного от узла другого типа;

8) Проверка стоимости IGP: предпочтительнее маршрут с наиболее низкой стоимостью IGP;

9) Проверка multipath маршрутов;

10) Проверка на уже выбранный маршрут: из двух полученных от узлов eBGP маршрутов предпочтительнее уже выбранный;

11) Проверка идентификатора маршрутизатора: предпочтительнее маршрут с наименьшим идентификатором;

12) Проверка кластера: предпочтительнее маршрут с наименьшей длиной списка кластеров;

13) Проверка соседства: предпочтительнее маршрут, полученный от соседнего маршрутизатора с более высоким адресом.

26.7.1.5 Согласование возможностей (Capability)

Согласование возможностей позволяет BGP-маршрутизаторам обмениваться информацией о своих возможностях и определять наиболее подходящие параметры маршрутизации. Данный процесс позволяет улучшать производительность и безопасность BGP-сети, а также выбирать устройствам оптимальные маршруты на основе их возможностей и требований.

26.7.2 Настройка

Настройка BGP-маршрутизатора осуществляется на следующем уровне конфигурации:

```
[edit router bgp]
```

Для выключения BGP-маршрутизатора и удаления всех его настроек применяется команда:

```
# del router bgp
```

26.7.2.1 ASN и ID маршрутизатора

Для определения идентификатора автономной системы BGP-маршрутизатора применяется команда:

```
[edit router bgp]
# set local-as <local-as-id>
```

где `<local-as-id>` – число от 1 до 4294967295.

Данная команда включает BGP-маршрутизатор с указанным номером AS. Команда является обязательной для работы протокола. Протокол BGP использует идентификатор AS для определения того, является ли соединение BGP внутренним или внешним.

Для определения идентификатора маршрутизатора применяется команда:

```
[edit router bgp]
# set router-id <router-id>
```

где `<router-id>` – IPv4-адрес в формате `A.B.C.D`.

Если идентификатор не задан явно, выбирается наибольший из IP-адресов интерфейсов.

26.7.2.2 Настройка соседства с другими маршрутизаторами

Для установления соединения между BGP-маршрутизаторами необходимо настроить соединение как для соседнего, так и для локального маршрутизатора. При настройке соединения необходимо указать автономную систему соседнего маршрутизатора. По данной информации BGP определяет тип соседнего маршрутизатора:

– внутренний BGP-сосед (iBGP-сосед) — соседний маршрутизатор, находящийся в той же автономной системе, что и локальный маршрутизатор (iBGP-соседи не обязательно непосредственно соединены);

– внешний BGP-сосед (eBGP-сосед) — соседний маршрутизатор, находящийся в автономной системе, отличной от автономной системы локального маршрутизатора (по умолчанию, eBGP-соседи должны быть непосредственно соединены).

Существенные отличия между iBGP- и eBGP-маршрутизаторами выражаются в процессе отправки обновлений BGP и добавления маршрутов в таблицу маршрутизации.

Для настройки соединения с соседним маршрутизатором применяется команда:

```
[edit router bgp]
# set neighbor <neighbor-id> remote-as internal|external|<as-id>
```

где

– `<neighbor-id>` – идентификатор существующего соседнего маршрутизатора;

– `internal|external` – тип соседнего маршрутизатора;

– `<as-id>` – номер AS соседнего маршрутизатора.

При установлении соединения с соседним маршрутизатором проверяется, что:

– маршрутизатор получил запрос на TCP-соединение с адресом отправителя, находящегося в списке соседей данного маршрутизатора;

– номер автономной системы локального маршрутизатора совпадает с номером автономной системы, указанным на соседнем маршрутизаторе (исключение: настройки конфедераций);

– идентификаторы маршрутизаторов (router-id) отличаются друг от друга;

– соседние маршрутизаторы проходят аутентификацию, в случае если она настроена.

Для удобства настройки однотипных соединений предусмотрено создание именованных групп настроек, ссылаться на которые возможно при настройке соседства.

Для создания именованной группы настроек применяется команда:

```
[edit router bgp]
# set group <group-name>
```

где `<group-name>` – строка.

Пример конфигурации именованной группы настроек соседства:

```
router bgp {
  group mygrp remote-as 2
  neighbor 10.0.0.1 peer-group mygrp
  neighbor 10.0.0.2 peer-group mygrp
}
```

В данной конфигурации группе mygrp с номером AS 2 принадлежат соседние маршрутизаторы с номером AS, указанным в группе.

Для установления соседства между напрямую подключёнными eBGP-маршрутизаторами с использованием loopback-адресов применяется команда:

```
[edit router bgp]
# set neighbor <neighbor-id> disable-connected-check
```

где <neighbor-id> – идентификатор существующего соседнего маршрутизатора.

Для определения адреса или интерфейса, с которых рассылаются обновления, применяется команда:

```
[edit router bgp]
# set neighbor <neighborid> update-source <address>|<interface-name>
```

где

– <neighbor-id> – идентификатор существующего соседнего маршрутизатора;

– <address> – IPv4-адрес в формате A.B.C.D или IPv6-адрес в формате A:B:...:H;

– <interface-name> – имя существующего интерфейса.

При необходимости для указания описания соседнего маршрутизатора применяется команда:

```
[edit router bgp]
# set neighbor <neighbor-id> description <description>
```

где

– <neighbor-id> – идентификатор существующего соседнего маршрутизатора;

– <description> – строка длиной от 1 до 80 символов.

Пример настройки соседства:

```
[edit router bgp]
# set neighbor 172.16.12.2 description RemoteFortics
# commit
# do show router bgp summary

IPv4 Unicast Summary:
BGP router identifier 192.168.0.1, local AS number 65001 VRF default vrf-id
0
BGP table version 1
RIB entries 1, using 128 bytes of memory
Peers 3, using 71 KiB of memory

Neighbor        V         AS   MsgRcvd   MsgSent   TblVer  InQ OutQ  Up/Down
```

```
State/PfxRcd   PfxSnt Desc
172.16.12.2     4      65024         5         5        1    0    0 00:01:44
1        1 RemoteFortics
172.16.14.4     4      65024         0         0        0    0    0    never
Active        0 N/A
```

Для настройки времени задержки перед принятием решения о том, какие соседние маршрутизаторы могут быть объединены в группу обновлений для формирования единого обновления для них, применяется команда:

```
[edit router bgp]
set coalesce-time <coalesce-time-value>
```

где <coalesce-time-value> – число миллисекунд от 0 до 4294967295, по умолчанию – 1000.

Для принудительного использования формата Extended Optional Parameters Length в OPEN-сообщениях (RFC 9072) применяется команда:

```
[edit router bgp]
# set neighbor <neighbor-id> extended-optional-parameters
```

где <neighbor-id> – идентификатор существующего соседнего маршрутизатора.

По умолчанию пропускная способность в расширенных сообществах (extended communities) передаётся в кодировке формата IEEE с плавающей точкой. В более ранних версиях протокола значение пропускной способности расширенного сообщества передаётся в кодировке uint32.

Для обеспечения обратной совместимости возможно отключение кодировки IEEE с плавающей точкой с помощью команды:

```
[edit router bgp]
# set neighbor <neighbor-id> disable-link-bw-encoding-ieee
```

где <neighbor-id> – идентификатор существующего соседнего маршрутизатора.

Для определения всех маршрутов от указанного соседа как менее предпочтительных применяется команда:

```
[edit router bgp]
# set neighbor <neighbor-id> graceful-shutdown
```

где <neighbor-id> – идентификатор существующего соседнего маршрутизатора.

Для настройки соседнего маршрутизатора, до которого отсутствует прямое подключение, применяется команда:

```
[edit router bgp]
# set neighbor <neighbor-id> enforce-multihop
```

где <neighbor-id> – идентификатор существующего соседнего маршрутизатора.

Для определения явного количества переходов до соседнего маршрутизатора, для которого отсутствует прямое подключение, применяется команда:

```
[edit router bgp]
# set neighbor <neighbor-id> ttl-security hops <hops>
```

где

– <neighbor-id> – идентификатор существующего соседнего маршрутизатора;

– <hops> – число от 1 до 256.

Для понижения приоритета пути (увеличения административной дистанции), полученного по eBGP, до указанной подсети применяется команда:

```
[edit router bgp]
# set ipv4 unicast network <network-address> backdoor
```

где <network-address> – IPv4-адрес в формате A.B.C.D/mask.

Примечание – Данная команда применима, если к указанной сети уже существует более приоритетный маршрут, полученный от другого протокола маршрутизации.

Для включения механизма обнаружения петель в путях AS на стороне отправителя и фильтрации указанных маршрутов перед их отправкой применяется команда:

```
[edit router bgp]
# set neighbor <neighbor-id> sender-as-path-loop-detection
```

где <neighbor-id> – идентификатор существующего соседнего маршрутизатора.

26.7.2.3 Несколько автономных систем

ПАК «Фортикс» поддерживает запуск нескольких автономных систем (AS) одновременно. Каждая настроенная AS соответствует своей виртуальной таблице маршрутизации (VRF). Таким образом, использование VRF позволяет управлять несколькими автономными системами в одном BGP-процессе.

Каждую из используемых автономных систем необходимо настроить на отдельном уровне конфигурации VRF, которая должна быть уникальна по отношении ко всем другим VRF, используемым для той же цели: две различные автономные системы не могут использовать одну и ту же VRF, при этом одна и та же AS может использоваться с разными VRF.

Для настройки дополнительных автономных систем или маршрутизатора, ориентированного на указанную виртуальную таблицу маршрутизации, применяется команда:

```
# set vrf <vfr-name> router bgp local-as <as-id>
```

где

– `<vfr-name>` – имя виртуальной таблицы маршрутизации;

– `<as-id>` – номер AS соседнего маршрутизатора.

Пример конфигурации нескольких автономных систем:

```
router bgp {
  local-as 65001
  neighbor 192.168.1.1 remote-as 65020
  neighbor 192.168.1.2 remote-as 65030
}
vrf VRF1 router bgp {
  local-as 65002
  neighbor 192.168.1.3 remote-as 65040
  neighbor 192.168.1.4 remote-as 65050
}
vrf VRF2 router bgp {
  local-as 65003
  neighbor 192.168.1.5 remote-as 65060
  neighbor 192.168.1.6 remote-as 65070
}
```

26.7.2.4 Выбор маршрута

В данном разделе представлены команды для определения критериев выбора наилучшего маршрута.

Для учёта длины наборов и последовательностей путей конфедерации при выборе наилучшего маршрута применяется команда:

```
[edit router bgp]
# set bestpath-selection as-path confed
```

Для использования нескольких параллельных путей в таблице маршрутизации применяется команда:

```
[edit router bgp]
# set bestpath-selection as-path multipath-relax
```

Для сравнения идентификаторов маршрутизаторов применяется команда:

```
[edit router bgp]
# set bestpath-selection compare-router-id
```

Для применения в таблице маршрутизации нескольких параллельных путей, полученных от соседних маршрутизаторов разных типов, применяется команда:

```
[edit router bgp]
# set bestpath-selection peer-type multipath-relax
```

Для использования атрибутов AIGP для выбора наилучшего маршрута применяется команда:

```
[edit router bgp]
# set bestpath-selection aigp
```

Для учёта полосы пропускания при выборе наилучшего маршрута применяется команда:

```
[edit router bgp]
# set bestpath-selection bandwidth ignore|skip-missing|default-weight-for-mi
ssing
```

где

– `ignore` – параметр, при указании которого игнорируется пропускная способность канала пути;

– `skip-missing` – параметр, при указании которого не используются пути, у которых отсутствует информация о пропускной способности;

– `default-weight-for-missing` – параметр, при указании которого устанавливается наименьший приоритет (1) для путей без информации о пропускной способности.

26.7.2.5 Административное расстояние

Для настройки значения метрики локальных маршрутов применяется команда:

```
[edit router bgp]
# set ipv4|ipv6 unicast distance bgp local <local-distance>
```

где

– `ipv4|ipv6` – уровень конфигурации IPv4/IPv6;

– `<local-distance>` – число то 1 до 255.

Для настройки значения метрики внутренних маршрутов применяется команда:

```
[edit router bgp]
# set ipv4|ipv6 unicast distance bgp internal <internal-distance>
```

где

– ipv4|ipv6 – уровень конфигурации IPv4/IPv6;

– <internal-distance> – число то 1 до 255.

Для настройки значения метрики внешних маршрутов применяется команда:

```
[edit router bgp]
# set ipv4|ipv6 unicast distance bgp external <external-distance>
```

где

– ipv4|ipv6 – уровень конфигурации IPv4/IPv6;

– <external-distance> – число то 1 до 255.

Для настройки значения метрики для указанного префикса применяется команда:

```
[edit router bgp]
# set ipv4|ipv6 unicast distance administrative <distance> prefix <network>
[route-map <route-map-name>]
```

где

– ipv4|ipv6 – уровень конфигурации IPv4/IPv6;

– <distance> – число то 1 до 255;

– <network> – Pv4-адрес в формате A.B.C.D/mask или IPv6-адрес в формате A:B:...:H/mask в зависимости от текущего уровня конфигурации;

– <route-map-name> – имя существующей карты маршрутов.

26.7.2.6 Требование к политикам EBGP

В рамках соответствия RFC 8212 BGP-маршрутизатор требует применения входящих и исходящих фильтров для сеансов EBGP. Без входящих фильтров маршруты не принимаются, без исходящих фильтров – не анонсируются. Для изменения данного поведения применяется команда:

```
[edit router bgp]
# set no-ebgp-requires-policy
```

Без применения данной команды (при включённом требовании наличия фильтрации и ненастроенных входящих и исходящих фильтрах) вывод команды `show router bgp summary` содержит состояние `Policy`:

```
> show router bgp summary

IPv4 Unicast Summary (VRF default):
BGP router identifier 192.168.0.1, local AS number 65001 vrf-id 0
BGP table version 0
RIB entries 0, using 0 bytes of memory
Peers 1, using 20 KiB of memory

Neighbor        V         AS   MsgRcvd   MsgSent   TblVer  InQ OutQ  Up/Down
State/PfxRcd   PfxSnt Desc
10.0.0.24       4      65002         3         3        0    0    0 00:00:34
(Policy) (Policy) N/A

Total number of neighbors 1
```

Вывод данной команды также содержит сообщение об отклонении входящих и/или исходящих обновлений для соответствующего семейства адресов:

```
> show router bgp neighbors
...
 For address family: IPv4 Unicast
  Update group 1, subgroup 1
  Packet Queue length 0
  Community attribute sent to this neighbor(all)
  Inbound updates discarded due to missing policy
  Outbound updates discarded due to missing policy
  0 accepted prefixes
```

26.7.2.7 Принудительное использование номера первой AS

Для настройки отказа в обновлении, полученном от внешнего узла, для которого не указан номер его автономной системы в начале AS_PATH, применяется команда:

```
[edit router bgp]
# set neighbor <neighbor-id> enforce-first-as
```

где `<neighbor-id>` – идентификатор существующего соседнего маршрутизатора.

Важно! Если внешним узлом является сервер маршрутов (Route-Server), рекомендуется отключить данную настройку.

26.7.2.8 Отключение проверки типа подключения соседнего EBGP-маршрутизатора

По умолчанию BGP проверяет нахождение eBGP-соседа в непосредственно присоединённой сети локального маршрутизатора. Для отключения данной проверки применяется команда:

```
[edit router bgp]
# set disable-ebgp-connected-route-check
```

26.7.2.9 Демпфирование маршрутов BGP

Flap Dampening — механизм, используемый в протоколе маршрутизации BGP для предотвращения петель и других нежелательных состояний сети, вызванных частыми изменениями в состоянии соединений. Данный механизм позволяет снизить объём маршрутного трафика, передаваемого партнёрам, и уровень нагрузки на этих партнёров без существенного воздействия на время схождения сети. Механизм работает путём введения штрафа или задержки для обработки обновлений BGP, если маршрутизатор обнаруживает частые изменения в состоянии соединений или маршрутов.

В ПАК «Фортикс» предусмотрены команды для управления данным механизмом. Для определения времени «полужизни» применяется команда:

```
[edit router bgp]
# set ipv4|ipv6 unicast bgp dampening half-life-time <half-life-time>
```

где

– `ipv4|ipv6` – уровень конфигурации IPv4/IPv6;

– `<half-life-time>` – число минут от 1 до 45.

По истечении указанного в команде времени штраф на маршруте уменьшается экспоненциально до половины своего текущего значения.

Для определения значения порога повторного использования в механизме демпфирования применяется команда:

```
[edit router bgp]
# set ipv4|ipv6 unicast bgp dampening start-reusing <start-reusing>
```

где

– `ipv4|ipv6` – уровень конфигурации IPv4/IPv6;

– `<start-reusing>` – число от 1 до 20000.

При уменьшении количества накопленных штрафных очков до порога повторного использования интерфейс выходит из подавленного состояния и его непосредственно подключенный маршрут становится доступным другим устройствам в сети.

Для определения размера штрафа, выше которого маршрут подавляется, применяется команда:

```
[edit router bgp]
# set ipv4|ipv6 unicast bgp dampening start-suppressing <start-suppressing>
```

где

– `ipv4|ipv6` – уровень конфигурации IPv4/IPv6;

– `<start-suppressing>` – число от 1 до 50000.

Для определения максимального промежутка времени, в течение которого маршрут может игнорироваться, применяется команда:

```
[edit router bgp]
# set ipv4|ipv6 unicast bgp dampening max-duration <max-duration>
```

где

– `ipv4|ipv6` – уровень конфигурации IPv4/IPv6;

– `<max-duration>` – число минут от 1 до 255.

26.7.2.10 BGP MED

Атрибут BGP MED (Multi-Exit Discriminator) используется для выбора пути трафика в BGP, поступающего в автономную систему с несколькими точками выхода.

Атрибут используется принимающей AS для выбора наилучшего пути среди нескольких для достижения пункта назначения, транслируемого соседней AS. Меньшее значение MED предпочтительнее.

При использовании атрибута MED оказывается влияние на выбор пути для трафика, входящего в AS, и оптимизируется поток трафика между текущей и соседними AS.

Значение MED не распространяется за пределы соседней AS и может вызвать неожиданные проблемы с выбором пути при неправильном использовании.

В ПАК «Фортикс» доступно использование данного атрибута. Для сравнения различных значений MED, объявленных соседними маршрутизаторами в одной AS, для выбора наилучшего маршрута применяется команда:

```
[edit router bgp]
# set bestpath-selection deterministic-med
```

По умолчанию атрибут MED проверяется только при сравнении маршрутов из одной и той же AS.

Для сравнения атрибута MED для маршрутов, пришедших с разных AS, применяется команда:

```
[edit router bgp]
# set bestpath-selection always-compare-med
```

26.7.2.11 Механизм плавного перезапуска (graceful-restart)

Механизм плавного перезапуска BGP позволяет другим узлам BGP продолжать пересылать пакеты данных по известным маршрутам при восстановлении информации протокола маршрутизации.

При перезапуске BGP-маршрутизатора все узлы BGP обнаруживают прерывание сеанса, а затем – его возобновление. Данный переход приводит к колебаниям в сети и вызывает перерасчёт BGP-маршрутов, создание обновлений маршрутизации BGP и изменения в таблицах пересылки.

Механизм graceful-restart обеспечивает следующие функции:

– позволяет маршрутизатору, на котором осуществляется процесс перезапуска BGP-сессии, указывать соседнему узлу маршруты, которые он может сохранить в своей таблице пересылки на время перезапуска (возможность плавного перезапуска отправляется в сообщении OPEN во время установления сеанса);

– позволяет маршрутизатору объявлять всем остальным узлам маршруты, полученные от перезапускаемого маршрутизатора.

Для включения механизма применяется команда:

```
[edit router bgp]
# set neighbor <neighbor-id> graceful-restart
```

где `<neighbor-id>` – идентификатор существующего соседнего маршрутизатора.

Для отключения механизма применяется команда:

```
[edit router bgp]
# set neighbor <neighbor-id> graceful-restart disable
```

где `<neighbor-id>` – идентификатор существующего соседнего маршрутизатора.

Механизм graceful-restart-helper позволяет маршрутизаторам входить в режим помощника для поддержки плавного перезапуска соседнего маршрутизатора.

Для настройки механизма применяется команда:

```
[edit router bgp]
# set neighbor <neighbor-id> graceful-restart helper
```

где `<neighbor-id>` – идентификатор существующего соседнего маршрутизатора.

26.7.2.12 Анонсирование сетей

Для добавления анонсирования сетей для указанной подсети применяется команда:

```
[edit router bgp]
# set ipv4|ipv6 unicast network <network>
```

где

– `ipv4|ipv6` – уровень конфигурации IPv4/IPv6;

– `<network>` – IPv4-адрес в формате `A.B.C.D/mask` или IPv6-адрес в формате `A:B:...:H/mask` в зависимости от текущего уровня конфигурации.

Пример конфигурации с анонсированием сетей:

```
router bgp {
  local-as 65001
  ipv4 unicast network 10.0.0.0/8
}
```

В данной конфигурации сеть `10.0.0.0/8` объявляется всем соседним маршрутизаторам.

26.7.2.13 Роли BGP

Использование ролей BGP обеспечивает простой способ обнаружения и предотвращения утечек маршрутов (RFC 9234). Для включения механизма необходимо настроить локальную роль для взаимодействия с соседним маршрутизатором.

Для настройки доступны следующие роли:

– provider: может распространять любые маршруты к customer;

– customer: может распространять к provider локально созданные и полученные от другого customer маршруты (остальные маршруты не распространяются);

– rs-server (Route Server): может распространять любой доступный маршрут к rs-client;

– rs-client (Route Server Client): может распространять любой маршрут, полученный от customer или локально созданный, к rs-server (остальные маршруты не распространяются);

– peer: может распространять любой маршрут, полученный от customer или локально созданный, к другому peer (остальные маршруты не распространяются).

Значения ролей согласовываются на этапе определения соседства. Если роли маршрутизаторов соответствуют допустимым значениям, осуществляется обмен маршрутной информацией.

Допустимые пары для согласования:

– provider – customer;

– peer – peer;

– rs-server – rs-client.

