

ViPNet Coordinator HW 5

Настройка с помощью командного интерпретатора

Версия продукта: 5.4.2

ViPNet Coordinator HW50
ViPNet Coordinator HW100
ViPNet Coordinator HW1000
ViPNet Coordinator HW2000
ViPNet Coordinator HW5000
ViPNet Coordinator VA

infotecs

© АО «ИнфоТеКС», 2026

ФРКЕ.465614.003ИС2

Версия продукта: 5.4.2

Этот документ входит в комплект поставки продукта ViPNet, и на него распространяются все условия лицензионного соглашения.

Ни одна из частей этого документа не может быть воспроизведена, опубликована, сохранена в электронной базе данных или передана в любой форме или любыми средствами, такими как электронные, механические, записывающие или иначе, для любой цели без предварительного письменного разрешения АО «ИнфоТеКС».

ViPNet® является зарегистрированным товарным знаком АО «ИнфоТеКС».

Все названия компаний и продуктов, которые являются товарными знаками или зарегистрированными товарными знаками, принадлежат соответствующим владельцам.

Все условия эксплуатации и ограничения на использование ViPNet Coordinator HW приведены в Правилах пользования, Лицензионном соглашении с конечным пользователем либо в другой эксплуатационной документации, сопровождающей ViPNet Coordinator HW.

АО «ИнфоТеКС»

125167, г. Москва, вн. тер. г. муниципальный округ Хорошевский, ул. Викторенко, д. 9, стр. 1, помещ. 47

Телефон: +7 (495) 737-6192, 8 (800) 250-0260 — бесплатный звонок из России (кроме Москвы)

Сайт: infotecs.ru

Служба поддержки: hotline@infotecs.ru

Содержание

Введение **14**
О документе 15
Соглашения документа 16
Обратная связь 18

Глава 1. Работа с командным интерпретатором **19**
Основные сведения по работе с командным интерпретатором 20
Интерфейс командного интерпретатора 21
Сокращенный ввод команд 21
Автодополнение команд 21
Контекстная справка 21
Сочетания клавиш 23
Выбор консоли при локальном подключении 24
Локальное подключение с помощью консоли 25
Удаленное подключение по SSH 26

Глава 2. Настройка подключения к сети **28**
Настройка сетевых интерфейсов Ethernet 29
Назначение дополнительных IP-адресов 31
Просмотр параметров сетевых интерфейсов 32
Подключение к мобильной сети 3G/4G 33
Настройка доступа через сеть мобильного оператора 36
Подключение к сети Wi-Fi 38
Просмотр настроек динамических интерфейсов 40
Изменение значения MTU для сетевых интерфейсов 41
Настройка обработки трафика из нескольких VLAN 42
Настройка агрегированных сетевых интерфейсов 44
Режимы работы агрегированного интерфейса 44
Создание агрегированного интерфейса 47
Настройка агрегированного канала между HW и коммутатором 48
Настройка агрегированного канала между двумя HW 51
Настройка получения параметров от DHCP-сервера 53

Глава 3. Настройка VPN **54**
Общие принципы настройки VPN 55

Команды настройки iplir.conf 55
Настройка подключения к внешней сети 58
Режим «Со статической трансляцией адресов» 58
Режим «С динамической трансляцией адресов» 60
Просмотр сведений об узлах ViPNet 62
Настройка виртуальных IP-адресов 63
Общие сведения о виртуальных IP-адресах 63
Настройка диапазонов виртуальных IP-адресов 64
Настройка видимости узлов 65
Настройка туннелирования на сетевом уровне 68
Общие сведения о туннелировании 68
Ручная настройка туннелирования 69
Настройка туннелей между открытыми узлами 71
Настройка туннелей между узлами ViPNet и открытыми узлами 73
Настройка IP-адресов доступа к узлу и их приоритета 76
Настройка TCP-туннеля 79
Настройка сервера TCP-туннелей 79
Настройка TCP-клиента 80
Сценарии использования VPN 82
Объединение удаленных сегментов сети ViPNet 82
Настройка туннелирования на канальном уровне 83
Общие сведения о L2OverIP 83
Особенности реализации L2OverIP 85
Сценарии использования L2OverIP 85
Настройка L2OverIP для сегментов сети 87
Настройка L2OverIP для сегментов сети с VLAN 89
Настройка L2OverIP для ViPNet Coordinator VA 90

Глава 4. Настройка межсетевого экрана 92
О фильтрации трафика 93
Типы трафика 93
Классификация трафика с помощью DPI 94
Принципы фильтрации трафика 95
Настройка режима работы и параметров межсетевого экрана 101
Настройка антиспуфинга 102
Обработка фрагментированных IP-пакетов 104
Регистрация MAC-адресов источников сессий 105
Настройка аппаратной фильтрации трафика 106
Объекты сетевых фильтров и правил трансляции адресов 108

Системные объекты ... 108
Группы объектов «ViPNet-узлы», «IP-адреса», «Интерфейсы», «Протоколы» и «Расписания» ... 110
Создание группы объектов ... 110
Просмотр групп объектов ... 111
Удаление групп объектов ... 112
Группа объектов «Веб-клиенты» ... 113
Группа объектов «URL-категории» ... 115
Обновление базы URL-категорий ... 115
Настраиваемые URL-категории ... 116
Фильтрация по URL-категориям в содержимом веб-страниц ... 118
Группа объектов «Страны» ... 119
Настройка SSL/TLS-инспекции трафика ... 121
Настройка основных параметров SSL/TLS-инспекции ... 121
Настройка исключений из SSL/TLS-инспекции ... 123
Настройка SSL-сертификата ... 125
Особенности SSL/TLS-инспекции ... 126
Настройка подключения к ICAP-серверам ... 128
Настройка сетевых фильтров ... 131
Общие сведения о сетевых фильтрах ... 131
Создание сетевого фильтра ... 133
Адрес отправителя ... 137
Адрес получателя ... 139
Протокол ... 139
Приложение ... 140
Прикладной протокол ... 141
Группа приложений ... 141
Пользователь ... 142
Расписание ... 142
SSL/TLS-инспекция ... 143
Проверка правилами IPS ... 143
Проверка на ICAP-серверах ... 144
URL-адрес ... 144
Веб-клиенты ... 145
IP-адрес прокси-клиента ... 146
URL-категория ... 146
Регистрация IP-пакетов ... 146
Регистрация сессий ... 147
Действие ... 147

Изменение сетевого фильтра ... 148
Просмотр сетевых фильтров ... 149
Удаление сетевого фильтра ... 151
Настройка регистрации IP-пакетов и сессий при срабатывании фильтров ... 152
Блокирование сайтов по доменным именам ... 153
Блокирование поддоменов с помощью DNS-фильтров ... 154
Особенности фильтрации трафика по URL-адресам и URL-категориям ... 154
Примеры использования транзитных фильтров ... 155
Настройка фильтрации трафика по пользователю ... 155
Настройка фильтрации трафика Torrent-клиентов ... 156
Деактивация транзитных фильтров открытой сети после обновления ПО ... 156
Настройка правил трансляции адресов ... 158
Общие сведения о трансляции сетевых адресов ... 158
Трансляция адреса источника ... 159
Трансляция адреса назначения ... 160
Создание правила трансляции адресов ... 161
Просмотр, изменение, удаление правил трансляции сетевых адресов ... 162
Сценарии использования правил трансляции адресов ... 164
Настройка доступа ПК локальной сети к интернету ... 164
Настройка доступа к серверу в DMZ ... 165
Настройка доступа к узлам локальной сети с помощью дополнительных IP-адресов ... 166
Настройка доступа удаленных клиентов по протоколу PPTP ... 167
Настройка обработки прикладных протоколов DNS, FTP, H.323, SCCP, SIP ... 168
О прикладных протоколах ... 168
Настройка параметров обработки прикладных протоколов ... 171
Особенности обработки протокола SIP ... 174

Глава 5. Настройка сетевых служб ... 176
Настройка DHCP-сервера ... 177
Настройка DHCP-relay ... 179
Сценарии настройки DHCP-сервера и DHCP-relay ... 181
Настройка локального DHCP-сервера ... 181
Настройка внешнего DHCP-сервера и DHCP-relay ... 182
Использование DHCP-сервера и DHCP-relay в разных сетях ... 183
Использование сторонних DHCP-серверов ... 186
Одновременное использование DHCP-сервера и DHCP-relay ... 188
Использование запасного DHCP-сервера ... 189
Настройка DNS-сервера ... 191

Настройка NTP-сервера ... 193
Организация работы клиентов удаленного офиса с корпоративными DNS- и NTP-серверами ... 195
Настройка взаимодействия с Active Directory ... 197
Настройка учетной записи технологического пользователя ... 198
Подключение к контроллерам доменов ... 200
Настройка взаимодействия с LDAP-сервером ... 202
Получение и импорт сертификатов ... 203
Настройка параметров Captive portal ... 204
Настройка точки доступа сети Wi-Fi ... 207

Глава 6. Настройка маршрутизации ... 209
Общие сведения о маршрутизации ... 210
Принципы маршрутизации ... 211
Просмотр таблиц маршрутизации ... 215
Настройка статической маршрутизации ... 217
Создание статических маршрутов ... 217
Удаление статических маршрутов ... 218
Настройка балансировки IP-трафика ... 219
Просмотр статических маршрутов ... 220
Настройка маршрутов протоколов DHCP и PPP ... 221
Настройка административной дистанции для маршрутов DHCP-протокола ... 221
Настройка метрики для маршрутов DHCP-протокола ... 222
Настройка метрики для маршрутов PPP-протокола ... 223
Изменение метрики по умолчанию для маршрутов протоколов DHCP и PPP ... 224
Просмотр настроек DHCP в режиме клиента ... 224
Просмотр маршрутов DHCP/PPP-протокола ... 224
Настройка OSPF ... 226
Общие сведения о протоколе OSPF ... 226
Настройка протокола OSPF ... 228
Настройка перераспределения маршрутов ... 231
Просмотр настроек протокола OSPF ... 232
Настройка протокола OSPF в сетях со множественным доступом ... 232
Просмотр состояния каналов связи между маршрутизаторами ... 234
Просмотр информации о соседних маршрутизаторах ... 234
Просмотр маршрутов, сформированных по протоколу OSPF ... 235
Настройка маршрутизации по протоколу OSPF между удаленными сегментами сети ... 236
Настройка L2OverIP ... 237

Настройка OSPF ... 238
Настройка BGP ... 239
Общие сведения о протоколе BGP ... 239
Настройка соседей ... 239
Анонсирование подсетей и перераспределение маршрутов ... 241
Настройка фильтров и префикс-листов маршрутов ... 242
Настройка карт маршрутов ... 245
Настройка распространения маршрутов внутри AS ... 250
Поддержка ECMP и UCMP ... 252
Настройка резервирования каналов с помощью BGP ... 253
Настройка BFD ... 255
Настройка MultiWAN ... 257
Настройка политик маршрутизации ... 258
Настройка проверки состояния шлюзов (DGD) ... 260
Резервирование каналов доступа в интернет ... 262
Обеспечение связи между прокси-сервером и клиентами из разных сетей ... 264
Обработка приоритизированного трафика ... 265

Глава 7. Настройка предотвращения вторжений ... 267
Общие сведения об IPS ... 268
Параметры IPS по умолчанию ... 270
Включение и выключение IPS ... 271
Обновление базы правил IPS ... 272
Обновление базы вредоносного ПО ... 274
Просмотр настроек IPS ... 276
Настройка регистрации событий IPS ... 278
Восстановление базы правил IPS ... 279

Глава 8. Настройка параметров безопасности ... 280
Управление локальными учетными записями ... 281
Параметры учетных записей ... 281
Полномочия ролей по управлению учетными записями ... 281
Управление учетными записями ... 283
Предотвращение подбора пароля учетных записей ... 287
Настройка оповещения об истечении срока действия ключей ... 288
Просмотр сведений о ключе защиты обновлений и ключах обмена ... 289
Обновление ключей по истечении срока их действия ... 291
Перевыпуск ключей локального SSH-сервера ... 292
Настройка доступа сетевых интерфейсов к оперативной памяти ... 293

Глава 9. Настройка системных параметров 294
Настройка даты и времени 295
Настройка подключения к веб-интерфейсу 296
Выбор профиля производительности 298
Установка допустимого времени неактивности сессии пользователя 299
Просмотр активных сессий пользователей 300
Перезагрузка ViPNet Coordinator HW 301
Установка серийного номера 302
Просмотр лицензии 303
Использование резервного раздела в исполнениях с двумя накопителями 305
Сброс к заводским настройкам 306

Глава 10. Резервное копирование и восстановление настроек 308
Управление копиями конфигурации VPN 309
Создание копии конфигурации VPN 309
Просмотр списка копий конфигурации VPN 310
Восстановление настроек из копии конфигурации VPN 310
Удаление копии конфигурации VPN 311
Управление индивидуальной конфигурацией 313
Резервное копирование индивидуальной конфигурации 313
Восстановление из резервной копии индивидуальной конфигурации 315
Управление универсальной конфигурацией 318
Экспорт универсальной конфигурации 319
Импорт настроек универсальной конфигурации 319

Глава 11. Обеспечение отказоустойчивости 323
Настройка системы защиты от сбоев 324
Назначение системы защиты от сбоев 324
Работа системы защиты от сбоев в одиночном режиме 324
Работа системы защиты от сбоев в режиме кластера 325
Развертывание кластера 327
Параметры, влияющие на скорость переключения узлов кластера 333
Развертывание кластера совместно с DHCP-сервером и DHCP-relay 334
Запуск и завершение работы системы защиты от сбоев 335
Переключение системы защиты от сбоев в одиночный режим 336
Замена неисправного узла кластера 336
Работа кластера с коммутационным оборудованием 338
Подключение к пассивному узлу кластера по SSH 338
Просмотр информации о работе системы защиты от сбоев 340

Текущее состояние системы защиты от сбоев ... 340
Журнал переключений ... 342
Подключение ViPNet Coordinator HW к ИБП ... 344
Управление режимом производительности ... 347

Глава 12. Настройка транспортного сервера MFTP ... 348
Назначение транспортного сервера MFTP ... 349
Настройка протоколирования событий транспортного сервера MFTP ... 350
Настройка транзитного режима ... 351

Глава 13. Обновление программного обеспечения ... 352
Проверка ЭП файла обновления ... 353
Предварительные действия ... 353
Установка корневого сертификата и CRL ... 355
Проверка электронной подписи ... 357
Обновление ПО с версий 4.5.x до версии 5.4.x ... 359
Обновление ПО с версий 5.1.x, 5.2.x и 5.3.x до версии 5.4.x ... 364
Обновление ПО в кластере ... 367
Возврат к ПО версий 4.5.x ... 369
Возврат к ПО версий 5.1.x, 5.2.x и 5.3.x ... 372
Локальное обновление DPI ... 374

Глава 14. Работа с журналами ... 375
Журнал IP-пакетов ... 376
Журнал сессий ... 386
Журналы аудита и СКЗИ ... 387
Журнал MFTP ... 389
Журнал DNS-запросов ... 390
Системный журнал ... 391
Экспорт журнала IP-пакетов на USB-носитель ... 394
Экспорт журналов аудита, СКЗИ, MFTP, DNS-запросов и системного журнала на USB-носитель ... 396
Экспорт журнала IP-пакетов или журнала сессий по сети в формате CEF ... 397

Глава 15. Мониторинг работы ... 401
Мониторинг по SNMP ... 402
Настройка SNMP-агента ... 403
Мониторинг кластера ... 407
Мониторинг ViPNet-узлов ... 409

Мониторинг нагрузки ... 410
Блокировка источников повышенной сетевой нагрузки ... 412
Просмотр статистики передачи данных ... 414

Глава 16. Проверка работоспособности ... 415
Контроль целостности файлов ПО ... 416
Статистический контроль последовательностей случайных чисел ... 418
Проверка фильтрации транзитного трафика ... 420

Приложение A. Сетевые фильтры по умолчанию ... 421

Приложение B. Группы объектов ... 425

Приложение C. База URL-категорий ... 427

Приложение D. Типы событий журнала IP-пакетов ... 436

Приложение E. Структура записи журнала IP-пакетов в формате CEF ... 439

Приложение F. Структура записи журнала сессий в формате CEF ... 444

Приложение G. Базы управляющей информации (MIB) для протокола SNMP ... 446
MIB-II System ... 446
IF-MIB ... 450
IP-MIB ... 453
IP-FORWARD-MIB ... 459
Ethernet-Like MIB ... 463
TCP-MIB ... 464
UDP-MIB ... 467
HOST-RESOURCES-MIB ... 468
LM-SENSORS-MIB ... 474
NOTIFICATION-LOG-MIB ... 475
UCD-SNMP-MIB ... 476
UCD-DISKIO-MIB ... 480
NET-SNMP-MIB ... 481
SNMP-MPD-MIB ... 486
SNMP-TARGET-MIB ... 486
SNMP-USER-BASED-SM-MIB ... 486
SNMP-VIEW-BASED-ACM-MIB ... 488
SNMP-FRAMEWORK-MIB ... 490

VIPNET-MIB ... 491
VIPNETHW-MIB ... 493
VIPNETFWLOAD-MIB ... 494
VIPNETVPN-MIB ... 496
MonitoringAgent-MIB ... 497
System-MonitoringAgent-MIB ... 497

Приложение H. Службы ПО ViPNet Coordinator HW ... 498

Приложение I. Поддерживаемые приложения ... 501

Приложение J. Поддерживаемые прикладные протоколы ... 505

Приложение K. Поддерживаемые группы приложений ... 508

Приложение L. Особенности фильтрации по приложениям и прикладным протоколам ... 516

Приложение M. Поддерживаемые MIME-типы ... 518

Приложение N. Использование ViPNet Coordinator HW в качестве МЭ типа А четвертого класса защиты ... 522

Приложение O. Возможные неполадки ... 523

Блокирование медиа-сессии SIP-соединения при завершении сигнальной сессии по таймауту ... 523
Неполадки в работе сервисов IP-телефонии, видео- и аудиоконференций после переключения кластера ... 523
Не отображаются активные пользователи при настройке взаимодействия с Active Directory ... 524
Пропадает связь с контроллером Active Directory ... 524
После обновления базы правил IPS отображается неправильный статус ... 525
После настройки системного времени недоступна аутентификация пользователей ... 526
Ошибка обновления справочников, ключей и лицензий ... 526
Ошибка обновления ПО, справочников, ключей и лицензий ... 526
Ошибка локального обновления ПО ViPNet Coordinator VA ... 527
Ошибка обновления ПО версий 4.5.1/4.5.2 до версии 5.1.0 ... 527
При удалённом обновлении ПО обновился только один узел кластера ... 528
Ошибка создания резервной копии индивидуальной конфигурации на ViPNet Prime ... 528

Низкая скорость обработки трафика на интерфейсах 1G исполнения ViPNet Coordinator HW5000 ... 528
Сбои в работе агрегированного канала ... 529
Циклическая перезагрузка ViPNet Coordinator HW ... 529
Особенности добавления объектов лицензирования DPI и IPS ... 530
Особенности увеличения объёма оперативной памяти виртуальной машины ViPNet Coordinator VA ... 530
Нарушена связь ViPNet Coordinator HW с узлами защищенной сети ... 530
Особенности передачи трафика между ViPNet Coordinator HW версий 4.5.x–5.2.1 и 5.3.x ... 531
Особенности работы ViPNet Coordinator HW 5.3.1 с ViPNet Prime 1.9.5 ... 531
При подключении к сети Wi-Fi сетевой интерфейс не получает IP-адрес от DHCP-сервера ... 531

Приложение Р. Термины и сокращения ... 533



Введение

О документе 15

Соглашения документа 16

Обратная связь 18

О документе

В документе описаны основные сценарии настройки многофункционального шлюза безопасности ViPNet Coordinator HW с помощью командного интерпретатора. Документ предназначен для администраторов сетей ViPNet.

Соглашения документа



Внимание! Все сценарии работы с ViPNet Coordinator HW приведены для суперадминистратора `admin` в режимах просмотра или настройки.

Обозначение	Описание
	**Внимание!** Содержит критически важную информацию
	**Примечание.** Содержит рекомендательную информацию
	**Совет.** Содержит полезные приемы и хорошие практики
Название	Название элемента интерфейса: окна, вкладки, поля, кнопки, ссылки
Клавиша+Клавиша	Сочетание клавиш: нажмите первую клавишу и, не отпуская ее, нажмите вторую
Меню > Команда	Последовательность элементов или действий
`Код`	Имя файла, службы, интерфейса, путь или команда

Описание команд:

- Приглашение команд, которые могут быть выполнены аудитором или администратором в режиме просмотра, заканчивается символом >:

  ```
  hostname> firewall local show
  ```

- Приглашение команд, которые могут быть выполнены администратором в режиме настройки, заканчивается символом #:

  ```
  hostname# admin upgrade software
  ```

- Параметры, которые должны быть заданы аудитором или администратором, заключены в угловые скобки <>:

  ```
  inet bonding delete <номер>
  ```

  При вводе в командный интерпретатор параметры вводятся без угловых скобок:

  ```
  hostname# inet bonding delete 1
  ```

- Необязательные параметры или ключевые слова заключены в квадратные скобки `[]`:

  ```
  firewall <тип> add name @<имя> <состав> [exclude <исключения>]
  ```

  При вводе в командный интерпретатор необязательные параметры или ключевые слова вводятся без квадратных скобок:

  ```
  hostname# firewall ip-object add name @IP_group_1 110.35.14.0/24 exclude
  110.35.14.3,110.35.14.13
  ```

- Если при вводе команды можно указать один из нескольких параметров, допустимые варианты заключены в фигурные скобки `{}` и разделены вертикальной чертой `|`:

```
inet ntp mode {on | off}
```

При вводе в командный интерпретатор выбранные варианты параметров вводятся без фигурных скобок:

```
hostname# inet ntp mode off
```

- Идентификатор сетевого узла ViPNet указывается в шестнадцатеричном формате с префиксом `0x`:

  ```
  hostname# iplir ping 0x270e000a
  ```

Обратная связь

Контактная информация

- Единый многоканальный телефон:

  +7 (495) 737-6192,

  8 (800) 250-0-260 — бесплатный звонок из России (кроме Москвы).

- Служба поддержки: hotline@infotecs.ru.

  Форма для обращения в службу поддержки через сайт.

  Телефон для клиентов с расширенной поддержкой: +7 (495) 737-6196.

- Отдел продаж: soft@infotecs.ru.

Дополнительная информация на сайте ИнфоТеКС

- О продуктах ViPNet.
- О решениях ViPNet.
- Часто задаваемые вопросы.
- Форум пользователей продуктов ViPNet.

Если вы обнаружили уязвимости в продуктах компании, сообщите о них по адресу security-notifications@infotecs.ru. Распространение информации об уязвимостях продуктов ИнфоТеКС регулируется политикой ответственного разглашения.



1

Работа с командным интерпретатором

Основные сведения по работе с командным интерпретатором 20

Интерфейс командного интерпретатора 21

Выбор консоли при локальном подключении 24

Локальное подключение с помощью консоли 25

Удаленное подключение по SSH 26

Основные сведения по работе с командным интерпретатором

Работа в командном интерпретаторе возможна при локальном или удалённом подключении к ViPNet Coordinator HW:

- Локальное подключение с помощью консоли.
- Удаленное подключение по SSH.

Независимо от способа подключения командный интерпретатор запускается автоматически. Для аутентификации вы можете использовать учётные записи пользователей двух типов: локальные и централизованные. Подробнее см. документ «Подготовка к работе», раздел «Роли и учетные записи пользователей».

После успешной аутентификации командный интерпретатор находится в режиме просмотра, в котором доступны команды просмотра настроек. Строка приглашения интерпретатора в режиме просмотра заканчивается символом `>`.

Чтобы вводить команды по настройке и управлению ViPNet Coordinator HW, доступные для роли вашей учётной записи, перейдите в режим настройки. Для этого выполните команду `enable`. Строка приглашения интерпретатора в режиме настройки заканчивается символом `#`.

Одновременно могут быть запущены несколько копий командного интерпретатора, в которых открыты сессии пользователей различных типов и ролей. При этом интерпретаторы могут находиться в разных режимах.

- Чтобы просмотреть информацию обо всех запущенных сессиях пользователей, выполните команду `who`.
- Чтобы из режима настройки перейти в режим просмотра, выполните команду `exit`.
- Чтобы выйти из командного интерпретатора:
  - В режиме просмотра или настройки нажмите **Ctrl**+**D**.
  - В режиме просмотра выполните команду `exit`.

  При этом в консоли снова появится приглашение для аутентификации пользователя.

Интерфейс командного интерпретатора

Командный интерпретатор принимает текстовые команды, состоящие из слов, разделённых пробелами, латинских и специальных символов. Для облегчения ввода команд в интерпретаторе предусмотрены:

- сокращённый ввод команд (см. Сокращенный ввод команд);
- автодополнение команд;
- контекстная справка;
- сочетания клавиш.

Сокращенный ввод команд

Лексемы команды распознаются по минимальному числу символов, отличающих вводимую команду от других. Например, только у двух команд первая лексема начинается с символа «i» (`inet` и `iplir`): для указания первой команды достаточно набрать `in`, для указания второй — `ip`. Таким образом, вместо полной команды `iplir option mode` достаточно ввести `ip o mo`.

Если среди введенных символов есть ошибочные, то вся команда считается ошибочной, даже если ее можно однозначно определить по первым правильно введенным символам, например, команда `iplor o mo` будет ошибочной.

Автодополнение команд

Если введённые символы однозначно определяют команду или параметр команды, то вы можете автоматически дополнить недостающие символы, нажав **Tab**:

```
hostname> en<Tab>

hostname> enable _
```

Автодополнение работает только для слова, на котором находится курсор. Автодополнение не работает для параметров, значение которых вы задаёте (например, имена создаваемых объектов).

Контекстная справка

Контекстная справка позволяет вам просмотреть информацию о командах и параметрах, ввод которых возможен в текущей ситуации. Контекстная справка вызывается с помощью символа `?`.

Чтобы просмотреть список всех доступных вам групп команд, в приглашении командного интерпретатора введите символ ?:

```
hostname# ?
 license           shows information about license status and expiration date
 inet              a group of commands intended for working with routing,
                   interfaces and network tools
 failover          manage command for Failover daemon
 iplir
 machine           a group of system commands
 webui             manage WebUI service
 admin             perform management tasks
 enable            switch to the administrator mode
 exit              exit the command line interface
 version           view the versions of the appliance
 who               view currently running sessions of the command line interface
 vpn               manage VPN services
 debug             manage displaying syslog messages on the current console
 service           manage additional services
 firewall          firewall's objects commands
 mftp              manage MFTP daemon
 users             Manage local users
 alg               manage application-level gateway
 healthmond        control healthmond daemon

hostname# _
```

Левая колонка списка содержит первое слово группы команд, правая — краткое описание ее назначения.

В случае ввода символа ? в процессе набора команд, интерпретатор предложит вам варианты завершения текущего или следующего слова команды, в зависимости от положения курсора:

```
hostname> servi?

service manage additional services

hostname> service ?

http-proxy      manage HTTP proxy

cert            manage certificates

ips             manage IPS services

vpn             manage VPN services
```

```
dpi             manage DPI services
user-control    setup commands of user-control service
hostname> _
```

После информации о вариантах завершения команды отображается приглашение интерпретатора с ранее введенной командой для редактирования. Редактировать команды можно как обычно: стирать символы клавишей **Backspace** или **Delete**, перемещаться по тексту с помощью клавиш со стрелками влево и вправо.

Сочетания клавиш

Сочетание клавиш	Действие
Ctrl+U	стереть всю команду
Ctrl+K	стереть всё от курсора до конца строки
Ctrl+A	перейти в начало строки
Ctrl+E	перейти в конец строки
Ctrl+B	перейти на один символ назад
Ctrl+F	перейти на один символ вперед
Ctrl+H	стереть символ перед курсором
Ctrl+W	стереть слово перед курсором

Выбор консоли при локальном подключении

При локальном подключении к ViPNet Coordinator HW в качестве консоли вы можете использовать:

- Монитор и клавиатуру, подключаемые к портам VGA и PS/2.
- Компьютер, подключаемый к консольному порту (DB9 или RJ45). В этом случае используйте клиент удаленного доступа, например PuTTY, и задайте параметры подключения:
  - Terminal — VT100+.
  - Remote character set — KOI8-R.
  - Connection type — Serial:
    - Speed — 38400.
    - Data — 8.
    - Parity — None.
    - Stopbits — 1.
    - Flow Control — None.

Одновременно к ViPNet Coordinator HW можно подключить две консоли. В этом случае при каждом включении ViPNet Coordinator HW необходимо выбрать консоль для дальнейшей работы:

1. На обе консоли выводится приглашение нажать любую клавишу. Если в течение 10 секунд вы не нажмете клавишу ни на одной из консолей, то считается, что клавиша нажата на консоли монитора и клавиатуры.
2. На консоль, на которой нажата клавиша, выводится список возможных консолей и приглашение выбрать нужную. Если в течение 5 секунд вы не выберите консоль, то автоматически выбирается консоль монитора и клавиатуры.

Все последующие сообщения о загрузке и приглашение аутентификации будут выводиться на выбранной консоли.

Локальное подключение с помощью консоли

Выберите и настройте консоль (см. Выбор консоли при локальном подключении). В приглашении введите имя и пароль локального пользователя.

```
Product: ViPNet Coordinator HW

Platform: HW1000C

License: HW1000C

Software version: 5.4.0-5617

(C) 2025, JSC InfoTeCS

Website: www.infotecs.ru

Email: soft@infotecs.ru

Phone for Russia: 8 800 250-0-260

Phone for Moscow and international calls: +7 495 737-61-92

login as: admin

Password:

Last login: Tue Feb  8 13:27:12 MSK 2025 from 10.0.112.104 on tty1

Loading command shell, please wait...

Starting the command line interface of Platform: HW1000C
```



Примечание. Для предотвращения подбора пароля учетных записей реализована прогрессивная задержка ввода пароля, оповещение о попытках подбора пароля и временная блокировка учетной записи локального пользователя после 10 неудачных попыток ввода пароля. Количество таких попыток отображается при каждой успешной аутентификации в строке `Password guessing attempts registered`.

Если на ViPNet Coordinator HW истекают или уже истекли сроки действия ключей защиты, обмена или закрытого ключа сертификата пользователя (см. Настройка оповещения об истечении срока действия ключей), то на экран будет выведено оповещение, например, `WARNING: Your authentication key expire. Validity period < 7 day(s).`

Удаленное подключение по SSH

По умолчанию удаленное подключение к ViPNet Coordinator HW по SSH запрещено. Если вы не разрешили подключение при инициализации устройства, сделайте это сейчас (см. «Подготовка к работе», раздел «После инициализации»).

Удаленное подключение по SSH следует выполнять с узлов защищённой сети, связанных с ViPNet Coordinator HW.

Для защиты рабочего места установите средство антивирусной защиты.

Аутентификация может выполняться для:

- пользователей с локальными учётными записями;
- пользователей с централизованными учётными записями, созданными в ViPNet Prime — возможна только при наличии доступа ViPNet Coordinator HW к ViPNet Prime.

При использовании централизованной учётной записи в командном интерпретаторе необходимо использовать префикс `prime`, например `prime/admin`.

Для подключения вы можете использовать любой клиент удаленного доступа, поддерживающий SSH и аутентификацию по паролю, например, PuTTY:

1. Запустите PuTTY и в параметрах сессии укажите IP-адрес интерфейса ViPNet Coordinator HW, по которому выполняется подключение, TCP-порт 22, кодировку KOI8-R.
2. В приглашении введите имя и пароль пользователя.

```
login as: admin
Keyboard-interactive authentication prompts from server:
Password:
End of keyboard-interactive prompts from server
Last login: Thu Feb 10 11:48:21 MSK 2025 on tty1
Last login: Thu Feb 10 12:00:19 2025 from 10.0.113.72
Product: ViPNet Coordinator 1000
Platform: HW1000C
License: HW1000C
Software version: 5.4.0-6124
(C) 2026, JSC InfoTeCS
Website: www.infotecs.ru
Email: soft@infotecs.ru
Phone for Russia: 8 800 250-0-260
Phone for Moscow and international calls: +7 495 737-61-92
Loading command shell, please wait...
Starting the command line interface of Platform: HW1000C
```

Примечание. При удаленном подключении по SSH прогрессивная задержка ввода пароля, оповещения о попытках подбора пароля, временная блокировка учетной записи локального пользователя после 10-ти неудачных попыток ввода пароля и сроках действия ключей такие же, как и при локальном подключении с помощью консоли.



2

Настройка подключения к сети

Настройка сетевых интерфейсов Ethernet 29

Назначение дополнительных IP-адресов 31

Просмотр параметров сетевых интерфейсов 32

Подключение к мобильной сети 3G/4G 33

Настройка доступа через сеть мобильного оператора 36

Подключение к сети Wi-Fi 38

Просмотр настроек динамических интерфейсов 40

Изменение значения MTU для сетевых интерфейсов 41

Настройка обработки трафика из нескольких VLAN 42

Настройка агрегированных сетевых интерфейсов 44

Настройка получения параметров от DHCP-сервера 53

Настройка сетевых интерфейсов Ethernet

Внимание! Не изменяйте параметры сетевых интерфейсов, задействованных в работе кластера (см. Развертывание кластера). Это может вызвать сбои в его работе.

Сетевым интерфейсам Ethernet ViPNet Coordinator HW присваиваются имена `eth0`, `eth1` и так далее по количеству интерфейсов. Чтобы настроить подключение к сети, задайте параметры сетевых интерфейсов Ethernet:

1. Задайте класс интерфейса:

   ```
   hostname# inet ifconfig <имя интерфейса> class {access | trunk | slave}
   ```

   - По умолчанию назначен класс `access`.
   - Если требуется, чтобы данный интерфейс обрабатывал трафик из нескольких VLAN, назначьте ему класс `trunk`.
   - Если вы хотите объединить данный интерфейс с другими в составе агрегированного интерфейса, назначьте ему класс `slave`.

2. Присвойте интерфейсу IP-адрес одним из способов:

   - Чтобы включить на интерфейсе режим автоматического получения параметров от DHCP-сервера:

     ```
     hostname# inet ifconfig <имя интерфейса> dhcp
     ```

     Дополнительно см. Настройка получения параметров от DHCP-сервера.

     Внимание! IP-адрес, получаемый от DHCP-сервера, не должен принадлежать подсетям, в которые входят IP-адреса других интерфейсов ViPNet Coordinator HW.

   - Чтобы присвоить интерфейсу статический IP-адрес:

     ```
     hostname# inet ifconfig <имя интерфейса> address <IP-адрес> netmask <маска сети>
     ```

     Например, чтобы присвоить интерфейсу `eth1` IP-адрес 192.168.10.1 и маску подсети 255.255.255.0, выполните:

     ```
     hostname# inet ifconfig eth1 address 192.168.10.1 netmask 255.255.255.0
     ```

     Если до выполнения этой команды интерфейс работал в режиме DHCP, данные о DNS- и NTP-серверах, полученные по протоколу DHCP, будут потеряны.

     Примечание. При задании IP-адреса действуют ограничения:

     - нельзя задать IP-адрес 0.*.*.*;
     - нельзя задать маски подсети 0.0.0.0, 255.255.255.254 и 255.255.255.255;
     - для разных сетевых интерфейсов нельзя задать IP-адреса, относящиеся к одной подсети или широковещательному каналу (broadcast).

3 Включите сетевой интерфейс:

```
hostname# inet ifconfig <имя интерфейса> up
```

4 Если хотя бы на одном используемом интерфейсе Ethernet задано автоматическое получение маршрутов от DHCP-сервера, проверьте, что хотя бы один маршрут по умолчанию получен:

```
hostname# inet show routing
```

Если маршрут по умолчанию не был получен, задайте статический маршрут по умолчанию. Маршрут по умолчанию также необходимо задать при ручной настройке параметров интерфейса Ethernet.



Внимание! Убедитесь, что заданный в маршруте шлюз по умолчанию доступен для сетевого узла ViPNet Coordinator HW. Если шлюз по умолчанию окажется недоступен, многие функции ViPNet Coordinator HW не будут работать (например, виртуальные IP-адреса, обработка прикладных протоколов, сетевые службы и другие).

5 Выполните дополнительные настройки:

- Задайте дополнительные IP-адреса для сетевого интерфейса.
- Настройте маршрутизацию.
- Измените значение MTU для сетевого интерфейса.

6 При необходимости вы можете сбросить параметры сетевого интерфейса:

```
hostname# inet ifconfig <имя интерфейса> reset
```

Назначение дополнительных IP-адресов

С помощью дополнительных IP-адресов вы можете разделить сеть на логические подсети. Например, чтобы разрешить доступ в интернет только некоторым узлам, когда в остальной сети доступ закрыт.



Примечание. Максимальное количество сетевых интерфейсов определяется исполнением ViPNet Coordinator HW. Подробнее см. документ «Подготовка к работе», раздел «Функциональные ограничения исполнений».

Чтобы добавить дополнительный IP-адрес:

1 Проверьте, что на интерфейсе задан статический основной IP-адрес и класс `access`:

```
hostname# inet show interface <имя интерфейса>
```

В выводе команды:

- Назначен IP-адрес, например:

  `inet 192.168.0.1 netmask 255.255.255.0 broadcast 192.168.0.255`

- В строке `Configured by DHCP` значение `no`.
- В строке `Class` значение `access`.

Если на интерфейсе не настроен статический IP-адрес, выберите другой интерфейс или измените настройки (см. Настройка сетевых интерфейсов Ethernet).

2 Добавьте дополнительный IP-адрес:

```
hostname# inet ifconfig <имя интерфейса> address add <IP-адрес> netmask <маска подсети>
```

После выполнения команды создается виртуальный сетевой интерфейс с именем `<интерфейс>:номер`, где `номер` — очередной свободный номер (нумерация дополнительных IP-адресов начинается с 0). На созданном виртуальном интерфейсе задаются указанные IP-адрес и маска подсети.

Например, чтобы добавить на интерфейс `eth1` дополнительный IP-адрес 192.168.10.2 с маской подсети 255.255.255.0:

```
hostname# inet ifconfig eth1 address add 192.168.10.2 netmask 255.255.255.0
```

Будет создан виртуальный интерфейс `eth1:0` с IP-адресом 192.168.10.2 и маской подсети 255.255.255.0.

Просмотр параметров сетевых интерфейсов

Чтобы просмотреть параметры сетевого интерфейса:

```
hostname> inet show interface <имя интерфейса>
```

Если интерфейс не указан, отобразится информация обо всех сетевых интерфейсах.

На экран будет выведена информация:

- IP-адрес и маска подсети;
- MAC-адрес;
- настройки DHCP;
- класс и состояние интерфейса;
- параметры агрегированного интерфейса;
- другие параметры.

Подробное описание всех параметров см. в документе «Справочник команд и конфигурационных файлов».

Для просмотра параметров виртуального интерфейса:

```
hostname> inet show interface <имя интерфейса>.<номер>
```

Подключение к мобильной сети 3G/4G

Подключение к мобильной сети 3G/4G по протоколу PPP доступно на аппаратных платформах со встроенным модемом:

- HW50 A1 (если модем входит в комплект поставки);
- HW50 N3;
- HW100 N3.

До начала работы подключите необходимые услуги мобильного оператора и установите SIM-карту (см. документ «Подготовка к работе», раздел «Установка SIM-карты»).

При подключении к сети на ViPNet Coordinator HW, в зависимости от оператора, могут передаваться:

- маршрут по умолчанию в сеть оператора;
- адрес DNS-сервера оператора.

Чтобы настроит подключение к мобильной сети:

1 Выключите модем:

```
hostname# inet usb-modem mode off
```

2 В зависимости от маршрутизации в вашей сети настройте обработку маршрута по умолчанию и адреса DNS-сервера, передаваемых оператором:

2.1 Чтобы отказаться от получения маршрута по умолчанию:

```
hostname# inet usb-modem set route off
```

2.2 Чтобы изменить значение метрики маршрута по умолчанию:

```
hostname# inet usb-modem set route-metric <метрика>
```

Подробнее см. Настройка метрики для маршрутов PPP-протокола.

2.3 Чтобы отказаться от получения адреса DNS-сервера:

```
hostname# inet usb-modem set dns off
```

3 Задайте настройки подключения к сети вашего оператора:

- Настройки подключения к сетям МТС, Билайн, Мегафон или SkyLink предустановлены в ViPNet Coordinator HW, поэтому, если вы будете использовать услуги одного из этих операторов, выберите его:

  ```
  hostname# inet usb-modem set provider {mts | beeline | megafon | skylink}
  ```

- Если вы будете пользоваться услугами другого оператора, настройте параметры подключения:

  - Задайте имя нового оператора:

```
hostname# inet usb-modem add provider <имя оператора>
```

- Укажите IP-адрес или доменное имя сервера доступа:

  ```
  hostname# inet usb-modem set connection address {<IP-адрес> | <доменное имя>}
  ```

- Задайте номер доступа:

  ```
  hostname# inet usb-modem set phone <номер доступа>
  ```

- Укажите имя пользователя и пароль подключения, если вы используете авторизацию:

  ```
  hostname# inet usb-modem set user <имя пользователя>
  hostname# inet usb-modem set password <пароль>
  ```

- Выберите нового оператора для подключения:

  ```
  hostname# inet usb-modem set provider <имя оператора>
  ```

Например:

```
hostname# inet usb-modem add provider xtelecom
hostname# inet usb-modem set connection address internet.xtelecom.ru
hostname# inet usb-modem set phone *99***1#
hostname# inet usb-modem set user xtelecom
hostname# inet usb-modem set password xtelecom
hostname# inet usb-modem set pin 1234
hostname# inet usb-modem set provider xtelecom
```

4 Укажите PIN-код, если SIM-карта защищена:

```
hostname# inet usb-modem set pin <PIN-код>
```

Примечание. Вы можете отменить использование PIN-кода:
`hostname# inet usb-modem reset pin`

---

5 Проверьте текущие параметры подключения:

```
hostname# inet show usb-modem
```

6 Включите модем:

```
hostname# inet usb-modem mode on
```

Подключение может занять несколько минут.

7 Проверьте статус подключения:

```
hostname# inet show usb-modem
```

- Вывод команды при успешном подключении:

  ```
  3G/4G modem is found
  Cellular provider: MTS
  SIM card: OK
  PIN code: 1234
  PIN verification: OK
  3G/4G connection is enabled
  Use DHCP response information: gateway(yes) DNS(yes)
  ```

```
Route metric: default (70)
Connection interface: ppp0
```

- Если в выводе присутствуют сообщения о неверном PIN-коде или отсутствующей (поврежденной) SIM-карте, например:

  ```
  3G/4G modem is found
  Cellular provider: MTS
  SIM card: error
  PIN code: 1234
  PIN verification: failed
  ...
  ```

  выключите модем, устраните причину (вставьте или замените SIM-карту, задайте правильный PIN-код) и заново включите модем.

Настройка доступа через сеть мобильного оператора

Вы можете настроить доступ узлов защищённой сети и открытых узлов из внешней сети в сеть ViPNet через сеть мобильного оператора.

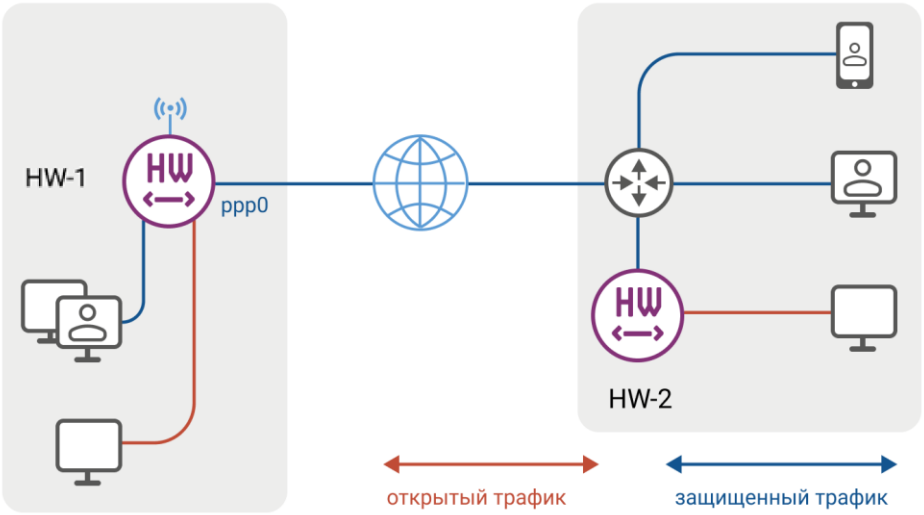


Рисунок 1. Использование модема для доступа через сеть мобильного оператора

1 Установите режим подключения к внешней сети «Со статической трансляцией адресов».

2 Выключите модем:

```
hostname# inet usb-modem mode off
```

3 Настройте подключение к сети оператора со статическим IP-адресом:

3.1 Добавьте нового оператора, например Билайн:

```
hostname# inet usb-modem add provider static-beeline
```

3.2 Задайте IP-адрес или доменное имя сервера доступа:

```
hostname# inet usb-modem set connection address static.beeline.ru
```

3.3 Задайте номер доступа:

```
hostname# inet usb-modem set phone *99#
```

3.4 Задайте имя и пароль пользователя:

```
hostname# inet usb-modem set user beeline
hostname# inet usb-modem set password beeline
```

3.5 Измените скрипт, используемый для подключения:

```
hostname# inet usb-modem modify chatscript
```

3.5.1 Замените строку:

```
OK AT+CGDCONT=1,"IP","\U"
```

на строку:

```
OK AT+CGDCONT=1,"IP","static.beeline.ru"
```

3.5.2 Сохраните изменения (**Ctrl+X**). Затем нажмите **y** и **Enter**.

3.6 Установите оператора `static-beeline` в качестве текущего:

```
hostname# inet usb-modem set provider static-beeline
```

3.7 Включите модем:

```
hostname# inet usb-modem mode on
```

3.8 Просмотрите полученный от оператора статический IP-адрес интерфейса `ppp0`:

```
hostname# inet show interface ppp0
...
inet <IP-адрес ppp0> netmask <маска подсети> destination <IP-адрес шлюза>
...
```

4 На HW-1 добавьте `<IP-адрес ppp0>` как адрес доступа:

```
hostname# iplir node ViPNetID HW-1 access-point add <IP-адрес ppp0>
```

5 На HW-2 задайте ViPNetID HW-1 в качестве сервера соединений:

```
hostname# iplir option connection-server ViPNetID HW-1
```

6 Настройте туннелирование открытых узлов (см. Ручная настройка туннелирования).

Подключение к сети Wi-Fi

Внимание!

- Подключение к сети Wi-Fi возможно только на аппаратных платформах HW50 N2 и HW100 N2.
- Адаптер Wi-Fi отображается как сетевой интерфейс `wlan0`.
- Не поддерживается подключение к сети Wi-Fi в кластере.
- Не поддерживается одновременное использование ViPNet Coordinator HW как клиента и точки доступа Wi-Fi.
- Все настройки подключения в сети Wi-Fi должны выполняться при выключенном сетевом интерфейсе Wi-Fi (wlan0). Если интерфейс включен, выключите его:

  ```
  hostname# inet wifi mode off
  ```

Чтобы подключить ViPNet Coordinator HW к сети Wi-Fi:

1. Проверьте параметры работы и текущие настройки адаптера Wi-Fi:

   ```
   hostname# inet show wifi
   ```

2. Переключите интерфейс Wi-Fi в режим клиента, если он работает в режиме точки доступа:

   ```
   hostname# inet wifi role client
   ```

3. Укажите параметры доступа к сети Wi-Fi, к которой вы хотите подключиться:

   Примечание. Список доступных сетей Wi-Fi (кроме скрытых) можно посмотреть командой:
   ```
   hostname# inet wifi scan
   ```

   - Если аутентификация в сети не требуется:

     ```
     hostname# inet wifi client authentication open
     ```

     Затем введите имя сети.

   - Если для аутентификации используется режим WPA-PSK или WPA2-PSK:

     ```
     hostname# inet wifi client authentication {wpa-psk | wpa2-psk}
     ```

     Затем введите имя сети и пароль.

4. Сетевой интерфейс `wlan0` работает в режиме автоматического получения параметров от DHCP-сервера, но вы можете настроить дополнительные параметры:

   - выключить автоматическое получение адресов DNS-серверов:

     ```
     hostname# inet ifconfig <имя интерфейса> dhcp dns off
     ```

   - выключить автоматическое получение NTP-серверов:

     ```
     hostname# inet ifconfig <имя интерфейса> dhcp ntp off
     ```

   - выключить автоматическое получение маршрутов от DHCP-сервера:

     ```
     hostname# inet ifconfig <имя интерфейса> dhcp route off
     ```

   - задать специфичное значение метрики для маршрутов, полученных от DHCP-сервера:

```
hostname# inet ifconfig <имя интерфейса> dhcp route-metric <1-255>
```

Вы можете задать ряд параметров, которые будут присваиваться маршрутам DHCP-сервера (см. Настройка маршрутов протоколов DHCP и PPP). Также вы можете просмотреть параметры режима DHCP на сетевых интерфейсах.

5 Включите сетевой интерфейс `wlan0`:

```
hostname# inet wifi mode on
```

6 Проверьте параметры подключения к сети Wi-Fi:

```
hostname# inet show wifi
```

Просмотр настроек динамических интерфейсов

При подключении к мобильной сети (см. Подключение к мобильной сети 3G/4G) или сети Wi-Fi (см. Подключение к сети Wi-Fi) на ViPNet Coordinator HW автоматически добавляются динамические интерфейсы, входящие в одну из групп:

- `ppp` — при подключении к мобильной сети через модем;
- `wifi` — при подключения к сети Wi-Fi.

Добавленные динамические интерфейсы активны и пропускают IP-трафик. Дополнительные настройки динамических интерфейсов, аналогичные настройкам статических интерфейсов, не требуются. Записи обо всех IP-пакетах, прошедших через динамические интерфейсы, регистрируются в журнале IP-пакетов.

Чтобы просмотреть настройку динамического интерфейса, например `ppp0`:

```
hostname# iplir show adapter ppp0

Adapter ppp0 in group ppp

Allow traffic = on

Type = external
```

Чтобы просмотреть список активных динамических интерфейсов:

```
hostname# iplir show adapters groups
```

Чтобы просмотреть список всех активных интерфейсов, включая динамические интерфейсы:

```
hostname# iplir show adapters

Active interface    Allowtraffic

eth0                on

eth1                on

eth2                on

ppp0 from ppp on
```

Изменение значения MTU для сетевых интерфейсов

По умолчанию для передачи данных через сетевой интерфейс используется размер MTU 1500 байт. Чтобы оптимизировать передачу данных через интерфейс, измените размер MTU:

```
hostname# inet ifconfig <имя интерфейса> mtu <значение MTU>
```

Значение MTU задается в байтах, допустимый диапазон значений — `1280–9000`. Чтобы вернуть значение MTU по умолчанию, в качестве значения MTU укажите `auto`.

При изменении значения MTU учитывайте:

- Значение MTU, заданное для интерфейса класса `trunk`, автоматически применяется ко всем виртуальным интерфейсам класса `vlan`, созданным на этом физическом интерфейсе. Изменять значения MTU для отдельных интерфейсов класса `vlan` нельзя.
- Значение MTU, заданное для агрегированного интерфейса, будет использоваться на всех подчиненных физических интерфейсах класса `slave`. Изменять значения MTU для отдельных интерфейсов класса `slave` нельзя. По умолчанию при создании агрегированного интерфейса для всех подчиненных физических интерфейсов автоматически задается значение MTU 1500 байт. Если вы исключаете подчиненный физический интерфейс из агрегированного, для исключенного интерфейса устанавливается значение MTU 1500 байт.
- В зависимости от платформы виртуализации, на которой развернуто исполнение ViPNet Coordinator VA, накладываются следующие ограничения:
    - VMware vSphere — для изменения MTU необходимо предварительно настроить платформу виртуализации, разрешив использование Jumbo-кадров.
    - Oracle VM VirtualBox — изменение MTU не поддерживается при использовании сетевых устройств AMD.

Особенности обработки транзитных IP-пакетов

Если MTU на входящем интерфейсе транзитного IP-пакета меньше, чем MTU на исходящем интерфейсе, то IP-пакет будет отправлен без изменений. Иначе IP-пакет будет фрагментирован в соответствии с MTU исходящего интерфейса.

Настройка обработки трафика из нескольких VLAN

Вы можете использовать ViPNet Coordinator HW для обработки трафика в физической локальной сети, разделённой на несколько независимых виртуальных локальных сетей — VLAN. Это возможно благодаря поддержке виртуальных сетевых интерфейсов и тегированию (маркировке) трафика в соответствии со стандартом IEEE 802.1Q. Каждой VLAN присваивается идентификатор из диапазона от 1 до 4094 (значения 0 и 4095 зарезервированы).

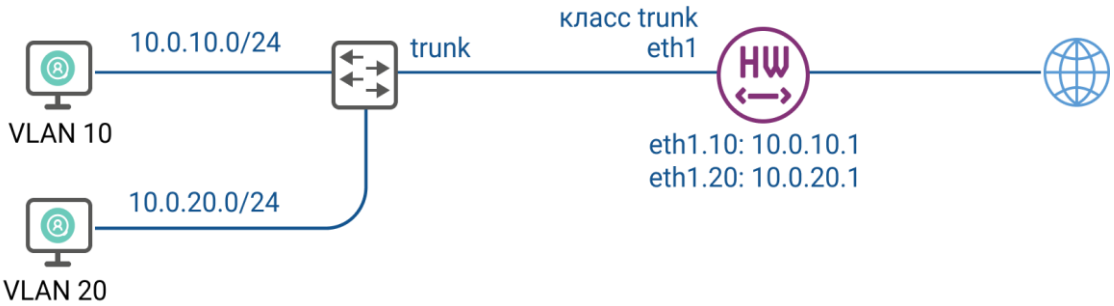


Рисунок 2. Обработка трафика из нескольких VLAN

Чтобы настроить обработку трафика из нескольких VLAN:

1. Подключите один из сетевых интерфейсов ViPNet Coordinator HW к коммутатору, объединяющему виртуальные сети.
2. Назначьте физическому интерфейсу класс `trunk`:

   ```
   hostname# inet ifconfig <имя физического интерфейса> class trunk
   ```

3. Создайте виртуальные интерфейсы, которые будут соответствовать виртуальным сетям за коммутатором:

   ```
   hostname# inet ifconfig <имя физического интерфейса> vlan add <номер виртуального интерфейса>
   ```

   Имя виртуального интерфейса — `<имя физического интерфейса.номер виртуального интерфейса>`, например, `eth1.10`. По умолчанию интерфейс пропускает трафик.

4. Добавьте виртуальные интерфейсы в конфигурационный файл `iplir.conf` и включите прохождение трафика:

   ```
   hostname# iplir adapter add <имя виртуального интерфейса> traffic on
   ```

   Чтобы позже запретить прохождение трафика, например для отладки:

   ```
   hostname# iplir adapter traffic <имя виртуального интерфейса> off
   ```

5. Задайте параметры виртуальных интерфейсов:

   - Включите на интерфейсе режим автоматического получения параметров от DHCP-сервера:

     ```
     hostname# inet ifconfig <имя виртуального интерфейса> dhcp
     ```

При необходимости задайте дополнительные параметры для режима DHCP (см. Настройка получения параметров от DHCP-сервера).

- Присвойте интерфейсу статический IP-адрес:

  ```
  hostname# inet ifconfig <имя виртуального интерфейса> address <IP-адрес> netmask <маска подсети>
  ```

  Если до выполнения этой команды интерфейс работал в режиме DHCP, данные о DNS- и NTP-серверах, полученные по протоколу DHCP, будут потеряны.

6 Включите физический интерфейс, к которому подключен коммутатор:

```
hostname# inet ifconfig <физический интерфейс> up
```

Настройка агрегированных сетевых интерфейсов

Чтобы увеличить пропускную способность сетевых интерфейсов ViPNet Coordinator HW или повысить надежность канала связи, вы можете объединить несколько физических сетевых интерфейсов в один логический — агрегированный сетевой интерфейс. При этом соответствующие каналы связи объединяются на канальном уровне сетевой модели OSI.

Например, если вам нужен канал связи с пропускной способностью выше 1 Гбит/с, а на вашем исполнении ViPNet Coordinator HW есть только гигабитные сетевые интерфейсы, вы можете объединить два или три из них в один агрегированный. При этом даже если один из объединенных интерфейсов выйдет из строя, агрегированный канал связи продолжит работать.

Кроме того, вы можете использовать агрегированный сетевой интерфейс только для резервирования канала связи, без увеличения его пропускной способности. В этом случае весь трафик будет передаваться через один из подчиненных физических интерфейсов, остальные же начинают работать только при его сбое.

Агрегированные каналы связи целесообразно использовать в отказоустойчивых сетях, по каналам которых передаются большие объемы данных, например, в сетях центров обработки данных.

Чтобы задать распределение нагрузки по подчиненным физическим интерфейсам, выберите один из режимов работы агрегированного интерфейса.



Внимание! Работоспособность агрегированных интерфейсов в ViPNet Coordinator VA не гарантируется. Если вам необходимо использовать агрегированный канал для ViPNet Coordinator VA, настройте его на платформе виртуализации.

Режимы работы агрегированного интерфейса

Таблица 1. Режимы работы агрегированного интерфейса

Режим	Описание
`balance-rr`	Подходит для балансировки нагрузки подчиненных физических интерфейсов и для защиты от сбоев. Применяется в сетях с простой топологией. Исходящие IP-пакеты, попадающие на агрегированный интерфейс, отправляются через подчиненные интерфейсы поочередно: первый пакет отправляется через один подчиненный интерфейс, второй пакет — через следующий подчиненный интерфейс и так далее.

`balance-xor`	Предназначен для защиты от сбоев и распределения нагрузки. IP-пакеты отправляются от отправителя к получателю всегда через один и тот же подчиненный интерфейс, для определения которого используется хэш-функция. Алгоритм вычисления хэш-функции можно задать: `inet ifconfig <имя агрегированного интерфейса> bonding xmit-hash-policy <алгоритм>` Вы можете задать один из алгоритмов: • `layer2` — используются MAC-адреса отправителя и получателя, одинаковыми считаются сетевые узлы с одинаковыми MAC-адресами; • `layer2+3` — используются MAC-адреса и IP-адреса отправителя и получателя, одинаковыми считаются сетевые узлы с одинаковыми MAC-адресами и IP-адресами; • `layer3+4` — используются IP-адреса отправителя и получателя, а также номера портов TCP и UDP (при наличии), одинаковыми считаются сетевые узлы с одинаковыми IP-адресами, а также портами TCP или UDP.
`balance-tlb`	Предназначен для балансировки нагрузки на подчиненных физических интерфейсах. Рекомендуется использовать при передаче большого числа IP-пакетов разного размера, когда режимы `balance-rr` и `balance-xor` не распределяют нагрузку равномерно. Ведется подсчет размера исходящих пакетов, переданных через каждый из подчиненных интерфейсов, и на основе этого выбирается интерфейс, через который будет передан пакет, попавший на агрегированный интерфейс. **Примечание.** Для работы агрегированного интерфейса в режиме `balance-tlb` необходимо, чтобы все подчиненные физические интерфейсы были подключены к сети через коммутатор.
`802.3ad`	Предназначен для балансировки нагрузки с использованием протокола LACP. Агрегированный интерфейс работает следующим образом: • Среди подчиненных однотипных физических интерфейсов формируются группы — «агрегаторы», скорость передачи данных на интерфейсах которых одинакова (например, группа гигабитных интерфейсов и группа 10-гигабитных интерфейсов). Параметры физических интерфейсов `mtu`, `duplex` и `autoneg`, объединяемых в группу, должны совпадать.

	• Активный агрегатор выбирается в соответствии с режимом выбора, задаваемым:
	`inet ifconfig <имя интерфейса> bonding ad-select <режим>`
	Вы можете выбрать один из режимов выбора:
	`stable` — первоначально выбирается агрегатор с наибольшей суммарной пропускной способностью подчиненных физических интерфейсов, а в дальнейшем выбор нового агрегатора выполняется только в случае сбоя всех подчиненных интерфейсов текущего агрегатора.
	`bandwidth` — первоначально выбирается агрегатор с наибольшей пропускной способностью подчиненных физических интерфейсов, а в дальнейшем, при добавлении, удалении или сбое подчиненных физических интерфейсов, в агрегаторах производится перегруппировка подчиненных физических интерфейсов и выполняется выбор нового агрегатора.
	`count` — первоначально выбирается агрегатор с наибольшим количеством подчиненных физических интерфейсов, а в дальнейшем, при добавлении, удалении или сбое подчиненных физических интерфейсов, в агрегаторах производится перегруппировка подчиненных физических интерфейсов и выполняется выбор нового агрегатора.
	• Внутри активного агрегатора подчиненный физический интерфейс, через который отправляются исходящие пакеты, выбирается аналогично режиму `balance-xor`.
	• С другим сетевым оборудованием происходит обмен LACPDU-пакетами с периодичностью, задаваемой:
	`inet ifconfig <имя интерфейса> bonding lacp-rate <slow | fast>`
	В случае выбора параметра `slow` обмен пакетами по протоколу LACP выполняется каждые 30 секунд, в случае выбора параметра `fast` — каждую секунду.
	Обмен пакетами позволяет определить сбой подчиненного интерфейса даже в том случае, если этот интерфейс подключен к другому сетевому узлу не напрямую.
	Примечание. Механизм MC-LAG (MLAG) не поддерживается, поэтому физические порты разных ViPNet Coordinator HW нельзя использовать в одном агрегированном интерфейсе.

`active-backup`	Предназначен для защиты от сбоев, но не для балансировки нагрузки на подчиненных физических интерфейсах. Один из подчиненных физических интерфейсов назначается основным (автоматически или явно с помощью команды `inet ifconfig bonding primary`), и все исходящие IP-пакеты отправляются через него. При этом, в случае сбоя на основном подчиненном интерфейсе пакеты будут отправляться через другие подчиненные интерфейсы.
`broadcast`	Предназначен для защиты от сбоев. IP-пакеты, попадающие на агрегированный интерфейс, отправляются через все подчиненные физические интерфейсы одновременно. **Примечание**. Режим `broadcast` требует настройки сетевого оборудования, предотвращающей дальнейшую передачу по сети нескольких копий пакетов. Если агрегированный канал работает в режиме `broadcast`, то организовать на нем защиту соединения по технологии L2OverIP невозможно.

Создание агрегированного интерфейса

1 Для физических интерфейсов, которые вы хотите объединить, установите класс `slave`:

```
hostname# inet ifconfig <имя интерфейса> class slave
```

2 Создайте агрегированный интерфейс:

```
hostname# inet bonding add <номер> mode <режим> slaves <интерфейс 1> [<интерфейс 2>] [<интерфейс N>]
```

, где:

- `<номер>` — номер агрегированного интерфейса. Возможные значения: 0, 1, 2, 3, 4, 5, 6, 7. Вы можете создать до восьми агрегированных интерфейсов с номерами с именами `bond<номер>`.
- `<режим>` — режим работы агрегированного интерфейса.
- `<интерфейс 1>`, `<интерфейс 2>`, `<интерфейс N>` — имена физических интерфейсов, подчиненных создаваемому агрегированному интерфейсу. При создании агрегированного интерфейса необходимо задать не менее одного подчиненного интерфейса. Ограничения на количество подчиненных интерфейсов в составе агрегированного интерфейса нет.

Вы можете добавлять или удалять подчиненные интерфейсы в любой момент времени:

- Добавить подчиненный интерфейс:

  ```
  hostname# inet ifconfig <агрегированный интерфейс> bonding add <имя подчиненного интерфейса>
  ```

- Удалить подчиненный интерфейс:

  ```
  hostname# inet ifconfig <агрегированный интерфейс> bonding delete <имя подчиненного интерфейса>
  ```

3 Добавьте агрегированный интерфейс в конфигурационный файл `iplir.conf` и включите прохождение трафика:

```
hostname# iplir adapter add <агрегированный интерфейс> traffic on
```

Чтобы позже запретить прохождение трафика, например для отладки:

```
hostname# iplir adapter traffic <агрегированный интерфейс> off
```

4 По умолчанию агрегированному интерфейсу назначается класс `access`. Чтобы интерфейс обрабатывал трафик из нескольких VLAN, назначьте ему класс `trunk`.

5 Измените значение MTU агрегированного интерфейса, если хотите оптимизировать передачу данных через него.

6 Задайте частоту проверки соединения на подчиненных интерфейсах. По умолчанию соединение на подчиненных физических интерфейсах проверяется каждые 0,1 секунды. Вы можете изменить это значение и задать частоту от 1 до 1000 миллисекунд:

```
hostname# inet ifconfig <агрегированный интерфейс> bonding miimon <частота в миллисекундах>,
```

где `<имя агрегированного интерфейса>` — `bond{0,1,2,3,4,5,6,7}`.

7 Настройте дополнительные параметры выбранного режима, например для режима `balance-xor` задайте алгоритм вычисления хэш-функции:

```
hostname# inet ifconfig <агрегированный интерфейс> bonding xmit-hash-policy layer2
```

8 Назначьте агрегированному интерфейсу динамический или статический IP-адрес:

- Включите на агрегированном интерфейсе режим автоматического получения параметров от DHCP-сервера:

  ```
  hostname# inet ifconfig <агрегированный интерфейс> dhcp
  ```

  Дополнительно см. Настройка получения параметров от DHCP-сервера.

- Назначьте агрегированному интерфейсу статический IP-адрес:

  ```
  hostname# inet ifconfig <агрегированный интерфейс> address <IP-адрес> netmask <маска подсети>
  ```

  Если до выполнения этой команды агрегированный интерфейс работал в режиме DHCP, данные о DNS- и NTP-серверах, полученные по протоколу DHCP, будут потеряны.

9 Последовательно включите все подчиненные физические интерфейсы:

```
hostname# inet ifconfig <подчиненный интерфейс> up
```

10 Включите агрегированный интерфейс:

```
hostname# inet ifconfig <агрегированный интерфейс> up
```

Чтобы изменить режим работы агрегированного интерфейса, удалите его, а затем создайте заново. При изменении параметров агрегированного интерфейса возможно кратковременное пропадание соединения (до 1 секунды).

Настройка агрегированного канала между HW и коммутатором

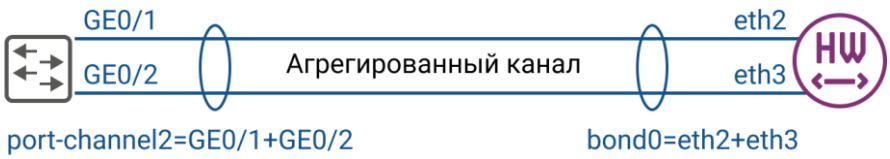


Рисунок 3. Агрегированный канал между ViPNet Coordinator HW и коммутатором

При передаче IP-пакетов от ViPNet-клиентов через коммутатор MAC-адрес, IP-адрес и порт сетевого узла отправителя не подменяется, поэтому следует использовать режимы, связанные с распределением нагрузки по MAC-адресам, IP-адресам и портам: `balance-xor`, `balance-tlb` и `802.3ad`.