Для определения локальной роли маршрутизатора применяется команда:

```
[edit router bgp]
# set neighbor <neighbor-id> local-role role provider|rs-server|rs-client|cu
stomer|peer
```

где

– `<neighbor-id>` – идентификатор существующего соседнего маршрутизатора;

– `provider|rs-server|rs-client|customer|peer` – роль.

Для включения жёсткого требования наличия роли у соседнего маршрутизатора применяется команда:

```
[edit router bgp]
# set router bgp neighbor <neighbor-id> local-role strict-mode
```

где <neighbor-id> – идентификатор существующего соседнего маршрутизатора.

26.7.2.14 Настройка согласования возможностей

При настройке соседства между BGP-маршрутизаторами осуществляется обмен информацией о поддерживаемых возможностях. Для включения строгого режима сравнения возможностей применяется команда:

```
[edit router bgp]
# set neighbor <neighbor-id> strict-capability-match
```

где <neighbor-id> – идентификатор существующего соседнего маршрутизатора.

Если возможности отличаются, при использовании данной команды соединение сбрасывается.

Для отключения функции отправки информации о поддерживаемых возможностях применяется команда:

```
[edit router bgp]
# set neighbor <neighbor-id> dont-capability-negotiate
```

где <neighbor-id> – идентификатор существующего соседнего маршрутизатора.

Для полного игнорирования возможностей удалённого соседа и принудительного использования локальных применяется команда:

```
[edit router bgp]
# set neighbor <neighbor-id> override-capability
```

где <neighbor-id> – идентификатор существующего соседнего маршрутизатора.

Для использования функции поддержки динамических возможностей применяется команда:

```
[edit router bgp]
# set neighbor <neighbor-id> capability dynamic
```

где <neighbor-id> – идентификатор существующего соседнего маршрутизатора.

Данная настройка позволяет сообщать об изменении возможностей узла BGP без необходимости перезапуска сеанса.

26.7.2.15 Поддержка IPv6

По умолчанию всем соседним маршрутизаторам объявляется только семейство одноадресных (unicast) IPv4-адресов. Прёем обновлений осуществляется только для одноадресных IPv4-адресов.

Для включения поддержки IPv6 для соответствующего семейства адресов применяется команда:

```
[edit router bgp]
# set ipv6 unicast neighbor <neighbor> activate
```

где `<neighbor-id>` – идентификатор существующего соседнего маршрутизатора.

Пример конфигурации одновременной поддержки одноадресных IPv4- и IPv6-адресов:

```
bgp {
  local-as 65002
  neighbor 10.0.0.23 remote-as 65001
  neighbor 2000::1 remote-as 65003
  ipv4 unicast {
    neighbor 10.0.0.23 activate
    network 192.168.1.0/24
  }
  ipv6 unicast {
    neighbor 2000::1 activate
    network 2000::99/64
  }
}
```

26.7.2.16 Суммирование маршрутов

Суммирование маршрутов в BGP – процесс объединения нескольких маршрутов с одинаковой метрикой (стоимостью) в один маршрут. Данный процесс позволяет уменьшить количество информации, передаваемой между маршрутизаторами, и улучшить масштабируемость BGP.

Маршруты с одинаковой стоимостью, полученные маршрутизатором от различных соседей, суммируются в один. Данный процесс может осуществляться как на уровне автономной системы, так и для некоторого префикса сети.

Например, если у маршрутизатора есть два пути с одинаковой метрикой к одной и той же сети, при этом один из них проходит через AS100, а другой – через AS200, маршрутизатор может суммировать эти два маршрута в один для минимизации количества обновлений BGP, которые он отправляет своим соседям.

Таким образом, суммирование маршрутов уменьшает количество обновлений BGP, что снижает нагрузку на сеть и улучшает масштабируемость. Уменьшение количества обновлений приводит к уменьшению количества изменений в сети, что улучшает её стабильность. Уменьшение количества маршрутов снижает объём трафика, передаваемого по сети.

26.7.2.16.1 Суммирование IPv4 маршрутов

Для настройки суммарного маршрута для указанной подсети применяется команда:

```
[edit router bgp]
# set ipv4 unicast aggregate-address <aggregate-address>
```

где `<aggregate-address>` – IPv4-адрес в формате `A.B.C.D/mask`.

Для применения данной команды в таблице BGP необходимо наличие более конкретного (более длинного) префикса.

Например, если необходимо создать суммарный префикс 10.0.0.0/24, следует убедиться, что есть любой другой меньший префикс в таблице BGP (например, 10.0.0.1/32 или 10.0.0.0/26).

Для применения карты маршрутов к суммарному префиксу используется команда:

```
[edit router bgp]
# set ipv4 unicast aggregate-address <aggregate-address> route-map <route-ma
p-name>
```

где

– `<aggregate-address>` – IPv4-адрес в формате `A.B.C.D/mask`;

– `<route-map-name>` – имя существующей карты маршрутов.

26.7.2.16.2 Суммирование IPv6 маршрутов

Для суммирования IPv6-маршрутов для указанной подсети применяется команда:

```
[edit router bgp]
# set ipv6 unicast aggregate-address <aggregate-address> [route-map <route-m
ap-name>]
```

где

– <aggregate-address> – IPv6-адрес в формате A:B:...:H/mask;

– <route-map-name> – имя существующей карты маршрутов.

26.7.2.17 Перераспределение маршрутов

Перераспределение маршрутов из других протоколов осуществляется в соответствии с выбранным семейством адресов – для семейства IPv4-адресов доступно перераспределение маршрутов протокола OSPFv2 и недоступно перераспределение OSPFv3.

Для настройки перераспределения маршрутов между протоколами маршрутизации применяется команда:

```
[edit router bgp]
# set ipv4|ipv6 unicast redistribute <redistribute-protocol> [metric <metric
>] [route-map <route-map-name>]
```

где

– ipv4|ipv6 – уровень конфигурации IPv4/IPv6;

– <redistribute-protocol> – протокол маршрутизации;

– <metric> – значение метрики от 0 до 4294967295;

– <route-map-name> – имя существующей карты маршрутов.

26.7.2.18 Сообщества

26.7.2.18.1 Атрибуты сообществ BGP

Атрибуты сообществ BGP используются для реализации политики маршрутизации. В ПАК «Фортикс» предусмотрена настройка атрибутов сообществ согласно сетевой политике. Атрибут сообщества — это набор значений сообщества, каждый из которых имеет длину 4 октета.

Атрибут может быть задан в виде значения AS:VAL, где

– AS — два октета старшего порядка в числовом формате;

– VAL — два октета младшего порядка в числовом формате.

Данный формат применим для определения значения политики, ориентированной на AS.

Атрибут может быть задан в виде одного из зарезервированных значений:

– accept-own – используется в протоколе BGP для принятия собственных анонсов (данный атрибут позволяет маршрутизатору BGP принимать собственные анонсы маршрутов от других соседей BGP, если они были изменены);

– accept-own-nexthop – используется в протоколе BGP для указания на возможность роутера использовать свой собственный адрес в качестве следующего перехода для анонсированных маршрутов;

– additive – используется в протоколе BGP для указания того, что объявление маршрутной информации должно быть добавлено к таблице маршрутов без замены существующих объявлений;

– blackhole – используется в протоколе BGP для обозначения маршрута, который должен быть удалён из таблицы маршрутизации;

– graceful-shutdown – используется в протоколе BGP для уведомления соседних устройств о том, что данный соседний BGP-маршрутизатор будет отключён, что позволяет соседним устройствам предпринять необходимые действия во избежание проблем с маршрутизацией;

– internet – используется в протоколе BGP для обозначения маршрута, ведущего во внешнюю сеть (если атрибут не указан, маршрут считается внутренним);

– llgr-stale – используется в протоколе BGP для сохранения устаревших маршрутов в течение более длительного промежутка времени после сбоя сеанса;

– local-AS – используется в протоколе BGP для обозначения маршрута, не объявляемого внешним узлам BGP (если соседний маршрутизатор является частью конфедерации, он считается внешним узлом BGP и маршрут узлу не объявляется);

– no-advertise – используется в протоколе BGP для обозначения маршрута, не объявляемого другим узлам BGP;

– no-export – используется в протоколе BGP для обозначения маршрута, не объявляемого за пределами границ конфедерации BGP (если соседний узел BGP является частью конфедерации BGP, считается, что узел находится внутри границы конфедерации BGP, поэтому маршрут объявляется узлу);

– no-llgr– используется в протоколе BGP для обозначения маршрутизаторов, получение маршрутов от которых даёт маршрутизатору право разрешать, отклонять или изменять маршруты при наличии или отсутствии данного сообщества;

– no-peer – используется для обозначения маршрута, который не нужно объявлять между соседними маршрутизаторами;

– route-filter-v4 и route-filter-translated-v4 – используются для фильтрации VPN IPv4-маршрутов;

– route-filter-v6 и route-filter-translated-v6 – используются для фильтрации VPN IPv6-маршрутов.

26.7.2.18.2 Списки сообществ (Communities Attribute)

Списки сообществ — определяемые администратором списки значений атрибутов сообщества. Данные списки используются для сопоставления атрибутов сообщества или управления ими в сообщениях UPDATE.

В ПАК «Фортикс» предусмотрены следующие типы списков:

– standard – содержит явные значения атрибутов;

– expanded – содержит регулярные выражения (так как регулярное выражение интерпретируется при каждом использовании, списки сообществ данного типа работают медленнее, чем standard списки).

Список типа standard может содержать значение атрибута сообщества в явном виде или в виде зарезервированного значения.

Для создания списка типа standard и указания в нём атрибута в явном виде применяется команда:

```
# set router community-list standard <standard-list-name> seq <seq> action d
eny|permit community <community-value>
```

где

– <standard-list-name> – слово;

– <seq-value> – порядковый номер правила от 1 до 4294967295;

– deny|permit – запрещающая или разрешающая политика;

– <value> – значение атрибута в формате AS:VAL.

Для создания списка типа standard и указания в нём атрибута в виде зарезервированного значения применяется команда:

```
# set router community-list standard <standard-list-name> seq <seq-value> ac
tion deny|permit community-attr <community-attr-value>
```

где

– <standard-list-name> – слово;

– <seq-value> – порядковый номер правила от 1 до 4294967295;

– deny|permit – запрещающая или разрешающая политика;

– <community-attr-value> – атрибут в виде зарезервированного значения из представленного в командной строке списка.

Для создания списка типа expanded и указания в нём атрибута в виде регулярного выражения применяется команда:

```
# set router community-list expanded <expanded-list-name> seq <seq-value> ac
tion deny|permit community <community-regex>
```

где

– <expanded-list-name> – слово;

– <seq-value> – порядковый номер правила от 1 до 4294967295;

– deny|permit – запрещающая или разрешающая политика;

– <community-regex> – шаблон соответствия в формате регулярного выражения.

Для просмотра актуальных списков применяется команда:

```
> show router community-list
```

26.7.2.18.3 Атрибуты расширенных сообществ (Extended Communities Attribute)

Атрибуты расширенных сообществ применяются в технологии MPLS VPN/BGP. Данные атрибуты позволяют использовать Route Target или Site of Origin для реализации сетевых политик.

Для создания списка типа standard и указания в нём атрибута в явном виде применяется команда:

```
# set router extcommunity-list standard <standard-list-name> seq <seq-value>
action deny|permit community <community-value>
```

где

– <standard-list-name> – слово;

– <seq-value> – порядковый номер правила от 1 до 4294967295;

– deny|permit – запрещающая или разрешающая политика;

– <community-value> – значение атрибута в формате AS:VAL.

Для создания списка типа `standard` и указания в нём атрибута в виде зарезервированного значения применяется команда:

```
# set router extcommunity-list standard <standard-list-name> seq <seq-value>
action deny|permit community-attr <community-attr-value>
```

где

– `<standard-list-name>` – слово;

– `<seq-value>` – порядковый номер правила от 1 до 4294967295;

– `deny|permit` – запрещающая или разрешающая политика;

– `<community-attr-value>` – атрибут в виде зарезервированного значения из представленного в командной строке списка.

Для создания списка типа `expanded` и указания в нём атрибута в виде регулярного выражения применяется команда:

```
# set router extcommunity-list expanded <expanded-list-name> seq <seq-value>
action deny|permit community <community-regex>
```

где

– `<expanded-list-name>` – слово;

– `<seq-value>` – порядковый номер правила от 1 до 4294967295;

– `deny|permit` – запрещающая или разрешающая политика;

– `<community-regex>` – шаблон соответствия в формате регулярного выражения.

Для просмотра актуальных списков применяется команда:

```
> show router extcommunity-list
```

26.7.2.18.4 Атрибуты больших сообществ (Large Communities Attribute)

Атрибуты BGP Large Communities аналогичны стандартным атрибутам BGP сообщества, за исключением того, что атрибуты большого сообщества состоят из трёх компонентов, каждый из которых имеет длину 4 октета. Большие сообщества обеспечивают дополнительный функционал и удобство по сравнению с традиционными сообществами; наличие у глобальной части ширины 4 октета допускает беспрепятственное применение в сетях, использующих 4-байтовые номера ASN (например, `AS:VAL1:VAL2`). Предусмотрены списки сообществ типа `standard` и `expanded`.

Для создания списка типа standard и указания в нём атрибута в явном виде применяется команда:

```
# set router large-community-list standard <standard-list-name> seq <seq-val
ue> action deny|permit community <community-value>
```

где

– <standard-list-name> – слово;

– <seq-value> – порядковый номер правила от 1 до 4294967295;

– deny|permit – запрещающая или разрешающая политика;

– <community-value> – значение атрибута в формате AS:VAL1:VAL2.

Для создания списка типа standard и указания в нём атрибута в виде зарезервированного значения применяется команда:

```
# set router large-community-list standard <standard-list-name> seq <seq-val
ue> action deny|permit community-attr <community-attr-value>
```

где

– <standard-list-name> – слово;

– <seq-value> – порядковый номер правила от 1 до 4294967295;

– deny|permit – запрещающая или разрешающая политика;

– <community-attr-value> – атрибут в виде зарезервированного значения из представленного в командной строке списка.

Для создания списка типа expanded и указания в нём атрибута в виде регулярного выражения применяется команда:

```
# set router large-community-list expanded <expanded-list-name> seq <seq-val
ue> action deny|permit community <community-regex>
```

где

– <expanded-list-name> – слово;

– <seq-value> – порядковый номер правила от 1 до 4294967295;

– deny|permit – запрещающая или разрешающая политика;

– <community-regex> – шаблон соответствия в формате регулярного выражения.

Для просмотра актуальных списков применяется команда:

```
> show router large-community-list
```

26.7.2.18.5 Использование атрибутов

В картах маршрутов (route-map) предусмотрено сопоставление (match) или определение (set) атрибутов сообществ BGP. При использовании данной функции реализуется сетевая политика на основе атрибутов сообществ BGP. Настройка данной функции осуществляются на следующем уровне конфигурации:

```
[edit router route-map <route-map-name>]
```

где <route-map-name> – имя существующей карты маршрутов.

Для определения значения сообщества в UPDATE-сообщениях в явном виде применяется команда:

```
[edit router route-map <route-map-name>]
# set community value <community-value>
```

где

– <route-map-name> – имя существующей карты маршрутов;

– <community-value> – значение атрибута в формате AS:VAL.

Для определения значения сообщества в UPDATE-сообщениях в виде зарезервированного значения применяется команда:

```
[edit router route-map <route-map-name>]
# set community attribute <community-attr-value>
```

где

– <route-map-name> – имя существующей карты маршрутов;

– <community-attr-value> – атрибут в виде зарезервированного значения из представленного в командной строке списка.

Для определения значения сообщества в UPDATE-сообщениях из списка стандартных сообществ применяется команда:

```
[edit router route-map <route-map-name>]
# set community-list <community-list-name>
```

где

– <route-map-name> – имя существующей карты маршрутов;

– <community-list-name> – имя существующего списка стандартных сообществ.

Для определения значения расширенного сообщества в UPDATE-сообщениях в явном виде применяется команда:

```
[edit router route-map <route-map-name>]
# set extcommunity rt <rt-value> soo <soo-value>
```

где

– <route-map-name> – имя существующей карты маршрутов;

– <rt-value> – значение атрибура Route Target в формате A.B.C.D:<0-65535> или <0-4294967295>:<0-65535>;

– <soo-value> – значение атрибура Site of Origin в формате A.B.C.D:<0-65535> или <0-4294967295>:<0-65535>.

Для определения значения расширенного сообщества в UPDATE-сообщениях из списка расширенных сообществ применяется команда:

```
[edit router route-map <route-map-name>]
# set extcommunity-list <extcommunity-list-name>
```

где

– <route-map-name> – имя существующей карты маршрутов;

– <extcommunity-list-name> – имя существующего списка расширенных сообществ.

Для определения значения большого сообщества в UPDATE-сообщениях в явном виде применяется команда:

```
[edit router route-map <route-map-name>]
# set large-community value <large-community-value>
```

где

– <route-map-name> – имя существующей карты маршрутов;

– <large-community-value> – значение атрибута в формате AS:VAL1:VAL2.

Для определения значения большого сообщества в UPDATE-сообщениях из списка больших сообществ применяется команда:

```
[edit router route-map <route-map-name>]
# set large-community-list <list-name>
```

где

– <route-map-name> – имя карты маршрутов;

– <list-name> – имя существующего списка больших сообществ.

Для определения соответствия сообщества списку стандартных сообществ применяется команда:

```
[edit router route-map <route-map-name>]
# set match community-list <community-list-name>
```

где

– <route-map-name> – имя существующей карты маршрутов;

– <community-list-name> – имя существующего списка стандартных сообществ.

Для определения соответствия расширенного сообщества списку расширенных сообществ применяется команда:

```
[edit router route-map <route-map-name>]
# set match extcommunity-list <extcommunity-list-name>
```

где

– <route-map-name> – имя существующей карты маршрутов;

– <extcommunity-list-name> – имя существующего списка расширенных сообществ.

Для определения соответствия большого сообщества списку больших сообществ применяется команда:

```
[edit router route-map <route-map-name>]
# set match large-community-list <large-community-list-name>
```

где

– <route-map-name> – имя существующей карты маршрутов;

– <large-community-list-name> – имя существующего списка больших сообществ.

26.7.2.19 Настройка BGP tcp-mss

Опция TCP-MSS применяется в BGP для определения максимального размера сегмента в байтах для TCP-соединений, используемых для обмена маршрутной информацией между соседними BGP-маршрутизаторами. Данная опция позволяет узлам корректно согласовывать MTU и устанавливать соответствующее значение MSS для предотвращения фрагментации пакетов при обмене BGP-сообщениями.

Для настройки данной опции применяется команда:

```
[edit router bgp]
# set neighbor <neighbor-id> tcp-mss <tcp-mss>
```

где

– <neighbor-id> – идентификатор существующего соседнего маршрутизатора;

– <tcp-mss> – максимальный размер сегмента в байтах от 1 до 65535.

26.7.2.20 Настройка быстрой сходимости

При переходе узла BGP в состояние «недоступен» сеанс BGP завершается немедленно, при этом немедленно завершаются только сеансы EBGP с одним переходом. Сеансы IBGP и многопереходные сеансы EBGP завершают сеанс по истечении таймера удержания.

Для настройки немедленного завершения сеансов BGP при переходе однорангового узла в состояние «недоступен» применяется команда:

```
[edit router bgp]
# set fast-convergence
```

По данной команде настройка применяется ко всем настроенным соседям.

Пример конфигурации с быстрой сходимостью:

```
router bgp {
  local-as 65001
  fast-convergence
  neighbor 192.168.1.1 remote-as 65001
  neighbor ff00::1 remote-as 65001
  ipv4 unicast neighbor 192.168.1.1 activate
  ipv6 unicast neighbor ff00::1 activate
}
```

26.7.3 Диагностика

Для просмотра IPv4-таблицы маршрутизации BGP протокола применяется команда:

```
> show router bgp ipv4 [<prefix> [bestpath|multipath]]
```

где

– <prefix> – IPv4-адерес в формате A.B.C.D/mask префикса сети для отображения в таблице;

– bestpath – параметр, при указании которого отображаются только bestpath-маршруты;

– multipath – параметр, при указании которого отображаются только multipath-маршруты.

Для просмотра IPv6-таблицы маршрутизации BGP протокола применяется команда:

```
> show router bgp ipv6 [<prefix> [bestpath|multipath]]
```

где

– `<prefix>` – IPv6-адерес в формате `A:B:...:H/mask` префикса сети для отображения в таблице;

– `bestpath` – параметр, при указании которого отображаются только bestpath-маршруты;

– `multipath` – параметр, при указании которого отображаются только multipath-маршруты.

Для просмотра информации о соседнем IPv4-маршрутизаторе применяется команда:

```
> show router bgp ipv4 neighbors <neighbor-id>
```

где `<neighbor-id>` – идентификатор существующего соседнего маршрутизатора.

Для просмотра информации о соседнем IPv6-маршрутизаторе применяется команда:

```
> show router bgp ipv6 neighbors <neighbor-id>
```

где `<neighbor-id>` – идентификатор существующего соседнего маршрутизатора.

Для просмотра всех IPv4-маршрутов, полученных по протоколу BGP, применяется команда:

```
> show router unicast ipv4 bgp
```

Для просмотра всех IPv6-маршрутов, полученных по протоколу BGP, применяется команда:

```
> show router unicast ipv6 bgp
```

26.8 ISIS

26.8.1 Введение

ISIS (Intermediate System to Intermediate System) – протокол маршрутизации, предназначенный для использования в крупных, сложных и динамических IP-сетях.

ISIS работает на 3 уровне модели OSI (сетевой уровень) и обеспечивает функции маршрутизации и сходимости для сетей IP. Одним из ключевых преимуществ протокола ISIS является его способность быстро и эффективно обрабатывать топологические изменения в сети. Данный протокол обеспечивает высокую масштабируемость и производительность, что позволяет использовать его в крупных сетевых инфраструктурах. Протокол ISIS является надёжным и

эффективным протоколом маршрутизации для сетевых инфраструктур, требующих высокой масштабируемости, производительности и способности обрабатывать сложные топологические изменения.

В сети ISIS разделение областей осуществляется по маршрутизаторам (а не по интерфейсам, как в OSPF). То есть, ISIS-маршрутизатор, в отличие от OSPF, не может находиться одновременно в различных областях.

ПАК «Фортикс» поддерживает два уровня доменов ISIS:

– L1 – соседство между маршрутизаторами формируется внутри одной области;

– L2 – соседство между маршрутизаторами может формироваться как внутри области, так и между разными областями.

На основе данных уровней можно выделить три типа маршрутизаторов в ISIS-домене:

– L1-маршрутизаторы – устройства, взаимодействие с другими маршрутизаторами которых осуществляются на уровне L1;

– L2-маршрутизаторы – устройства, все соседства которых организованы на уровне L2;

– L1/L2-маршрутизаторы – устройства, поддерживающие взаимодействия обоих уровней.

Всё множество L2-взаимодействий между маршрутизаторами непрерывно (связь L2-маршрутизаторов представляет собой ядро сети). На маршрутизаторе возможно формирование соседства обоих уровней через один интерфейс (маршрутизатор может на одном и том же интерфейсе формировать соседство уровня L1 и L2).

Для описания процесса ISIS используются следующие термины:

– LSP (Link-state Packet) – пакет состояния канала;

– CSNP (Complete Sequence Number PDU) – список всех состояний каналов (LSP) в базе данных состояний маршрутизатора (CSNP содержит LSP-идентификатор, время жизни (lifetime), порядковый номер и контрольную сумму для каждой записи в базе данных);

– PSNP (Partial Sequence Number PDU) – запрос ISIS-маршрутизатора, посылаемый для получения некоторой LSP-информации из базы данных соседнего маршрутизатора.

26.8.2 Настройка

Для включения ISIS-маршрутизатора в зоне с указанным идентификатором применяется команда:

```
# set router isis area <area-tag>
```

где `<area-tag>` – строка.

Для выключения ISIS-маршрутизатора и удаления всех его настроек применяется команда:

```
# del router isis
```

Настройка ISIS-маршрутизатора осуществляется на следующем уровне конфигурации:

```
[edit router isis area <area-tag>]
```

где `<area-tag>` – идентификатор существующей зоны.

Настройка сетевых интерфейсов ISIS осуществляется на следующем уровне конфигурации:

```
[edit router isis interface]
```

Идентификатор зоны (Area Tag), в которую входит ISIS-маршрутизатор, является условным именем, которое не участвует в процессе маршрутизации и не влияет на взаимодействие между устройствами. Применяется для настроек интерфейса, которые относятся к текущему ISIS-процессу.

Для определения идентификатора сети в ISO формате применяется команда:

```
[edit router isis area <area-tag>]
# set area-address <area-address>
```

где

– `<area-tag>` – идентификатор существующей зоны;

– `<area-address>` – идентификатор сети, который состоит из нескольких частей:

– AFI: Authority and Format Identifier: часть номера области длиной 1 байт;

– Area-ID: номер области, которой принадлежит маршрутизатор, длиной от 0 до 12 байт;

– System-ID: уникальный идентификатор маршрутизатора длиной 6 байт (по части System-ID маршрутизаторы узнают друг друга при определении топологии);

– Selector: принадлежность адреса длиной 1 байт (в ПАК «Фортикс» всегда имеет значение «00»).

При определении идентификатора сети применяется шестнадцатеричная система счисления; отдельные части адреса и 2-байтовые последовательности внутри Area-ID и System-ID разделяются точками.

Пример применения команды для определения идентификатора сети:

```
[edit router isis area 1]
# set area-address 49.0001.92168.3324.8700.00
```

Для настройки типа маршрутизатора в зависимости от уровня домена применяется команда:

```
[edit router isis area <area-tag>]
# set is-type level-1|level-2|level-1-2
```

где

– `<area-tag>` – идентификатор зоны (строка);

– `level-1|level-2|level-1-2` – уровень домена.

В ПАК «Фортикс» для ISIS-маршрутизации по умолчанию включена поддержка динамического имени хоста. Для её отключения применяется команда:

```
[edit router isis area <area-tag>]
# set disable-dynamic-hostname
```

где `<area-tag>` – идентификатор существующей зоны.

Для добавления в журнал работы более подробной информации об изменениях отношений смежности между маршрутизаторами применяется команда:

```
[edit router isis area <area-tag>]
# set log-adjacency-changes
```

где `<area-tag>` – идентификатор существующей зоны.

Для настройки поддержки формата пакета применяется команда:

```
[edit router isis area <area-tag>]
# set metric-style narrow|transition|wide
```

где

– `<area-tag>` – идентификатор существующей зоны;

– `narrow` – старый формат TLV с малой метрикой;

– `wide` – новый формат с большей метрикой;

– `transition` – оба формата.

Для настройки использования бита перезагрузки применяется команда:

```
[edit router isis area <area-tag>]
# set overload-bit
```

где <area-tag> – идентификатор существующей зоны.

Для настройки перераспределения IPv4-маршрутов между протоколами маршрутизации применяется команда:

```
[edit router isis area <area-tag>]
# set redistribute ipv4 <redistribute-protocol> level 1|2 [metric <metric>]
[route-map <route-map-name>]
```

где

– <area-tag> – идентификатор существующей зоны;

– <redistribute-protocol> – протокол маршрутизации;

– 1|2 – уровень домена;

– <metric> – значение метрики от 0 до 16777215;

– <route-map-name> – имя существующей карты маршрутов.

Для настройки перераспределения IPv6-маршрутов между протоколами маршрутизации применяется команда:

```
[edit router isis area <area-tag>]
# set redistribute ipv6 <redistribute-protocol> level 1|2 [metric <metric>]
[route-map <route-map-name>]
```

где

– <area-tag> – идентификатор существующей зоны;

– <redistribute-protocol> – протокол маршрутизации;

– 1|2 – уровень домена;

– <metric> – значение метрики от 0 до 16777215;

– <route-map-name> – имя существующей карты маршрутов.

26.8.2.1 Настройка аутентификации

Для настройки пароля аутентификации области в виде указанного открытого текста применяется команда:

```
[edit router isis area <area-tag>]
# set area-password password-type clear password <password>
```

где

– <area-tag> – идентификатор существующей зоны;

– <password> – строка длиной от 1 до 254 символов.

Для настройки указанного пароля аутентификации области с использованием MD5 хэш-суммы применяется команда:

```
[edit router isis area <area-tag>]
# set area-password password-type md5 password <password>
```

где

– <area-tag> – идентификатор существующей зоны;

– <password> – строка длиной от 1 до 254 символов.

Для настройки пароля аутентификации домена в виде указанного открытого текста применяется команда:

```
[edit router isis area <area-tag>]
# set domain-password password-type clear password <password>
```

где

– <area-tag> – идентификатор существующей зоны;

– <password> – строка длиной от 1 до 254 символов.

Для настройки указанного пароля аутентификации домена с использованием MD5 хэш-суммы применяется команда:

```
[edit router isis area <area-tag>]
# set domain-password password-type md5 password <password>
```

где

– <area-tag> – идентификатор существующей зоны;

– <password> – строка длиной от 1 до 254 символов.

26.8.2.2 Настройка таймеров

Для настройки минимального интервала повторной передачи одного и того же LSP для области (level-1) или домена (level-2) применяется команда:

```
[edit router isis area <area-tag>]
# set lsp timers level-1|level-2 generation-interval <generation-interval-va
lue>
```

где

– <area-tag> – идентификатор существующей зоны;

– level-1 – домен уровня 1 (область);

– level-2 – домен уровня 2 (домен);

– <generation-interval-value> – число секунд от 1 до 120.

Для настройки времени существование LSP для области (level-1) или домена (level-2) применяется команда:

```
[edit router isis area <area-tag>]
# set lsp timers level-1|level-2 maximum-lifetime <maximum-lifetime-value>
```

где

– <area-tag> – идентификатор существующей зоны;

– level-1 – домен уровня 1 (область);

– level-2 – домен уровня 2 (домен);

– <maximum-lifetime-value> – число секунд от 350 до 65535.

Для настройки интервала обновления LSP для области (level-1) или домена (level-2) применяется команда:

```
[edit router isis area <area-tag>]
# set lsp timers level-1|level-2 refresh-interval <refresh-interval-value>
```

где

– <area-tag> – идентификатор существующей зоны;

– level-1 – домен уровня 1 (область);

– level-2 – домен уровня 2 (домен);

– <refresh-interval-value> – число секунд от 0 до 65535.

Для настройки минимального интервала вычислений SPF для области (level-1) или домена (level-2) применяется команда:

```
[edit router isis area <area-tag>]
# set spf minimum-interval level-1|level-2 <minimum-interval-value>
```

где

– <area-tag> – идентификатор существующей зоны;

– level-1 – домен уровня 1 (область);

– level-2 – домен уровня 2 (домен);

– <minimum-interval-value> – число секунд от 0 до 120.

26.8.2.3 Настройка интерфейсов

Настройка сетевых интерфейсов ISIS осуществляется на следующем уровне конфигурации:

```
[edit router isis interface <interface-name>]
```

где <interface-name> – имя существующего интерфейса.

Для активации процесса ISIS на интерфейсе для IPv4-маршрутизации применяется команда:

```
[edit router isis interface <interface-name>]
# set ipv4 area <area-tag>
```

где

– <interface-name> – имя существующего интерфейса;

– <area-tag> – идентификатор существующей зоны.

Для активации процесса ISIS на указанном интерфейсе для IPv6-маршрутизации применяется команда:

```
[edit router isis interface <interface-name>]
# set ipv6 area <area-tag>
```

где

– <interface-name> – имя существующего интерфейса;

– <area-tag> – идентификатор существующей зоны.

Важно! Идентификатор зоны <area-tag> должен быть таким же, как в основных настройках маршрутизатора ISIS.

Для настройки указанного интерфейса в зависимости от уровня домена применяется команда:

```
[edit router isis interface <interface-name>]
# set circuit-type level-1|level-2|level-1-2
```

где

– <interface-name> – имя существующего интерфейса;

– level-1 – домен уровня 1;

– level-2 – домен уровня 2;

– level-1-2 – домен обоих уровней.

Для перевода указанного интерфейса в пассивный режим применяется команда:

```
[edit router isis interface <interface-name>]
# set passive
```

где <interface-name> – имя существующего интерфейса;

Для включения поддержки BFD на указанном интерфесе применяется команда:

```
[edit router isis interface <interface-name>]
# set bfd <bfd-profile>
```

где

– <interface-name> – имя существующего интерфейса;

– <bfd-profile> – имя BFD-профиля длиной от 1 до 24 символов.

Для настройки интервала передачи CSNP для области (level-1) или домена (level-2) на указанном интерфейсе применяется команда:

```
[edit router isis interface <interface-name>]
# set csnp-interval level-1|level-2 <csnp-interval>
```

где

– <interface-name> – имя существующего интерфейса;

– level-1 – домен уровня 1 (область);

– level-2 – домен уровня 2 (домен);

– <csnp-interval> – число секунд от 1 до 600.

Для настройки интервала передачи PSNP для области (level-1) или домена (level-2) на указанном интерфейсе применяется команда:

```
[edit router isis interface <interface-name>]
# set psnp-interval level-1|level-2 <psnp-interval>
```

где

– <interface-name> – имя существующего интерфейса;

– level-1 – домен уровня 1 (область);

– level-2 – домен уровня 2 (домен);

– <psnp-interval> – число секунд от 1 до 120.

Для настройки метрики для области (level-1) или домена (level-2) на указанном интерфейсе применяется команда:

```
[edit router isis interface <interface-name>]
# set metric level-1|level-2 <metric>
```

где

– <interface-name> – имя существующего интерфейса;

– level-1 – домен уровня 1 (область);

– level-2 – домен уровня 2 (домен);

– <metric> – число от 0 до 16777215.

26.8.3 Диагностика

Для просмотра общей информации об ISIS-маршрутизаторе применяется команда:

```
> show router isis summary
```

Для просмотра информации об интерфейсах, участвующих в ISIS-маршрутизации, применяется команда:

```
> show router isis interface [<interface-name>|detail]
```

где

– <interface-name> – имя существующего интерфейса;

– detail – параметр, при указании которого отображается детализированная информация.

Для просмотра информации о соседних ISIS-маршрутизаторах, доступных для обмена информацией, применяется команда:

```
> show router isis neighbor [detail]
```

где [detail] – параметр, при указании которого отображается детализированная информация.

Для просмотра таблицы ISIS-маршрутизации применяется команда:

```
> show router isis route backup|level-1|level-2|prefix-sid
```

где

– backup – параметр, при указании которого отображаются backup-маршрутизаторы;

– level-1 – параметр, при указании которого отображаются маршрутизаторы домена уровня 1;

– level-2 – параметр, при указании которого отображаются маршрутизаторы домена уровня 2;

– prefix-sid – параметр, при указании которого отображаются SID-префиксы.

Для просмотра всех IPv4-маршрутов, полученных по протоколу ISIS, применяется команда:

```
> show router unicast ipv4 isis
```

Для отображения всех IPv6-маршрутов, полученных по протоколу ISIS, применяется команда:

```
> show router unicast ipv6 isis
```

26.8.4 Пример конфигурации

На рисунке 5 представлена схема с упрощённой топологией ISIS-домена и основная конфигурация ISIS-маршрутизаторов. Маршрутизаторы R1 (level-1) и R2 (level-1-2) принадлежат к зоне A1, маршрутизатор R3 (level-2) – к зоне A2.

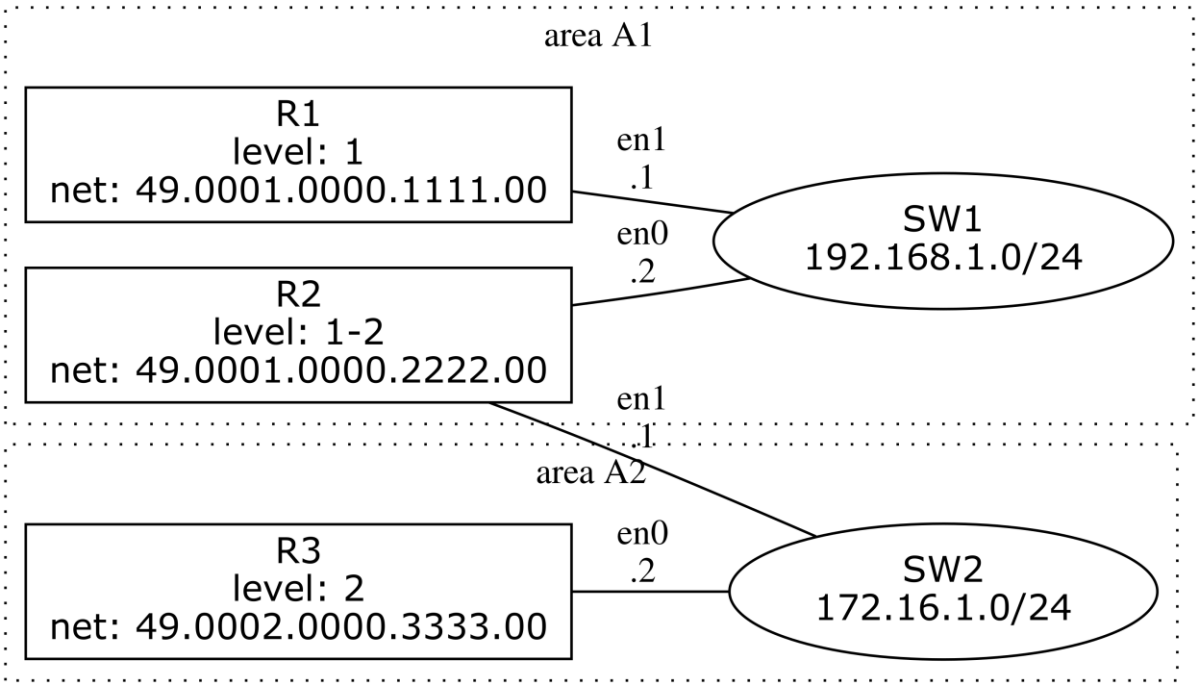

Рисунок 5 – Пример конфигурации ISIS.

Конфигурация маршрутизатора R1:

```
interface {
  ether en0 {
    enable
    ipv4 address 10.0.1.1/24
  }
  ether en1 {
    enable
    ipv4 address 192.168.1.1/24
  }
```

```
}
router isis {
  area A1 {
    is-type level-1
    area-address 49.0001.0000.1111.00
    area-address 49.1111.2222.0000.00
  }
  interface en1 {
    ipv4 area A1
    circuit-type level-1
  }
}
system hostname R1
```

Доступные соседние маршрутизаторы для маршрутизатора R1:

```
> show router isis neighbor
Area A1:
  System Id           Interface   L  State        Holdtime SNPA
 R2                  en1         1  Up           28       0800.2747.5067
```

Конфигурация маршрутизатора R2:

```
interface {
  ether en0 {
    enable
    ipv4 address 192.168.1.2/24
  }
  ether en1 {
    enable
    ipv4 address 172.16.1.1/24
  }
}
router isis {
  area A1 {
    is-type level-1-2
    area-address 49.0001.0000.2222.00
  }
  interface en0 {
    ipv4 area A1
    circuit-type level-1-2
  }
  interface en1 {
    ipv4 area A1
    circuit-type level-1-2
  }
}
system {
  hostname R2
  ipv4 forwarding
}
```

Доступные соседние маршрутизаторы для маршрутизатора R2:

```
> show router isis neighbor
Area A1:
  System Id           Interface   L  State        Holdtime SNPA
 R1                  en0         1  Up           29       0800.2735.6da7
 R3                  en1         2  Up           30       0800.271a.9d0d
```

Конфигурация маршрутизатора R3:

```
interface {
  ether en0 {
    enable
    ipv4 address 172.16.1.2/24
  }
  ether en1 {
    enable
    ipv4 address 10.0.255.1/24
  }
}
router isis {
  area A2 {
    is-type level-2
    area-address 49.0002.0000.3333.00
  }
  interface en0 {
    ipv4 area A2
    circuit-type level-2
  }
}
system hostname R3
```

Доступные соседние маршрутизаторы для маршрутизатора R3:

```
> show router isis neighbor
Area A2:
  System Id           Interface   L  State        Holdtime SNPA
 R2                  en0         2  Up           28       0800.271b.7022
```

26.9 BFD

26.9.1 Введение

BFD (Bidirectional Forwarding Detection) – протокол, предназначенный для обеспечения высокопроизводительной и надёжной сигнализации о состоянии канала связи. Используется в сетях, требующих высокой доступности и надёжности.

BFD обеспечивает быструю и надёжную проверку состояния канала. Протокол работает на сетевом уровне и позволяет устройствам быстро реагировать на изменения в сети: обнаруживать

отказы связи и восстанавливать соединения. Данный механизм позволяет минимизировать простои и обеспечивать высокую доступность сервисов.

Принцип работы BFD основан на периодической отправке и приёме специальных сообщений BFD между устройствами. Если устройства не получают данные сообщения в течение некоторого периода, протокол объявляет о проблеме с соединением. Время обнаружения отказа и время восстановления могут быть настроены в соответствии с требованиями к производительности и надёжности сети.

В ПАК «Фортикс» протокол BFD может использоваться в комбинации с другими протоколами динамической маршрутизации, такими как RIP, OSPFv2, OSPFv3, BGP, ISIS, и совместно со статической маршрутизацией.

Данный протокол предназначен для обеспечения надёжной и высокодоступной сетевой инфраструктуры, особенно в критически важных средах.

26.9.2 Настройка

Для обеспечения совместной работы протокола BFD с другими протоколами маршрутизации необходимо:

1) активировать работу протокола;

2) создать именованный профиль в настройках протокола BFD;

3) при необходимости внести изменения в работу протокола с помощью соответствующих настроек профиля;

4) связать выбранный протокол маршрутизации с именованным профилем протокола BFD.

26.9.2.1 Активация работы протокола

Для включения протокола BFD применяется команда:

```
# set router bfd
```

Важно! Данная команда только активирует работу протокола на маршрутизаторе, не оказывая влияния на работу протоколов статической и динамической маршрутизации.

Для выключения протокола и удаления всех его настроек применяется команда:

```
# del router bfd
```

26.9.2.2 Создание и настройка именованного профиля

Для создания именованного профиля с помощью команды:

```
# set router bfd profile <profile-name>
```

где <profile-name> – строка длиной от 1 до 64 символов.

26.9.2.2.1 Настройка профиля

В ПАК «Фортикс» пустой профиль по умолчанию является рабочим и доступным для использования, при этом его настройки изменяемы.

Настройка профиля осуществляется на следующем уровне конфигурации:

```
[edit router bfd profile <profile-name>]
```

где <profile-name> – имя существующего профиля.

Для настройки множителя обнаружения для определения потери пакетов применяется команда:

```
[edit router bfd profile <profile-name>]
# set detect-multiplier <detect-multiplier-value>
```

где

– <profile-name> – имя существующего профиля;

– <detect-multiplier-value> – число от 2 до 255.

Интервал передачи на удалённой стороне умножается на заданное в данной команде значение для определения таймера обнаружения потери соединения. Например, если в локальной системе множитель обнаружения равен 3, а в удалённой системе интервал передачи – 300 миллисекунд, локальная система обнаружит сбой через 900 миллисекунд.

Для настройки минимального значения TTL для входящего управляющего пакета BFD для сеансов с несколькими переходами применяется команда:

```
[edit router bfd profile <profile-name>]
# set minimum-ttl <minimum-ttl-value>
```

где

– <profile-name> – имя существующего профиля;

– <minimum-ttl-value> – число от 1 до 254.

Данная настройка применяется для усиления требований к проверке пакетов (во избежание получения пакетов управления BFD от других сеансов).

Для перевода текущего сеанса в пассивный режим применяется команда:

```
[edit router bfd profile <profile-name>]
# set passive-mode
```

где <profile-name> – имя существующего профиля.

В указанном режиме маршрутизатор не устанавливает BFD-соединение самостоятельно и ожидает управляющих пакетов от другого BFD-маршрутизаторам перед ответом. Данный механизм применяется во избежание отправки излишних управляющих пакетов BFD-протокола.

Для настройки минимального интервала приёма пакетов управления применяется команда:

```
[edit router bfd profile <profile-name>]
# set receive-interval <receive-interval-value>
```

где

– <profile-name> – имя существующего профиля;

– <receive-interval-value> – число миллисекунд от 10 до 60000.

Для настройки минимального интервала передачи для отправки пакетов управления применяется команда:

```
[edit router bfd profile <profile-name>]
# set transmit-interval <transmit-interval-value>
```

где

– <profile-name> – имя существующего профиля;

– <transmit-interval-value> – число миллисекунд от 10 до 60000.