В режиме `802.3ad` для определения подчиненного физического интерфейса, через который отправляется пакет, используется хэш-функция, поэтому пакеты от одного и того же отправителя к одному и тому же получателю всегда будут отправляться через один и тот же подчиненный физический интерфейс. Хэш-функция вычисляется по алгоритму `layer3+4`, поэтому учитываются IP-адреса и порты TCP или UDP отправителей и получателей.

Чтобы настроить агрегированный канал:

1. Установите для физических интерфейсов `eth2` и `eth3` класс `slave`:

   ```
   hostname# inet ifconfig eth2 class slave
   hostname# inet ifconfig eth3 class slave
   ```

2. Создайте агрегированный интерфейс с режимом работы `802.3ad`:

   ```
   hostname# inet bonding add 0 mode 802.3ad slaves eth2 eth3
   ```

3. Задайте алгоритм вычисления хэш-функции:

   ```
   hostname# inet ifconfig bond0 bonding xmit-hash-policy layer3+4
   ```

4. Добавьте агрегированный интерфейс в конфигурационный файл `iplir.conf` и включите прохождение трафика:

   ```
   hostname# iplir adapter add bond0 traffic on
   ```

   Чтобы позже запретить прохождение трафика, например для отладки:

   ```
   hostname# iplir adapter traffic bond0 off
   ```

5. Задайте IP-адрес агрегированного интерфейса:

   ```
   hostname# inet ifconfig bond0 address 10.10.10.1 netmask 255.255.255.0
   ```

6. Соедините интерфейсы `eth2` и `eth3` с интерфейсами коммутатора.

7. Последовательно включите все подчиненные физические интерфейсы:

   ```
   hostname# inet ifconfig eth2 up
   hostname# inet ifconfig eth3 up
   ```

8. Включите агрегированный сетевой интерфейс:

   ```
   hostname# inet ifconfig bond0 up
   ```

Чтобы настроить подключение к агрегированному каналу на коммутаторе, например Cisco Catalyst 2960-S:

1. Предварительно объедините интерфейсы коммутатора, к которым подключены ViPNet-клиенты, а также интерфейсы, которые будут подключены к агрегированному каналу, в виртуальную сеть, например VLAN 116.

2. Подключитесь к коммутатору и перейдите в режим администратора:

   ```
   switch> enable
   ```

3. Перейдите в режим настройки:

   ```
   switch# configure terminal
   ```

4. Создайте логический интерфейс `port-channel`, например с номером 2:

   ```
   interface Port-channel2
       switchport access vlan 116
       switchport mode access
   exit
   ```

5. Укажите физические интерфейсы, например `GigabitEthernet0/1` и `GigabitEthernet0/2`, которые будут входить в состав логического интерфейса `port-channel2`. Они будут использоваться для подключения к агрегированному каналу.

```
interface GigabitEthernet0/1
    switchport access vlan 116
    switchport mode access
    channel-group 2 mode active
exit
interface GigabitEthernet0/2
    switchport access vlan 116
    switchport mode access
    channel-group 2 mode active
exit
```

6 Настройте интерфейсы, к которым подключены ViPNet-клиенты:

```
interface GigabitEthernet<номер интерфейса>
    switchport access vlan <номер VLAN>
    switchport mode access
end
```

Теперь трафик между коммутатором и координатором будет идти по агрегированному каналу, состоящему из двух подчиненных физических каналов. В случае отказа одного из подчиненных каналов оставшийся продолжает работу и сессии с отказавшего канала перенаправляются на оставшийся.

Настройка агрегированного канала между двумя HW

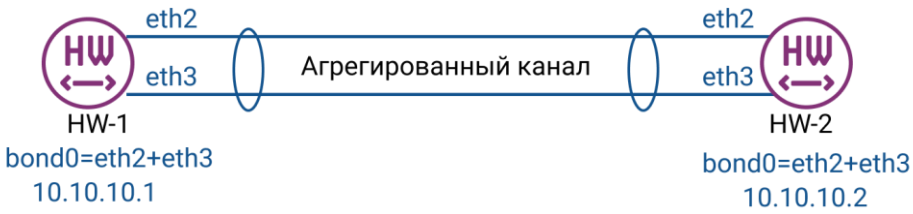


Рисунок 4. Агрегированный канал между двумя ViPNet Coordinator HW

При передаче IP-пакетов через ViPNet Coordinator HW MAC-адрес, порт и IP-адрес сетевого узла отправителя подменяются, поэтому следует использовать режимы `balance-rr`, `active-backup` и `broadcast`.

В режиме `balance-rr` исходящие пакеты, попадающие на агрегированный интерфейс, отправляются через подчиненные физические интерфейсы поочередно: первый пакет отправляется через один подчиненный интерфейс, второй пакет — через следующий подчиненный интерфейс и так далее. По агрегированному каналу будет отправляться как защищенный, так и открытый трафик.

Примечание. В режиме `balance-rr` может измениться порядок следования IP-пакетов, что приведет к искажению передачи некоторых типов трафика, например видео или звука.

Чтобы настроить агрегированный канал:

1 На обоих HW:

1.1 Установите для физических интерфейсов `eth2` и `eth3` класс `slave`:

```
hostname# inet ifconfig eth2 class slave
hostname# inet ifconfig eth3 class slave
```

1.2 Создайте агрегированный интерфейс с режимом работы `balance-rr`:

```
hostname# inet bonding add 0 mode balance-rr slaves eth2 eth3
```

1.3 Добавьте агрегированный интерфейс в конфигурационный файл `iplir.conf` и включите прохождение трафика:

```
hostname# iplir adapter add bond0 traffic on
```

Чтобы позже запретить прохождение трафика, например для отладки:

```
hostname# iplir adapter traffic bond0 off
```

2 Задайте IP-адреса агрегированных интерфейсов:

- На HW-1:

```
hostname# inet ifconfig bond0 address 10.10.10.1 netmask 255.255.255.0
```

- На HW-2:

  ```
  hostname# inet ifconfig bond0 address 10.10.10.2 netmask 255.255.255.0
  ```

3. Соедините интерфейс `eth2` HW-1 с интерфейсом `eth2` HW-2.
4. Соедините интерфейс `eth3` HW-1 с интерфейсом `eth3` HW-2.
5. На обоих HW:

   5.1. Последовательно включите подчиненные физические интерфейсы:

   ```
   hostname# inet ifconfig eth2 up
   hostname# inet ifconfig eth3 up
   ```

   5.2. Включите агрегированный интерфейс:

   ```
   hostname# inet ifconfig bond0 up
   ```

Теперь трафик между координаторами будет идти по агрегированному каналу, состоящему из двух подчиненных физических каналов. В случае отказа одного из подчиненных каналов оставшийся продолжает работу. При возобновлении работы подчиненного канала работа агрегированного канала продолжится в режиме `balance-rr`.

Настройка получения параметров от DHCP-сервера

Внимание!

Необходимо обеспечить доверенный канал передачи данных между ViPNet Coordinator HW и внешними системами (в том числе взаимодействующими системами защиты информации других типов), например выделенный физический канал или сеть ViPNet. Допускается осуществлять защиту каналов передачи данных организационными мерами, исключающими возможность утечки или перехвата защищаемых данных, или с помощью сертифицированных средств криптографической защиты информации.

При использовании режима автоматического получения параметров от DHCP-сервера сетевой интерфейс получает:

- собственный IP-адрес и маску подсети;
- IP-адреса DNS-серверов;
- IP-адреса NTP-серверов;
- маршруты.

Примечание. Отправка указанных параметров должна быть настроена на DHCP-сервере.

Вы можете отключить получение параметров от DHCP-сервера:

- Чтобы отключить получение IP-адресов DNS-серверов:

  ```
  hostname# inet ifconfig <имя интерфейса> dhcp dns off
  ```

- Чтобы отключить получение IP-адресов NTP-серверов:

  ```
  hostname# inet ifconfig <имя интерфейса> dhcp ntp off
  ```

- Чтобы отключить получение маршрутов:

  ```
  hostname# inet ifconfig <имя интерфейса> dhcp route off
  ```

Чтобы задать специфичное значение метрики для маршрутов, полученных от DHCP-сервера:

```
hostname# inet ifconfig <имя интерфейса> dhcp route-metric <1-255>
```

Подробнее см. в документе «Справочник команд и конфигурационных файлов».

Вы можете задать ряд параметров, которые будут присваиваться маршрутам DHCP-сервера (см. Настройка маршрутов протоколов DHCP и PPP). Чтобы просмотреть параметры, которые заданы для режима DHCP на всех сетевых интерфейсах, см. Просмотр настроек DHCP в режиме клиента.

3

Настройка VPN

Общие принципы настройки VPN 55

Настройка подключения к внешней сети 58

Просмотр сведений об узлах ViPNet 62

Настройка виртуальных IP-адресов 63

Настройка туннелирования на сетевом уровне 68

Настройка IP-адресов доступа к узлу и их приоритета 76

Настройка TCP-туннеля 79

Сценарии использования VPN 82

Настройка туннелирования на канальном уровне 83

Общие принципы настройки VPN

Начиная с версии ПО ViPNet Coordinator HW 5.3.0 часть параметров VPN может быть настроена как в конфигурационных файлах, так и с помощью команд. Подробнее об этих командах и их соответствии параметрам конфигурационных файлов см. в разделе Команды настройки iplir.conf.

Вы можете выполнить следующие настройки VPN:

- Настройка подключения к внешней сети.
- Настройка виртуальных IP-адресов.
- Настройка туннелирования на сетевом уровне.
- Настройка туннелирования на канальном уровне.

Команды настройки iplir.conf

Примечание. При выполнении команд из группы `iplir option` изменение параметров в файле `iplir.conf` происходит с задержкой 60 сек.

Таблица 2. Команды настройки параметров секции [adapter]

Параметр	Описание параметра	Команда
type	Тип интерфейса относительно сети ViPNet: внутренний или внешний	inet ifconfig type

Таблица 3. Команды настройки параметров секции [debug]

Параметр	Описание параметра	Команда
debuglevel	Уровень важности событий, регистрируемых в системном журнале	iplir option syslog-level

Таблица 4. Команды настройки параметров секции [dynamic]

Параметр	Описание параметра	Команда
forward_id	Идентификатор сервера соединений	iplir option connection-server
timeout	Период отправки IP-пакетов серверу соединений для поддержания активности соединения	iplir option keepalive-timeout

Таблица 5. Команды настройки параметров секции [id]

Параметр	Описание параметра	Команда
accessiplist	Параметры доступа к узлу ViPNet: IP-адрес, порт, метрика	iplir node access-point
avail_mon	Проверка доступности узла ViPNet: включена или выключена	iplir node availability-monitoring
blockforward	Блокирование транзитных IP-пакетов: включено или выключено	iplir node blockforward
fqdn	Доменное имя узла ViPNet	iplir node domain-name
fixfirewall	Режим подключения ViPNet Coordinator HW к VPN-сети: статический или динамический	iplir option mode
proxyid	Идентификатор сервера соединений в динамическом режиме	iplir option connection-server

Таблица 6. Команды настройки параметров секции [misc]

Параметр	Описание параметра	Команда
be_dg_coordinator	Обнаружение ViPNet Coordinator HW другими координаторами в качестве шлюза по умолчанию	iplir option be-default-gateway
client_pollinterval	Период опроса ViPNet-клиентов	iplir option ping-timeout
mssdecrease	Количество байт, на которое будет уменьшен максимальный размер TCP-сегмента (MSS)	iplir option mss-decrease
timediff	Максимально допустимое расхождение времени между отправкой и приемом IP-пакетов	iplir option maxtimediff
timesync	Синхронизация времени на ViPNet Coordinator HW в со временем на сервере IP-адресов: включена или выключена	iplir option sync-time
udp_ports_count	Количество портов UDP	iplir option udp-ports-count

Таблица 7. Команды просмотра параметров

Команда	Параметры
inet show interface state	Секция [adapter]
iplir option show	Секции [debug] и [dynamic]
iplir node show	Секция [id]

Команда	Параметры
iplir node list	Список идентификаторов узлов
iplir option show	Секция [misc]

Настройка подключения к внешней сети

Режим подключения ViPNet Coordinator HW к внешней сети зависит от особенностей настройки оборудования провайдера, обеспечивающего доступ в интернет, и топологии вашей сети. Выберите и настройте один из режимов:

1. Режим «Со статической трансляцией адресов» применяется:
   - при подключении через устройство Static NAT;
   - при подключении напрямую.
2. Режим «С динамической трансляцией адресов» применяется:
   - при подключении через устройство Dynamic NAT с возможностью работы только через сервер соединений;
   - при каскадном подключении ViPNet Coordinator HW.

Режим «Со статической трансляцией адресов»

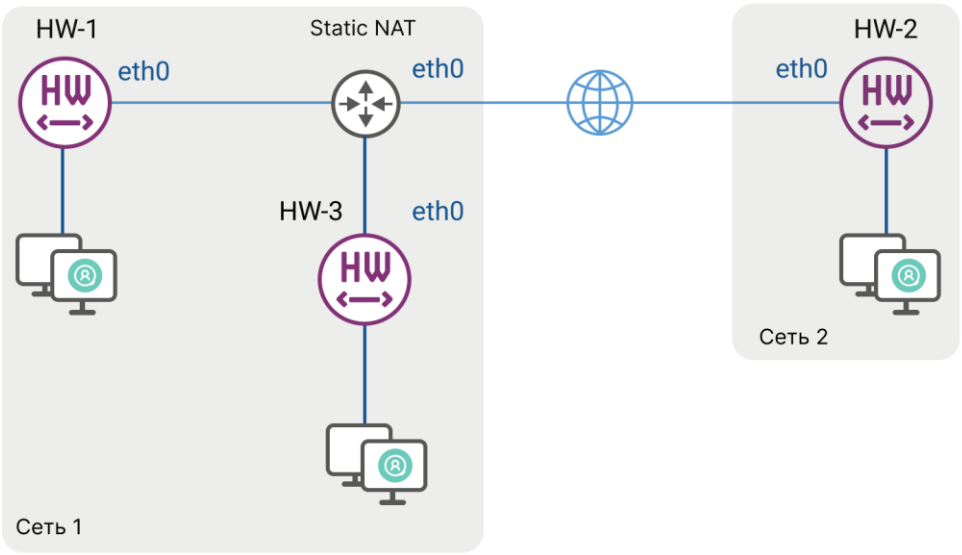


Рисунок 5. Режим «Со статической трансляцией адресов». подключение через устройство Static NAT и напрямую

1. Настройте HW-1 (подключение через Static NAT):

   1.1 Задайте режим «Со статической трансляцией адресов»:

   ```
   hostname# iplir option mode static
   ```

1.2 По умолчанию в этом режиме используется диапазон из 255-ти портов UDP: 55777–56031. Начальный порт диапазона вы можете изменить в ViPNet Prime или в секции файла `iplir.conf` (параметр `port` собственной секции `[id]`). Также вы можете изменить количество портов в диапазоне с помощью команды `iplir option udp-ports-count`.

2 Для узлов ViPNet сети 1, расположенных за HW-1, задайте ViPNetID HW-1 в качестве сервера соединений.

3 Настройте HW-2 (подключение напрямую):

3.1 Задайте публичный IP-адрес интерфейса `eth0`:

```
hostname# inet ifconfig eth0 address <IP-адрес> netmask <маска>
```

3.2 Настройте маршрутизацию к устройству Static NAT:

3.3 Задайте режим «Со статической трансляцией адресов»:

```
hostname# iplir option mode static
```

3.4 Настройте диапазон портов UDP как на шаге 1.2 сценария.

4 Для узлов ViPNet сети 2, задайте ViPNetID HW-2 в качестве сервера соединений.

5 На устройстве Static NAT задайте правила трансляции адресов:

5.1 пропускать UDP-пакеты с трансляцией адреса источника на IP-адрес интерфейса `eth0` устройства Static NAT:

- адрес источника: IP-адрес доступа HW-1;
- порт источника: диапазон портов UDP HW-1;
- адрес назначения: любой;
- порт назначения: любой;

5.2 пропускать UDP-пакеты с трансляцией адреса назначения на IP-адрес и порт HW-1:

- адрес источника: любой;
- порт источника: любой;
- адрес назначения: IP-адрес интерфейса `eth0` устройства Static NAT;
- порт назначения: начальный порт диапазона портов UDP HW-2.

Если через устройство Static NAT к внешней сети подключается еще один координатор — HW-3:

1 Настройте для него диапазона портов UDP, в котором начальный порт не входит в диапазон портов UDP HW-1, как на шагах 1.1 и 1.2.

2 На устройстве Static NAT добавьте правила трансляции адресов:

2.1 пропускать UDP-пакеты с трансляцией адреса источника на IP-адрес интерфейса `eth0` устройства Static NAT:

- адрес источника: IP-адрес доступа HW-3;
- порт источника: диапазон портов UDP HW-3;
- адрес назначения: любой;

- порт назначения: любой;

2.2 пропускать UDP-пакеты с трансляцией адреса назначения на IP-адрес и порт HW-3:

- адрес источника: любой;
- порт источника: любой;
- адрес назначения: IP-адрес интерфейса `eth0` устройства Static NAT;
- порт назначения: начальный порт диапазона портов UDP HW-2.

Режим «С динамической трансляцией адресов»

Подключение через Dynamic NAT

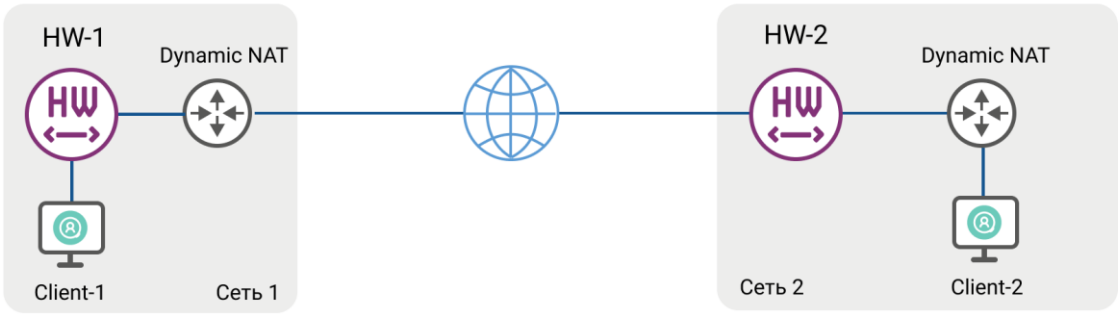


Рисунок 6. Режим «С динамической трансляцией адресов». установка соединения через сервер соединений

Для работы HW-1 сети 1 в режиме «С динамической трансляцией адресов» необходим постоянно доступный сервер соединений — HW-2 сети 2, работающий в режиме «Со статической трансляцией адресов». Соединение между узлами Client-1 и Client-2 устанавливается через сервер соединений. Для поддержки соединения HW-1 периодически отправляет IP-пакеты на сервер соединений HW-2.

Примечание. Период отправки таких IP-пакетов по умолчанию составляет 25 секунд. Этого достаточно для работы через большинство устройств Dynamic NAT. При необходимости вы можете изменить этот период с помощью команды `iplir option keepalive-timeout`.

Чтобы настроить подключение:

1 На HW-1 задайте режим «С динамической трансляцией адресов» и укажите ViPNetID HW-2 в качестве сервера соединений:

```
hostname# iplir option mode dynamic ViPNetID HW-2
```

2 Для узла Client-1 задайте ViPNetID HW-1 в качестве сервера соединений.

3 На HW-2 задайте режим «Со статической трансляцией адресов»:

```
hostname# iplir option mode static
```

4 Для узла Client-2 задайте ViPNetID HW-2 в качестве сервера соединений.

Каскадное подключение

Чтобы защитить трафик внутреннего сегмента локальной сети, используйте каскадное подключение координатора HW-2, которое обеспечивает автоматическую маршрутизацию защищенного трафика из внутреннего сегмента сети как в локальную, так и в глобальную сеть.

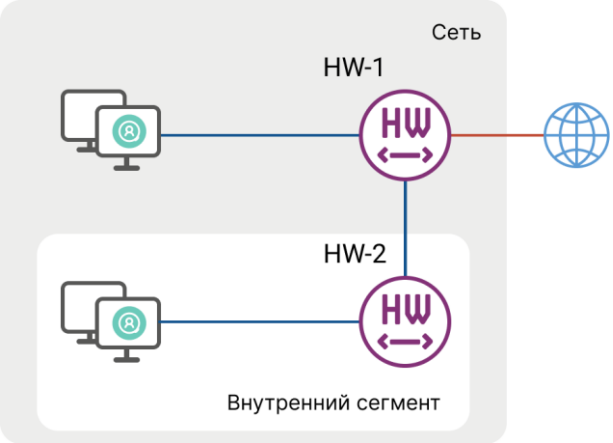


Рисунок 7. Каскадное подключение ViPNet Coordinator HW

Чтобы настроить каскадное подключение HW-2 через HW-1, задайте на нем режим «С динамической трансляцией адресов» и укажите ViPNetID HW-1 в качестве сервера соединений:

```
hostname# iplir option mode dynamic ViPNetID HW-1
```

Просмотр сведений об узлах ViPNet

Вы можете просмотреть сведения об узлах ViPNet, для которых с вашим узлом установлены связи:

1. Просмотрите список таких узлов ViPNet:

   ```
   hostname# iplir node list
   ```

2. Проверьте соединение с узлом ViPNet, сведения о котором вы хотите просмотреть, по его идентификатору (`ViPNetID`):

   ```
   hostname# iplir ping ViPNetID
   ```

   Внимание! Если статус координатора ViPNet отображается некорректно, проверьте параметр `server_pollinterval` в секции `[misc]` файла `iplir.conf`. Значение параметра должно быть одинаковым для всех координаторов сети.

3. Просмотрите сведения об этом узле:

   ```
   hostname# iplir node ViPNetID show
   ```

Чтобы просмотреть сведения о собственном узле ViPNet, выполните команду:

```
hostname# iplir option show
```

Настройка виртуальных IP-адресов

Общие сведения о виртуальных IP-адресах

При подключении удаленных пользователей к ресурсам локальной сети, а также при организации взаимодействия локальных сетей с помощью VPN может возникать конфликт IP-адресов: два сетевых узла, находящиеся в разных сетях, имеют одинаковые частные IP-адреса. Использование виртуальных IP-адресов позволяет решить эту проблему без изменения текущего адресного пространства сетей.

Каждый узел сети ViPNet при получении справочников автоматически назначает виртуальные IP-адреса для доступа ко всем узлам защищённой сети, с которыми у него имеется связь. Если среди них есть координаторы, виртуальные IP-адреса назначаются также для всех узлов, которые эти координаторы туннелируют. Каждому реальному IP-адресу узла ставится в соответствие виртуальный IP-адрес. В результате каждый узел защищённой сети имеет собственный список виртуальных IP-адресов для доступа к узлам сети ViPNet.

Приложения на узле защищённой сети могут использовать виртуальные IP-адреса для соединения с другими узлами. При отправке IP-пакета ViPNet-драйвер узла защищённой сети подменяет виртуальный IP-адрес получателя на реальный и отправляет адресату. В момент приема ответного IP-пакета из сети ViPNet-драйвер передает его приложению после подмены реального IP-адреса отправителя на виртуальный. Это происходит только в случае успешной расшифровки IP-пакета с помощью ключей отправителя, что обеспечивает защиту от подмены адреса отправителя.

Виртуальные IP-адреса для узлов защищённой сети закрепляются за уникальными идентификаторами узлов ViPNet. Виртуальные IP-адреса для туннелируемых узлов закрепляются за реальными IP-адресами.

При добавлении новых связей с узлами защищённой сети, а также новых реальных IP-адресов для узлов, с которыми уже существует связь, узел защищённой сети присваивает им свободные виртуальные IP-адреса из используемого диапазона виртуальных адресов. При удалении связей между узлами или удалении реальных IP-адресов, виртуальные IP-адреса освобождаются и могут использоваться повторно. Виртуальные IP-адреса, выделенные для туннелируемых узлов, могут измениться при добавлении новых IP-адресов туннелируемых узлов.

Если узел защищённой сети имеет несколько сетевых интерфейсов или несколько IP-адресов на интерфейсе, то виртуальные адреса для них назначаются по правилу: для каждого следующего IP-адреса второй октет виртуального адреса увеличивается на единицу, начиная с нуля, например 11.**0**.0.1, 11.**1**.0.1, 11.**2**.0.1 и далее.

Настройка диапазонов виртуальных IP-адресов

По умолчанию ViPNet Coordinator HW назначает виртуальные IP-адреса из двух диапазонов IP-адресов:

- узлам защищённой сети и одиночным туннелируемым узлам — из диапазона 11.0.0.1/8;

  Примечание. Одиночный туннелируемый узел — это узел, IP-адрес которого явно, а не в составе диапазона IP-адресов, указан в настройках туннелирования координатора.

- туннелируемым узлам (туннелям) — из диапазона 12.0.0.1/8.

Вы можете изменить диапазоны IP-адресов, заданные по умолчанию:

Внимание! При изменении диапазона все виртуальные IP-адреса на ViPNet Coordinator HW будут назначены заново.

1 Завершите работу управляющей службы:

```
hostname# iplir stop
```

2 Откройте файл `iplir.conf` для редактирования:

```
hostname# iplir config
```

3 В секции `[virtualip]` задайте диапазон IP-адресов для формирования виртуальных IP-адресов узлов защищённой сети и одиночных туннелируемых узлов одним из следующих способов:

   - Задайте начальный и конечный IP-адреса диапазона виртуальных IP-адресов в параметрах `startvirtualip` и `maxvirtualip`. Последний октет IP-адресов не должен быть равен 0. При этом `maxvirtualip` должен быть больше `startvirtualip`.
   - Задайте начальный IP-адрес диапазона виртуальных IP-адресов в параметре `startvirtualip`. Значение должно быть меньше 11.0.255.254 (так как начальный IP-адрес 12.0.0.1 задан по умолчанию для формирования виртуальных IP-адресов туннелей). При этом значение параметра `maxvirtualip` останется равным 11.0.255.254. Если значение `startvirtualip` задать в виде `x.0.0.1`, то параметру `maxvirtualip` будет автоматически присвоено значение `x.255.255.254`.
   - Задайте начальный IP-адрес диапазона виртуальных IP-адресов с маской подсети в параметре `startvirtualip` (допустимые маски подсети — /8 или /16, например: `startvirtualip = 11.0.0.1/8`). При этом не присваивайте значение параметру `maxvirtualip`, и сам параметр не будет использоваться в конфигурационном файле, а диапазон виртуальных IP-адресов будет ограничен IP-адресом, указанным в параметре `startvirtualip` с маской подсети /16 (пример: `11.0.0.1/16`).

     Внимание! Чтобы избежать ошибок при назначении начальных IP-адресов для генератора виртуальных IP-адресов, следует учитывать:

     - Значение первого октета должно быть в диапазоне 1–239.
     - Значение второго и третьего октетов должно быть в диапазоне 0–255.
     - Значение четвертого октета должно быть в диапазоне 1–254.

4 Начальный IP-адрес для формирования диапазонов виртуальных IP-адресов туннелируемых узлов задается автоматически: `starttunnelvirtualip = <x>.0.0.1`, где `x` больше первого октета `startvirtualip` на 1. Вы можете задать его вручную. Для этого введите значение в параметр `starttunnelvirtualip`. При этом первый октет должен быть больше первого октета `startvirtualip` и не должен быть равен 0, 127, 224-239, 255.

5 Сохраните изменения (**Ctrl+O**) и закройте редактор (**Ctrl+X**).

6 Запустите управляющую службу:

```
hostname# iplir start
```

Следует учитывать, что любой диапазон виртуальных IP-адресов, как по умолчанию, так и заданный вручную, будет пересекаться с одним из диапазонов реальных IP-адресов интернета. Поэтому при взаимодействии узла с открытыми ресурсами интернета может возникнуть конфликт, если у открытого ресурса IP-адрес совпадет с виртуальным IP-адресом одного из узлов сети ViPNet. Соединение с таким открытым ресурсом будет невозможно. В этом случае доступ к этому ресурсу можно настроить одним из способов:

- сменить диапазон виртуальных IP-адресов;
- работать с ресурсом через прокси-сервер.

При этом работать с узлами защищённой сети через прокси-сервер нельзя. Поэтому при использовании прокси-сервера требуется указать IP-адреса узлов защищённой сети в качестве исключений.

Настройка видимости узлов

В настройках ViPNet Coordinator HW вы можете задать видимость узлов защищённой сети и узлов, туннелируемых другим координатором, по реальным или виртуальным IP-адресам. При этом узлы, туннелируемые ViPNet Coordinator HW, будут подключаться к узлам защищённой сети и туннелируемым узлам других координаторов по тем же IP-адресам, что и ViPNet Coordinator HW. Например, если в настройках ViPNet Coordinator HW задано использование виртуальных IP-адресов для подключения к определенным узлам защищённой сети, то узлы, туннелируемые этим ViPNet Coordinator HW, также будут подключаться к ним по виртуальным IP-адресам.



Внимание! При использовании видимости по виртуальным IP-адресам на ViPNet Coordinator HW необходимо задать валидный маршрут по умолчанию. Вы могли задать такой маршрут при инициализации ViPNet Coordinator HW (см. документ «Подготовка к работе», раздел «После инициализации», шаг 6 сценария). Если вы обновили ПО ViPNet Coordinator HW, проверьте маршрут по умолчанию.

По умолчанию на ViPNet Coordinator HW используются следующие настройки видимости:

- узлы ViPNet, находящиеся в одном и том же широковещательном сегменте, доступны по виртуальным IP-адресам;
- туннелируемые узлы (узлы, туннелируемые другими координаторами) доступны по реальным IP-адресам;

- остальные узлы сети ViPNet доступны по виртуальным IP-адресам.

Видимость каждого узла ViPNet определяется с помощью параметров файла `iplir.conf` следующим образом:

1. Если в секции `[id]` узла присутствует параметр `visibility`, то видимость узла определяется значением этого параметра.
2. Если в секции `[id]` узла нет параметра `visibility`, но при этом сеть, которой принадлежит узел, указана в параметре `subnet_real` или `subnet_virtual` секции `[visibility]`, то видимость узла определяется значением этого параметра.
3. В иных случаях видимость узла определяется значением параметра `default` секции `[visibility]`.

То есть индивидуальные настройки видимости узлов приоритетнее настроек видимости сетей, а настройки видимости сетей приоритетнее настроек видимости по умолчанию.

Видимость туннелируемых узлов определяется с помощью параметров файла `iplir.conf` следующим образом:

1. Если в секции `[id]`, которая относится к туннелирующему координатору, присутствует параметр `tunnelvisibility`, то видимость туннелируемых узлов определяется значением этого параметра.
2. Если в секции `[id]`, которая относится к туннелирующему координатору, нет параметра `tunnelvisibility`, то видимость туннелируемых узлов определяется значением параметра `tunneldefault` секции `[visibility]`.

Настройка видимости узлов ViPNet

1. Завершите работу управляющей службы:

   ```
   hostname# iplir stop
   ```

2. Откройте файл `iplir.conf` для редактирования:

   ```
   hostname# iplir config
   ```

3. Чтобы настроить параметры видимости узлов защищённой сети по умолчанию и параметры видимости сетей ViPNet, в секции `[visibility]`:
   - установите параметр `default` в одно из значений:
     - `real` — для доступа к узлам используются их реальные IP-адреса;
     - `virtual` — для доступа к узлам используются их виртуальные IP-адреса.
   - при необходимости укажите идентификаторы вашей сети ViPNet и доверенных сетей в одном из параметров:
     - `subnet_real` — идентификаторы сетей ViPNet, для которых необходимо настроить видимость узлов по реальным IP-адресам;
     - `subnet_virtual` — идентификаторы сетей ViPNet, для которых необходимо настроить видимость узлов по виртуальным IP-адресам.

     Вы можете указать один либо несколько идентификаторов через запятую.

4 Чтобы настроить параметры видимости отдельных узлов защищённой сети, в соответствующих секциях `[id]` параметр `visibility` установите в одно из значений:

- `real` — всегда обращаться к узлу по его реальному адресу;
- `virtual` — всегда обращаться к узлу по его виртуальному адресу.



Внимание! До изменения видимости узла защищённой сети, не находящегося с ViPNet Coordinator HW в одном широковещательном сегменте, с виртуальной на реальную, выполните команду `inet ping` на виртуальный IP-адрес этого узла. Иначе после изменения видимости доступ к узлу по реальному IP-адресу будет отсутствовать.

До изменения видимости сети ViPNet с виртуальной на реальную, для каждого узла защищённой сети, не находящегося с ViPNet Coordinator HW в одном широковещательном сегменте, выполните команду `inet ping` на виртуальный IP-адрес этого узла. Иначе после изменения видимости сети ViPNet доступ к узлам по реальному IP-адресу, на которые не была выполнена команда `inet ping`, будет отсутствовать.

5 Сохраните изменения (**Ctrl+O**) и закройте редактор (**Ctrl+X**).

6 Запустите управляющую службу:

```
hostname# iplir start
```

Настройка видимости туннелируемых узлов

1 Завершите работу управляющей службы:

```
hostname# iplir stop
```

2 Откройте файл `iplir.conf` для редактирования:

```
hostname# iplir config
```

3 Чтобы настроить параметры видимости туннелируемых узлов по умолчанию, в секции `[visibility]` установите параметр `tunneldefault` в одно из значений:

- `real` — для доступа к туннелируемым узлам используются их реальные IP-адреса.
- `virtual` — для доступа к туннелируемым узлам используются их виртуальные IP-адреса.

4 Чтобы настроить параметры видимости туннелируемых узлов, в секциях `[id]`, которые относятся к туннелирующим координаторам, в параметре `tunnelvisibility` установите одно из значений:

- `real` — всегда обращаться к туннелируемым узлам по их реальным адресам.
- `virtual` — всегда обращаться к туннелируемым узлам по их виртуальным адресам.

5 Сохраните изменения (**Ctrl+O**) и закройте редактор (**Ctrl+X**).

6 Запустите управляющую службу:

```
hostname# iplir start
```

Настройка туннелирования на сетевом уровне

Общие сведения о туннелировании

Туннелирование применяется для защиты IP-трафика на потенциально опасном участке сети и для доступа к открытому узлу. Туннелирование предполагает направление IP-трафика узла не напрямую на другой узел, а через координатор, где трафик фильтруется и защищается криптографическими методами. Также настройки туннелирования открытых узлов, которые задает администратор сети ViPNet, хранятся на координаторах сети ViPNet, выполняющих туннелирование этих узлов.

Узлы, которые будут туннелироваться координатором, задаются в ViPNet Prime (см. документ «ViPNet Prime. Руководство администратора», раздел «Создание туннелируемых адресов ресурсов»). Эта информация автоматически передаётся на узлы защищённой сети в составе справочников. Для взаимодействия между узлом защищённой сети и туннелируемым узлом, а также между двумя туннелируемыми узлами, необходимо создать связи между ними в ViPNet Prime.

Если ViPNet Coordinator HW работает в условиях отсутствия связи с ViPNet Prime, вы можете настроить туннелирование локально на ViPNet Coordinator HW (см. Ручная настройка туннелирования). Затем IP-адреса туннелируемых узлов необходимо задать вручную на каждом связанном координаторе.

Если настройки туннелирования были заданы вручную, а затем поступили настройки из ViPNet Prime, выполняется их слияние:

- если с настройками туннелирования из ViPNet Prime получены новые IP-адреса туннелируемых узлов, то они добавляются в ViPNet Coordinator HW;
- если заданные локально IP-адреса туннелируемых узлов были удалены из настроек туннелирования, полученных из ViPNet Prime, то эти IP-адреса будут удалены.

После изменения настроек туннелирования может возникнуть конфликт между реальными IP-адресами узлов из широковещательного сегмента вашего ViPNet Coordinator HW и реальными IP-адресами узлов, туннелируемых удаленным координатором, или между реальными IP-адресами туннелируемых узлов. Чтобы устранить возможные конфликты, на координаторе, туннелирующем узлы с конфликтующими IP-адресами, задайте видимость туннелируемых узлов по виртуальным IP-адресам (см. Настройка видимости узлов).

Ручная настройка туннелирования

Примечание. Настраивайте туннелирование на координаторе только когда централизованная настройка туннелирования в ViPNet Prime не используется, иначе настройки на координаторе могут быть заменены настройками из ViPNet Prime.

Чтобы настроить туннелирование для открытых узлов, подключенных к ViPNet Coordinator HW, или настроить доступ к туннелируемым узлам удаленного координатора:

1 Завершите работу управляющей службы:

```
hostname# iplir stop
```

2 Откройте конфигурационный файл `iplir.conf` для редактирования:

```
hostname# iplir config
```

3 Выберите режим задания виртуальных IP-адресов для туннелируемых узлов. Для этого в секции `[misc]` установите параметр `tunnel_virt_assignment` в одно из значений:

- `auto` (по умолчанию) — при задании реальных IP-адресов туннелируемых узлов виртуальные IP-адреса для них назначаются автоматически.

  Внимание! Если все возможные адреса из диапазонов виртуальных IP-адресов для туннелируемых узлов заняты, то следующим узлам в качестве виртуальных копируются реальные адреса. При этом режим назначения принудительно переключается в ручной (`manual`).

- `manual` — виртуальные IP-адреса для туннелируемых узлов задаются вручную. При этом реальные IP-адреса туннелируемых узлов могут быть заданы как вручную, так и получены из ViPNet Prime.

4 Для туннелирования открытых узлов, подключенных к ViPNet Coordinator HW, в собственной секции `[id]` (первая секция) измените значение параметра `tunnel`:

- при автоматическом режиме задания виртуальных IP-адресов (см. предыдущий шаг):

  ```
  tunnel = <ip1>-<ip2>
  ```

  где, `<ip1>-<ip2>` — диапазон реальных IP-адресов туннелируемых узлов (начальный и конечный IP-адреса диапазона).

  Виртуальные IP-адреса для заданного диапазона будут сформированы автоматически.

  Например, чтобы ViPNet Coordinator HW туннелировал IP-адреса с 192.168.201.5 по 192.168.201.10, а виртуальные IP-адреса для этого диапазона были назначены автоматически, задайте:

  ```
  tunnel= 192.168.201.5-192.168.201.10
  ```

- при ручном режиме задания виртуальных IP-адресов (см. предыдущий шаг):

  ```
  tunnel = <ip1>-<ip2> to <ip3>-<ip4>
  ```

где,

<ip1>-<ip2> — диапазон реальных IP-адресов туннелируемых узлов (начальный и конечный IP-адреса диапазона),

<ip3>-<ip4> — диапазон виртуальных IP-адресов (начальный и конечный IP-адреса диапазона), которые будут использоваться вместо реальных IP-адресов туннелируемых узлов, если на узле, который к ним обращается, настроена видимость по виртуальным IP-адресам.

Параметр <ip4> можно не указывать, он формируется путем прибавления к <ip3> разницы между <ip2> и <ip1>.



Внимание! При задании виртуальных IP-адресов в ручном режиме автоматическая проверка повторного использования одних и тех же IP-адресов не производится. Поэтому убедитесь, что задаваемые диапазоны виртуальных IP-адресов не пересекаются.

Например, чтобы координатор туннелировал IP-адреса с 192.168.201.5 по 192.168.201.10, а виртуальными IP-адресами для этого диапазона были IP-адреса с 192.168.111.5 по 192.168.111.10, задайте:

```
tunnel = 192.168.201.5-192.168.201.10 to 192.168.111.5-192.168.111.10
```



Внимание! На всех туннелируемых узлах сети настройте статические маршруты для защищаемого трафика через ViPNet Coordinator HW или укажите ViPNet Coordinator HW в качестве шлюза по умолчанию.

5 Для настройки доступа к узлам, туннелируемым удаленным координатором, в секции [id] соответствующего координатора измените значение параметра tunnel:

```
tunnel = <ip1>-<ip2> to <ip3>-<ip4>
```

где,

<ip1>-<ip2> — диапазон реальных IP-адресов узлов, туннелируемых данным координатором (начальный и конечный IP-адреса диапазона),

<ip3>-<ip4> — диапазон виртуальных IP-адресов (начальный и конечный IP-адреса диапазона), которые используются вместо реальных IP-адресов туннелируемых узлов данного координатора, если на узле, который к ним обращается, настроена видимость по виртуальным IP-адресам.

6 Задайте использование IP-адресов <ip3>-<ip4> на каждом узле защищённой сети, с которого необходим доступ к туннелируемым узлам.

7 Сохраните изменения (**Ctrl+O**) и закройте редактор (**Ctrl+X**).

8 Запустите управляющую службу:

```
hostname# iplir start
```

Настройка туннелей между открытыми узлами

Примечание. В примере ниже указаны реальные IP-адреса туннелируемых узлов и настроена видимость узлов по реальным адресам.

Рассмотрим пример:

- В одном из офисов находится сервер данных, к которому обращаются пользователи из другого офиса.
- IP-адрес сервера 192.168.1.2. IP-адреса пользователей 192.168.2.2-192.168.2.4.
- Установка ПО ViPNet на сервер данных и компьютеры пользователей невозможна.

Необходимо, чтобы весь обмен данными через интернет происходил с шифрованием трафика.

Чтобы решить эту задачу, в каждом из офисов устанавливается ViPNet Coordinator HW, который выступает в роли криптошлюза для компьютеров локальной сети:

- HW-1 имеет частный IP-адрес 192.168.1.1 и идентификатор 0x00010101 в сети ViPNet;
- HW-2 имеет частный IP-адрес 192.168.2.1 и идентификатор 0x00020201 в сети ViPNet.

В результате компьютеры 1, 2, 3 смогут обращаться к серверу по адресу 192.168.1.2. При этом на участке между HW 1 и 2 пакеты будут передаваться в зашифрованном виде.

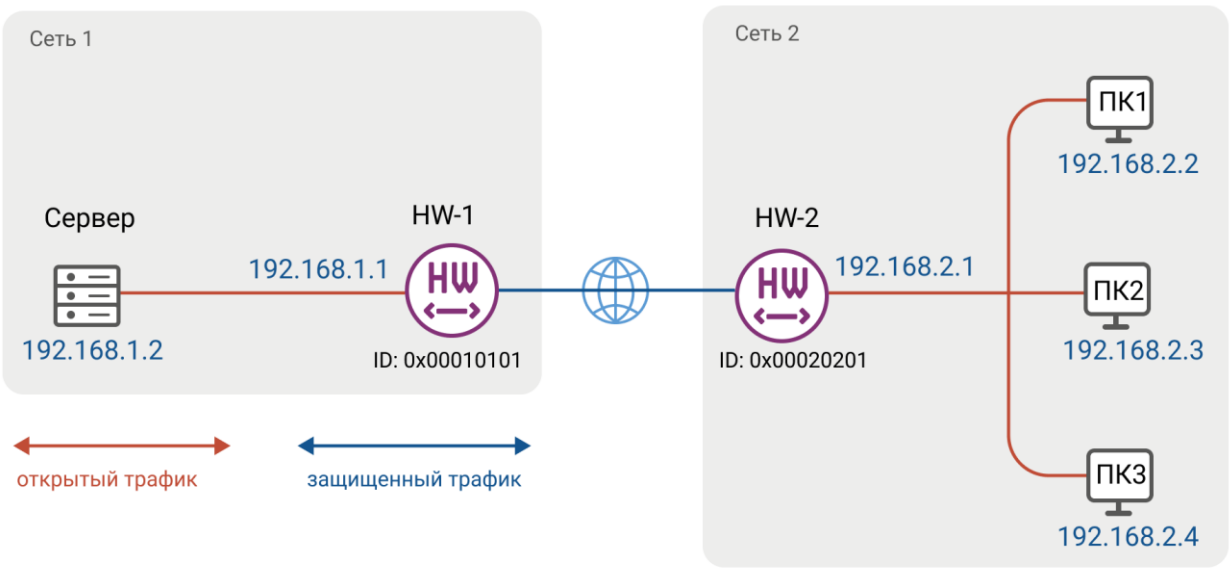


Рисунок 8. Настройка туннелей между открытыми узлами

Чтобы настроить работу туннелей:

1 На компьютерах 1, 2, 3 в качестве шлюза по умолчанию задайте частный IP-адрес HW-2, на сервере — частный IP-адрес HW-1.

2 На каждом ViPNet Coordinator HW задайте IP-адреса компьютеров, которые туннелирует он сам и противоположный ViPNet Coordinator HW. Адреса туннелируемых узлов можно задать двумя способами:

- Централизованно в ViPNet Prime. В этом случае для каждого ViPNet Coordinator HW задаются только адреса узлов, которые туннелирует он сам. После рассылки обновлений справочников и ключей заданные адреса появятся в настройках обоих ViPNet Coordinator HW. Этот способ является предпочтительным.
- Локально на ViPNet Coordinator HW путем редактирования конфигурационного файла `iplir.conf` (подробнее см. в документе «Справочник команд и конфигурационных файлов», в разделе «Файл iplir.conf»).

Для локальной настройки туннелей:

2.1 На HW-1:

- Завершите работу управляющей службы:

  ```
  hostname# iplir stop
  ```

- Откройте конфигурационный файл `iplir.conf` для редактирования:

  ```
  hostname# iplir config
  ```

- В собственную секцию `[id]` (содержащую параметр `id= 0x00010101`) добавьте параметр:

  ```
  tunnel= 192.168.1.2-192.168.1.2 to 192.168.1.2-192.168.1.2
  ```



Примечание. Если на вашем ViPNet Coordinator HW виртуальные адреса для туннелируемых узлов задаются автоматически (по умолчанию), то вместо этой строки вы можете записать только первую ее часть:
`tunnel= 192.168.1.2-192.168.1.2`
В этом случае строка будет автоматически дополнена дублирующимся IP-адресом после запуска управляющей службы. Это справедливо для всех строк, начинающихся с `tunnel=`.

- В секцию `[id]`, описывающую HW-2 (содержащую параметр `id= 0x00020201`), добавьте параметр:

  ```
  tunnel= 192.168.2.2-192.168.2.4 to 192.168.2.2-192.168.2.4
  ```

- Сохраните изменения (**Ctrl+O**) и закройте редактор (**Ctrl+X**).
- Запустите управляющую службу:

  ```
  hostname# iplir start
  ```

2.2 На HW-2:

- Завершите работу управляющей службы:

  ```
  hostname# iplir stop
  ```

- Откройте конфигурационный файл `iplir.conf` для редактирования:

  ```
  hostname# iplir config
  ```

- В собственную секцию `[id]` (содержащую параметр `id= 0x00020201`) добавьте параметр:

  ```
  tunnel= 192.168.2.2-192.168.2.4 to 192.168.2.2-192.168.2.4
  ```

- В секцию `[id]`, описывающую HW-1 (содержащую параметр `id= 0x00010101`), добавьте параметр:

  ```
  tunnel= 192.168.1.2-192.168.1.2 to 192.168.1.2-192.168.1.2
  ```

- Сохраните изменения (**Ctrl+O**) и закройте редактор (**Ctrl+X**).
- Запустите управляющую службу:

  ```
  hostname# iplir start
  ```

3 Убедитесь, что в настройках каждого ViPNet Coordinator HW разрешен трафик для заданных туннелируемых узлов. По умолчанию на ViPNet Coordinator HW разрешен трафик для всех туннелируемых узлов, но эта настройка могла быть изменена. Подробнее см. в разделе Ограничение доступа туннелируемых узлов.

Настройка туннелей между узлами ViPNet и открытыми узлами



Примечание. Описанный в этом разделе сценарий вы можете реализовать только в ручном режиме назначения виртуальных адресов для туннелируемых узлов (параметру `tunnel_virt_assignment` присвоено значение `manual` в секции `[misc]` файла `iplir.conf`). Подробнее см. раздел Ручная настройка туннелирования.

Рассмотрим модифицированную схему использования туннелей, когда на компьютеры 1, 2, 3 установлена программа ViPNet Client for Windows, а сервер остается незащищенным.

Пусть компьютерам 1, 2, 3 присвоены в сети ViPNet идентификаторы 0x00020202, 0x00020203, 0x00020204 соответственно.

В этом случае, когда туннелируется только сервер, организовать туннель можно двумя способами:

- Централизованно с помощью ViPNet Prime. В этом случае задайте для HW-1 в качестве IP-адреса туннелируемого соединения IP-адрес сервера и разошлите справочники на HW-1 и все связанные с ним узлы вашей сети ViPNet.

  Мы рекомендуем использовать этот способ.

- Локально редактированием конфигурационного файла `iplir.conf` HW-1 и настройки программы ViPNet Client for Windows на компьютерах 1, 2, 3.

Чтобы организовать туннель локально:

1 На HW-1 задайте адрес туннелируемого сервера:

1.1 Завершите работу управляющей службы:

```
hostname# iplir stop
```

1.2 Откройте конфигурационный файл `iplir.conf` для редактирования:

```
hostname# iplir config
```

1.3 В собственную секцию `[id]` добавьте параметр:

```
tunnel= 192.168.1.2-192.168.1.2 to 192.168.1.2-192.168.1.2
```

1.4 Сохраните изменения (**Ctrl+O**) и закройте редактор (**Ctrl+X**).

1.5 Запустите управляющую службу:

```
hostname# iplir start
```

2 Если в настройках HW-1 для туннелируемых узлов задан фильтр по умолчанию, то никакие дополнительные настройки не нужны. Иначе на HW-1 задайте фильтры туннелируемых узлов, разрешающие трафик между сервером и компьютерами 1, 2, 3:

2.1 Просмотрите фильтры туннелируемых узлов, заданных на HW-1:

```
hostname# firewall tunnel show
```

2.2 Удалите фильтры туннелируемых узлов:

```
hostname# firewall tunnel delete <номер фильтра>
```

2.3 Добавьте фильтры туннелируемых узлов:

```
hostname# firewall tunnel add src 192.168.1.2 dst 0x00020202,0x00020203,0x00020204 pass
```

```
hostname# firewall tunnel add src 0x00020202,0x00020203,0x00020204 dst 192.168.1.2 pass
```

Эти фильтры разрешают трафик в обоих направлениях между туннелируемым сервером и защищенными компьютерами 1, 2, 3.

3 На компьютерах 1, 2, 3 в программе ViPNet Client for Windows задайте для HW-1 в качестве IP-адреса для туннелирования IP-адрес 192.168.1.2 (подробнее см. документ «ViPNet Client for Windows. Руководство пользователя», раздел «Настройка доступа к туннелируемым узлам»).

После произведенных настроек компьютеры 1, 2, 3 смогут обращаться к серверу по адресу 192.168.1.2. При этом на участке между ViPNet Coordinator HW 1 и 2 пакеты будут передаваться в зашифрованном виде. Если требуется ограничить доступ к серверу со стороны некоторых узлов, например запретить доступ к серверу компьютеру 1, то на HW-1 вместо приведенных выше фильтров туннелируемых узлов добавьте следующие:

```
hostname# firewall tunnel add src 192.168.1.2 dst 0x00020203,0x00020204 pass
```

```
hostname# firewall tunnel add src 0x00020203,0x00020204 dst 192.168.1.2 pass
```

В результате изменения настроек защищенное взаимодействие с сервером будет доступно только компьютерам 2 и 3.

Для случая, когда на сервере установлен веб-сервис, к которому разрешено обращаться компьютерам 2 и 3, но запрещено компьютеру 1, приведенные выше фильтры надо изменить следующим образом:

```
hostname# firewall tunnel add src 192.168.1.2 dst 0x00020203,0x00020204 tcp sport 80 pass
```

```
hostname# firewall tunnel add src 0x00020203,0x00020204 dst 192.168.1.2 tcp dport 80 pass
```

После изменения настроек компьютерам 2 и 3 будет доступно защищенное взаимодействие только с веб-сервисом.

Настройка IP-адресов доступа к узлу и их приоритета

Каждый узел ViPNet взаимодействует с другим узлом, с которым у него есть связь, по определенному адресу доступа. Однако нередко некоторые узлы подключены к нескольким независимым каналам связи и имеют несколько адресов доступа, каждый из которых может использоваться для связи с другими узлами.

Приоритеты каналов связи зависят от метрик, настроенных на сетевом узле, которому необходимо получить доступ к защищенному сегменту сети.

Исходя из значений метрик каналов, ViPNet Coordinator HW будет выбирать более приоритетный канал связи. Для этого при включении ViPNet Coordinator HW отправляет служебные сообщения на все известные адреса доступа узлов с определенной задержкой, равной метрике, заданной для этих адресов в миллисекундах. Выбор канала для связи производится с учетом следующего:

- Адрес с наименьшей метрикой считается наиболее приоритетным. Соединение с узлом устанавливается по адресу с наименьшей метрикой всегда, когда этот адрес доступен.
- Если адрес с наименьшей метрикой недоступен или если все метрики равны, то соединение с узлом устанавливается по тому адресу, доступность которого определяется быстрее в результате опроса.
- Если помимо адресов с заданными метриками, есть адреса, для которых метрика установлена автоматически (`auto`), то ее значение всегда будет на 100 миллисекунд больше максимального значения заданной метрики. То есть канал с автоматически определяемой метрикой всегда будет иметь самый низкий приоритет по сравнению с каналами, для которых метрика задана вручную.
- После установления соединения с узлом определение доступности других его адресов выполняется только при разрыве текущего соединения. Задержка в выборе альтернативного канала связи может составлять от 7 до 70 секунд.

Адреса доступа для узлов, связанных с ViPNet Coordinator HW, настраиваются одним из способов:

- в секциях `[id]` файла `iplir.conf`;
- командой `iplir node access-point`.

Настройка в iplir.conf

Каждый адрес доступа узла указывается в параметре `accessiplist` секции `[id]`, количество данных параметров в секции не ограничено.

Примечание. IP-адреса доступа узла могут быть настроены в ViPNet Prime. В этом случае они будут указаны в соответствующих секциях `[id]` файла `iplir.conf`. Для таких адресов вы также можете настроить приоритет, изменив значения метрик, которые по умолчанию определяются как `auto`.

Чтобы указать IP-адреса доступа к какому-либо узлу, связанному с ViPNet Coordinator HW, и определить приоритеты этих адресов:

1. Завершите работу управляющей службы:

   ```
   hostname# iplir stop
   ```

2. Откройте файл `iplir.conf` для редактирования:

   ```
   hostname# iplir config
   ```

3. В параметрах `accessiplist` секции `[id]` соответствующего узла выполните одно из действий:

   - Укажите IP-адреса доступа к узлу и задайте метрики маршрутов для каждого из этих адресов в следующем виде:

     ```
     accessiplist= <IP-адрес доступа>, <метрика>, [<порт>]
     ```

     При задании значения метрики необходимо учитывать следующее:

     - рекомендуется указывать значения метрик больше максимального времени задержки при прохождении служебного сообщения и ответа на него по соответствующему каналу связи, но не превышающее 9999 миллисекунд;
     - рекомендуемая минимальная разница между метриками — 100 миллисекунд. Чем больше разница между наименьшей метрикой и остальными метриками, тем меньше вероятность того, что в случае кратковременного сбоя самого приоритетного канала во время процедуры определения адреса доступа будет выбран менее приоритетный канал. При использовании менее приоритетного канала сетевой узел быстрее сможет вернуться к работе через самый приоритетный канал, когда тот станет доступен.

   - Если вы уже указали IP-адреса доступа ранее или они были получены из ViPNet Prime автоматически, в параметре `accessiplist` задайте метрики маршрутов для этих адресов в соответствии с рекомендациями, описанными выше.

4. Сохраните изменения (**Ctrl+O**, затем нажмите **Enter**) и закройте редактор (**Ctrl+X**).

5. Запустите управляющую службу:

   ```
   hostname# iplir start
   ```

В результате в параметры `accessiplist` файла `iplir.conf` автоматически будут добавлены реальный IP-адрес сетевого интерфейса узла, через который будут передаваться IP-пакеты для выбранного IP-адреса доступа, условный номер этого интерфейса и тип регистрации данного IP-адреса доступа узла в виде:

```
accessiplist= <IP-адрес доступа>, <метрика>, <реальный IP-адрес узла>, <номер интерфейса>,
<тип регистрации>, [<порт>]
```

Например, запись об автоматическом добавлении IP-адреса 89.135.15.2 с метрикой 1 будет выглядеть следующим образом:

```
accessiplist= 89.135.15.2, 1, 0.0.0.0, 0, auto
```

Настройка командой iplir node access-point

Чтобы указать IP-адреса доступа к какому-либо узлу, связанному с ViPNet Coordinator HW, и определить приоритеты этих адресов, выполните команду:

```
hostname# iplir node <id_узла> access-point {add | delete} <IP-адрес доступа> [port <порт>]
[metric <метрика>]
```

где:

- `<id_узла>` — ViPNetID узла;
- действие:
  - `add` — добавить IP-адреса доступа;
  - `delete` — удалить IP-адреса доступа.



Примечание. В отличие от настройки IP-адресов доступа в `iplir.conf`, перезапуск управляющей службы после выполнения команды не требуется.

Особенности настройки IP-адресов доступа

IP-адрес доступа, заданный вручную, при выборе канала приоритетнее IP-адреса доступа, полученного из ViPNet Prime, поскольку имеет меньшее значение метрики. Чтобы использовать IP-адрес доступа из ViPNet Prime, измените значение его метрики, заданной по умолчанию как `auto`.

См. подробное описание:

- параметра `accessiplist` — в документе «Справочник команд и конфигурационных файлов», секция `[id]` файла `iplir.conf`;
- команды `iplir node access-point` — в документе «Справочник команд и конфигурационных файлов», раздел «Команды группы iplir».

Настройка TCP-туннеля

При удаленном подключении клиентов к сетям ViPNet может возникать проблема с передачей IP-пакетов по протоколу UDP из-за того, что данный протокол блокируется некоторыми интернет-провайдерами. Но в этих случаях обычно разрешен доступ по протоколу TCP через порты 80 (HTTP) и 443 (HTTPS).

Для решения проблемы доступа можно организовать взаимодействие клиентов с другими узлами сети ViPNet через TCP-туннель, настроенный на сервере соединений этих клиентов.

Если клиент TCP-туннеля не может связаться со своим сервером соединений (сервером TCP-туннелей) по протоколу UDP, он автоматически начинает устанавливать с ним соединение через TCP-туннель. Сервер соединений (сервер TCP-туннелей) передает полученные от клиента IP-пакеты дальше на узлы назначения по протоколу UDP.

ViPNet Coordinator HW может работать в режиме сервера TCP-туннелей или клиента TCP-туннеля, подключаясь к своему серверу соединений.

Настройка сервера TCP-туннелей

Примечание. При соединении через TCP-туннель клиентам не будут приходить уведомления в случае рассинхронизации времени.

Условия работы TCP-туннеля

- ViPNet Coordinator HW должен иметь публичный IP-адрес, поскольку для установления TCP-соединения клиент использует именно публичный IP-адрес доступа сервера соединений. Поэтому в файле `iplir.conf` в параметре `accessiplist` собственной секции `[id]` должен быть задан хотя бы один публичный адрес.
- На ViPNet Coordinator HW должен быть запущен сервер TCP-туннелей и настроен порт для входящих TCP-соединений (см. описание ниже).
- На клиентах TCP-туннеля заданный порт должен совпадать с номером порта, который используется на ViPNet Coordinator HW для TCP-соединений. Номер порта поступает клиенту от сервера соединений в составе служебной информации. Если служебная информация не поступила, то порт на клиенте можно задать вручную.

Настройка работы TCP-туннеля

1 Убедитесь, что служба `iplircfg` запущена:

```
hostname# failover show info
```

2 Назначьте ViPNet Coordinator HW роль сервера TCP-туннелей (установлена по умолчанию):

```
hostname# iplir tcptunnel role server
```

3 По умолчанию для подключения клиентов TCP-туннелей к ViPNet Coordinator HW задан порт 80, но если в ViPNet Prime задан другой порт, он изменится в настройках ViPNet Coordinator HW. Чтобы просмотреть, какой порт задан:

```
hostname# iplir show tcptunnel-info
```

Порт указан в параметре `TCP server port`.

Если этот порт используется другой службой, измените номер порта:

```
hostname# iplir tcptunnel server port <номер порта>
```

4 Запустите сервер TCP-туннелей:

```
hostname# iplir tcptunnel server on
```

Если номер порта был изменён, то на все клиенты TCP-туннеля будет отправлена информация с новым номером порта для TCP-соединений.

Настроить сервер TCP-туннелей также можно путём редактирования конфигурационного файла `iplir.conf`.

Примечание. В случае если протокол UDP перестал блокироваться, соединение по данному протоколу восстановится при следующих условиях:

- по истечении тайм-аута отправки служебных IP-пакетов с клиента на сервер соединений (по умолчанию тайм-аут равен 5 минутам);
- после проверки соединения этого узла с другим;
- после смены IP-адреса узла (например, при изменении точки доступа к интернету).

Настройка TCP-клиента

Примечание. Работа ViPNet Coordinator HW в качестве клиента TCP-туннеля возможна только при подключении к сети в режиме «С динамической трансляцией адресов» (см. Настройка подключения к внешней сети).

---

1 Убедитесь, что служба `iplircfg` запущена:

```
hostname# failover show info
```

2 Назначьте ViPNet Coordinator HW роль клиента:

```
hostname# iplir tcptunnel role client
```

3 Выберите режим подключения:

```
hostname# iplir tcptunnel client mode {auto | forced}
```

- `auto` — автоматическое включение TCP-туннеля при пропадании соединения по UDP и выключение при его появлении;
- `forced` — TCP-туннель устанавливается всегда, когда возможно, даже при доступе к серверу соединения по UDP.

4 Задайте порт для подключения к серверу TCP-туннелей:

```
hostname# iplir tcptunnel client port <порт>
```

Этот порт должен совпадать с номером порта, заданным на сервере TCP-туннелей.

Если порт используется какой-либо другой службой, нужно задать другой порт на клиенте и сервере TCP-туннелей.

5 Включите режим клиента TCP-туннелей:

```
hostname# iplir tcptunnel client on
```

Настроить клиента TCP-туннелей также можно путём редактирования конфигурационного файла `iplir.conf`.

Сценарии использования VPN

Объединение удаленных сегментов сети ViPNet

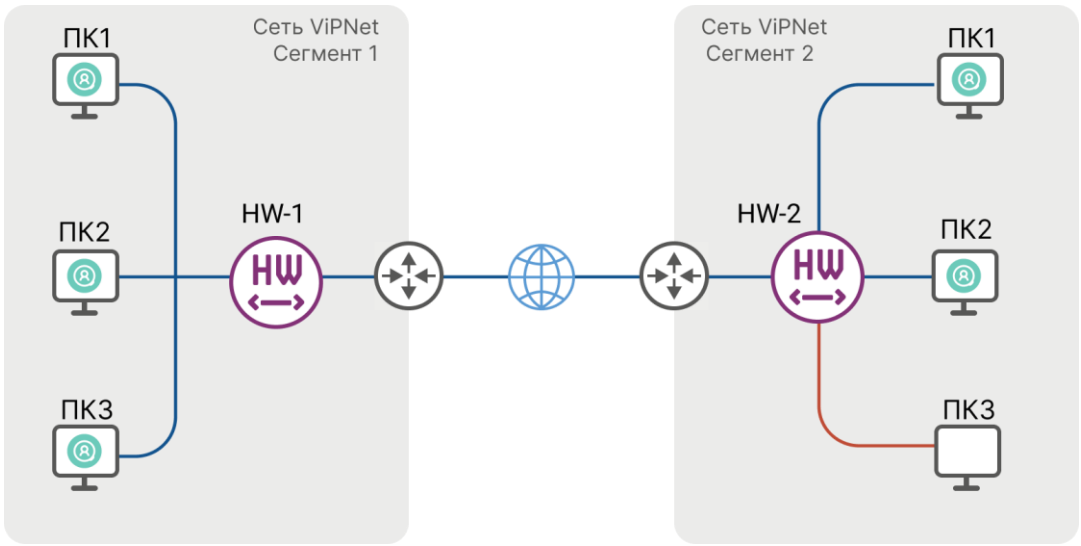


Рисунок 9. Объединение удаленных сегментов сети ViPNet

Чтобы объединить удаленные сегменты сети ViPNet:

1. В каждом сегменте за шлюзом установите HW.
2. В каждом сегменте на ПК, которые должны быть ViPNet-клиентами, установите ПО ViPNet Client
3. В ViPNet Prime создайте связи между ViPNet-клиентами.
4. Для открытого узла ПК3 создайте туннель. Для этого на каждом HW задайте IP-адрес ПК3 в качестве туннелируемого адреса (см. Настройка туннелей между узлами ViPNet и открытыми узлами).

Настройка туннелирования на канальном уровне

Общие сведения о L2OverIP

ViPNet Coordinator HW поддерживает технологию L2OverIP, которая позволяет объединять удалённые сегменты сети на канальном уровне модели OSI так, что их узлы находятся в одном широковещательном домене.

L2OverIP предполагает взаимодействие между узлами нескольких удалённых сегментов сети через ViPNet Coordinator HW, которые установлены на границах этих сегментов. ViPNet Coordinator HW перехватывает Ethernet-кадры, отправляемые из его сегмента сети в другой, упаковывает их в зашифрованные IP-пакеты и передаёт их другому ViPNet Coordinator HW, который, в свою очередь, расшифровывает поступившие IP-пакеты, извлекает из них исходные кадры и передаёт получателям в своем сегменте.

Сетевой интерфейс ViPNet Coordinator HW, к которому подключаются узлы сегмента сети, должен иметь класс:

- `access` со статическим IP-адресом для физических интерфейсов `eth`, виртуальных интерфейсов `vlan` или агрегированных интерфейсов `bond`;
- `trunk` для физических интерфейсов `eth` или агрегированных интерфейсов `bond`.



Внимание! В исполнении HW50 технология L2OverIP поддерживается только на сетевых интерфейсах класса `access`.

С помощью L2OverIP можно объединить несколько сегментов сети:

- сегменты без VLAN, находящиеся за сетевыми интерфейсами класса `access`;
- виртуальная сеть VLAN из одного сегмента и виртуальная сеть VLAN из другого сегмента;
- все виртуальные сети VLAN из одного сегмента со всеми виртуальными сетями другого сегмента (для этого необходимо указать сетевые интерфейсы класса `trunk`, за которыми находятся виртуальные сети VLAN; адреса виртуальных сетей VLAN должны совпадать);
- одна из виртуальных сетей VLAN сегмента и сегмент без VLAN, находящийся за сетевым интерфейсом класса `access`.

При использовании L2OverIP ViPNet Coordinator HW работает как виртуальный сетевой коммутатор, хранящий в памяти таблицу MAC-адресов сетевых узлов, от которых поступает сетевой трафик.

Каждому сегменту сети назначается свой номер порта, который задается в настройках L2OverIP. Порт, заданный для собственного сегмента сети, называется локальным. Порты, заданные на ViPNet

Coordinator HW в других сегментах, называются удаленными. Трафик самого ViPNet Coordinator HW всегда относится к порту с номером 0.

Виртуальный коммутатор может по-разному обрабатывать одноадресные Ethernet-кадры с неизвестным MAC-адресом получателя: блокировать либо обрабатывать как многоадресные с рассылкой на все удаленные порты. Последняя возможность позволяет использовать L2OverIP для схемы, когда два ViPNet Coordinator HW объединены с помощью агрегированного канала и каждый из физических каналов работает через свою пару ViPNet Coordinator HW. Кадры, которыми обмениваются два узла из разных сегментов, могут в одном направлении постоянно пересылаться через одну пару ViPNet Coordinator HW, а в другом направлении — через другую. В этом случае адрес получателя кадров будет определяться как неизвестный, и для обработки пакетов многоадресной рассылки следует использовать режим `smart-broadcast`.

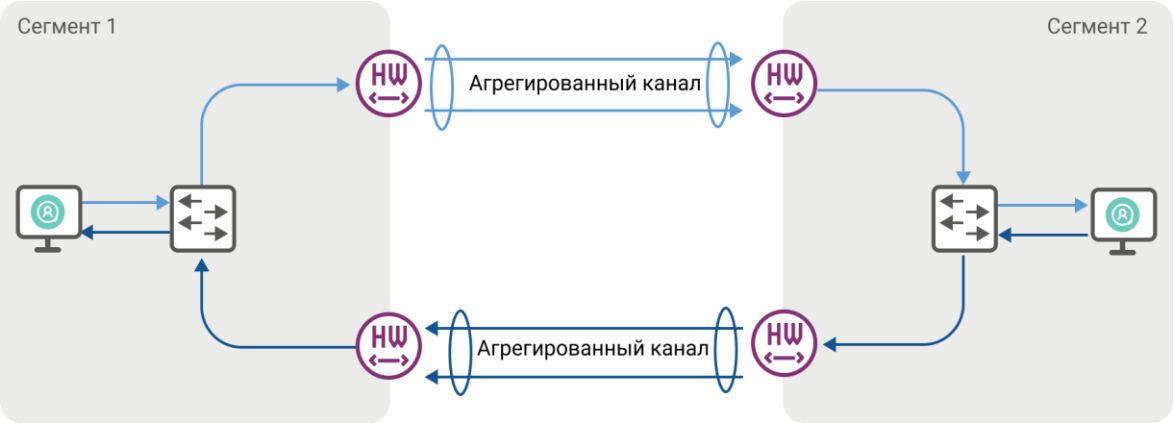


Рисунок 10. Схема работы сети с парами ViPNet Coordinator HW, объединенных с помощью агрегированных каналов

Рассылка Ethernet-кадров с неизвестным MAC-адресом получателя выполняется в соответствии режимом обработки:

- кадры, принятые из локального порта, пересылаются на все удаленные порты и на порт с номером 0;
- кадры, принятые из удаленного порта, пересылаются на локальный порт и на порт с номером 0;
- кадры, принятые из порта с номером 0, в зависимости от выбранного режима либо блокируются, либо пересылаются на локальный порт и на все удаленные порты.

Настройка L2OverIP в кластере выполняется на активном узле. При переключении узлов кластера таблица MAC-адресов не передается пассивному узлу. Коммутация кадров восстановится, когда узлы из разных сегментов, взаимодействующие друг с другом, заново отправят ARP-запросы.

Особенности реализации L2OverIP

- Сегменты сети, объединяемые по L2OverIP, должны быть изолированы друг от друга. Сетевое взаимодействие между ними должно осуществляться только по каналам связи между ViPNet Coordinator HW, установленными на границах объединяемых сегментов.
- ViPNet Coordinator HW позволяет объединять не более 31 сегмента сети.
- Используйте не более 252 IP-адресов во всех объединяемых сегментах сети. Превышение этого количества может привести к снижению пропускной способности сети в связи с возрастанием служебного трафика в широковещательном домене.
- Для исполнения ViPNet Coordinator VA в настройках платформы виртуализации включите неразборчивый режим (Promiscuous Mode) на интерфейсе, к которому привязан адаптер виртуальной машины.
- Поиск IP-пакетов, переданных по L2OverIP, в журнале IP-пакетов необходимо выполнять по признакам исходных IP-пакетов: IP-адрес источника и получателя, номер TCP- и UDP-порта, интерфейс.

Сценарии использования L2OverIP

При настройке туннелирования на канальном уровне каждый сегмент сети подключается к одному из сетевых интерфейсов ViPNet Coordinator HW, установленному на границе сегмента. Если сегмент сети состоит из нескольких VLAN, они должны быть объединены с помощью коммутатора в транковый порт, к которому подключается один из сетевых интерфейсов ViPNet Coordinator HW.

Чтобы настроить L2OverIP, на каждом ViPNet Coordinator HW:

1 Укажите сетевой интерфейс, сегмент сети которого будет объединяться с другим сегментом по L2OverIP:

```
hostname# iplir set l2overip interface <рабочий интерфейс>
```

Примечание. Если требуется объединить отдельную VLAN одного сегмента сети с другим сегментом сети, на ViPNet Coordinator HW, стоящем на границе сегмента с VLAN, укажите в качестве рабочего интерфейса виртуальный интерфейс VLAN в формате `<физический интерфейс>.<номер виртуального интерфейса>`.

---

2 Задайте параметры локального сегмента сети, указав уникальный номер порта и IP-адрес внешнего интерфейса:

```
hostname# iplir set l2overip local-port <номер порта> <IP-адрес внешнего интерфейса>
```

В качестве номера порта вы можете задать значение из интервала 1–31. Каждому сегменту необходимо назначить свой номер порта.

3 Задайте параметры удаленного сегмента сети — номер порта сегмента и IP-адрес видимости внешнего интерфейса (`local-port`) удаленного ViPNet Coordinator HW:

```
hostname# iplir set l2overip remote-port <номер порта> <IP-адрес видимости удаленного ViPNet Coordinator HW>
```

В зависимости от настройки видимости удаленного ViPNet Coordinator HW укажите его реальный или виртуальный IP-адрес. Если ViPNet Coordinator HW имеет более одного адреса видимости для удаленного ViPNet Coordinator HW (секция `[id]` конфигурационного файла iplir.conf, соответствующая удаленному координатору, содержит более одного параметра `ip`), настройте видимость удаленного ViPNet Coordinator HW по реальным адресам и укажите его реальный IP-адрес.



Примечание. Вы можете удалить параметры удаленного сегмента:

```
hostname# iplir set l2overip remote-port <номер порта> delete
```

или изменить IP-адрес видимости:

```
hostname# iplir set l2overip remote-port <номер порта> <новый IP-адрес>
```

Если оба ViPNet Coordinator HW имеют более одного адреса видимости друг для друга, необходимо настроить видимость по реальным адресам.

---

4 При необходимости измените время жизни MAC-адреса в таблице MAC-адресов виртуального коммутатора (см. Общие сведения о L2OverIP) при отсутствии трафика, поступающего от этого адреса:

```
hostname# iplir set l2overip mac-ttl <время жизни MAC-адреса>
```

Время жизни MAC-адреса задается в секундах. Значение по умолчанию — 300 секунд. Задайте значение из интервала 60–86400.

5 Добавьте сетевые фильтры защищенной сети, разрешающие любые соединения по протоколу 97:

```
hostname# firewall vpn add src @local dst @any proto 97 pass
hostname# firewall vpn add src @any dst @local proto 97 pass
```

6 Включите службу L2OverIP:

```
hostname# iplir set l2overip mode switch
```

7 Проверьте текущее состояние и настройки L2OverIP:

```
hostname# iplir show l2overip config
```



Внимание! На двух ViPNet Coordinator HW, соединенных по L2OverIP, IP-адреса локального и удаленного сегментов должны быть настроены симметричным образом. То есть на каждом ViPNet Coordinator HW в качестве IP-адреса удаленного сегмента должен быть указан IP-адрес видимости сетевого интерфейса, который задан на втором ViPNet Coordinator HW в качестве внешнего интерфейса локального сегмента.

Настройка L2OverIP для сегментов сети

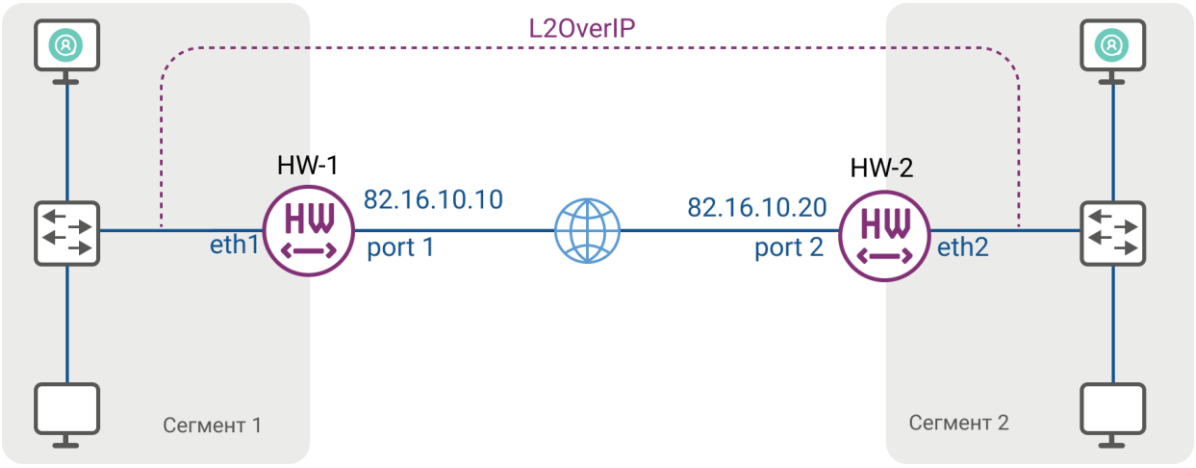


Рисунок 11. Защита соединения удаленных сегментов сети на канальном уровне модели OSI

Настройте L2OverIP на каждом HW:

1 Укажите сетевой интерфейс, сегмент сети которого будет объединяться с другим сегментом:

- HW-1:

```
hostname# iplir set l2overip interface eth1
```

- HW-2:

```
hostname# iplir set l2overip interface eth2
```

Если сегментов больше двух, аналогичным образом укажите интерфейс на остальных HW.

2 Задайте параметры локального сегмента сети, указав уникальный номер порта и адрес внешнего интерфейса:

- HW-1:

```
hostname# iplir set l2overip local-port 1 82.16.10.10
```

- HW-2:

```
hostname# iplir set l2overip local-port 2 82.16.10.20
```

Если сегментов больше двух, укажите номер порта и адрес внешнего интерфейса на остальных HW. Каждому сегменту необходимо назначить свой номер порта.

3 Задайте параметры удаленного сегмента сети — номер порта сегмента и IP-адрес видимости внешнего интерфейса (local-port) удаленного HW:

- HW-1:

```
hostname# iplir set l2overip remote-port 2 82.16.10.20
```

- HW-2:

```
hostname# iplir set l2overip remote-port 1 82.16.10.10
```

В зависимости от настройки видимости удаленного HW укажите его реальный или виртуальный IP-адрес. Если ViPNet Coordinator HW имеет более одного адреса видимости для удаленного ViPNet Coordinator HW (секция `[id]` конфигурационного файла iplir.conf,

соответствующая удаленному координатору, содержит более одного параметра `ip`), настройте видимость удаленного ViPNet Coordinator HW по реальным адресам и укажите его реальный IP-адрес.

Если сегментов больше двух, добавьте параметры всех удаленных сегментов и выполните аналогичную настройку на остальных HW.

4 Добавьте сетевые фильтры защищенной сети, разрешающие любые соединения по протоколу 97:

```
hostname# firewall vpn add src @local dst @any proto 97 pass
hostname# firewall vpn add src @any dst @local proto 97 pass
```

5 Включите службу L2OverIP:

```
hostname# iplir set l2overip mode switch
```

6 Убедитесь в корректности выполненных настроек:

```
hostname# iplir show l2overip config
```

Дополнительные настройки параметров удаленного сегмента

Чтобы изменить адрес видимости удаленного сегмента:

```
hostname# iplir set l2overip remote-port <номер порта> <новый адрес>
```

После изменения параметров удаленного сегмента перезапустите службу L2OverIP:

```
hostname# iplir set l2overip mode none
hostname# iplir set l2overip mode switch
```

Чтобы удалить параметры удаленного сегмента:

```
hostname# iplir set l2overip remote-port <номер порта> delete
```

Настройка L2OverIP для сегментов сети с VLAN

С помощью L2OverIP можно объединять сегменты сети, состоящие из нескольких VLAN. В каждом сегменте VLAN должны быть объединены с помощью коммутатора в транковый порт, к которому подключается интерфейс ViPNet Coordinator HW.

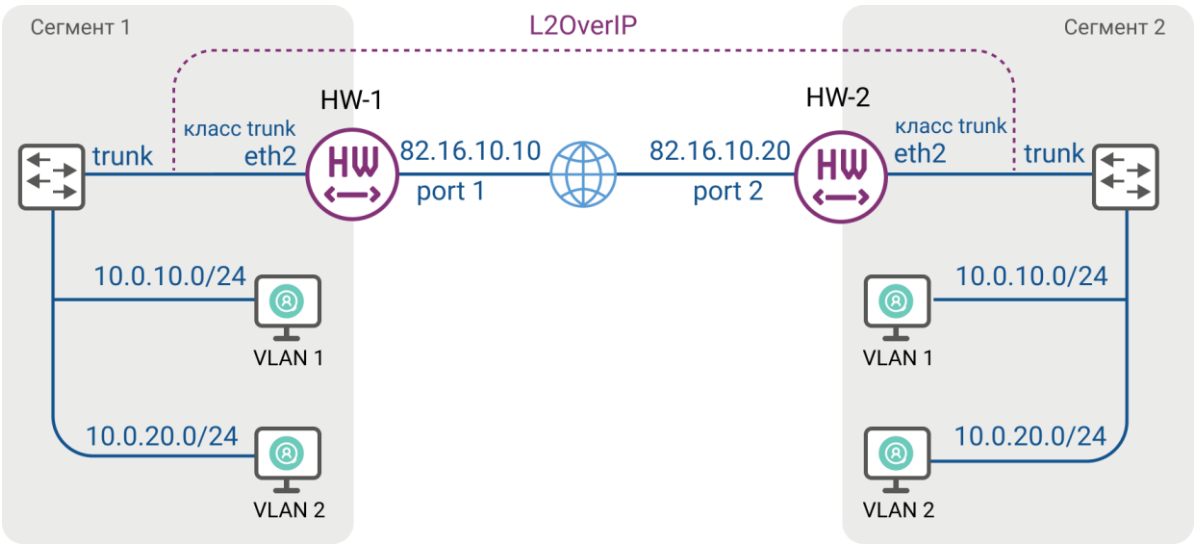


Рисунок 12. Схема объединения сегментов с VLAN

Настройте L2OverIP на каждом HW:

1 Установите класс `trunk` для сетевого интерфейса `eth2`:

```
hostname# inet ifconfig eth2 class trunk
```

Примечание. Если для ViPNet Coordinator VA в настройках виртуальной машины выбраны сетевые адаптеры VirtIO, для корректной работы L2OverIP смените тип адаптеров на vmxnet3.

---

2 Укажите сетевой интерфейс `eth2`, сегмент сети которого будет объединяться с другим удаленным сегментом:

```
hostname# iplir set l2overip interface eth2
```

3 Укажите параметры локального сегмента сети:

- HW-1:

  ```
  hostname# iplir set l2overip local-port 1 82.16.10.10
  ```

- HW-2:

  ```
  hostname# iplir set l2overip local-port 2 82.16.10.20
  ```

4 Укажите параметры удаленного сегмента сети:

- HW-1:

  ```
  hostname# iplir set l2overip remote-port 2 82.16.10.20
  ```

- HW-2:

```
hostname# iplir set l2overip remote-port 1 82.16.10.10
```

5 Добавьте сетевые фильтры защищенной сети, разрешающие любые соединения по протоколу 97:

```
hostname# firewall vpn add src @local dst @any proto 97 pass
hostname# firewall vpn add src @any dst @local proto 97 pass
```

6 Включите службу L2OverIP:

```
hostname# iplir set l2overip mode switch
```

Если необходимо объединить только один VLAN одного сегмента с таким же VLAN другого сегмента, то в качестве рабочего интерфейса L2OverIP вместо физического интерфейса `eth1` укажите виртуальный интерфейс VLAN, например, `eth2.10`.

Также с помощью L2OverIP можно объединить один VLAN одного сегмента с другим сегментом сети, в котором нет VLAN.

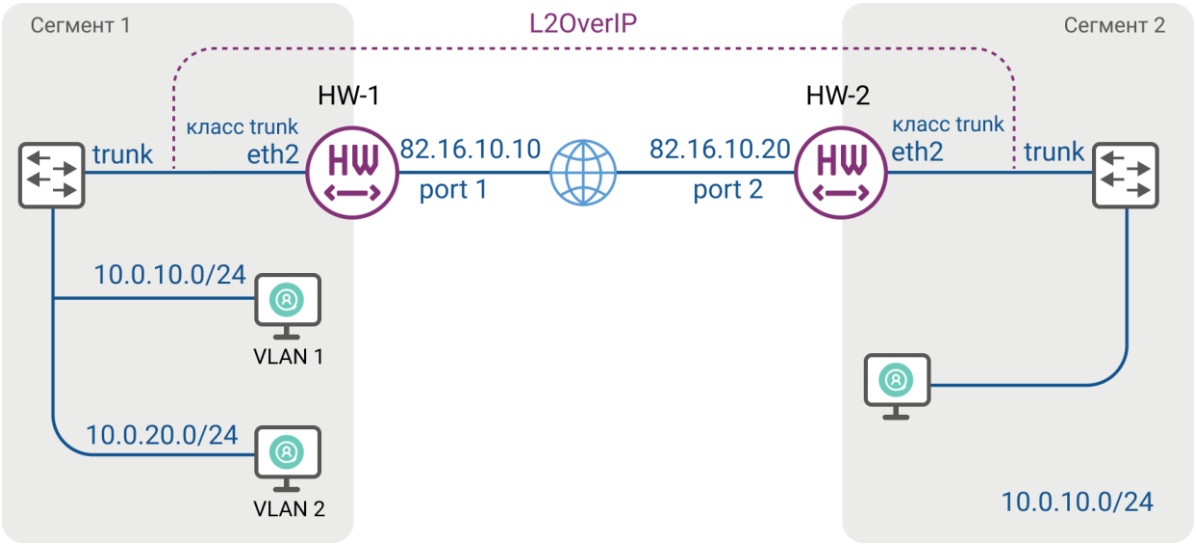


Рисунок 13. Схема объединения одним VLAN с сегментом без VLAN

В этом случае измените настройку предыдущего сценария:

1 Создайте виртуальные интерфейсы для VLAN только на HW-1.

2 На HW-1 в качестве рабочего интерфейса укажите виртуальный интерфейс VLAN:

```
hostname# iplir set l2overip interface eth2.10
```

3 На HW-2 в качестве рабочего интерфейса укажите физический интерфейс, к которому подключен сегмент:

```
hostname# iplir set l2overip interface eth2
```

Настройка L2OverIP для ViPNet Coordinator VA

С помощью L2OverIP можно объединять сегменты сети, расположенные за ViPNet Coordinator VA. В этом случае настройте платформу виртуализации, например VMware vSphere ESXi:

1 Запустите vSphere Client.

2 Выберите **Home** > **Inventory** > **Hosts and Clusters**.

3 Установите «неразборчивый» режим, при котором разрешен прием всех пакетов вне зависимости от того, кому они адресованы:

3.1 В окне настроек виртуального коммутатора **vSphere Standard Switch** откройте вкладку **Security**.

3.2 В списке **Promiscuous Mode** выберите **Accept**.

4 Убедитесь, что в списках **MAC Address Changes** и **Forged Transmits** также выбран **Accept**.

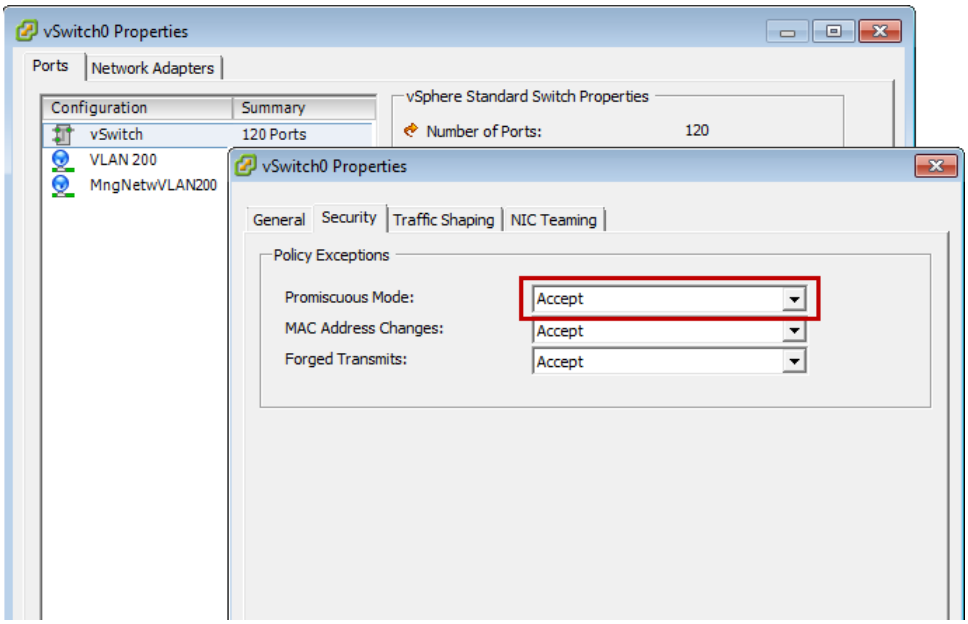


Рисунок 14. Установка неразборчивого режима на виртуальном коммутаторе

Примечание. Если вы используете распределенный виртуальный коммутатор vSphere Distributed Switch, задайте аналогичные настройки для этого коммутатора в разделе **Home** > **Inventory** > **Networking**.



4

Настройка межсетевого экрана

О фильтрации трафика 93

Настройка режима работы и параметров межсетевого экрана 101

Настройка аппаратной фильтрации трафика 106

Объекты сетевых фильтров и правил трансляции адресов 108

Настройка SSL/TLS-инспекции трафика 121

Настройка подключения к ICAP-серверам 128

Настройка сетевых фильтров 131

Настройка правил трансляции адресов 158

Настройка обработки прикладных протоколов DNS, FTP, H.323, SCCP, SIP 168

О фильтрации трафика

Типы трафика

Фильтрации подвергается весь трафик, который проходит через ViPNet Coordinator HW:

- → открытый трафик — незашифрованный трафик между открытыми (или открытым и защищённым) узлами;
- → защищённый трафик — зашифрованный трафик между узлами сети ViPNet.

Открытый трафик может быть локальным или транзитным:

- локальный трафик — трафик, в котором ViPNet Coordinator HW является получателем или отправителем IP-пакетов;
- транзитный трафик — трафик, в котором ViPNet Coordinator HW не является ни получателем, ни отправителем IP-пакетов.

ViPNet Coordinator HW обрабатывает трафик, разделяя его на следующие типы:

- открытый локальный трафик — между открытым узлом и ViPNet Coordinator HW;
- защищённый трафик — трафик между узлами сети ViPNet;
- туннелируемый трафик — трафик между двумя открытыми (или открытым и защищённым) узлами, зашифрованный в пределах сети ViPNet;

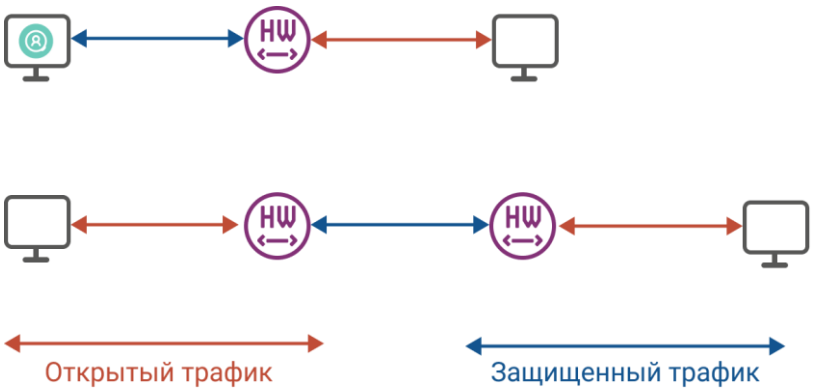


Рисунок 15. Туннелируемый трафик

- открытый транзитный трафик — трафик между открытыми (или открытым и защищённым) узлами, проходящий через координатор, который не является ни отправителем, ни получателем IP-пакетов.



Рисунок 16. Открытый транзитный трафик

Для каждого типа трафика можно настроить соответствующие сетевые фильтры (см. Создание сетевого фильтра).

Классификация трафика с помощью DPI

ViPNet Coordinator HW может классифицировать открытый транзитный и туннелируемый трафик с помощью DPI:

- по прикладным протоколам;
- по приложениям (см. Поддерживаемые приложения);
- по группам приложений и прикладных протоколов.

Возможность классификации трафика и использования прикладных протоколов, приложений и групп в сетевых фильтрах определяется лицензией.

Независимо от наличия лицензии и сетевых фильтров с параметрами прикладных протоколов, приложений и групп, проводится предварительная классификация трафика по начальным IP-пакетам:

- если IP-пакеты классифицированы, то в журнале IP-пакетов при срабатывании фильтров на пакеты этих сессий будет указываться результат классификации (прикладной протокол и приложение);
- если IP-пакеты не классифицированы, то в журнале IP-пакетов при срабатывании фильтров на пакеты этих сессий результат классификации будет отсутствовать;

Если лицензия назначена, классификация трафика включена по умолчанию, в том числе автозапуск DPI при перезагрузке ViPNet Coordinator HW.

Внимание! После назначения лицензии, разрешающей использование и обновление DPI, перезагрузите ViPNet Coordinator HW.

Чтобы выключить DPI:

```
hostname# service dpi stop
```

Чтобы включить DPI заново:

```
hostname# service dpi start
```

Чтобы включить или выключить автозапуск DPI, выполните:

```
hostname# service dpi mode {on | off}
```

Чтобы просмотреть текущие настройки DPI, выполните:

```
hostname# service dpi show status
```

Для поддержания набора классифицируемых прикладных протоколов, приложений и их групп в актуальном состоянии обновляйте DPI вручную (см. Локальное обновление DPI).

Принципы фильтрации трафика

- Все входящие и исходящие открытые и защищенные IP-пакеты обрабатываются сетевыми фильтрами в порядке убывания приоритета этих фильтров.
- Если IP-пакет соответствует условию одного из фильтров, он пропускается или блокируется этим фильтром; при этом фильтры с более низким приоритетом не применяются.
- Если IP-пакет был пропущен одним из фильтров, ответные IP-пакеты (включая служебные ICMP-пакеты) в рамках текущего соединения будут пропускаться автоматически.
- Если IP-пакет не был обработан ни одним из фильтров, он блокируется фильтром по умолчанию.



Внимание! TCP-порт 2047 и UDP-порт 2046 являются служебными портами ViPNet Coordinator HW, поэтому входящий открытый трафик, поступающий на эти порты, блокируется.

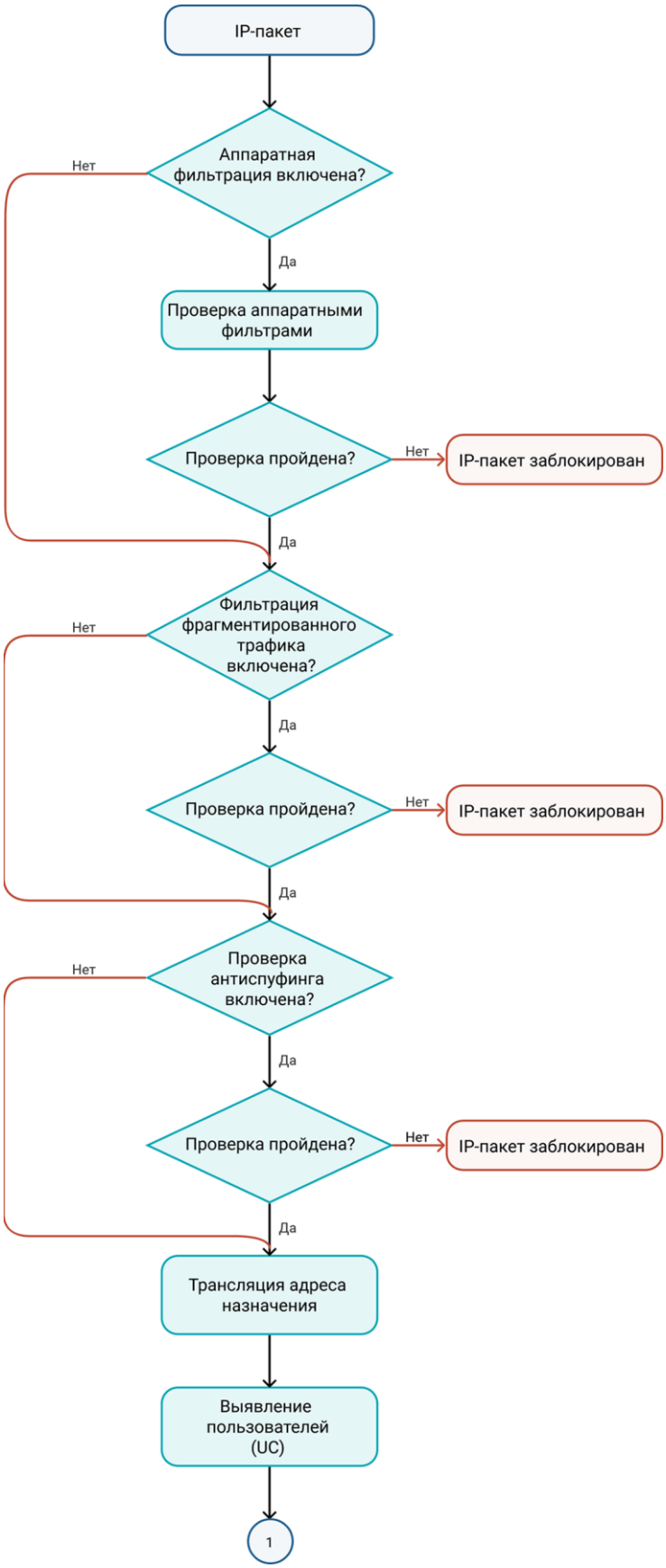


Рисунок 17. Схема фильтрации трафика. Часть 1

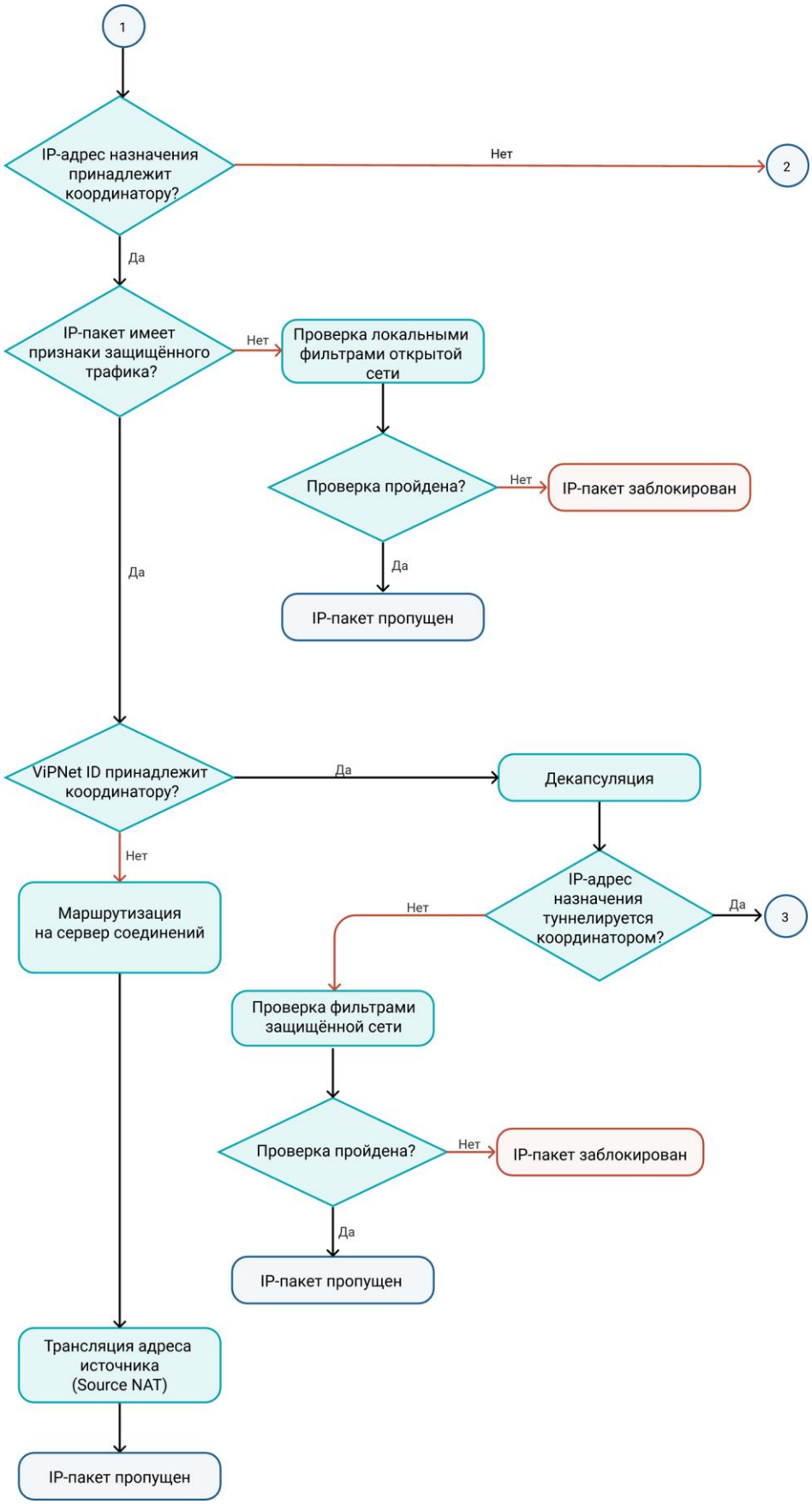


Рисунок 18. Схема фильтрации трафика. Часть 2

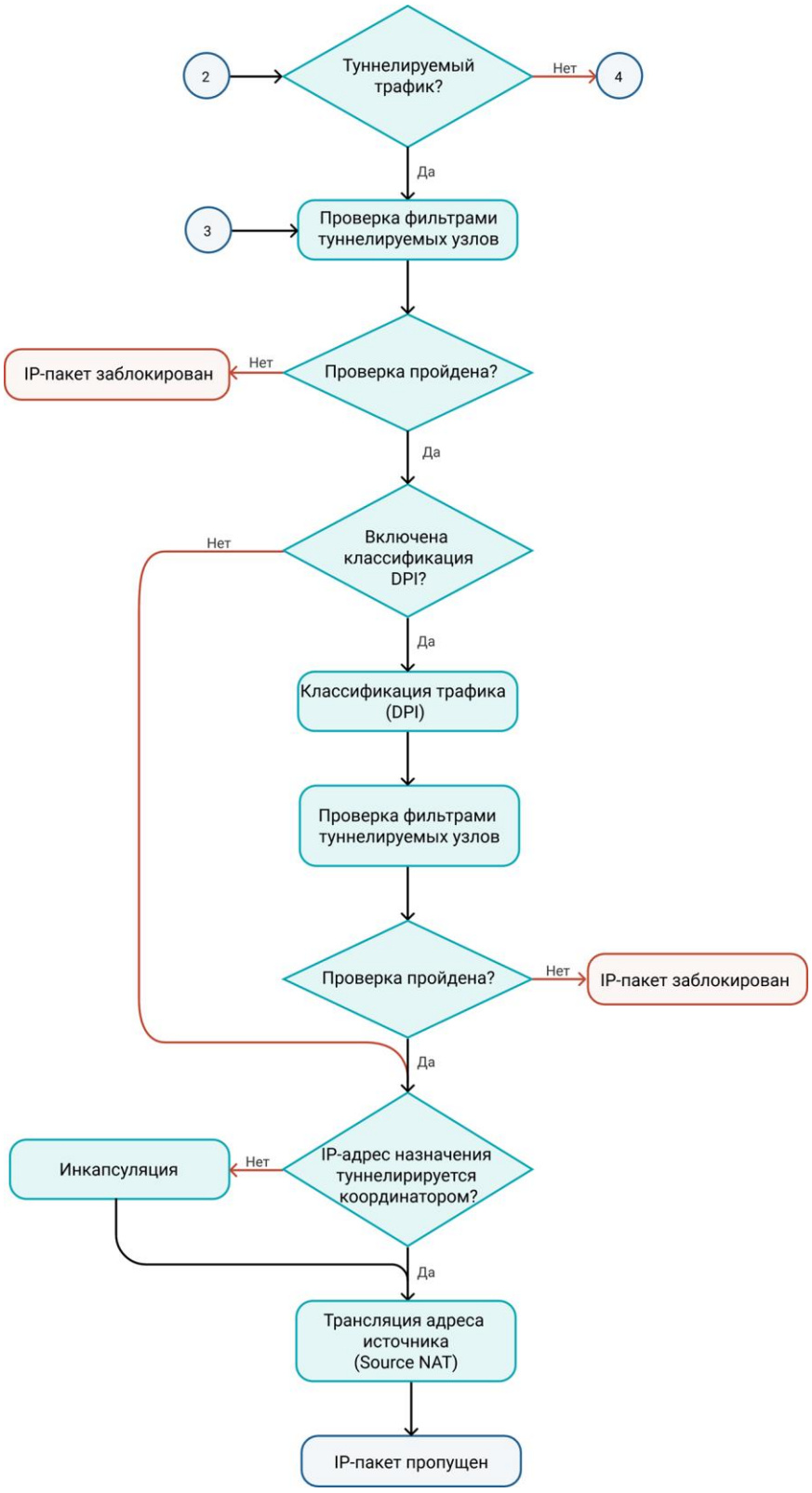


Рисунок 19. Схема фильтрации трафика. Часть 3

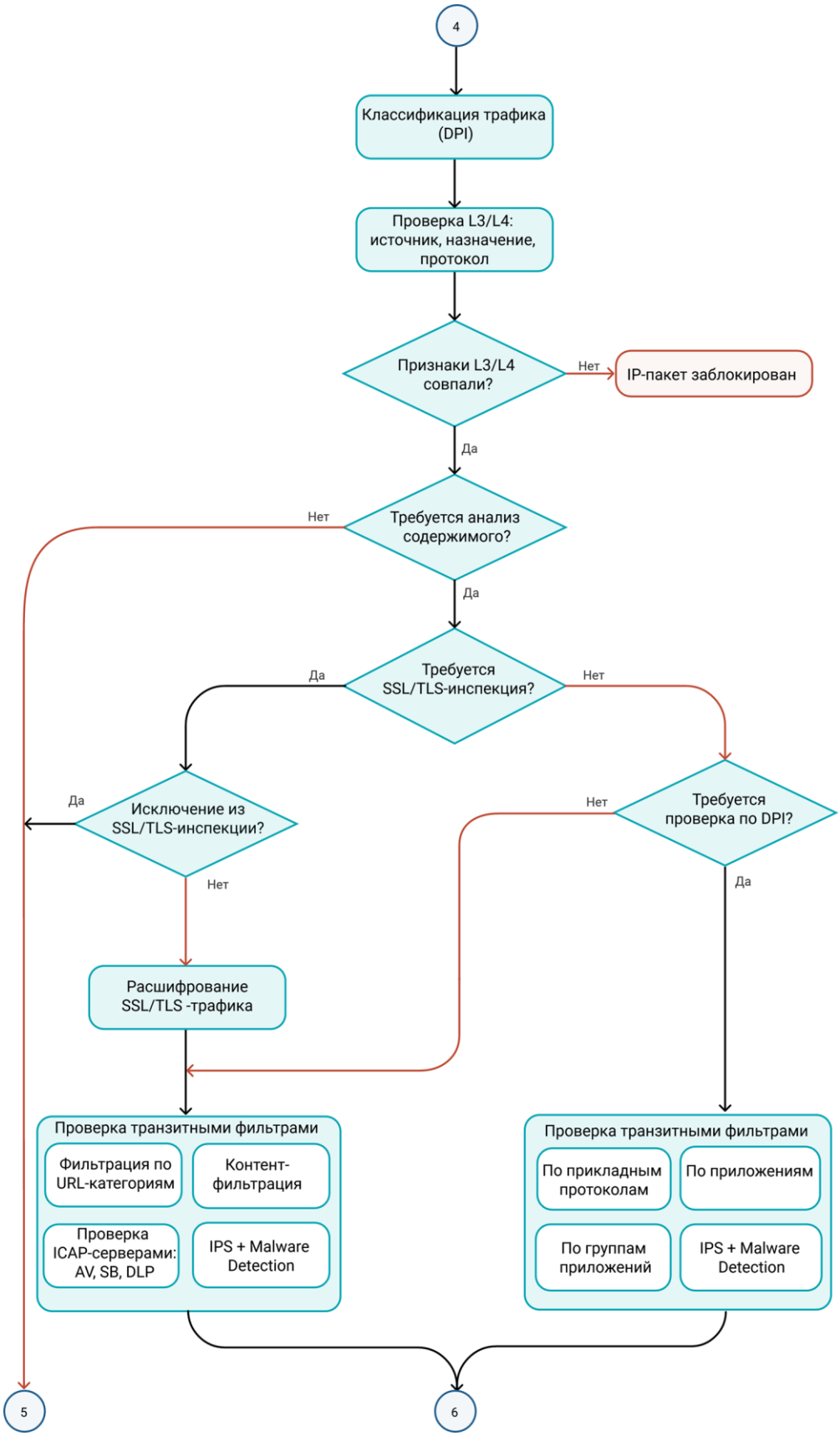


Рисунок 20. Схема фильтрации трафика. Часть 4

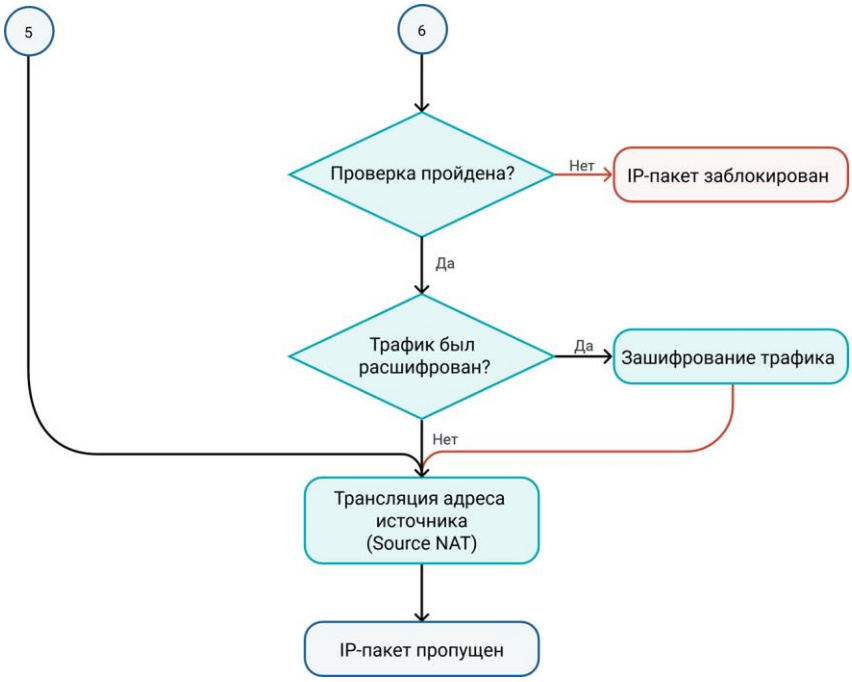


Рисунок 21. Схема фильтрации трафика. Часть 5

Настройка режима работы и параметров межсетевого экрана

Режимы работы МЭ

ViPNet Coordinator HW поддерживает три режима работы МЭ:

- `whitelist` — блокировать транзитный трафик (трафик туннелируемых узлов и транзитный трафик открытой сети), кроме разрешенного фильтрами туннелируемых узлов и транзитными фильтрами открытой сети;
- `blacklist` — пропускать транзитный трафик, не запрещенный фильтрами туннелируемых узлов и транзитными фильтрами открытой сети;
- `block` — блокировать весь трафик (трафик защищенной сети, трафик туннелируемых узлов, локальный трафик открытой сети и транзитный трафик открытой сети).

По умолчанию установлен режим `whitelist`. Чтобы переключить режим работы МЭ, выполните:

```
hostname# firewall mode {whitelist | blacklist | block}
```



Внимание! При переключении в режим блокировки всего трафика удаленный доступ к устройству по SSH и с помощью веб-интерфейса будет запрещен. Введите `Y` и нажмите **Enter**, чтобы подтвердить переключение.

Параметры МЭ

Также вы можете изменить параметры МЭ, заданные по умолчанию:

```
hostname# firewall settings <параметр> <значение>
```

Параметры и значения по умолчанию (время указано в секундах):

- `antispoofing` — антиспуфинг (по умолчанию — `off`);
- `block-fragmented-packets` — блокирование входящих фрагментированных IP-пакетов на всех сетевых интерфейсах (по умолчанию — `off`);
- `bypass-tunnel-ips-dpi` — обход обработки туннельного трафика подсистемами DPI и IPS (по умолчанию — `off`);
- `connection-ttl-ip` — время жизни соединений по протоколу IP при отсутствии в них активности (по умолчанию — 300);
- `connection-ttl-tcp` — время жизни соединений по протоколу TCP при отсутствии в них активности (по умолчанию — 1800);
- `connection-ttl-udp` — время жизни соединений по протоколу UDP при отсутствии в них активности (по умолчанию — 40);

- `connection-ttl-stream-udp` — время жизни потокового UDP-соединения (по умолчанию — 180);
- `timeout-tcp-syn-recv` — максимальное время жизни TCP-соединения в режиме ожидания установления соединения до перехода в состояние «установлено» (по умолчанию — 30);
- `timeout-tcp-syn-sent` — максимальное время жизни TCP-соединения в режиме запроса установления соединения до перехода в состояние «установлено» (по умолчанию — 60);
- `timeout-tcp-wait` — максимальное время ожидания продолжения TCP-соединения (по умолчанию — 15);
- `timeout-icmp` — время жизни ICMP-соединения (по умолчанию — 10);
- `max-connections` — максимальное количество одновременно установленных соединений (транзитных, служебных и управляющих) в зависимости от исполнения;
- `log-invalid-packet` — регистрация событий о нарушении параметров таблицы соединений в журнале IP-пакетов (по умолчанию — `off`);
- `log-queue` — регистрация событий об отклоненных IP-пакетах в журнале IP-пакетов (по умолчанию — `off`).

Просмотр настроек

Чтобы посмотреть текущие режим работы и параметры МЭ, выполните:

```
hostname# firewall settings show
```

Настройка антиспуфинга

В ViPNet Coordinator HW реализован антиспуфинг — возможность блокирования входящих IP-пакетов от отправителей, IP-адреса которых недопустимы на данном сетевом интерфейсе узла. Антиспуфинг работает как для открытого, так и для защищенного трафика. При этом открытые IP-пакеты, полученные в результате декапсуляции защищенных IP-пакетов, не проверяются антиспуфингом, так как уже не относятся к сети отправителя. Эти IP-пакеты, как и обычные открытые IP-пакеты, после проверки антиспуфингом обрабатываются сетевыми фильтрами.

Основная задача антиспуфинга — защита от сетевых атак, называемых спуфингом. При спуфинге злоумышленник посылает на какой-либо компьютер IP-пакет, в котором в качестве адреса отправителя указан не адрес злоумышленника, а адрес какого-либо другого узла, которому разрешено соединение с данным координатором. Например, таким образом можно отправить открытый пакет из интернета через координатор, задав в качестве адреса отправителя адрес частной внутренней сети, которая также подключена к данному координатору. Правила антиспуфинга позволяют исключить такую возможность.

1 По умолчанию антиспуфинг выключен. Проверьте его текущее состояние:

```
hostname# firewall settings show
Firewall mode    default
Antispoofing     off
```

...

2 Если антиспуфинг выключен, включите его для повышения уровня безопасности сети:

```
hostname# firewall settings antispoofing on
```

При включении антиспуфинга на сетевом узле на основе таблицы маршрутизации автоматически задаются правила антиспуфинга.



Внимание! При использовании сложных схем маршрутизации на узле (с метриками маршрутов или асимметричными маршрутами) функция антиспуфинга может работать некорректно.

Правила антиспуфинга применяются для открытого транзитного трафика:

- Для всех сетевых интерфейсов, кроме интерфейса, соответствующего маршруту по умолчанию, блокируются IP-пакеты, адреса отправителей которых не совпадают с адресами, маршрутизируемыми через данный интерфейс.
- Для сетевого интерфейса, соответствующего маршруту по умолчанию, блокируются IP-пакеты, адреса отправителей которых совпадают с зарегистрированными маршрутами других интерфейсов.

Пример настройки антиспуфинга

Таблица 8. Таблица маршрутизации на сетевом узле

Сетевой адрес	Маска подсети	Адрес шлюза	Интерфейс	Метрика
0.0.0.0	0.0.0.0	10.0.8.1	10.0.8.54	20
10.0.8.0	255.255.255.0	On-link	10.0.8.54	276
10.0.8.54	255.255.255.255	On-link	10.0.8.54	276
10.0.8.255	255.255.255.255	On-link	10.0.8.54	276
127.0.0.0	255.0.0.0	On-link	127.0.0.1	306
127.0.0.1	255.255.255.255	On-link	127.0.0.1	306
127.255.255.255	255.255.255.255	On-link	127.0.0.1	306
192.168.48.0	255.255.255.0	On-link	192.168.48.1	276
192.168.48.1	255.255.255.255	On-link	192.168.48.1	276
192.168.48.255	255.255.255.255	On-link	192.168.48.1	276
192.168.59.0	255.255.255.0	On-link	192.168.59.1	276
192.168.59.1	255.255.255.255	On-link	192.168.59.1	276
192.168.59.255	255.255.255.255	On-link	192.168.59.1	276
224.0.0.0	224.0.0.0	On-link	127.0.0.1	306
224.0.0.0	224.0.0.0	On-link	10.0.8.54	276

224.0.0.0	224.0.0.0	On-link	192.168.48.1	276
224.0.0.0	224.0.0.0	On-link	192.168.59.1	276
255.255.255.255	255.255.255.255	On-link	127.0.0.1	306
255.255.255.255	255.255.255.255	On-link	10.0.8.54	276
255.255.255.255	255.255.255.255	On-link	192.168.48.1	276
255.255.255.255	255.255.255.255	On-link	192.168.59.1	276

Сетевой узел имеет четыре интерфейса, один из которых с адресом 127.0.0.1 (loopback).

При включении антиспуфинга на узле будут заданы следующие правила:

- На интерфейсе с адресом 192.168.48.1 разрешены входящие пакеты только от узлов с IP-адресами 192.168.48.0/24.
- На интерфейсе с адресом 192.168.59.1 разрешены входящие пакеты только от узлов с IP-адресами 192.168.59.0/24.
- На интерфейсе с адресом 10.0.8.54 разрешены все входящие пакеты, кроме пакетов от узла с IP-адресами 192.168.48.0/24, 192.168.59.0/24.

Обработка фрагментированных IP-пакетов

ViPNet Coordinator HW при шифровании трафика добавляет к каждому IP-пакету служебный заголовок (выполняет инкапсуляцию), вследствие чего размер сформированного ViPNet-пакета может получиться больше заданного в MTU и потребует фрагментации. В свою очередь, некоторые сервисы не позволяют фрагментировать свои пакеты (например, видео-трафик), используя флаг Don't fragment (DF). В любом случае, обработка фрагментированных пакетов снижает пропускную способность сети (так как два пакета вместо одного суммарно длиннее, и их обработка требует больше ресурсов), поэтому в ViPNet Coordinator HW предусмотрены средства решения этой проблемы.

Установка TCP-соединения

На этапе установки соединения по протоколу TCP сервер и клиент обмениваются значениями MSS (максимальная длина сегмента), которые основаны на MTU их сетевых интерфейсов, и в итоге принимается минимальное из двух значений. В результате инкапсуляции IP-пакета ViPNet Coordinator HW учитывает размер, на который был увеличен IP-пакет после инкапсуляции, и уменьшает значение MSS с учетом этих данных.

Также вы можете настроить дополнительное уменьшение размера MSS с помощью команды `iplir option mss-decrease`.

Обработка IP-пакетов с флагом Don't fragment (DF)

Рассмотрим случай, когда ViPNet Coordinator HW туннелирует сетевые узлы, которые отправляют через него IP-пакеты с размером, не превышающим размер MTU, заданный на внешнем сетевом интерфейсе ViPNet Coordinator HW. При шифровании трафика размер IP-пакета может превысить MTU, и в этом случае IP-пакет будет фрагментирован.

Если же такой IP-пакет имеет флаг DF, запрещающий фрагментацию, то, в зависимости от его размера, будет выполнен один из сценариев:

- Если размер IP-пакета после инкапсуляции не превышает MTU, то ViPNet Coordinator HW его пропустит и сбросит флаг DF (который не восстановится при последующей декапсуляции).
- Если размер IP-пакета после инкапсуляции превышает MTU, то ViPNet Coordinator HW его отбросит (при этом в журнале IP-пакетов появится запись о блокировке с кодом события 97) и отправит ICMP-сообщение о необходимости фрагментации IP-пакета (ICMP type 3, code 4) его отправителю. В зависимости от настройки отправителя IP-пакетов необходимо выполнить одно из действий:
    - Если отправитель IP-пакетов с флагом DF не получает (не обрабатывает) такие ICMP-сообщения, то ему необходимо самостоятельно уменьшить размер IP-пакетов.
    - Если отправитель IP-пакетов с флагом DF принимает и корректно обрабатывает ICMP-сообщения ICMP type 3, code 4 (в соответствии с RFC 4459), то такой трафик будет пропущен.

Блокировка входящих фрагментированных пакетов

Фрагментированные IP-пакеты используются как средство сетевой атаки «отказ в обслуживании» (DDoS). В качестве меры защиты от такой атаки включите на межсетевом экране блокирование всех входящих фрагментированных IP-пакетов на всех интерфейсах с помощью команды `firewall settings block-fragmented-packets on`. Подробнее см. Настройка режима работы и параметров межсетевого экрана.

Регистрация MAC-адресов источников сессий

ViPNet Coordinator HW работает в режиме промежуточного сервера приложений и регистрирует в системном журнале MAC-адреса источников сессий (разрешенных и заблокированных). Если источник сессии расположен за сетевым устройством (NAT, маршрутизатор или прокси-сервер), регистрируется MAC-адрес этого устройства, и вместе с ним — IP-адрес источника, запрашиваемый в сессии адрес веб-ресурса (доменное имя, URL или URI) и действие (`pass` или `drop`), например:

```
Jun 24 14:26:25 2025 va100-56450057 sslsplit[7623]: 192.168.1.2 8a:47:4f:a8:c3:d8 yandex.ru/ pass.
```

Настройка аппаратной фильтрации трафика

Часть исполнений ViPNet Coordinator HW поддерживает аппаратную фильтрацию трафика, которая выполняется на физических интерфейсах, тем самым снижая загрузку ЦП устройства.

По умолчанию фильтры аппаратной фильтрации не заданы и весь трафик обрабатывается ЦП. Вы можете добавить такие фильтры, блокирующие трафик по IP-адресам отправителя и получателя и MAC-адресу отправителя непосредственно на физических интерфейсах до обработки трафика ЦП. Заданные фильтры действуют одновременно на всех физических интерфейсах, поддерживающих аппаратную фильтрацию.

Чтобы добавить фильтр, блокирующий трафик:

1 По IP-адресу отправителя или получателя:

`hostname# firewall blacklist add {src | dst} ip <адрес>`, где:

- направление:
  - `src` — отправитель;
  - `dst` — получатель;
- `<адрес>` — IP-адрес.

2 На основании MAC-адреса отправителя:

`hostname# firewall blacklist add src mac <адрес>`, где:

- направление:
  - `src` — отправитель;
- `<адрес>` — MAC-адрес.



Примечание. MAC-адрес необходимо задавать в полном формате, используя в качестве разделителя двоеточие или тире, например `40-8D-5C-4A-7D-BE`.

Чтобы просмотреть список фильтров:

```
hostname# firewall blacklist show
```

Если какой-либо фильтр более не нужен, удалите его:

- фильтр по IP-адресу:

  `hostname# firewall blacklist delete {src | dst} ip <адрес>`

- фильтр по MAC-адресу:

  `hostname# firewall blacklist delete src mac <адрес>`

Особенности аппаратной фильтрации

1. Максимальное количество аппаратных фильтров по IP- и MAC-адресам определяется исполнением ViPNet Coordinator HW.
2. Фильтры применяются только на физических интерфейсах в режимах access или slave.
3. Аппаратная фильтрация на сетевых картах Intel применяется только для входящего трафика.

Объекты сетевых фильтров и правил трансляции адресов

Системные объекты, объекты и группы объектов позволяют упростить настройку сетевых фильтров и правил трансляции адресов — их можно задавать в параметрах фильтров и правил вместо перечисления отдельных объектов. К ним относятся:

- системные объекты;
- группы объектов «ViPNet-узлы», «IP-адреса», «Интерфейсы», «Протоколы» и «Расписания» (заданы по умолчанию и их можно настраивать);
- группа объектов «Веб-клиенты» (неизменяемые, заданные по умолчанию; кроме того, можно настраивать свои группы веб-клиентов);
- группа объектов «URL-категории» (неизменяемые, из базы URL-категорий; кроме того, можно настраивать свои URL-категории);
- группа объектов «Страны» (неизменяемые, из базы GeoIP);
- группы объектов, полученные из Policy Management (модуль Prime) (их нельзя изменять и указывать в настраиваемых сетевых фильтрах и правилах трансляции).

Системные объекты

Системные объекты заданы по умолчанию. Они используются для задания адресов отправителей и получателей IP-пакетов в сетевых фильтрах и правилах трансляции адресов, а также при создании настраиваемых групп объектов (Узлы ViPNet, IP-адреса, Интерфейсы, Протоколы, Расписания). Системные объекты не отображаются в группах объектов, их нельзя ни изменить, ни удалить.

Таблица 9. Системные объекты

Имя системного объекта	Описание и область применения
`allclients` (Все клиенты)	Все клиенты, с которыми у узла есть связь. Можно использовать в фильтрах защищённой сети и фильтрах туннелируемых узлов для задания адреса отправителя для входящих соединений узла или адреса получателя для исходящих соединений узла.
`allcoordinators` (Все координаторы)	Все координаторы, с которыми у узла есть связь. Можно использовать в фильтрах защищённой сети и фильтрах туннелируемых узлов для задания адреса отправителя для входящих соединений узла или адреса получателя для исходящих соединений узла.

`broadcast` (Широковещательные адреса)	Все широковещательные адреса. Можно использовать в фильтрах защищённой сети и фильтрах открытой сети для идентификации широковещательных адресов получателей. Использование других адресов совместно с этой группой недопустимо.
`local` (Мой узел)	Собственный узел ViPNet Coordinator HW. Можно использовать в фильтрах защищённой сети и фильтрах открытой сети для задания адреса отправителя для исходящих соединений узла или адреса получателя для входящих соединений узла. Использование других адресов совместно с этой группой недопустимо.
`remote` (Другие узлы)	Другие узлы (любые, кроме собственного). Можно использовать в фильтрах защищённой сети и фильтрах открытой сети для задания адреса отправителя для входящих соединений узла или адреса получателя для исходящих соединений узла. Использование других адресов совместно с этой группой недопустимо.
`tunneledip` (Туннелируемые IP-адреса)	Все IP-адреса, туннелируемые координатором. Можно использовать в фильтрах туннелируемых узлов для задания адреса отправителя для входящих соединений узла или адреса получателя для исходящих соединений узла.
`multicast` (Групповые адреса)	Диапазон IP-адресов для групповой рассылки (224.0.0.0 – 239.255.255.255). Можно использовать в фильтрах открытой сети для задания адреса получателя. Использование других адресов совместно с этой группой недопустимо.
`any` (Любое значение)	Можно использовать в сетевых фильтрах и правилах трансляции адресов. Объект `any` обозначает: • для локальных и транзитных фильтров открытой сети — все IP-адреса; • для фильтров защищённой сети — все VPN-узлы; • для фильтров туннелируемых узлов — все IP-адреса или все VPN-узлы; • для протоколов — все протоколы; • для расписаний — все время (постоянно). Использование других условий совместно с объектом `any` недопустимо.

Группы объектов «ViPNet-узлы», «IP-адреса», «Интерфейсы», «Протоколы» и «Расписания»

Настраиваемые группы объектов:

- «ViPNet-узлы» — содержат любую комбинацию узлов сети ViPNet, используется в фильтрах защищенной сети и фильтрах туннелируемых узлов. По умолчанию не заданы.
- «IP-адреса» — содержат любую комбинацию IP-адресов, диапазонов IP-адресов и доменных имен, используется в фильтрах открытой сети, фильтрах туннелируемых узлов и правилах трансляции сетевых адресов. Состав по умолчанию:
  - `PrivateNetworkIP` (частные IP-адреса) — IP-адреса локальных сетей: 10.0.0.0/8; 172.16.0.0/12; 192.168.0.0/16;
  - `InternetIP` (публичные IP-адреса) — IP-адреса за исключением частных IP-адресов;
- «Интерфейсы» — содержат любую комбинацию сетевых интерфейсов, используется в фильтрах открытой сети и фильтрах туннелируемых узлов. По умолчанию не заданы.
- «Протоколы» — содержат любую комбинацию сетевых протоколов и портов, используется в фильтрах открытой и защищенной сетей, фильтрах туннелируемых узлов и правилах трансляции адресов. Состав см. в приложении Группы объектов «Протоколы» по умолчанию.
- «Расписания» — содержит любую комбинацию параметров, определяющих время действия сетевого фильтра, используется в фильтрах открытой и защищенной сетей, фильтрах туннелируемых узлов. Состав по умолчанию:
  - `Workdays` — рабочие дни недели (с понедельника по пятницу);
  - `Weekends` — выходные дни недели (суббота и воскресенье).

Создание группы объектов

Чтобы создать группу объектов, выполните:

`hostname# firewall <тип объектов> add name @<имя> <состав> [exclude <исключения>]`, где:

- параметр `<тип объектов>` может принимать одно из следующих значений:
  - `vpn-object` — узлы ViPNet;
  - `ip-object` — IP-адреса или доменные имена;
  - `interface-object` — сетевые интерфейсы;
  - `service-object` — протоколы;
  - `schedule-object` — расписания;
- имя группы объектов должно быть уникальным, допустимые символы: буквы (`A–Z`, `a–z`), цифры (`0–9`) и символы (`_.`);

- в параметрах `<состав>` и `<исключения>` указываются объекты, входящие в группу и исключаемые из группы соответственно, причем:
  - IP-адреса и идентификаторы узлов ViPNet указываются через запятую или в виде диапазона;
  - сетевые интерфейсы разделяются пробелом, и перед именем каждого сетевого интерфейса необходимо указать слово `interface`;
  - протоколы или расписания указываются в соответствии с синтаксисом в разделах Протокол и Расписание;
  - количество объектов в группе не должно превышать 1000.

Примеры создания групп объектов

Чтобы создать группу IP-адресов, содержащую сегмент сети за исключением нескольких IP-адресов:

```
hostname# firewall ip-object add name @IP_group_1 110.35.14.0/24 exclude
110.35.14.3,110.35.14.13
```

Чтобы создать группу расписания, содержащую выходные дни с 9 до 23 часов:

```
hostname# firewall schedule-object add name @weekend weekly sa su at 09:00-23:00
```

Чтобы создать группу сетевых интерфейсов, содержащую интерфейсы `eth0` и `eth1`:

```
hostname# firewall interface-object add name @intgroup interface eth0 interface eth1
```

Просмотр групп объектов

Чтобы просмотреть группы объектов, в том числе полученные из Policy Management (модуль Prime), выполните команду:

```
hostname> firewall <тип группы> show
```

где `<тип группы>`:

- `ip-object` — группы IP-адресов;
- `vpn-object` — группы ViPNet-узлов;
- `interface-object` — группы сетевых интерфейсов;
- `service-object` — группы протоколов;
- `schedule-object` — группы расписаний;
- `object` — все типы группы.

По каждому типу группы объектов отображаются:

- название типа группы объектов:
  - `VPN Objects` — ViPNet-узлы;

    - `Ip Objects` — IP-адреса;
    - `Interface Objects` — интерфейсы;
    - `Service Objects` — протоколы;
    - `Schedule Objects` — расписания;
- `Current Rules Set Id` — номер текущей конфигурации сетевых фильтров и правил трансляции адресов;
- `Num` — порядковый номер группы;
- `Name` — имя группы;
- `Creation Type` — тип группы:
    - `Policy` — группа из Policy Management (модуль Prime);
    - `User` — задана по умолчанию или настраиваемая группа;
- `Inclusion` — объекты, входящие в группу;
- `Exclusion` — объекты, не входящие в группу.

```
Ip Objects
Current Rules Set Id: 31
================================================================================
Num  Name                                          Creation type
Inclusion                          Exclusion
================================================================================
1    PrivateNetworkIP                              User
10.0.0.0/255.0.0.0, 172.16.0.0/
255.240.0.0, 192.168.0.0/255.255.0.0
--------------------------------------------------------------------------------
2    InternetIP                                    User
@any                               @PrivateNetworkIP
--------------------------------------------------------------------------------
Service Objects
Current Rules Set Id: 31
================================================================================
Num  Name                                          Creation type
Inclusion                          Exclusion
================================================================================
1    DHCP                                          User
udp: from 67-68 to 67-68
--------------------------------------------------------------------------------
2    CITRIX                                        User
tcp: to 1494
--------------------------------------------------------------------------------
3    DNS                                           User
udp: to 53
--------------------------------------------------------------------------------
```

Рисунок 22. Просмотр групп объектов

Удаление групп объектов

Вы можете удалить группу объектов, если она не используется в других группах объектов, сетевых фильтрах или правилах трансляции адресов.