26.9.2.2.1.1 Команды настройки эхо-режима

Для включения эхо-режима применяется команда:

```
[edit router bfd profile <profile-name>]
# set echo echo-mode
```

где <profile-name> – имя существующего профиля.

По умолчанию данный режим отключен.

П р и м е ч а н и е – После включения эхо-режима рекомендуется увеличить интервал передачи управляющих пакетов для снижения использования полосы пропускания, например с помощью команды `set transmit-interval 2000`.

Для настройки интервала передачи для отправки эхо-пакетов BFD применяется команда:

```
[edit router bfd profile <profile-name>]
# set echo transmit-interval <transmit-interval-value>
```

где

– `<profile-name>` – имя существующего профиля;

– `<transmit-interval-value>` – число миллисекунд от 10 до 60000.

Для настройки интервала приёма эхо-пакетов BFD применяется команда:

```
[edit router bfd profile <profile-name>]
# set echo receive-interval <receive-interval-value>
```

где

– `<profile-name>` – имя существующего профиля;

– `<receive-interval-value>` – число миллисекунд от 10 до 60000.

Для отключения приёма эхо-пакетов BFD применяется команда:

```
[edit router bfd profile <profile-name>]
# set echo receive-interval disable
```

где `<profile-name>` – имя существующего профиля.

26.9.2.3 Использование BFD в различных протоколах маршрутизации

Для использования протокола BFD в процессах других протоколов в настройках маршрутизации указывается имя профиля.

Ниже представлены форматы команд для использования профиля BFD в различных протоколах. Настройки применимы глобально или для указанного интерфейса/маршрута.

26.9.2.3.1 Протокол BGP

Для использования профиля BFD в протоколе BGP применяется команда:

```
# set router bgp neighbor <neighbor-address> bfd <profile-name>
```

где

– <neighbor-address> – IPv4-адрес в формате A.B.C.D или IPv6-адрес в формате A:B:...:H соседнего маршрутизатора;

– <profile-name> – имя существующего профиля.

26.9.2.3.2 Протокол OSPF

```
# set router ospf ipv4 interface <interface-name> bfd <profile-name>
```

где

– <interface> – имя существующего интерфейса;

– <profile-name> – имя существующего профиля.

26.9.2.3.3 Протокол OSPFv3

```
# set router ospf ipv6 interface <interface-name> bfd <profile-name>
```

где

– <interface> – имя существующего интерфейса;

– <profile-name> – имя существующего профиля.

26.9.2.3.4 Протокол RIP

```
# set router rip ipv4 interface <interface-name> bfd <profile-name>
```

где

– <interface> – имя существующего интерфейса;

– <profile-name> – имя существующего профиля.

26.9.2.3.5 Протокол ISIS

```
# set router isis interface <interface-name> bfd <profile-name>
```

где

– <interface> – имя существующего интерфейса;

– <profile-name> – имя существующего профиля.

26.9.2.3.6 Статическая маршрутизация

Для использования протокола BFD в настройках маршрутов (см. раздел «Стандартная статическая маршрутизация») указывается имя профиля. Таким образом, для использования протокола BFD в статической маршрутизации применяются следующие команды:

```
# set router unicast ipv4|ipv6 to <network> via gw <gateway> [dist <distance
>] [nexthop-vrf <nexthop-vrf-name>] bfd <profile-name>
# set router unicast ipv4|ipv6 to <network> via interface <interface-name> [
dist <distance>] [nexthop-vrf <nexthop-vrf-name>] bfd <profile-name>
# set router unicast ipv4|ipv6 to <network> via gw <gateway> interface <inte
rface-name> [dist <distance>] [nexthop-vrf <nexthop-vrf-name>] bfd <profile-
name>
# set router unicast ipv4|ipv6 to <network> via blackhole drop|reject [dist
<distance>] [nexthop-vrf <nexthop-vrf-name>] bfd <profile-name>
```

где

– ipv4|ipv6 – уровень конфигурации IPv4/IPv6;

– <network> – IPv4-адрес в формате A.B.C.D/mask или IPv6-адрес в формате A:B:...:H/mask префикса сети в зависимости от уровня конфигурации;

– <interface-name> – имя существующего интерфейса;

– <gateway> – следующий IPv4-адрес или IPv6-адрес маршрута в зависимости от уровня конфигурации;

– <distance> – административное расстояние от 1 до 255;

– <nexthop-vrf-name> – имя существующей виртуальной таблицы маршрутизации;

– drop|reject – режим отбрасывания пакетов (drop – пакеты отбрасываются без уведомления, reject – пакеты отбрасываются с ICMP-сообщением destination host unreachable);

– <profile-name> – имя существующего профиля.

26.9.3 Диагностика

Для просмотра информации о настройках состояния BFD-протокола для статической маршрутизации применяется команда:

```
> show router bfd static route
```

Для просмотра информации о всех BFD-узлах применяется команда:

```
> show router bfd peers [brief|counters]
```

где

– `brief` – параметр, при указании которого отображается информация в табличной форме;

– `counters` – параметр, при указании которого отображается информация о счётчиках.

Для просмотра статистики применяется команда:

```
> show router bfd distributed
```

27 Виртуальная маршрутизация (VRF)

VRF (Virtual Routing and Forwarding) – технология маршрутизации, позволяющая создавать виртуальные маршрутизаторы и сети внутри одного физического устройства. Данная технология используется для изоляции трафика между различными сетевыми доменами, обеспечивая безопасность и эффективность работы сети. Таким образом, с помощью VRF возможно разделение сети на несколько виртуальных, каждая из которых имеет свои собственные виртуальные таблицы маршрутизации (VRF-таблицы) и политики безопасности.

В ПАК «Фортикс» предусмотрено использование нескольких виртуальных таблиц маршрутизации, для каждой из которых задаётся имя, используемое в пределах одного устройства. По умолчанию в системе определена одна виртуальная таблица маршрутизации с зарезервированным именем `default`, являющаяся основной. Для создания дополнительных таблиц маршрутизации указывается имя VRF-таблицы и сетевые интерфейсы, соответствующие ей.

Для создания виртуальной таблицы маршрутизации применяется команда:

```
# set vrf <vrf-name>
```

где `<vrf-name>` – слово.

Пример применения команд для создания виртуальной таблицы маршрутизации:

```
# set vrf VRF1
# commit
# exit
> show vrf
vrf VRF1 id 14 table 32768 (configured)
```

Для удаления виртуальной таблицы маршрутизации применяется команда:

```
# del vrf <vrf-name>
```

где `<vrf-name>` – имя существующей виртуальной таблицы маршрутизации.

Настройка виртуальных таблиц маршрутизации осуществляется на следующем уровне конфигурации:

```
[edit vrf <vrf-name>]
```

где `<vrf-name>` – имя существующей виртуальной таблицы маршрутизации.

Для определения интерфейсов, соответствующих указанной виртуальной таблице маршрутизации, применяется команда:

```
[edit vrf <vrf-name>]
# set interface <interface-name>
```

где

– <vrf-name> – имя существующей виртуальной таблицы маршрутизации;

– <interface-name> – имя существующего интерфейса.

Пример применения команды для определения интерфейсов, соответствующих виртуальной таблице маршрутизации:

```
[edit vrf VRF1]
# set interface en1
# commit
```

При создании виртуальной таблицы маршрутизации автоматически создаётся одноименный VRF-интерфейс. Для просмотра интерфейсов, соответствующих VRF-таблице, применяется команда:

```
> show interface vrf <vfr-interface-name>
```

где <vfr-interface-name> – имя существующего VRF-интерфейса виртуальной таблицы маршрутизации.

Пример применения команды для просмотра VRF-интерфейсов:

```
> show interface vrf VRF1
en1 [ether]: <BROADCAST,MULTICAST> mtu 1500 qdisc noop master VRF1 state DOW
N group default qlen 1000
    link/ether 08:00:27:35:6d:a7 brd ff:ff:ff:ff:ff:ff
```

При создании VRF-таблицы автоматически создаётся маршрут по умолчанию (kernel-маршрут) с максимально высокой метрикой (недостижимый маршрут):

```
K>* 0.0.0.0/0 [255/8192] unreachable (ICMP unreachable)
```

Данная настройка гарантирует возможность переопределения недостижимого маршрута протоколами маршрутизации.

В ПАК «Фортикс» возможно применение VRF-таблиц с некоторыми службами и протоколами маршрутизации. Для этого на уровне конфигурации таблиц маршрутизации указываются настройки службы или протокола.

Для использования служб в VRF-домене применяется команда:

```
[edit vrf <vrf-name>]
# set service <service-name> enable
```

где

– `<vrf-name>` – имя существующей виртуальной таблицы маршрутизации;

– `<service-name>` – имя службы ПАК «Фортикс».

Для использования протоколов маршрутизации в VRF-домене применяется команда:

```
[edit vrf <vrf-name>]
# set router <router-protocol> ipv4|ipv6
```

где

– `<vrf-name>` – имя существующей виртуальной таблицы маршрутизации;

– `<router-protocol>` – протокол маршрутизации;

– `ipv4|ipv6` – уровень конфигурации IPv4/IPv6.

Для просмотра информации о протоколе маршрутизации, работающем в VRF-домене, применяются стандартные команды данного протокола для просмотра информации. При этом после слова `show` в команде указывается имя таблицы маршрутизации (`vrf <vrf-name>`).

Пример применения команд для просмотра информации о работе протокола маршрутизации OSPFv2 в виртуальном домене VRF1:

```
> show vrf VRF1 router ospf ipv4
VRF Name: VRF1
 OSPF Routing Process, Router ID: 1.1.1.1
 Supports only single TOS (TOS0) routes
```

Пример применения команд для просмотра информации об IPv4-таблице маршрутизации VRF1:

```
> show vrf VRF1 router unicast ipv4
Codes: K - kernel route, C - connected, L - local, S - static,
       R - RIP, O - OSPF, I - IS-IS, B - BGP, T - Table, v - VNC,
       V - VNC-Direct, t - Table-Direct,
       > - selected route, * - FIB route, q - queued, r - rejected, b - back
up
       t - trapped, o - offload failure

VRF VRF1:
K>* 0.0.0.0/0 [255/8192] unreachable (ICMP unreachable), 00:33:45
```

Важно! При одновременном использовании основной таблицы маршрутизации и виртуальной таблицы маршрутизации полная изоляция сетевых интерфейсов на устройстве

невозможна: если интерфейс «A» принадлежит основной таблице маршрутизации, а интерфейс «B» размещён в виртуальной таблице маршрутизации, то устройства из сети интерфейса «B» будут иметь доступ к интерфейсу «A», но устройства из сети интерфейса «A» не будут иметь доступ к интерфейсу «B». Для обеспечения полной изоляции сетевых интерфейсов внутри одного хоста рекомендуется применять отдельные виртуальные таблицы маршрутизации VRF, избегая при этом использования основной таблицы маршрутизации. Такой подход гарантирует изоляцию каждого интерфейса.

28 Мультикаст маршрутизация

Мультикаст-маршрутизация (далее по тексту – многоадресная маршрутизация, мультикаст, multicast) — технология, позволяющая экономить полосу пропускания посредством снижения трафика за счёт одновременной доставки единого потока информации множеству получателей.

Мультикаст является неотъемлемой технологией для передачи данных в реальном времени и потоковой передачи мультимедиа (используется в различных приложениях, таких как IPTV, дистанционное обучение, видеоконференции и т.д.).

Существуют несколько схем передачи сетевого трафика:

– одноадресная рассылка (unicast) — присутствует один отправитель и один получатель;

– широковещательная рассылка (broadcast) — присутствует один отправитель, получателями являются все устройства в широковещательном сегменте сети;

– произвольная рассылка (anycast) — одноадресная рассылка ближайшему узлу;

– многоадресная рассылка (multicast) — присутствует один отправитель, получателями являются некоторые устройства.

Подмножество принимающих устройств в мультикаст называется группой многоадресной рассылки, узлы, принадлежащие к группе многоадресной рассылки, – членами группы. Многоадресная рассылка ПАК «Фортикс» основана на данной групповой концепции. Группа многоадресной рассылки — это произвольное число получателей, присоединившихся к группе для получения потока данных от отправителя. Получатели (члены группы) могут располагаться в любой частной объединённой сети. Для получения данных от источника узлы присоединяются к соответствующей группе. Для отправки пакетов в группу не обязательно являться членом данной группы, при этом получать отправленные в группу пакеты могут только участники группы.

Для идентификации группы используется групповой адрес, по которому доставляются пакеты многоадресной рассылки. При одноадресной рассылке адрес получателя однозначно идентифицирует один хост. При многоадресной рассылке IP-адреса получателей не идентифицируют определённый хост. Для получения данных, отправленных на адрес многоадресной рассылки, хост присоединяется к группе, которую идентифицирует данный адрес: данные отправляются на адрес многоадресной рассылки и принимаются всеми хостами, присоединившимися к группе. Адрес группы многоадресной рассылки назначается на источнике, при этом назначаемые адреса должны соответствовать диапазону адресов многоадресной

рассылки. Для многоадресной рассылки зарезервированы IP адреса от 224.0.0.0 до 239.255.255.255.

ПАК «Фортикс» поддерживает следующие механизмы мультикаст-маршрутизации:

– статическая маршрутизация – используется для создания статических маршрутов в сети (позволяет определять правила, по которым маршрутизатор направляет пакеты в сеть; имеет ряд преимуществ, таких как простота настройки и отсутствие необходимости в обновлении маршрутов, при этом не может автоматически адаптироваться к изменениям в сети, что может привести к проблемам с производительностью);

– протокол IGMP – используется для управления группами мультикаст (позволяет узлам сообщать маршрутизатору об их необходимости присоединения к некоторой группе мультикаст; обеспечивает взаимодействие между узлами и маршрутизаторами);

– протокол PIM-SM (Protocol Independent Multicast) – используется для определения оптимального пути для мультикаст-трафика и координации обмена информацией между маршрутизаторами в сети (является одним из основных протоколов для мультикаст-маршрутизации).

28.1 Статическая мультикаст маршрутизация

Для добавления статического IPv4-мультикаст-маршрута применяется команда:

```
# set router multicast ipv4 from <from-interface-name> group <group-address> source <source-address> to <to-interface-name>
```

где

– `<from-interface-name>` – имя существующего интерфейса для входящего мультикаст-трафика;

– `<group-address>` – IPv4-адрес группы;

– `<source-address>` – IPv4-адрес источника;

– `<to-interface-name>` – имя существующего интерфейса для исходящего мультикаст-трафика.

Для добавления статического IPv6-мультикаст-маршрута:

```
# set router multicast ipv6 from <from-interface-name> group <group-address> source <source-address> to <to-interface-name>
```

где

– <from-interface-name> – имя существующего интерфейса для входящего мультикаст-трафика;

– <group-address> – IPv6-адрес группы;

– <source-address> – IPv6-адрес источника;

– <to-interface-name> – имя существующего интерфейса для исходящего мультикаст-трафика.

28.2 Настройка IGMP

ПАК «Фортикс» допускает работу в режиме проксирования мультикаст-данных, пересылая данные с входящего интерфейса на один или несколько исходящих. Для использования данного режима настраиваются входящий и исходящий интерфейсы. При наличии входящего и хотя бы одного исходящего интерфейса работа маршрутизатора активируется.

Настройка интерфейсов IGMP-маршрутизатора осуществляется на следующем уровне конфигурации:

```
[edit router igmp]
```

Для определения входящего (upstream) интерфейса применяется команда:

```
[edit router igmp]
# set input interface <interface-name>
```

где <interface-name> – имя существующего интерфейса.

Для определения исходящего (downstream) интерфейса применяется команда:

```
[edit router igmp]
# set output interface <interface-name>
```

где <interface-name> – имя существующего интерфейса.

Доступно определение нескольких исходящих интерфейсов.

Для управления объёмом информации, заносимой в журнал, применяется команда:

```
[edit router igmp]
# set log low|high
```

где

– low – параметр, при указании которого информация в журнал заносится менее подробно;

– high – параметр, при указании которого информация в журнал заносится более подробно.

Для использования функции быстрого выхода из группы применяется команда:

```
[edit router igmp]
# set quickleave
```

При нахождении источника мультикаст-данных в сети, отличной от сети входящего интерфейса, для корректной работы указывается адрес сети источника для входящего интерфейса с помощью команды:

```
[edit router igmp]
# set input interface <interface-name> subnet <subnet-address>
```

где

– <interface-name> – имя существующего входящего (upstream) интерфейса;

– <subnet-address> – IPv4-адрес в формате A.B.C.D/mask.

Для определения минимального значение TTL на указанном интерфейсе применяется команда:

```
[edit router igmp]
# set input|output interface <interface-name> threshold <threshold-value>
```

где

– input|output – тип интерфейса;

– <interface-name> – имя существующего интерфейса;

– <threshold-value> – число от 1 до 255.

Пакеты с более низким значением TTL отбрасываются.

28.3 Настройка PIM

Настройка PIM-маршрутизатора осуществляется на следующем уровне конфигурации:

```
# edit router pim ipv4
```

Включение PIM-маршрутизатора осуществляется автоматически при наличии необходимых для его работы настроек, отдельной команды для включения маршрутизатора не предусмотрено.

Административное расстояние одноадресной маршрутизации и метрика маршрутов настраиваются статически на каждом PIM-маршрутизаторе, так как автоматически данные параметры маршрутизаторами не определяются.

Для определения значения административного расстояния применяется команда:

```
[edit router pim ipv4]
# set default route distance <distance-value>
```

где `<distance-value>` – число от 1 до 255, по умолчанию – 101.

Для определения значения метрики применяется команда:

```
[edit router pim ipv4]
# set default route metric <metric-value>
```

где `<metric-value>` – число от 1 до 1024, по умолчанию – 1024.

Для обеспечения работы PIM-маршрутизатора необходимо указать интерфейсы, на которых он запускается, с помощью команды:

```
[edit router pim ipv4]
# set interface <interface-name> [priority <priority-value>] [scoped <scoped
-address>] [threshold <threshold-value>] [subnet <subnet-address>]
```

где

– `<interface-name>` – имя существующего интерфейса;

– `<priority-value>` – значение приоритета DR от 1 до 4294967294;

– `<threshold-value>` – минимальное значение TTL на интерфейсе от 1 до 255, по умолчанию – 1;

– `<subnet-address>` – IPv4-адрес сети источника мультикаст-данных, который указывается при нахождении источника мультикаст-данных вне сети входящего интерфейса, в формате `A.B.C.D/mask`;

– `<scoped-address>` – IPv4-адрес группы, исключённой из мультикаст-передачи, в формате `A.B.C.D/mask`.

Приоритет DR (Designated router – выделенный маршрутизатор) отправляется во всех сообщениях PIM Hello и используется вместо IP-адреса при всех выборах DR, если его объявляют все маршрутизаторы PIM в локальной сети. Чем меньше значение приоритета, тем маршрутизатор приоритетнее как DR.

Особенностью работы PIM-маршрутизатора является распространение многоадресной рассылки из точек встречи (RP/Rendezvous Points). Каждая RP обрабатывает распространение

одной или нескольких групп многоадресной рассылки. Возможна настройка маршрутизатора для объявления его в качестве кандидата на RP (CRP) или запроса статического RP-адреса для одной или нескольких групп многоадресной рассылки.

Для настройки статического адреса RP применяется команда:

```
[edit router pim ipv4]
# set rp static address <pr-address> group <group-address>
```

где

– <pr-address> – IPv4-адрес в формате A.B.C.D;

– <group-address> – IPv4-адрес мультикаст-группы в формате A.B.C.D/mask.

Для настройки CRP применяется команда:

```
[edit router pim ipv4]
# set rp candidate address <pr-address> group <group-address> [priority <pri
ority-value>] [interval <interval-value>]
```

где

– <pr-address> – IPv4-адрес RP в формате A.B.C.D/mask;

– <group-address> – IPv4-адрес мультикаст-группы в формате A.B.C.D/mask;

– <priority-value> – значение приоритета кандидата от 0 до 255, по умолчанию – 0;

– <interval-value> – интервал объявления CRP в секундах от 10 до 16383, по умолчанию – 60.

Приоритет кандидата демонстрирует, насколько важен данный CRP по сравнению с другими. Чем ниже значение приоритета, тем важнее CRP.

Для отслеживания всех RP предусмотрена функция Bootstrap Router (BSR). Выбранный BSR периодически объявляет набор RP в сообщениях Bootstrap. Для использования данной функции настраивается кандидат BSR (CBSR) с помощью команды:

```
[edit router pim ipv4]
# set bsr candidate [address <candidate-address>] [priority <priority>]
```

где

– <priority-value> – значение приоритета кандидата от 0 до 255, по умолчанию – 0;

– <candidate-address> – IPv4-адрес кандидата в формате A.B.C.D/mask.

Конфигурация маршрутизатора-кандидата (CBSR) схожа с конфигурацией CRP. Если адрес не указан, маршрутизатор использует самый высокий активный IP-адрес. Если приоритет не указан, значение приоритета маршрутизатора считается равным 0.

В домене маршрутизации возможно наличие нескольких путей от назначенного маршрутизатора (DR) отправителя многоадресной рассылки до получателя. При присоединении получателей к группам многоадресной рассылки все данные принимаются через общее дерево (RPT) от каждой точки встречи (RP). Так как в большинстве случаев маршрут через общее дерево не оптимален, при превышении объёма настраиваемого порога на маршрутизаторе последнего перехода или на самом RP, осуществляется попытка переключения на дерево кратчайшего пути (SPT) от источника многоадресной рассылки к получателю.

Для настройки значения порога скорости трафика применяется команда:

```
[edit router pim ipv4]
# set spt-threshold rate <rate-value>
```

где `<rate-value>` – число битрейтов от 0 до 4294967295.

Для настройки значения порога количества пакетов применяется команда:

```
[edit router pim ipv4]
# set spt-threshold packets <packets-value>
```

где `<packets-value>` – число от 0 до 4294967295.

Для определения интервала осуществления сопоставления значений с пороговыми применяется команда:

```
[edit router pim ipv4]
# set spt-threshold interval <interval-value>
```

где `<interval-value>` – число секунд от 5 до 1000000.