Для удаления группы объектов выполните:

```
hostname# firewall object delete @<имя группы объектов>
```

При попытке удаления группы объектов, используемой в другой группе объектов, сетевом фильтре или правиле трансляции адресов, появится сообщение об ошибке со списком всех групп, фильтров и правил, которые используют данную группу. Удалите эти группы, фильтры и правила, затем выполните команду для удаления группы еще раз.

Группа объектов «Веб-клиенты»

В транзитных фильтрах открытой сети в качестве параметра фильтрации вы можете задавать группы веб-клиентов, содержащие строки из значений HTTP-заголовков User-Agent (далее — строки user-agent).

По умолчанию заданы группы веб-клиентов для браузеров Chrome, Edge, Firefox, Opera и Yandex:

- Chrome:
  - `Mozilla/* (*) AppleWebKit/* (*) Chrome/* Safari/*`
  - `Mozilla/* (*) AppleWebKit/* (*) CriOS/* Mobile/* Safari/*`
  - `Mozilla/* (*) AppleWebKit/* (*) Chrome/* Mobile Safari/*`
- Edge:
  - `Mozilla/*  (*) AppleWebKit/* (*) Chrome/* Safari/* Edg/*`
  - `Mozilla/* (*) AppleWebKit/* (*) Version/* EdgiOS/* Mobile/ Safari/`
  - `Mozilla/* (*) AppleWebKit/* (*) Chrome/* Mobile Safari/* EdgA/*`
- Firefox:
  - `Mozilla/* (*) Gecko/* Firefox/*`
  - `Mozilla/* (*) AppleWebKit/* (*) FxiOS/* Mobile/* Safari/*`
  - `Mozilla/* (*) Gecko/* Firefox/*`
- Opera:
  - `Mozilla/* (*) AppleWebKit/* (*) Chrome/* Safari/* OPR/*`
  - `Mozilla/* (*) AppleWebKit/* (*) Chrome/* Mobile Safari/* OPR/*`
- Yandex:
  - `Mozilla/* (*) AppleWebKit/* (*) Chrome/* YaBrowser/* Safari/*`
  - `Mozilla/ (*) AppleWebKit/* (*) Version/* YaBrowser/* Mobile/*`
  - `Mozilla/* (*) AppleWebKit/* (*) Chrome/* YaBrowser/* Mobile Safari/*`

Вы не можете изменить состав этих групп веб-клиентов или удалить их, но можете создать свои настраиваемые группы веб-клиентов.

Создание настраиваемой группы веб-клиентов

1 Создайте группу:

`hostname# firewall inspector user-agents create <имя группы>`, где

имя группы:

- допустимые символы: буквы (A–Z, a–z), цифры (0–9) и символы (. , () - _ / \);
- длина: 1–64 символа.

При выполнении команды вы можете задать описание группы длиной до 64 символов или нажать **Enter**, чтобы не указывать его.

Максимальное количество настраиваемых групп веб-клиентов — 20.

2 Добавьте в группу строки user-agent:

```
hostname# firewall inspector user-agents edit <имя группы> add
Please type user-agent expression: <строка user-agent>
```

В одной команде вы можете добавить только одну строку user-agent:

- строка должна соответствовать синтаксису HTTP-заголовка User-Agent;
- допустимые символы: буквы (A–Z, a–z), цифры (0–9), символы (`~!@#$%^&*()-_=+{}[]|\/:;"<>,.);
- символ * используется как маска в соответствии с синтаксисом HTTP-заголовка User-Agent;
- длина: 1–64 символа.

Максимальное количество строк user-agent в группе — 10.

Просмотр групп веб-клиентов

Чтобы просмотреть состав группы:

```
hostname# firewall inspector user-agents show <имя группы>
```

Помимо самих строк user-agent, отображаются их идентификаторы (ID).

Чтобы просмотреть список всех групп, выполните команду без указания имени группы.

Изменение настраиваемой группы веб-клиентов

Вы можете удалить строку user-agent из состава группы, зная ее идентификатор:

```
hostname# firewall inspector user-agents edit <имя группы> remove <идентификатор>
```

Чтобы удалить все строки user-agent группы:

```
hostname# firewall inspector user-agents edit <имя группы> clear
```

Удаление настраиваемой группы веб-клиентов

Если настраиваемая группа веб-клиентов больше не нужна, сначала удалите ее из сетевых фильтров, а затем удалите саму группу:

```
hostname# firewall inspector user-agents delete <имя группы>
```

Группа объектов «URL-категории»

В транзитных фильтрах открытой сети и фильтрах туннелируемых узлов вы можете задавать URL-категории — предварительно сформированные по определенным признакам группы адресов веб-ресурсов и масок. Используйте категории из обновляемой базы URL-категорий (см. База URL-категорий), а при необходимости создайте свои настраиваемые URL-категории.

Обновление базы URL-категорий

База URL-категорий публикуется на сервере обновления `https://updateids.infotecs.ru`, или другом, указанном в документе комплекта поставки. В нем же указаны имя пользователя и пароль на доступ к серверу обновления.

По умолчанию база URL-категорий не установлена. При наличии действующего объекта лицензирования «Обновление URL» вы можете:

- обновить базу URL-категорий с сервера, в том числе настроить обновление по расписанию;
- скачать базу URL-категорий с сервера, записать на USB-носитель и обновить вручную.

Обновление по расписанию

1 Адрес сервера обновления по умолчанию — `updateids.infotecs.ru`. Если необходимо использовать другой сервер, задайте его IP-адрес или доменное имя:

```
hostname# firewall inspector url-categories update server address <IP-адрес или доменное имя>
```

2 Задайте имя пользователя для доступа к серверу обновления базы URL-категорий:

```
hostname# firewall inspector url-categories update server login <имя пользователя>
```

3 Задайте пароль пользователя для доступа к серверу обновления базы URL-категорий:

```
hostname# firewall inspector url-categories update server password
```

4 Если политики безопасности вашей компании запрещают подключение к внешним серверам напрямую, вы можете обновлять базу URL-категорий через прокси-сервер в вашей сети:

4.1 Задайте IP-адрес или доменное имя прокси-сервера:

```
hostname# firewall inspector url-categories update proxy address <IP-адрес или доменное имя>
```

4.2 По умолчанию используется TCP-порт 3128. При необходимости измените его:

```
hostname# firewall inspector url-categories update proxy port <порт>
```

4.3 В зависимости от типа узла прокси-сервера (открытый или защищенный), создайте разрешающий сетевой фильтр (локальный фильтр открытой сети или фильтр защищенной сети), пропускающий трафик от ViPNet Coordinator HW на TCP-порт прокси-сервера.



Примечание. Чтобы вернуться к обновлению базы URL-категорий напрямую, выполните:

```
hostname# firewall inspector url-categories update proxy address none
```

5 По умолчанию обновление по расписанию выключено. Чтобы настроить расписание и включить обновление:

5.1 Задайте расписание:

```
hostname# firewall inspector url-categories update schedule <расписание>
```

В расписании вы можете указать время и день:

- `daily at <чч:мм>` — ежедневно в указанное время;
- `weekly on <день недели> at <чч:мм>` — в указанное время определенного дня недели.

5.2 Включите обновление по расписанию:

```
hostname# firewall inspector url-categories update on
```

6 Принудительно обновите базу URL-категорий:

```
hostname# firewall inspector url-categories update fetch
```

7 Просмотрите сведения о базе URL-категорий и проверьте настройки ее обновления:

```
hostname# firewall inspector url-categories update info
```

Далее база URL-категорий будет обновляться по расписанию.

Обновление с USB-носителя вручную

Если политики безопасности вашей компании запрещают подключение к внешним серверам, вы можете обновить базу URL-категорий с USB-носителя вручную:

1 Скачайте с сервера обновления и запишите на USB-носитель актуальную базу URL-категорий.

2 Обновите базу URL-категорий с USB-носителя вручную:

```
hostname# firewall inspector url-categories update usb
```

Далее отслеживайте актуальность базы URL-категорий самостоятельно и обновляйте ее с USB-носителя вручную.

Удаление базы URL-категорий

В некоторых случаях необходимо удалить базу URL-категорий:

```
hostname# firewall inspector url-categories update reset
```

После выполнения команды:

- обновление базы URL-категорий по расписанию будет выключено;
- будут сохранены настройки сервера обновления, прокси-сервера и расписания.

Настраиваемые URL-категории

По умолчанию настраиваемые URL-категории не заданы. Чтобы создать такую URL-категорию и добавить в нее ресурсы:

1 Задайте имя URL-категории:

`hostname# firewall inspector url-categories create <имя URL-категории>`, где

имя URL-категории:

- допустимые символы: буквы (A–Z, a–z), цифры (0–9) и символы (`~!@#$%^&*()-_=+{}[]|\/:;"<>,.);
- длина: 1–64 символа.

При выполнении команды вы можете задать описание описание URL-категорий длиной до 256 символов или нажать **Enter**, чтобы не указывать его.

Максимальное количество настраиваемых URL-категорий — 80.

2 Добавьте в нее адреса веб-ресурсов или маски:

`hostname# firewall inspector url-categories edit <имя> add <адрес или маска>`

В одной команде вы можете добавить только один адрес веб-ресурса или одну маску.

Допустимые символы адреса веб-ресурса:

- домена: буквы (A–Z, a–z, А–Я, а–я), цифры (0–9), символы (-.);
- URI: буквы (A–Z, a–z), цифры (0–9), символы (-._~:/?#[]@!$&'()*+,;=%);
- URL: буквы (A–Z, a–z), цифры (0–9) и символы (+.-;/?:@$_!*'());
- URN: буквы (A–Z, a–z), цифры (0–9) и символы (()+,-.:=@;$_!*'%/?#);

Строку URI, URL или URN, содержащую символ ('), необходимо заключать в двойные кавычки (").

Маска:

- допустимые символы: такие же, как в URI;
- минимальная длина без учета (.) — 3;
- использование *:
  - * в начале URI — дополняет произвольное, в том числе нулевое, количество символов до URI;
  - * в конце URI — дополняет произвольное количество символов после URI;
  - * в конце и начале URI — дополняет произвольное количество символов до и после URI;
  - * — любой адрес веб-ресурса;
  - ** — любой адрес веб-ресурса;
  - *** — поиск * в адресе веб-ресурса.

Максимальное количество адресов веб-ресурсов или масок в настраиваемой URL-категории — 500.



Внимание! При добавлении ресурса в URL-категорию необходимо учитывать все ресурсы, к которым выполняются запросы. Например, если ресурс, который определен как `*example.com*`, выполняет запросы к `static.example.org`, для корректной работы необходимо добавить оба ресурса в категорию.

3 Проверьте состав созданной URL-категории:

```
hostname# firewall inspector url-categories list <имя URL-категории>
```

4 Чтобы удалить из настраиваемой URL-категории адрес веб-ресурса или маску:

```
hostname# firewall inspector url-categories edit < URL-категории> remove <адрес или маска>
```

5 Если настраиваемая URL-категория больше не используется, удалите ее:

```
hostname# firewall inspector url-categories delete <имя URL-категории>
```

6 Чтобы просмотреть список всех URL-категорий, как настраиваемых, так и из базы URL-категорий:

```
hostname# firewall inspector url-categories list
```



Примечание. При задании настраиваемой URL-категории в сетевом фильтре перед именем необходимо добавлять символ `#`, например `#myurlcat`. Подробнее см. URL-категория.

Фильтрация по URL-категориям в содержимом веб-страниц

Вы можете настроить автоматическое удаление ссылок на определённые ресурсы в содержимом веб-страниц. Для этого добавьте адреса ресурсов в URL-категорию и укажите её в блокирующем сетевом фильтре.

По умолчанию фильтрация включена.

Чтобы настроить фильтрацию ссылок в содержимом веб-страниц:

1 Создайте URL-категорию и добавьте ресурсы, доступ к которым нужно заблокировать:

```
firewall inspector url-categories create VideoServices
firewall inspector url-categories edit VideoServices add *rutube.ru*
```

2 Добавьте сетевой фильтр, запрещающий трафик для URL-категории, например:

```
firewall forward add 1 rule "Block Video Services" src 172.16.0.0/24 dst @any url-category #VideoServices ssl decrypt drop
```

3 Проверьте настройку фильтрации:

```
firewall inspector url-categories secure-content show
```

Если фильтрация включена, отображается `Content inspection for blocked URL categories is ON`.

Если фильтрация выключена, выполните:

```
firewall inspector url-categories secure-content on
```

После настройки на веб-странице не будут открываться ссылки на заблокированные ресурсы URL-категории.

Группа объектов «Страны»

В локальных и транзитных фильтрах открытой сети в качестве адресов отправителя и получателя IP-пакетов вы можете задавать объекты группы «Страны» (коды стран Alpha 2 или числовые коды в соответствии с ISO-3166), содержащиеся в базе GeoIP. База публикуется на сервере обновления `https://updateids.infotecs.ru`, или другом ресурсе, указанном в документе комплекта поставки. В нем же указаны имя пользователя и пароль на доступ к серверу обновления. По умолчанию установлена база GeoIP из состава дистрибутива ViPNet Coordinator HW.

Чтобы поддерживать базу GeoIP в актуальном состоянии, обновляйте базу с USB-носителя вручную:

1. Просмотрите сведения о базе GeoIP:

   ```
   hostname# service geoip show status
   ```

2. Скачайте с сервера обновления и запишите на USB-носитель актуальную базу GeoIP (файл базы формата `*.tar.gz` и файл ЭП формата `*.tar.gz.sig`).

3. Обновите базу GeoIP с USB-носителя:

   ```
   hostname# service geoip update usb
   ```

При необходимости вы можете восстановить базу GeoIP до версии, поставляемой в составе дистрибутива ViPNet Coordinator HW:

```
hostname# service geoip restore-default
```

Списки исключений и добавлений IP-адресов стран

Для каждой страны вы можете настроить список исключений и дополнений IP-адресов. При фильтрации трафика IP-адрес отправителя или получателя сначала проверяется по этому списку. Если IP-адреса нет в списке, то проверка продолжается по IP-адресам страны, содержащимся в базе GeoIP. Обновление или восстановление базы GeoIP не влияет на списки исключений и дополнений IP-адресов стран. По умолчанию списки исключений и дополнений IP-адресов стран не настроены.

Чтобы добавить IP-адреса в список страны, выполните:

```
hostname# service geoip <страна> add {exclusion | inclusion} <адреса>
```

где:

- `<страна>` — ISO 3166-1 alpha-2 код страны;
- `exclusion` — добавить адреса как исключения IP-адресов страны;
- `inclusion` — добавить адреса как дополнения IP-адресов страны;
- `<адреса>` — IP-адреса:

- одиночные IP-адреса;
- диапазоны IP-адресов;
- подсети в нотации CIDR;
- одиночные IP-адреса, диапазоны IP-адресов, подсети или их сочетания, указанные через запятую.

Чтобы исключить IP-адреса, ранее добавленные в список, выполните:

```
hostname# service geoip <страна> delete {exclusion | inclusion} <адреса>
```

где:

- `exclusion` — удалить адреса–исключения IP-адресов страны;
- `inclusion` — удалить адреса–дополнения IP-адресов страны.

Чтобы просмотреть список исключений и добавлений IP-адресов страны, выполните:

```
hostname# service geoip <страна> show [exclusion | inclusion]
```

Настройка SSL/TLS-инспекции трафика

ViPNet Coordinator HW может инспектировать транзитный SSL/TLS-трафик между узлами сети, расположенными за ViPNet Coordinator HW, и внешними ресурсами, а именно — идентифицировать SSL/TLS-сессии с помощью DPI и расшифровывать их, используя для этого SSL-сертификат, которым подписываются сертификаты при встраивании в сессии. По умолчанию параметры SSL/TLS-инспекции заданы, но при необходимости вы можете изменить их:

- Настройка основных параметров SSL/TLS-инспекции.
- Настройка исключений из SSL/TLS-инспекции.
- Настройка SSL-сертификата.

Последовательность SSL/TLS-инспекции трафика см. в разделе Принципы фильтрации трафика на рисунке «Схема фильтрации трафика. Часть 4».

Чтобы использовать SSL/TLS-инспекцию в фильтрации транзитного трафика, создайте транзитные фильтры открытой сети с указанием параметра SSL/TLS-инспекции и параметров фильтрации:

- URL-категории;
- URL-адрес веб-ресурса, в том числе MIME-тип передаваемых данных и метод HTTP-запроса;
- проверка на ICAP-серверах:
  - антивирусная проверка;
  - проверка в песочнице;
  - проверка в DLP-системе.
- проверка IPS, в том числе Malware Detection.

Настройка основных параметров SSL/TLS-инспекции

1 Измените инспектируемые протоколы:

```
hostname# firewall inspector ssl-decryption protocols {allow-all | <протокол> {allow | block}}
```

Особенности настройки:

- По умолчанию разрешены все протоколы: `ssl3`, `tls10`, `tls11`, `tls12`, `tls13`.

- В одной команде вы можете указать только один протокол и действие с ним (`allow` — разрешить, `block` — запретить).
- Чтобы разрешить все протоколы, укажите `allow-all`.
- Должен быть разрешен минимум один протокол.
- Трафик запрещенных протоколов блокируется.
- Использование устаревших протоколов `ssl3`, `tls10`, `tls11` потенциально небезопасно. Чтобы ViPNet Coordinator HW блокировал их трафик:
  - запретите инспекцию этих протоколов:

    ```
    hostname# firewall inspector ssl-decryption protocols ssl3 block
    hostname# firewall inspector ssl-decryption protocols tls10 block
    hostname# firewall inspector ssl-decryption protocols tls11 block
    ```

  - и выключите их в исключениях SSL/TLS-инспекции (см. Настройка исключений из SSL/TLS-инспекции).
- Сетевой узел, устанавливающий соединений с внешним ресурсом через ViPNet Coordinator HW, поддерживает свой набор протоколов `ssl3`, `tls10`, `tls11`, `tls12`, `tls13`. Если вы запрещаете какой-либо из них на ViPNet Coordinator HW, то узел не сможет установить соединение с помощью этого протокола, но попытается установить соединение с помощью других протоколов своего набора.
- Из-за особенностей встраивания в сессию корневого SSL-сертификата для `ssl3` также должен быть разрешен `tls10`.

2 Измените алгоритмы (обмена ключами, шифрования, хэширования) и наборы шифров для протокола TLS:

```
hostname# firewall inspector ssl-decryption algorithms {allow-all | {<алгоритм> |
<набор шифров> {allow | block}}}
```

Особенности настройки:

- По умолчанию разрешены все алгоритмы и наборы шифров:
  - алгоритмы обмена ключами: `RSA`, `DHE`, `ECDHE`;
  - алгоритмы шифрования: `3DES`, `RC4`, `AES`, `AES128`, `AES256`, `AESGCM`;
  - алгоритмы хэширования: `MD5`, `SHA1`, `SHA256`, `SHA384`;
  - наборы шифров TLS 1.2: `TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256`, `TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256`, `TLS_RSA_WITH_AES_256_GCM_SHA384`, `TLS_RSA_WITH_AES_128_GCM_SHA256`, `TLS_DHE_DSS_WITH_AES_256_GCM_SHA384`, `TLS_DHE_RSA_WITH_AES_256_GCM_SHA384`, `TLS_DHE_DSS_WITH_AES_128_GCM_SHA256`, `TLS_DHE_RSA_WITH_AES_128_GCM_SHA256`, `TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384`, `TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384`;
  - наборы шифров TLS 1.3: `TLS_AES_256_GCM_SHA384`, `TLS_AES_128_GCM_SHA256`.
- В одной команде вы можете задать только одно значение параметра `<алгоритм>` или `<набор шифров>` и действие с ним (`allow` — разрешить, `block` — запретить).

- Чтобы разрешить все алгоритмы и наборы шифров, укажите `allow-all`.
- Необходимо разрешить минимум по одному алгоритму из групп обмена ключами, шифрования и хэширования.
- Трафик, в котором используются запрещенный алгоритмы и наборы шифров, блокируется.
- В названиях алгоритмов и наборов шифров разрешены строчные и прописные буквы латинского алфавита.
- Если протокол TLS 1.2 запрещен, то заданные наборы шифров TLS 1.2 не используется.
- Если наборы шифров TLS 1.3 запрещены, то трафик TLS 1.3 не будет расшифровываться, даже если протокол TLS 1.3 разрешен.

3 Измените действие с инспектируемой SSL/TLS-сессией:

```
hostname# firewall inspector ssl-decryption option <параметр> <действие>
```

Особенности настройки:

- Обработка сессии выполняется до расшифрования ее трафика на основании сертификата.
- Действия по умолчанию:
  - сессия с двухсторонним TLS (`client-auth`) — `bypass` (пропускать без инспекции);
  - сессия с просроченным сертификатом (`expired-cert`) — `block` (блокировать);
  - сессия с сертификатом, не предназначенный для аутентификации (`not-intended`) — `block`;
  - сессия с самоподписанным сертификатом (`self-signed`) — `block`.
- Возможные действия:
  - для `client-auth` — `block` и `bypass`;
  - для `expired-cert`, `not-intended` и `self-signed` — `block` и `allow` (инспектировать).

4 Проверьте настройку общих параметров SSL/TLS-инспекции:

```
hostname# firewall inspector ssl-decryption show
```

Настройка исключений из SSL/TLS-инспекции

ViPNet Coordinator HW поддерживает работу с исключениями SSL/TLS-инспекции — протоколами и ресурсами, которые обрабатываются до расшифрования трафика. Если протокол или ресурс добавлен в исключения, то их трафик не инспектируется. По умолчанию из инспекции исключены устаревшие протоколы SSL 3, TLS 1.0 и TLS 1.1. В список исключений ресурсов по умолчанию добавлены адреса ресурсов, как правило, не требующих инспекции, например, `microsoft.com`, `google.com`, `apple.com` и другие. Вы не можете удалить эти ресурсы. В дополнение к ним, в список исключений вы можете добавить свои настраиваемые ресурсы. Кроме адресов ресурсов для работы исключений необходимы сертификаты этих ресурсов, для получения которых ViPNet Coordinator HW должен иметь доступ к интернету. Для всех ресурсов списка вы можете настроить

обработку ресурсов по их альтернативным именам (SAN), указанным в сертификатах, и расписание обновления сертификатов.

Чтобы настроить исключения из SSL/TLS-инспекции:

1 По умолчанию инспектируется (`off`) трафик протоколов `tls12, tls13`. При необходимости измените исключения протоколов:

```
hostname# firewall inspector ssl-decryption exclusion protocols {<протокол> {on | off}}
```

где:

- `<протокол>` — один из протоколов: `ssl3`, `tls10`, `tls11`, `tls12`, `tls13`;
- `on` — исключить протокол (инспекция не проводится, нерасшифрованный трафик пропускается);
- `off` — не исключать протокол (инспекция проводится).



Внимание! Использование устаревших протоколов `ssl3`, `tls10`, `tls11` потенциально небезопасно.

2 Проверьте наличие сертификатов ресурсов по умолчанию:

```
hostname# firewall inspector ssl-decryption exclusion list default
Default:
Ssl-decryption exclusion ON
activation.sls.microsoft.com
.
```

Если сертификат загружен, строка ресурса должна иметь вид:

```
activation.sls.microsoft.com [O=Microsoft Corporation]
```

3 Если сертификаты отсутствуют, загрузите их вручную:

```
hostname# firewall inspector ssl-decryption exclusion update fetch
```

4 Включите нужные ресурсы списка исключений, заданного по умолчанию, чтобы пропускать их трафик без инспекции:

```
hostname# firewall inspector ssl-decryption exclusion set <адрес> on
```

5 При необходимости добавьте свои настраиваемые ресурсы в список исключений:

5.1 Добавьте ресурс в список исключений:

```
hostname# firewall inspector ssl-decryption exclusion add <адрес>
```

где `<адрес>` — доменное имя или маска.

Примечание. Доменное имя может состоять из букв (`A-Z`, `a-z`), цифр (`0-9`) и символов (`-` `.`). Маска позволяет задать несколько схожих доменных имен:

- состоит из символов доменного имени и символа (`*`);
- `*` означает произвольное количество символов;
- минимальное количество символов в маске, включая `*` — 5.

При добавлении ресурс должен быть доступен.

5.2 Включите его в списке исключений:

```
hostname# firewall inspector ssl-decryption exclusion set <адрес> on
```

5.3 Чтобы удалить ресурс из списка исключений:

```
hostname# firewall inspector ssl-decryption exclusion delete <адрес>
```

5.4 Проверьте настраиваемые ресурсы списка исключений:

```
hostname# firewall inspector ssl-decryption exclusion list user
```

6 По умолчанию обновление сертификатов ресурсов списка исключений по расписанию отключено (`off`). Задайте расписание обновления сертификатов или обновляйте их вручную:

```
hostname# firewall inspector ssl-decryption exclusion update {fetch | <время> [day <день>]}
```

где:

- `fetch` — обновить сертификаты вручную;
- `<время>` — время обновления в формате `<hh:mm>`, где `hh` – часы, `mm` – минуты;
- `<день>` — один из дней недели: `Sunday`, `Monday`, `Tuesday`, `Wednesday`, `Thursday`, `Friday`, `Saturday`.

7 Чтобы не исключать из SSL/TLS-инспекции все ресурсы списка исключений по альтернативным именам (по умолчанию — `on`):

```
hostname# firewall inspector ssl-decryption exclusion san off
```

8 Чтобы просмотреть текущие параметры исключений SSL/TLS-инспекции:

```
hostname# firewall inspector ssl-decryption exclusion show
```

Настройка SSL-сертификата

По умолчанию в качестве SSL-сертификата, которым подписываются сертификаты, встраиваемые в SSL/TLS-сессии, используется самоподписанный сертификат ViPNet Coordinator HW.

Чтобы браузеры или другие приложения не выдавали предупреждение о подмене сертификата, установите SSL-сертификат в хранилище сертификатов каждого сетевого узла (или приложения), SSL/TLS-трафик которого вы хотите инспектировать:

1 Экспортируйте на USB-носитель сертификат, используемый для расшифровки трафика:

```
hostname# firewall inspector ssl-decryption export-cert
```

2 Скопируйте сертификат с USB-носителя на все узлы пользователей, чей SSL/TLS-трафик вы хотите анализировать.

3 Установите SSL-сертификат в хранилище сертификатов на каждом узле.

В качестве SSL-сертификата вы также можете использовать сторонний сертификат, подписанный удостоверяющим центром (УЦ):

1 Проверьте поле `keyUsage` и поле `cA` расширения `BasicConstraints` стороннего сертификата:

   - `keyUsage = critical, keyCertSign`
   - `BasicConstraints: cA = TRUE`

   Если значения полей отличаются, используйте другой сторонний сертификат.

2 Импортируйте сторонний сертификат и его закрытый ключ в локальное хранилище сертификатов ViPNet Coordinator HW.

```
hostname# service cert import
```

Примечание.

- Поддерживается импорт файлов с расширениями `*.pem` и `*.cer`.
- Если в локальном хранилище нет корневого сертификата УЦ, которым подписан сторонний сертификат, также импортируйте и его.

3 Выберите сторонний сертификат в качестве SSL-сертификата:

```
hostname# firewall inspector ssl-decryption cert <имя файла сертификата>
```

4 Установите в хранилище сертификатов сетевых узлов SSL-сертификат и корневой сертификат УЦ (если отсутствует).

Чтобы заново использовать в качестве SSL-сертификата самоподписанный сертификат ViPNet Coordinator HW:

```
hostname# firewall inspector ssl-decryption recreate-cert
```

Учитывайте, что при выполнении команды самоподписанный сертификат будет перевыпущен, поэтому экспортируйте его на USB-носитель и установите в хранилище сертификатов сетевых узлов.

Особенности SSL/TLS-инспекции

- Сетевые фильтры с SSL/TLS-инспекцией рекомендуется располагать в конце списка фильтров.
- В текущей версии ViPNet Coordinator HW встраивание в SSL/TLS-сессию и срабатывание запрещающего правила фиксируется в системном журнале.
- К исключенным из SSL/TLS-инспекции ресурсам не применяются правила межсетевого экрана. Если ресурс или протокол исключен из инспекции, то его трафик считается доверенным и будет пропускаться без дальнейшей обработки межсетевым экраном. При этом трафик пропускается:

- только в том случае, если создан сетевой фильтр, который содержит параметр SSL/TLS-инспекции (см. SSL/TLS-инспекция);
- только для тех узлов, для которых в таком фильтре совпадают критерии L3/L4 (адрес отправителя и адрес получателя), если они заданы.

- Возможна некорректная работа исключений SSL/TLS-инспекции для ресурсов с часто меняющимися сертификатами, например `google.com`.
- Возможна некорректная работа SSL/TLS-инспекции для ресурсов, которые используются для обновления ПО, например серверов обновления Microsoft: `https://*.update.microsoft.com`.
- Одновременно с SSL/TLS-инспекцией в сетевых фильтрах не поддерживаются:
  - фильтрация по признакам, которые обрабатываются системой DPI: **Приложения** (`dpiapp`), **Группы приложений** (`dpigroup`) и **Прикладные протоколы** (`dpiprotocol`).
  - фильтрация по действительному IP-адресу прокси-клиента (`proxy-client`);
  - фильтрация по группам объектов «Веб-клиенты» (`user-agent`);
  - действие отклонить (`reject`).
- SSL/TLS-инспекция может быть неприменима для трафика мобильных приложений:
  - Некоторые браузеры не используют системное хранилище сертификатов, поэтому они не доверяют сертификатам, встраиваемым в SSL/TLS-сессии и подписанным SSL-сертификатом ViPNet Coordinator HW. Если это поддерживается браузером, вы можете установить SSL-сертификат в хранилище сертификатов. Иначе рекомендуется использовать другой браузер или исключить необходимые ресурсы из инспекции.
  - Инспекция трафика мобильных приложений, которые используют механизмы противодействия перехвату трафика (например, SSL Pinning), приводит к недоступности сервиса. В этом случае рекомендуется исключить такие ресурсы из инспекции.
- Некоторые ресурсы вместо транспортного протокола TCP и SSL/TLS-шифрования могут использовать протокол QUIC. SSL/TLS-инспекция трафика таких ресурсов не поддерживается. Чтобы обеспечить инспекцию таких сессий, вы можете:
  - Отключить использование протокола QUIC в браузере.
  - Создать сетевой фильтр для блокировки протокола QUIC:

    ```
    hostname# firewall forward add 1 src @any dst @any dpiprotocol QUIC drop
    ```
- Не поддерживается SSL/TLS-инспекция сессий с двусторонней TLS-аутентификацией сервера и клиента (Mutual TLS). Чтобы разрешить взаимодействие сетевых узлов, которые используют двустороннюю аутентификацию, вы можете:
  - Отключить SSL/TLS-инспекцию в сетевом фильтре, разрешающем прохождение трафика между этими узлами.
  - Добавить эти узлы в список исключений SSL/TLS-инспекции.

Настройка подключения к ICAP-серверам

Внимание!

Необходимо обеспечить доверенный канал передачи данных между ViPNet Coordinator HW и внешними системами (в том числе взаимодействующими системами защиты информации других типов), например выделенный физический канал или сеть ViPNet. Допускается осуществлять защиту каналов передачи данных организационными мерами, исключающими возможность утечки или перехвата защищаемых данных, или с помощью сертифицированных средств криптографической защиты информации.

ViPNet Coordinator HW поддерживает взаимодействие с внешними ICAP-серверами в режимах инспекции и репликации HTTP-трафика.

Режим инспекции трафика

В режиме инспекции трафика ICAP-сервер выполняет одну из проверок, соответствующую его типу:

- антивирусную проверку;
- проверку в песочнице (Sandbox-системе);
- проверку в DLP-системе (предотвращение утечек информации).

Проверена совместимость ViPNet Coordinator HW по протоколу ICAP с внешними системами, указанными в таблице ниже. Также возможна работа с другими системами, которые поддерживают взаимодействие по протоколу ICAP.

Таблица 10. Внешние системы, с которыми проверено взаимодействие

Тип	Название	Производитель
Антивирус	Kaspersky Web Traffic Security	АО «Лаборатория Касперского»
Песочница (Sandbox-система)	AVSOFT ATHENA	ООО «АВ Софт»
DLP-система	SearchInform КИБ	ООО «СёрчИнформ»

Проверки задаются в транзитных фильтрах открытой сети. В одном фильтре вы можете указать только один тип проверки.

Одновременно вы можете использовать несколько ICAP-серверов разных типов. При этом трафик пересылается на все из них. В случае, если используется несколько серверов одного типа, ViPNet Coordinator HW ожидает получение ответа:

- если трафик пропущен — от всех из них;
- если трафик заблокирован — от первого ответившего ICAP-сервера.

В зависимости от ответа срабатывают транзитные фильтры открытой сети.

Также вы можете настроить предварительную проверку трафика ICAP-сервером на основании части сообщения, что позволяет увеличить скорость обработки трафика МЭ.



Внимание! При обнаружении вируса проверяемый файл может быть скачан частично из-за особенности потоковой проверки. При этом скачанный фрагмент файла не несет угрозы.

Режим репликации трафика

В режиме репликации трафик пересылается на ICAP-сервер без ожидания ответа от него.

Настройка подключения к ICAP-серверу

1 Добавьте ICAP-сервер: задайте имя и тип ICAP-сервера, выберите режим взаимодействия с ICAP-сервером и укажите IP-адрес ICAP-сервера:

```
hostname# firewall inspector icap-server add <имя> type {av | sandbox | dlp} response {required | ignore} address <адрес>
```

- Тип ICAP-сервера:
  - `av` — антивирус;
  - `sandbox` — песочница;
  - `dlp` — DLP-система.
- Режим `required` (переслать и ожидать ответ ICAP-сервера) предназначен для инспекции трафика, режим `ignore` (переслать) — для репликации трафика.

2 Для ICAP-сервера в режиме `required` задайте дополнительные параметры:

```
hostname# firewall inspector icap-server <имя> option <параметр> <значение>
```



Примечание. В одной команде вы можете задать только один параметр ICAP-сервера. Чтобы задать несколько параметров, выполните команды последовательно с каждым из них.

- `tcp-port` — TCP-порт подключения к ICAP-серверу;



Примечание. Чтобы на одном IP-адресе или доменном имени использовать ICAP-серверы разных типов, задайте для них разные номера TCP-портов.

- `preview-size` — максимальный размер сообщения в байтах, передаваемого на ICAP-сервер в режиме предварительной проверки;
- `response-time` — период проверки доступности ICAP-сервера;
- `bypass` — обработка трафика, если ICAP-сервер недоступен;

- `description` — описание ICAP-сервера;
- `reqmod-mode` — режим модификации запроса;
- `reqmod-path` — путь к ICAP-серверу в режиме модификации запроса reqmod;
- `respmod-mode` — режим модификации ответа;
- `respmod-path` — путь к ICAP-серверу в режиме модификации ответа respmod;
- `username` — передача имени пользователя на ICAP-сервер;
- `header-username` — имя заголовка, используемого для передачи имени пользователя на ICAP-сервер;
- `user-ip-address` — передача IP-адреса пользователя на ICAP-сервер;
- `header-user-ip` — имя заголовка, используемого для передачи IP-адреса пользователя на ICAP-сервер;
- `user-mac-address` — передача MAC-адреса пользователя на ICAP-сервер;
- `header-user-mac` — имя заголовка, используемого для передачи MAC-адреса пользователя на ICAP-сервер.

3 Проверьте параметры ICAP-сервера:

```
hostname# firewall inspector icap-server show <имя>
```

4 Включите передачу трафика на ICAP-сервер:

```
hostname# firewall inspector icap-server <имя> state on
```

Изменение дополнительных параметров ICAP-сервера

При изменении дополнительных параметров подключенного сервера учитывайте:

- При смене режима взаимодействия с ICAP-сервера (`icap-response`) с `ignore` на `required` необходимо задать тип ICAP-сервера (`type`) и настроить нужные сетевые фильтры.
- При смене типа ICAP-сервера (`type`) необходимо заново настроить сетевые фильтры, в которых заданы параметры инспекции, определяемые изменяемыми типами.
- При включении режимов `reqmod-mode` и `respmod-mode` необходимо задать соответствующий для режима путь к ICAP-серверу.

Удаление подключения к неиспользуемому ICAP-серверу

Если ICAP-сервер более не используется, удалите его:

```
hostname# firewall inspector icap-server delete <имя>
```

Настройка сетевых фильтров

Общие сведения о сетевых фильтрах

Типы фильтров

Фильтры различаются по типу IP-трафика (защищенный, туннелируемый, открытый локальный и транзитный), который они обрабатывают:

- Фильтры защищенной сети — разрешают или блокируют обмен IP-трафиком с узлами сети ViPNet, с которыми ViPNet Coordinator HW имеет связь.
- Фильтры туннелируемых узлов — разрешают или блокируют IP-трафик между туннелируемыми узлами и узлами сети ViPNet, с которыми ViPNet Coordinator HW имеет связь.
- Локальные фильтры открытой сети — разрешают или блокируют IP-трафик между ViPNet Coordinator HW и открытыми узлами.
- Транзитные фильтры открытой сети — разрешают или блокируют IP-трафик между открытыми (или открытым и защищенным) узлами, проходящий через ViPNet Coordinator HW.

Также фильтры разделяются на группы:

- Служебные фильтры — предустановленные фильтры, применяющиеся первыми при обработке IP-пакета; недоступны для изменения пользователем.
- Фильтры политик безопасности — фильтры и правила трансляции адресов в составе политик безопасности Policy Management (модуль Prime); применяются немедленно после поступления политик на ViPNet Coordinator HW; недоступны для изменения пользователем.
- Настраиваемые фильтры — фильтры, предустановленные по умолчанию и фильтры, создаваемые пользователем; доступны для изменения пользователем.
- Блокирующий фильтр по умолчанию; недоступен для изменения пользователем.

Порядок применения фильтров

Сетевые фильтры применяются в порядке, указанном на рисунке ниже.

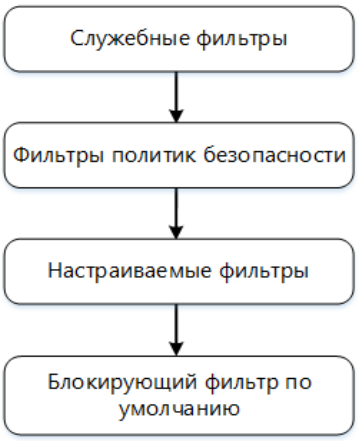


Рисунок 23. Порядок применения фильтров

Настройка сетевых фильтров

В настраиваемых сетевых фильтрах вы можете задать следующие параметры:

- адрес отправителя и получателя IP-пакетов, на которые действует фильтр;
- протоколы, используемые для передачи этих IP-пакетов: TCP, UDP, ICMP, IP и группы протоколов;
- для транзитного фильтра открытой сети и фильтра туннелируемых узлов:
  - приложения;
  - прикладные протоколы;
  - группы приложений и прикладных протоколов;
  - пользователи Active Directory или Captive Portal;
  - фильтрация по URL-категориям;
- расписание применения фильтра — ежедневно, еженедельно или по календарю;
- для транзитного фильтра открытой сети:
  - SSL/TLS-инспекция трафика;
  - проверка IPS;
  - проверку на ICAP-серверах (только в настройке с помощью командного интерпретатора):
    - антивирусная проверка;
    - проверка в песочнице;
    - проверка в DLP-системе;
  - контентная фильтрация с указанием URL-адреса веб-ресурса, HTTP-метода и MIME-типа;
  - фильтрация по действительному IP-адресу прокси-клиента;

    - фильтрация по группам объектов «Веб-клиенты»;
- регистрация IP-пакетов при срабатывании фильтра;
- регистрация сессий при срабатывании фильтра;
- действие, применяемое к IP-пакетам:
    - блокировать;
    - пропускать;
    - отклонить и отправить ICMP-уведомление.

Эти параметры вы можете использовать при настройке фильтра как с помощью командного интерпретатора, так и с помощью веб-интерфейса.

Максимальное количество сетевых фильтров зависит от исполнения ViPNet Coordinator HW (см. документ «Подготовка к работе», раздел «Рекомендованное количество сетевых фильтров»).

Подсчет срабатываний фильтров

Для каждого фильтра ведется постоянный подсчет срабатываний, начиная с момента первого включения ViPNet Coordinator HW до первого сброса срабатываний из ViPNet Prime вручную, и далее — между сбросами срабатываний из ViPNet Prime. Перезагрузка ViPNet Coordinator HW, обновление ПО или переключение узлов кластера не влияют на подсчет срабатываний. Просмотр срабатываний фильтров доступен только в веб-интерфейсе ViPNet Coordinator HW.

Создание сетевого фильтра

Для каждого типа трафика создаются отдельные сетевые фильтры, которые хранятся в соответствующей таблице (см. Просмотр сетевых фильтров).

Чтобы создать сетевой фильтр, выполните команду:

```
hostname# firewall <тип> add [<номер>] [rule <имя>] src <адрес отправителя> dst <адрес получателя> [<транспортный протокол>] [dpiapp <приложение>] [dpiprotocol <прикладной протокол>] [dpigroup <группа приложений>] [dnuser <пользователь>] [<расписание>] [url-category <url-категория>] [ssl {decrypt | bypass}] [ips {on | off}] [av {on | off}] [sb {on | off}] [dlp {on | off}] [url <url-адрес> [type <mime-тип>] [mthd <http-метод>]] [proxy-client <IP-адрес>] [user-agent <веб-клиенты>] [log {on | off}] [sessions {on | off} [state {all | begin_end | begin}]] <действие>
```

указав следующие параметры:

- `<тип>` — тип фильтра:
    - `vpn` — фильтр защищенной сети.
    - `tunnel` — фильтр туннелируемых узлов.
    - `local` — локальный фильтр открытой сети.
    - `forward` — транзитный фильтр открытой сети.

Примечание. Применение блокирующего фильтра защищенной сети, либо блокирующего локального фильтра открытой сети, либо блокирующего фильтра туннелируемых узлов к установленному соединению не блокирует его работу до истечения времени жизни соединения. После этого при попытке повторного соединения на него уже будет действовать новый блокирующий фильтр.

Блокирующий транзитный фильтр открытой сети действует сразу после его применения. Если разрешенное ранее соединение попадает под действие блокирующего транзитного фильтра, то оно будет заблокировано сразу, не дожидаясь истечения времени жизни соединения.

- `<номер>` — порядковый номер сетевого фильтра в таблице, определяющий его приоритет. Чем меньше номер, тем выше приоритет фильтра (наиболее приоритетный фильтр имеет номер 1). Если заданный номер меньше максимального номера в таблице фильтров, номера фильтров, следующих за новым фильтром, автоматически увеличиваются на единицу (их приоритет понижается).
- `<имя>` — имя сетевого фильтра. Если имя состоит из нескольких слов, разделенных пробелом, заключите его в кавычки, например, `rule "number one"`.

Примечание. При создании сетевого фильтра можно не указывать его номер. В этом случае фильтру будет присвоен номер, следующий за номером последнего фильтра в соответствующей таблице, и он будет иметь самый низкий приоритет.

Имя сетевого фильтра можно не указывать, в таком случае фильтр будет создан без имени.

- Параметры, определяющие процесс обработки IP-пакетов этим фильтром:
  - Адрес отправителя.
  - Адрес получателя.
  - Протокол.
  - Для транзитных фильтров открытой сети и фильтров туннелируемых узлов:
    - Приложение.
    - Прикладной протокол.
    - Группа приложений.

Примечание. При задании приложения необходимо учитывать ограничения, действующие для некоторых приложений (см. Особенности фильтрации по приложениям и прикладным протоколам). Если вы выбрали отдельное приложение или прикладной протокол, то вы не можете выбрать группу приложений и наоборот.

Если вы уже указали приложение, то выбор прикладных протоколов будет ограничен протоколами, которые поддерживает выбранное приложение.

При создании транзитных фильтров открытой сети и фильтров туннелируемых узлов необходимо учитывать следующие особенности использования параметров приложения и прикладного протокола для блокировки неизвестного трафика:

- `dpiapp unknown` — классификация приложения завершена, приложение не определено (не входит в список известных приложений). Может использоваться для блокировки всех неизвестных приложений.
- `dpiprotocol unknown` — классификация протокола завершена, протокол не определен (не входит в список известных прикладных протоколов). Может использоваться для блокировки всех неизвестных прикладных протоколов.

- Пользователь.

Примечание. Сетевые фильтры, в которых заданы пользователи сети, имеют ограничения:

- Поддерживаются только пользователи, имена которых заданы латиницей.
- Если IP-пакет попадает под действие сетевого фильтра, в котором задан пользователь, то IP-адрес этого пользователя сопоставляется с адресом источника или назначения IP-пакета. Фильтр сработает в том случае, если адрес источника или назначения IP-пакета совпадет с адресом пользователя Active Directory или Captive portal.
- В случае, когда на одном сетевом узле, подключенном к контроллеру домена Active Directory, выполнили вход несколько пользователей, будут действовать сетевые фильтры для последнего пользователя, который вошел в домен.

- URL-категория.

- Расписание.
- Для транзитных фильтров открытой сети:
  - Проверка правилами IPS.
  - Проверка на ICAP-серверах.
  - URL-адрес.
  - IP-адрес прокси-клиента.
  - Веб-клиенты.
  - SSL/TLS-инспекция.
- Регистрация IP-пакетов.
- Регистрация сессий.
- Действие.

Примеры создания сетевых фильтров

Чтобы разрешить отправку FTP-запросов со своего узла открытому узлу с адресом 192.168.2.4, выполните команду:

```
hostname# firewall local add src @local dst 192.168.2.4 service @FTP pass
```

Чтобы создать локальный фильтр, блокирующий IP-пакеты, отправляемые узлом с адресом 192.168.30.1 через порт 2525 на порт 443 открытого узла с адресом 172.16.35.1 по протоколу TCP/IP, выполните команду:

```
hostname# firewall local add src 192.168.30.1 dst 172.16.35.1 tcp sport 2525 dport 443 drop
```

Чтобы создать фильтр защищенной сети, разрешающий отправку IP-пакетов от узла ViPNet с идентификатором 0x1a12000a на свой узел:

```
hostname# firewall vpn add src 0x1a12000a dst @local pass
```

Чтобы создать фильтр, разрешающий отправку открытых транзитных IP-пакетов от узла с адресом 192.168.0.1 на узел с адресом 192.168.30.3 через ViPNet Coordinator HW, выполните команду:

```
hostname# firewall forward add src 192.168.0.1 dst 192.168.30.3 pass
```

Чтобы создать фильтр, разрешающий отправку IP-пакетов от туннелируемого узла с адресом 192.168.0.1 на узел ViPNet с идентификатором 0x1234abab:

```
hostname# firewall tunnel add src 192.168.0.1 dst 0x1234abab pass
```

Чтобы создать фильтр, разрешающий отправку IP-пакетов от туннелируемого узла с адресом 192.168.0.1 туннелируемому узлу с адресом 192.168.2.3:

```
hostname# firewall tunnel add src 192.168.0.1 dst 192.168.2.3 pass
```

Чтобы создать транзитный фильтр открытой сети, блокирующий IP-пакеты приложения Zoom по протоколу SSL для пользователя `ivanov`, выполните команду:

```
hostname# firewall forward add src @any dst @any dpiapp Zoom dpiprotocol SSL dnuser ivanov
drop
```

Чтобы создать транзитный фильтр открытой сети с номером 333, который запрещает STUN и QUIC трафик с ресурсов Zoom и Microsoft Teams для пользователей PetrovPP, SidorovKP и Ivan Ivanov, выполните команду:

```
hostname# firewall forward add 333 src @any dst @any dpiapp Zoom,"Microsoft Teams"
dpiprotocol STUN,QUIC dnuser PetrovPP,SidorovKP,"Ivan Ivanov" drop
```

Чтобы создать транзитный фильтр открытой сети с номером 444, запрещающий трафик мессенджеров и онлайн трансляций (группа `Messaging` и `Streaming`) для пользователей PetrovPP и SidorovKP, выполните команду:

```
hostname# firewall forward add 444 src @any dst @any dpigroup Messaging,Streaming dnuser
PetrovPP,SidorovKP drop
```

Адрес отправителя

Адрес отправителя IP-пакетов является обязательным параметром сетевого фильтра и описывается лексемой:

```
src <адрес отправителя>
```

Возможные значения адреса отправителя:

- для локальных фильтров открытой сети:
  - IP-адрес или доменное имя узла;

> **Примечание.** При задании адреса отправителя в виде доменного имени на DNS-сервер отправляется соответствующий запрос для разрешения данного имени. DNS-запись и время её жизни (TTL, «Time to live»), полученные в ответ на такой запрос, сохраняются в кеше. По истечении времени её жизни отправляется новый запрос на DNS-сервер для актуализации данных в кеше. Если полученные данные отличаются, происходит перезагрузка сетевых фильтров в драйвере ViPNet.
>
> Если разрешения указанного в сетевом фильтре доменного имени по каким-либо причинам не произошло, то такой фильтр не загружается в драйвер ViPNet до тех пор, пока в результате отправки повторных запросов на DNS-сервер не будет получен корректный ответ.

  - диапазон IP-адресов узлов — два ограничивающие диапазон IP-адреса, разделенные дефисом. При этом значение второго IP-адреса (конца диапазона) должно быть больше первого (начала диапазона), например:

    ```
    src 192.168.1.1-192.168.1.10
    ```

  - маска подсети — IP-адрес подсети в формате классовой или бесклассовой адресации CIDR (Classless Inter-Domain Routing), например:

    `src 192.168.1.0/24` или `src 192.168.1.0/255.255.255.0`

  - доменное имя узла, например:

    ```
    src mydomain.ru
    ```

> **Примечание.** При необходимости вы можете задать несколько IP-адресов и доменных имен отправителей IP-пакетов в одной лексеме, перечислив их через запятую, например:
> `src 192.168.30.2,192.169.1.1,mydomain.ru`

  - системные объекты `any` (любое значение), `local` (собственный узел) или `remote` (другие узлы) либо одна или несколько пользовательских групп IP-адресов. Имя группы необходимо дополнить символом «`@`», несколько групп указываются через запятую. Например:

    ```
    src @IP_group_1,@IP_group_2
    ```

> **Внимание!** Использование других адресов отправителей IP-пакетов совместно с системными объектами `any`, `local` и `remote` недопустимо.

- сетевой интерфейс собственного узла, через который будут проходить IP-пакеты, в следующем виде:

  ```
  src interface {<имя интерфейса> | @<имя группы интерфейсов> | byip {<IP-адрес> | <диапазон IP-адресов> | <маска подсети>}}
  ```

- для транзитных фильтров открытой сети: то же, что для локальных фильтров открытой сети, но в таких фильтрах можно использовать только системный объект `any`;
- для фильтров защищенной сети:
  - идентификатор узла сети ViPNet, например:

    ```
    src 0x1a12000a
    ```

  - системные объекты `any`, `allcoordinators`, `allclients`, `local` или `remote` либо пользовательские группы узлов ViPNet. Имя системного объекта или группы необходимо дополнить символом «`@`», несколько объектов или групп указываются через запятую. Например:

    ```
    src @allclients,@allcoordinators
    ```

  - идентификатор сети ViPNet, например:

    ```
    src 0x1a12
    ```



Примечание. При задании адреса отправителя для фильтров защищенной сети:

- В одной лексеме можно указать несколько идентификаторов узлов или сетей ViPNet, пользовательских групп узлов ViPNet и системные объекты `allcoordinators` или `allclients`, перечислив их через запятую. Например: `src @allcoordinators,0x1a12000a`
- Нельзя указывать IP-адреса, доменные имена, маски адресов и сетевой интерфейс узла.
- Нельзя использовать другие адреса отправителей совместно с объектами `any`, `local` и `remote`.

- для фильтров туннелируемых узлов: то же, что для локальных фильтров открытой сети и фильтров защищенной сети, но в таких фильтрах можно использовать только системные группы объектов `any`, `allcoordinators`, `allclients`, `tunneledip`.



Внимание! Если в фильтре туннелируемых узлов в качестве адреса отправителя указан адрес узла защищённой сети, то в качестве адреса получателя в этом фильтре должен быть указан адрес открытого узла, и наоборот.

- для локальных фильтров и транзитных фильтров открытой сети:
  - страну:

    ```
    src cc <страна>
    ```

    Страна задаётся кодом Alpha 2 (прописные буквы) или числовым кодом в соответствии с ISO-3166. Несколько кодов указываются в списке через запятую.

  - MAC-адрес:

    ```
    src mac <MAC-адрес>
    ```

    MAC-адрес необходимо задавать в полном формате, используя в качестве разделителя двоеточие или тире, например `40-8D-5C-4A-7D-BE`. В одном фильтре можно указать

только один MAC-адрес. Запрещено указывать MAC-адреса интерфейсов ViPNet Coordinator HW.

Адрес получателя

Адрес получателя IP-пакетов является обязательным параметром сетевого фильтра. Синтаксис адреса получателя повторяет синтаксис адреса отправителя, за исключением следующих особенностей:

- Адрес получателя описывается после адреса отправителя лексемой:

  `dst <адрес получателя>`

- Для задания адреса получателя нельзя использовать сетевой интерфейс узла.
- Для задания адреса получателя, помимо пользовательских групп объектов, можно использовать системные объекты:
  - Для локальных фильтров открытой сети: `any`, `local`, `remote`, `broadcast`, `multicast`.

    Внимание! Использование других адресов отправителей IP-пакетов совместно с системными объектами `any`, `local`, `remote`, `broadcast` и `multicast` недопустимо.

  - Для транзитных фильтров открытой сети: `any`.
  - Для фильтров защищенной сети: `any`, `allcoordinators`, `allclients`, `local`, `remote`, `broadcast`.
  - Для фильтров туннелируемых узлов: `any`, `allcoordinators`, `allclients`, `tunneledip`.
  - Для локальных фильтров и транзитных фильтров открытой сети — страну:

    `dst cc <страна>`

    Страна задаётся кодом Alpha 2 (прописные буквы) или числовым кодом в соответствии с ISO-3166. Несколько кодов указываются в списке через запятую.

Протокол

Протокол не является обязательным параметром сетевого фильтра.

Протоколы можно указывать, используя:

- Имена протоколов, написанные строчными буквами и разделенные пробелами, например:

  `tcp udp icmp`

  В этом случае также можно задать дополнительные параметры для протоколов, например:
  - для протоколов TCP и UDP: `sport` (порт или диапазон портов источника пакета) и/или `dport` (порт или диапазон портов назначения пакета). При использовании обоих этих параметров сначала необходимо указать параметр `sport`, затем — параметр `dport`. Возможно указать несколько портов или диапазонов портов, в этом случае необходимо

указать название протокола (`tcp` или `udp`) перед каждым номером порта (диапазоном портов). Например: `tcp sport 2525 tcp dport 443 tcp dport 4444-4445`.

- для протокола TCP: в том числе с `sport` и `dport` для локальных и транзитных фильтров открытой сети флаги TCP-сегмента: `ack`, `fin`, `psh`, `rst`, `syn`, `urg`, `cwr`, `ece`, например:

  `tcp sport 2525 tcp dport 443 +syn -urg -cwr`, где:

  - `+` — флаг установлен;
  - `-` — флаг сброшен;



Примечание. Сетевой фильтр обрабатывает соединение по первому соответствию TCP-флагов в IP-пакете. Чтобы трафик соответствовал условиям этого фильтра, необходимо, чтобы набор TCP-флагов был одинаковым для каждого пакета в рамках сессии. Отличие набора TCP-флагов как минимум в одном из пакетов приведёт к блокировке соединения.

- для протокола ICMP: только параметр `type` (тип пакета) либо параметр `type` вместе с параметром `code` (код пакета). Например: `icmp type 3 code 1`. Если параметр `code` не задан, то под условие будут подпадать все ICMP-пакеты указанного типа;

- номера протоколов. В этом случае для каждого протокола необходимо указать ключевое слово `proto` и его номер. Например, для протоколов TCP, UDP и ICMP: `proto 6 proto 17 proto 1`;



Внимание! При использовании номеров протоколов задать дополнительные параметры протоколов невозможно.

- пользовательские группы протоколов, в том числе заданные по умолчанию, в виде:

  `service @<имя группы>`

  Например: `service @DNS`.

Приложение

Приложение — необязательный параметр `dpiapp` транзитного фильтра открытой сети и фильтра туннелируемых узлов. Позволяет анализировать трафик, характерный для определенного сервиса. Например:

- Запрещающий сетевой фильтр для приложения BitTorrent будет блокировать трафик как программы BitTorrent, так и других Torrent-клиентов.
- Запрещающий сетевой фильтр для приложения Telegram будет блокировать трафик приложения Telegram, а также браузерную версию Telegram.

Список приложений приведен в приложении.

Внимание! В транзитном фильтре открытой сети запрещено совместно указывать параметры `dpiapp` и `ssl`.

Приложения необходимо указывать по их названиям. Вы можете указать несколько приложений в списке через запятую. При задании приложения, содержащего пробелы, его название необходимо заключить в двойные кавычки:

```
dpiapp "Google Mail",Telegram,Facebook
```

Прикладной протокол

Прикладной протокол — необязательный параметр `dpiprotocol` транзитного фильтра открытой сети и фильтра туннелируемых узлов. В отличие от приложения, анализируется только трафик, характерный для прикладного протокола.

Внимание! В транзитном фильтре открытой сети запрещено совместно указывать параметры `dpiprotocol` и `ssl`.

Список прикладных протоколов приведен в приложении.

Прикладные протоколы необходимо указывать по их названиям. Вы можете указать несколько прикладных протоколов в списке через запятую. Название протокола, содержащее пробелы, необходимо заключить в двойные кавычки:

```
dpiprotocol "Microsoft Teams Call",HTTP,SSL
```

Внимание! Если в транзитном фильтре открытой сети или фильтре туннелируемых узлов вы указали параметр `dpiapp`, например `aliexpress`, то в качестве параметра `dpiprotocol` вы можете использовать только связные прикладные протоколы, относящиеся к этому приложению: `flash`, `http`, `ssl`.

Группа приложений

Группа приложений — необязательный параметр `dpigroup` транзитного фильтра открытой сети и фильтра туннелируемых узлов. Объединяет приложения и прикладные протоколы, классифицированные DPI, по признаку схожего назначения.

Список поддерживаемых групп приложений приведен в приложении.

Внимание! В транзитном фильтре открытой сети запрещено совместно указывать параметры `dpigroup` и `ssl`.

Группы приложений необходимо указывать по их названиям. Вы можете указать несколько групп в списке через запятую. Название группы, содержащее пробелы, необходимо заключить в двойные кавычки:

```
dpigroup "Voice over IP","Remote Control",Streaming
```

Внимание! В транзитном фильтре открытой сети или фильтре туннелируемых узлов запрещено совместно с параметром `dpigroup` указывать дополнительные параметры `dpiapp` и `dpiprotocol`.

Пользователь

Пользователь — необязательный параметр `dnuser` транзитного фильтра открытой сети и фильтра туннелируемых узлов. Чтобы иметь возможность указывать пользователя при создании фильтра, настройте подключение к Active Directory или Captive portal (см. Настройка взаимодействия с LDAP-сервером).

Пользователей необходимо указывать, используя их доменные имена (без указания имени самого домена) или имена, зарегистрированные на Captive portal. Вы можете указать несколько пользователей в списке через запятую. При задании имени пользователя, содержащего пробелы, его необходимо заключить в двойные кавычки:

```
dnuser ivanov_v,petrov_a,"petr ivanov"
```

Внимание! Для сетевых фильтров, в которых заданы пользователи сети, существуют следующие ограничения:

- Текущая версия ViPNet Coordinator HW поддерживает работу только с именами пользователей, заданными латиницей. Не используйте при создании сетевых фильтров реквизиты пользователей, заданных в других раскладках.
- Если IP-пакет попадает под действие сетевого фильтра, в котором задан пользователь, то IP-адрес этого пользователя сопоставляется с адресом источника или назначения IP-пакета. Фильтр сработает в том случае, если адрес источника или назначения IP-пакета совпадет с адресом пользователя Active Directory или Captive portal.
- В случае, когда на одном сетевом узле, подключенном к контроллеру домена Active Directory, выполнили вход несколько пользователей, то будут действовать сетевые фильтры для последнего пользователя, который вошел в домен.

Расписание

Расписание задаёт время действия сетевого фильтра и не является его обязательным параметром. Описывается одной из следующих лексем:

- `daily <чч:мм>-<чч:мм>` — фильтр действует ежедневно в течение заданного интервала времени. Время указывается в 24-часовом формате: `чч` — часы, `мм` — минуты.
- `weekly [mo] [tu] [we] [th] [fr] [sa] [su] [at <чч:мм>-<чч:мм>]` — фильтр действует еженедельно в заданные дни недели:
  - `mo` — понедельник;
  - `tu` — вторник;
  - `we` — среда;

- `th` — четверг;
- `fr` — пятница;
- `sa` — суббота;
- `su` — воскресенье.

o `calendar <дд.мм.гггг>-<дд.мм.гггг> [at <чч:мм>-<чч:мм>]` — фильтр действует в заданные даты и интервал времени. Дата указывается в следующем формате:

- `дд` — день;
- `мм` — месяц;
- `гггг` — год.

o `schedule @<имя группы объектов>` — фильтр действует по расписанию, описанному группой объектов соответствующего типа.

Для задания расписания можно использовать соответствующие пользовательские группы, в том числе заданные по умолчанию.

SSL/TLS-инспекция

Параметр SSL/TLS-инспекции не является обязательным, применяется в транзитных фильтрах открытой сети и задается лексемой `ssl`:

- `decrypt` — инспектировать трафик SSL/TLS-сессий;
- `bypass` — пропускать трафик SSL/TLS-сессий без инспекции.



Внимание! В транзитном фильтре открытой сети запрещено совместно указывать параметр `ssl` и параметры `dpiapp`, `dpiprotocol`, `dpigroup`. Подробнее см. Ограничения SSL/TLS-инспекции (см. Особенности SSL/TLS-инспекции).

Совместно с параметром `ssl` вы можете указать URL-адрес, URL-категорию, проверку IPS и проверку на ICAP-серверах (`av`, `sb`, `dlp`).

До использования этого параметра в фильтрах проверьте настройку SSL/TLS-инспекции трафика, заданную по умолчанию, и при необходимости измените её (см. Настройка SSL/TLS-инспекции трафика).

Проверка правилами IPS

Параметр проверки правилами IPS не является обязательным, применяется в транзитных фильтрах открытой сети и задается лексемой `ips`:

- `on` — включить проверку трафика;
- `off` — не проверять трафик.

До использования этого параметра в фильтрах проверьте настройку предотвращения вторжений, заданную по умолчанию, и при необходимости измените её (см. Настройка предотвращения вторжений).



Примечание. В текущей версии ViPNet Coordinator HW в журнале сессий, в т.ч. при экспорте журнала по сети в формате CEF, срабатывание фильтра, для которого включена проверка правилами IPS, фиксируется без учёта обработки IPS.

Для обнаружения фактических срабатываний вы можете использовать фильтр по событиям 67 и 142 в журнале IP-пакетов.

Проверка на ICAP-серверах

Параметры проверки HTTP-трафика на внешних ICAP-серверах не являются обязательными, применяются в транзитных фильтрах открытой сети и задается следующими лексемами:

- `av` — антивирусная проверка:
  - `on` — включить;
  - `off` — выключить;
- `sb` — проверка в песочнице:
  - `on` — включить;
  - `off` — выключить;
- `dlp` — проверка в DLP-системе:
  - `on` — включить;
  - `off` — выключить.

До использования этих параметров в фильтрах настройте подключение ViPNet Coordinator HW к ICAP-серверам (см. Настройка подключения к ICAP-серверам).

URL-адрес

Параметр фильтрации по URL-адресу веб-ресурса не является обязательным, применяется в транзитных фильтрах открытой сети и задается лексемой `url <URL-адрес>`.

При задании URL-адреса веб-ресурса вы можете использовать буквы (`A–Z`, `a–z`), и цифры (`0–9`) и символы (`-._~:/?#[]@!$&'()*+,;=%`). Кроме адреса вы можете задать маску веб-ресурса:

- допустимые символы: такие же, как в URL-адресе веб-ресурса;
- использование `*`:
  - `*` в начале URI — дополняет произвольное, в том числе нулевое, количество символов до URI;
  - `*` в конце URI — дополняет произвольное количество символов после URI;

- `*` в конце и начале URI — дополняет произвольное количество символов до и после URI;
- `*` — любой адрес веб-ресурса;
- `**` — любой адрес веб-ресурса;
- `***` — поиск `*` в адресе веб-ресурса.



Примечание. Префикс `!` в адресе веб-ресурса или маске означает инверсию действия сетевого фильтра по отношению к ним, например, `!cloud.mail.ru` в фильтре с действием `pass`, означает блокировку этого ресурса при срабатывании фильтра.

Вместе с URL-адресом веб-ресурса или маской вы можете дополнительно указать:

- `mthd` — метод HTTP-запроса (`CONNECT`, `DELETE`, `GET`, `HEAD`, `OPTIONS`, `PATCH`, `POST`, `PUT`, `TRACE`);
- `type` — тип передаваемых данных (см. Поддерживаемые MIME-типы),

а именно: `url <url-адрес> [mthd <метод>] [type <тип>]`.

Вы можете указать нескольких url-адресов или масок, в том числе для каждого из них метод HTTP-запроса и тип данных:
`url <URL-адрес1>,<URL-адрес2>,<URL-адресN> [mthd <метод1>,<метод2>,<методN>] [type <тип1>,<тип2>,<типN>]`

- URL-адреса, маски, значения методов и типов необходимо указывать через запятую и без пробелов между ними;
- необходимо заключать в двойные кавычки (`"`):
  - URL-адреса и маски, содержащие запятые;
  - строку типа данных, содержащую пробелы;
- метод или тип, не задаваемые явно (что означает любой метод или тип), указываются символом `*`, например:

  ```
  url planner.mail.ru,plus.yandex.ru mthd *,GET type "application/x-tex",*
  ```

- если для всех URL-адресов или масок метод или тип не заданы явно, то ключевые слова `mthd` или `type` опускаются, например:

  ```
  url planner.mail.ru,plus.yandex.ru type "application/x-tex",*
  ```

Веб-клиенты

Параметр фильтрации по группам объектов «Веб-клиенты» не является обязательным, применяется в транзитных фильтрах открытой сети и задается лексемой `user-agent <веб-клиенты>`. Вы можете использовать группы веб-клиентов для браузеров Chrome, Edge, Firefox, Opera и Yandex, заданные по умолчанию, или настроить свои группы веб-клиентов (см. Группа объектов «Веб-клиенты»).

IP-адрес прокси-клиента

Параметр фильтрации по действительному IP-адресу прокси-клиента — сетевого узла, расположенного за прокси-сервером или балансировщиком нагрузки. Действительный IP-адрес соответствует адресу в заголовке `X-Forwarded-For` HTTP-запроса. Параметр не является обязательным, применяется в транзитных фильтрах открытой сети и задается лексемой `proxy-client <IP-адрес>`.

URL-категория

Параметр фильтрации по URL-категории не является обязательным, применяется в транзитных фильтрах открытой сети и фильтрах туннелируемых узлов. Задается лексемой `url-category <url-категория>`. Вы можете использовать категории из базы URL-категорий (см. Обновление базы URL-категорий) или настроить свои URL-категории (см. Настраиваемые URL-категории).

Если в названии URL-категории содержатся пробелы, его необходимо задавать в одинарных или двойных кавычках:

```
url-category "Advertisements and Pop-Ups"
```

Для использования настраиваемой URL-категории необходимо добавлять символ `#` перед её названием. Если используются кавычки, символ `#` добавляется внутри кавычек:

```
url-category #VideoServices
```

```
url-category "#Prohibited external services"
```

Вы можете указать несколько URL-категорий в списке через запятую:

```
url-category "Advertisements and Pop-Ups",Arts,#VideoServices
```

где `Advertisements and Pop-Ups`, `Arts` — категории из базы URL-категорий, `VideoServices` — настраиваемая URL-категория.

Регистрация IP-пакетов

Необязательный параметр, определяющий регистрацию IP-пакетов в журнале IP-пакетов при срабатывании фильтра. Описывается лексемой `log {on | off}`:

- `on` — регистрировать IP-пакеты;
- `off` — не регистрировать IP-пакеты.

Значение по умолчанию:

- `off` — для фильтра с действием пропускать (`pass`);
- `on` — для фильтра с действием блокировать (`drop`) или отклонить (`reject`).

Подробнее см. Настройка регистрации IP-пакетов и сессий при срабатывании фильтров.

Регистрация сессий

Необязательный параметр, определяющий регистрацию сессий в журнале сессий при срабатывании фильтра. Описывается лексемой `sessions {on | off} [state {all | begin_end | begin}]`:

- `on` — регистрировать сессии;
- `off` — не регистрировать сессии.

Значение по умолчанию:

- `off` — для фильтра с действием пропускать (`pass`), в котором не указан параметр `ips`;
- `on` — для фильтра:
  - с действием пропускать (`pass`) и параметром `ips` (будут регистрироваться сессии, вызвавшие срабатывание правила IPS с действием «предупреждать»);
  - с действием блокировать (`drop`) или отклонить (`reject`);
  - полученного из Policy Management (модуль Prime) в составе политик безопасности.

Вы можете настроить регистрацию определенных состояний сессии (`state`):

- `all` — отслеживать все состояния сессии;
- `begin` — отслеживать начало сессии;
- `begin_end` — отслеживать начало и окончание сессии (по умолчанию).

Примечание. При отслеживании всех состояний (`all`) в журнале сессий регистрируются внутренние состояния сессии в соответствии с протоколом 3–4 уровня OSI.

Подробнее см. Настройка регистрации IP-пакетов и сессий при срабатывании фильтров.

Действие

Обязательный параметр сетевого фильтра. Определяет действие фильтра с IP-пакетом, соответствующим его условию:

- `pass` — пропускать IP-пакет;
- `drop` — блокировать IP-пакет;
- `reject` — отклонить IP-пакет и отправить ICMP-сообщение:
  - `reject` — отправляет сообщение `Destination port unreachable`;
  - `rej-net-unreachable` — отправляет сообщение `Destination net unreachable`;
  - `rej-host-unreachable` — отправляет сообщение `Destination host unreachable`;
  - `rej-proto-unreachable` — отправляет сообщение `Destination protocol unreachable`;

- `rej-net-prohibited` — отправляет сообщение `Network administratively prohibited`;
- `rej-host-prohibited` — отправляет сообщение `Host administratively prohibited`;
- `rej-admin-prohibited` — отправляет сообщение `Communication administratively prohibited`;
- `rej-tcp-reset` — отправляет сообщение `TCP reset` (только для TCP-пакетов).

Изменение сетевого фильтра

Вы можете изменить ранее созданный сетевой фильтр, добавив в него дополнительные значения параметров или изменить их:

```
hostname# firewall <тип> change append {<номер> | rule <имя>} [src <адрес отправителя>] [dst <адрес получателя>] [<транспортный протокол>] [dpiapp <приложение>] [dpiprotocol <прикладной протокол>] [dpigroup <группа приложений>] [dnuser <пользователь>] [<расписание>] [ips {on | off}] [av {on | off}] [sb {on | off}] [dlp {on | off}] [url <url-адрес> [type <mime-тип>] [mthd <http-метод>]] [user-agent <веб-клиенты>] [url-category <url-категория>] [ssl {decrypt | bypass}] [log {on | off}] [sessions {on | off} [state {all | begin_end | begin}]]
```

Для параметров `src <адрес отправителя>`, `dst <адрес получателя>`, `<транспортный протокол>`, `dpiapp <приложение>`, `dpiprotocol <прикладной протокол>`, `dpigroup <группа приложений>`, `dnuser <пользователь>`, `<расписание>`, `url <url-адрес> [type <mime-тип>] [mthd <http-метод>]`, `user-agent <веб-клиенты>`, `url-category <url-категория>` указанное значение добавляется к имеющимся в сетевом фильтре.

Для параметров `ips {on | off}`, `av {on | off}`, `sb {on | off}`, `dlp {on | off}`, `[proxy-client <IP-адрес>]`, `ssl {decrypt | bypass}`, `log {on | off}`, `[sessions {on | off} [state {all | begin_end | begin}]]` задается указанное значение.

При необходимости вы можете указать несколько параметров. Для сохранения изменений в строке `Do you want to perform the action on the above rule? [Yes/No]` введите `y` и нажмите **Enter**.

Чтобы в сетевой фильтр `1 RuleName1 src 192.168.1.1,2.2.2.2/24 dst @local drop` добавить адрес нового отправителя, выполните команду:

```
hostname# firewall local change append 1 src 192.168.3.3
```

В результате фильтр будет изменен: `1 RuleName1 src 192.168.1.1,2.2.2.2/24,192.168.3.3 dst @local drop`.

Чтобы изменить приоритет сетевого фильтра (порядковый номер в таблице сетевых фильтров соответствующего типа), выполните команду:

```
hostname# firewall <тип> move rule <текущий номер> to <новый номер>
```

В результате приоритет сетевого фильтра и, соответственно, его порядковый номер в таблице будут изменены. При этом номера фильтров, следующих за этим фильтром, автоматически увеличатся на единицу, то есть их приоритет понизится.

Просмотр сетевых фильтров

Для просмотра всех сетевых фильтров, включая правила трансляции адресов, выполните:

```
hostname# firewall rules show
```

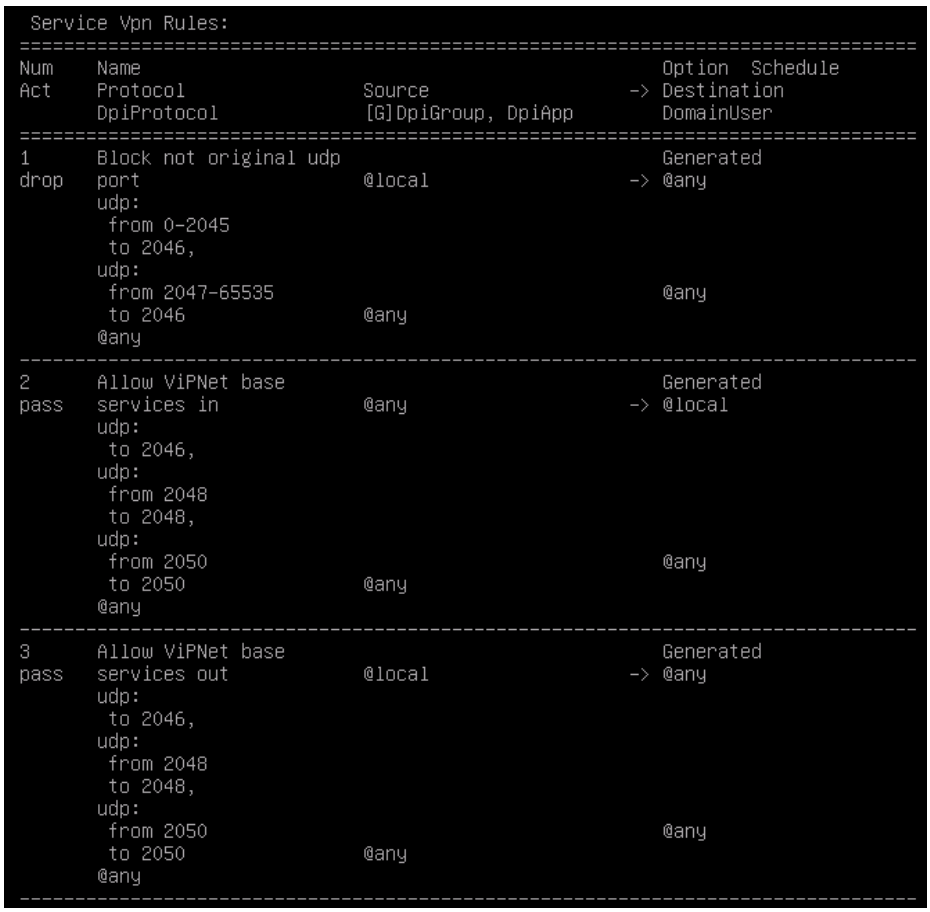


Рисунок 24. Фрагмент списка сетевых фильтров

Для просмотра сетевых фильтров определенного типа выполните:

```
hostname# firewall <тип> show
```

Например, для просмотра локальных фильтров открытой сети:

```
hostname# firewall local show
```

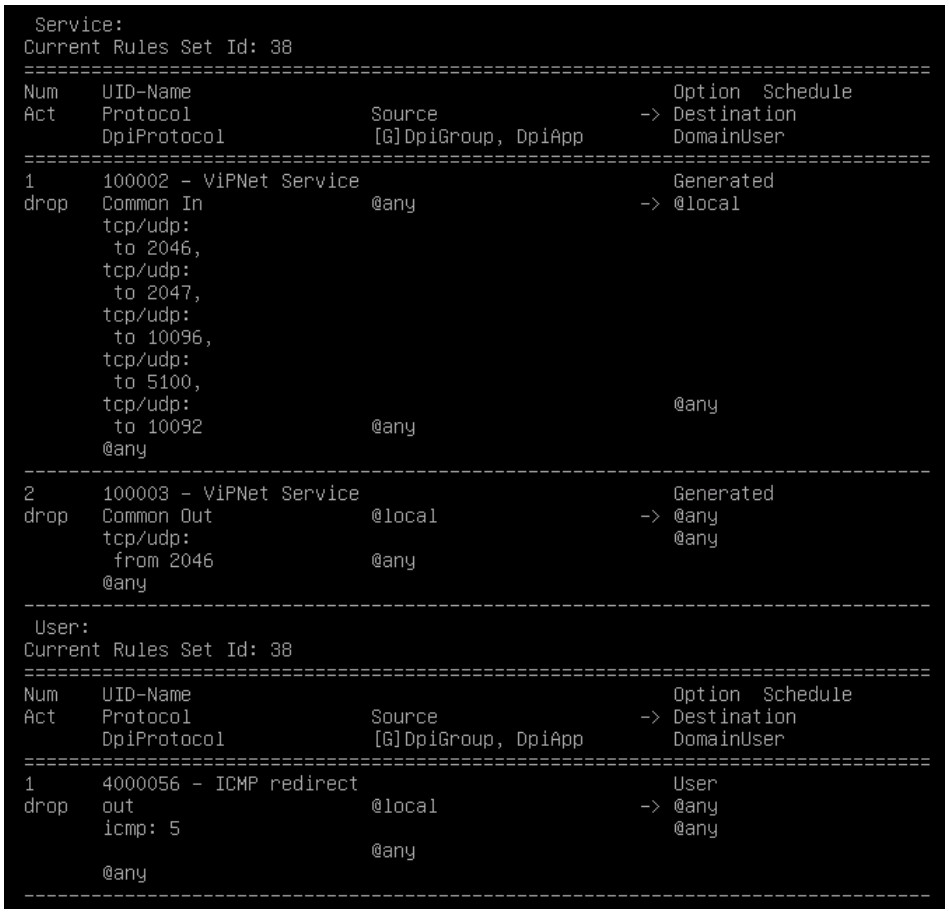


Рисунок 25. Фрагмент списка локальных фильтров открытой сети

Для просмотра сетевых фильтров с конкретными параметрами выполните:

```
hostname# firewall <тип> show [<параметр>]
```

указав в качестве параметра:

- `<номер>` — порядковый номер фильтра или правила трансляции в таблице, определяющий его приоритет;
- `rule <имя>` — имя фильтра или правила трансляции;
- `src <адрес отправителя>` — адрес отправителя IP-пакетов;
- `dst <адрес получателя>` — адрес получателя IP-пакетов;
- `<транспортный протокол>` — транспортный протокол, по которому передаются IP-пакеты;
- для транзитных фильтров открытой сети и фильтров туннелируемых узлов:
  - `dpiapp <приложение>` — приложение;
  - `dpiprotocol <прикладной протокол>` — прикладной протокол;
  - `dpigroup <группа приложений>` — группа приложений;
  - `dnuser <пользователь>` — пользователь Active Directory или Captive Portal;

    - `url-category` — фильтрация по URL-категориям из базы или настраиваемым URL-категориям;
- `<расписание>` — расписание применения фильтра или правила трансляции;
- для транзитных фильтров открытой сети:
    - `ssl` — инспекция трафика SSL/TLS-сессий;
    - `ips` — проверка IPS;
    - `av` — антивирусная проверка;
    - `sb` — проверка в песочнице;
    - `dlp` — проверка в DLP-системе;
    - `url` — контентная фильтрация:
        - `URL-адрес` — URL-адрес веб-ресурса или маска;
        - `MIME-тип` — тип передаваемых данных;
        - `HTTP-метод` — метод HTTP-запроса;
    - `proxy-client` — фильтрация по IP-адресу прокси-клиента;
    - `user-agent` — фильтрация по группам объектов «Веб-клиенты»;
- `log` — регистрация IP-пакетов при срабатывании фильтра;
- `sessions` — регистрация сессий при срабатывании фильтра;
- `<действие>` — действие с IP-пакетами, соответствующими условиям фильтра или правила трансляции.

При необходимости вы можете указать несколько параметров. Например, для просмотра локального фильтра открытой сети с несколькими адресами отправителей или одним адресом получателя:

```
hostname# firewall local show src 192.168.30.2,192.169.1.1,admydomain.ru dst 192.168.0.1
```



Внимание! Поиск сетевых фильтров для отображения осуществляется по строгому совпадению с указанными параметрами. Например:

- если указан параметр `src 192.168.1.10`, отобразится фильтр, содержащий адрес `src 192.168.1.10`, но не отобразится фильтр, содержащий адрес `src 192.168.1.10-192.168.1.11`.
- если указан параметр `rule Name`, отобразится фильтр с именем `Name`, но не отобразится фильтр с именем `Name1`.

Удаление сетевого фильтра

Чтобы удалить ненужный сетевой фильтр:

- Если вы знаете порядковый номер фильтра:

```
hostname# firewall <тип> delete <номер>
```

Например:

```
hostname# firewall local delete 7
```

- Если вы не знаете номер фильтра, то выполните поиск по известным вам параметрам:

  ```
  hostname# firewall <тип> delete <параметр>,
  ```

  где в качестве `<параметр>` можете указать имя, адрес отправителя, адрес получателя, протокол или действие. Вы можете указать несколько параметров. Например, для удаления локальных фильтров открытой сети с адресом отправителя 192.168.20.2:

  ```
  hostname# firewall local delete src 192.168.20.2
  ```

  Внимание! Поиск сетевых фильтров выполняется по строгому совпадению с указанными параметрами.

  Будет выведен список подходящих сетевых фильтров:

  - Если в результате поиска найдено несколько сетевых фильтров:
    - введите номер фильтра из столбца `Num`, чтобы удалить только его;
    - введите `a`, чтобы удалить все фильтры списка;
  - Если найден один фильтр, подтвердите его удаление: введите `y`.

После удаления изменятся номера (приоритеты) фильтров. Номера фильтров с более низким приоритетом уменьшатся на единицу.

Настройка регистрации IP-пакетов и сессий при срабатывании фильтров

Каждый сетевой фильтр содержит параметры `log` и `sessions`, которые определяют:

- регистрировать обработанные им IP-пакеты в журнале IP-пакетов или нет;
- регистрировать сессию в журнале сессий или нет.

Вы можете задать значения этих параметров в командах `firewall add` и `firewall change`. Описание параметров см. в разделах Регистрация IP-пакетов и Регистрация сессий.



Примечание. Значение параметра `log` учитывается, только если выбран способ регистрации IP-пакетов по фильтрам. При этом настраивать параметр `log` вы можете независимо от используемого способа регистрации IP-пакетов. Подробнее о способах регистрации IP-пакетов см. Журнал IP-пакетов.

Чтобы просмотреть настройку регистрации IP-пакетов и регистрации сессий при срабатывании фильтров определённого типа, выполните команду:

```
hostname# firewall <тип фильтра> show
```

Если регистрация IP-пакетов для фильтра включена, то в выводе команды перед именем фильтра отображается префикс `[LOG]`.

Если регистрация сессий для фильтра включена, то в выводе команды перед именем фильтра отображается префикс `[SESS]`.

Чтобы включить регистрацию IP-пакетов при срабатывании всех настраиваемых фильтров с действиями блокировать (`drop`) и отклонить (`reject`), выполните команду:

```
hostname# firewall rules log-blocked

This will turn on logging for all user rules with action drop or reject.

Continue? [Yes/No]: y
```

Блокирование сайтов по доменным именам

Для корректной работы запрещающих сетевых фильтров, в которых в качестве адресов отправителей или получателей заданы доменные имена:

1. Задайте для ViPNet Coordinator HW IP-адрес внешнего DNS-сервера, например 8.8.8.8:

   ```
   hostname# inet dns forwarders add 8.8.8.8
   ```

2. Создайте разрешающие локальные фильтры для протокола DNS:

   ```
   hostname# firewall local add 1 rule "Allow DNS 1" src 8.8.8.8 dst @local service @DNS pass

   hostname# firewall local add 2 rule "Allow DNS 2" src @local dst 8.8.8.8 service @DNS pass
   ```

   Эти фильтры разрешат обмен трафиком между ViPNet Coordinator HW и внешним DNS-сервером.

3. Создайте сетевые фильтры, запрещающие обмен трафиком между клиентами защищенной сети и любым DNS-сервером, кроме заданного на шаге 1:

   ```
   hostname# firewall forward add 1 rule "Deny DNS forward" src @any dst @any service @DNS drop

   hostname# firewall vpn add 2 rule "Deny DNS vpn" src @local dst @any service @DNS drop

   hostname# firewall vpn add 3 rule "Deny DNS vpn" src @any dst @local service @DNS drop

   hostname# firewall tunnel add 1 rule "Deny DNS tunnel" src @any dst @any service @DNS drop
   ```

4. Задайте IP-адрес ViPNet Coordinator HW в качестве DNS-сервера для клиентов защищенной сети.

После этого вы можете создавать запрещающие сетевые фильтры для доменных имен сайтов.

Если сайт представляет собой распределенный сетевой ресурс, включающий «зеркала» или контент других сетевых ресурсов, то блокирование по доменным именам будет частичным. Полностью блокировать работу с таким сайтом можно, если в запрещающем транзитном фильтре открытой сети использовать параметры DPI-классификации трафика. Например:

- Фильтр `firewall forward add src @any dst facebook.com drop` частично блокирует работу с сайтом `facebook.com`.
- Фильтр `firewall forward add src @any dst @any dpiapp facebook, "facebook cloud" drop` полностью блокирует работу сайтом `facebook.com`.

Блокирование поддоменов с помощью DNS-фильтров

В сетевых фильтрах ViPNet Coordinator HW нет возможности задавать шаблон доменного имени (`*.<доменное имя>`), указывающий на группу поддоменов, но вы можете блокировать обращение к ним с помощью DNS-фильтров. Блокируемые поддомены задаются в DNS-фильтрах в виде шаблонов доменных имен. При поступлении DNS-запроса к заблокированному поддомену локальный DNS-сервер возвращает ошибку `NXDOMAIN` (имя неизвестно).



Внимание! Фильтрация DNS-запросов работает только для узлов сети, использующих локальный DNS-сервер в качестве сервера имен.

Чтобы заблокировать доступ ко всем поддоменам домена `google.com`:

1. Настройте локальный DNS-сервер (см. Настройка DNS-сервера).
2. Создайте DNS-фильтр для блокирования поддоменов домена `google.com`:

   ```
   hostname# inet dns filter add *.google.com
   ```

3. Проверьте, что `*.google.com` добавлен в список заблокированных поддоменов:

   ```
   hostname# inet dns filter list
   ```

4. Перезапустите DNS-сервер:

   ```
   hostname# inet dns stop
   hostname# inet dns start
   ```

Если блокировать поддомены домена `google.com` больше не нужно:

1. Удалите DNS-фильтр:

   ```
   hostname# inet dns filter delete *.google.com
   ```

2. Перезапустите DNS-сервер.

Особенности фильтрации трафика по URL-адресам и URL-категориям

Фильтрацию трафика по URL-адресам и URL-категориям можно задавать в транзитных фильтрах открытой сети и фильтрах туннелируемых узлов. При настройке фильтрации учитывайте следующее:

- Размещайте сетевые фильтры с параметрами URL-адреса и URL-категории в конце списка фильтров.
- Для настройки доступа к веб-ресурсу вместо фильтра с указанием доменного имени ресурса в параметре назначения, используйте фильтры с параметрами URL-адреса и URL-категории.
- Если URL-адрес одного веб-ресурса является частью другого, то при настройке доступа располагайте фильтры в следующем порядке: первым — фильтр по более длинному URL-адресу, затем — фильтр по более короткому, например, первым — разрешающий фильтр по `docs.infotecs.ru`, затем — запрещающий фильтр по `infotecs.ru`.
- Размещайте разрешающие сетевые фильтры с параметрами DPI после фильтров с параметрами URL-адреса и URL-категории.
- Для настройки доступа к веб-ресурсам используйте либо фильтры с параметрами DPI, либо фильтры с параметрами URL-адреса и URL-категории.
- В сетевых фильтрах с параметром URL-адреса используйте соответствующие MIME-типы, например, фильтр на `application/gzip` не будет срабатывать на `application/x-gzip`.
- Не используйте запрещающий фильтр с параметрами URL-адреса и URL-категории как фильтр по умолчанию, поскольку это может нарушить доступ к кросс-доменным веб-ресурсам.

Примеры использования транзитных фильтров

По умолчанию после инициализации ViPNet Coordinator HW весь транзитный трафик блокируется. Вы можете создавать транзитные фильтры и задействовать их для управления трафиком.

Настройка фильтрации трафика по пользователю

Предположим, что вам нужно настроить фильтрацию трафика для пользователя с именем `ivanov` в локальной сети, защищённой ViPNet Coordinator HW, таким образом, чтобы:

- разрешить отправку электронных писем только с помощью корпоративного почтового приложения Microsoft Outlook и запретить использование сторонних почтовых сервисов;
- запретить доступ к социальной сети Facebook;
- запретить доступ к облачным файловым сервисам Dropbox и Google Drive.

Для реализации данной политики безопасности создайте следующие сетевые фильтры:

1 Транзитный фильтр, блокирующий трафик группы приложений Mail:

```
hostname# firewall forward add src @any dst @any dpigroup Mail dnuser ivanov drop
```

2 Транзитный фильтр, разрешающий отправку писем через приложение Microsoft Outlook:

```
hostname# firewall forward add src @any dst @any dpiapp "Microsoft Outlook" dnuser ivanov pass
```

3 Транзитный фильтр, блокирующий трафик приложения социальной сети Facebook:

```
hostname# firewall forward add src @any dst @any dpiapp Facebook dnuser ivanov drop
```

4 Транзитный фильтр, блокирующий трафик приложений облачных файловых сервисов Dropbox и Google Drive:

```
hostname# firewall forward add src @any dst @any dpiapp Dropbox,"Google Drive" dnuser ivanov drop
```

Настройка фильтрации трафика Torrent-клиентов

Чтобы заблокировать работу Torrent-клиентов на компьютерах локальной сети, защищённой ViPNet Coordinator HW, создайте запрещающие сетевые фильтры для протоколов:

- BitTorrent — протокол обмена файлами между Torrent-клиентами;
- Teredo — протокол инкапсуляции пакетов IPv6 в IPv4, позволяющий Torrent-клиентам обмениваться файлами даже при блокировке протокола BitTorrent.

Для создания запрещающих сетевых фильтров выполните команду:

```
hostname# firewall forward add src @any dst @any dpiprotocol bittorrent,teredo drop
```

В результате выполненных действий вы заблокируете работу Torrent-клиентов в вашей сети.

Деактивация транзитных фильтров открытой сети после обновления ПО

После обновления ПО ViPNet Coordinator HW могут измениться схемы описания прикладных протоколов, приложений и групп приложений. В этом случае транзитные фильтры будут изменены:

- Если транзитный фильтр содержит параметр (прикладной протокол, приложение или группу приложений), который отсутствует в новой схеме, то такой параметр не учитывается и помечается как неподдерживаемый (**Unsupported**).

- Если в транзитном фильтре остаются только неподдерживаемые параметры, то фильтр помечается как неактивный (**Inactive**) и не используется для фильтрации трафика.

```
 User:
Current Rules Set Id: 10
================================================================================
Num    UID-Name                                          Option  Schedule
Act    Protocol              Source                   -> Destination
       DpiProtocol           [G]DpiGroup, DpiApp         DomainUser
================================================================================
1      4000001 -                                         User
drop   @any                  @any                     -> @any
                                                          @any
       @any                  opera mini
--------------------------------------------------------------------------------
2      4000002 -                                         User
pass   @any                  @any                     -> @any
                                                          @any
       @any                  @any
--------------------------------------------------------------------------------
3      (inactive)  -                                     User
drop   @any
                             @any                     -> @any
       @any                                              @any
                             youku tudou, skype
--------------------------------------------------------------------------------
4      (unsupported)  -                                  User
drop   @any                                              @any
                             @any                     -> @any
       @any
                             comodounite(unsupported)
--------------------------------------------------------------------------------
```

Рисунок 26. Отображение неактивного правила

При необходимости, вы можете изменить неактивный фильтр, но не сможете его активировать.

Настройка правил трансляции адресов

Общие сведения о трансляции сетевых адресов

Трансляция сетевых адресов (NAT) — механизм преобразования IP-адресов одной сети в IP-адреса другой сети в соответствии с RFC 2663.



Внимание! Правила трансляции сетевых адресов, описанные в этом разделе, относятся только к открытому трафику.

ViPNet Coordinator HW может выполнять:

- Трансляцию адреса источника (динамическую трансляцию или masquerading).

  В этом случае при прохождении через координатор IP-пакетов от отправителей с частными IP-адресами в них заменяется адрес отправителя на внешний (реальный) адрес интерфейса координатора или адрес из другой сети. При получении ответных пакетов в них подменяется IP-адрес получателя обратно на частный IP-адрес, и в таком виде пакет доставляется в частную сеть.

  Используется:

  - Для подключения локальной сети к интернету, когда количество узлов локальной сети превышает выданное поставщиком услуг интернета количество публичных IP-адресов. В результате локальные сети, использующие частные IP-адреса, получают доступ к ресурсам интернета.
  - Для балансировки нагрузки сети.

- Трансляцию адреса назначения (статическая трансляция или port forwarding).

  В этом случае IP-пакеты, приходящие из интернета на определенный порт внешнего адреса координатора, перенаправляются на указанный адрес внутренней сети путем подмены в них адреса получателя, а у ответных пакетов от узла внутренней сети подменяется адрес отправителя.

  Используется для организации доступа к ресурсам локальной сети из интернета. В результате локальные сети, использующие частные адреса, могут быть доступны пользователям интернета по публичным IP-адресам.

- Одновременную трансляцию сетевых адресов источника и назначения.

  Используется в сложных схемах маршрутизации трафика.

Трансляция сетевых адресов настраивается с помощью правил. При этом координатор должен иметь как минимум два сетевых интерфейса:

- внешний — имеет публичный IP-адрес и обеспечивает доступ в интернет;

- внутренний — имеет частный IP-адрес.

Подсчет срабатываний правил трансляции адресов

Для каждого правила трансляции сетевых адресов ведется постоянный подсчет срабатываний, начиная с момента первого включения ViPNet Coordinator HW до первого сброса срабатываний из ViPNet Prime вручную, и далее — между сбросами срабатываний из ViPNet Prime. Перезагрузка ViPNet Coordinator HW, обновление ПО или переключение узлов кластера не влияют на подсчет срабатываний. Просмотр срабатываний правил трансляции адресов доступен только в веб-интерфейсе ViPNet Coordinator HW.

Трансляция адреса источника

Трансляция адреса источника предназначена для организации доступа узлов локальной сети в интернет. Правило трансляции адреса источника ставит в соответствие нескольким частным IP-адресам локальных сетевых узлов публичный IP-адрес координатора. Таким образом, узлы локальной сети могут устанавливать соединения с узлами в интернете от имени публичного IP-адреса координатора.



Рисунок 27. Организация доступа в интернет при помощи правила трансляции IP-адреса источника

Если на координаторе настроено правило трансляции адреса источника, то транзитные IP-пакеты, проходящие через координатор из локальной сети в интернет, будут преобразованы:

- В момент передачи IP-пакета из локальной сети в интернет координатор преобразует IP-адрес (или IP-адрес и порт) отправителя пакета для протоколов TCP и UDP. Для пакетов протокола ICMP преобразуется адрес отправителя, остальные параметры запоминаются. При этом частный IP-адрес отправителя заменяется на публичный IP-адрес внешнего сетевого интерфейса координатора, обеспечивающего доступ во внешнюю сеть. При дальнейшей передаче в интернете пакет имеет публичный IP-адрес отправителя. Номера портов отправителя (для протоколов TCP и UDP) и запоминаемые параметры (для протокола ICMP) пакетов имеют уникальные значения для всех исходящих IP-соединений внешнего сетевого интерфейса координатора. После преобразования пакет отправляется адресату в интернете.
- При прохождении ответных IP-пакетов ViPNet Coordinator HW производит обратное преобразование указанных параметров. То есть в момент передачи ответного IP-пакета координатор заменяет в нем IP-адрес получателя на частный IP-адрес узла локальной сети, которому адресован ответный пакет. Преобразование происходит на основании уникальных номеров портов, присвоенных исходящим пакетам (для протоколов TCP и UDP), и

запоминаемых параметров исходящих пакетов (для протокола ICMP). Номера портов (для протоколов TCP и UDP) также преобразуются в свои истинные значения. Затем ответные пакеты передаются через внутренний сетевой интерфейс узлу локальной сети, которому адресован пакет.

Примечание. Для всех протоколов, кроме TCP, UDP и ICMP, преобразуются только IP-адреса. Для протоколов с частичным преобразованием трансляция адреса источника не будет работать, если несколько узлов локальной сети одновременно инициируют соединение с одним и тем же IP-адресом публичной сети.

Трансляция адреса назначения

Трансляция адреса узла назначения применяется для организации доступа из интернета к серверам локальной сети, не имеющим публичного IP-адреса. Правило трансляции адреса назначения ставит в соответствие частным IP-адресам локальных сетевых узлов публичный IP-адрес координатора. Таким образом, по публичному IP-адресу внешние пользователи могут получить доступ к ресурсам локальной сети.

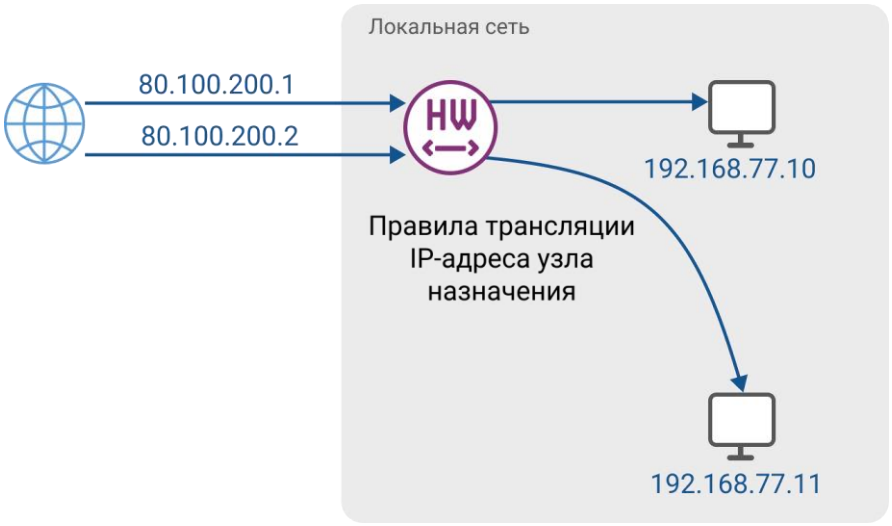


Рисунок 28. Доступ к внутренним ресурсам при помощи правил трансляции IP-адресов узлов назначения

Если для публичного IP-адреса координатора задано правило трансляции адреса назначения, то при обращении к этому IP-адресу из интернета будут выполняться преобразования:

- Во входящих IP-пакетах от внешнего узла координатор подменяет адрес получателя (публичный IP-адрес координатора) локальным IP-адресом в соответствии с правилом. Затем пакет передаётся через внутренний сетевой интерфейс на узел локальной сети, которому адресован пакет.
- При прохождении ответных IP-пакетов (в рамках уже созданной сессии) координатор производит обратную замену IP-адресов. Адрес отправителя (IP-адрес локального узла) подменяется публичным IP-адресом внешнего сетевого интерфейса координатора. Затем ответный пакет отправляется узлу в интернете.

Таким образом, при передаче в интернете IP-пакет выглядит так, будто отправитель и получатель этого пакета имеют публичные IP-адреса.



Внимание! При трансляции адреса узла назначения инициировать соединение может только внешний сетевой узел. Чтобы локальный сетевой узел мог также иметь доступ в интернет (двусторонний NAT), необходимо в дополнение к правилу трансляции адреса узла назначения задать также правило трансляции адреса источника.

Создание правила трансляции адресов



Примечание. Правила трансляции адресов работают только при наличии транзитных фильтров открытой сети, пропускающих трафик от узлов, к которым они будут применяться.

Чтобы создать правило трансляции адресов, выполните команду:

`hostname# firewall nat add [<номер>] [rule <имя>] src <адрес отправителя> dst <адрес получателя> [<протокол>] [<расписание>] change {src <адрес отправителя> | dst <адрес получателя>}`, указав следующие параметры:

- Порядковый номер правила в таблице, определяющий его приоритет. Чем меньше порядковый номер правила, тем выше его приоритет (наиболее приоритетное правило имеет номер 1). При создании правила с порядковым номером, меньшим максимального номера в таблице правил, номера правил, следующих за этим правилом, автоматически увеличиваются на единицу (то есть их приоритет понижается).
- Имя правила. Если имя состоит из нескольких слов, разделенных пробелом, заключите его в кавычки (например, `rule "number one"`).



Примечание. При создании правила трансляции адресов можно не указывать его номер. В этом случае правилу будет присвоен номер, следующий за номером последнего правила в таблице, и оно будет иметь самый низкий приоритет.

Имя правила можно не указывать, правило будет создано без имени.

- Параметры, определяющие обработку трафика:
  - адрес отправителя и адрес получателя являются обязательными параметрами правила и задаются в виде IP-адреса или доменного имени узла, диапазона IP-адресов узлов, списка IP-адресов или доменных имен узлов, маски адресов подсети, доменного имени сети, одной или нескольких пользовательских групп IP-узлов;
  - протокол и расписание являются необязательными параметрами правила и задаются так же, как для сетевых фильтров;
  - действие правила в виде одной из лексем:
    - для трансляции адреса источника: `change src {<адрес> | auto}`, указав адрес (внешний адрес координатора или адрес из другой сети), на который будет

заменяться адрес отправителя пакетов, либо параметр `auto`, чтобы адрес отправителя автоматически заменялся на публичный адрес внешнего сетевого интерфейса координатора.



Примечание. При использовании в `change src` IP-адреса, не принадлежащего ViPNet Coordinator HW, на сетевом устройстве, расположенным за ViPNet Coordinator HW, настройте обратную маршрутизацию на ViPNet Coordinator HW (или на другое устройство, например для балансировки) для корректной обработки ответного трафика.

Если на сетевом устройстве нельзя настроить обратную маршрутизацию, используйте в `change src` только IP-адреса, принадлежащие ViPNet Coordinator HW, или автоматическое определение адреса исходящего интерфейса (`auto`).

- для трансляции адреса и/или порта назначения: `change dst <адрес>:[<порт>]`, указав адрес и/или порт узла локальной сети, которому будут перенаправляться пакеты.



Примечание. Созданное правило трансляции сетевых адресов будет работать для новых соединений. Для уже установленных соединений правило будет работать после истечения времени жизни соединения. Чтобы принудительно применить правило трансляции сетевых адресов, выполните сброс соединений:

```
hostname# firewall conntrack flush
```

Примеры создания правил трансляции адресов

- Чтобы при отправке пакета узлом с адресом 10.0.0.1 внешнему узлу с адресом 185.37.128.163 частный адрес отправителя пакета заменялся на публичный адрес внешнего сетевого интерфейса координатора, создайте правило трансляции адреса источника:

  ```
  hostname# firewall nat add src 10.0.0.1 dst 185.37.128.163 change src auto
  ```

- Чтобы во входящих пакетах на публичный IP-адрес координатора от внешнего узла mydomain.ru адрес получателя подменялся на 10.0.0.7, создайте правило трансляции адреса назначения:

  ```
  hostname# firewall nat add src mydomain.ru dst 192.0.2.1 change dst 10.0.0.7
  ```

- Чтобы во входящих пакетах на публичный IP-адрес и порт 8080 координатора от внешнего узла mydomain.ru адрес получателя подменялся на 10.0.0.7 и порт 8080, создайте правило трансляции адреса назначения:

  ```
  hostname# firewall nat add src mydomain.ru dst 192.0.2.1 tcp dport 8080 change dst
  10.0.0.7:8080
  ```

Просмотр, изменение, удаление правил трансляции сетевых адресов

Вы можете просмотреть, изменить или удалить правила трансляции сетевых адресов, заданные на ViPNet Coordinator HW.

Чтобы просмотреть правила, выполните одну из команд:

- для просмотра всех правил:

  ```
  hostname> firewall nat show
  ```

- для просмотра правил с конкретными параметрами:

  ```
  hostname> firewall nat show <параметр>,
  ```

  указав в качестве параметра порядковый номер, имя, адрес отправителя, адрес получателя или протокол. При необходимости вы можете указать несколько параметров.

Примечание. Поиск правил трансляции сетевых адресов выполняется по строгому совпадению с указанными параметрами.

В результате выполнения команды будет отображена таблица, содержащая правила трансляции сетевых адресов.

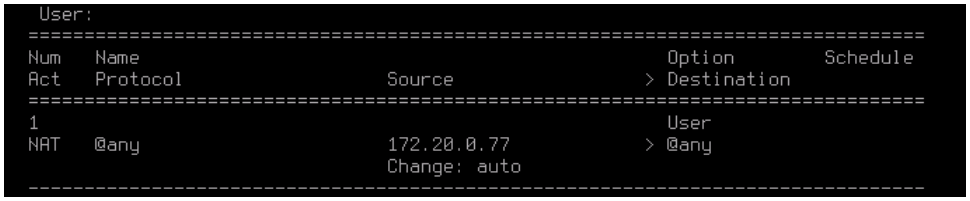


Рисунок 29. Просмотр правил трансляции сетевых адресов

Таблица содержит следующие столбцы:

- `Num` — порядковый номер правила, определяющий его приоритет.
- `Name` — имя правила.
- `Option` — категория правила: для правил из Policy Management (модуль Prime) — `Policy`, для правил пользователя — `User`.
- `Schedule` — расписание применения правила.
- `Act` — действие правила (`NAT`).
- `Source` — адрес источника до или после трансляции.
- `Destination` — адрес назначения до или после трансляции.
- `Protocol` — протокол.

Внимание! Если из Policy Management (модуль Prime) поступили правила трансляции сетевых адресов, в которых указан порт, но не указан протокол, они будут применены для протоколов TCP и UDP. Чтобы не открывать лишние порты, укажите протоколы для этих правил в Policy Management (модуль Prime) и отправьте политики еще раз.

Изменение и удаление правил трансляции сетевых адресов выполняется аналогично изменению и удалению сетевых фильтров:

```
hostname# firewall nat change append <номер> <параметры>
```

```
hostname# firewall nat delete <параметры>
```

Подробнее см. в разделах Изменение сетевого фильтра и Удаление сетевого фильтра.

Сценарии использования правил трансляции адресов

Настройка доступа ПК локальной сети к интернету

С помощью правил трансляции адреса источника вы можете настроить доступ ПК локальной сети к интернету:

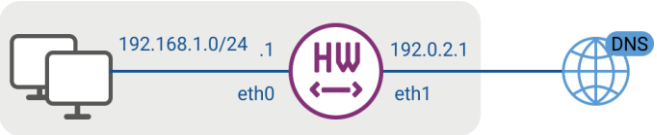


Рисунок 30. Доступ ПК локальной сети к интернету

1 Создайте правило трансляции адреса источника: частных IP-адресов сети 192.168.1.0/24 в IP-адрес 192.0.2.1 внешнего сетевого интерфейса HW:

```
hostname# firewall nat add src 192.168.1.0/24 dst @InternetIP change src 192.0.2.1
```

2 Создайте разрешающий транзитный фильтр открытой сети для доступа с использованием любого протокола:

```
hostname# firewall forward add src 192.168.1.0/24 dst @InternetIP pass
```

3 Создайте разрешающие транзитные фильтры открытой сети для обращения к публичным DNS-серверам:

```
hostname# firewall forward add src 192.168.1.0/24 dst @InternetIP tcp dport 53 pass
hostname# firewall forward add src 192.168.1.0/24 dst @InternetIP udp dport 53 pass
```

Настройка доступа к серверу в DMZ

В локальной сети наиболее уязвимыми для сетевых атак являются узлы, которые взаимодействуют с внешними системами или предоставляют различные сервисы внешним пользователям, например почтовые или веб-серверы. В случае атаки на них под угрозой оказывается вся локальная сеть. Для защиты локальную сеть разбивают на сегменты, размещая серверы в демилитаризованной зоне (DMZ). Эту зону отделяют от внутреннего сегмента межсетевым экраном, который контролирует трафик между сегментами. При этом сервисы, предоставляемые серверами, доступны как внешним пользователям, так и пользователям локальной сети. В то же время внутренний сегмент недоступен внешним пользователям.

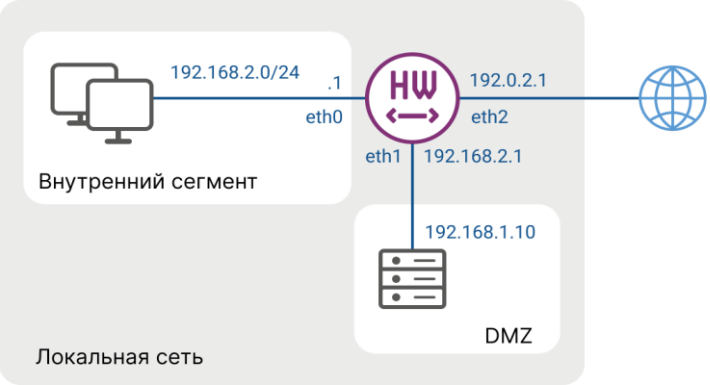


Рисунок 31. Размещения общедоступного сервера в DMZ

Чтобы настроить доступ для сетевых узлов во внутреннем сегменте и DMZ:

1 Убедитесь, что TCP-туннель выключен:

```
hostname# iplir show tcptunnel-info
```

2 Если TCP-туннель включен, выключите его:

```
hostname# iplir tcptunnel server off
```

3 Создайте транзитные фильтры открытой сети:

3.1 фильтр, разрешающий доступ из внутреннего сегмента с любыми IP-адресами:

```
hostname# firewall forward add src 192.168.2.0/24 dst @any pass
```

3.2 фильтр, разрешающий доступ веб-сервером по протоколу HTTP с любых IP-адресов:

```
hostname# firewall forward add src @any dst 192.168.1.10 tcp dport 80 pass
```

Остальной транзитный трафик будет блокироваться сетевым фильтром по умолчанию.

4 Создайте правила трансляции сетевых адресов:

- правило для доступа в интернет из внутреннего сегмента:

```
hostname# firewall nat add src 192.168.2.0/24 dst @InternetIP change src 192.0.2.1
```

- правило для доступа к серверу в DMZ из интернета:

```
hostname# firewall nat add src @InternetIP dst 192.0.2.1 tcp dport 80 change dst
192.168.1.10
```

Настройка доступа к узлам локальной сети с помощью дополнительных IP-адресов

Вы можете настроить доступ к сетевым узлам локальной сети, например к почтовому и веб-серверу, из интернета с помощью дополнительных IP-адресов на внешнем интерфейсе HW и правил статической трансляции адресов.

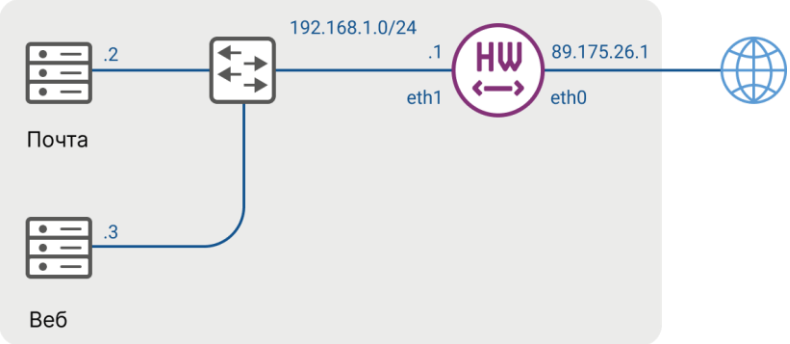


Рисунок 32. Доступ к серверам локальной сети из интернета

Чтобы настроить доступ:

1 На внешнем интерфейсе `eth0` задайте дополнительные IP-адреса:

```
hostname# inet ifconfig eth0 address add 89.175.26.2 netmask 255.255.255.0
hostname# inet ifconfig eth0 address add 89.175.26.3 netmask 255.255.255.0
```

2 Создайте правила трансляции адреса получателя:

```
hostname# firewall nat add src @InternetIP dst 89.175.26.2 tcp dport 25 change dst
192.168.1.2:25
hostname# firewall nat add src @InternetIP dst 89.175.26.3 tcp dport 80 change dst
192.168.1.3:80
```

3 Создайте разрешающие сетевые фильтры:

```
hostname# firewall forward add src @InternetIP dst 192.168.1.2 tcp dport 25 pass


hostname# firewall forward add src @InternetIP dst 192.168.1.3 tcp dport 80 pass
```

Теперь почтовый сервер будет доступен из интернета по адресу 89.175.26.2:25, а веб-сервер — по адресу 89.175.26.3:80.

Настройка доступа удаленных клиентов по протоколу PPTP

Вы можете настроить доступ удаленных клиентов по протоколу PPTP к серверу, установленному в локальной сети.

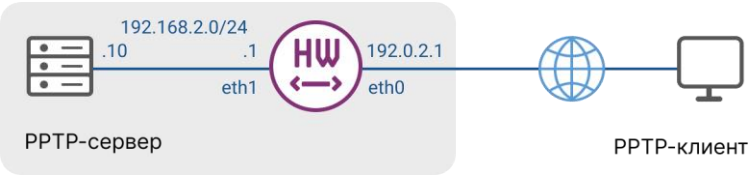


Рисунок 33. Доступ удаленных клиентов по протоколу PPTP

Протокол PPTP VPN одновременно использует два соединения — TCP- и GRE-соединение. Когда PPTP-клиент обращается к PPTP-серверу, клиент инициирует TCP-соединение с портом назначения 1723. После этого PPTP-сервер инициирует соединение по IP-протоколу GRE, который инкапсулирует пакеты протокола PPTP в IP-пакеты. Через GRE-соединение происходит пересылка данных, а TCP-соединение используется как управляющий канал для поддержки GRE-соединения.

Чтобы настроить доступ:

1 Добавьте правила трансляции адресов:

1.1 правило трансляции адреса источника для GRE:

```
hostname# firewall nat add 1 src 192.168.2.10 dst @InternetIP service @GRE change src 192.0.2.1
```

1.2 правила трансляции адреса назначения для TCP и GRE:

```
hostname# firewall nat add 2 src @InternetIP dst 192.0.2.1 tcp dport 1723 change dst 192.168.2.10
```

```
hostname# firewall nat add 3 src @InternetIP dst 192.0.2.1 service @GRE change dst 192.168.2.10
```

2 Добавьте транзитные фильтры открытой сети:

```
hostname# firewall forward add 1 src 192.168.2.10 dst @InternetIP service @GRE pass
```

```
hostname# firewall forward add 2 src @InternetIP dst 192.168.2.10 tcp dport 1723 pass
```

```
hostname# firewall forward add 3 src @InternetIP dst 192.168.2.10 service @GRE pass
```

Настройка обработки прикладных протоколов DNS, FTP, H.323, SCCP, SIP

О прикладных протоколах

Прикладные протоколы обеспечивают работу пользовательских сетевых сервисов, например, IP-телефонии, DNS-службы, FTP-службы. При использовании данных служб IP-адреса часто передаются в теле IP-пакета. Эта особенность может повлиять на доступность сервисов в защищенной сети с виртуальной адресацией или трансляцией сетевых адресов. Кроме того, некоторые прикладные протоколы, помимо управляющего соединения, открывают для передачи данных дополнительные соединения на случайно выбранный порт. Поскольку номер порта заранее неизвестен, то для IP-пакетов невозможно создать разрешающий сетевой фильтр, следовательно, соединение будет заблокировано.

ViPNet Coordinator HW может выполнять роль шлюза прикладного уровня, который позволяет решить перечисленные выше проблемы, обеспечивая:

- Подмену виртуального IP-адреса узла защищённой сети в теле IP-пакета на реальный.
- Статическую и динамическую трансляцию IP-адреса при передаче транзитного трафика (только для протокола FTP).
- Включение сетевого фильтра, пропускающего IP-пакеты, для дополнительного соединения на случайно выбранный порт, который используется прикладным протоколом. При этом для установления управляющего соединения с открытыми узлами на узле необходимо задать соответствующие фильтры открытой сети.



Внимание! Обработка прикладного протокола в сетевом трафике, проходящем трансляцию сетевых адресов назначения, поддерживается только для прикладного протокола FTP в случае, когда FTP-клиент создает соединение с ViPNet Coordinator HW, который перенаправляет трафик к FTP-серверу по открытому каналу.

В ViPNet Coordinator HW можно настроить обработку следующих прикладных протоколов:

- DNS — для доступа к сетевым узлам по доменным именам.
- FTP — для передачи файлов между FTP-клиентом и FTP-сервером.

  Команды FTP-протокола EPRT и EPSV, используемые некоторыми FTP-клиентами, не поддерживаются ViPNet Coordinator HW.
- H.323 — для передачи мультимедийных данных в IP-сетях (IP-телефония, видео- и аудиоконференции).

Передача мультимедийных данных с использованием протокола H.323 возможна только между телекоммуникационными серверами, туннелируемыми ViPNet Coordinator HW. При этом на координаторе должен быть разрешен весь туннелируемый трафик, поскольку между телекоммуникационными серверами могут устанавливаться дополнительные соединения.

- SCCP — для передачи сообщений между Skinny-клиентами (проводными и беспроводными IP-телефонами Cisco) и сервером голосовой почты (Cisco Unity Connection и Cisco Unified Communication Manager (CallManager)).

  Передача мультимедийных данных с использованием протокола SCCP возможна, если сервер голосовой почты туннелируется координатором ViPNet Coordinator HW.

  Примечание. ViPNet Coordinator HW также поддерживает обработку прикладного протокола Cisco NetMeeting для организации видеоконференций, но только при использовании видимости по реальным IP-адресам между клиентским ПО Cisco Meeting App в сети ViPNet и туннелируемым сервером Cisco Meeting Server.

- SIP — для установки соединений, включающих обмен мультимедийными данными между клиентами (IP-телефония, видео- и аудиоконференции).

  Не поддерживаются SIP-клиенты и телекоммуникационные серверы, использующие при подключении протокол TLS, «компактные поля» (compact headers) или сжатие данных в сообщениях SIP.

  Для некоторых SIP-клиентов могут не обрабатываться такие дополнительные данные, как телефонные справочники, информация о доступности абонента и другие.

По умолчанию установка соединения с открытыми узлами запрещена. Чтобы разрешить ее, создайте разрешающий сетевой фильтр.

Обработка протокола DNS

В сетях ViPNet приложения могут использовать виртуальные IP-адреса, реально не существующие в сети и уникальные на каждом сетевом узле, что позволяет избежать конфликтов при наличии пересекающихся адресов в разных сетях.

Чтобы узлы внутренней сети ViPNet могли обращаться к удаленным узлам ViPNet по доменным именам через туннелируемый DNS-сервер, требуются дополнительные настройки на DNS-сервере и узлах сети ViPNet:

1. На DNS-сервере настройте поддержку динамического изменения DNS-записей. Как правило, по умолчанию DNS-серверы не поддерживают эту настройку.
2. Для клиентов, к которым будут обращаться по DNS-имени:
   - **2.1** В ViPNet Prime укажите корпоративный DNS-сервер.
   - **2.2** На самих клиентах настройте автоматическую регистрацию на DNS-сервере.
3. На туннелирующем координаторе включите обработку протокола.

Обработка протокола FTP

При передаче файлов между клиентом и сервером по протоколу FTP устанавливается как минимум два TCP-соединения:

- для отправки команд на сервер и получения ответов от него (управляющее TCP-соединение);
- для передачи данных (дополнительное TCP-соединение).

Установка TCP-соединений по протоколу FTP происходит в следующем порядке:

1. Клиент создает управляющее TCP-соединение с сервером со своего порта из диапазона 1024-65535 на 21-й порт сервера.
2. В зависимости от выбранного режима передачи данных, клиент отправляет по управляющему соединению:
   - номер порта, открытого клиентом для получения данных с сервера (активный режим);
   - запрос на номер порта сервера, к которому будет подключаться клиент (пассивный режим).
3. В зависимости от используемого режима передачи данных, соединение устанавливается одним из двух способов:
   - сервер создает дополнительное соединение для передачи данных на указанный клиентом порт (активный режим);
   - сервер по управляющему соединению передает клиенту номер порта, к которому клиент создает дополнительное соединение (пассивный режим).

Таким образом, в активном режиме соединение для передачи данных создает сервер, а в пассивном — клиент.

Для установки управляющего и дополнительного соединений в активном или пассивном режиме работы протокола FTP:

1. Создайте фильтр открытой сети, разрешающий исходящее TCP-соединение на 21-й порт FTP-сервера.
2. Для разрешения дополнительного соединения в активном режиме работы включите обработку протокола FTP (см. Настройка параметров обработки прикладных протоколов), которая добавляет необходимый сетевой фильтр.
3. Для разрешения дополнительного соединения в пассивном режиме работы настройки не требуются.

Обработка протокола SIP

SIP-клиент отправляет запрос (например, приглашение для установки соединения, подтверждение приема ответа на запрос, завершение соединения) другому SIP-клиенту с указанием его SIP-адреса. В зависимости от способа установки соединения запрос направляется второму клиенту либо напрямую, либо через SIP-сервер. Вызываемый клиент передает вызывающему клиенту ответ на запрос (например, информацию об успешной обработке запроса, отклонении вызова, ошибке при

обработке запроса). По умолчанию TCP- и UDP-соединения устанавливаются через порты 5060 и 5080.

Чтобы установить соединение между SIP-клиентами:

1 Убедитесь, что включена обработка протокола SIP.

2 Если хотя бы один из SIP-клиентов является открытым узлом, создайте фильтр открытой сети, разрешающий входящее и исходящее соединение по протоколам TCP и UDP на порты 5060 и 5080.



Примечание. Некоторые SIP-клиенты, например SIP-клиент компании Zoiper, могут устанавливать соединения TCP и UDP не через порт 5060, а через динамический порт, выбранный произвольно из определенного диапазона. Поэтому если хотя бы один из SIP-клиентов является открытым узлом, возможность использования динамических портов необходимо отключить в настройках SIP-клиента.

При установке соединений между SIP-клиентами действуют ограничения:

- Между SIP-клиентами нельзя использовать статическую или динамическую трансляцию IP-адресов.
- Если хотя бы один из SIP-клиентов является открытым узлом, то для всех узлов защищённой сети должна быть настроена видимость по реальным IP-адресам.

Настройка параметров обработки прикладных протоколов

Просмотр текущих настроек

```
hostname# alg show

H323 direct media: off

H323 direct h245: off

SIP direct media: off

SIP insert rport: off

SIP expect asymmetric response: off

SIP expect asymmetric request: off

SIP strict translation: on
================================================================================
SERVICE        PROTOCOL PORTS                                          ON/OFF
================================================================================
FTP            TCP      21                                             ON
--------------------------------------------------------------------------------
DNS            UDP      53                                             ON
--------------------------------------------------------------------------------
```

```
H323            TCP      1720                                                ON
--------------------------------------------------------------------------------
H323            UDP      1719                                                ON
--------------------------------------------------------------------------------
SCCP            TCP      2000                                                ON
--------------------------------------------------------------------------------
SIP             TCP      5060,5080                                           ON
--------------------------------------------------------------------------------
SIP             UDP      5060,5080                                           ON
--------------------------------------------------------------------------------
```

В результате выполнения команды отображаются:

- Параметры настройки обработки протокола SIP:
  - `SIP insert rport` — автоматическое добавление параметра `rport` в SIP-запросы, проходящие через ViPNet Coordinator HW;
  - `SIP expect asymmetric response` — автоматическое добавление сетевых фильтров, пропускающих ответы от SIP-сервера к SIP-клиентам с UDP-портов, отличных от открытой сигнальной сессии;
  - `SIP expect asymmetric request` — автоматическое добавление сетевых фильтров, пропускающих запросы от SIP-клиентов к SIP-серверу с UDP-портов, отличных от открытой сигнальной сессии;
  - `SIP strict translation` — условия трансляции IP-адресов внутри SIP-сообщений:
    - `on` — транслировать IP-адреса и порты в SIP-сообщениях, только если они совпадают с IP-адресом и портом в IP-пакете;
    - `off` — транслировать IP-адреса в SIP-сообщениях без проверки соответствия порта из SIP-сообщения портам в IP-пакете;
- Таблица с параметрами обработки прикладных протоколов, содержащая следующие столбцы:
  - `SERVICE` — прикладной протокол: `DNS`, `FTP`, `H.323`, `SCCP`, `SIP`;
  - `PROTOCOL` — транспортный протокол, используемый прикладным протоколом;
  - `PORTS` — порты, используемые прикладным протоколом;
  - `ON/OFF` — состояние обработки: `ON` (включена) или `OFF` (выключена).

Настройка параметров обработки

По умолчанию обработка прикладных протоколов DNS, FTP, H.323, SCCP, SIP включена. Чтобы настроить обработку какого-либо из них:

```
hostname# alg module <прикладной протокол> process <транспортный протокол> <порты> on
```

указав:

- один из прикладных протоколов: `dns`, `ftp`, `h323`, `sccp` или `sip`;
- один из транспортных протоколов: `tcp` или `udp`;

- порт, диапазон портов либо список, состоящий из портов или их диапазонов, разделенных запятой.

Чтобы изменить ранее выбранный транспортный протокол или порты для обработки какого-либо прикладного протокола, необходимо настроить и включить обработку этого прикладного протокола заново. Например, если кроме стандартных портов для обработки данных, передаваемых по протоколу SIP, используются еще несколько портов для протокола UDP, то их можно добавить:

```
hostname# alg module sip process udp 10000,21-65 on
```

По умолчанию передача медиапотоков между SIP- и H.323-клиентами задана через сервер, а передача медиапотоков напрямую блокируются. Чтобы разрешить передачу медиапотоков между клиентами напрямую:

```
hostname# alg module <H323|SIP> direct-media off
```

При этом определяющими будут настройки на SIP- и H.323-клиентах, в зависимости от которых медиапотоки могут передаваться или напрямую, или через сервер.

Для согласования параметров связи между клиентами протокол H.323 использует протокол H.245. По умолчанию согласование параметров задано через сервер. Чтобы разрешить согласование параметров связи между клиентами напрямую:

```
hostname# alg module H323 direct-h245 off
```

При этом определяющими будут настройки на H.323-клиентах, в зависимости от которых параметры связи могут согласовываться или напрямую, или через сервер.

Чтобы настройки передачи медиапотоков и согласование параметров связи вступили в силу, сбросьте установленные соединения:

```
hostname# firewall conntrack flush
```

Примечание. На ViPNet Coordinator HW, установленном на границе защищаемой сети, рекомендуется использовать передачу медиапотоков и согласование параметров связи через сервер. Иначе, если необходимо взаимодействие клиентов напрямую, разместите ViPNet Coordinator HW внутри защищенного периметра.

Чтобы выключить обработку прикладного протокола:

```
hostname# alg module <прикладной протокол> process off
```

Примечание. После настройки обработки прикладных протоколов (включить или выключить обработку, изменить порт) необходимо перезапустить приложение (например, DNS-, FTP-, SIP-клиент) или устройство (например, SIP-телефон).

Настройка синхронизации сессий в кластере

По умолчанию синхронизация сессий прикладных протоколов в кластере выключена. Чтобы ее включить, на обоих узлах:

1 Завершите работу системы защиты от сбоев:

```
hostname# failover stop
```

2 Откройте файл `failover.ini` для изменения:

```
hostname# failover config edit
```

3 В секции `[misc]` задайте `syncalgtcp = yes`.

4 Нажмите **Ctrl+O**, затем **Ctrl+X**.

5 Запустите систему защиты от сбоев:

```
hostname# failover start
```

Чтобы выключить синхронизацию сессий, на шаге 3 предыдущего сценария задайте `syncalgtcp = no`.

Особенности обработки протокола SIP

Для передачи данных между устройствами с помощью протокола SIP сначала устанавливается соединение между участниками SIP-диалога (сигнальная сессия), в рамках которой согласовываются параметры передачи данных. Затем создаётся соединение по протоколу RTP для передачи мультимедийных данных (RTP-сессия).

Для RTP-сессии используются произвольные и отличные от сигнальной сессии порты. Номера этих портов заранее неизвестны. Чтобы RTP-трафик не блокировался при прохождении через ViPNet Coordinator HW:

1 Включите обработку протокола SIP, если она выключена. При этом укажите порт или порты, которые будут использоваться для установления соединения.

   Во время звонка с SIP-устройства ViPNet Coordinator HW будет извлекать IP-адреса и номера портов для RTP-сессии из пакетов сигнальной сессии и создавать временные сетевые фильтры, пропускающие RTP-трафик по полученным портам.

2 Для обработки SIP-трафика на прикладном уровне необходимо разрешить установление сигнальной сессии. Для этого создайте транзитные сетевые фильтры, разрешающие трафик по протоколу SIP.

Прохождение SIP-трафика также зависит от условий вашей сети и настроек SIP-устройств:

- По умолчанию временные сетевые фильтры для RTP-трафика автоматически создаются на ViPNet Coordinator HW только для IP-адресов участников SIP-диалога. Если для медиапотока используется отдельный медиасервер или организован непрямой маршрут прохождения голоса, RTP-трафик будет блокироваться (в разговоре будет отсутствовать звук). Чтобы временные сетевые фильтры для RTP-трафика создавались и пропускали трафик между любыми IP-адресами, которые указаны в SIP-сообщениях:

  ```
  hostname# alg module sip direct-media off
  ```

- Если ViPNet Coordinator HW транслирует адреса SIP-трафика на сетевом уровне, то трансляция адресов на прикладном уровне выполняется при условии, что IP-адрес и порт в SIP-сообщении совпадают с IP-адресом и портом из IP/UDP-заголовков пакета (до трансляции на сетевом уровне). Если в сети используется SIP-устройство, которое меняет порт источника, например

голосовой шлюз, и трансляция на прикладном уровне не выполняется, отключите проверку соответствия портов в UDP-заголовке пакета и SIP-сообщении:

```
hostname# alg module sip strict-translation off
```

- По умолчанию временные сетевые фильтры на ViPNet Coordinator HW автоматически создаются только для медиапотока, а ответы на SIP-запросы должны поступать в рамках уже открытой сигнальной сессии. Если в сети есть устройства, которые маршрутизируют SIP-сообщения на прикладном уровне, то новые запросы или ответы могут поступать с других или на другие, заранее неизвестные UDP-порты. Отправка SIP-сообщений с другими портами создаёт новые соединения, которые будут блокироваться.
  - Чтобы ViPNet Coordinator HW создавал временные пропускающие фильтры для ответов, поступающих по новым соединениям:

    ```
    hostname# alg module sip expect-asymmetric-response on
    ```

    В результате будут автоматически создаваться пропускающие фильтры с параметрами:

    `<IP-адрес сервера>:<любой порт> -> <IP-адрес клиента>:<исходящий порт первого соединения от клиента>`.
  - Чтобы ViPNet Coordinator HW создавал временные пропускающие фильтры для запросов, поступающих по новым соединениям:

    ```
    hostname# alg module sip expect-asymmetric-request on
    ```

    В результате будут автоматически создаваться пропускающие фильтры с параметрами:

    `<IP-адрес клиента>:<любой порт> -> <IP-адрес сервера из поля Contact предыдущего ответа от сервера>:<порт из поля Contact предыдущего ответа от сервера>`.
- По умолчанию SIP-сервер отвечает на порт, который указан в SIP-запросе, а не в заголовке UDP. Если IP-пакет, содержащий SIP-запрос, проходит через трансляцию адресов, то в заголовке UDP может измениться порт источника. В результате порт, указанный в SIP-запросе, не будет совпадать с портом из UDP-заголовка и ответ на запрос не достигнет SIP-клиента.

  В этом случае используйте параметр RFC-3581 `Symmetric Routing` (`rport`), чтобы SIP-сервер отвечал на адрес и порт из IP/UDP-заголовков и ответы отправлялись в уже открытую сессию:
  - включите этот параметр на SIP-клиентах, если это возможно;
  - или на ViPNet Coordinator HW включите добавление `rport` во все проходящие через него запросы:

    ```
    hostname# alg module sip insert-rport on
    ```



5

Настройка сетевых служб

Настройка DHCP-сервера 177

Настройка DHCP-relay 179

Сценарии настройки DHCP-сервера и DHCP-relay 181

Настройка DNS-сервера 191

Настройка NTP-сервера 193

Организация работы клиентов удаленного офиса с корпоративными DNS- и NTP-серверами 195

Настройка взаимодействия с Active Directory 197

Настройка взаимодействия с LDAP-сервером 202

Настройка точки доступа сети Wi-Fi 207

Настройка DHCP-сервера

В состав ViPNet Coordinator HW входит DHCP-сервер. Он динамически назначает IP-адреса сетевым узлам (DHCP-клиентам). Также DHCP-сервер может передать дополнительные параметры — IP-адреса шлюза по умолчанию, DNS-, NTP-сервера и другие.