28.4 Диагностика

Для просмотра таблицы мультикаст маршрутизации применяется команда:

```
> show router multicast ipv4|ipv6 [groups|vifs]
```

где

– `ipv4|ipv6` – уровень конфигурации IPv4/IPv6;

– `groups` – параметр, при указании которого отображаются присоединенные группы;

– `vifs` – паоаметр, при указании которого отображаются виртуальные интерфейсы.

Для просмотра информации о мультикаст-группах применяется команда:

```
> show router multicast ipv4 groups
```

Для просмотра информации о виртуальных интерфейсах (vif) применяется команда:

```
> show router multicast ipv4 vifs
```

Для просмотра информации о работе PIM-маршрутизатора применяется команда:

```
> show router pim ipv4 [compat|crp|igmp|interfaces|mrt|rp|status]
```

где

– `compat` – параметр, при указании которого отображается статус PIM в режиме compat;

– `crp` – параметр, при указании которого отображается набор CRP;

– `igmp` – параметр, при указании которого отображается статус интерфейса IGMP и членство в группах;

– `interfaces` – параметр, при указании которого отображается таблица интерфейсов PIM;

– `mrt` – параметр, при указании которого отображается таблица многоадресной маршрутизации;

– `rp` – параметр, при указании которого отображается установленная RP;

– `status` – параметр, при указании которого отображается статус PIM.

29 Обслуживание

29.1 Общие сведения

ПО ПАК «Фортикс» представлено в виде файлов с расширением **.fors**, используемых для обновления установленных прошивок ПО на платформе. На одной платформе возможна одновременная установка нескольких прошивок ПО ПАК «Фортикс». Далее по тексту для установленных прошивок применяются термины **система** или **software**.

Для каждой системы возможно выделение собственной закреплённой за ней области для хранения данных. Данная область называется **слот данных** или **data-slot**. Возможно наличие системы без слота данных в пассивном режиме на устройстве хранения данных, при этом функционирование данной системы не осуществляется. Для вновь установленной системы слот данных выделяется автоматически при загрузке или привязывается вручную к уже существующему слоту данных.

Идентификация каждой системы и каждого слота данных осуществляется уникальным именем, используемым для осуществления различных действий над установленными прошивками ПО и слотами данных.

Для активной (загруженной в настоящее время на платформе) системы и слота данных применим ограниченный набор действий в связи с возможными нарушениями работы системы, которые могут возникнуть из-за изменений (например, удаление активного слота данных недоступно).

Для систем ПАК «Фортикс» предусмотрены следующие загрузочные признаки:

– default – система, загружаемая по-умолчанию;

– fallback – система, загружаемая в случае невозможности загрузки `default` системы (например, из-за аппаратного или программного сбоя);

– current – активная система.

Для просмотра данных признаков применяется команда:

```
> show system software
```

В выводе команды указываются следующие загрузочные признаки в круглых скобках:

– D – default: после перезагрузки система с флагом D загружается по умолчанию;

– F – fallback: при возникновении проблем с загрузкой системы по умолчанию (с флагом D) осуществляется откат к резервной системе (с флагом F);

– C – current: загруженная в данный момент система;

– d – user default: система помечена администратором как система по умолчанию, но произошёл откат к резервной системе по какой-либо причине.

29.2 Управление прошивками и системами

Для установки новой прошивки ПО ПАК «Фортикс» с указанным именем из fors-файла применяется команда:

```
> system software install <file-name> [<system-name>]
```

где

– `<file-name>` – полное имя fors-файла или имя файла относительно домашней директории пользователя;

– `<system-name>` – строка.

Для настройки загрузочного признака системы применяется команда:

```
> system software boot default|fallback <system-name>
```

где

– `default|fallback` – загрузочный признак системы;

– `<system-name>` – имя существующей системы.

Для удаления существующей системы применяется команда:

```
> system software remove <system-name> [with-data-slot]
```

где

– `<system-name>` – имя существующей системы;

– `with-data-slot` – параметр, при указании которого система удаляется с привязанным к ней слотом данных.

Возможно удаление только той системы, у которой нет ни одного признака успешной загрузки (default, fallback, current).

Для переименования установленной системы применяется команда:

```
> system software rename <system-name> <new-system-name>
```

где

– <system-name> – текущее имя системы;

– <new-system-name> – строка.

Для привязки системы к существующему слоту данных применяется команда:

```
> system software bind <system-name> [<dataslot-name>]
```

где

– <system-name> – имя существующей системы;

– <dataslot-name> – имя существующего слота данных.

Если параметр <dataslot-name> не указан, система отвязывается от её текущего слота данных (невозможно для активной системы). Привязка для активной системы или для уже привязанного к какой-либо системе слота данных невозможна.

Для осуществления миграции применяется команда:

```
> system software migrate <system-name> [force] [reboot]
```

где

– <system-name> – имя существующей системы, на которую осуществляется миграция;

– force – параметр, при указании которого миграция осуществляется даже в случае, если система <system-name> привязана к другому слоту данных (при этом система <system-name> предварительно отвязывается от указанного слота данных и привязывается к текущему);

– reboot – параметр, при указании которого осуществляется перезагрузка после успешной миграции.

Миграция подразумевает установку загрузочного признака default на систему <system-name>, привязку к ней текущего слота данных и перезагрузку на новую default-систему <system-name>. Данный механизм применим после обновления системы при необходимости использования текущей конфигурации.

Для осуществления безопасной миграции применяется команда:

```
> system software safe-migrate <system-name> [force]
```

где

– <system-name> – имя существующей системы, на которую осуществляется миграция;

– force – параметр, при указании которого миграция осуществляется даже в случае, если система <system-name> привязана к другому слоту данных (при этом система <system-name>

предварительно отвязывается от указанного слота данных и привязывается к клонированному слоту данных).

29.3 Управление слотами данных

Для создания нового пустого слота данных с указанным именем применяется команда:

```
> system data-slot create <dataslot-name>
```

где <dataslot-name> – строка.

Для клонирования слота данных применяется команда:

```
> system data-slot clone <dataslot-name> <new-dataslot-name>
```

где

– <dataslot-name> – имя существующего слота данных, содержимое которого дублируется в новый слот данных;

– <new-dataslot-name> – строка.

Для переименования существующего слота данных применяется команда:

```
> system data-slot rename <dataslot-name> <dataslot-new-name>
```

где

– <dataslot-name> – текущее имя слота данных;

– <dataslot-new-name> – строка.

Для удаления существующего слота данных применяется команда:

```
> system data-slot remove <dataslot-name>
```

где <dataslot-name> – имя существующего слота данных.

Данная команда неприменима для привязанных к какой-либо системе слотов данных.

29.4 Информационные команды

Для просмотра информации о версии системы применяется команда:

```
> show version
```

Пример вывода команды для просмотра информации о версии системы:

```
Software: Fortics 1.0d-250825
Version: 1.0
Revision: r1.d0cc757757
```

```
Date: 2025.08.25 12:55:20
Kernel: 5.10.226 x86_64 console=ttyS0,115200
Status: cer r1 debug
HWID: 010-00001
Hash (kernel): 921c3f947945a49b2a91daec2c23056b4c242493df967e7c7f828e0df1d73
700
Hash (rootfs): 0e375df2f4ae7df399178312cec21087fe5ef551998e554bee43f70a9a99c
b66
Hash (loader): 60b4acc007dc982e1874dddf642d212fadb9cb0f32ff061b6da94db5e7f97
d32
Hash (crypto): b418266bcdd7b2ac8fc6d98b7e0e9e437c30416dcb9486cdc426a8a85a804
879
```

Для просмотра информации об установленных системах, их загрузочных признаках, слотах данных применяется команда:

```
> show system software
```

Для просмотра списка установленных систем применяется команда:

```
> show system software list
```

Для просмотра подробной информации об установленной системе применяется команда:

```
> show system software info [<system-name>|*]
```

где

– `<system-name>` – имя системы, о которой выводится информация;

– * – параметр, при указании которого отображается информация о всех системах.

Для просмотра списка слотов данных применяется команда:

```
> show system data-slot
```

29.5 Лицензия системы

Доступный функционал в системе определяется лицензией, которая содержит описание разрешённых и запрещённых возможностей. Предусмотрены следующие типы лицензии:

– `built-in` – встроенная (предустановленная) лицензия, добавленная при создании дистрибутива (в системе допустимо наличие только одной лицензии данного типа);

– `installed` – лицензия, установленная из fors-файла (в системе допустимо наличие нескольких лицензий данного типа);

– `user` – лицензия, установленная пользователем командой из системы (в системе допустимо наличие только одной лицензии данного типа).

Для просмотра текущей лицензии применяется команда:

```
> show system software license
```

Пример вывода команды для просмотра текущей лицензии:

```
Info: License type: installed (valid)
Info: License data: {
        «license»: {
                «ALL»: true,
                «DESCRIPTION»: «Full»
        }
}
```

Для описания лицензии по умолчанию используются слудующие поля:

– ALL: признак, используемый по умолчанию для всего функционала системы (возможные значения: true – всё разрешено, false – всё запрещено);

– LIMITS: ограничения для системы, на которую устанавливается лицензия (опционально);

– DESCRIPTION: описание лицензии.

Поле LIMITS задаёт ограничения для системы, на которую устанавливается лицензия, по следующим параметрам:

– ncpu – область допустимых значений числа CPU;

– memsz – область допустимых значений объёма памяти в байтах;

– version – область допустимых значений версий системы (версия системы указывается в формате `x.y` или `x.y[-z]`, где x,y,z – числа);

– variant – допустимый вариант системы («d» – отладочная система, «vm» – система для виртуальных машин, «» – система без варианта);

– validtime – период действия лицензии (время указывается в формате `yyyy.mm.dd`).

Ограничения в поле LIMITS задаются с помощью критериев min и max (кроме ограничения variant, которое задаётся строкой), определяющих область допустимых значений ограничения:

– если min и max не указаны – ограничений нет;

– если указан только min – допустимые значения определяются областью [min; UNLIMITED];

– если указан только max – допустимые значения определяются областью [UNLIMITED; max];

– если указан min и max – допустимые значения определяются областью [min; max].

Остальные поля лицензии определяют разрешённый (true) или запрещённый (false) функционал системы.

Пример описания лицензии:

```
«ALL» : false,
«dns» : true,
```

В этом примере запрещён весь функционал, кроме dns.

Для добавления лицензии применяется команда:

```
> system software license add <license-file>
```

где `<license-file>` – полное имя файла лицензии или имя файла относительно домашней директории пользователя.

При добавлении лицензии проверяется, удовлетворяет ли система, на которую устанавливается лицензия, ограничениям поля LIMITS устанавливаемой лицензии. Для ограничений ncpu, memsz, version, validtime проверяется соответствие характеристик системы области допустимых значений ограничений поля LIMITS устанавливаемой лицензии (при этом значение version системы в формате, отличном от принятого в области допустимых значений ограничения version поля LIMITS устанавливаемой лицензии, считается неудовлетворительным); для ограничения variant вариант системы проверяется на равенство заданному в устанавливаемой лицензии ограничению. В случае несоответствия характеристик системы ограничениям поля LIMITS устанавливаемой лицензии добавление лицензии из файла `<license-file>` невозможно.

В системе возможно наличие нескольких лицензий. Для выбора одной применяемой лицензии осуществляется следующий алгоритм:

1) Проверяется лицензия типа user. Если система удовлетворяет огранмчениям user-лицензии, применяется данная лицензия, иначе – п.2.

2) Проверяются лицензии типа installed. Применяется первая лицензия, ограничениям которой удовлетворяет система. Если применимых лицензий типа installed нет – п.3.

3) Проверяется лицензия типа build-in. Данная лицензия всегда применима.

Для удаления лицензии, установленной пользователем из системы, применяется команда:

```
> system software license remove
```

29.6 Контроль целостности

Для осуществления контроля целостности основных компонентов системы, которые находятся на системном диске, применяется команда:

```
> show system software integrity
```

Данная команда демонстрирует соответствие посчитанного хэш ядра, корневой файловой системы и загрузчика эталонным значениям. При успешной проверке выводится сообщение `Software integrity: OK`. При несоответствии посчитанных значений эталонным выводятся некорректное значение хэш компонента системы с маркером `(wrong)` и сообщение о нарушении целостности `Software integrity: ERROR`.

Пример применения команды для осуществления контроля целостности (успешный):

```
root@Fortics> show system software integrity
Software integrity: OK
```

В данном примере все хэш соответствуют эталонным значениям.

Пример применения команды для осуществления контроля целостности (неуспешный):

```
root@Fortics> show system software integrity
LOADER: 3f539a213e97c802cc229d474c6aa32a825a360b2a933a949fd925208d9ce1bb (wr
ong)
Software integrity: ERROR
```

В данном примере файл загрузчика повреждён, т.е. целостность файла нарушена.

В ПАК «Фортикс» предусмотрен механизм контроля целостности по расписанию.

Для запуска проверки целостности с указанной частотой применяется команда:

```
# set system software-integrity <software-integrity-value>
```

где `<software-integrity-value>` – число минут от 1 до 1440.

При нарушении целостности в период проверки выводится сообщение уровня ALERT и осуществляется принудительный перезапуск системы.

Также данная настройка определяет период проведения динамического контроля физического датчика случайных чисел (см. подраздел «Динамический и регламентный контроль ФДСЧ»).

30 Скрипты

ПАК «Фортикс» позволяет автоматизировать действия администратора с помощью сценариев (скриптов) на языке программирования Lua.

Для интеграции скриптов в систему команд необходимо:

– (опционально) создать директории для хранения файлов-скриптов в диретории `/system/scripts/`;

– загрузить файлы-скрипты в подкаталоги;

– запустить скрипт в командной строке с помощью команды `@` режима администрирования.

Иерархия директорий в `/system/scripts` доступна как параметр команды `@`.

Для выполнения скрипта, находящегося в созданной директории, применяется команда:

```
> @ <directory> <script>
```

где

– `<directory>` – имя директории относительно директории `/system/scripts/`;

– `<script>` – имя скрипта.

Например, для выполнение скрипта `enable_all.lua` из каталога `/system/scripts/iface` применяется команда:

```
> @ iface enable_all.lua
```

Для команд-скриптов применимо автодополнение по клавише `<Tab>`.

Для создания скриптов непосредственно в командной строке необходимо:

1) Запустить текстовый редактор для файла-скрипта:

```
> edit <file-path>
```

где `<file-path>` – полное имя файла-скрипта или имя файла относительно домашней директории пользователя.

2) В текстовом редакторе непосредственно записать текст скрипта.

3) Использовать комбинацию клавиш `<C>` + `<O>` для сохранения файла и `<C>` + `<X>` для выхода из текстового редактора.

Пример создания скрипта непосредственно на ПАК «Фортикс»:

Запуск текстового редактора для файла-скрипта:

```
> edit /system/scripts/hello.lua
```

Запись скрипта в текстовом редакторе:

```
print «Hello, Fortics!»
```

Сохранение файла-скрипта: <C> + <O>.

Выход из текстового редактора: <C> + <X>.

Запуск созданного скрипта:

```
> @ hello.lua
Hello, Fortics!
```

30.1 Дескрипторы

Для использования параметров, указываемых после имени скрипта при его запуске, применяются описатели параметров (дескрипторы) или массив ARGS, в который помещаются параметры.

Пример текста скрипта без дескрипторов:

```
print(«Hello, «,ARGS[1])
```

Запуск скрипта из примера:

```
@ hello.lua world
Hello, world
```

Дескрипторы представляют собой строки заголовка скрипта, начинающиеся с --@. Данные строки воспринимаются окружением Lua как комментарии. Для описания параметров предусмотрены следующие дескрипторы:

– @help <Help> – текстовое описание скрипта, которое выводится по горячей клавише <?> перед набором имени скрипта;

– @arg <id>:<value> <Help> – обязательный параметр, где <id> – идентификатор параметра, <value> – тип параметра в формате строки, <Help> – текстовое описание параметра;

– @arg* <id>:<value> – массив обязательных параметров (1 или более), где <id> – идентификатор параметра, <value> – тип параметра в формате строки;

– @opt <id>:<value> – необязательный параметр, где <id> – идентификатор параметра, <value> – тип параметра в формате строки или списка (см. ниже);

– @opt* <id>:<value> – массив необязательных параметров, где <id> – идентификатор параметра, <value> – тип параметра в формате строки.

В окружении Lua любые задаваемые параметры являются строками независимо от значения в <value>, которое задаётся только для отображения в справке.

В качестве <value> допустимо указание списка из возможных вариантов строк, например:

```
--@arg op:set|del Operation
```

В данном примере параметр op принимает только значения set или del.

Для описания специфики выполнения скрипта предусмотрены следующие дескрипторы:

– @timeout – максимальный интервал выполнения скрипта, запущенного не интерактивно (в фоновом режиме), по истечении которого выполнение скрипта останавливается, где <sec> – число секунд, по умолчанию – 30;

– @noerror – отключение режима остановки выполнения скрипта по ошибке (по умолчанию скрипт останавливается при любой ошибке).

Пример текста скрипта с дескрипторами:

```
--@help Example
--@arg msg:string Message string
print(«Hello,»,ARGS.msg)
```

При запуске указанного скрипта отображаются подсказки по горячей клавише <?> и осуществляется проверка на корректность всех значений параметров.

30.2 Функции

Скрипты выполняются в ограниченном окружении Lua, в котором доступны следующие стандартные функции:

– dofile;

– ipairs;

– pairs.

– print;

– tonumber;

– tostring;

– type.

В ПАК «Фортикс» предусмотрены специфичные для данной среды исполнения функции.

30.2.1 Функции set_config() и del_config()

Функции `set_config()` и `del_config()` позволяют устанавливать и удалять узлы в конфигурации candidate. Предусмотрено два способа работы с функциями:

– непосредственное указание пути к узлу конфигурации в формате командной строки для операций;

– использование специального объекта (применим при генерации пути к узлу конфигурации в формате командной строки для операций).

Пример применения функции `set_config()` с непосредственным указанием пути к узлу конфигурации в формате командной стркои для операций:

```
set_config [[interface ether en0 description «en0»
interface ether en0 description «en1»
interface ether en0 description «en2»
interface ether en0 description «en3»]]
```

Пример использования специального объекта:

```
cfg = set_config()
for i = 0, 3 do
  cfg:printf('interface ether en%d description «en%d»\n', i, i)
end
cfg:apply()
```

Важно! Функции `set_config()` и `del_config()` оптимизированы для выполнения групп операций. Данные функции работают значительно быстрее, чем последовательные вызовы для выполнения каждой операции по отдельности. Например, выполнение следующих последовательных операций:

```
set_config 'interface ether en0 description «en0»'
set_config 'interface ether en0 description «en1»'
set_config 'interface ether en0 description «en2»'
set_config 'interface ether en0 description «en3»'
```

значительно медленнее, чем выполнение следующей группы операций:

```
set_config [[interface ether en0 description «en0»
interface ether en0 description «en1»
interface ether en0 description «en2»
interface ether en0 description «en3»]]
```

Важно! Данные функции изменяют конфигурацию candidate. Для применения указанных изменений к конфигурации running необходимо выполнить команду `commit`.

30.2.2 Функция load_config()

Функция `load_config()` позволяет дополнять конфигурацию candidate фрагментами конфигурации. Данная функция изменяет конфигурацию candidate.

Пример применения функции `load_config()`:

```
load_config [[interface {
  ether en0 {
    description «en0»
    enable
  }
}]]
```

В указанном примере добавляются/изменяются параметры `enable` и `description`, при этом другие параметры конфигурации остаются неизменными.

Для замены конфигурации интерфейса целиком перед применением рассматриваемой функции выполняется функция `del_config()`:

```
del_config «interface ether en0»
load_config [[interface {
  ether en0 {
    description «en0»
    enable
  }
}]]
```

30.2.3 Функция commit()

Функция `commit()` осуществляет фиксацию конфигурации с помощью команды `commit`.

Применение функции `commit()`:

```
commit()
```

Пример применения функции `commit()`:

```
set_config 'interface ether en0 description «en0»'
commit()
```

Применение функции `commit()` для указанного узла конфигурации:

```
commit 'path'
```

где `path` – путь к узлу конфигурации в формате командной строки.

Пример применения функции commit() для указанного узла конфигурации:

```
set_config 'interface ether en0 description «en0»'
commit 'interface ether en0'
```

30.2.4 Функция revert()

Функция revert() отменяет изменения в конфигурации candidate.

Применение функции:

```
revert()
```

Для применения revert() для указанного узла конфигурации используется конструкция:

```
revert 'path'
```

где path – путь к узлу конфигурации в формате командной строки.

30.2.5 Функция exit()

Функция exit() соответствует стандартной функции Lua os.exit().

Применение функции:

```
exit(true)
```

30.2.6 Функция command()

Функция command() позволяет выполнять последовательность команд режима администрирования.

Применение функции command():

```
command('<command-adm>')
```

где <command-adm> – команда режима администрирования.

Пример применения функции command():

```
command('show version')
```

По умолчанию вывод команды на экран подавляется и возвращается в виде двух таблиц stdout и stderr, например:

```
out = command 'show version'
print(out[2]) -- Показать версию (вторая строка вывода)
```

Для стандартного выполнения команды и получения её вывода в качестве второго параметра задается `true`.

Применение функции с указанием второго параметра `true`:

```
command('<command>', true)
```

где `<command>` – команда режима администрирования.

Пример применения функции с указанием второго параметра `true`:

```
command('show version', true)
```

Данная функция не возвращает таблицы с `stdout` и `stderr`.

Пример выполнения последовательности команд:

```
command([[show version
show system software]], true)
```

30.2.7 Функция file()

Функция `file()` позволяет получать содержимое файлов или создавать текстовые файлы.

Пример применения функции `file()`:

```
file(«hello.txt», «Hello, World!»)
command(«cat hello.txt», true)
txt = file 'hello.txt'
txt = txt:gsub('World', 'Fortics')
file(«hello2.txt», txt)
command(«cat hello2.txt», true)
```

30.2.8 Функция sleep()

Функция `sleep()` позволяет скрипту переходить в режим сна на указанное время.

Пример применения функции `sleep()`:

```
sleep(1)
```

30.2.9 Функция getenv()

Функция `getenv()` соответствует стандартной функции Lua `os.getenv` и позволяет получать переменные окружения. Некоторые службы ПАК «Фортикс», которые могут быть

интегрированы со скриптами, передают информацию о событиях с помощью переменных окружения.