DHCP-сервер может обслуживать DHCP-клиентов, которые находятся:

- в одной сети с DHCP-сервером, в том числе в сегментах сети, объединённых по L2OverIP;
- в удалённых подсетях с помощью агента DHCP-relay.

Чтобы настроить DHCP-сервер:

1 Включите сетевой интерфейс, на котором будет работать DHCP-сервер:

```
hostname# inet ifconfig <интерфейс> up
```

2 Задайте этот интерфейс для работы DHCP-сервера:

```
hostname# inet dhcp server add interface <интерфейс>
```



Примечание. Можно указать Ethernet-, VLAN-, Wi-Fi или агрегированный интерфейс, у которого настроен статический IP-адрес.

Если вы указали `wlan0`, настройте точку доступа к сети Wi-Fi.

3 Задайте диапазон IP-адресов, выделяемых клиентам:

```
hostname# inet dhcp server add range <начальный IP-адрес> <конечный IP-адрес>
{interface <интерфейс> | remote subnet <подсеть> mask <маска>}
```

Диапазон IP-адресов должен принадлежать сети интерфейса или заданной подсети (при указании `remote subnet`). IP-адрес интерфейса не должен входить в этот диапазон.



Примечание. DHCP-сервер может выделять клиентам любые диапазоны IP-адресов. Если локальная сеть маршрутизируется в интернет, используйте диапазоны, которые установлены стандартом для частных сетей: `10.0.0.0/8`, `172.16.0.0/12`, `192.168.0.0/16`.

4 Задайте дополнительные параметры:

- IP-адрес шлюза по умолчанию:

  ```
  hostname# inet dhcp server add router <IP-адрес> {interface <интерфейс> | remote
  subnet <подсеть> mask <маска> | host <имя узла>}
  ```

  IP-адрес шлюза должен принадлежать сети интерфейса и не должен входить в диапазон IP-адресов, выделяемых клиентам. В случае указания `remote subnet` IP-адреса шлюза должен принадлежать к указанной подсети `<subnet>`.

- IP-адрес DNS-сервера:

  ```
  hostname# inet dhcp server add dns <IP-адрес> [{interface <интерфейс> | remote
  subnet <подсеть> mask <маска> | host <имя узла>}]
  ```

- IP-адрес NTP-сервера:

```
hostname# inet dhcp server add ntp <IP-адрес> [{interface <интерфейс> | remote
subnet <подсеть> mask <маска> | host <имя узла>}]
```

Например, чтобы задать адрес DNS-сервера 192.168.15.41 для клиентов другой сети с адресом 192.168.1.0/24:

- Задайте `eth0` в качестве сетевого интерфейса, на котором DHCP-сервер будет обрабатывать запросы от агента DHCP-relay, работающего в удалённой подсети 192.168.1.0/24:

  ```
  hostname# inet dhcp server add relay-interface eth0 remote subnet 192.168.1.0 mask
  255.255.255.0
  ```

- Задайте адрес DNS-сервера 192.168.15.41 для клиентов сети 192.168.1.0/24:

  ```
  hostname# inet dhcp server add dns 192.168.15.41 remote subnet 192.168.1.0 mask
  255.255.255.0
  ```

5. Проверьте настройки DHCP-сервера:

   ```
   hostname# inet show dhcp server
   ```

6. Включите автоматический запуск DHCP-сервера:

   ```
   hostname# inet dhcp server mode on
   ```

   По умолчанию автоматический запуск DHCP-сервера выключен.

7. Запустите DHCP-сервер:

   ```
   hostname# inet dhcp server start
   ```

Чтобы просмотреть список клиентов DHCP-сервера:

`hostname# inet show dhcp server lease [{last | all | full}]`, где:

- `last` — вывести текущий список клиентов DHCP-сервера (по умолчанию).
- `all` — вывести полный список клиентов DHCP-сервера с историей аренды IP-адресов.
- `full` — вывести полный список клиентов DHCP-сервера без форматирования вывода.

Если несколько клиентов получили одинаковые IP-адреса, возможно, у них совпадает идентификатор DHCP-клиента (UID). Чтобы избежать этого, в сетевых настройках клиентов задайте MAC-адрес в качестве идентификатора DHCP.

Настройка DHCP-relay

ViPNet Coordinator HW можно использовать в качестве агента DHCP-relay. Он принимает от узлов DHCP-запросы и передаёт их DHCP-серверу. Ответы, полученные от DHCP-сервера, агент DHCP-relay перенаправляет сетевым узлам.

Внимание! Для приема и перенаправления DHCP-запросов через DHCP-relay необходимо, чтобы DHCP-сервер поддерживал Option 82 Suboption 5.

Агент DHCP-relay используется, когда сетевые узлы не могут обращаться напрямую к DHCP-серверу. Например, в разветвлённой сети из нескольких подсетей, в которых нет своего DHCP-сервера.

Агент DHCP-relay может работать с несколькими локальными сетями. Это могут быть как сети, подключённые к разным физическим сетевым интерфейсам ViPNet Coordinator HW, так и виртуальные локальные сети, подключённые к одному физическому интерфейсу.

К DHCP-серверу через ViPNet Coordinator HW могут обращаться узлы защищённой сети и открытые узлы. DHCP-сервер может быть защищённым, открытым или туннелируемым узлом.

Внимание!

Необходимо обеспечить доверенный канал передачи данных между ViPNet Coordinator HW и внешними системами (в том числе взаимодействующими системами защиты информации других типов), например выделенный физический канал или сеть ViPNet. Допускается осуществлять защиту каналов передачи данных организационными мерами, исключающими возможность утечки или перехвата защищаемых данных, или с помощью сертифицированных средств криптографической защиты информации.

Если агент DHCP-relay перенаправляет запросы на DHCP-сервер, который туннелируется другим координатором, настройте между координаторами видимость по реальным IP-адресам (см. Настройка видимости узлов). Если между ними настроена видимость по виртуальным адресам, ответы от DHCP-сервера будут отправляться на реальный адрес ViPNet Coordinator HW, выступающего в качестве агента DHCP-relay, и не будут доставлены.

Чтобы запустить DHCP-relay:

1 Задайте список сетевых интерфейсов, через которые DHCP-relay должен получать DHCP-запросы от клиентов. Чтобы добавить интерфейс в список:

```
hostname# inet dhcp relay [<номер копии>] add listen-interface <имя интерфейса>
```

Если номер копии процесса DHCP-relay не задан, то используется номер 1.

На каждом добавляемом сетевом интерфейсе должен быть задан статический IP-адрес, принадлежащий адресному пространству соответствующей подсети. Сетевой интерфейс, который используется для соединения с удаленным сервером может также получать IP-адрес по DHCP.

2 Задайте внешний DHCP-сервер для перенаправления DHCP-запросов клиентов и сетевой интерфейс ViPNet Coordinator HW для доступа к удаленному серверу:

```
hostname# inet dhcp relay [<номер копии>] add external-interface <имя интерфейса>
server <IP-адрес внешнего DHCP-сервера>
```

Внимание!

- Внешний DHCP-сервер должен быть доступен по протоколу ICMP. Если он недоступен, и при этом не задан резервный DHCP-сервер (см. шаг 3), клиенты могут не получать ответы на DHCP-запросы.
- В случае, если по событию DGD произойдет переключение внешних сетевых интерфейсов, то служба DHCP-relay, использующая один из этих интерфейсов в качестве внешнего, будет недоступна.

3 Укажите сетевой интерфейс ViPNet Coordinator HW, который должен использоваться для доступа к резервному DHCP-серверу, если он есть в сети:

```
hostname# inet dhcp relay [<номер копии>] add backup-interface <имя интерфейса> server
<IP-адрес сервера>
```

Примечание. Если внешний DHCP-сервер не отвечает на ICMP-запросы, служба DHCP-relay переключится на использование резервного сервера. При восстановлении подключения будет использоваться основной сервер.

4 Включите автоматический запуск DHCP-relay при загрузке ViPNet Coordinator HW:

```
hostname# inet dhcp relay mode on
```

По умолчанию автоматический запуск DHCP-relay выключен.

5 Запустите DHCP-relay:

```
hostname# inet dhcp relay [<номер копии>] start
```

6 Посмотрите настройки DHCP-relay и его текущее состояние:

```
hostname# inet show dhcp relay [<номер копии>]
```

Примечание. Чтобы впоследствии завершить работу DHCP-relay и одновременно сбросить все его настройки, а также выключить автоматический запуск при загрузке ViPNet Coordinator HW:

```
hostname# inet dhcp relay reset
```

Сценарии настройки DHCP-сервера и DHCP-relay

Настройка локального DHCP-сервера

Вы можете настроить DHCP-сервер ViPNet Coordinator HW для назначения сетевых параметров узлам локальной сети:

1 Остановите DHCP-сервер, если он был запущен:

```
hostname# inet dhcp server stop
```

2 Подключите один из интерфейсов ViPNet Coordinator HW к коммутационному оборудованию локальной сети.

3 Задайте на нем статический IP-адрес, принадлежащий адресному пространству локальной сети:

```
hostname# inet ifconfig <имя интерфейса> address <IP-адрес> netmask <маска>
```

4 Включите интерфейс:

```
hostname# inet ifconfig <имя интерфейса> up
```

5 Задайте этот интерфейс для работы DHCP-сервера:

```
hostname# inet dhcp server add interface <имя интерфейса>
```

6 Задайте диапазон IP-адресов, выделяемых клиентам:

```
hostname# inet dhcp server add range <начальный IP-адрес> <конечный IP-адрес> interface <имя интерфейса>
```

Диапазон IP-адресов должен принадлежать сети интерфейса. При этом IP-адрес интерфейса не должен входить в этот диапазон.

7 Задайте срок (время аренды в секундах), на который клиентам предоставляются IP-адреса:

```
hostname# inet dhcp server add default-lease-time <время аренды>
```

8 Задайте IP-адрес шлюза по умолчанию, если его необходимо передавать клиентам:

```
hostname# inet dhcp server add router <IP-адрес> interface <имя интерфейса>
```

9 Задайте IP-адрес DNS-и NTP-сервера, если их необходимо передавать клиентам:

```
hostname# inet dhcp server add dns <IP-адрес> interface <имя интерфейса>
hostname# inet dhcp server add ntp <IP-адрес> interface <имя интерфейса>
```



Примечание. Вы можете задать другие параметры, передаваемые DHCP-сервером своим клиентам. Подробнее см. в документе «Справочник команд и конфигурационных файлов».

10 Проверьте текущие параметры DHCP-сервера:

```
hostname# inet show dhcp server
```

11 Включите автоматический запуск DHCP-сервера:

```
hostname# inet dhcp server mode on
```

12 Запустите DHCP-сервер:

```
hostname# inet dhcp server start
```

Внимание! Вместе с IP-адресом DHCP-сервер предоставляет клиентам свой IP-адрес в качестве адресов DNS- и NTP-сервера. Поэтому клиенты будут отправлять запросы на разрешение имен и синхронизацию времени через соответствующие службы, запущенные на ViPNet Coordinator HW. Если эти службы не запущены, то клиенты не смогут работать с доменными именами и синхронизировать свое время.

Настройка внешнего DHCP-сервера и DHCP-relay

С помощью DHCP-relay вы можете настроить получение сетевых параметров для узлов локальной сети (сеть 2) от внешнего DHCP-сервера, подключенного к HW-1 (сеть 1).

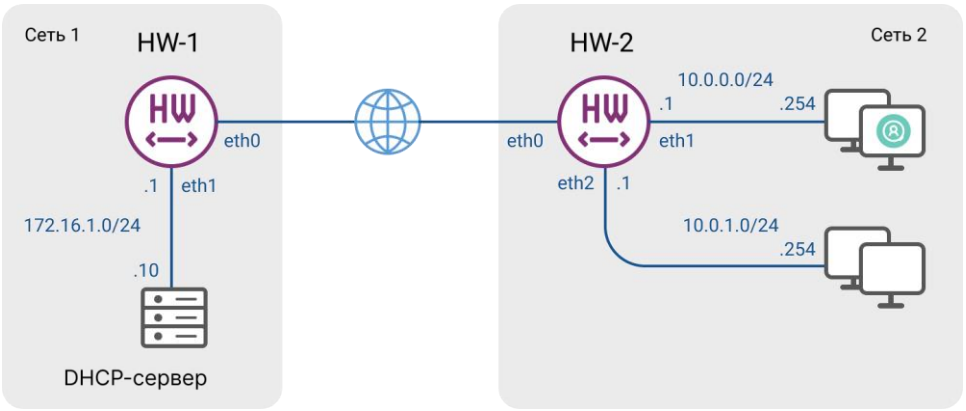


Рисунок 34. Использование DHCP-relay и внешнего DHCP-сервера

1 На HW-1, туннелирующем DHCP-сервер, и HW-2, DHCP-relay которого принимает запросы от клиентов, настройте видимость по реальным IP-адресам (см. Настройка видимости узлов).

2 На HW-2 настройте DHCP-relay:

2.1 Задайте на интерфейсах `eth1` и `eth2` статические IP-адреса из подсетей 10.0.0.0/24 и 10.0.1.0/24:

```
hostname# inet ifconfig eth1 address 10.0.0.1 netmask 255.255.255.0
hostname# inet ifconfig eth2 address 10.0.1.1 netmask 255.255.255.0
```

2.2 Задайте `eth1` и `eth2` в качестве интерфейсов, принимающих DHCP-запросы:

```
hostname# inet dhcp relay add listen-interface eth1
hostname# inet dhcp relay add listen-interface eth2
```

2.3 Задайте IP-адрес внешнего DHCP-сервера:

```
hostname# inet dhcp relay add external-interface eth0 server 172.16.1.10
```

2.4 Проверьте текущие параметры DHCP-relay:

```
hostname# inet show dhcp relay
```

2.5 Включите автоматический запуск DHCP-relay:

```
hostname# inet dhcp relay mode on
```

2.6 Запустите DHCP-relay:

```
hostname# inet dhcp relay start
```

Использование DHCP-сервера и DHCP-relay в разных сетях

В этом примере рассматриваются три сети ViPNet, в которых где HW-1 работает как DHCP-сервер, а HW-2 и 3 работают как агенты DHCP-relay.

DHCP-сервер (HW-1) работает для следующих DHCP-клиентов:

- клиенты сети 1 (диапазон 192.168.2.10-20);
- TFTP-сервер (192.168.3.20), передающий данные для тонкого клиента в сети 3;
- узлы защищённой сети 2 (диапазон 172.16.0.10-20);
- туннелируемые узлы 2 (диапазон 172.16.1.10-20);
- тонкий клиент в сети 3, получающий данные от TFTP-сервера в сети 1.

Для HW-1 настроена видимость по реальным IP-адресам с координаторами, работающими в качестве агентов DHCP-relay.

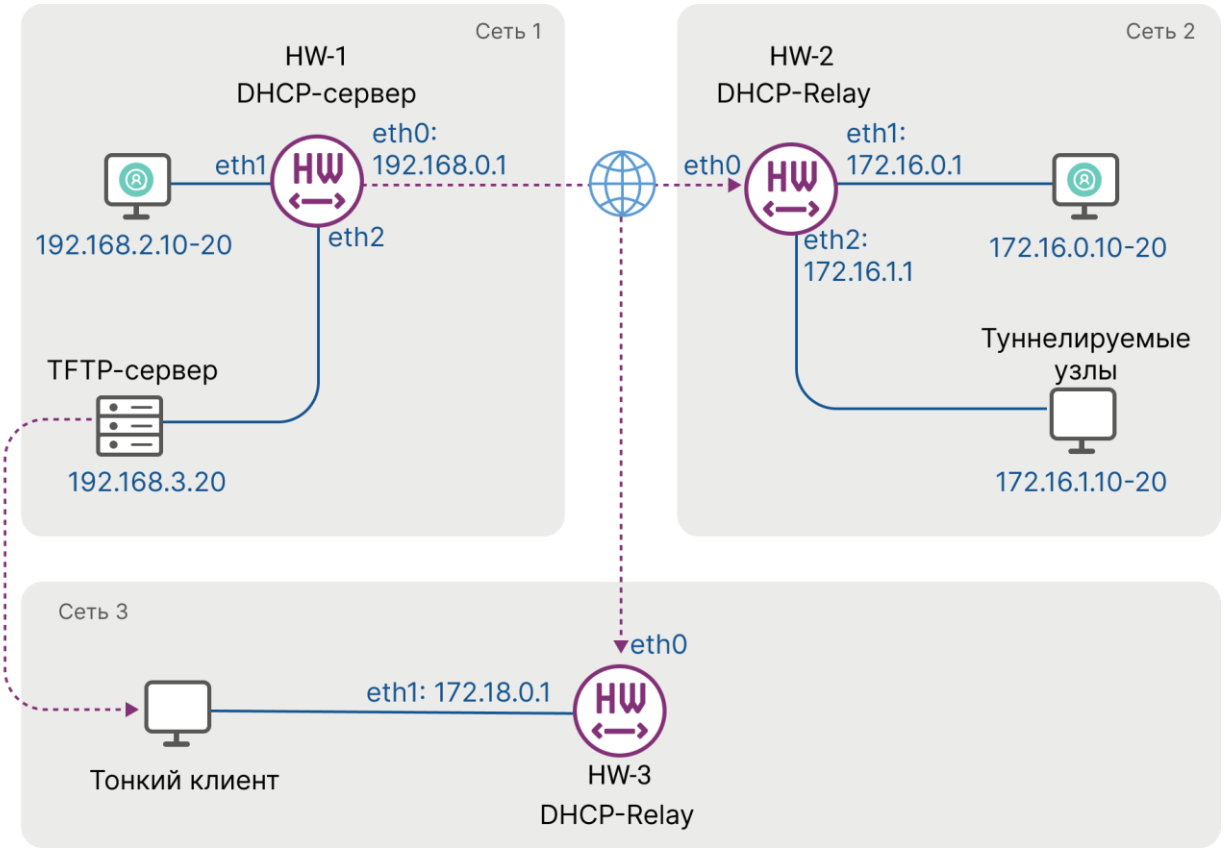


Рисунок 35. Использование DHCP-сервера и DHCP-relay в разных сетях

На HW-1 настройте DHCP-сервер:

1. Задайте рабочие сетевые интерфейсы DHCP-сервера:
   - для сетей 2 и 3:

     ```
     hostname# inet dhcp server add interface eth0
     ```

   - для сети 1:

     ```
     hostname# inet dhcp server add interface eth1
     ```

   - для TFTP-сервера:

     ```
     hostname# inet dhcp server add interface eth2
     ```

2. Добавьте подсеть узлов защищённой сети 2 в качестве удаленной подсети для DHCP-сервера:

   ```
   hostname# inet dhcp server add relay-interface eth0 remote subnet 172.16.0.0 mask 255.255.255.0
   ```

3. Добавьте подсеть туннелируемых узлов сети 2 в качестве удаленной подсети для DHCP-сервера:

   ```
   hostname# inet dhcp server add relay-interface eth0 remote subnet 172.16.1.0 mask 255.255.255.0
   ```

4. Задайте диапазоны IP-адресов, выделяемых DHCP-сервером:

- для сети 1:

  ```
  hostname# inet dhcp server add range 192.168.2.10 192.168.2.20 interface eth1
  ```

- для узлов защищённой сети 2:

  ```
  hostname# inet dhcp server add range 172.16.0.10 172.16.0.20 remote subnet
  172.16.0.0 mask 255.255.255.0
  ```

- для туннелируемых узлов сети 2:

  ```
  hostname# inet dhcp server add range 172.16.1.10 172.16.1.20 remote subnet
  172.16.1.0 mask 255.255.255.0
  ```

5 Задайте IP-адрес шлюза по умолчанию:

- для сети 2:

  ```
  hostname# inet dhcp server add router 172.16.0.1 remote subnet 172.16.0.0 mask
  255.255.255.0
  ```

- для туннелируемых узлов сети 2:

  ```
  hostname# inet dhcp server add router 172.16.1.1 remote subnet 172.16.1.0 mask
  255.255.255.0
  ```

6 Добавьте узлы сети 3 в качестве удаленной подсети для DHCP-сервера:

```
hostname# inet dhcp server add relay-interface eth0 remote subnet 172.18.0.0 mask
255.255.255.0
```

7 Задайте IP-адрес шлюза по умолчанию для сети 3:

```
hostname# inet dhcp server add router 172.18.0.1 remote subnet 172.18.0.0 mask
255.255.255.0
```

8 Зарезервируйте IP-адрес 192.168.3.20 для TFTP-сервера:

```
hostname# inet dhcp server add host TFTP hardware <MAC-адрес TFTP-сервера> address
192.168.3.20 interface eth2
```

9 Задайте для тонкого клиента IP-адрес TFTP-сервера и путь к файлу с параметрами загрузки:

```
hostname# inet dhcp server add tftp 192.168.3.20 file <путь к файлу на TFTP-сервере>
remote subnet 172.18.0.0 mask 255.255.255.0
```

10 Запустите DHCP-сервер:

```
hostname# inet dhcp server start
```

11 Включите автоматический запуск DHCP-сервера:

```
hostname# inet dhcp server mode on
```

На HW-2 настройте DHCP-relay:

1 Задайте `eth0` как внешний интерфейс DHCP-relay:

```
hostname# inet dhcp relay add external-interface eth0 server 192.168.0.1
```

2 Задайте `eth1` как слушающий интерфейс для узлов защищённой сети:

```
hostname# inet dhcp relay add listen-interface eth1
```

3 Задайте `eth2` как слушающий интерфейс для туннелируемых узлов:

```
hostname# inet dhcp relay add listen-interface eth2
```

4 Запустите DHCP-relay:

```
hostname# inet dhcp relay start
```

5 Включите автоматический запуск DHCP-relay:

```
hostname# inet dhcp relay mode on
```

На HW-3 настройте DHCP-relay:

1 Задайте `eth0` для связи с внешним DHCP-сервером:

```
hostname# inet dhcp relay add external-interface eth0 server 192.168.0.1
```

2 Задайте `eth1` как принимающий запросы от клиентов к DHCP-серверу:

```
hostname# inet dhcp relay add listen-interface eth1
```

3 Запустите DHCP-relay:

```
hostname# inet dhcp relay start
```

4 Включите автоматический запуск DHCP-relay:

```
hostname# inet dhcp relay mode on
```

Использование сторонних DHCP-серверов

В этом примере рассматриваются две сети ViPNet, в которых HW-1 туннелирует два сторонних DHCP-сервера, а HW-2 работает как агент DHCP-relay для клиентов своей сети.

Туннелируемые DHCP-серверы, подключенные к HW-1, работают для следующих DHCP-клиентов сети 2:

- DHCP-сервер 1 — для узлов защищённой сети (диапазон 192.168.0.100-200).
- DHCP-сервер 2 — для туннелируемых VoIP-телефонов (диапазон 172.16.0.10-20). DHCP-сервер 2 также выступает в роли VoIP-сервера для VoIP-телефонов в сети 1.

На HW-2 запущены две копии DHCP-relay, принимающие запросы от узлов защищённой сети и туннелируемых узлов. Между координаторами настроена видимость по реальным IP-адресам.

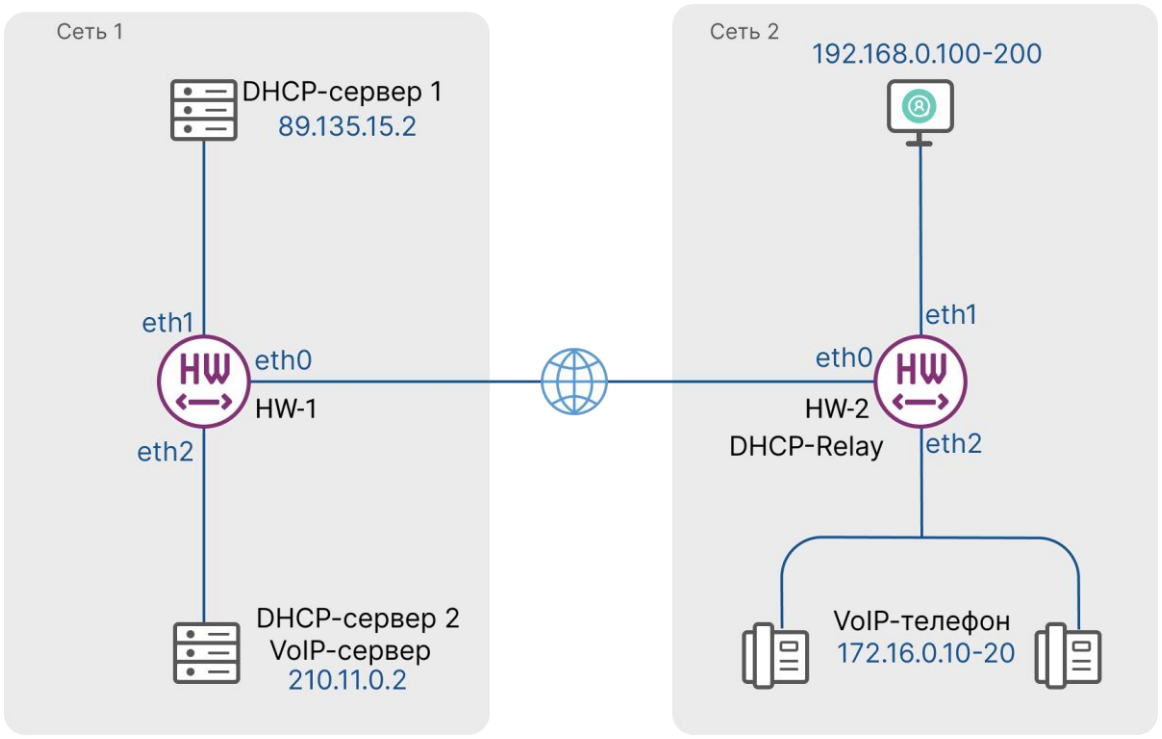


Рисунок 36. Использование сторонних DHCP-серверов

На HW-2:

1 Настройте DHCP-relay для узлов защищённой сети:

1.1 Задайте `eth0` как внешний интерфейс DHCP-relay для узлов защищённой сети:

```
hostname# inet dhcp relay 1 add external-interface eth0 server 89.135.15.2
```

1.2 Задайте `eth1` как слушающий интерфейс для узлов защищённой сети:

```
hostname# inet dhcp relay 1 add listen-interface eth1
```

2 Настройте DHCP-relay для туннелируемых узлов:

2.1 Задайте `eth0` как внешний интерфейс DHCP-relay для туннелируемых узлов:

```
hostname# inet dhcp relay 2 add external-interface eth0 server 210.11.0.2
```

2.2 Задайте `eth2` как слушающий интерфейс для туннелируемых узлов:

```
hostname# inet dhcp relay 2 add listen-interface eth2
```

3 Запустите DHCP-relay (обе копии):

```
hostname# inet dhcp relay 1 start
hostname# inet dhcp relay 2 start
```

4 Включите автоматический запуск DHCP-relay:

```
hostname# inet dhcp relay mode on
```

Одновременное использование DHCP-сервера и DHCP-relay

В этом примере рассматриваются две сети ViPNet, где HW-1 туннелирует сторонний DHCP-сервер, а HW-2 работает одновременно как агент DHCP-relay для своих туннелируемых узлов и как DHCP-сервер для узлов защищённой сети.

Между HW-2 и туннелируемым DHCP-сервером настроена видимость по реальным IP-адресам.

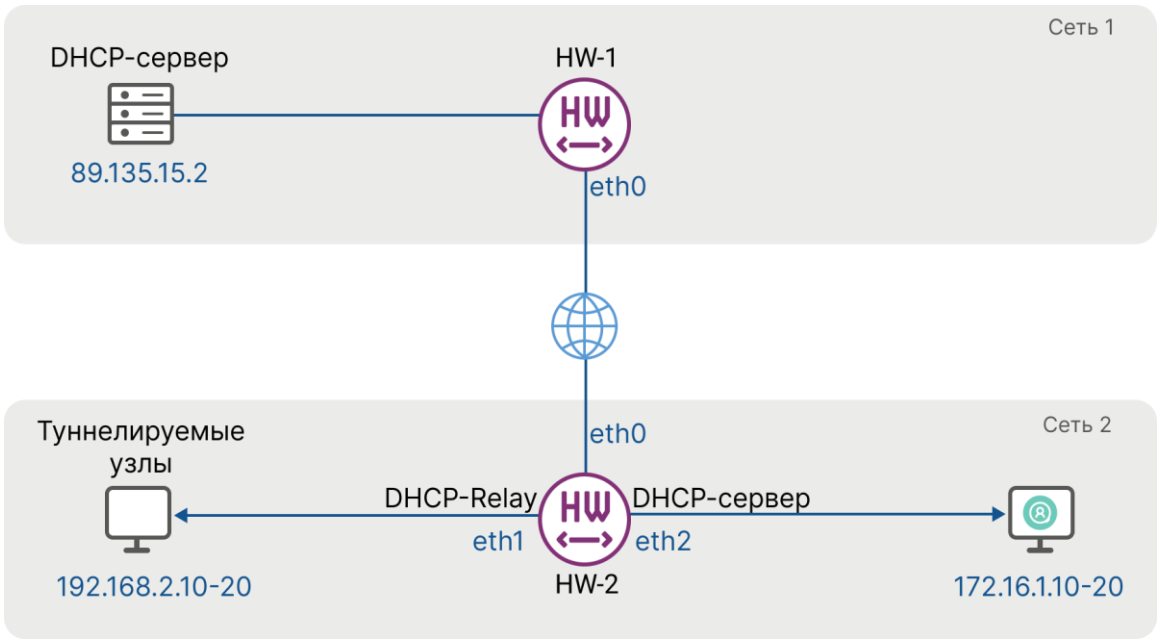


Рисунок 37. Одновременное использование DHCP-сервера и DHCP-relay

На HW-2:

1 Настройте DHCP-relay, принимающий данные от DHCP-сервера, стоящего за HW-1:

1.1 Задайте `eth0` как внешний интерфейс DHCP-relay:

```
hostname# inet dhcp relay add external-interface eth0 server 89.135.15.2
```

1.2 Задайте `eth1` как слушающий интерфейс для туннелируемых узлов:

```
hostname# inet dhcp relay add listen-interface eth1
```

1.3 Запустите DHCP-relay:

```
hostname# inet dhcp relay start
```

1.4 Включите автоматический запуск DHCP-relay:

```
hostname# inet dhcp relay mode on
```

2 Настройте DHCP-сервер:

2.1 Задайте рабочий сетевой интерфейс DHCP-сервера:

```
hostname# inet dhcp server add interface eth2
```

2.2 Задайте диапазон IP-адресов, выделяемых DHCP-сервером для узлов защищённой сети:

```
hostname# inet dhcp server add range 172.16.0.10 172.16.0.20 interface eth2
```

2.3 Запустите DHCP-сервер:

```
hostname# inet dhcp server start
```

2.4 Включите автоматический запуск DHCP-сервера:

```
hostname# inet dhcp server mode on
```

Использование запасного DHCP-сервера

В этом примере рассматриваются две сети ViPNet, где HW-2 туннелирует два сторонних DHCP-сервера, один из которых является запасным, а HW-1 работает как агент DHCP-relay для клиентов своей сети:

- Между координаторами настроена видимость по реальным IP-адресам.
- В сети 2 туннелируемые DHCP-серверы, подключенные к HW-2, работают для узлов защищённой сети 1 (диапазон 192.168.0.100-200).
- На HW-1 для DHCP-relay настроен слушающий интерфейс, принимающий запросы от узлов защищённой сети, а также внешний интерфейс, настроенный на соединение как с основным, так и с запасным DHCP-серверами.

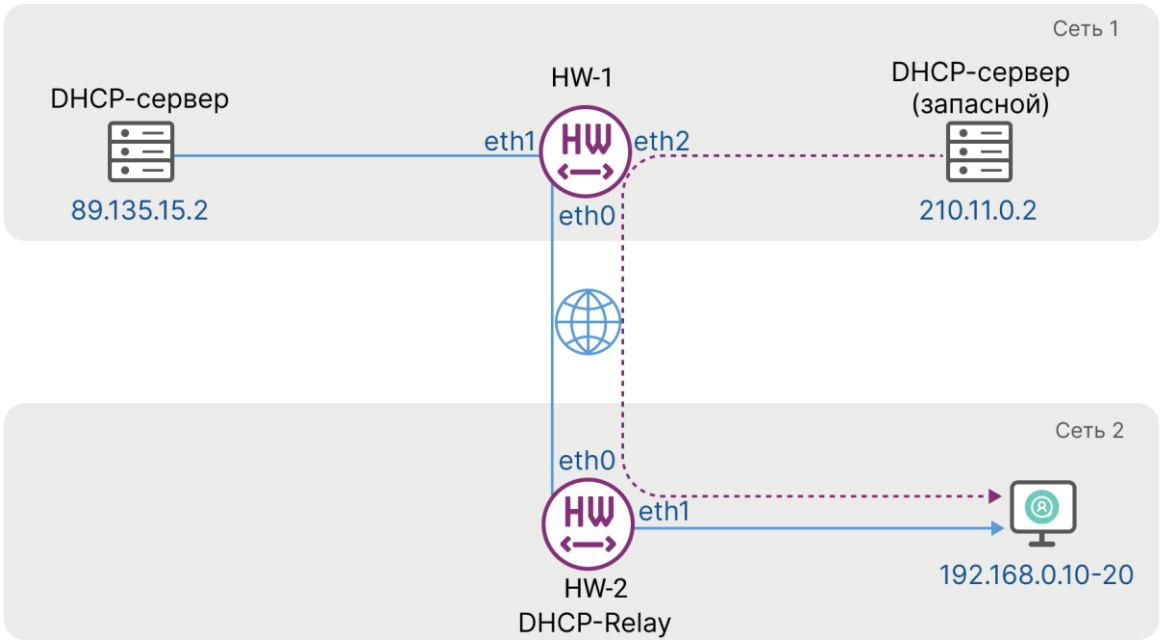


Рисунок 38. Использование DHCP-relay для запасного DHCP-сервера

На HW-1:

1 Задайте `eth0` как внешний интерфейс DHCP-relay:

```
hostname# inet dhcp relay add external-interface eth0 server 89.135.15.2
```

2 Задайте `eth0` как интерфейс DHCP-relay, подключенный к запасному DHCP-серверу:

```
hostname# inet dhcp relay add backup-interface eth0 server 210.11.0.2
```

3 Задайте `eth1` как слушающий интерфейс для узлов защищённой сети:

```
hostname# inet dhcp relay add listen-interface eth1
```

4 Запустите DHCP-relay:

```
hostname# inet dhcp relay start
```

5 Включите автоматический запуск DHCP-relay:

```
hostname# inet dhcp relay mode on
```

Настройка DNS-сервера

DNS-сервер преобразует доменные имена в IP-адреса в ответ на запросы сетевых узлов (DNS-клиентов).

Локальный DNS-сервер перенаправляет поступающие к нему DNS-запросы на вышестоящие DNS-серверы и передает полученные ответы DNS-клиентам. По умолчанию локальный DNS-сервер преобразует доменные имена с использованием корневых DNS-серверов из домена `root-servers.net`. Этот список можно дополнить DNS-серверами пересылки (forwarders).



Внимание! В качестве DNS-серверов пересылки используйте доверенные DNS-серверы из сети ViPNet. Ответы на запросы DNS-клиентов, приходящие не от доверенных DNS-серверов, могут быть скомпрометированы.

Список дополнительных DNS-серверов:

- Можно получить от внешнего DHCP-сервера.

  На сетевом интерфейсе должен быть установлен режим автоматического получения параметров от DHCP-сервера, а DHCP-сервер должен отправлять информацию о DNS-серверах.

  Если режим DHCP установлен на нескольких интерфейсах ViPNet Coordinator HW, то результат обработки собственных DNS-запросов и запросов DNS-клиентов не определён, так как неизвестно, какой интерфейс будет включён первым и какой список DNS-серверов пересылки получит ViPNet Coordinator HW.

  Настраивайте получение информации о DNS-серверах только на одном интерфейсе. Данные об адресах DNS-серверов поступают автоматически, откажитесь от их получения:

  ```
  hostname# inet ifconfig <интерфейс> dhcp dns off
  ```

- Задать вручную.



Внимание! Если DNS-серверы пересылки недоступны, но при этом доступны корневые DNS-серверы, DNS-клиенты будут получать ответы на свои запросы с задержкой.

Команды для работы с локальным DNS-сервером

- Указать IP-адреса узлов и подсетей, узлам которых разрешены запросы к DNS-серверу:

  ```
  hostname# inet dns clients add {<IP-адрес> | <IP-адрес/длина маски>}
  ```

  По умолчанию DNS-запросы к серверу разрешены для любых узлов.

- Посмотреть список IP-адресов, которым разрешены DNS-запросы к серверу:

  ```
  hostname# inet dns clients list
  ```

- Удалить IP-адреса из списка адресов, которым разрешены DNS-запросы к серверу:

  ```
  hostname# inet dns clients delete {<IP-адрес> | <IP-адрес/длина маски>}
  ```

- Добавить IP-адрес DNS-сервера, на который ViPNet Coordinator HW будет перенаправлять DNS-запросы:

  ```
  hostname# inet dns forwarders add <IP-адрес>
  ```

  Если необходимо перенаправлять DNS-запросы для определенных зон, то добавьте для каждой такой зоны IP-адрес DNS-сервера пересылки с указанием параметра `<for-zone>`:

  ```
  hostname# inet dns forwarders add <IP-адрес> [for-zone <имя зоны>]
  ```

  Если необходимо перенаправлять DNS-запросы для определенных зон исключительно на указанный DNS-сервер пересылки, без резервного обращения к корневым DNS-серверам, добавьте ключевое слово `only`:

  ```
  hostname# inet dns forwarders add <IP-адрес> [for-zone <имя зоны> [only]]
  ```

- Посмотреть список DNS-серверов пересылки:

  ```
  hostname# inet dns forwarders list
  ```

- Удалить DNS-сервер из списка:

  ```
  hostname# inet dns forwarders delete <IP-адрес>
  ```

  Для удаления из списка DNS-сервера пересылки, заданного для определенной зоны, укажите параметр `<for-zone>`:

  ```
  hostname# inet dns forwarders delete <IP-адрес> [for-zone <имя зоны>]
  ```



Примечание. При добавлении двух и более DNS-серверов пересылки, серверы, добавленные без указания имени зоны, имеют приоритет и будут использоваться для перенаправления всех DNS-запросов вне зависимости от наличия серверов пересылки для отдельных зон. При этом появится сообщение:

```
Forward DNS address <адрес> resolves both named zone and all requests
```

При изменении конфигурации внешних DNS-серверов перезапустите локальный DNS-сервер:

```
hostname# inet dns stop
hostname# inet dns start
```

- Включить или выключить автоматический запуск DNS-сервера при загрузке ViPNet Coordinator HW:

  ```
  hostname# inet dns mode {on | off}
  ```

  Текущее состояние задано при установке справочников и ключей.

- Запустить или остановить DNS-сервер:

  ```
  hostname# inet dns {start | stop}
  ```

- Посмотреть текущие параметры DNS-сервера:

  ```
  hostname# inet show dns
  ```

Настройка NTP-сервера

В состав ViPNet Coordinator HW входит локальный NTP-сервер. Он используется для синхронизации времени на ViPNet Coordinator HW и на других сетевых узлах (NTP-клиентах).

По умолчанию локальный NTP-сервер синхронизирует время с публичными NTP-серверами:

- `ntp1.vniiftri.ru`;
- `ntp2.vniiftri.ru`;
- `ntp.ix.ru`.

Вы можете добавить синхронизацию времени с другими NTP-серверами (публичными или корпоративными).



Примечание. Не устанавливайте одновременно синхронизацию времени на платформе виртуализации и виртуальной машине ViPNet Coordinator HW. Если это необходимо, то для синхронизации используйте один и тот же NTP-сервер.

Дополнительные NTP-серверы:

- Можно получить от внешнего DHCP-сервера.

  На сетевом интерфейсе должен быть установлен режим автоматического получения параметров от DHCP-сервера и DHCP-сервер должен отправлять информацию о NTP-серверах.

  Если режим DHCP установлен на нескольких сетевых интерфейсах ViPNet Coordinator HW, то результат синхронизации времени на ViPNet Coordinator HW и на NTP-клиентах не определен, так как неизвестно, какой сетевой интерфейс будет включен первым и какой список дополнительных NTP-серверов получит ViPNet Coordinator HW.

  Настраивайте получение адресов NTP-серверов только на одном интерфейсе и откажитесь от их получение от других интерфейсов, на которых включен режим DHCP:

  ```
  hostname# inet ifconfig <интерфейс> dhcp ntp off
  ```

- Добавить вручную.

Дополнительный NTP-сервер может находиться как в защищенной, так и в открытой сети:

- Если дополнительный NTP-сервер — узел защищенной сети, видимый по реальному адресу, то в файле `iplir.conf` в секции `[id]` для этого узла установите параметр `visibility` в значение `real`. Описание секции и параметра см. в документе «Справочник команд и конфигурационных файлов», в разделе «Файл iplir.conf».
- Если дополнительный NTP-сервер — узел открытой сети, добавьте разрешающий фильтр открытой сети для входящего трафика от NTP-сервера:

  ```
  hostname# firewall local add src @any dst @local udp dport 123 pass
  ```

Команды для работы с локальным NTP-сервером

- Добавить адрес дополнительного NTP-сервера:

  `hostname# inet ntp add {server | peer} {<IP-адрес> | <доменное имя>}`, где

  - `server` — если NTP-сервер только рассылает данные о времени.
  - `peer` — если NTP-сервер рассылает и получает данные о времени.

- Удалить адрес дополнительного NTP-сервера:

  `hostname# inet ntp delete {server | peer} {<IP-адрес> | <доменное имя>}`

- Посмотреть список NTP-серверов:

  `hostname# inet ntp list`

- Включить автоматический запуск локального NTP-сервера при загрузке ViPNet Coordinator HW:

  `hostname# inet ntp mode on`

- Разрешить переход в изолированный (orphan) режим при потере соединения с внешними NTP-серверами:

  `hostname# inet ntp orphan on <stratum>`, где

  `<stratum>` — уровень внешнего NTP-сервера (от 1 до 10). Если со всеми внешними NTP-серверами меньше указанного уровня не удается установить соединение в течение 5 минут, то локальный NTP-сервер переходит в изолированный режим. По умолчанию значение `<stratum>` равно 5. Значение `stratum` задается в настройках NTP-сервера.

  Внимание! Разрешите переход локального NTP-сервера в изолированный режим, если ViPNet Coordinator HW используется в качестве NTP-сервера для внутренней сети. Иначе клиенты ViPNet Coordinator HW не будут получать информацию о точном времени при потере соединения ViPNet Coordinator HW с внешними NTP-серверами, так как в этом случае локальный NTP-сервер будет считаться недостоверным.

- Запустить или остановить NTP-сервер:

  `hostname# inet ntp {start | stop}`

  Внимание! NTP-серверы, указанные по доменному имени, будут доступны, только если запущен DNS-сервер.

  События о попытках подключения к NTP-серверам регистрируются в системном журнале.

- Посмотреть текущие параметры и состояние локального NTP-сервера:

  `hostname# inet show ntp`

  Внимание! Изменение времени на вышестоящем NTP-сервере более чем на 1000 секунд вперед или назад может привести к аварийному завершению работы локального NTP-сервера. В этом случае запустите локальный NTP-сервер:

  `hostname# inet ntp start`

Организация работы клиентов удаленного офиса с корпоративными DNS- и NTP-серверами

Рассмотрим пример, когда у организации есть несколько офисов, при этом в центральном офисе установлены корпоративные DNS- и NTP-серверы. Требуется, чтобы к этим серверам могли обращаться клиенты, находящиеся в удаленном офисе:

1. В сетевых настройках клиентов задайте IP-адрес ViPNet Coordinator HW в качестве DNS- и NTP-серверов. Клиенты удаленного офиса будут направлять запросы на разрешение доменных имен и на синхронизацию времени на ViPNet Coordinator HW.
2. На ViPNet Coordinator HW настройте обращение к корпоративному DNS-серверу:
   2.1 Проверьте текущий список DNS-серверов пересылки:
   ```
   hostname# inet dns forwarders list
   ```
   По умолчанию DNS-запросы перенаправляются на корневые DNS-серверы из домена `root-servers.net`.
   2.2 Добавьте IP-адрес корпоративного DNS-сервера:
   ```
   hostname# inet dns forwarders add <IP-адрес>
   ```
   2.3 Проверьте текущие параметры DNS-сервера:
   ```
   hostname# inet show dns
   ```
   2.4 Запустите DNS-сервер:
   ```
   hostname# inet dns start
   ```
   2.5 Включите автоматический запуск DNS-сервера при загрузке ViPNet Coordinator HW:
   ```
   hostname# inet dns mode on
   ```
3. На ViPNet Coordinator HW настройте обращение к корпоративному NTP-серверу:
   3.1 Проверьте текущий список NTP-серверов:
   ```
   hostname# inet ntp list
   ```
   3.2 Добавьте IP-адрес корпоративного NTP-сервера:
   ```
   hostname# inet ntp add server {<IP-адрес> | <доменное имя>}
   ```
   3.3 Проверьте текущие параметры NTP-сервера:
   ```
   hostname# inet show ntp
   ```
   3.4 Запустите NTP-сервер:

```
hostname# inet ntp start
```

3.5 Включите автоматический запуск NTP-сервера при загрузке ViPNet Coordinator HW:

```
hostname# inet ntp mode on
```

Настройка взаимодействия с Active Directory

Если в вашей сети используется служба каталогов Active Directory, то вы можете настроить ее взаимодействие с ViPNet Coordinator HW, чтобы использовать имена пользователей сети в фильтрах туннелируемых узлов и транзитных фильтрах открытой сети. Для этого:

1. На контроллерах доменов настройте учетную запись технологического пользователя (см. Настройка учетной записи технологического пользователя).
2. На ViPNet Coordinator HW настройте его подключение к контроллерам доменов (см. Подключение к контроллерам доменов).



Внимание!

Необходимо обеспечить доверенный канал передачи данных между ViPNet Coordinator HW и внешними системами (в том числе взаимодействующими системами защиты информации других типов), например выделенный физический канал или сеть ViPNet. Допускается осуществлять защиту каналов передачи данных организационными мерами, исключающими возможность утечки или перехвата защищаемых данных, или с помощью сертифицированных средств криптографической защиты информации.

При настройке учитывайте:

- ViPNet Coordinator HW поддерживает контроллеры домена:
  - Windows Server 2012 R2 (английская и русская версии).
  - Windows Server 2016 (английская и русская версии).
- Максимальное количество контроллеров доменов, подключаемых к ViPNet Coordinator HW — 10.
- ViPNet Coordinator HW периодически опрашивает контроллеры доменов для проверки их доступности и обновления списка активных пользователей. При недоступности контроллера домена ViPNet Coordinator HW будет предпринимать попытки соединиться с ним в течение 5 минут. Наличие нескольких недоступных контроллеров доменов может привести к существенным временным задержкам при обновлении списка активных пользователей.
- Для каждого контроллера домена установлено допустимое время отсутствия связи с ним (по умолчанию — 1800 секунд). Если по истечении этого времени связь с контроллером домена не восстановлена:
  - пользователи, связанные только с ним, удаляются из списка активных;
  - открытые пользовательские сессии остаются активными;
  - обработка трафика транзитными фильтрами открытой сети и фильтрами туннелируемых узлов по пользователям, удаленным из списка активных, не проводится.

- Если сетевые узлы, с которых подключаются пользователи, и контроллер домена туннелируются разными ViPNet Coordinator HW, настройте между узлами и контроллером видимость по реальным IP-адресам.

Настройка учетной записи технологического пользователя

Соответствие пользователей сети и IP-адресов устройств, с которых было выполнено подключение, определяется по журналу контроллера домена. Чтобы служба `uc` ViPNet Coordinator HW могла получать данные журнала, создайте учетную запись технологического пользователя для подключения ViPNet Coordinator HW к контроллеру домена и настройте ее полномочия:

1 С помощью оснастки консоли управления **Active Directory Users and Computers**:

1.1 Создайте учетную запись технологического пользователя с произвольным именем, например Иван Петров (`ivan.petrov@test.vn.com`).

1.2 Включите учетную запись технологического пользователя в группы:

- **Читатели журнала событий (Event Log Readers)**.
- **Пользователи DCOM (Distributed COM Users)**.
- **Операторы сервера (Server operator)**.
- **Пользователи домена (Domain Users)**.



Примечание. Учетная запись технологического пользователя может не обладать правами **Администратор домена**.

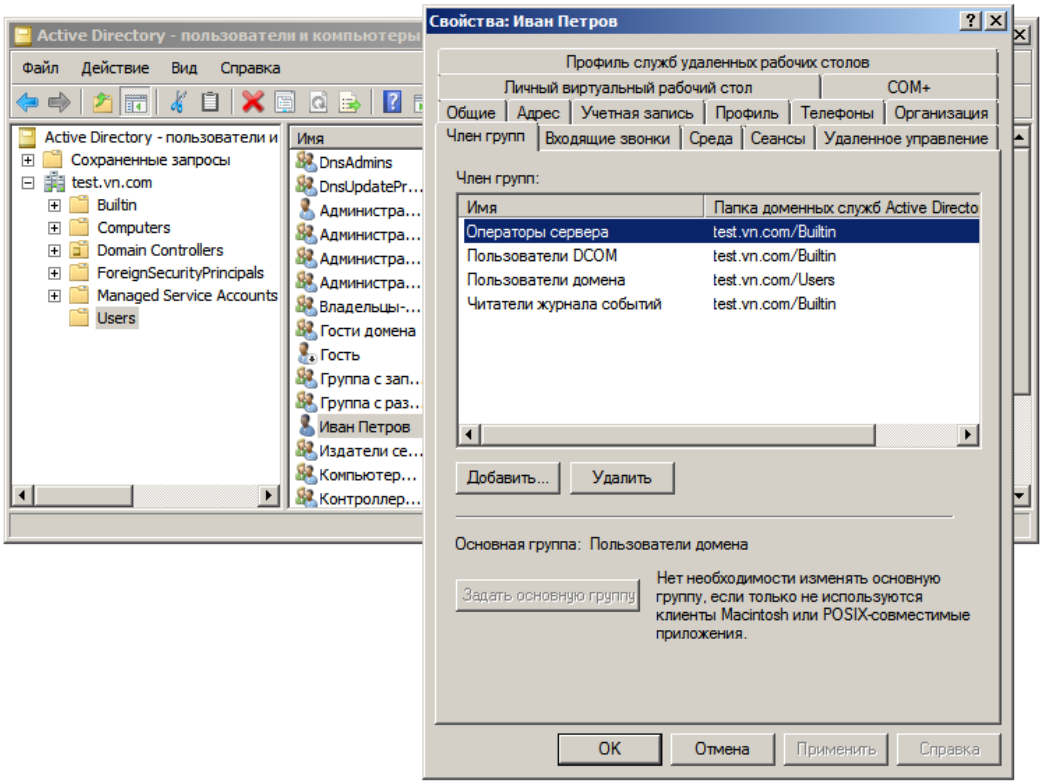


Рисунок 39. Создание учетной записи технологического пользователя Иван Петров

2 С помощью оснастки консоли управления **Windows Management Infrastructure**:

2.1 Добавьте учетную запись технологического пользователя Иван Петров (`ivan.petrov@test.vn.com`) в разделы инфраструктуры WMI:

- **Root/CIMV2**.
- **Root/directory/LDAP**.

2.2 В каждом из перечисленных разделов выберите:

- **Enable Account (Включить учетную запись)**.
- **Remote Enable (Включить удалённо)**.

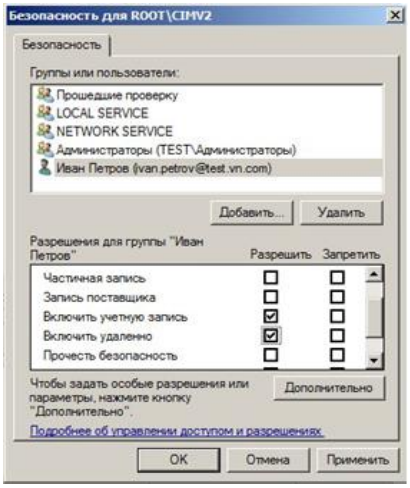


Рисунок 40. Добавление учетной записи технологического пользователя Иван Петров (ivan.petrov@test.vn.com) в инфраструктуру WMI и задание полномочий

Подключение к контроллерам доменов

1 Остановите службу идентификации пользователей сети `uc`:

```
hostname# service user-control stop
```

2 Настройте подключение к контроллеру домена:

`hostname# service user-control ad set controller <адрес> user <имя>`, указав:

- `<адрес>` — IP-адрес или доменное имя контроллера домена;
- `<имя>` — имя учетной записи технологического пользователя (см. Настройка учетной записи технологического пользователя);

> **Примечание.** Если технологический пользователь контроллера домена имеет несколько имен входа, то для настройки взаимодействия контроллера домена и ViPNet Coordinator HW используйте имя, указанное в группе **Пред-Windows (Pre-Windows)**.

- пароль технологического пользователя.

3 При необходимости измените допустимое время отсутствия связи с контроллером домена (по умолчанию — 1800 секунд):

```
hostname# service user-control ad set controller <адрес> connection-timeout
<время>
```

4 Повторите шаги 2 и 3, чтобы настроить подключение к ещё одному контроллеру домена. Максимальное количество контроллеров доменов, подключаемых к ViPNet Coordinator HW — 10.

5 Создайте сетевые фильтры, разрешающие трафик к контроллерам доменов:

```
hostname# service user-control fw-rules apply
```



Внимание! Выполняйте команду `service user-control fw-rules apply` после изменения адресов контроллеров доменов, чтобы обновить сетевые фильтры.

6 Запустите службу службу идентификации пользователей сети `uc`:

```
hostname# service user-control start
```



Внимание! Наличие нескольких недоступных контроллеров доменов может привести к существенной задержке запуска службы `uc`.

7 Просмотрите сведения о подключенных контроллерах доменов:

```
hostname# service user-control ad show
```

8 Просмотрите список активных пользователей сети:

```
hostname# service user-control active-users
```

Чтобы удалить подключения <prodict_name> к контроллерам доменов:

- ко всем контроллерам доменов:

  ```
  hostname# service user-control ad reset
  ```

- к выбранному контроллеру домена:

  ```
  hostname# service user-control ad reset controller <адрес>
  ```

Если вы решили отказаться от идентификации пользователей сети с помощью Active Directory и Captive Portal:

1 Остановите службу идентификации пользователей сети `uc`:

```
hostname# service user-control stop
```

2 Удалите разрешающие сетевые фильтры, созданные ранее для работы службы:

```
hostname# service user-control fw-rules delete
```

Настройка взаимодействия с LDAP-сервером

В ряде случаев невозможно реализовать политику безопасного доступа пользователей из внутренней сети компании в Интернет с использованием аутентификации в службе каталогов Active Directory:

- в IT-инфраструктуре компании не используется служба каталогов Active Directory;
- сотрудники компании используют мобильные устройства с iOS и Android, которые нельзя аутентифицировать в Active Directory.

Тогда для аутентификации пользователей, в том числе подключающихся с мобильных устройств, используются Captive portal, встроенный в ViPNet Coordinator HW, и LDAP-сервер:

1. Пользователь подключается к внутренней сети (например, через точку доступа Wi-Fi, подключенную к ViPNet Coordinator HW) и переходит в браузере на внешний веб-ресурс.
2. ViPNet Coordinator HW переадресует запрос пользователя на страницу аутентификации Captive portal.
3. Пользователь вводит имя и пароль, Captive portal отправляет запрос на LDAP-сервер для проверки данных учетной записи пользователя.
4. LDAP-сервер отправляет на Captive portal результат проверки учетных данных пользователя.
5. Если проверка пользователя на LDAP-сервере прошла успешно, то пользователь видит на странице Captive portal ссылку для перехода на запрошенный веб-ресурс.

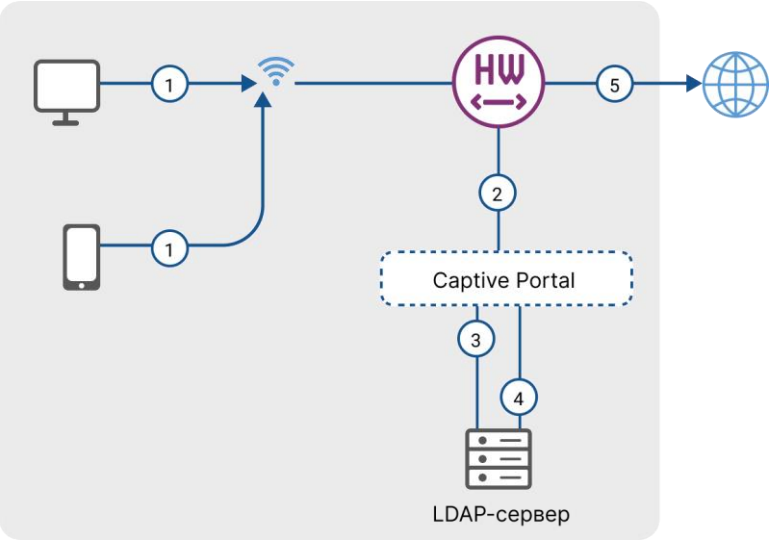


Рисунок 41. Аутентификация пользователей с помощью Captive portal и LDAP-сервера

Примечание. Во внутренней сети компании должен быть установлен LDAP-сервер. Для хранения учетных данных пользователей в LDAP-каталоге должны использоваться следующие атрибуты:

- `uid` — для имени пользователя.
- `userPassword` — для пароля пользователя.

Captive portal определяет пользователей по их уникальным IP-адресам и поэтому не сможет определить пользователей, которые находятся за NAT с трансляцией адреса источника.

Чтобы настроить взаимодействие с LDAP-сервером:

1. Получите и импортируйте в локальное хранилище ViPNet Coordinator HW необходимые сертификаты (см. Получение и импорт сертификатов).
2. Настройте параметры Captive portal (см. Настройка параметров Captive portal).

После этого доступ в Интернет будет определяться правилами межсетевого экрана. Для пользователей, не прошедших аутентификацию, доступ в Интернет будет заблокирован, в том числе запросы к внешним DNS-серверам. Поэтому для нормальной работы пользователей во внутренней сети используйте локальные DNS-серверы (см. Настройка DNS-сервера).

Получение и импорт сертификатов

Импортируйте в локальное хранилище сертификатов ViPNet Coordinator HW:

- Корневой сертификат УЦ, выпустившего сертификат LDAP-сервера. Корневой сертификат необходим для проверки подлинности сертификата LDAP-сервера. Вы можете загрузить его с сайта УЦ, указанного в сертификате LDAP-сервера.
- Сертификат веб-сервера Captive portal. Сертификат обеспечивает защиту данных (имени пользователя и пароля), которые пользователь передает при аутентификации на Captive portal. Для получения сертификата создайте запрос в формате PKCS#12 и передайте его в УЦ; в ответ на запрос вы получите сертификат веб-сервера Captive portal.

Примечание. Вы можете создать запрос на сертификат не только в ViPNet Coordinator HW, но и с помощью других средств. В этом случае начните выполнять действия с шага 5 и импортируйте в локальное хранилище не только сертификат, но и закрытый ключ, которым он подписан.

Для получения и импорта сертификатов в локальное хранилище:

1. Создайте запрос на сертификат веб-сервера Captive portal:

   ```
   hostname# service cert request create name <имя> bits <длина ключа> digest {sha256 | sha384 | sha512},
   ```

   указав следующие параметры:

   - `<имя>` — имя сертификата.

- `<длина ключа>` — размер создаваемого RSA-ключа в битах, можно задавать следующие значения: 2048, 3072, 4096.
- `sha256` — алгоритм хэширования SHA-256;
- `sha384` — алгоритм хэширования SHA-384;
- `sha512` — алгоритм хэширования SHA-512.

2 Экспортируйте файл запроса на USB-носитель:

```
hostname# service cert request export <имя файла запроса на сертификат>
```

3 Перешлите файл запроса в УЦ и получите сертификат веб-сервера Captive portal.

4 Скопируйте сертификат веб-сервера Captive portal и корневой сертификат УЦ, выдавшего сертификат LDAP-сервера, на USB-носитель и импортируйте их в локальное хранилище сертификатов:

```
hostname# service cert import
```



Примечание. Вы можете импортировать сертификаты как в кодировке DER, так и в Base64.

5 Импортируйте на устройства пользователей, проходящих аутентификацию через Captive portal, корневой сертификат УЦ, выдавшего сертификат веб-сервера Captive portal, и список аннулированных сертификатов этого УЦ.

Настройка параметров Captive portal

Настройте параметры взаимодействия Captive portal с LDAP-сервером:

1 Выберите корневой сертификат УЦ, выдавшего сертификат LDAP-сервера, из локального хранилища сертификатов:

```
hostname# service user-control cp set ldap cacert <сертификат>,
```

где `<сертификат>` — имя файла корневого сертификата, установленного в локальное хранилище ViPNet Coordinator HW.



Совет. Чтобы командный интерпретатор автоматически подставил имя корневого сертификата, подходящего для установки (или вывел список сертификатов, если вы импортировали несколько корневых сертификатов), нажмите **Tab**.

2 Задайте параметры соединения Captive portal с LDAP-сервером:

```
hostname# service user-control cp set ldap <адрес LDAP-сервера> identity <имя служебной учетной записи> basedn <база поиска>,
```

указав следующие параметры:

- `<адрес LDAP-сервера>` — IP-адрес или доменное имя LDAP-сервера. Доменное имя может иметь длину до 253 символов и содержать латинские буквы (`A-z`), цифры (`0-9`), знаки «минус» и «точка».
- `<имя служебной учетной записи>` — выделенное имя в (DN, в соответствии с RFC 4514)) служебной учетной записи LDAP-сервера, которая обладает правами на чтение записей LDAP-сервера. Выделенное имя служебной учетной записи может иметь длину до 256 любых символов, кроме `" / \ [ ] : ; | + * ? < >`. Выделенное имя служебной учетной записи должно быть заключено в двойные кавычки (`""`).
- `<база поиска>` — выделенное имя (DN, в соответствии с RFC 4514)) базы поиска, от которой начинаются операции поиска в LDAP-каталоге. Выделенное имя базы поиска может иметь длину до 128 любых символов, кроме `" / \ [ ] : ; | + * ? < >`. Выделенное имя базы должно быть заключено в двойные кавычки (`""`).

3 Введите пароль служебной учетной записи LDAP-сервера.



Внимание! Если вы введете неверный пароль служебной учетной записи LDAP-сервера, то это может стать причиной следующих ситуаций:

- Статус LDAP-сервера будет отображаться неверно.
- Если на LDAP-сервере выключен прием анонимных запросов, то на веб-портале Captive portal не будет работать аутентификация пользователей. При этом в случае, если на LDAP-сервере включен прием анонимных запросов, то на веб-портале Captive portal будет работать аутентификация пользователей независимо от того, верно ли указан пароль к служебной учетной записи LDAP-сервера или нет.

---

4 Выберите сертификат веб-сервера Captive portal из локального хранилища сертификатов:

```
hostname# service user-control cp set hostcert <имя файла сертификата> hostkey <имя файла закрытого ключа>
```



Внимание! Если вы выбрали сертификат веб-сервера Captive portal и хотите отказаться от его использования, то вам необходимо сбросить настройки Captive portal:

```
hostname# service user-control cp reset
```

Сброс настроек Captive portal необходимо выполнить также в том случае, если вы удалили сертификат веб-сервера Captive portal и не хотите использовать вместо него другой сертификат.

---

5 Задайте режим соединения с LDAP-сервером:

```
hostname# service user-control cp set connection-secure <режим соединения>,
```

где `<режим соединения>` может принимать значения:

- `stls` — режим соединения Start TLS, устанавливает соединения на порт LDAP 389;
- `ldaps` — режим соединения на порт LDAP 636;
- `none` — режим открытого соединения. Используется по умолчанию.

6 Проверьте работу Captive portal:

```
hostname# service user-control cp show
```

7 После изменения настроек взаимодействия с LDAP-сервером создайте разрешающие сетевые фильтры:

```
hostname# service user-control fw-rules apply
```

8 Чтобы просмотреть список активных пользователей Captive portal:

```
hostname# service user-control active-users
```

Настройка точки доступа сети Wi-Fi

Примечание. Использование ViPNet Coordinator HW в качестве точки доступа Wi-Fi возможно только в исполнениях со встроенными адаптерами Wi-Fi: ViPNet Coordinator HW50 A, B на аппаратной платформе HW50 N2 и ViPNet Coordinator HW100 C на аппаратной платформе HW100 N2.

Если ViPNet Coordinator HW работает в режиме точки доступа, то он не сможет подключаться к другим сетям Wi-Fi.

Чтобы использовать ViPNet Coordinator HW в качестве точки доступа Wi-Fi:

1. Отключите сетевой интерфейс `wlan0`:

   ```
   hostname# inet wifi mode off
   ```

2. Переключите `wlan0` в режим точки доступа:

   ```
   hostname# inet wifi role access-point
   ```

3. Задайте способ аутентификации пользователей и имя вашей сети Wi-Fi:

   - Аутентификация не требуется:

     ```
     hostname# inet wifi access-point authentication open
     ```

     Затем введите имя сети.

   - Для аутентификации требуется использовать пароль. Вы можете выбрать режим аутентификации WPA-PSK или WPA2-PSK:

     ```
     hostname# inet wifi access-point authentication {wpa-psk | wpa2-psk}
     ```

     Затем введите имя сети и пароль. Заданный пароль сообщите пользователям вашей сети Wi-Fi.

4. Точка доступа поддерживает стандарты:

   - IEEE 802.11b — 2,4 ГГц, скорость соединения до 11 Мбит/с.
   - IEEE 802.11g — 2,4 ГГц, скорость соединения до 54 Мбит/с (используется по умолчанию).

   Вы можете изменить стандарт связи:

   ```
   hostname# inet wifi access-point hwmode {b | g}
   ```

5. Задайте номер используемого канала Wi-Fi:

   ```
   hostname# inet wifi access-point channel <номер канала>
   ```

   По умолчанию используется канал номер 1. Допустимые номера: 1–11.

6. Назначьте сетевому интерфейсу `wlan0` статический IP-адрес:

   ```
   hostname# inet ifconfig wlan0 address <IP-адрес> netmask <маска подсети>
   ```

7. Включите сетевой интерфейс `wlan0`:

```
hostname# inet wifi mode on
```

8 Для связи между устройствами, которые подключены к сети Wi-Fi, и устройствами, подключенными к сети Ethernet, создайте транзитные фильтры открытой сети, пропускающие IP-пакеты между этими сетями.

9 Настройте параметры DHCP-сервера для интерфейса `wlan0` (см. Настройка DHCP-сервера).

6

Настройка маршрутизации

Общие сведения о маршрутизации 210

Принципы маршрутизации 211

Просмотр таблиц маршрутизации 215

Настройка статической маршрутизации 217

Настройка маршрутов протоколов DHCP и PPP 221

Настройка OSPF 226

Настройка BGP 239

Настройка BFD 255

Настройка MultiWAN 257

Общие сведения о маршрутизации

ViPNet Coordinator HW поддерживает маршрутизацию IP-трафика в сетях со сложной структурой. Маршрутизация — процесс выбора маршрута следования IP-пакета, передаваемого в сети от одного узла другому. Он выбирается из подмножества маршрутов, имеющихся в таблице маршрутизации ViPNet Coordinator HW.

Маршруты могут быть:

- статические — добавляются в таблицу маршрутизации вручную;
- динамические — добавляются в таблицу маршрутизации с помощью алгоритмов на основе информации о топологии и состоянии сети, предоставляемой протоколами динамической маршрутизации.

Динамическая маршрутизация позволяет:

- автоматически формировать таблицу маршрутизации;
- автоматически выбирать по определенным критериям лучший маршрут из нескольких доступных, в том числе, при сбое других маршрутизаторов в сети;
- распределять нагрузку IP-трафика, передаваемого в сети.

ViPNet Coordinator HW может маршрутизировать IP-трафик с использованием следующих видов маршрутов:

- статических, в том числе на основе маршрутов с несколькими шлюзами;
- получаемых по протоколам DHCP и PPP;
- динамических, формируемых протоколами OSPF, BGP.

Принципы маршрутизации

В ViPNet Coordinator HW для хранения маршрутов используются:

- Таблица маршрутизации по умолчанию (Main) — содержит:
  - статические маршруты, заданные вручную (Static).
  - маршруты в подсети, к которым подключены сетевые интерфейсы (Connected);
  - маршруты, полученные по протоколам DHCP, PPP, OSPF и BGP.
- Пользовательские таблицы маршрутизации — содержат только статические маршруты, заданные вручную, и используются для создания политик маршрутизации (см. Настройка MultiWAN).

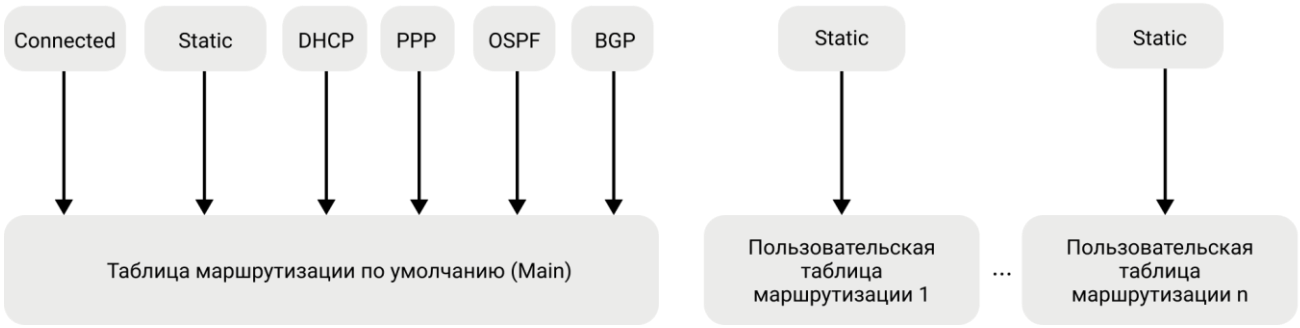


Рисунок 42. Формирование таблиц маршрутизации

В маршрутизации трафика участвуют не все маршруты, содержащиеся в таблице маршрутизации, а только лучшие маршруты в каждую сеть (подробнее см. «Формирование списка лучших маршрутов» ниже).

Характеристики маршрутов

- Источник получения маршрута: Connected, Static, PPP, DHCP, OSPF, BGP — определяет, каким образом был получен маршрут.
- Административная дистанция — определяет приоритет маршрута от каждого источника. Учитывается, когда в таблице маршрутизации есть несколько маршрутов в одну и ту же сеть:
  - Чем меньше административная дистанция, тем более приоритетным считается маршрут.
  - Административная дистанция задаётся для каждого статического маршрута.
  - Административная дистанция маршрутов протокола PPP отдельно не задаётся и равна дистанции маршрутов протокола DHCP.
  - Административная дистанция маршрутов протоколов OSPF и BGP задаётся не для конкретного маршрута, а для всех маршрутов протокола.
  - Административная дистанция статических маршрутов не может совпадать с дистанцией, заданной для маршрутов протоколов OSPF и BGP.

Примечание. Для каждого типа маршрутов задана административная дистанция по умолчанию:

- для статических маршрутов — 10;
- для маршрутов протоколов DHCP и PPP — 70;
- для маршрутов протокола OSPF — 110;
- для маршрутов протокола iBGP — 200;
- для маршрутов протокола eBGP — 20.

Для первых двух типов маршрутов вы можете изменять значение административной дистанции, для маршрутов остальных типов изменить это значение невозможно.

- Метрика — определяет приоритет маршрутов протоколов DHCP, PPP и OSPF. Чем меньше метрика, тем выше приоритет маршрута.
  - Для маршрутов протокола DHCP метрики указываются вручную, причём на каждом сетевом интерфейсе, на котором включен режим DHCP и настроен параметр получения маршрутов от DHCP-сервера. Таким образом, если на разные сетевые интерфейсы будут получены одинаковые маршруты в одну и ту же сеть, то будет выбран маршрут с наименьшей метрикой.
  - Для маршрутов протокола PPP метрика также может быть задана вручную в том случае, если ViPNet Coordinator HW подключён к нескольким сетям, одной из которых является сеть 3G/4G, а в другой установлен DHCP-сервер. Если метрики для маршрутов протоколов DHCP и PPP не были заданы, то используется метрика по умолчанию.
  - Для маршрутов протокола OSPF метрика (стоимость) вычисляется автоматически.
- Вес — определяет долю IP-трафика, который будет проходить по маршруту через указанный шлюз. Используется в статических маршрутах и multipath-маршрутах протокола BGP. Вес задаётся для шлюза. Позволяет настроить балансировку передаваемого IP-трафика между несколькими шлюзами, когда часть IP-пакетов направляется на один шлюз, а часть — на другой.

Политики маршрутизации

Выбор, по какой таблице маршрутизировать трафик, определяется активной политикой маршрутизации. В качестве активной политики вы можете выбрать:

- Политику маршрутизации по умолчанию — выбрана автоматически после инициализации ViPNet Coordinator HW. Политика использует маршруты из таблицы маршрутизации по умолчанию (Main). Настройка политики недоступна.

- Одну из пользовательских политик маршрутизации — создаются пользователем. С помощью таких политик вы можете разделить IP-трафик по признакам и маршрутизировать его по разным таблицам маршрутизации (см. Настройка функции MultiWAN).

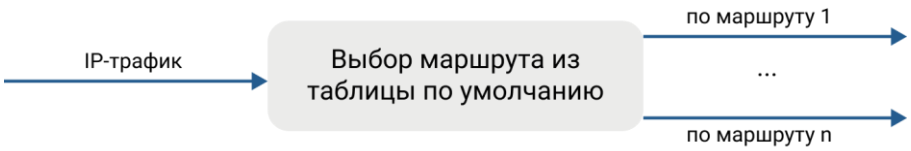


Рисунок 43. Маршрутизация при политике по умолчанию

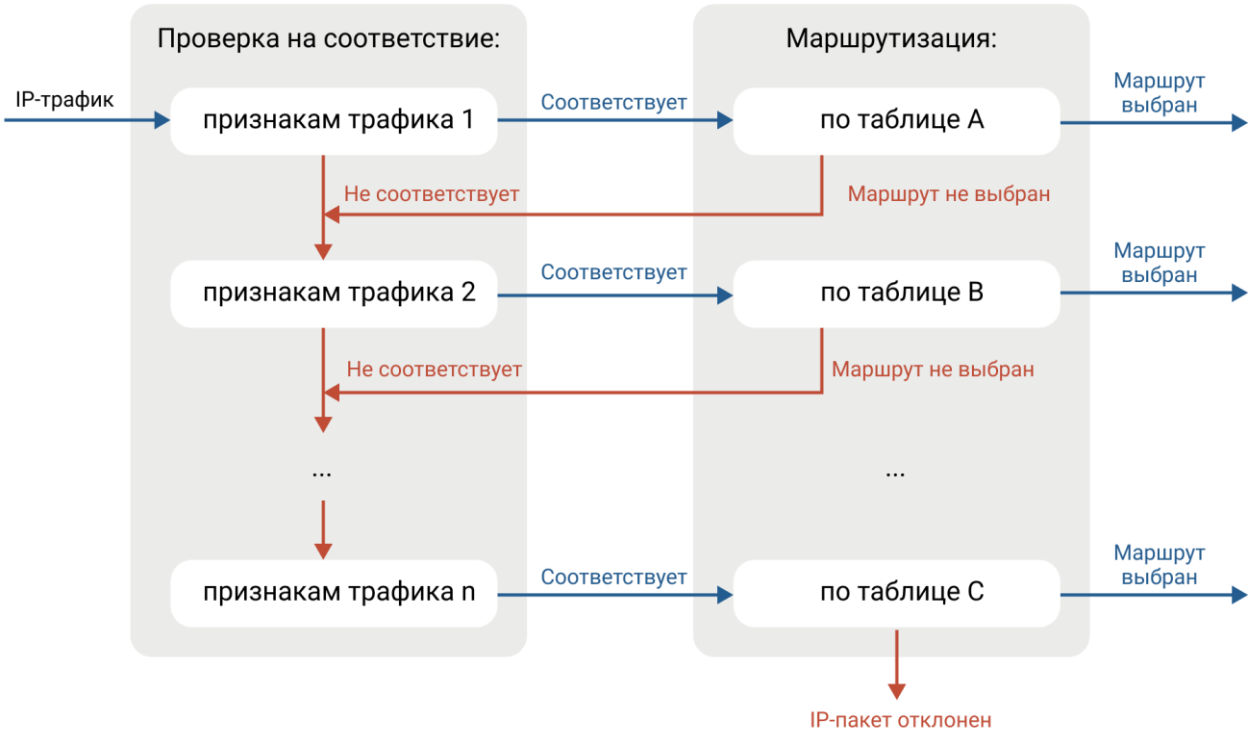


Рисунок 44. Маршрутизация при пользовательской политике

Пользовательская политика маршрутизации состоит из правил маршрутизации. Для каждого правила задаются:

- Приоритет — определяет в каком порядке правила будут применяться к трафику.
- Признаки трафика — задают условия, которым должен соответствовать трафик. Если признаки не указаны, правило распространяется на весь трафик.
- Таблица маршрутизации, по которой должен обрабатываться трафик, соответствующий заданным признакам трафика. Можно указать пользовательскую таблицу или таблицу по умолчанию.

Принципы маршрутизации при использовании пользовательской политики:

- IP-пакет последовательно проходит проверку правилами маршрутизации в соответствии с их приоритетом.
- Если IP-пакет соответствует всем признакам, заданным в правиле, он будет обработан по указанной таблице маршрутизации.

- Если IP-пакет не соответствует хотя бы одному из признаков правила, он передаётся на проверку следующему по приоритету правилу маршрутизации.

Формирование списка лучших маршрутов

В маршрутизации участвуют только лучшие статические и динамические маршруты в каждую сеть. Остальные маршруты в таблице игнорируются. Лучшие маршруты определяются в каждой таблице маршрутизации по следующим правилам:

- Из нескольких маршрутов в одну сеть лучшим признаётся маршрут с меньшей административной дистанцией, даже если маршруты получены из разных источников (Static, DHCP, PPP, OSPF, BGP). Например, имеется два маршрута в сеть 10.0.5.0 с маской 255.255.255.0. Для первого маршрута задана административная дистанция — 10, для второго — 30. В результате в маршрутизации будет участвовать первый маршрут. Если дистанции маршрутов, полученных из одного источника, равны, будут участвовать оба маршрута.
- Из нескольких маршрутов с разными префиксами (например, 10.0.0.0/8 и 10.0.0.0/16) лучшими признаются все маршруты.

Выбор маршрута из списка лучших

В процессе маршрутизации для каждого IP-пакета выбирается маршрут из списка лучших маршрутов. При наличии нескольких маршрутов в нужную сеть применяются правила:

- Из нескольких лучших маршрутов DHCP в одну сеть будет выбран маршрут с наименьшей метрикой. Если метрики равны, маршруты будут выбраны в соответствии со стратегией ECMP (equal-cost multi-path routing).
- Из нескольких лучших маршрутов в одну сеть с разным префиксом (маской подсети), будет выбран маршрут с наиболее длинным префиксом.
- Маршруты от одного источника в одну и ту же сеть объединяются в один маршрут с несколькими шлюзами (multi-hop route):
  - Статические маршруты — по признаку одинаковых административных дистанций маршрутов.
  - Маршруты DHCP и PPP — по признаку одинаковых метрик маршрутов.
  - Маршруты OSPF и BGP — маршрутизаторами OSPF и BGP.

  При просмотре такие маршруты отображаются в виде одного маршрута с несколькими шлюзами:

```
10.100.2.0/24 [30/23]  (weight 1) via 10.1.30.202, eth1
                       (weight 1) via 10.1.31.201, eth2
```



Внимание! Если хотя бы один из шлюзов объединённого маршрута multi-hop route выйдет из строя, работоспособность маршрута не гарантируется.

Просмотр таблиц маршрутизации

Чтобы просмотреть список всех маршрутов в таблице маршрутизации по умолчанию (Main):

```
hostname> inet show routing
```

```
xf> inet show routing
Codes: * - FIB route,  > - selected route,  A - Babel,  B - BGP,
          C - connected,  D - DHCP/PPP,  E - EIGRP,  F - PBR,
          I - IS-IS,  K - kernel route,  O - OSPF,  R - RIP,
          S - static,  T - Table,  V - VNC-Direct,
Routing table MAIN (254)
B>* 10.5.0.0/24         [200/0] (weight 1) 172.16.0.5, eth1, 02:04:45
B>* 10.44.0.0/22        [200/0] (weight 1) 172.16.0.5, eth1, 02:04:45
B>* 10.44.8.128/26      [200/0] (weight 1) 172.16.0.5, eth1, 02:04:45
B>* 10.44.9.176/30      [200/0] (weight 1) 172.16.0.5, eth1, 02:04:45
B>* 10.44.9.180/31      [200/0] (weight 1) 172.16.0.5, eth1, 02:04:45
D   0.0.0.0/0           [70/70] 172.19.0.100, eth2
K>* 0.0.0.0/0          172.18.0.10, eth0
S   0.0.0.0/0           [10/0] 172.18.0.10, eth0
D>* 10.0.3.3/32         [70/70] 172.19.0.2, eth2
D>* 10.1.3.5/32         [70/70] 172.19.0.4, eth2
O>* 10.4.0.0/24         [110/20] 172.18.0.4, eth0, 02
K>* 10.10.0.0/16       (weight 1) 172.16.0.213, eth1
  *                    (weight 1) 172.18.0.123, eth0
  *                    (weight 1) 172.19.0.32, eth2
S   10.10.0.0/16        [10/0] (weight 1) 172.18.0.123, eth0
                               (weight 1) 172.16.0.213, eth1
                               (weight 1) 172.19.0.32, eth2
K>* 10.11.1.0/24       172.18.0.12, eth0
C>* 127.0.0.0/8        is directly connected, lo
C>* 172.16.0.0/24      is directly connected, eth1
O   172.18.0.0/24       [110/10] is directly connected, eth0, 02
C>* 172.18.0.0/24      is directly connected, eth0
C>* 172.19.0.0/24      is directly connected, eth2
```

Рисунок 45. Просмотр таблицы маршрутизации MAIN

Таблица 11. Атрибуты маршрутов

Атрибут	Расшифровка в командном интерпретаторе	Пояснение
C	connected	Маршрут в подсеть, к которой подключен один из интерфейсов ViPNet Coordinator HW
S	static	Статический маршрут
O	OSPF	Маршрут протокола OSPF
B	BGP	Маршрут протокола BGP
D	DHCP/PPP	Маршрут протокола DHCP или PPP-сервером

>	selected route	Лучший маршрут — отображается, если в таблице есть несколько маршрутов в одну и ту же сеть с разной административной дистанцией
*	FIB route	Маршрут, признанный лучшим и участвующий в маршрутизации



Примечание. В таблице маршрутизации могут присутствовать другие атрибуты, кроме описанных в таблице выше. Эти атрибуты зарезервированы для других протоколов маршрутизации и в текущей версии ViPNet Coordinator HW не используются.

Вес статического маршрута отображается при наличии нескольких маршрутов в одну сеть. Если маршрут единственный, его вес принимается равным единице.

Чтобы просмотреть определённые типы маршрутов из таблицы маршрутизации по умолчанию:

```
hostname> inet show routing {static table default | dhcp | ospf | bgp}
```

где:

- `static table default` — просмотр статических маршрутов;
- `dhcp` — просмотр маршрутов протоколов DHCP и PPP;
- `ospf` — просмотр маршрутов протокола OSPF;
- `bgp` — просмотр маршрутов протокола BGP.

Чтобы просмотреть содержимое пользовательской таблицы маршрутизации:

```
hostname> inet show routing static table {<номер таблицы> | name <имя таблицы>}
```

где:

- `<номер таблицы>` — номер пользовательской таблицы маршрутизации;
- `<имя таблицы>` — имя пользовательской таблицы маршрутизации.

Настройка статической маршрутизации

Если ViPNet Coordinator HW функционирует в сети, конфигурация которой не меняется или в которой используется минимальное количество путей для доставки IP-пакетов, то вы можете настроить маршрутизацию на ViPNet Coordinator HW с помощью статических маршрутов. Статическая маршрутизации может потребоваться, когда нет возможности использовать маршрутизаторы, работающие по протоколам динамической маршрутизации, или в следующих случаях:

- Чтобы направлять часть IP-трафика по конкретным маршрутам (например, есть требование направлять IP-трафик по самому надежному каналу связи) или через конкретный шлюз.
- Нужен статический маршрут по умолчанию, если работа по протоколам динамической маршрутизации невозможна.
- Чтобы распределять передачу IP-трафика по нескольким маршрутам.

Создание статических маршрутов

Вы можете добавить статические маршруты в таблицу маршрутизации по умолчанию или создать пользовательские таблицы маршрутизации. Пользовательские таблицы используются для создания политик маршрутизации (см. Принципы маршрутизации).

- Чтобы добавить маршрут по умолчанию в таблицу маршрутизации по умолчанию:

  ```
  hostname# inet route add default next-hop <IP-адрес шлюза> [distance <1-255> [weight <1-255>]]
  ```

- Чтобы добавить статический маршрут в таблицу маршрутизации по умолчанию:

  ```
  hostname# inet route add <IP-адрес назначения> [netmask <маска>] next-hop <IP-адрес шлюза> [distance <1-255> [weight <1-255>]]
  ```



Совет. Если вам требуется добавить один статический маршрут с несколькими шлюзами, создайте несколько статических маршрутов в одну и ту же сеть с одинаковой административной дистанцией, указав в каждом по одному шлюзу. В результате эти маршруты будут просуммированы и объединены в один с несколькими шлюзами. Как правило, такие маршруты требуются для балансировки нагрузки, поэтому в маршрутах также должен быть задан вес шлюзам (см. ниже).

- Чтобы добавить маршрут в пользовательскую таблицу маршрутизации (см. Настройка MultiWAN):

```
hostname# inet route add {<IP-адрес назначения> [netmask <маска>] | default} next-hop
<IP-адрес шлюза> table <номер таблицы> [name <имя таблицы>] [distance <1-255> [weight
<1-255>]]
```

Если указанной таблицы маршрутизации не существует, она будет создана с заданными именем и номером.

Во всех командах вы можете задать необязательные параметры: `distance` — административную дистанцию маршрута и `weight` — вес шлюза.

Административная дистанция задаётся, чтобы назначить приоритет маршруту. Если вы не укажете значение административной дистанции, то оно будет задано автоматически: `distance=10`. Если вы укажете административную дистанцию, и её значение будет совпадать со значением административной дистанции, заданной протоколам динамической маршрутизации, появится сообщение, что маршрут не может быть добавлен. В этом случае создайте маршрут с другим значением административной дистанции.

Вес задается в маршруте для шлюза. Его требуется задавать в том случае, если создаётся несколько маршрутов в одну сеть с разными шлюзами, между которыми требуется производить балансировку нагрузки. Подробнее см. раздел Настройка балансировки IP-трафика.

Если маршрут, добавленный в таблицу маршрутизации по умолчанию, будет определён как лучший, то он будет участвовать в маршрутизации IP-трафика.

Для использования пользовательских таблиц маршрутизации создайте политику маршрутизации и активируйте её (см. Настройка MultiWAN).

Удаление статических маршрутов

Вы можете удалить маршрут по умолчанию или статический маршрут:

- Чтобы удалить маршрут по умолчанию из таблицы маршрутизации по умолчанию:

  ```
  hostname# inet route delete default next-hop <IP-адрес шлюза>
  ```

- Чтобы удалить статический маршрут из таблицы маршрутизации по умолчанию:

  ```
  hostname# inet route delete <IP-адрес назначения> [netmask <маска подсети>] next-hop
  <IP-адрес шлюза>
  ```

- Чтобы удалить маршрут из пользовательской таблицы маршрутизации:

  ```
  hostname# inet route delete {<IP-адрес назначения> [netmask <маска подсети>] | default}
  next-hop <IP-адрес шлюза> table <номер таблицы> [name <имя таблицы>]
  ```

Если при вводе команды вы не указали маску подсети или IP-адрес шлюза, и в процессе проверки будет установлено, что в таблице маршрутизации есть несколько маршрутов в указанную сеть, то на экран будет выведен список этих маршрутов. Для удаления всех выбранных маршрутов введите `y` и нажмите **Enter**. Аналогичная ситуация возникнет при удалении маршрута с несколькими шлюзами.

После удаления маршрута будет выбран новый лучший маршрут в ту же сеть.

Примечание. Если требуется удалить все статические маршруты, включая все маршруты по умолчанию, воспользуйтесь командой:

```
hostname# inet route clear [table {<номер таблицы> | name <имя таблицы>}]
```

Настройка балансировки IP-трафика

Если вы хотите ускорить процесс отправки IP-пакетов в сеть назначения, вы можете создать несколько статических маршрутов в данную сеть через разные шлюзы и настроить балансировку IP-трафика между этими маршрутами. Это позволит в процессе разных TCP-соединений отправлять часть IP-пакетов по одному маршруту, часть — по-другому, что повысит скорость передачи IP-пакетов в сеть назначения. Балансировка IP-трафика настраивается с помощью одного из параметров маршрутов — веса (`weight`). При этом все маршруты, которые будут участвовать в балансировке IP-трафика, должны иметь одинаковую административную дистанцию, то есть иметь одинаковый приоритет.

Примечание. При маршрутизации маршруты в одну сеть назначения и с одинаковой дистанцией объединяются в один маршрут с несколькими шлюзами (multi-hop route). При просмотре таблицы маршрутизации они отображаются как один маршрут с несколькими шлюзами (см. Принципы маршрутизации).

Для настройки балансировки IP-трафика:

1. Создайте нужное количество маршрутов с одинаковым адресом назначения и с разными шлюзами.
2. Задайте каждому маршруту одинаковую административную дистанцию.
3. Задайте в каждом маршруте вес шлюзу. IP-трафик будет распределяться между шлюзами в соответствии с соотношением их весов. Например:
   - если вы создаёте 2 маршрута и в каждом маршруте вес шлюза равен 1, то IP-трафик будет разделён между этими маршрутами поровну, то есть 50% IP-трафика будет передаваться по одному маршруту, 50% — по второму;
   - если вы создаёте 3 маршрута, и в первом маршруте вес шлюза равен 1, во втором — вес шлюза равен 2, в третьем — вес шлюза равен 3, то по второму маршруту будет передаваться в два раза больше IP-трафика, чем по первому, по третьему — в три раза больше, чем по первому.

Пример команд для создания статических маршрутов с весом шлюзов равным 1:

```
hostname# inet route add 10.0.5.0 netmask 255.255.255.0 next-hop 10.0.1.1 distance 20
weight 1

hostname# inet route add 10.0.5.0 netmask 255.255.255.0 next-hop 10.0.4.3 distance 20
weight 1
```

Примечание. Если в процессе создания маршрута вы не укажете вес шлюза, то шлюзу автоматически будет назначен вес равный 1. Вы не можете задать вес равный 0.

Балансировка IP-трафика будет осуществляться только если созданные маршруты признаны лучшими (см. Принципы маршрутизации).

Просмотр статических маршрутов

Чтобы просмотреть список всех статических маршрутов, содержащихся в таблице маршрутизации по умолчанию и в пользовательских таблицах маршрутизации:

```
hostname> inet show routing static
```

```
hw> inet show routing static
Table 254 (MAIN)
Destination      Netmask          Next hop         Distance Weight
-----------      -------          --------         -------- ------
0.0.0.0          0.0.0.0          172.18.0.10      10       1
10.10.0.0        255.255.0.0      172.16.0.213     10       1
10.10.0.0        255.255.0.0      172.18.0.123     10       1
10.10.0.0        255.255.0.0      172.19.0.32      10       1
10.11.1.0        255.255.255.0    172.18.0.12      10       1
10.11.1.112      255.255.255.240  172.16.0.210     10       1
10.11.3.128      255.255.255.192  172.16.0.22      10       1
10.11.3.128      255.255.255.192  172.18.0.10      100      200
10.11.5.123      255.255.255.255  172.18.0.10      234      128
```

Рисунок 46. Просмотр статических маршрутов

В списке для каждого маршрута указаны: IP-адрес назначения, маска сети, шлюз, административная дистанция маршрута и вес шлюза.

Настройка маршрутов протоколов DHCP и PPP

Если на каком-либо сетевом интерфейсе ViPNet Coordinator HW включен режим DHCP и настроено автоматическое получение маршрутов (см. Настройка сетевых интерфейсов Ethernet), то в процессе маршрутизации будут использоваться эти маршруты. В этом случае настройте дополнительные параметры:

1. Настройте административную дистанцию для протокола DHCP. Это позволит определить приоритет маршрутов DHCP-сервера среди всех маршрутов в таблице маршрутизации по умолчанию (статических маршрутов, маршрутов протокола OSPF, если такие есть).
2. Если режим DHCP включен на нескольких сетевых интерфейсах, настройте метрики протокола DHCP на каждом сетевом интерфейсе, на котором включен этот режим. Это позволит определить приоритет среди маршрутов DHCP-сервера в одну и ту же сеть, полученных с разных сетевых интерфейсов.

Если ViPNet Coordinator HW подключен к сети 3G/4G и получает информацию для маршрута по умолчанию от PPP-сервера провайдера (см. Подключение к мобильной сети 3G/4G), и при этом он также подключен к другой сети и получает в ней маршрутную информацию от DHCP-сервера, то в этом случае задайте метрику для PPP-протокола. Это позволит определить, какой маршрут по умолчанию (сформированный на основе шлюза по умолчанию от PPP-сервера или предоставленный DHCP-сервером) является приоритетным. Административная дистанция для этого протокола не задается и равна дистанции для протокола DHCP.

Настройка административной дистанции для маршрутов DHCP-протокола

Если на ViPNet Coordinator HW настроено взаимодействие с DHCP-сервером, от которого поступают маршруты, а также настроена статическая маршрутизация (см. Настройка статической маршрутизации) или динамическая маршрутизация (см. Настройка OSPF), то задайте административную дистанцию для маршрутов протокола DHCP. Административная дистанция определит приоритет данных маршрутов среди всех остальных, и в случае, если будет обнаружено несколько маршрутов в одну и ту же сеть из разных источников, будет выбран тот маршрут, у которого выше приоритет. Чем меньше значение административной дистанции, тем выше приоритет маршрута.

В настройках ViPNet Coordinator HW вы можете:

- Задать административную дистанцию для маршрутов, поступающих от DHCP-сервера:

  ```
  hostname# inet dhcp client route-distance <1-255>
  ```

Эта дистанция будет определять приоритет всех маршрутов DHCP-сервера, независимо от того, на какой сетевой интерфейс они поступили.

- Задать административную дистанцию для маршрутов по умолчанию вместе с общей административной дистанцией для всех маршрутов DHCP-сервера:

  `hostname# inet dhcp client route-distance <1-255> [default-route <1-255>],`

  где `default-route <1-255>` — значение административной дистанции для маршрутов по умолчанию.

  Эта дистанция будет определять приоритет только маршрутов по умолчанию. Если дистанция не задана, то у маршрутов по умолчанию дистанция и приоритет будет таким же, как и у других маршрутов DHCP-сервера.

При необходимости перед или после настройки административной дистанции вы можете посмотреть, на каких сетевых интерфейсах включен режим DHCP и какая административная дистанция задана. Подробнее см. раздел Просмотр настроек DHCP в режиме клиента.

Настройка метрики для маршрутов DHCP-протокола

Если на ViPNet Coordinator HW режим DHCP включён на нескольких сетевых интерфейсах, то может сложиться ситуация, когда с этих интерфейсов поступят разные маршруты от DHCP-сервера в одну и ту же сеть. В этом случае требуется определить лучший маршрут, чтобы использовать его при маршрутизации трафика. Параметром, позволяющим выбрать лучший маршрут, выступает метрика маршрута. Её можно задать на каждом сетевом интерфейсе, на котором включён режим DHCP, чтобы определить приоритет маршрутов DHCP-сервера на разных сетевых интерфейсах. Чем меньше значение метрики, тем выше приоритет маршрута. Если на разных сетевых интерфейсах заданы одинаковые метрики, то поступившие маршруты в одну и ту же сеть будут объединены в один маршрут с несколькими шлюзами.

В ViPNet Coordinator HW вы можете задать или удалить метрику для маршрутов DHCP-сервера на конкретном сетевом интерфейсе (далее — специфичная метрика). Если специфичная метрика не задана, то вместо неё используется метрика по умолчанию.

- Чтобы добавить специфичную метрику на сетевом интерфейсе:

  `hostname# inet ifconfig <имя интерфейса> dhcp route-metric <1-255>`

Примечание. Задать специфичную метрику для протокола DHCP вы можете на сетевых интерфейсах следующих типов:

- Ethernet (см. Настройка сетевых интерфейсов Ethernet).
- VLAN.
- Wi-Fi (wlan) (см. Подключение к сети Wi-Fi).
- Агрегированный интерфейс.

Если режим DHCP включен только на одном сетевом интерфейсе, то настройка специфичной метрики не требуется, поскольку для группы маршрутов в рамках одного сетевого интерфейса она всегда будет одинаковой.

- Чтобы удалить метрику, заданную на сетевом интерфейсе:

  ```
  hostname# inet ifconfig <имя интерфейса> dhcp route-metric none
  ```

  После удаления метрики на этом интерфейсе будет использоваться метрика по умолчанию.

При необходимости перед или после настройки метрик вы можете посмотреть, на каких сетевых интерфейсах включен режим DHCP и какие метрики заданы. Подробнее см. раздел Просмотр настроек DHCP в режиме клиента.

Настройка метрики для маршрутов PPP-протокола

Одновременно с подключением к мобильной сети ViPNet Coordinator HW может быть подключен к другим сетям, в которых маршруты распространяются по DHCP-протоколу. В этом случае ViPNet Coordinator HW также будет получать маршруты по умолчанию в эти сети. Чтобы маршрут по умолчанию PPP-протокола имел приоритет выше, чем маршруты по умолчанию DHCP-протокола, задайте метрику для PPP-протокола (далее — специфичную метрику). Причем она должна быть меньше любой метрики маршрутов по умолчанию, полученных по DHCP-протоколу. Если специфичная метрика не будет задана, то вместо нее будет использоваться метрика по умолчанию (см. Изменение метрики по умолчанию для маршрутов протоколов DHCP и PPP). В этом случае маршруты по умолчанию PPP- и DHCP-протокола будут иметь одинаковый приоритет.

- Чтобы добавить специфичную метрику для PPP-протокола:

  ```
  hostname# inet usb-modem set route-metric <1-255>
  ```

- Чтобы удалить специфичную метрику для PPP-протокола:

  ```
  hostname# inet usb-modem set route-metric none
  ```

  После удаления метрики для протокола PPP будет использоваться метрика по умолчанию.

Изменение метрики по умолчанию для маршрутов протоколов DHCP и PPP

Если для маршрутов протоколов DHCP и PPP не задавались специфичные метрики, то для определения приоритета маршрутов будет использоваться метрика по умолчанию (первоначально — 70).

Чтобы изменить метрику:

```
hostname# inet dhcp client route-default-metric <1-255>
```

Просмотр настроек DHCP в режиме клиента

Вы можете просмотреть следующие параметры DHCP в режиме клиента:

- административная дистанция, которая задана для маршрутов, поступающих от DHCP-сервера (см. Настройка административной дистанции для маршрутов DHCP-протокола);
- метрика по умолчанию (см. Настройка метрики для маршрутов DHCP-протокола);
- сетевые интерфейсы, на которых включен режим DHCP;
- специфичные метрики на сетевых интерфейсах, если такие заданы;
- разрешение на автоматическое получение IP-адресов, адресов DNS- и NTP-серверов.

Чтобы посмотреть указанные настройки:

```
hostname> inet show dhcp client
```

В результате выполнения команды указанные настройки будут отражены в следующем виде:

```
hw50-2b3b0014# inet show dhcp client
Administrative distance for DHCP/PPP routes: 70
Default metric for DHCP/PPP routes: 70

Interface  DHCP  Routes  Metric   DNS  NTP
---------  ----  ------  ------   ---  ---
     eth0    no     yes  default  yes  yes
     eth1    no     yes  default  yes  yes
     eth2    no     yes  default  yes  yes
hw50-2b3b0014#
```

Рисунок 47. Просмотр настроек DHCP-режима

Просмотр маршрутов DHCP/PPP-протокола

Чтобы просмотреть список маршрутов, полученных от DHCP/PPP-сервера:

```
hostname> inet show routing dhcp
```

```
hw-va-16310046# inet show routing dhcp
DHCP routes currently available: (* = RIB route)
>* 0.0.0.0/0 [35/23] via 10.1.30.5, eth1
>* 10.100.1.0/24 [30/23] via 10.1.30.201, eth1
>* 10.100.2.0/24 [30/23] via 10.1.30.202, eth1
 *                      via 10.1.30.202, eth1
hw-va-16310046#
```

Рисунок 48. Просмотр маршрутов DHCP-сервера

В списке для каждого маршрута указаны: атрибут, IP-адрес назначения, маска сети, шлюз и имя сетевого интерфейса, на который поступил маршрут. Если маршрут определён как лучший маршрут в сеть, перед ним указан атрибут «*».

Настройка OSPF

Настройка динамической маршрутизации по протоколу OSPF имеет смысл в том случае, если в сети, в которой установлен ViPNet Coordinator HW, одновременно выполняются следующие условия:

- используются другие OSPF-маршрутизаторы, и они напрямую связаны с ViPNet Coordinator HW;
- используется протокол OSPF версии 2;
- поддерживается многоадресное вещание (multicast);
- по требованиям безопасности вашей организации разрешена передача IP-трафика по протоколу OSPF между сетевыми узлами.

В процессе настройки маршрутизации по протоколу OSPF вам потребуется:

- включить использование протокола OSPF;
- указать сети, к которым подключен ViPNet Coordinator HW и которые будут участвовать в маршрутизации по протоколу OSPF, и области маршрутизации;
- создать ряд сетевых фильтров.



Внимание! При использовании OSPF необходимо настроить аутентификацию.

Если ViPNet Coordinator HW непосредственно связан с другими координаторами, рекомендуется при задании IP-адреса доступа этих координаторов указывать метрику `1`. В этом случае при наличии нескольких альтернативных маршрутов защищенный трафик всегда будет передаваться по кратчайшему маршруту — через соседний координатор.

При необходимости вы также можете настроить Настройка перераспределения маршрутов.

Общие сведения о протоколе OSPF

Протокол OSPF — внутренний шлюзовой протокол (Interior Gateway Protocol, IGP), используется для распространения данных маршрутизации внутри одной автономной системы.

Реализация протокола OSPF в ViPNet Coordinator HW имеет ограничения: из RFC 2328 не поддерживаются:

- изменение пропускной способности reference-bandwidth — cost, auto-cost;
- настройка метрик маршрутов;
- перераспределение (redistribute) маршрутов, кроме заданных статически и полученных по DHCP;

- настройка параметров взаимодействия соседних маршрутизаторов — HelloInterval и DeadInterval;
- другие типы областей (area type), кроме backbone и standard;
- настройка типа сети (network types), — задан тип Broadcast;
- фильтрация по политике импорта и экспорта маршрутов;
- виртуальные каналы (Virtual Links).

OSPF-маршрутизация работает следующим образом:

1. OSPF-маршрутизаторы устанавливают связь друг с другом посредством многоадресной (multicast) рассылки.
2. OSPF-маршрутизаторы начинают обмениваться сообщениями типа LSA (Link State Advertisements), в которых передают информацию о состоянии каналов связи с помощью однонаправленной (unicast) рассылки.
3. При получении LSA-сообщения информация из него заносится в базу данных (link state database). Если LSA-сообщение содержит новую информацию о канале связи по сравнению с той, которая содержится в базе данных, то оно передаётся маршрутизаторам-соседям.
4. На каждом маршрутизаторе по алгоритму Дейкстры (SPF algorithm) вычисляется множество кратчайших маршрутов ко всем сетям назначения и их стоимость. Таким образом, каждый OSPF-маршрутизатор имеет собственное представление о состоянии каналов связи и топологии сети, но при этом все маршрутизаторы используют одну базу данных состояний каналов связи для вычисления кратчайших маршрутов.

Межсетевая среда, в которой находятся OSPF-маршрутизаторы, представляется как совокупность областей маршрутизации, соединённых друг с другом через некоторую базовую область.

Выделяют следующие типы областей маршрутизации:

- Базовая или область 0 (backbone area) — с ней должны быть соединены все остальные области автономной системы.
- Стандартная (standard area) — граничит как с другими областями, так и с другими автономными системами.
- Стандартная тупиковая (stub area) — граничит только с другими областями.
- Полностью тупиковая (totally stubby area) — граничит только с одной областью.
- Не полностью тупиковая (not-so-stubby area) — стандартная тупиковая область, которая может взаимодействовать с другими автономными системами с помощью пограничных маршрутизаторов (ABR).

Каждый OSPF-маршрутизатор входит в определённую область маршрутизации и обменивается информацией только с маршрутизаторами, входящими в эту же область. При этом обмен идет не напрямую, а через посредника — маршрутизатор, выбранный главным в этой области. Информация между разными областями передаётся через маршрутизатор, который располагается на границе этих областей. Если автономная система взаимодействует с другой автономной системой, то информация передаётся через маршрутизатор, который располагается на границе

систем. Такой подход позволяет уменьшить объём рассылаемых LSA-сообщений, тем самым уменьшить нагрузку на маршрутизаторы и повысить скорость построения таблиц маршрутизации.

Выделяют следующие типы маршрутизаторов:

- Внутренний (internal router, IR) — все его сетевые интерфейсы находятся в одной области.
- Назначенный (designated router, DR) — выбран главным среди всех внутренних маршрутизаторов в одной области.
- Резервный назначенный (backup designated router, BDR) — берёт на себя функции главного в случае, если главный маршрутизатор вышел из строя.
- Межобластной граничный (area border router, ABR) — соединяет несколько областей OSPF одной автономной системы.
- Граничный маршрутизатор автономной системы (autonomous system boundary router, ASBR) — граничит с другой автономной системой, работающей по другому протоколу динамической маршрутизации (IGRP, EIGRP, IS-IS, RIP, BGP, Static).



Примечание. Для проверки подлинности маршрутов, полученных с других устройств по протоколу OSPF, мы рекомендуем настроить аутентификацию на маршрутизаторах.

Протокол OSPF поддерживает два способа аутентификации:

- простая аутентификация на пароле (simple password authentication). Одинаковый пароль настраивается на интерфейсах, через которые передаётся информация по протоколу OSPF. Пароль передаётся в открытом виде.
- криптографическая аутентификация (cryptographic authentication). Общий секретный ключ и идентификатор ключа настраиваются на интерфейсах, через которые передаётся информация по протоколу OSPF. Ключ передаётся в зашифрованном виде (используется алгоритм хэширования md5).

Аутентификация настраивается для соседних маршрутизаторов. По умолчанию протокол OSPF не использует аутентификацию.

Настройка протокола OSPF

Для настройки протокола OSPF:

1 Включите использование протокола:

```
hostname# inet ospf mode on
```

2 Укажите сеть, в которой осуществляется обмен информацией по протоколу OSPF:

```
hostname# inet ospf network add <IP-адрес назначения> netmask <маска сети> area
<0-4294967295>
```

К данной сети должен быть подключен сетевой интерфейс ViPNet Coordinator HW.

С помощью параметра `area` задайте область маршрутизации, в которую входит ViPNet Coordinator HW (см. Общие сведения о протоколе OSPF).

Примечание. Вы можете указать не более 128 сетей, в которых осуществляется обмен информацией по протоколу OSPF.

3 Для защиты от получения ложной информации от других устройств по протоколу OSPF, настройте аутентификацию. По умолчанию обмен информацией по протоколу OSPF происходит без аутентификации.

Внимание! Настройки аутентификации на маршрутизаторах, которые обмениваются информацией, должны быть одинаковыми.

3.1 Включите аутентификацию в выбранной области маршрутизации:

- Аутентификация на простом пароле:

  ```
  hostname# inet ospf area <area> auth on pswd
  ```

- Криптографическая аутентификация:

  ```
  hostname# inet ospf area <area> auth on md5,
  ```

  где `<area>` — область маршрутизации.

3.2 Установите пароль (при аутентификации на пароле) или добавьте ключ (при криптографической аутентификации) на интерфейсе, за которым находится область маршрутизации:

- Установка пароля:

  ```
  hostname# inet ospf interface <интерфейс> password
  ```

- Добавление ключа:

  ```
  hostname# inet ospf interface <интерфейс> keys add <keyid>
  ```

  Примечание. На каждом интерфейсе вы можете создать не более 255 ключей с уникальным `keyid` и только один пароль.

4 Создайте на ViPNet Coordinator HW следующие фильтры открытой сети:

- Фильтры, разрешающие входящий однонаправленный (unicast) и многоадресный (multicast) IP-трафик по протоколу OSPF от всех соседних OSPF-маршрутизаторов, с которыми взаимодействует ViPNet Coordinator HW:

  ```
  hostname# firewall local add 1 rule "Allow OSPF unicast" src <IP-адрес
  OSPF-маршрутизатора> dst @local service @OSPF pass
  ```

```
hostname# firewall local add 2 rule "Allow OSPF multicast" src <IP-адрес
OSPF-маршрутизатора> dst @multicast service @OSPF pass
```

Фильтры должны быть созданы для каждого соседнего OSPF-маршрутизатора в области, в которой находится ViPNet Coordinator HW.



Примечание. В фильтрах вместо service @OSPF вы можете указать proto 89.

- Фильтр, разрешающий исходящий трафик ViPNet Coordinator HW по протоколу OSPF на любой IP-адрес назначения:

  ```
  hostname# firewall local add 3 rule "Allow OSPF outcoming" src @local dst @any
  service @OSPF pass
  ```

Подробнее о создании сетевых фильтров см. в разделе Создание сетевого фильтра.

5 Если между координаторами сети ViPNet установлены связи на уровне пользователей (в том числе между координатором и ViPNet xFirewall), разрешите трафик протокола OSPF в защищенной сети:

```
hostname# firewall vpn add 1 rule "Allow OSPF outcoming" src @local dst @any service
@OSPF pass
```

```
hostname# firewall vpn add 2 rule "Allow OSPF incoming" src @any dst @local service
@OSPF pass
```



Внимание! Если вы не настроите указанные фильтры, то ViPNet Coordinator HW не сможет работать по протоколу OSPF (см. Общие сведения о протоколе OSPF).

Впоследствии вы можете отказаться от использования протокола OSPF для маршрутизации:

```
hostname# inet ospf mode off
```

Если в подсети прекращено использование протокола OSPF, удалите ее:

```
hostname# inet ospf network delete <IP-адрес назначения> netmask <маска подсети> area
<0-4294967295>
```

Чтобы отключить аутентификацию для области маршрутизации, выполните:

```
hostname# inet ospf area <area> auth off
```

При необходимости удалите пароль или ключ для аутентификации:

- Удаление пароля:

  ```
  inet ospf interface <интерфейс> password remove
  ```

- Удаление одного ключа:

  ```
  inet ospf interface <интерфейс> keys remove <keyid>
  ```

- Удаление всех ключей, добавленных для интерфейса:

  ```
  inet ospf interface <интерфейс> keys remove all
  ```

Настройка перераспределения маршрутов

Одна распределенная сеть может состоять из нескольких автономных систем, в каждой из которых используется своя политика маршрутизации: Static, DHCP или OSPF. Чтобы автономные системы могли обмениваться маршрутами, на маршрутизаторе, расположенном на их границе необходимо настроить перераспределение маршрутов. Вы можете использовать ViPNet Coordinator HW как граничный маршрутизатор, который может перераспределять статические маршруты и маршруты, полученные по DHCP, в протокол OSPF.

Например, чтобы HW-2 HW-3 могли получать маршруты, используемые на R-4 и R-5, настройте перераспределение маршрутов на HW-1.

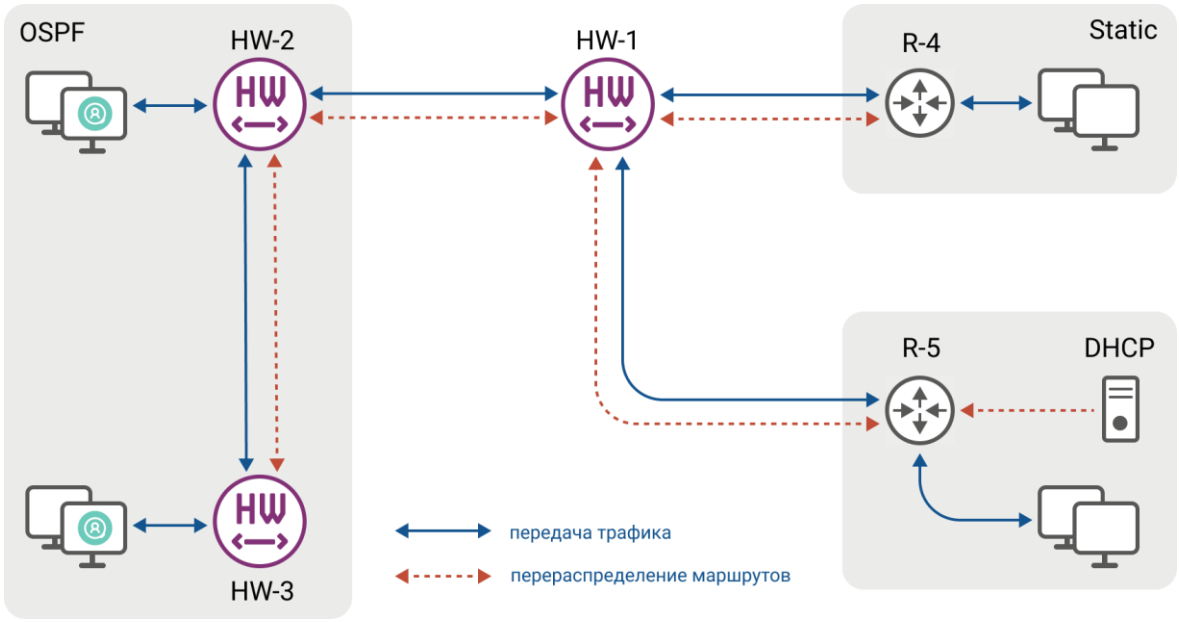


Рисунок 49. Перераспределение маршрутов между автономными системами

Включите перераспределение маршрутов:

```
hostname# inet ospf redistribute add {static | dhcp}
```

указав один из параметров:

- `static` — перераспределять статические маршруты;
- `dhcp` — перераспределять маршруты от DHCP-сервера.

Чтобы выключить перераспределение маршрутов:

```
hostname# inet ospf redistribute delete {static | dhcp}
```

Просмотр настройки перераспределения маршрутов см. разделе Просмотр настроек протокола OSPF.

Просмотр настроек протокола OSPF

Вы можете просмотреть следующие параметры протокола OSPF:

- состояние автоматического запуска протокола OSPF при загрузке ViPNet Coordinator HW: включен или выключен;
- статус использования протокола OSPF: включен или выключен;
- список сетей, в которых ViPNet Coordinator HW выполняет маршрутизацию по протоколу OSPF (IP-адреса, маски и области);
- статус перераспределения маршрутов: доступно или недоступно.

Чтобы посмотреть указанные настройки, выполните команду:

```
hostname> inet ospf show configuration
```

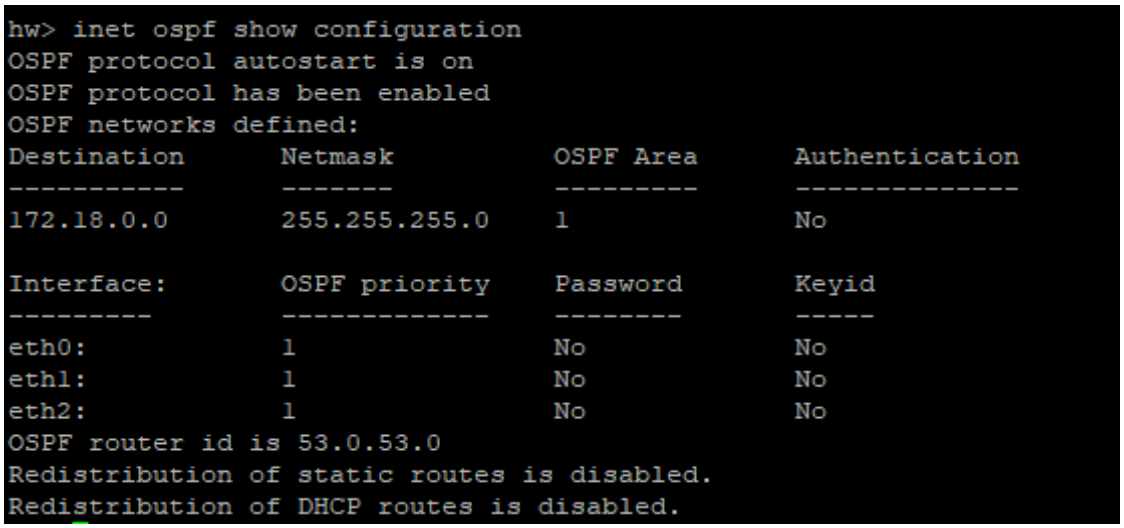


Рисунок 50. Просмотр настроек протокола OSPF

Настройка протокола OSPF в сетях со множественным доступом

ViPNet Coordinator HW выполняет фильтрацию трафика между узлами сегмента локальной сети и внешними сетями. Вы можете сделать сегмент локальной сети частью сети со множественным доступом, входящей в область с маршрутизацией по протоколу OSPF. Когда в сети со множественным доступом становится больше двух маршрутизаторов, необходимо, для сокращения служебного трафика между маршрутизаторами, выбрать среди них назначенный маршрутизатор DR и резервный назначенный маршрутизатор BDR. Выбор роли DR или BDR происходит на основании параметров приоритета `priority` или идентификатора `router-id` маршрутизаторов:

- маршрутизатор с наивысшим значением приоритета становится DR;
- маршрутизатор с наивысшим значением приоритета из оставшихся становится BDR;

- маршрутизатор с приоритетом 0 не может стать DR или BDR;
- если у маршрутизаторов одинаковые приоритеты, то маршрутизатор с наивысшим идентификатором становится DR, а с наивысшим из оставшихся — BDR;
- появление в сети со множественным доступом нового маршрутизатора с более высоким приоритетом, чем у текущего DR, не влияет на роли текущих DR и BDR;
- процедура выбора нового DR или BDR запускается, если текущий DR или BDR выходят из строя.

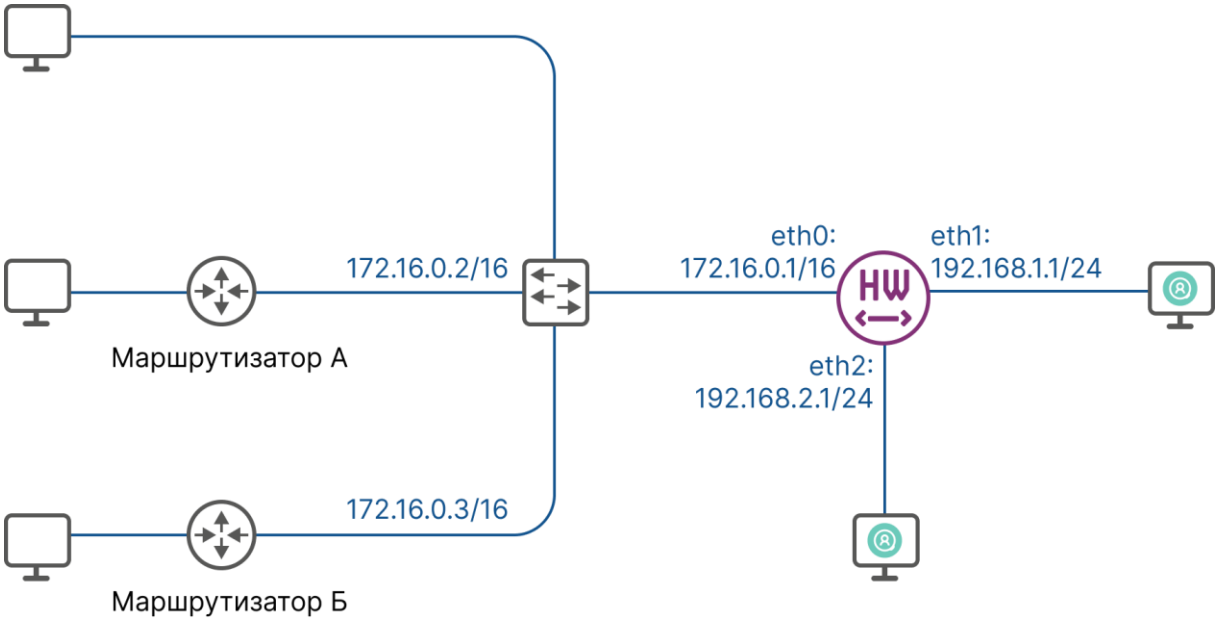


Рисунок 51. ViPNet Coordinator HW в сети со множественным доступом

Приоритет является параметром интерфейса ViPNet Coordinator HW. По умолчанию на всех интерфейсах ViPNet Coordinator HW установлен приоритет — 1. Вы можете изменить значение приоритета интерфейса ViPNet Coordinator HW на целое число из диапазона от 0 до 255:

```
hostname# inet ospf priority <значение приоритета> interface <имя интерфейса>
```

Идентификатор ViPNet Coordinator HW представляет собой число в формате адреса протокола IPv4, которое однозначно идентифицирует ViPNet Coordinator HW в пределах одной автономной области. По умолчанию идентификатор равен максимальному значению IP-адреса из назначенных на интерфейсах ViPNet Coordinator HW. Вы можете изменить значение идентификатора:

```
hostname# inet ospf router-id <адрес IPv4>
```

Внимание! Если в сети со множественным доступом у двух маршрутизаторов будут одинаковые идентификаторы `router-id`, то такие маршрутизаторы не смогут установить отношения соседства.

Чтобы посмотреть текущие значения параметров `priority` и `router-id` ViPNet Coordinator HW:

```
hostname# inet ospf show configuration
```

Просмотр состояния каналов связи между маршрутизаторами

Кроме настроек протокола OSPF вы также можете просмотреть информацию о состоянии каналов связи между всеми маршрутизаторами, работающими по протоколу OSPF. Она содержится в базе данных (link state database) (см. Общие сведения о протоколе OSPF) и синхронизируется на всех OSPF-маршрутизаторах. Именно на ее основе вычисляются динамические маршруты протокола OSPF. Для просмотра информации базы данных состояний каналов связи:

```
hostname> inet ospf show database
```

```
hw> inet ospf show database


              OSPF Router with ID (53.0.53.0)
            Router Link States Area (0.0.0.1)
Link ID         | ADV Router      |     Age    |    Seq#    |   CkSum  | Link count
4.4.4.4         | 4.4.4.4         |     777    | 0x8000000b |  0x1f79  | 1
53.0.53.0       | 53.0.53.0       |     334    | 0x80000009 |  0xd317  | 1

            Net Link States Area (0.0.0.1)
Link ID         | ADV Router      |     Age    |    Seq#    |   CkSum  | Link count
172.18.0.4      | 4.4.4.4         |     737    | 0x80000007 |  0x53b3  | 1

            AS External Link States
Link ID         | ADV Router      |     Age    |    Seq#    |   CkSum  | Route
10.4.0.0        | 4.4.4.4         |    1147    | 0x80000007 |  0x7426  | E2 10.4.0.0/24 [0x0]
10.53.0.0       | 4.4.4.4         |    1117    | 0x80000007 |  0x2643  | E2 10.53.0.0/16 [0x0]
10.55.8.0       | 4.4.4.4         |    1157    | 0x80000007 |  0xb826  | E2 10.55.8.0/25 [0x0]
10.55.9.168     | 4.4.4.4         |    1177    | 0x80000007 |  0xe9d2  | E2 10.55.9.168/29 [0x0]
10.55.9.185     | 4.4.4.4         |    1177    | 0x80000007 |  0x693b  | E2 10.55.9.185/32 [0x0]
```

Рисунок 52. Просмотр базы данных состояний каналов связи

Просмотр информации о соседних маршрутизаторах

В составлении маршрутов по протоколу OSPF участвуют все OSPF-маршрутизаторы, находящиеся в области маршрутизации ViPNet Coordinator HW. При необходимости вы можете просмотреть сведения об OSPF-маршрутизаторах, которые являются соседними для ViPNet Coordinator HW:

```
hostname> inet ospf show neighbour
```

В результате выполнения команды отобразится информация обо всех соседних OSPF-маршрутизаторах:

```
hw> inet ospf show neighbour
 Neighbor ID    |  Pri  | State       | Dead Time | Address       | Interface        | RXmtL | RqstL | DBsmL
 4.4.4.4        |   1   | Full/DR     | 38.722s   | 172.18.0.4    | eth0:172.18.0.1  |   0   |   0   |   0
```

Рисунок 53. Просмотр информации о соседних OSPF-маршрутизаторах

По каждому маршрутизатору отображается следующая информация:

- уникальный идентификатор OSPF-маршрутизатора, под которым он известен другим маршрутизаторам при работе по протоколу OSPF;
- приоритет маршрутизатора;
- тип маршрутизатора (см. Общие сведения о протоколе OSPF) (в случае, приведенном на рисунке, маршрутизатор-сосед является назначенным, на что указывает значение `DR` в поле `State`);
- интервал простоя маршрутизатора, по истечении которого он будет считаться неактивным (выключенным);
- IP-адрес маршрутизатора, по которому он доступен для обмена информацией по протоколу OSPF;
- IP-адрес активного сетевого интерфейса маршрутизатора;
- другие параметры.

Просмотр маршрутов, сформированных по протоколу OSPF

Чтобы просмотреть список динамических маршрутов, сформированных по протоколу OSPF:

```
hostname> inet show routing ospf
```

В результате отобразятся списки маршрутов в трёх разделах:

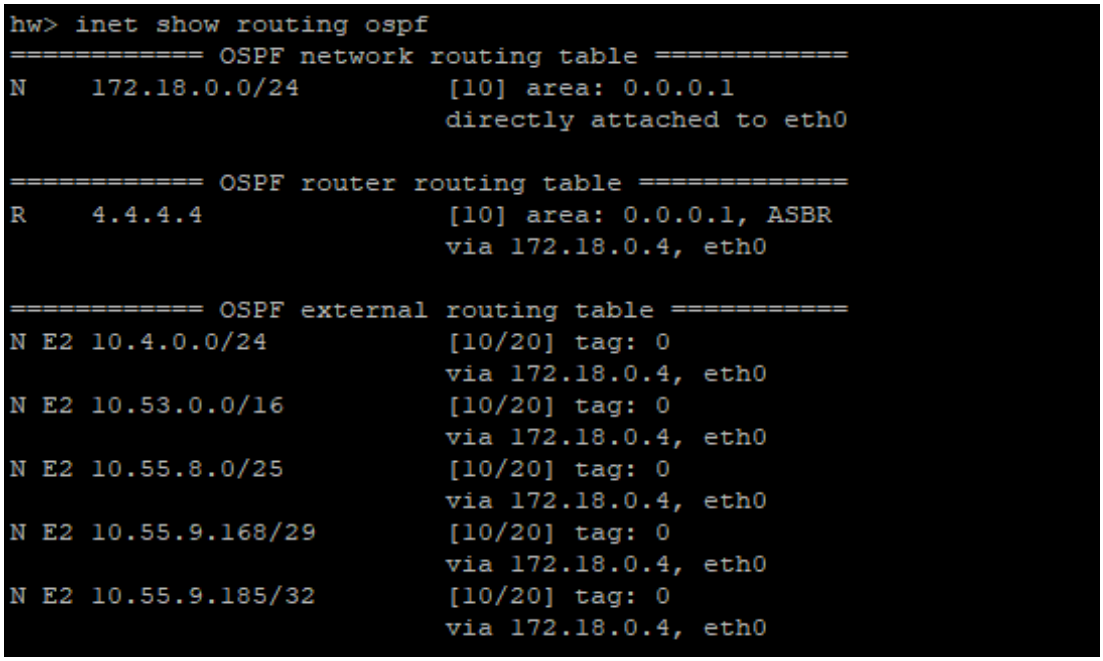


Рисунок 54. Просмотр маршрутов протокола OSPF

В каждом из разделов отображаются следующие маршруты:

- `OSPF network routing table` — маршруты, которые были сформированы по OSPF-протоколу в той области маршрутизации, к которой подключен ViPNet Coordinator HW. Если ViPNet Coordinator HW является межобластным маршрутизатором (ABR) (см. Общие сведения о протоколе OSPF), то в этом разделе будут присутствовать маршруты из всех областей, которые он объединяет.
- `OSPF router routing table` — маршруты до соседних OSPF-маршрутизаторов, которые находятся в области маршрутизации ViPNet Coordinator HW и выполняют перераспределение маршрутов (см. Настройка перераспределения маршрутов).
- `OSPF external routing table` — маршруты в другие автономные системы, поступившие при перераспределении от соседних OSPF-маршрутизаторов.

Настройка маршрутизации по протоколу OSPF между удаленными сегментами сети

Для маршрутизации по протоколу OSPF между удаленными сегментами сети необходимо, чтобы OSPF поддерживался на всем пути следования IP-пакетов. В сетях общего пользования это условие не выполняется. Объединив удаленные сегменты по L2OverIP вы сможете настроить маршрутизацию по протоколу OSPF между ними:

1 Настройте L2OverIP на HW-1 и HW-2 (см. Настройка L2OverIP).

2 Настройте OSPF на HW-3 и HW-4 (см. Настройка OSPF).

> **Примечание.** На HW-1 и HW-2 настройка OSPF не требуется, поскольку они не участвуют в маршрутизации IP-трафика.

3 На R-1 и R-2 настройте OSPF в соответствии с руководством на эти маршрутизаторы.

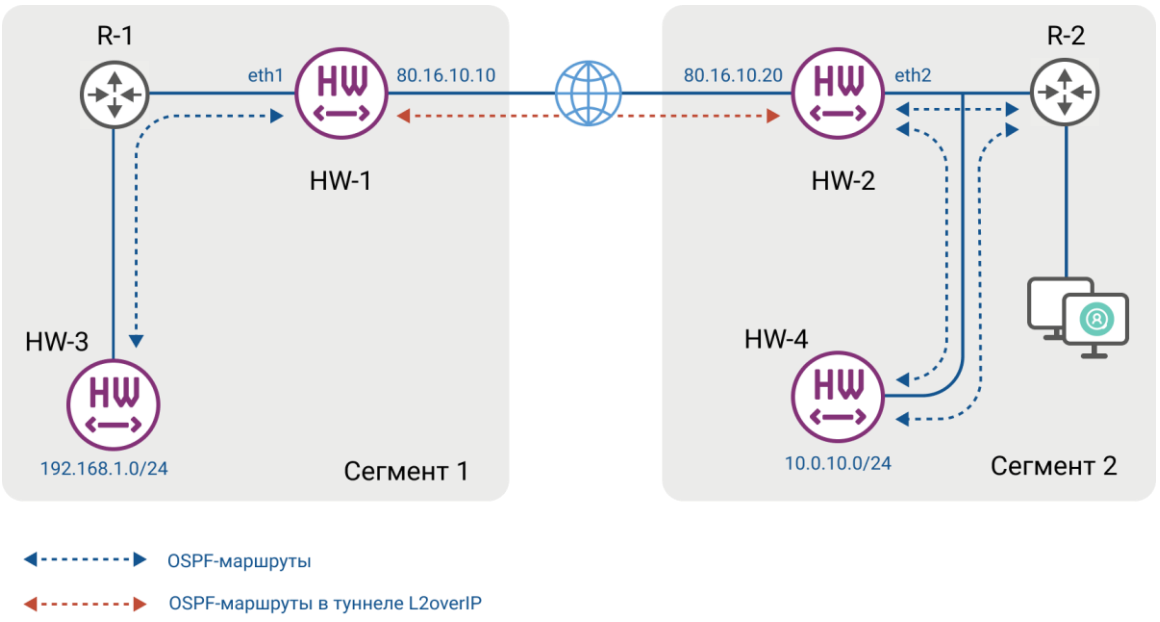


Рисунок 55. OSPF-маршруты между удаленными сегментами сети

Настройка L2OverIP

1 Укажите сетевой интерфейс, сегмент сети которого будет объединяться с другим сегментом по L2OverIP:

- HW-1:

```
hostname# iplir set l2overip interface eth1
```

- HW-2:

```
hostname# iplir set l2overip interface eth2
```

Если сегментов больше двух, аналогичным образом укажите рабочий интерфейс на остальных ViPNet Coordinator HW.