30.2.10 Функция stop_on_error()

По умолчанию любая ошибка останавливает выполнение скрипта. Для изменения режима обработки ошибок предусмотрено:

– применение дескриптора `@noerror` – выключает режим остановки выполнения скрипта по ошибке полностью;

– применение функции `stop_on_error(true|false)` – включает (`true`) или выключает (`false`) режим остановки по ошибке.

Функция `stop_on_error()` возвращает предыдущее значение режима.

Применение функции `stop_on_error()`:

```
stop_on_error(true|false)
```

Пример применения функции `stop_on_error()`:

```
old_mode = stop_on_error(false)
print(io.file(«hello.txt»))
stop_on_error(true)
```

Функции `noerror()` и `check_error()` меняют поведение обработки ошибок для указанных вызовов функций.

30.2.11 Функция noerror()

Функция `noerror()` позволяет отключать режим остановки выполнения скрипта по ошибке для указанной функции.

Пример применения функции `noerror()`:

```
-- проверить, существует ли файл
if noerror(file)(«test») then
  print «test is exist»
else
  print «test is not exist»
end
```

30.2.12 Функция check_error()

Функция check_error() позволяет включать режим остановки выполнения скрипта по ошибке для указанной функции.

Пример применения функции check_error():

```
--@noerror
del_config «interface ether en1 enable»
check_error(commit)()
print «Commit done!»
```

30.2.13 Функции time() и date()

Функции time() и date() соответствуют стандартным функциям Lua os.time() и os.date().

30.2.14 Функция send_smtp

Функция send_smtp позволяет отправлять e-mail сообщения на некоторый сервер.

Применение функции send_smtp:

```
send_smtp(<opt>, <message>)
```

где

– <opt> – lua-таблица, ключами которой являются опции, а значениями – значения опций;

– <message> – строка сообщения, которая может содержать получателей и отправителя (см. пример ниже).

Доступны следующие опции для таблицы <opt>:

– recipients – получатели, значение опции – адреса, указанные через «;», в кавычках;

– password – пароль для аутентификации на почтом сервере отправителя, значение опции – строка в кавычках;

– user – имя пользователя для аутентификации на почтовом сервере, значение опции – строка в кавычках;

– host – адрес почтового сервера, значение опции – строка в кавычках;

– from – отправитель письма, значение опции – строка в кавычках;

– `tls` – включение/отключение TLS для связи с почтовым сервером (все необходимые для проверки сертификаты сервера должны находиться в каталоге `/system/ssl/certs`, если проверка сертификата не отключена), значение опции – «on»/»off»;

– `auth` – включение/отключение аутентификации при связи с сервером, значение опции – «on»/»off», при значении «on» данной опции значения опций `user` и `password` должны быть определены;

– `tls-certcheck` – включение/отключение проверки сертификата почтового сервера при включенном tls, значение опции – «on»/»off».

Если опции `recipients` и/или `from` не указаны, их значения извлекаются из строки сообщения.

Пример определения значений опций `recipients` и `from` в строке сообщения:

```
local message = «From: best_programmer@zts.ru\n To: test@zts.ru\n Hello!\n»
```

Пример применения функции `send_smtp`:

```
local opts = {
  password = «Aqwl;vxcjk123»,
  user = «test@inbox.ru»,
  tls = «off»,
  host = «smtp.mail.ru»,
  auth = «on»,
}
local message = «From:test@inbox.ru\n Hello world!\n»

local ret, err = send_smtp(opts, message)
```

Допустимо указание значения nil строки сообщения. В этом случае отправляется пустое сообщение, при этом определение значений опций `from` и `recipients` обязательно.

30.2.15 Функция send_snmp

Функция `send_snmp` позволяет отправлять SNMP-сообщения trap/inform на удалённый сервер с помощью протокола SNMP второй и третьей версии.

Применение функции `send_snmp`:

```
send_snmp(<opt>, <message>)
```

где

– `<opt>` – lua-таблица, ключами которой являются опции, а значениями – значения опций;

– <message> – набор таблиц.

Доступны следующие опции для таблицы <opt>:

– snmtype – тип посылаемого сообщения, значение опции – «trap» или «inform», по умолчанию – «trap»;

– version – версия сообщения, значение опции – «2» или «3», по умолчанию – «2»;

– addr – адрес приёмника, значение опции – адрес хоста, для указания порта добавляется :<port>, где <port> – число от 1 до 65535;

– uptime – (опционально) время работы системы (по умолчанию указывается время работы после загрузки системы), значение опции – число секунд в кавычках;

– user – (только для v3) имя пользователя для аутентификации на сервере, значение опции – строка в кавычках;

– sec_engine_id – (только для v3) engineID, используемое при включённой аутентификации на принимающей стороне, значение опции – hex-значение в кавычках;

– auth_alg – (только для v3) алгоритм аутентификации, значение опции – «MD5»/»SHA»;

– auth_key – (только для v3) ключ аутентификации, значение опции – строка в кавычках;

– privacy_alg – (только для v3) алгоритм шифрования, значение опции – «DES»/»AES»;

– privacy_key – (только для v3) закрытый ключ, используемый для шифрования, значение опции – строка в кавычках;

– context_engine_id – (только для v3) engineID для контекста, значение опции – hex-значение в кавычках;

– community – (только для v2) идентификатор отправителя, значение опции – строка в кавычках.

Сообщение – это набор таблиц, где в начале указывается oid события и далее дополнительный oid. Каждая таблица в начале содержит базовый oid/mib, далее опциональное значение, которое является строкой или числом. Данное значение отправляется с типом ASN1_INTEGER или ASN1_STRING в зависимости от переданного значения.

Пример сообщения:

```
{1.2.3.4, «2»}
{1.2.3.4 , 2}
```

В первом случае сообщение отправится как ASN1_STRING, во втором – как ASN1_INTEGER.

Примеры:

```
local conf1 = {
  snmptype = «trap»,
  version = «3»,
  addr = «192.168.56.1:12345»,
  sec_engine_id = «0x8000123acd1ab43abbfff000fa»,
  user = «test»,
  auth_alg = «MD5»,
  auth_key = «testsnmp»,
  privacy_alg = «DES»,
  privacy_key = «testSNMP»,
}
send_snmp(conf1, {«SNMPv2-MIB::coldStart»}, {«iso.3.6.1.6.3.1.1.6.2», 2},
{«SNMPv2-MIB::sysName.0», «My Device»}) --Send snmpv3 trap with auth and pri
vacy. uptime from system

local conf2 = {
 version = «3»,
 addr = «192.168.56.1:12345»,
 user = «test2»,
}
send_snmp(conf2, {«SNMPv2-MIB::coldStart»}, {«iso.3.6.1.6.3.1.1.6.2», 2},
{«SNMPv2-MIB::sysName.0», «My Device»}) -- --Send snmpv3 trap without auth a
nd privacy, uptime from system

local conf3 = {
  addr = «192.168.56.1:12345»,
  community = «public»,
}
send_snmp(conf2, {«SNMPv2-MIB::coldStart»}, {«iso.3.6.1.6.3.1.1.6.2», 2},
{«SNMPv2-MIB::sysName.0», «My Device»}) -- --Send snmpv2 trap
```

30.2.16 Функция journal

Функция `journal` позволяет отправлять сообщения в системный журнал.

Предусмотрены следующие уровни отправляемых в журнал сообщений:

– `alert` – оповещение, требующее немедленной реакции администратора;

– `err` – ошибка;

– `warning` – предупреждение;

– `info` – информационное сообщение.

Пример применения функции `journal`:

```
journal(«alert», «No free space available!»)
```

Пример использования форматной строки в функции journal:

```
journal(«info», «%d days left», days)
```

30.2.17 Функции get, get_data, get_xpath

Функции get, get_data и get_xpath позволяют выполнять выборку из конфигурации running , возвращая lua-таблицу с данными. Функции get и get_data получают в качестве параметра путь к узлу конфигурации в формате командной строки. Функция get_xpath получает в качестве параметра путь в виде yang xpath-запроса.

Функция get возвращает узел. Функции get_data и get_xpath возвращают поддерево от корня конфигурации до узла. Функция get не может быть использована в тех случаях, когда под выборку попадает несколько элементов.

Для анализа структур применяется функция table.dump().

Пример применения функций get, get_data, get_xpath, table.dump():

```
local addr = get_data «interface ether en0 ipv4 address»
if not addr then
  exit()
end

printf(«data: %s\n\n», table.dump(addr, true))
for _, v in ipairs(addr[1][1][2]) do
  print(v[1].val)
end
print(addr:dump())

local enable = get «interface ether en0 enable»
printf(«data: %s\n\n», table.dump(enable, true))
printf(«enabled: %s\n», enable and enable[1] and true)
```

30.3 Библиотеки

В ПАК «Фортикс» поддерживаются следующие стандартные библиотеки Lua:

– table;

– string;

– math.

В ПАК «Фортикс» поддерживаются следующие нестандартные библиотеки:

– ipnet;

– rex.

30.4 Расширение стандартных библиотек

В ПАК «Фортикс» для удобства решения типовых задач стандартные библиотеки Lua расширены дополнительными функциями.

30.4.1 Расширение библиотеки string

– string.empty(<string>) – проверить, что строка состоит из пробелов и табуляций, где <string> – строка;

– string.strip(<string>,[набор символов]) – убрать разделители в конце строки, где <string> – строка;

– string.split(<string>, [макс. разбиений], [separator]) – разбить строку на массив строк, где <string> – строка, [separator] – разделитель;

– string.startswith(<string>, <prefix>) – проверить, что строка начинается с указанного префикса, где <string> – строка, <prefix> – префикс строки;

– string.endswith(<string>, <postfix>) – проверить, что строка заканчивается на указанный постфикс, где <string> – строка, <postfix> – постфикс строки;

– string.lines(<text>) – построчный итератор.

30.4.2 Расширение библиотеки table

– table.append(<dst>, <src>) – добавить элементы таблицы <src> в таблицу <dst>, где <dst> – lua-таблица, <src> – lua-таблица;

– table.clone(<src>) – клонировать таблицу, где <src> – lua-таблица;

– table.merge(<dst>, <src>) – внести в таблицу элементы таблицы без изменений, где <dst> – lua-таблица, <src> – lua-таблица;

– table.empty(<src>) – проверить, что таблица пуста, где <src> – lua-таблица;

– table.unpack(<src>) – распаковать таблицу в список значений, где <src> – lua-таблица;

– table.iter(<src>) – аналогична стандартной функции ipairs, при этом индекс не возвращается, где <src> – lua-таблица.

30.5 Пример скрипта

Пример скрипта, выполняющего команды для группы параметров:

```
--@help For iterator
--@arg start:int Start value
--@arg stop:int End value
--@arg op:set|del Command
--@arg* arg:path Path

local start = tonumber(ARGS.start)
local stop = tonumber(ARGS.stop)
local cmd = ''
for _, v in ipairs(ARGS.arg) do
  cmd = cmd .. string.quote(v) .. ' '
end
local cfg = ARGS.op == 'del' and del_config() or set_config()
for i=start, stop do
  cfg:printf(cmd..'\n', i)
end
cfg:apply()
```

Применение скрипта из примера:

```
@ for 0 10 set interface ether en%d enable
```

31 Средства криптографической защиты информации (СКЗИ)

31.1 Ключ доступа (КД)

Для работы со средствами криптографической защиты информации в ПАК «Фортикс» необходимо создать/загрузить ключ доступа (далее по тексту – КД).

В состав ПАК «Фортикс» входит устройство «Фортикс-Стена» с физическим датчиком случайных чисел (далее по тексту – ФДСЧ), с помощью которого генерируются ключи доступа.

КД используется системой для защиты следующих секретов, хранящихся в постоянной памяти ПАК «Фортикс»:

– симметричные ключи forsec-key (защита аутентифицированным шифрованием);

– асимметричные ключи forsec-keypair (защита аутентифицированным шифрованием);

– журнал событий СКЗИ (защита имитовставкой).

После генерации КД сохраняется на внешнем носителе или в постоянной памяти устройства «Фортикс-Стена». В случае сохранения на внешнем носителе ключ доступа понадобится при «холодном» перезапуске системы. В случае «тёплого» перезапуска системы носитель не потребуется, так как КД сохраняется в оперативной памяти устройства «Фортикс-Стена» (автоматически ключ доступа загрузится при условии наличия настройки `crypto access-key location hw-ram`, см. пункт «Загрузка КД»).

В рамках процедуры первоначального ввода системы СКЗИ в эксплуатацию необходимо:

1) инициализировать КД;

2) сохранить КД в постоянную память устройства «Фортикс-Стена» или на внешнем носителе;

3) загрузить КД с устройства «Фортикс-Стена» или внешнего носителя;

4) настроить автоматическую загрузку КД при перезагрузке ПАК «Фортикс».

31.1.1 Правила работы с КД

1) К каждому устройству ПАК «Фортикс» относится только один ключ доступа, который используется только на данном устройстве.

2) На носителе ключа доступа присутствует только один КД.

3) Ключ доступа сохраняется только один раз и только на одном носителе.

4) Утеря или компрометация КД автоматически означает компрометацию всех данных, защищённых данным КД. В случае указанного инцидента все ключи forsec-keypair/forsec-key объявляются недействительными.

5) В случае технической неисправности носителя КД все данные на нём полностью очищаются без возможности восстановления или носитель уничтожается.

31.1.2 Инициализация нового КД

Для инициализации нового КД с помощью ФДСЧ устройства «Фортикс-Стена» применяется команда:

```
> crypto access-key init
```

31.1.3 Сохранение КД

После генерации ключ доступа необходимо сохранить в постоянной памяти устройства «Фортикс-Стена» или на внешнем носителе.

Для сохранения ключа доступа в постоянной памяти устройства «Фортикс-Стена» применяется команда:

```
> crypto access-key store hw-rom
```

Для сохранения ключа доступа на внешнем носителе применяется команда:

```
> crypto access-key store <path-to-dir>
```

где `<path-to-dir>` – полное имя директории на внешнем носителе, в которую сохраняется КД, относительно директории `/media`.

Пример применения команды для сохранения ключа доступа на внешнем носителе:

```
> crypto access-key store /media/flash0/dir/
```

При сохранении КД запрашивается ввод пароля, используемый в последствии для защиты КД.

Для сохранения КД без парольной защиты вместо ввода пароля при запросе необходимо нажать клавишу `<Enter>` без ввода пароля (поскольку при сохранении КД пароль запрашивается дважды для подтверждения, для сохранения КД без парольной защиты необходимо нажать клавишу `<Enter>` без ввода пароля дважды).

П р и м е ч а н и е – Рекомендуется использование парольной защиты КД.

Если на внешнем носителе уже существует КД, запрашивается подтверждение о перезаписи старого контейнера КД новым.

После успешного сохранения КД удаляется из оперативной памяти ПАК «Фортикс».

31.1.4 Загрузка КД

КД может быть загружен одним из следующих способов:

– вручную с помощью команды режима администрирования;

– автоматически при загрузке системы.

31.1.4.1 Ручная загрузка КД

Для загрузки КД вручную с указанного носителя применяется команда:

```
> crypto access-key load hw-rom|hw-ram|<path-to-dir>
```

где

– `hw-rom` – постоянная память устройства «Фортикс-Стена»;

– `hw-ram` – оперативная память устройства «Фортикс-Стена»;

– `<path-to-dir>` – полное имя директории на внешнем носителе относительно директории `/media`.

При выполнении данной команды у пользователя запрашивается пароль, которым защищён КД (если он установлен).

При успешном выполнении команды КД загружается в ядро ПАК «Фортикс» и сохраняется в оперативную память устройства «Фортикс-Стена» (`hw-ram`) без пароля для того, чтобы при «тёплом» перезапуске существовала возможность загрузки КД без ввода пароля.

31.1.4.2 Автоматическая загрузка КД

Настройка автоматической загрузки КД осуществляется на следующем уровне конфигурации:

```
[edit crypto access-key]
```

На данном уровне конфигурации доступны следующие настройки:

– `location hw-rom|hw-ram|<path-to-dir>` – указать носитель, с которого загружается КД, где `hw-rom` – постоянная память устройства «Фортикс-Стена», `hw-ram` – оперативная память устройства «Фортикс-Стена», `<path-to-dir>` – полное имя директории на внешнем носителе относительно директории `/media`;

– `device-timeout <device-timeout-value>` – указать таймаут ожидания внешних носителей, где `<device-timeout-value>` – число секунд, по умолчанию – 10.

Возможно определение нескольких носителей, с которых загружается КД. При этом порядок определения в конфигурации настроек для указания носителей определяет порядок загрузки КД.

Так как внешние носители доступны не сразу при загрузке системы, в ПАК «Фортикс» предусмотрена настройка `device-timeout`.

Пример применения команд для настройки автоматической загрузки КД:

```
# edit crypto access-key
# set location hw-ram
# set location /media/flash0
# set device-timeout 10
# diff
+crypto {
+  access-key {
+    location hw-ram
+    location /media/flash0
+    device-timeout 10
+  }
+}
# commit
```

П р и м е ч а н и е – Применение данных настроек не инициирует загрузку КД из указанного в настройке `location` носителя. Для загрузки КД необходимо перезагрузить систему или выполнить команду режима администрирования `crypto access-key load`.

31.1.5 Состояние КД

Для просмотра текущего состояния КД применяется команда:

```
> show crypto access-key status
```

Возможные варианты вывода команды:

1) Если КД не загружен или не создан, выводится:

```
Info: No access key
```

2) Если КД сгенерирован, но не сохранён на носителе, выводится:

```
Info: Access key not stored
```

В этом случае необходимо выполнить команду `crypto access-key store`, а затем выполнить процедуру загрузки КД.

3) Если КД успешно загружен в оперативную память ПАК «Фортикс», выводится:

```
Info: Access key XXXXXXXX is loaded
```

где `XXXXXXXX` – отпечаток (идентификатор) КД в 16-ричном виде.

31.1.6 Экспорт КД

При использовании кластерного решения из двух и более ПАК «Фортикс» требуется наличие одинаковых КД на каждой ноде (устройстве) кластера.

Для экспорта КД с основного ПАК «Фортикс» на внешний носитель применяется команда:

```
> crypto access-key export <path-to-dir>
```

где `<path-to-dir>` – полное имя директории на внешнем носителе относительно директории `/media`.

31.1.7 Импорт КД

При использовании кластерного решения из двух и более ПАК «Фортикс» требуется наличие одинаковых КД на каждой ноде (устройстве) кластера.

В резервные ПАК «Фортикс» необходимо выполнить импорт КД, ранее экспортированного из основного ПАК.

Для импорта КД с указанного внешнего носителя применяется команда:

```
> crypto access-key replace save-to hw-rom load-from <path-to-dir>
```

где `<path-to-dir>` – полное имя директории на внешнем носителе относительно директории `/media`.

При успешном импорте после выполнения команды КД сохраняется в постоянную память устройства «Фортикс-Стена» и все секреты системы зашифровываются на новом КД.

П р и м е ч а н и е – Для успешного выполнения команды на резервном ПАК «Фортикс» в оперативной памяти ПАК «Фортикс» должен присутствовать старый (временный) КД.

Пример применения команды для импорта КД:

```
> crypto access-key replace save-to hw-rom load-from /media/flash0/dir/
```

31.1.8 Плановая замена КД

Для плановой замены КД и сохранения его на указанный носитель применяется команда:

```
> crypto access-key replace save-to hw-rom|<path-to-dir> gen-new
```

где

– `hw-rom` – постоянная память устройства «Фортикс-Стена»;

– `<path-to-dir>` – полное имя директории на внешнем носителе относительно директории `/media`.

Параметр `gen-new` указывает на генерацию нового КД с использованием ФДСЧ устройства «Фортикс-Стена».

При успешном выполнении команды все секреты системы зашифровываются на новом КД.

П р и м е ч а н и е – Для успешного выполнения команды в оперативной памяти ПАК «Фортикс» должен присутствовать старый КД.

Пример применения команды для плановой замены КД:

```
> crypto access-key replace save-to hw-rom gen-new
```

31.1.9 Удаление КД

Для удаления КД из оперативной памяти ПАК «Фортикс» применяется команда:

```
> crypto access-key clear memory
```

Для удаления КД из постоянной памяти устройства «Фортикс-Стена» применяется команда:

```
> crypto access-key clear hw-rom
```

Для удаления КД из оперативной памяти устройства «Фортикс-Стена» применяется команда:

```
> crypto access-key clear hw-ram
```

Для удаления КД с внешнего носителя применяется команда:

```
> crypto access-key clear <path-to-dir>
```

где <path-to-dir> – полное имя директории на внешнем носителе относительно директории /media.

31.2 Ключи forsec-key

Ключи forsec-key представляют собой строки симметричных ключей парно-выборочной связи определённой серии и абонента.

Для работы с ключами forsec-key необходим загруженный КД.

31.2.1 Импорт forsec-key

Для импорта ключей forsec-key с внешнего носителя применяется команда:

```
> crypto forsec-key import <path-to-dir>
```

где <path-to-dir> – полное имя директории на внешнем носителе относительно директории /media.

31.2.2 Просмотр информации о ключах forsec-key

Для просмотра информации о всех ключах forsec-key в системе применяется команда:

```
> show crypto forsec-key
```

Для каждой строки ключей выводится его серия, номер локального абонента, количество абонентов в серии, дата генерации матрицы ключей и дата импорта строки ключей.

Пример применения команды для получения информации о всех ключах forsec-key в системе и её вывода:

```
> show crypto forsec-key
Serial: 128, CN: 100, Serial size: 113, Gen date: 2024-02-16, Import date: 2
024-05-16
Serial: 128, CN: 7, Serial size: 113, Gen date: 2024-02-16, Import date: 202
4-05-16
Serial: 127, CN: 99, Serial size: 160, Gen date: 2024-05-13, Import date: 20
24-05-16
```

Для получения информации о ключах указанной серии применяется команда:

```
> show crypto forsec-key <serial-number>
```

где <serial-number> – номер серии.

Пример применения команды для получения информации о ключах указанной серии и её вывода:

```
> show crypto forsec-key 128
Serial: 128, CN: 100, Serial size: 113, Gen date: 2024-02-16, Import date: 2
024-05-16
Serial: 128, CN: 7, Serial size: 113, Gen date: 2024-02-16, Import date: 202
4-05-16
```

Для получения информации об указанной строке ключей применяется команда:

```
> show crypto forsec-key <serial-number> <local-peer-number>
```

где

– <serial-number> – номер серии;

– <local-peer-number> – номер локального абонента.

Пример применения команды для получения информации об указанной строке ключей и её вывода:

```
> show crypto forsec-key 128 100
Serial: 128, CN: 100, Serial size: 113, Gen date: 2024-02-16, Import date: 2
024-05-16
```

Для проверки доступности удалённого абонента для указанного ключа применяется команда:

```
> show crypto forsec-key <serial-number> <local-peer-number> <remote-peer-nu
mber>
```

где

– <serial-number> – номер серии;

– <local-peer-number> – номер локального абонента;

– <remote-peer-number> – номер удалённого абонента.

Пример применения команды для проверки доступности удалённого абонента для указанного ключа и её вывода:

```
> show crypto forsec-key 128 100 1
Access to peer 1 for key(serial= 128;CN = 100), status:GRANTED
> show crypto forsec-key 128 100 2
Access to peer 2 for key(serial= 128;CN = 100), status:DENIED
```

31.2.3 Удаление ключей forsec-key и блокировка абонента

Для удаления указанного ключа forsec-key применяется команда:

```
> crypto forsec-key remove <serial-number> <local-peer-number>
```

где

– <serial-number> – номер серии;

– <local-peer-number> – номер локального абонента.

Для блокировки удалённого абонента указанного ключа forsec-key применяется команда:

```
> crypto forsec-key remove <serial-number> <local-peer-number> <remote-peer-number>
```

где

– <serial-number> – номер серии;

– <local-peer-number> – номер локального абонента;

– <remote-peer-number> – номер удалённого абонента.

Пример применения команды для блокировки удалённого абонента указанного ключа forsec-key и её вывода:

```
> show crypto forsec-key 128 100 18
Access to peer 18 for key(serial= 128;CN = 100), status:GRANTED
> crypto forsec-key remove 128 100 18
Forsec-key peer key was successfully zeroized:128 100 {18}.
> show crypto forsec-key 128 100 18
Access to peer 18 for key(serial= 128;CN = 100), status:DENIED
```

Для удаления всех ключей forsec-key применяется команда:

```
> crypto forsec-key cleanup
```

Данная команда не может быть выполнена, если ключи forsec-key используются в туннеле fortun.

31.3 Ключи forsec-keypair

Ключи forsec-keypair представляют собой ключевые пары асимметричных ключей (открытый и закрытый ключи) или только открытые ключи (закрытый ключ при этом неизвестен).

Важно! Обмен открытыми ключами forsec-keypair между абонентами осуществляется по каналу, исключающему подмену ключей.

Для работы с ключами forsec-keypair необходим загруженный КД.

31.3.1 Генерация ключей forsec-keypair

Для генерации ключевой пары forsec-keypair с указанным именем применяется команда:

```
> crypto forsec-keypair generate <forsec-keypair-name>
```

где `<forsec-keypair-name>` – строка.

При генерации ключа forsec-keypair (открытого и закрытого ключей) фиксируется дата/время генерации ключа.

31.3.2 Экспорт и импорт ключей forsec-keypair

Для экспорта открытого ключа forsec-keypair (в бинарном виде) применяется команда:

```
> crypto forsec-keypair export <forsec-keypair-name> <path-to-file>
```

где

– `<forsec-keypair-name>` – имя существующего ключа forsec-keypair;

– `<path-to-file>` – полное имя файла или имя файла относительно домашней директории пользователя.

В файле `<path-to-file>` сохраняется открытый ключ forsec-keypair, его время жизни и имя.

Экспорт значения открытого ключа forsec-keypair в текстовом шестнадцатеричном виде описан ниже (см. пункт «Просмотр информации о ключах forsec-keypair»).

Для импорта открытого ключа forsec-keypair из указанного файла применяется команда:

```
> crypto forsec-keypair import <path-to-file>
```

где `<path-to-file>` – полное имя файла или имя файла относительно домашней директории пользователя.

В команде указывается путь к бинарному контейнеру с открытым ключом forsec-keypair, полученному с помощью команды `crypto forsec-keypair export`.

Для импорта открытого ключа forsec-keypair с указанным именем с помощью текстового значения применяется команда:

```
> crypto forsec-keypair add <forsec-keypair-name> hex
<forsec-keypair-text>
```

где

– <forsec-keypair-name> – строка;

– <forsec-keypair-text> – текст в 16-ричном виде.

Для импорта открытого ключа forsec-keypair с указанным именем из файла с текстовым 16-ричным значением применяется команда:

```
> crypto forsec-keypair add <forsec-keypair-name> file <path-to-file>
```

где

– <forsec-keypair-name> – строка;

– <path-to-file> – полное имя файла или имя файла относительно домашней директории пользователя.

Примеры применения команд для импорта открытого ключа forsec-keypair:

```
> crypto forsec-keypair add new_key hex D20C447D48964C4B43E97498D034B9D936DC
15C00713CA03B49C8333B6A2BB4A343D715E775A63CB02C05C9972C1E04C594EADF80023BFEA
146051603CA682C812B95CD05B557861A74016B867CE2E633E437F43E0631927064D5C95830C
A39185B413FE16B1D631AE9439FA02AAD415F3E88199EF73BF49B81FD3444ABA3C36
> crypto forsec-keypair add new_key2 file /home/user/hex_key
```

31.3.3 Просмотр информации о ключах forsec-keypair

Для получения информации о всех ключах forsec-keypair, присутствующих в ПАК «Фортикс», применяется команда:

```
> show crypto forsec-keypair
```

Пример вывода команды для получения информации о всех ключах forsec-keypair, присутствующих в ПАК «Фортикс»:

```
  Keyname                  HEX          Date           Usage
+ test                     3069CEFB     2024-02-14     fort1
+ test3                    D20C447D     2024-02-14
- test2                    A9B6118E     undefined      fort1
```

Каждая строка содержит информацию об открытом ключе или о ключевой паре.

В столбце «Keyname» указаны имена ключей forsec-keypair.

Знак «+» означает, что в системе указанному ключу forsec-keypair соответствует закрытый и открытый ключи.

Знак «-» означает, что в системе указанному ключу forsec-keypair соответствует только открытый ключ.

В столбце «HEX» указаны первые 4 байта открытого ключа forsec-keypair в 16-ричном виде.

В столбце «Date» указана дата генерации ключа forsec-keypair (значение «undefined» указано для ключей, импортированных с помощью команды `crypto forsec-keypair add`, см. ниже).

В столбце «Usage» указано имя интерфейса fortun, в котором задействован указанный ключ forsec-keypair.

Для получения информации об указанном ключе forsec-keypair применяется команда:

```
> show crypto forsec-keypair <forsec-keypair-name>
```

где `<forsec-keypair-name>` – имя существующего ключа forsec-keypair.

По данной команде отображается значение открытого ключа forsec-keypair в 16-ричном виде и дата генерации ключа forsec-keypair, значение закрытого ключа forsec-keypair не отображается.

Пример применения команды для получения информации об указанном ключе forsec-keypair и её вывода:

```
> show crypto forsec-keypair test3

KEY:
D20C447D48964C4B43E97498D034B9D936DC15C00713CA03B49C8333B6A2BB4A343D715E775A
63CB02C05C9972C1E04C594EADF80023BFEA146051603CA682C812B95CD05B557861A74016B8
67CE2E633E437F43E0631927064D5C95830CA39185B413FE16B1D631AE9439FA02AAD415F3E8
8199EF73BF49B81FD3444ABA3C36
Gen time:
2024-02-14
```

Для записи шестнадцатеричного значения открытого ключа forsec-keypair в указанный файл применяется команда:

```
> show crypto forsec-keypair <forsec-keypair-name> <path-to-file>
```

где

– `<forsec-keypair-name>` – имя существующего ключа forsec-keypair;

– <path-to-file> – полное имя файла или имя файла относительно домашней директории пользователя.

Пример применения команды для записи шестнадцатеричного значения открытого ключа forsec-keypair в указанный файл:

```
> show crypto forsec-keypair test3 test3
> cat test3
D20C447D48964C4B43E97498D034B9D936DC15C00713CA03B49C8333B6A2BB4A343D715E775A
63CB02C05C9972C1E04C594EADF80023BFEA146051603CA682C812B95CD05B557861A74016B8
67CE2E633E437F43E0631927064D5C95830CA39185B413FE16B1D631AE9439FA02AAD415F3E8
8199EF73BF49B81FD3444ABA3C36
```

31.3.4 Удаление ключей forsec-keypair

Для удаления указанного ключа forsec-keypair применяется команда:

```
> crypto forsec-keypair remove key <forsec-keypair-name>
```

где <forsec-keypair-name> – имя существующего ключа forsec-keypair.

Примечание – Удаление ключей, используемых в туннеле fortun, невозможно (см. пункт «Использование ключей в туннелях fortun»).

Для удаления всех неиспользуемых ключей forsec-keypair применяется команда:

```
> crypto forsec-keypair remove unused
```

Для удаления всех ключей forsec-keypair, в том числе используемых в туннелях, применяется команда:

```
> crypto forsec-keypair cleanup
```

Примечание – Применение данной команды необходимо осуществлять с осторожностью (см. пункт «Использование ключей в туннелях fortun»).

31.3.5 Электронная подпись с использованием ключей forsec-keypair

Формирование и проверка электронной подписи возможны с помощью ключей forsec-keypair.

Для формирования электронной подписи в указанную директорию применяется команда:

```
> crypto forsec-keypair sign <file-name> <forsec-keypair-name> <path-to-sign
-dir>
```

где

– <file-name> – полное имя подписываемого файла или имя файла относительно домашней директории пользователя;

– <forsec-keypair-name> – имя существующего ключа forsec-keypair;

– <path-to-sign-dir> – полное имя директории или имя директории относительно домашней директории пользователя.

При формировании файл подписи записывается в указанную директорию с именем <file-name>.sig.

Пример применения команды для формирования подписи:

```
> crypto forsec-keypair sign test_file.txt test3 /home/user/2/
```

Для проверки электронной подписи применяется команда:

```
> crypto forsec-keypair verify <file-name> <forsec-keypair-name> <path-to-sign-file>
```

где

– <file-name> – полное имя проверяемого файла или имя файла относительно домашней директории пользователя;

– <forsec-keypair-name> – имя существующего ключа forsec-keypair;

– <path-to-sign-file> – полное имя файла подписи или имя файла относительно домашней директории пользователя.

Пример применения команды для проверки подписи:

```
> crypto forsec-keypair verify test_file.txt test3 /home/user/2/test_file.txt.sig
```

31.4 Интерфейсы fortun

Интерфейс fortun – это туннельный интерфейс уровней L3 и L2 с поддержкой шифрования. Туннель может работать как в режиме шифрования, так и в режиме открытого трафика. Для работы в режиме шифрования требуется наличие ключа доступа в оперативной памяти ПАК «Фортикс» (см. пункт «Загрузка КД»).

Настройка интерфейса fortun осуществляется на следующем уровне конфигурации:

```
[edit interface fortun <fortun-interface-name>]
```

где <fortun-interface-name> – строка длиной от 1 до 15 символов.

На данном уровне конфигурации доступны следующие настройки, уникальные для интерфейсов fortun:

– `mode tun|tap` – указать режим интерфейса, где `tun` – режим L2, `tap` – режим L3, по умолчанию – `tun`;

– `id <id-value>` – указать идентификатор соединения, одинаковый на обеих сторонах туннеля, где `<id-value>` – число от 0 до 65535;

– `encap` – перейти на уровень конфигурации UDP-инкапсуляции;

– `keepalives` – перейти на уровень конфигурации keep-alive;

– `forsec-key` – перейти на уровень конфигурации использования ключей forsec-key для шифрования туннеля;

– `forsec-keypair` – перейти на уровень конфигурации использования ключей forsec-keypair для шифрования туннеля;

– `encryption` – включить режим шифрования туннеля;

– `ttl <ttl-value>` – указать время жизни пакета, где `<ttl-value>` – число от 0 до 255;

– `tos <tos-value>` – указать тип обслуживания, где `<tos-value>` – строка в формате `0x<hex-value>`;

– `ipv4|ipv6` – перейти на уровень конфигурации IPv4/IPv6 (кроме стандартных IP-настроек доступны настройки `local` и `remote`).

31.4.1 Минимальные настройки

Для работы туннеля достаточно определить его концы, настройки `id` и `enable`.

Пример минимальной настройки туннеля:

```
# edit interface fortun fort1
# set ipv4 local 10.10.10.1
# set ipv4 remote 10.10.10.34
# set id 128
# set enable
# diff
+interface {
+  fortun fort1 {
+    enable
+    ipv4 {
+      local 10.10.10.1
+      remote 10.10.10.34
+    }
+    id 128
+  }
```

```
+}
# commit
```

31.4.2 Настройка шифрования в интерефейсе fortun

В примере из пункта «Минимальные настройки» рассматривается настройка туннеля без шифрования трафика.

Для криптографической защиты туннеля необходимо указать настройку `encryption` и настроить использование ключей forsec-keypair или forsec-key.

31.4.2.1 Шифрование с использованием ключей forsec-key

Для корректной работы туннеля на обоих его концах должны совпадать серия ключей и настройка `id`; настройки `local-cn` и `remote-cn` (номера локального и удалённого абонентов) должны быть зеркально симметричными, при этом `local-cn` и `remote-cn` не должны быть равны друг другу.

Настройка режима шифрования на интерефейсе `fortun` с использованием ключей forsec-key осуществляется на следующем уровне конфигурации:

```
[edit interface fortun <fortun-interface-name> forsec-key]
```

где `<fortun-interface-name>` – имя существующего интерфейса `fortun`.

На данном уровне конфигурации доступны следующие настройки:

– `local-cn <local-cn-number>` – указать номер локального абонента, где `<local-cn-number>` – число от 0 до 65535;

– `remote-cn <remote-cn-number>` – указать номер удалённого абонента, где `<remote-cn-number>` – число от 0 до 65535;

– `serial <serial-number>` – указать номер серии ключа, где `<serial-number>` – число от 0 до 4294967295.

Дополнение примера, приведённого в пункте «Минимальные настройки», командами для настройки режима шифрования с использованием ключей forsec-key:

```
[edit interface fortun fort1]
# edit forsec-key
# set local-cn 14
# set remote-cn 19
# set serial 12345
```

```
# diff
+interface {
+  fortun fort1 {
+    enable
+    ipv4 {
+      local 10.10.10.1
+      remote 10.10.10.34
+    }
+    id 128
+    forsec-key {
+      serial 12345
+      local-cn 14
+      remote-cn 19
+    }
+    encryption
+  }
+}
# commit
```

31.4.2.2 Шифрование с использованием ключей forsec-keypair

Для корректной работы туннеля абонентам необходимо сгенерировать ключ forsec-keypair (каждому свой), а затем обменяться открытыми ключами forsec-keypair по каналу, гарантирующему защиту от подмены, и указать полученные ключи в настройках интерфейса `fortun`.

Настройка режима шифрования на интерефейсе `fortun` с использованием ключей forsec-keypair осуществляется на следующем уровне конфигурации:

```
[edit interface fortun <fortun-interface-name> forsec-keypair]
```

где `<fortun-interface-name>` – имя существующего интерфейса `fortun`.

На данном уровне конфигурации доступны следующие настройки:

– `local-key <local-key-name>` – указать имя ключа forsec-keypair, сгенерированного на ПАК «Фортикс», где `<local-key-name>` – имя существующего ключа forsec-keypair;

– `remote-key <remote-key-name>` – указать имя импортированного открытого ключа forsec-keypair удалённого абонента, где `<remote-key-name>` – имя существующего ключа forsec-keypair.

Дополнение примера, описанного в пункте «Минимальные настройки», командами для настройки режима шифрования с использованием ключей forsec-keypair:

```
[edit interface fortun fort1]
# edit forsec-keypair
# set local-key mykey
# set remote-key herson-key
# diff
+interface {
+  fortun fort1 {
+    enable
+    ipv4 {
+      local 10.10.10.1
+      remote 10.10.10.34
+    }
+    id 128
+    forsec-keypair {
+      local-key mykey
+      remote-key herson-key
+    }
+    encryption
+  }
+}
# commit
```

31.4.2.3 Использование ключей в туннелях fortun

Особенности работы с ключами forsec-key/forsec-keypair в интерфейсах fortun:

1) Для определения настроек `forsec-key`/`forsec-keypair` необходимо указание настройки `encryption`.

2) Загрузка ключевой информации интерфейса в ядро осуществляется в момент выполнения команды `commit` (а также при загрузке системы) без учёта состояния интерфейса (настройки `enable`), в связи с чем, в случае отсутствия в системе КД, в журнал записывается сообщение уровня ALERT о невозможности загрузки ключевой информации. Если в конфигурации интерфейса указана настройка `enable`, при успешной загрузке КД интерфейс автоматически становится доступным.

3) При конфигурировании туннеля `fortun` для настроек `forsec-keypair`/`forsec-key` предусмотрено автодополнение по клавише `Tab` (для `local-key`/`remote-key`/`serial`), которое работает только при наличии КД в оперативной памяти.

4) Если в конфигурации интерфейса `fortun` одновременно заданы настройки `forsec-keypair` и `forsec-key`, для шифрования используются ключи forsec-key.

31.4.2.4 Балансировка шифрования по ядрам

В ПАК «Фортикс» реализована возможность настройки балансировки шифрования по ядрам процессоров.

Для настройки балансировки шифрования по ядрам процессоров применяется команда:

```
# set crypto forsec smp-affinity <smp-affinity-number>
```

где `<smp-affinity-number>` – номера ядер процессоров.

Пример применения команды для настройки балансировки шифрования по ядрам процессоров:

```
# set crypto forsec smp-affinity 1-2,4
# commit
```

31.4.2.5 Защита от replay-атак

Для защиты от replay-атак используется специальное окно номеров пакетов, в рамках которого возможен приём трафика. Также возможен приём более позднего трафика. В случае получения (и успешного расшифрования) трафика окно сдвигается.

Для настройки размера окна применяется команда:

```
# set crypto forsec replay-window <replay-window-size>
```

где `<replay-window-size>` – число от 64 до 131008 пакетов или номеров, по умолчанию – 4096.

Пример применения команды для настройки размера окна:

```
# set crypto forsec replay-window 32
# commit
```

31.4.2.6 Таймаут ресинхронизации туннелей

Для отправки служебных сообщений синхронизации тунелей устанавливается настраиваемое ограничение. По умолчанию оно составляет одно сообщение в 30 секунд.

Для настройки значения таймаута применяется команда:

```
# set crypto forsec resync-delay <resync-delay-value>
```

где `<resync-delay-value>` – число секунд от 1 до 65535, по умолчанию – 30.

Пример применения команды для настройки значения таймаута:

```
# set crypto forsec resync-delay 5
# commit
```

31.4.3 Сетевые настройки туннелей fortun

31.4.3.1 Настройка UDP-инкапсуляции

Весь трафик fortun по умолчанию инкапсулируется в протокол UDP. В настройках интерфейса возможно указание портов получателя и отправителя (по умолчанию используются порты 505).

Настройка UDP-инкапсуляции осуществляется на следующем уровне конфигурации:

```
[edit interface fortun <fortun-interface-name> encap]
```

где `<fortun-interface-name>` – имя существующего интерфейса `fortun`.

На данном уровне конфигурации доступны следующие настройки:

– `sport <sport-number>` – указать порт отправителя, где `<sport-number>` – число от 0 до 65535;

– `dport <dport-number>` – указать порт получателя, где `<dport-number>` – число от 0 до 65535.

Дополнение примера, приведённого в пункте «Минимальные настройки», командами для настройки UDP-инкапсуляции:

```
[edit interface fortun fort1]
# edit encap
# set sport 501
# set dport 503
# diff
+interface {
+  fortun fort1 {
+    enable
+    ipv4 {
+      local 10.10.10.1
+      remote 10.10.10.34
+    }
+    id 128
+    encap {
+      sport 501
+      dport 503
+    }
+  }
+}
# commit
```

31.4.3.2 NAT-traversal

Для работы через NAT при неизвестном адресе/номере порта удалённого конца следует указать значение 0 UDP-порта и 0.0.0.0 IP-адреса удалённого абонента. В этом случае интерфейс ожидает входящий пакет от любого IP-адреса с любого порта.

Дополнение примера, приведённого в пункте «Минимальные настройки», командами для настройки NAT-traversal:

```
[edit interface fortun fort1]
# set encap dport 0
# set ipv4 remote 0.0.0.0
# diff
+interface {
+  fortun fort1 {
+    enable
+    ipv4 {
+      local 10.10.10.1
+      remote 0.0.0.0
+    }
+    encap dport 0
+    id 128
+  }
+}
# commit
```

31.4.3.3 Пинг-пробы

Пинг-пробы предназначены для определения статуса удалённого конца.

Настройка пинг-проб осуществляется на следующем уровне конфигурации:

```
[edit interface fortun <fortune-interface-name> keepalive]
```

где `<fortun-interface-name>` – имя существующего интерфейса `fortun`.

На данном уровне конфигурации доступны следующие настройки:

– `interval <interval-value>` – указать временной интервал пинг-проб, где `<interval-value>` – число секунд от 0 до 65535, по умолчанию – 3;

– `retries <retries-number>` – указать максимально допустимое количество пинг-проб, где `<retries-number>` – число от 0 до 65535, по умолчанию – 3.

При отсутствии ответной пробы через указанное в настройке `retries` количество попыток интерфейс переходит в состояние NO-CARRIER (отсутствие соединения).

Дополнение примера, приведённого в пункте «Минимальные настройки», командами для настройки пинг-проб:

```
[edit interface fortun fort1]
# edit keepalive
# set interval 10
# set retries 4
# diff
+interface {
+  fortun fort1 {
+    enable
+    ipv4 {
+      local 10.10.10.1
+      remote 10.10.10.34
+    }
+    keepalive {
+      interval 10
+      retries 4
+    }
+    id 128
+  }
+}
# commit
```

31.5 Генератор ключевых документов (ГКД)

Генератор ключевых документов (далее по тексту – ГКД) представляет собой программное обеспечение, выполняющее генерацию матрицы симметричных ключей для обеспечения защищённой парной связи между ПАК «Фортикс» по принципу «все со всеми». Матрица является квадратной и симметричной. Каждый элемент матрицы представляет собой два 256-разрядных ключа, которые возможно использовать в алгоритмах симметричного шифрования согласно ГОСТ Р 34.12-2018 [1]. Данная пара ключей используется для обеспечения защищённой связи между двумя абонентами (ПАК «Фортикс»). Абоненты идентифицируются порядковыми номерами (начиная с 1). Номера пары абонентов являются координатами элемента в матрице.

Генерация ключей осуществляется с использованием ФДСЧ устройства «Фортикс-Стена».

В процессе генерации матрица ключей находится только в оперативной памяти ПАК «Фортикс» и не сохраняется в постоянной памяти ПАК «Фортикс».

После генерации осуществляется запись матрицы в зашифрованном виде на внешний носитель. Ключи шифрования матрицы записываются на другой внешний носитель. Далее

ключевые данные удаляются из оперативной памяти ПАК «Фортикс» (с предварительной зачисткой псевдослучайными данными).

Далее строки матрицы выборочно загружаются в оперативную память ПАК «Фортикс» с внешнего носителя и осуществляется их последующий экспорт на ключевые носители абонентов. Строка может быть экспортирована только один раз.

Каждая матрица ключей идентифицируется номером (серией) – числом от 1 до 4294967295. Другими атрибутами матрицы являются: количество абонентов (от 2 до 10000), дата/время выпуска.

Для хранения ключей доступа к матрице, самой матрицы, ключевых документов абонентов на внешних носителях используется ключевой контейнер SymEx.

В каждом контейнере присутствует файл `info.txt`, который содержит информацию о матрице/строке в текстовом виде. Данный файл является исключительно информационным и не влияет на целостность контейнера.

Генерация и экспорт ключей осуществляются при отключённых сетевых интерфейсах.

Для работы генератора ключевых документов необходимо наличие ключа доступа в оперативной памяти ПАК «Фортикс».

31.5.1 Генерация ключей

При работе службы генерации ключей все сетевые кабели должны быть отключены или в конфигурации всех Ethernet-интерфейсов должна отсутствовать настройка `enable`.

Для отключения проверки на отсутствие подключения к сети применяется команда:

```
# set crypto matrix no-net-check
# commit
```

Указанная команда доступна для учётных записей администраторов СКЗИ.

П р и м е ч а н и е – Отключать данную проверку не рекомендуется, так как иначе пользователь ПАК «Фортикс», доступ которого к ключевой информации запрещён, имеет возможность подключиться к ПАК по сети (SSH, NETCONF и т.д.) и получить несанкционированный доступ к внешним носителям с ключевой информацией.

Для работы с ГКД используется в режиме генерации ключей.

Для входа в режим генерации ключей применяется команда:

```
> crypto matrix operate
(keygen)> _
```

Режим генерации ключей в командной строке отображается следующим образом:

```
(keygen)> _
```

Для просмотра текущего статуса службы генерации ключей применяется команда:

```
(keygen)> show status
Status: empty
```

Генерация ключей осуществляется службой только в статусе `empty`, иначе необходимо выполнить очистку службы.

Для очистки службы применяется команда:

```
(keygen)> cleanup
```

П р и м е ч а н и е – Очистка выполняется в фоновом режиме и, как правило, не занимает большого количества времени. После очистки службы рекомендуется выполнить команду `show status` повторно для проверки соответствия значения статуса службы (`Status: empty`).

Для запуска генерации матрицы ключей применяется команда:

```
(keygen)> generate <serial-number> <peer-number>
```

где

– `<serial-number>` – номер серии матрицы ключей от 1 до 4294967295;

– `<peer-number>` – количество абонентов от 2 до 10000.

После запуска генерация осуществляется в фоновом режиме.

Для отслеживания процесса генерации применяется команда:

```
(keygen)> show status [follow]
```

где `follow` – параметр, при указании которого используется режим непрерывного отслеживания прогресса.

Для прерывания отслеживания используется комбинация клавиш `<Ctrl>+<C>`.

При длительном процессе генерации матрицы возможен выход из режима генерации ключей и сессии, при этом генерация продолжится в фоновом режиме.

Для отслеживания статуса службы вне режима генерации ключей применяется команда:

```
> show crypto matrix status [follow]
```

Если генерация завершается с ошибкой, отражаемой в статусе, ключевые данные автоматически зачищаются и удаляются из оперативной памяти ПАК «Фортикс».

Возможные причины неуспешного завершения генерации:

– подключение сетевого кабеля к интерфейсу с указанной настройкой `enable` в конфигурации;

– недостаточный объём оперативной памяти ПАК «Фортикс»;

– некорректная работа ФДСЧ устройства «Фортикс-Стена» (устройство не отвечает или вырабатывает данные с энтропией неудовлетворительного качества).

После неуспешной генерации необходимо выполнить очистку с помощью команды:

```
(keygen)> cleanup
```

Очистка может быть выполнена вне режима генерации ключей с помощью команды:

```
> crypto matrix cleanup
```

При успешном завершении генерации служба переходит в следующее состояние:

```
Status: matrix generated
```

Далее необходимо подключить внешний носитель для сохранения на него ключей шифрования матрицы (main keys).

Для сохранения ключей шифрования матрицы на внешний носитель применяется команда:

```
(keygen)> save-main-keys <path-to-dir>
```

где `<path-to-dir>` – полное имя директории на внешнем носителе относительно директории `/media`.

Пример применения команды для сохранения ключей шифрования матрицы на внешний носитель:

```
(keygen)> save-main-keys /media/flash0
```

При успешном сохранении ключей шифрования матрицы служба переходит в следующее состояние:

```
Status: main keys saved
```

Далее необходимо подключить другой носитель и сохранить на него зашифрованную матрицу ключей.

Для сохранения зашифрованной матрицы ключей на внешний носитель применяется команда:

```
(keygen)> save-matrix <path-to-dir>
```

где <path-to-dir> – полное имя директории на внешнем носителе относительно директории /media.

В случае матриц больших объёмов процесс сохранения занимает длительное время, в течение которого на экране отображается прогресс сохранения.

После успешного сохранения матрицы автоматически инициируется зачистка ключевой информации в оперативной памяти ПАК «Фортикс», и (через некоторое время) служба переходит в состояние:

```
Status: empty
```

П р и м е ч а н и е – Рекомендуется хранить носитель с ключами шифрования матрицы и носитель с самой матрицей отдельно от друг друга.

31.5.2 Создание ключевых документов абонентов

Создание ключевых документов абонентов на основе матрицы ключей осуществляется в режиме генерации ключей.

Для входа в режим генерации ключей применяется команда:

```
> crypto matrix operate
```

Создание ключевых документов абонентов возможно только при нахождении службы генерации ключей в состоянии empty.

Для проверки состояния службы применяется команда:

```
(keygen)> show status
Status: empty
```

Если служба находится не в состоянии empty, необходимо выполнить очистку службы.

Для очистки службы применяется команда:

```
(keygen)> cleanup
(keygen)> show status
Status: empty
```

Далее необходимо ввести в систему ключи шифрования матрицы с внешнего носителя.

Для ввода ключей шифрования матрицы с подключённого к ПАК «Фортикс» внешнего носителя применяется команда:

```
(keygen)> load-main-keys <path-to-dir>
```

где <path-to-dir> – полное имя директории на внешнем носителе относительно директории /media.

В случае успешной загрузки отображается информация о матрице (серия, количество абонентов, дата/время выпуска) и служба переходит в следующее состояние:

```
Status: main keys loaded
```

При успешной загрузке команда show status отображает информацию о матрице.

Далее необходимо подключить носитель с зашифрованной матрицей ключей (носитель с ключами шифрования матрицы можно отключить).

П р и м е ч а н и е – Рекомендуется выполнить проверку целостности матрицы.

Для проверки целостности матрицы применяется команда:

```
(keygen)> check-matrix <path-to-dir>
```

где <path-to-dir> – полное имя директории на внешнем носителе относительно директории /media.

В случае матриц большого объёма процесс проверки занимает некоторое время, в течение которого отображается прогресс проверки.

Далее необходимо выборочно загрузить в оперативную память ПАК «Фортикс» строки ключей для абонентов с целью их последующего экспорта в качестве ключевых документов абонентов.

Для загрузки в оперативную память ПАК «Фортикс» строк ключей для указанных абонентов применяется команда:

```
(keygen)> load-key-line <path-to-dir> <peer-number>
```

где

– <path-to-dir> – полное имя директории на внешнем носителе относительно директории /media;

– <peer-number> – число от 1 до 10000.

Пример применения команды для загрузки в оперативную память ПАК «Фортикс» строк ключей для указанных абонентов:

```
(keygen)> load-key-line /media/flash0 1
(keygen)> load-key-line /media/flash0 2
...
```

Для просмотра списка загруженных строк применяется команда:

```
(keygen)> show key-lines
```

Для просмотра строки ключей указанного абонента применяется команда:

```
(keygen)> show key-line-status <peer-number>
```

где <peer-number> – число от 1 до 10000.

Далее необходимо подключить носитель для сохранения ключевого документа абонента и экспортировать строки ключей.

Для экспорта строк ключей указанного абонента на внешний носитель применяется команда:

```
(keygen)> export-key-line <path-to-dir> <peer-number>
```

где

– <path-to-dir> – полное имя директории на внешнем носителе относительно директории /media;

– <peer-number> – число от 1 до 10000.

Пример алгоритма создания ключевых документов:

1) Отключить носитель с матрицей ключей.

2) Подключить носитель ключевого документа абонента 1.

3) Экспортировать строку ключей для абонента 1:

```
(keygen)> export-key-line /media/flash0 1
```

4) Отключить носитель абонента 1.

5) Повторить пункты 2-4 для абонента 2:

```
(keygen)> export-key-line /media/flash0 2
```

6) Повторить для экспорта всех строк из оперативной памяти ПАК «Фортикс».

После экспорта строка автоматически удаляется из оперативной памяти ПАК «Фортикс».

П р и м е ч а н и е – Все строки, находящиеся в оперативной памяти ПАК «Фортикс», необходимо экспортировать на носители ключевых документов абонентов, так как при выполнении команды load-key-line данные строки помечаются как экспортированные в контейнере матрицы ключей и далее

повторное выполнение команды `load-key-line` для указанных строк невозможно. В случае перезагрузки устройства или выполнения команды `cleanup` неэкспортированные строки безвозвратно утрачиваются.

31.5.3 Диагностика

Для просмотра состояния службы применяются команды:

```
> show crypto matrix status
(keygen)> show status
```

Служба осуществляет запись значимых событий в журнал СКЗИ (см. подраздел «Журнал событий СКЗИ»).

При нештатном поведении службы (например, из-за внутренних ошибок) возможно проведение более подробной диагностики по системным сообщениям службы.

Для просмотра всех системных сообщений службы применяется команда:

```
> show journal service zmatrixd
```

31.6 Контейнер парольной защиты

В ПАК «Фортикс» реализована возможность создания контейнера для файла, защищённого паролем. Для успешного выполнения команд по настройке контейнераов необходимо наличие ключа доступа в оперативной памяти ПАК «Фортикс».

31.6.1 Создание контейнера парольной защиты

Для создания контейнера для указанного файла применяется команда:

```
> crypto encrypt <path-to-file>
```

где `<path-to-file>` – полное имя файла (размер файла не должен превышать 16 МБ) или имя файла относительно домашней директории пользователя.

При выполнении команды запрашивается пароль, который должен удовлетворять следующим требованиям:

1) длина пароля составляет не менее 8 символов;

2) пароль нетривиален.

В случае несоответствия пароля требованиям выполнение команды прерывается.

После выполнения команды исходный файл удаляется, в директории исходного файла создаётся файл с именем исходного файла и расширением «.cpt».

31.6.2 Расшифрование контейнера парольной защиты

Для извлечения файла из зашифрованного контейнера применяется команда:

```
> crypto decrypt <path-to-file-with-container> <path-to-save-decrypted-data>
```

где

– `<path-to-file-with-container>` – полное имя файла с зашифрованным контейнером или имя файла относительно домашней директории пользователя;

– `<path-to-save-decrypted-data>` – полное имя выходного файла или имя файла относительно домашней директории пользователя.

При выполнении команды запрашивается пароль.

31.7 Журнал событий СКЗИ

Подсистемы СКЗИ осуществляют запись значимых событий в специальный журнал событий СКЗИ, целостность и подлинность которого защищается ключом доступа.

Каждая запись в журнале представляет собой строку, содержащую дату, время и описание события. В журнале указываются локальные дата/время согласно настройке временной зоны.

Пример формата записи в журнале:

```
2025-03-24 09:20:04 : Security log created.
```

Журнал событий СКЗИ является многотомным и ротируемым. Журнал состоит из томов (частей), нумерующихся с нуля. Том с номером 0 является наиболее новым, в него записываются текущие события. В случае, когда при очередной записи размер тома с номером 0 превышает предельно допустимый, выполняется ротация, при которой все тома перенумеровываются по принципу «+1», и создаётся новый пустой том с номером 0. При этом, если количество томов достигло предельно допустимого, удаляется старший том (с наибольшим номером). События ротации и удаления томов регистрируются в журнале.

Возможна настройка предельных значений размера тома и количества томов в журнале. По умолчанию установлены значения 500 кБ и 11 томов (от 0-го до 10-го) соответственно.

Целостность журнала (нулевого тома) проверяется каждый раз при регистрации нового события и при перезапуске системы. В случае нарушения целостности генерируется событие уровня ALERT со звуковым оповещением. Также целостность тома журнала проверяется перед его просмотром. Возможно ручное инициирование проверки целостности томов с помощью команды.

Для регистрации событий и проверки целостности необходимо наличие ключа доступа в оперативной памяти ПАК «Фортикс».

Если в оперативной памяти ПАК «Фортикс» отсутствует ключ доступа или нарушена целостность журнала СКЗИ, при попытке регистрации события в системный журнал записывается сообщение о невозможности регистрации события СКЗИ.

Для просмотра содержимого младшего тома (с номером 0) применяется команда:

```
> show crypto log
```

Для просмотра журнала в случае отсутствия ключа доступа или нарушения целостности применяется команда:

```
> show crypto log no-check
```

Для просмотра номера старшего тома (с наибольшим номером) применяется команда:

```
> show crypto log oldest
```

Для просмотра содержимого тома с указанным номером применяется команда:

```
> show crypto log volume <volume-number> [no-check]
```

где

– `<volume-number>` – число от 0 до 65535;

– `no-check` – параметр, при указании которого проверка целостности тома не осуществляется.

Для проверки целостности тома с указанным номером применяется команда:

```
> crypto log check volume <volume-number>
```

где `<volume-number>` – число от 0 до 65535.

Для проверки целостности всех томов применяется команда:

```
> crypto log check all
```

Если целостность нарушена по каким-либо причинам, регистрация новых событий в журнале СКЗИ невозможна. Для возобновления работоспособности журнала необходимо выполнить его восстановление.

Для восстановления журнала применяется команда:

```
> crypto log repair
```

Команда обновляет имитозащиту всего журнала и регистрирует факт восстановления с указанием имени пользователя, инициировавшего данную команду. В журнал СКЗИ заносится уведомление о том, что достоверность предыдущих записей не гарантируется.

Если восстановление журнала не требуется, данная команда не осуществляет никаких действий и выводит соответствующее сообщение.

Для изменения максимального размера тома журнала применяется команда:

```
# set crypto log max-volume-size <max-volume-size-value>
```

где `<max-volume-size-value>` – число КБ от 1, по умолчанию – 500.

Для изменения предельного номера старшего тома журнала применяется команда:

```
# set crypto log max-volume-no <max-volume-no-number>
```

где `<max-volume-no-number>` – число от 1, по умолчанию – 10).

Указанные в настройках параметры применяются при регистрации очередного события в журнале СКЗИ. То есть (если необходимо) осуществляется ротация и удаление старых томов, имеющих больший номер, чем значение `<max-volume-no-number>`.

Для немедленного удаления старых томов применяется команда:

```
> crypto log trim-volumes
```

Для очистки журнала применяется команда:

```
> crypto log clear
```

По указанной команде удаляются тома, все события в которых старше трёх суток, при этом том с номером 0 никогда не удаляется. В журнале СКЗИ регистрируется факт очистки и имя инициировавшего её пользователя. Перед выполнением команды запрашивается подтверждение.

События, регистрируемые в журнале:

– создание журнала;

– ротация журнала;

– автоматическое удаление старых томов при ротации;

– очистка журнала администратором;

– факт входа администратора в режим генерации ключей (при выполнении команды ‘crypto matrix operate’) и имя его учётной записи;

– закрытие сессии администратора, использовавшего режим генерации ключей (при его выходе из всех командных оболочек);

– генерация матрицы ключей, атрибуты матрицы;

– ошибки генерации матрицы ключей;

– очистка ключевых данных в оперативной памяти ПАК «Фортикс»;

– сохранение матрицы и ключей шифрования на внешние носители;

– загрузка ключей шифрования матрицы в оперативную память ПАК «Фортикс»;

– загрузка строк ключей в оперативную память ПАК «Фортикс»;

– создание ключевых документов абонентов;

– выработка, удаление и ввод ключевых пар;

– факты окончания срока действия ключа доступа, ключей парно-выборочной связи и ключевых пар;

– ввод ключей и удаление ключей парно-выборочной связи;

– факты отказа от ввода ключей в связи с нарушением требования наличия ключа парно-выборочной связи указанного абонента в хранилище при настройке туннеля;

– нарушение целостности ПО ПАК «Фортикс»;

– выработка, экспорт, замена и удаление ключа доступа;

– факт окончания срока действия ключа доступа;

– файловые операции с ключевым хранилищем;

– дублированные из системного журнала события, попадающие под правила `action crypto-log` (см. раздел «Служба journal»);

– факт блокировки СКЗИ при обнаружении проблем с ФДСЧ;

– факт инициации администратором процедуры регламентного контроля ФДСЧ и имя его учётной записи;

– факт инициации регулярной процедуры динамического контроля ФДСЧ;

– факт завершения регламентного/динамического контроля ФДСЧ и его результат;

– ошибки при обращении к ключевым документам на внешних носителях.

31.8 Динамический и регламентный контроль ФДСЧ

Процедура регламентного контроля ФДСЧ устройства «Фортикс-Стена» представляет собой проверку на прохождение статистических тестов 4 кБ случайных данных, полученных от ФДСЧ.

Для выполнения регламентного контроля применяется команда:

```
> crypto rng check-phrng
```

При успешном прохождении регламентного контроля выводится следующее сообщение:

```
Info: PhRNG check passed successfully.
```

При неуспешном прохождении регламентного контроля выводится сообщение об ошибке и подсистема СКЗИ блокируется. (см. подраздел «Блокировка СКЗИ»).

Динамический контроль ФДСЧ аналогичен регламентному за исключением того, что динамический контроль запускается системой автоматически на регулярной основе.

Частота запуска динамического контроля определяется настройкой `system software-integrity` (см. подраздел «Контроль целостности»).

Динамический контроль проводится только в случае, если в конфигурации системы определена настройка `system software-integrity` и в постоянной памяти ПАК «Фортикс» присутствует ключ доступа.

Факт инициации и результат динамического контроля регистрируются в журнале событий СКЗИ.

31.9 Блокировка СКЗИ

Если при обращении к ФДСЧ обнаруживается его неработоспособность, подсистема СКЗИ блокируется.

Неработоспособность ФДСЧ может быть обнаружена в момент выполнения следующих операций:

– при загрузке системы и попытке осуществления начальной инициализации ПДСЧ;

– при попытке осуществления регулярной переинициализации ПДСЧ (раз в минуту);

– при проведении регламентного контроля ФДСЧ;

– при проведении динамического контроля ФДСЧ;

– при попытке осуществления генерации матрицы симметричных ключей;

– при попытке осуществления генерации ключевой пары асимметричных ключей.

При блокировке СКЗИ выполняются следующие действия:

1) Если в постоянной памяти ПАК «Фортикс» присутствует ключ доступа, в журнале событий СКЗИ регистрируется событие о неработоспособности ФДСЧ.

2) Ключ доступа зачищается/удаляется из постоянной памяти ПАК «Фортикс».

3) В системном журнале регистрируется событие уровня ALERT со звуковым оповещением.

4) В оперативной памяти ПАК «Фортикс» устанавливается признак блокировки СКЗИ. Данный признак запрещает выполнение команд загрузки/инициализации ключа доступа. Признак удаляется при перезагрузке системы.

5) Ключевой материал, присутствующий в памяти службы генерации матрицы ключей, зачищается/удаляется.

При выполнении процедуры блокировки СКЗИ невозможно выполнение следующих операций:

– загрузка/инициализация ключа доступа;

– запись в журнал событий СКЗИ;

– генерация матрицы симметричных ключей;

– генерация закрытых/открытых ключей;

– создание контейнеров парольной защиты;

– создание электронных подписей файлов;

– инициация новых туннелей `fortun`.

П р и м е ч а н и е – Инициированные до блокировки СКЗИ туннели `fortun` продолжат свою работу, так как они не нуждаются в ФДСЧ/ПДСЧ и их ключи шифрования находятся в постоянной памяти ПАК «Фортикс».

Ссылочные нормативные документы

1 ГОСТ Р 34.12-2018 Информационная технология. Криптографическая защита информации. Блочные шифры

2 ГОСТ Р 34.13-2018 Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров

3 ГОСТ Р 34.11-2012 Информационная технология. Криптографическая защита информации. Функция хэширования

Ссылочные документы

1 ПАК «Фортикс» Формуляр НВЦС.465651.001ФО

2 ПАК «Фортикс» Формуляр. Приложение А Спецификация поставки НВЦС.465651.001ФО1

3 СКЗИ «Фортикс» Формуляр ПБЦР.468269.003ФО

4 СКЗИ «Фортикс» Правила пользования ПБЦР.468269.003ПП

Лист регистрации изменений

Изм.	Номера листов (страниц)				Всего листов (страниц) в докум.	№ докум.	Входящий № сопроводительного докум. и дата	Подп.	Дата
	измененных	замененных	новых	аннулированных					