2 Задайте параметры локального сегмента сети, указав уникальный номер порта и адрес внешнего интерфейса:

- HW-1:

```
hostname# iplir set l2overip local-port 1 82.16.10.10
```

- HW-2:

```
hostname# iplir set l2overip local-port 2 82.16.10.20
```

3 Задайте параметры удаленного сегмента сети — номер порта сегмента и IP-адрес видимости внешнего интерфейса (local-port) удаленного HW:

- HW-1:

```
hostname# iplir set l2overip remote-port 2 82.16.10.20
```

- HW-2:

```
hostname# iplir set l2overip remote-port 1 82.16.10.10
```

В зависимости от настройки видимости удаленного HW укажите его реальный или виртуальный IP-адрес. Если ViPNet Coordinator HW имеет более одного адреса видимости для удаленного ViPNet Coordinator HW (секция `[id]` конфигурационного файла iplir.conf, соответствующая удаленному координатору, содержит более одного параметра `ip`), настройте видимость удаленного ViPNet Coordinator HW по реальным адресам и укажите его реальный IP-адрес.

4 На каждом из HW:

4.1 Добавьте сетевые фильтры защищенной сети, разрешающие любые соединения по протоколу 97:

```
hostname# firewall vpn add src @local dst @any proto 97 pass
hostname# firewall vpn add src @any dst @local proto 97 pass
```

4.2 Включите L2OverIP:

```
hostname# iplir set l2overip mode switch
```

4.3 Убедитесь в корректности выполненных настроек L2OverIP:

```
hostname# iplir show l2overip config
```

Настройка OSPF

1 На каждом из HW включите OSPF:

```
hostname# inet ospf mode on
```

2 Укажите сеть, в которой осуществляется обмен маршрутами:

- HW-3:

```
hostname# inet ospf network add 192.168.1.0 netmask 255.255.255.0 area 1
```

- HW-4:

```
hostname# inet ospf network add 10.0.10.0 netmask 255.255.255.0 area 1
```



Примечание. HW-3 и HW-4 принадлежат одной области маршрутизации.

3 На каждом из HW создайте сетевые фильтры открытой сети:

3.1 Фильтры, разрешающие входящий однонаправленный IP-трафик (unicast) и многоадресный IP-трафик (multicast) по протоколу OSPF от соседних OSPF-маршрутизаторов, с которыми взаимодействует HW:

- Если политика безопасности вашей организации не запрещает прохождение служебного IP-трафика по протоколу OSPF (IP:89) от любого узла, то создайте фильтры:

```
hostname# firewall local add 1 rule "Rule 1" src @any dst @local service @OSPF pass
```

```
hostname# firewall local add 2 rule "Rule 2" src @any dst @multicast service @OSPF pass
```

- Если запрещено создание фильтров, пропускающих служебный IP-трафик по протоколу OSPF от любых узлов, создайте аналогичные фильтры для каждого OSPF-маршрутизатора, который является соседним для HW.

Таблица 12. Фильтры для входящего OSPF-трафика на HW-3, HW-4

Координатор	Название	Источник	Назначение	Протокол	Действие
HW-3	Rule 1	<IP-адрес R-1>	@local	IP:89	pass
	Rule 2	<IP-адрес R-1>	@multicast	IP:89	pass
HW-4	Rule 1	<IP-адрес R-1>	@local	IP:89	pass
	Rule 2	<IP-адрес R-1>	@multicast	IP:89	pass
	Rule 3	<IP-адрес R-2>	@local	IP:89	pass
	Rule 4	<IP-адрес R-2>	@multicast	IP:89	pass

3.2 Фильтр, разрешающий исходящий IP-трафик HW по протоколу OSPF на любой IP-адрес назначения:

```
hostname# firewall local add 1 rule "Rule 1" src @local dst @any service @OSPF pass
```

Настройка BGP

Общие сведения о протоколе BGP

BGP (Border Gateway Protocol) — протокол динамической маршрутизации, предназначенный для обмена маршрутами между автономными системами (AS). AS — это совокупность IP-сетей и маршрутизаторов, управляемых одним или несколькими операторами, имеющими единую политику маршрутизации с интернетом.

Маршрутизатор ViPNet Coordinator HW поддерживает протокол BGP для обмена маршрутами с соседними маршрутизаторами, а также для передачи параметров, позволяющих выбрать лучшие маршруты.

Таблица 13. Порядок выбора лучшего маршрута

№	Параметр маршрута	Критерий выбора	Анонсирование
1	Вес (`weight`)	Выбирается маршрут с наибольшим весом	Нет
2	Значение `local preference`	Выбирается маршрут с наибольшим значением	Только внутри AS
3	Локальный или внешний	Локальные маршруты имеют приоритет	Нет
4	Длина (`AS-path`)	Выбирается маршрут наименьшей длины	Да
5	Происхождение (`Origin`)	Маршруты, полученные через IGP имеют приоритет	Да
6	Значение `MED`	Выбирается маршрут с наименьшим `MED`	Только внутри AS и в соседнюю AS
7	eBGP или iBGP	Маршруты eBGP имеют приоритет	Нет
8	Значение `Router ID`	Выбирается маршрут с наименьшим `Router ID`	Нет
9	Адрес соседа	Выбирается маршрут с наименьшим адресом	Нет

Настройка соседей

1 Включите BGP:

```
hostname# inet bgp on
```

2 Задайте номер AS:

```
hostname# inet bgp router as <as-number>
```

где `<as-number>` — номер вашей AS (целое число из диапазона 1–4294967295).

3 Чтобы изменить идентификатор маршрутизатора `Router ID`, заданный автоматически:

```
hostname# inet bgp router id <a.b.c.d>
```

где: `<a.b.c.d>` — идентификатор маршрутизатора в формате A.B.C.D (может принимать значения от 0.0.0.1 до 255.255.255.255);

4 Настройте соседей:

4.1 Чтобы добавить соседа:

`hostname# inet bgp neighbor add <IP-address> remote-as <as-number> [port <portnumber>]`, где:

- `<IP-address>` — IP-адрес соседа;
- `<as-number>` — номер AS соседа (целое число из диапазона 1–4294967295);
- `<portnumber>` — номер TCP-порта соседа для установления BGP-сессии. По умолчанию используется порт 179.

4.2 Чтобы изменить TCP-порт соседа:

`hostname# inet bgp neighbor <IP-address> set port <portnumber>`, где:

- `<IP-address>` — IP-адрес выбранного соседа;
- `<portnumber>` — порт для установления BGP-сессии.

4.3 Чтобы настроить TTL одним из способов для соседа:

- Включите или выключите TTL-Security:

  `hostname# inet bgp neighbor <IP-address> set ttl-security {<hops>|off}`, где:

  - `<IP-address>` — IP-адрес соседа;
  - `<hops>` — максимальное число переходов до соседа;
  - `off` — отключить TTL-Security.

- Включите или выключите eBGP-multihop:

  `hostname# inet bgp neighbor <IP-address> set ebgp-multihop {<ttl>|off}`, где:

  - `<IP-address>` — IP-адрес соседа;
  - `<ttl>` — значение TTL для исходящих пакетов BGP-сессии;
  - `off` — отключить eBGP-multihop.

4.4 Чтобы настроить MD5-аутентификацию с соседом, включите её и задайте пароль. (такой же пароль установите на соседе):

```
hostname# inet bgp neighbor <IP-address> set password
```

где `<IP-address>` — IP-адрес соседа.

4.5 Чтобы удалить соседа:

```
hostname# inet bgp neighbor <IP-address> delete
```

где `<IP-address>` — IP-адрес соседа.

5 Чтобы вывести список соседей и параметров доступа к ним:

```
hostname# inet bgp show neighbors list
```

6 Чтобы вывести список всех BGP-сессий:

```
hostname# inet bgp show summary
```

7 Чтобы перезапустить BGP-сессии с выбранным соседом или всеми соседями:

`hostname# inet bgp clear {all | <IP-address>}`, где:

- `<IP-address>` — IP-адрес соседа, BGP-сессия с которым будет перезапущена;
- `all` — перезапустить BGP-сессии со всеми соседями.

8 Чтобы сбросить настройки BGP:

```
hostname# inet bgp router reset
```

9 Чтобы выключить BGP:

```
hostname# inet bgp off
```

Анонсирование подсетей и перераспределение маршрутов

Настроенный по умолчанию маршрутизатор ViPNet Coordinator HW не распространяет информацию об известных ему подсетях и маршрутах. При этом он может получать ее от соседей и пересылать дальше, не передавая информацию о собственных подсетях. Чтобы передавать ее, настройте:

- Прямое анонсирование подсетей из заданного списка.
- Перераспределение маршрутов, полученных от соседей. Вы можете использовать карты маршрутов (route maps) для фильтрации и модификации распространяемых маршрутов.

Для маршрута по умолчанию также можно использовать механизм анонсирования default-originate. При этом:

- анонсирование настраивается для выбранного соседа;
- маршрут по умолчанию не попадает в BGP-таблицу;
- не требуется наличие статического маршрута в таблице маршрутизации.

Чтобы настроить анонсирование подсетей и перераспределение маршрутов:

1 Добавьте анонсируемые подсети. Для каждой подсети, которую вы хотите анонсировать, выполните:

`hostname# inet bgp network add <subnet> netmask <netmask>`, где:

- `<subnet>` — адрес IPv4 unicast-подсети, число в виде 4 октетов в формате A.B.C.D;

- `<netmask>` — маска подсети, число в виде 4 октетов в формате W.X.Y.Z.

2 Чтобы удалить подсеть из списка анонсируемых:

`hostname# inet bgp network delete <subnet> netmask <netmask>`, где:

- `<subnet>` — IP-адрес удаляемой подсети;
- `<netmask>` — маска удаляемой подсети.

3 Чтобы включить перераспределение статических или подключенных маршрутов:

`hostname# inet bgp network redistribute {connected | static} on`, где:

- `connected` — перераспределять подключенные маршруты;
- `static` — перераспределять статические маршруты.

4 Чтобы назначить карту маршрутов для фильтрации или модификации распространяемых маршрутов:

`hostname# inet bgp network redistribute {connected | static} route-map name <name>`, где:

- `connected` — применять карту к подключенным маршрутам;
- `static` — применять карту к статическим маршрутам;
- `name` — имя карты маршрутов.



Примечание. Вы можете назначить карту маршрутов только маршрутам, для которых было включено перераспределение на шаге 3.

5 Включите анонсирование маршрута по умолчанию. Для каждого соседа, которому вы хотите анонсировать маршрут, выполните:

`hostname# inet bgp neighbour <IP-адрес> set default-originate on`

где `<IP-адрес>` — IP-адрес соседа;

6 Чтобы просмотреть настройки анонсирования подсетей и перераспределения маршрутов:

`hostname# inet bgp show network`

Настройка фильтров и префикс-листов маршрутов

По умолчанию ViPNet Coordinator HW принимает все маршруты от своих соседей и распространяет им свои маршруты, признанные лучшими. Для фильтрации входящих и исходящих маршрутов используются:

- Префикс-листы — фильтрация маршрутов выполняется с учетом их назначения. Префикс-лист — это нумерованный список правил, которыми проверяется маршрут в порядке увеличения их номеров (до первого совпадения). При соответствии маршрута правилу к нему применяется заданное действие и дальнейшая проверка маршрута прекращается. При создании правил в

префикс-листах вы можете настроить проверку на точное совпадение с префиксом, либо проверку попадания в диапазон, определяемый длиной префикса.

- AS-path-фильтры — маршруты фильтруются с учетом порядка прохождения маршрута через автономные системы. AS-path-фильтр — это нумерованный список регулярных выражений, которыми проверяется параметр AS-path. Если AS-path в маршруте удовлетворяет условиям регулярного выражения из списка, то к маршруту применяется действие, заданное в фильтре.

Настройка префикс-листов

Чтобы создать и настроить префикс-лист:

1 Добавьте новый префикс-лист:

```
hostname# inet prefix-list add <name>
```

где `<name>` — имя префикс-листа.

2 Настройте правила для созданного префикс-листа:

2.1 Чтобы добавить правило в префикс-лист:

`hostname# inet prefix-list <name> [seq <num>] {permit | deny} {<subnet> [le <len>] [ge <len>] | any}`, где:

- `<name>` — имя префикс-листа;
- `<num>` — порядковый номер правила в префикс-листе;
- `permit` — разрешает маршрут при соответствии префикса подсети маршрута правилу;
- `deny` — блокирует маршрут при соответствии префикса подсети маршрута правилу;
- `<subnet>` — префикс unicast-подсети в формате CIDR;
  - `le` — задает условие «меньше или равно» при проверке префикса;
  - `ge` — задает условие «больше или равно» при проверке префикса;
  - `<len>` — длина префикса; целое число от 0 до 32;
  - `any` — любой префикс, эквивалент 0.0.0.0 le 32.

2.2 Чтобы удалить правило из префикс-листа:

`hostname# inet prefix-list <name> clear seq <num>`, где:

- `<name>` — имя префикс-листа;
- `<num>` — порядковый номер правила в префикс-листе.

3 Чтобы удалить префикс-лист:

```
hostname# inet prefix-list delete <name>
```

где `<name>` — имя префикс-листа.

4 Назначьте префикс-листы выбранным соседям:

4.1 Чтобы назначить префикс-лист выбранному соседу:

`hostname# inet bgp neighbor <ip-address> set prefix-list <name> {in | out}`, где:

- `<ip-address>` — IP-адрес соседа;

- `<name>` — имя префикс-листа;
- `in` — префикс-лист будет применяться к входящим маршрутам;
- `out` — префикс-лист будет применяться к исходящим маршрутам.

4.2 Чтобы отключить использование префикс-листа для выбранного соседа:

`hostname# inet bgp neighbor <ip-address> remove prefix-list {in | out}`, где:

- `<ip-address>` — IP-адрес соседа;
- `in` — отключить использование префикс-листа к входящим маршрутам;
- `out` — отключить использование префикс-листа к исходящим маршрутам.

Настройка AS-path-фильтров

Чтобы создать и настроить AS-path-фильтры:

1 Добавьте новый AS-path-фильтр:

`hostname# inet bgp as-path-filter add <name>`

где `<name>` — имя AS-path-фильтра.

2 Настройте для созданного AS-path-фильтра списки регулярных выражений:

2.1 Чтобы добавить регулярное выражение в AS-path-фильтр:

`hostname# inet bgp as-path-filter <name> [seq <num>] {permit | deny}`, где:

- `<name>` — имя AS-path-фильтра;
- `<num>` — порядковый номер регулярного выражения в фильтре;
- `permit` — разрешает маршрут при удовлетворении значения AS-path условиям регулярного выражения;
- `deny` — блокирует маршрут при удовлетворении значения AS-path условиям регулярного выражения.

2.2 Чтобы удалить регулярное выражение из AS-path-фильтра:

`hostname# inet bgp as-path-filter <name> clear seq <num>`, где:

- `<name>` — имя AS-path-фильтра;
- `<num>` — порядковый номер регулярного выражения в фильтре.

3 Чтобы удалить AS-path-фильтр:

`hostname# inet bgp as-path-filter delete <name>`

где `<name>` — имя AS-path-фильтра.

4 Назначьте AS-path-фильтры выбранным соседям:

4.1 Чтобы назначить AS-path-фильтр выбранному соседу:

`hostname# inet bgp neighbor <ip-address> set as-path-filter <name> {in | out}`, где:

- `<ip-address>` — IP-адрес соседа;

- `<name>` — имя AS-path-фильтра;
- `in` — фильтр будет применяться к входящим маршрутам;
- `out` — фильтр будет применяться к исходящим маршрутам.

4.2 Чтобы отключить использование AS-path-фильтра для выбранного соседа:

`hostname# inet bgp neighbor <ip-address> remove as-path-filter {in | out}`, где:

- `<ip-address>` — IP-адрес соседа;
- `in` — отключить использование фильтра к входящим маршрутам;
- `out` — отключить использование фильтра к исходящим маршрутам.

Просмотр информации о префикс-листах и AS-path-фильтрах

- Чтобы вывести список префикс-листов или содержимое выбранного префикс-листа:

  `hostname# inet prefix-list show [<name>]`

  где `<name>` — имя префикс-листа. Если параметр `<name>` не задан, то выведется список всех префикс-листов.

- Чтобы вывести список AS-path-фильтров или содержимое выбранного фильтра:

  `hostname# inet bgp show as-path-filter [<name>]`

  где `<name>` — имя AS-Path-фильтра. Если параметр `<name>` не задан, то выведется список всех AS-path-фильтров.

- Чтобы вывести назначенные на соседей префикс-листы, фильтры и карты маршрутов:

  `hostname# inet bgp show neighbors filters [<ip-address>]`

  где `<ip-address>` — IP-адрес соседа. Если параметр `<ip-address>` не задан, то будет выведен список всех соседей.

Настройка карт маршрутов

ViPNet Coordinator HW поддерживает карты маршрутов (route maps) — наборы правил, позволяющие фильтровать принимаемые или передаваемые маршруты, а также изменять их атрибуты. Вы можете создавать карты маршрутов и использовать их при настройке перераспределения маршрутов.

С помощью карт маршрутов вы можете настраивать следующие параметры передаваемых маршрутов:

- значение `next-hop`
- вес маршрута (`weight`);
- метрика маршрута (`MED`);
- значение `local preference`;
- `AS-path`;

- комьюнити (`community`).

Принципы обработки карт маршрутов

Карты маршрутов состоят из блоков (последовательности правил), которые определяют порядок обработки маршрута и проверяются до первого совпадения. Маршруты, которые не прошли карту маршрутов, отбрасываются. При описании блоков используются следующие условия проверки:

- Действие — определяет действие с маршрутом, соответствующим условиям блока: разрешить (`permit`) либо блокировать (`deny`).
- `Match` — условие совпадения маршрутов. Если в блоке задано нескольких условий, то действие будет применено к маршруту при совпадении хотя бы одного из условий.
- `Set` — изменение параметров маршрута. В разрешающем блоке определяет, как изменятся параметры маршрута при его соответствии блоку.
- `On-match` — указывает о необходимости перехода в другой блок карты маршрутов.

Настройка комьюнити-листов

Параметр `community` — это 32-битное целое число, используемое для маркировки маршрутной информации. Маршруту можно сопоставить несколько `community`, на основе которых можно задавать правила фильтрации, балансировки трафика и распределения нагрузки.

Комьюнити-лист (community list) — это последовательности разрешенных или запрещенных `community`. Если в одной последовательности содержится несколько `community`, то действие блока будет применено к маршрутам, содержащим все `community`. ViPNet Coordinator HW поддерживает следующие зарезервированные (well-known) комьюнити:

Таблица 14. Перечень поддерживаемых well-known комьюнити

Название	hex-обозначение	Обозначение ASN:NN	Источник
internet	0x00000000	0:0	Cisco
graceful-shutdown	0xFFFF0000	65535:0	RFC-8326
accept-own	0xFFFF0001	65535:1	RFC-7611
llgr-stale	0xFFFF0006	65535:6	draft-uttaro-idr-bgp-persistence-04
no-llgr	0xFFFF0007	65535:7	draft-uttaro-idr-bgp-persistence-04
blackhole	0xFFFF029A	65535:666	RFC-7999
no-export	0xFFFFFF01	65535:65281	RFC-1997
no-advertise	0xFFFFFF02	65535:65282	RFC-1997
local-AS	0xFFFFFF03	65535:65283	RFC-1997
no-peer	0xFFFFFF04	65535:65284	RFC-3765

Чтобы создать и настроить комьюнити-лист:

1 Создайте комьюнити-лист:

```
hostname# inet bgp community-list add <name>
```

где `<name>` — имя комьюнити-листа.

2 Добавьте в него правила:

```
hostname# inet bgp community-list <name> [seq <num>] {permit|deny} <community-line>,
```

где:

- `<name>` — имя комьюнити-листа;
- `<num>` — указывает точный номер правила в списке;
- `permit` — устанавливает проверку совпадения комьюнити;
- `deny` — устанавливает проверку отсутствия комьюнити;
- `<community-line>` — строка текста от 3 до 256 символов, которая может содержать:
  - одно или более комьюнити в формате AA:NN, разделенные пробелом (строка не может начинаться с пробела);
  - одно или более well-known комьюнити: internet, no-export, no-advertise, local-AS.

3 Чтобы впоследствии удалить добавленное правило:

```
hostname# inet bgp community-list <name> clear seq <num>
```

, где:

- `<name>` — имя комьюнити-листа;
- `<num>` — номер правила.

4 Чтобы вывести перечень комьюнити-листов:

```
hostname# inet bgp show community-list
```

5 Чтобы вывести правила, входящие в комьюнити-лист:

```
hostname# inet bgp show community-list <name>
```

где `<name>` — имя комьюнити-листа.

6 Чтобы удалить комьюнити-лист:

```
hostname# inet bgp community-list delete <name>
```

где `<name>` — имя комьюнити-листа.

Настройка карт маршрутов

Чтобы создать и настроить карту маршрутов:

1 Создайте карту маршрутов:

```
hostname# inet route-map add <name>
```

где `<name>` — имя карты.

2 Добавьте в карту маршрутов блоки правил и настройте их:

2.1 Чтобы добавить блок правил:

```
hostname# inet route-map <name> {permit|deny} <seq>
```

, где:

- `<name>` — имя карты маршрутов;
- `permit` — устанавливает для блока действие «разрешить»;
- `deny` — устанавливает для блока действие «запретить»;
- `<seq>` — номер блока в карте маршрутов.

2.2 Чтобы удалить блок:

`hostname# inet route-map <name> clear <seq>`, где:

- `<name>` — имя карты маршрутов;
- `<seq>` — номер блока в карте маршрутов.

2.3 Чтобы добавить в блок проверку совпадения с выбранным префикс-листом:

`hostname# inet route-map <name> <seq> match prefix-list <prefix-list-name>`, где:

- `<name>` — имя карты маршрутов;
- `<seq>` — номер блока в карте маршрутов;
- `<prefix-list-name>` — имя префикс-листа.

2.4 Чтобы добавить в блок проверку совпадения с выбранным AS-path-фильтром:

`hostname# inet route-map <name> <seq> match as-path <as-path-filter-name>`, где:

- `<name>` — имя карты маршрутов;
- `<seq>` — номер блока в карте маршрутов;
- `<as-path-filter-name>` — имя AS-path-фильтра.

2.5 Чтобы добавить в блок проверку совпадения с выбранным комьюнити-листом:

`hostname# inet route-map <name> <seq> match community <community-list-name> [exact-match]`, где:

- `<name>` — имя карты маршрутов;
- `<seq>` — номер блока в карте маршрутов;
- `<community-list-name>` — имя комьюнити-листа;
- `exact-match` — задает необходимость точного совпадения комьюнити в маршруте и комьюнити-листе.

2.6 Чтобы задать изменение параметра `next-hop` в маршруте:

`hostname# inet route-map <name> <seq> set next-hop <IP-address>`, где:

- `<name>` — имя карты маршрутов;
- `<seq>` — номер блока в карте маршрутов;
- `<IP-address>` — новое значение параметра `next-hop`.

2.7 Чтобы задать изменение веса маршрута:

`hostname# inet route-map <name> <seq> set weight <weight>`, где:

- `<name>` — имя карты маршрутов;

- <seq> — номер блока в карте маршрутов;
- <weight> — вес маршрута.

2.8 Чтобы задать изменение параметра MED:

hostname# inet route-map <name> <seq> set metric <metric>, где:

- <name> — имя карты маршрутов;
- <seq> — номер блока в карте маршрутов;
- <metric> — новое значение параметра MED.

2.9 Чтобы задать изменение параметра local-preference:

hostname# inet route-map <name> <seq> set local-preference <local-preference>, где:

- <name> — имя карты маршрутов;
- <seq> — номер блока в карте маршрутов;
- <local-preference> — новое значение параметра local-preference.

2.10 Чтобы задать для выбранного блока дополнение параметра AS-path:

hostname# inet route-map <name> <seq> set as-path-prepend <string>, где:

- <name> — имя карты маршрутов;
- <seq> — номер блока в карте маршрутов;
- <string> — строка, содержащая номера AS, разделенные пробелом.

2.11 Чтобы задать для выбранного блока обновление списка комьюнити в маршруте:

hostname# inet route-map <name> <seq> set community {[additive] <community-line>| none}, где:

- <name> — имя карты маршрутов;
- <seq> — номер блока в карте маршрутов;
- <community-line> — строка, содержащая номера комьюнити, разделенные пробелом. Может содержать одно или несколько комьюнити в формате AA:NN, а также well-known комьюнити: internet, no-export, no-advertise, local-AS;
- [additive] — задает необходимость дополнения существующего списка комьюнити строкой <community-line>;
- none — удалить все комьюнити из маршрута.

2.12 Чтобы задать директиву перехода к другому блоку при совпадении условий:

hostname# inet route-map <name> <seq> on-match {next|goto <number>}, где:

- <name> — имя карты маршрутов;
- <seq> — номер блока в карте маршрутов;
- <number> — номер блока в карте маршрутов, к которому нужно перейти при совпадении условий;

- `<next>` — перейти к следующему блоку при совпадении условий.

3 Чтобы удалить существующую карту маршрутов:

```
hostname# inet route-map delete <name>
```

где `<name>` — имя карты маршрутов.

4 Чтобы вывести список карт маршрутов, или данные об использовании выбранной карты маршрутов:

`hostname# inet route-map show [<name> [usage]]`, где:

- `<name>` — имя карты маршрутов;
- `usage` — вывести перечень объектов, в которых используется карта маршрутов.

5 Чтобы назначить карту маршрутов для обработки маршрутной информации, распространяемой между ViPNet Coordinator HW и выбранным соседом:

`hostname# inet bgp neighbor <ip-address> set route-map <name> {in|out}`, где:

- `<ip-address>` — IP-адрес соседа;
- `<name>` — имя карты маршрутов;
- `in` — применять карту маршрутов к входящим маршрутам;
- `out` — применять карту маршрутов к исходящим маршрутам.

6 Чтобы отключить использование карты маршрутов для обработки маршрутной информации, распространяемой между ViPNet Coordinator HW и выбранным соседом:

`hostname# inet bgp neighbor <ip-address> remove route-map {in|out}`, где:

- `<ip-address>` — IP-адрес соседа;
- `in` — отключить использование карты маршрутов для входящих маршрутов;
- `out` — отключить использование карты маршрутов для исходящих маршрутов.

Настройка распространения маршрутов внутри AS

Взаимодействие соседей внутри одной AS (iBGP-соседей) отличается от взаимодействия соседей из разных AS (eBGP-соседей) и имеет особенности:

- Параметры маршрутов (в том числе `next-hop`) не изменяются.
- Если маршрут получен от iBGP-соседа, то он может передаваться только eBGP-соседу.

В некоторых топологиях автономных систем эти особенности препятствуют распространению маршрутов внутри одной AS, а также прохождению трафика через транзитную AS. Чтобы обеспечить распространение маршрутов внутри автономной системы, используются следующие механизмы:

- Возможность модифицировать параметр `next-hop` для iBGP-соседей без использования карт маршрутов. Это обеспечивается включением опции `next-hop-self` и назначается для iBGP-соседей в соответствии с настройками соседства.
- Изменение логики работы ViPNet Coordinator HW с iBGP-соседями таким образом, что им передаются маршруты, полученные от других iBGP-соседей. Такой механизм называется отражение маршрутов (Route Reflection), при этом ViPNet Coordinator HW выступает в роли RR-сервера, распространяющего маршруты, а его iBGP-соседи — в роли RR-клиентов. Сервер и его клиенты образуют RR-кластер, обладающий уникальным идентификатором (Cluster ID). AS, в которой используется отражение маршрутов, может состоять из нескольких RR-кластеров, обладающих различными правилами обработки маршрутной информации.

Настройка next-hop-self

Чтобы включить возможность модификации параметра `next-hop` для iBGP-соседа:

```
hostname# inet bgp neighbor <IP-адрес> set next-hop-self on
```

где `<IP-адрес>` — IP-адрес iBGP-соседа.

Настройка Route Reflection

Чтобы настроить отражение маршрутов:

1. Задайте идентификатор RR-кластера `Cluster ID`:

   `hostname# inet bgp route-reflector cluster-id {<a.b.c.d>|auto}`, где:

   - `<a.b.c.d>` — идентификатор RR-кластера, число в виде 4 октетов в формате A.B.C.D;
   - `auto` — идентификатор RR-кластера будет назначен автоматически.

2. Добавьте iBGP-соседей в список клиентов Route Reflection:

   - Чтобы добавить IP-адрес iBGP-соседа в список клиентов:

     ```
     hostname# inet bgp route-reflector client add <IP-address>
     ```

     где `<IP-address>` — IP-адрес iBGP-соседа.

   - Чтобы удалить адрес iBGP-соседа из списка клиентов:

     ```
     hostname# inet bgp route-reflector client delete <IP-address>
     ```

     где `<IP-address>` — IP-адрес iBGP-соседа.

3. Чтобы включить применение карты маршрутов к отраженным маршрутам:

   ```
   hostname# inet bgp route-reflector outbound-policy on
   ```

4. Чтобы вывести текущие настройки Route Reflection:

   ```
   hostname# inet bgp show route-reflector
   ```

Поддержка ECMP и UCMP

Протокол BGP может обеспечить балансировку трафика между шлюзами доступа с помощью механизмов ECMP (Equal Cost Multi Path) и UCMP (Unequal Cost Multi Path). Балансировка выполняется при наличии нескольких эквивалентных (multipath) маршрутов в таблице маршрутизации.

По умолчанию при наличии нескольких шлюзов доступа для трафика выбирается лучший маршрут в соответствии с правилами выбора маршрута (см. Общие сведения о протоколе BGP). При этом весь трафик идет через шлюз, соответствующий лучшему маршруту и балансировка трафика не выполняется.

Поддержка ECMP позволяет встраивать несколько эквивалентных маршрутов, полученных по протоколу BGP, в таблицу маршрутизации. При этом каждому из соседей будет передан только один маршрут. Маршруты считаются эквивалентными при совпадении их параметров.



Внимание! Длина `AS-path` меняется при распространении маршрутной информации, поэтому, если используется проверка AS-path, вес маршрутов из одной AS может отличаться. Чтобы использовать ECMP, отключите проверку `AS-path` при встраивании маршрутов.

Чтобы отключить проверку `AS-path` при встраивании эквивалентных маршрутов:

```
hostname# inet bgp router bestpath as-path-relax on
```

Поддержка UCMP предполагает добавление в маршрут расширенного комьюнити `Link bandwidth`. При получении нескольких эквивалентных маршрутов они добавляются в таблицу маршрутизации с весом, пропорциональным значению `Link bandwidth`.



Внимание! Использование UCMP возможно, только если маршрутизаторы соседей поддерживают обработку комьюнити `Link bandwidth`.

Чтобы настроить режим обработки эквивалентных маршрутов с расширенным комьюнити `Link bandwith`:

`hostname# inet bgp router bestpath bandwith {ignore|skip|min|default}`, где:

- `ignore` — значение `Link bandwidth` будет проигнорировано, все эквивалентные маршруты будут встроены с весом 1;
- `skip` — маршруты из набора эквивалентных маршрутов без `Link bandwidth` будут проигнорированы и не будут встроены в таблицу маршрутизации;
- `min` — маршруты из набора эквивалентных маршрутов без `Link bandwidth` будут встроены в таблицу маршрутизации с весом 1;
- `default` — возвращает поведения по умолчанию: если хотя бы один маршрут из набора эквивалентных маршрутов будет без `Link bandwidth`, маршруты будут встроены в таблицу маршрутизации с весом 1.

Чтобы просмотреть настройки выбора лучшего маршрута:

```
hostname# inet bgp show bestpath
```

Настройка резервирования каналов с помощью BGP

С помощью BGP вы можете настроить резервирование каналов связи сегментов корпоративной сети (AS 1 и AS 3), подключенных к сети провайдера (AS 2) так, чтобы:

- трафик между сегментом и провайдером передавался по выбранному основному каналу при его доступности;
- при обрыве основного канала передача трафика переключалась на резервный канал;
- при восстановлении работоспособности основного канала передача трафика переключалась обратно.

Для выбора основного канала используется вес, назначаемый маршрутам, поступающим от провайдера. По умолчанию вес маршрутов равен нулю. С помощью карты маршрутов назначьте маршрутам от R-1.1 и R-2.1 вес 100, чтобы выбрать основные каналы. Если какой-либо из них станет недоступен, передача трафика переключится на резервный, и вернется обратно при его восстановлении.

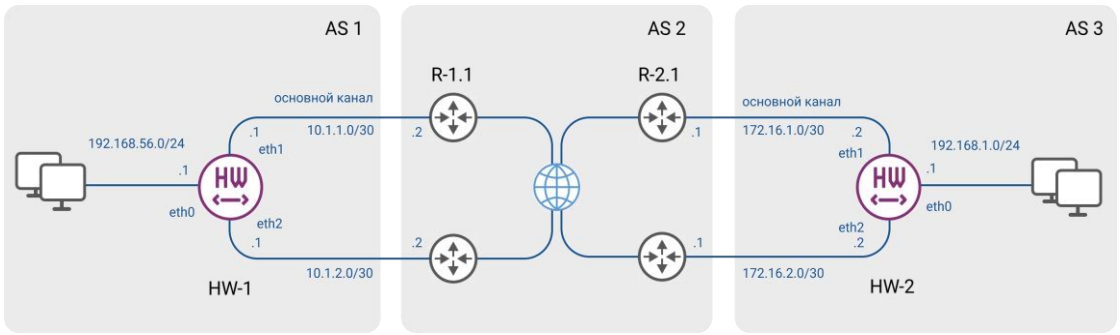


Рисунок 56. Подключение сегментов корпоративной сети (AS 1 и AS 3) к сети провайдера (AS 2)

1 Настройте BGP на HW-1:

1.1 Включите BGP:

```
hostname# inet bgp on
```

1.2 Задайте номер автономной системы:

```
hostname# inet bgp router as 1
```

1.3 Настройте соседство с R-1.1 и R-1.2:

```
hostname# inet bgp neighbor add 10.1.1.2 remote-as 2
hostname# inet bgp neighbor add 10.1.2.2 remote-as 2
```

1.4 Проверьте, что с R-1.1 и R-1.2 установлены сессии:

```
hostname# inet bgp show summary
```

1.5 Проверьте, что в BGP-таблице есть маршруты до R-1.1 и R-1.2:

```
hostname# inet bgp show
```

1.6 Создайте карту маршрутов с именем SET_WEIGHT_100:

```
hostname# inet route-map add SET_WEIGHT_100
```

1.7 Добавьте в карту маршрутов блок 1:

```
hostname# inet route-map SET_WEIGHT_100 permit 1
```

1.8 Добавьте в блок 1 карты маршрутов действие «установить вес 100»:

```
hostname# inet route-map SET_WEIGHT_100 1 set weight 100
```

1.9 Назначьте карту маршрутов SET_WEIGHT_100 для применения к входящим маршрутам от R-1.1:

```
hostname# inet bgp neighbor 10.1.1.2 set route-map SET_WEIGHT_100 in
```

2 Настройте BGP на HW-2:

2.1 Включите BGP:

```
hostname# inet bgp on
```

2.2 Задайте номер автономной системы:

```
hostname# inet bgp router as 3
```

2.3 Настройте соседство с R-2.1 и R-2.2:

```
hostname# inet bgp neighbor add 172.16.1.1 remote-as 2
hostname# inet bgp neighbor add 172.16.2.1 remote-as 2
```

2.4 Проверьте, что с R-2.1 и R-2.2 установлены сессии:

```
hostname# inet bgp show summary
```

2.5 Проверьте, что в BGP-таблице есть маршруты до R-2.1 и R-2.2:

```
hostname# inet bgp show
```

2.6 Создайте карту маршрутов с именем SET_WEIGHT_100:

```
hostname# inet route-map add SET_WEIGHT_100
```

2.7 Добавьте в карту маршрутов блок 1:

```
hostname# inet route-map SET_WEIGHT_100 permit 1
```

2.8 Добавьте в блок 1 карты маршрутов действие «установить вес 100»:

```
hostname# inet route-map SET_WEIGHT_100 1 set weight 100
```

2.9 Назначьте карту маршрутов SET_WEIGHT_100 для применения к входящим маршрутам от R-2.1:

```
hostname# inet bgp neighbor 172.16.1.1 set route-map SET_WEIGHT_100 in
```

Настройка BFD

ViPNet Coordinator HW поддерживает работу протокола BGP с несколькими шлюзами и перенаправляет трафик при отказе одного из них. Для обнаружения отказа могут использоваться `hello`-сообщения BGP. Но вы можете настроить BFD, чтобы обнаруживать отказ значительно быстрее. При этом между ViPNet Coordinator HW и соседом устанавливается BFD-сессия, которая и выявляет отказ, после чего уведомляет BGP о необходимости переключения на альтернативный маршрут. Это происходит еще до выявления проблем BGP-сессии с соседом.

Для настройки параметров обнаружения отказа используется BFD-профиль, применяемый к соседу.

Таблица 15. Параметры BFD-профиля

Параметр	Описание	Диапазон	По умолчанию
`detect-multiplier`	Множитель — количество «потерянных» контрольных пакетов, превышение которого считается отказом.	2-255	3
`receive-interval`	Минимальный интервал приема контрольных пакетов, мс.	10-60000	300
`transmit-interval`	Минимальный интервал передачи контрольных пакетов, мс.	10-60000	300

Чтобы настроить BFD:

1. Включите BFD и разрешите его автозапуск:

   ```
   hostname# inet bfd on
   ```

2. Если для вашей сети не подходят параметры BFD-профиля по умолчанию (`default`), настройте профили с нужными значениями:

   - Чтобы создать BFD-профиль:

     ```
     hostname# inet bfd profile add <имя> <detect-multiplier> <receive-interval>
     <transmit-interval>
     ```

     где:

     - `<имя>` — имя BFD-профиля;
     - `<detect-multiplier>` — множитель;
     - `<receive-interval>` — интервал приема;
     - `<transmit-interval>` — интервал передачи.

   - Чтобы обновить параметры BFD-профиля:

     ```
     hostname# inet bfd profile update <имя> <detect-multiplier> <receive-interval>
     <transmit-interval>
     ```

   - Чтобы удалить BFD-профиль:

```
hostname# inet bfd profile delete <имя>
```

- Чтобы просмотреть настройки BFD-профилей:

```
hostname# inet bfd show profile
```

3 Настройте BFD-пиринг с соседями:

- Чтобы включить BFD-пиринг с соседом:

```
hostname# inet bgp neighbor <адрес> set bfd [profile <имя>]
```

где:

- `<адрес>` — IP-адрес соседа;
- `<имя>` — имя BFD-профиля.



Примечание. В двух случаях BFD-сессия с соседом будет установлена только после первого установления BGP-сессии с ним:

- всегда для iBGP-соседа;
- для eBGP-соседа при TTL, отличном от единицы.

Для eBGP-соседа с TTL, равным единице, BFD-сессия устанавливается вне зависимости от BGP-сессии.

- Чтобы выключить BFD-пиринг с соседом:

```
hostname# inet bgp neighbor <адрес> remove bfd
```

где `<адрес>` — IP-адрес соседа.

4 Чтобы просмотреть текущее состояние BFD-пиринга:

```
hostname# inet bfd show [status [<адрес>]]
```

где:

- `status` — состояние подключения к BFD-пирам;
- `<адрес>` — IP-адрес BFD-пира.

Без указания ключевого слова `status` отображаются общие настройки BFD-пиринга, список BFD-пиров и используемых BFD-профилей. Иначе отображается состояние состояние BFD-сессий со всеми или выбранным пиром:

- IP-адрес пира;
- ID маршрутизатора;
- ID пира;
- статус сессии;
- время установленной сессии или время, в течение которого сессия не может быть установлена;
- параметры собственного профиля: множитель, интервал приема, интервал передачи;
- параметры профиля пира: множитель, интервал приема, интервал передачи.

Если BFD-сессия еще не установлена (см. примечание выше), отображается `Status: down`.

Настройка MultiWAN

Если для доступа ViPNet Coordinator HW в интернет используется несколько шлюзов (провайдеров), то вы можете настроить политики маршрутизации для различных случаев. Например, для распределения нагрузки между каналами связи или для резервирования каналов при использовании нескольких интернет-провайдеров на случай отказа одного из них (чтобы избежать потерь трафика).

Для этих целей в ViPNet Coordinator HW реализована технология MultiWAN, позволяющая настроить поведение ViPNet Coordinator HW в случае недоступности одного из интернет-шлюзов. Эта технология представлена в ViPNet Coordinator HW следующими функциями:

- Пользовательские таблицы маршрутизации (см. Создание статических маршрутов). С их помощью вы можете задать различные маршруты для различных ситуаций. Например, основную таблицу маршрутизации и дополнительную таблицу маршрутизации на случай, если шлюз основного провайдера станет недоступен и потребуется перенаправить трафик через шлюз альтернативного провайдера.
- Политики маршрутизации (см. Настройка политик маршрутизации). С их помощью вы можете задать условия, при которых трафик будет перенаправляться по заданным таблицам маршрутизации.
- Проверка состояния шлюзов (Dead Gateway Detection, DGD) (см. Настройка проверки состояния шлюзов (DGD)). С помощью этой функции вы можете задавать выполнение политики маршрутизации в зависимости от доступности или недоступности шлюза.

Особенности настройки

- Не добавляйте в пользовательские таблицы маршрутизации маршруты, противоречащие маршрутам в таблице по умолчанию.
- Не используйте динамические маршруты, получаемые по протоколам DHCP и OSPF при настройке маршрутизации для резервирования канала доступа в интернет (при использовании DHCP отключите автоматическое получение маршрутов: `hostname# inet ifconfig <интерфейс> dhcp route off`). Динамические маршруты записываются в таблицу по умолчанию и будут задействованы с соответствующим приоритетом. Не используйте канал с динамическими маршрутами в качестве резервного канала.
- Добавляйте маршруты только в пользовательские таблицы маршрутизации, а таблицу по умолчанию изменяйте лишь в крайнем случае.
- Перед активацией политики маршрутизации убедитесь, что она настроена корректно и не нарушит связь ViPNet Coordinator HW с узлом, с которого вы настраиваете ViPNet Coordinator HW.
- Не используйте одинаковые IP-адреса для проверки шлюзов DGD и для параметров `testip` при работе в кластере — это может привести к циклической перезагрузке обоих узлов кластера.

- После добавления проверки шлюза DGD по протоколу TCP и портам 80 и 443 необходимо создать соответствующий разрешающий сетевой фильтр: источник — **Мой узел ViPNet**, назначение — IP-адрес шлюза, порты назначения 80 и 443.

Настройка политик маршрутизации

Примечание. Принципы использования политик маршрутизации см. в разделе Принципы маршрутизации.

Для применения пользовательской политики маршрутизации необходимо добавить в неё правила маршрутизации и выбрать её в качестве активной.

Каждое правило состоит из условий, которые применяются к трафику (признаки трафика), и действия, которое выполняется, если трафик соответствует условиям.

Чтобы создать правило маршрутизации или добавить условия применения к уже существующему правилу:

```
hostname# inet policy rule add <имя политики> <приоритет> match {address {from | to} <IP-адрес/маска> | {inbound-interface | outbound-interface} <интерфейс> | dscp <значение метки DSCP>}
```

- В параметре `<имя политики>` задайте имя создаваемой политики маршрутизации или укажите имя существующей политики.
- В параметре `<приоритет>` задайте приоритет правила маршрутизации в диапазоне 1024–2048. Чем меньше значение, тем выше приоритет. Если правило с указанным приоритетом уже существует, условие применения правила будет добавлено в это правило.
- После ключевого слова `match` задайте условия применения правила маршрутизации (признаки трафика):
  - `address from <IP-адрес/маска>` — IP-пакеты получены от указанной подсети;
  - `address to <IP-адрес/маска>` — IP-пакеты отправлены в указанную подсеть;
  - `inbound-interface` — IP-пакеты поступили на указанный интерфейс;
  - `outbound-interface` — IP-пакеты отправлены с указанного интерфейса;
  - `dscp <значение метки DSCP>` — IP-пакеты с меткой DSCP (Differentiated Services Code Point).

После создания правила маршрутизации с условиями применения, необходимо задать действие для этого правила (см. ниже).

Чтобы задать действие для существующего правила или создать правило маршрутизации, применяемое для всего IP-трафика:

```
hostname# inet policy rule add <имя политики> <приоритет> {table {<номер таблицы> | name <имя таблицы> | default} | block}
```

- В параметре `<имя политики>` укажите имя существующей политики маршрутизации или задайте имя создаваемой политики.
- В параметре `<приоритет>` укажите приоритет существующего правила маршрутизации, чтобы задать его действие, или задайте приоритет для создания нового правила маршрутизации, которое будет применяться ко всему IP-трафику. Приоритет задаётся в диапазоне 1024–2048.
- Задайте действие правила:
  - Чтобы обрабатывать IP-пакет по пользовательской таблице маршрутизации, укажите:

    ```
    table {<номер таблицы> | name <имя таблицы>}
    ```
  - Чтобы обрабатывать IP-пакет по таблице маршрутизации по умолчанию, укажите:

    ```
    table default
    ```
  - Чтобы заблокировать IP-пакет, укажите:

    ```
    block
    ```



Внимание! Чтобы не нарушить прохождение IP-трафика между локальными сетями (сетевыми интерфейсами ViPNet Coordinator HW), в каждую пользовательскую политику маршрутизации добавьте правило для всего трафика (без признаков) с таблицей маршрутизации по умолчанию. Только эта таблица содержит маршруты в локальную сеть (`connected`). При этом мы рекомендуем присвоить такому правилу наивысший приоритет в политике и очистить таблицу по умолчанию от статических и динамических маршрутов.

Чтобы активировать пользовательскую политику маршрутизации:

```
hostname# inet policy active <имя политики>
```

Чтобы активировать политику маршрутизации по умолчанию:

```
hostname# inet policy active default
```



Примечание. Чтобы узнать, какая политика маршрутизации действует в настоящий момент времени:

```
hostname# inet show policy rule active
```

Примеры

- Чтобы добавить в политику `policy1` правило высшего приоритета, которое будет передавать IP-пакеты от подсети 192.168.1.0/30 на обработку по таблице маршрутизации `table1`:

  ```
  hostname# inet policy rule add policy1 1024 match address from 192.168.1.0/30
  hostname# inet policy rule add policy1 1024 table name table1
  ```
- Чтобы добавить в политику `policy2` правило с приоритетом 1025, которое будет передавать все IP-пакеты на обработку по таблице маршрутизации по умолчанию (Main):

  ```
  hostname# inet policy rule add policy2 1025 table default
  ```
- Чтобы добавить в политику `policy2` правило с приоритетом 1026, которое будет блокировать IP-пакеты, поступающие на сетевой интерфейс `eth1`:

  ```
  hostname# inet policy rule add policy2 1026 match inbound-interface eth1
  hostname# inet policy rule add policy2 1026 block
  ```

- Чтобы добавить в правило с приоритетом 1024 дополнительное условие применения — обработку IP-пакетов с меткой DSCP со значением `0x80`:

  ```
  hostname# inet policy rule add policy1 1024 match dscp 0x80
  ```

Настройка проверки состояния шлюзов (DGD)

1 Запустите службу DGD:

  ```
  hostname# inet dgd mode on
  ```

2 Для каждого шлюза настройте проверку его состояния с помощью отправки запросов на тестовый IP-адрес или IP-адрес шлюза:

  ```
  hostname# inet dgd next-hop add <имя шлюза> {address <адрес шлюза> | interface <интерфейс>} [test-address <тестовый адрес>] {check | no-check} {icmp | tcp80 | tcp443}
  ```

  - В параметре `<имя шлюза>` задайте произвольное имя шлюза, которое будет использоваться при настройке DGD.
  - Укажите IP-адрес шлюза в параметре `<адрес шлюза>` или имя сетевого интерфейса ViPNet Coordinator HW в параметре `<интерфейс>` — если интерфейс, через который доступен шлюз, получает IP-адрес по DHCP/PPP.
  - В параметре `<тестовый адрес>` укажите IP-адрес сетевого узла, по которому будет проверяться доступность шлюза. Если значение не задано, в качестве тестового IP-адреса будет использоваться IP-адрес шлюза. Несколько шлюзов могут иметь один и тот же тестовый IP-адрес.

    Внимание! Не используйте одинаковые IP-адреса для проверки шлюзов DGD и для параметров `testip` при работе в кластере — это может привести к циклической перезагрузке обоих узлов кластера.

  - `check` — включить проверку состояния шлюза.
  - `no-check` — выключить проверку состояния шлюза.
  - `icmp` — использовать широковещательный запрос ICMP для проверки состояния шлюза.
  - `tcp80` — использовать TCP-соединение по порту 80 для проверки состояния шлюза.
  - `tcp443` — использовать TCP-соединение по порту 443 для проверки состояния шлюза.

3 Если вы настроили проверку шлюза с использованием TCP-соединения, создайте разрешающий сетевой фильтр:

  ```
  hostname# firewall local add src @local dst <тестовый адрес> tcp dport 80 tcp dport 443 pass
  ```

4 Добавьте правило проверки состояния шлюза, при выполнении которого будет действовать определённая политика маршрутизации:

  ```
  hostname# inet dgd rule add <имя правила> match-next-hop <имя шлюза> {up | down}
  ```

  - В параметре `<имя правила>` задайте уникальное имя правила проверки состояния шлюза.
  - В параметре `<имя шлюза>` укажите имя шлюза, заданное на шаге 2.

- Выберите условие применения правила:
  - `up` — правило будет применяться, если шлюз доступен.
  - `down` — правило будет применяться, если шлюз недоступен.

Созданное правило не будет использоваться, пока не задано действие правила (см. шаг 5).

Вы можете добавить несколько условий в одно правило (например, чтобы правило выполнялось, когда один шлюз доступен, а другой не доступен). Для этого выполните повторно данную команду с указанием того же имени правила, но другого имени шлюза.

5 Задайте действие правила, созданного на предыдущем шаге:

```
hostname# inet dgd rule add <имя правила> action-priority <приоритет> service {log
command <текст сообщения> | route command policy active {<имя политики> | default}}
```

- В параметре `<имя правила>` укажите имя правила проверки состояния шлюза.
- В параметре `<приоритет>` задайте приоритет правила: от 1 до 255. Чем меньше значение, тем выше приоритет правила.
- Выберите действие, которое будет выполняться при соблюдении всех условий правила, заданных на предыдущем шаге:
  - `log command <текст сообщения>` — записать событие с текстом `<текст сообщения>` в системный журнал.
  - `route command policy active <имя политики>` — активировать политику маршрутизации с именем `<имя политики>`.
  - `route command policy active default` — активировать политику маршрутизации по умолчанию.



Примечание. События переключения политики маршрутизации, а также изменение доступности шлюзов записываются в системный журнал. Примеры записей см. в приложении События системного журнала и журнала аудита.

6 Чтобы настроить общие параметры для проверки доступности шлюзов:

```
hostname# inet dgd configuration {default | interval-time <интервал> | response-time
<время> | retries-count <число проверок> | syslog-level <уровень важности>}
```

- `interval-time <интервал>` — задать время в секундах, через которое производится проверка соединения с тестовым IP-адресом шлюза. Возможные значения: 1–120.
- `response-time <время>` — задать время в секундах, в течение которого ожидается ответ от тестового IP-адреса шлюза. Возможные значения: 1–120.
- `retries-count <число проверок>` — задать число проверок IP-адреса шлюза, при достижении которого шлюз считается нерабочим. Возможные значения: 1–10.
- `syslog-level <уровень важности>` — изменить уровень важности событий, записываемых в системный журнал. Возможные значения: 0–4.
- `default` — сброс параметров на значения по умолчанию:
  - `interval-time` — 3 секунды;
  - `response-time` — 3 секунды;

- `retries-count` — 3 проверки;
- `syslog-level` — 3-й уровень (информационные сообщения).

7 Чтобы просмотреть параметры проверки доступности шлюзов и состояние шлюзов:

```
hostname# inet show dgd next-hop
```

Полный список команд по настройке проверки состоянию шлюзов см. в документе «Справочник команд и конфигурационных файлов».

Резервирование каналов доступа в интернет

В этом примере сеть ViPNet имеет выход в интернет через двух провайдеров: основного (шлюз GW-1) и запасного (шлюз GW-2). Чтобы в случае потери соединения со шлюзом одного провайдера переключаться на другой шлюз, необходимо настроить резервирование каналов доступа в интернет с помощью MultiWAN.

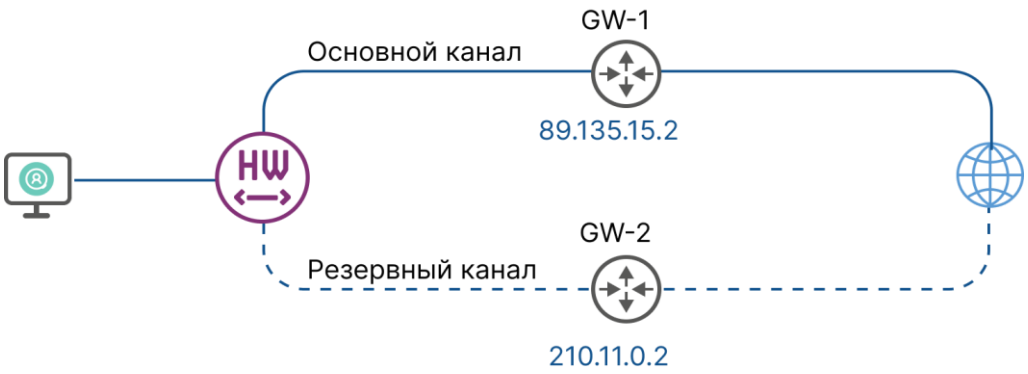


Рисунок 57. Резервирование каналов доступа в интернет

Для настройки резервирования каналов доступа:

1 Удалите маршруты по умолчанию из таблицы по умолчанию:

```
hostname# inet route delete default
```

2 Добавьте маршруты по умолчанию для шлюзов GW-1 и GW-2:

```
hostname# inet route add default next-hop 89.135.15.2 table 1024 name GW-1
hostname# inet route add default next-hop 210.11.0.2 table 1025 name GW-2
```

3 Создайте политики маршрутизации, по которым трафик будет маршрутизироваться через шлюз GW-2, когда недоступен шлюз GW-1:

3.1 Добавьте более приоритетные правила для таблицы по умолчанию:

```
hostname# inet policy rule add route-via-GW-2-policy 1024 table default
hostname# inet policy rule add route-via-GW-1-policy 1024 table default
```

3.2 Добавьте менее приоритетные правила для пользовательских таблиц:

```
hostname# inet policy rule add route-via-GW-2-policy 1025 table name GW-2
hostname# inet policy rule add route-via-GW-1-policy 1025 table name GW-1
```

Примечание. Приоритет у правил по таблице по умолчанию должен быть выше, чем у общих правил маршрутизации, применяющихся для всего трафика.

4 Запустите службу DGD:

```
hostname# inet dgd mode on
```

5 Настройте проверку доступности шлюзов провайдеров GW-1 и GW-2:

```
hostname# inet dgd next-hop add GW-1 address 89.135.15.2 check icmp
hostname# inet dgd next-hop add GW-2 address 210.11.0.2 check icmp
```

6 Создайте правила службы DGD, по которым действует политика маршрутизации `route-via-GW-1-policy`, если доступен шлюз провайдера GW-1:

```
hostname# inet dgd rule add GW-1-up match-next-hop GW-1 up
hostname# inet dgd rule add GW-1-up action-priority 1 service route command policy active route-via-GW-1-policy
```

7 Создайте правила службы DGD, по которым действует политика маршрутизации `route-via-GW-2-policy`, если доступен шлюз провайдера GW-2, а шлюз провайдера GW-1 недоступен:

```
hostname# inet dgd rule add GW-1-down match-next-hop GW-1 down
hostname# inet dgd rule add GW-1-down match-next-hop GW-2 up
hostname# inet dgd rule add GW-1-down action-priority 1 service route command policy active route-via-GW-2-policy
```

8 Создайте правила службы DGD, по которым действует политика маршрутизации по умолчанию и создается запись в системном журнале, если недоступны шлюзы обоих провайдеров:

```
hostname# inet dgd rule add all-down match-next-hop GW-1 down
hostname# inet dgd rule add all-down match-next-hop GW-2 down
hostname# inet dgd rule add all-down action-priority 2 service log command All-Routers-Down
```

9 Перезапустите службу DGD для применения новых правил:

```
hostname# inet dgd mode off
hostname# inet dgd mode on
```

Так вы обеспечите маршрутизацию трафика между двумя сетями ViPNet даже в случае недоступности одного из провайдеров.

В качестве резервного канала связи можно использовать встроенный модем (для исполнений HW50 A1, HW50 N3 и HW100 N3). В этом случае для работы сценария резервирования, описанного выше, требуется выполнить дополнительные действия:

1 Отключите модем и получение маршрутов:

```
hostname# inet usb-modem mode off
hostname# inet usb-modem set route off
```

2 Откройте конфигурационный файл модема для редактирования:

```
hostname# inet usb-modem modify config
```

3 В первую строку добавьте символ «:» и любой неиспользуемый IP-адрес (например, `:10.255.255.254`). Это будет IP-адрес шлюза.

   Сохраните изменения и закройте файл конфигурации.

4 Включите модем:

```
hostname# inet usb-modem mode on
```

5 Создайте таблицу маршрутизации для модема:

```
hostname# inet route add default next-hop 10.255.255.254 table 1026 name ModemTable
```

6 Выполните действия по настройке резервирования каналов доступа в интернет, как описано в сценарии выше. Используйте назначенный адрес шлюза (в примере `10.255.255.254`) вместо адреса шлюза провайдера GW-2 и созданную таблицу маршрутизации (`ModemTable`) вместо таблицы маршрутизации `GW-2`.

Примечание. При ручном отключении модема (с помощью команды inet usb-modem mode off) проверка состояния шлюза модемного интерфейса будет работать некорректно. В этом случае отключите проверку состояния шлюза модемного интерфейса:

```
hostname# inet dgd next-hop add <имя модемного шлюза> address <IP-адрес модемного шлюза> test-address <тестовый IP-адрес модемного шлюза> no-check icmp
```

Обеспечение связи между прокси-сервером и клиентами из разных сетей

Защищенные клиенты выходят в интернет через прокси-сервер, расположенный в другой сети и стоящий за координатором этой сети. Используется диапазон виртуальных IP-адресов по умолчанию (11.0.0.0/8); видимость сетевых узлов — по виртуальным IP-адресам.

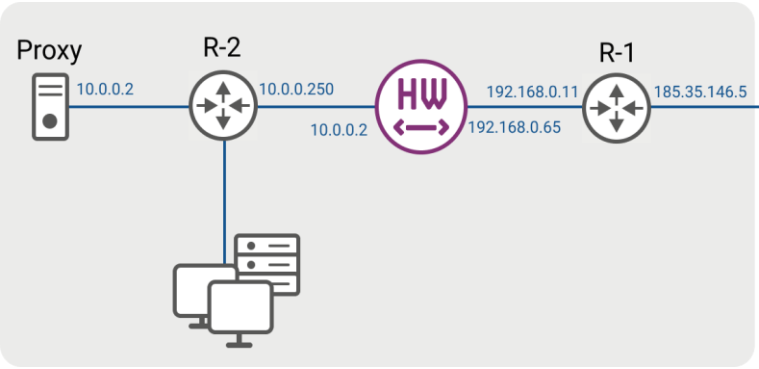


Рисунок 58. Связь между туннелируемыми узлами и узлами защищённой сети

Чтобы настроить туннелирование всех IP-адресов интернета, так чтобы прокси-сервер, расположенный за HW, мог получать запросы на доступ к ресурсам интернет от защищенных клиентов и отправлять на них ответы:

1 В ViPNet Prime задайте для HW диапазоны туннелируемых IP-адресов:

```
1.0.0.1-10.0.0.0
13.0.0.0-172.16.0.0
172.31.255.255-192.168.0.0
192.168.255.255-255.255.255.254
```

2 На HW:

2.1 Создайте маршрут по умолчанию до внутреннего сетевого интерфейса R-1:

```
hostname# inet route add default next-hop 192.168.0.11
```

2.2 Создайте таблицу PROXY-DEFAULT для маршрутизации трафика до прокси-сервера через R-2:

```
hostname# inet route add default next-hop 10.0.0.250 table 1025 name PROXY-DEFAULT
```

2.3 Создайте правило политики маршрутизации для IP-пакетов с узлов защищённой сети по таблице маршрутизации PROXY-DEFAULT:

```
hostname# inet policy rule add ClientToProxy 1024 match address from 11.0.0.0/8
hostname# inet policy rule add ClientToProxy 1024 table name PROXY-DEFAULT
```

2.4 Создайте правило политики маршрутизации для обработки остального трафика по таблице маршрутизации по умолчанию (default):

```
hostname# inet policy rule add ClientToProxy 1025 table default
```

2.5 Активируйте политику маршрутизации:

```
hostname# inet policy active ClientToProxy
```

3 На R-2 и прокси-сервере создайте маршрут от HW до виртуальных IP-адресов клиентов (11.0.0.0/8). Например, если вы используете iproute2:

```
hostname# ip route add 11.0.0.0/8 via 10.0.0.2
```

В результате трафик от узлов защищённой сети до туннелируемых узлов будет поступать на HW, расшифровываться и после обработки в соответствии с заданной политикой маршрутизации отправляться на прокси-сервер (или внутренние ресурсы) через R-2. Ответные IP-пакеты от прокси-сервера (или внутренних ресурсов) будут поступать на HW, шифроваться и затем отправляться на узлы защищённой сети через R-1.

Обработка приоритизированного трафика

В ViPNet Coordinator HW реализована поддержка протокола классификации сетевого трафика DiffServ. Использование этого протокола предполагает, что в заголовок каждого IP-пакета может быть добавлена DSCP-метка, задающая приоритет обработки пакета.

Когда на ViPNet Coordinator HW поступают IP-пакеты с DSCP-метками, по значению метки определяется принадлежность каждого IP-пакета к одному из 8 классов приоритета. IP-пакеты, принадлежащие к классу с более высоким приоритетом, всегда обрабатываются раньше пакетов, принадлежащих к менее приоритетным классам.

При зашифровании и расшифровании (инкапсуляции и декапсуляции) IP-пакета DSCP-метка перемещается соответственно из закрытой в открытую или из открытой в закрытую часть IP-пакета. Поэтому в случае, когда на ViPNet Coordinator HW приходит открытый IP-пакет с DSCP-меткой, ViPNet Coordinator HW его зашифровывает и отправляет далее получателю. По пути следования IP-пакета его DSCP-метка может быть снята или изменена и останется такой после расшифрования.

ViPNet Coordinator HW поддерживает следующие политики обработки трафика с учётом приоритета в соответствии с RFC 2474 и RFC 2475:

- Assured Forwarding — гарантированная переадресация.
- Class Selector — политика, обеспечивающая обратную совместимость с полем IP Precedence.
- Default PHB (Best Effort) — негарантированная доставка.

ViPNet Coordinator HW гарантирует обработку трафика в соответствии с его приоритетом в том случае, если на сетевом оборудовании (например, коммутаторе), подключенном к ViPNet Coordinator HW, поддерживается эта функция, а также включено управление потоком передачи данных (Ethernet Flow Control).

7

Настройка предотвращения вторжений

Общие сведения об IPS 268

Параметры IPS по умолчанию 270

Включение и выключение IPS 271

Обновление базы правил IPS 272

Обновление базы вредоносного ПО 274

Просмотр настроек IPS 276

Настройка регистрации событий IPS 278

Восстановление базы правил IPS 279

Общие сведения об IPS

В ViPNet Coordinator HW входит система предотвращения вторжений IPS (Intrusion Prevention System). IPS предназначена для обнаружения и нейтрализации сетевых атак и вредоносного ПО (Malware Detection). Использование IPS расширяет возможности ViPNet Coordinator HW по защите сетей. Для анализа сетевого трафика в IPS применяются следующие методы:

- Для обнаружения сетевых атак:
  - Сигнатурный метод — анализ заголовков протоколов и содержимого IP-пакетов, а именно:
    - заголовков транспортных протоколов, по которым необходимо отслеживать IP-пакеты (протокол, IP адреса и порты источника и получателя);
    - заголовков и параметров прикладных протоколов;
    - содержимого IP-пакетов с целью обнаружения сигнатур сетевых атак.
  - Эвристический метод — обнаружение признаков сетевых угроз:
    - аномалий в служебных заголовках IP-пакетов;
    - аномалий при декодировании и фрагментации IP-пакетов;
    - попыток сканирования портов и удаленного выполнения произвольного кода.
- Для обнаружения вредоносного ПО — обнаружение вредоносных сигнатур в содержимом IP-пакетов по протоколам HTTP, HTTPS, SMTP, IMAP, POP3, FTP и SMB.



Внимание! При обнаружении вредоносного ПО проверяемый файл может быть скачан частично из-за особенности потоковой проверки. При этом скачанный фрагмент файла не несет угрозы.

Правила обнаружения сетевых атак (далее — правила IPS) входят в состав базы правил IPS. Сигнатуры вредоносного ПО входят в состав базы вредоносного ПО. Обе базы формируются специалистами ИнфоТеКС, регулярно обновляются и публикуются на официальном сервере обновления ИнфоТеКС (см. Обновление базы правил IPS).

Каждое срабатывание правила IPS или обнаружение сигнатуры вредоносного ПО регистрируется:

- в системном журнале — краткая информация о событии;
- в журнале IP-пакетов — подробная информация о событии.

Особенности анализа сетевого трафика и регистрации событий

- В некоторых случаях для обнаружения угрозы выполняется анализ цепочки IP-пакетов и к моменту срабатывания блокирующего правила часть пакетов уже будет пропущена для обработки.

- Во время анализа пакета может сработать несколько правил IPS. При этом в системном журнале регистрируются все события, а в журнале IP-пакетов регистрируется событие на срабатывание первого правила или блокирующего правила (при наличии такого).
- IPS может пропустить отложенную атаку, если от момента открытия сессии атаки до момента отправки вредоносного ПО в этой сессии на ViPNet Coordinator HW открывались и закрывались другие сессии.
- В IPS отсутствует в явном виде режим обнаружения угроз без их блокировки (IDS). Для работы IPS в режиме обнаружения необходимо для всех блокирующих правил IPS вручную переключить действие при их срабатывании с **Блокировать** на **Предупреждать**. Поскольку для каждого правила IPS действие при срабатывании настраивается индивидуально, то при настройке IPS в режиме обнаружения угроз используйте групповые операции с правилами.

Особенность применения лицензии IPS



Внимание! После назначения лицензии IPS перезагрузите ViPNet Coordinator HW. Иначе использование IPS будет недоступно.

Параметры IPS по умолчанию

Таблица 16. Параметры IPS по умолчанию

Параметр	Значение
Предотвращение вторжений	Включено
Обнаружение вредоносного ПО	Выключено
Включение IPS при перезагрузке	Разрешено
Сервер обновления базы правил IPS и базы вредоносного ПО	https://updateids.infotecs.ru
Обновление базы правил IPS и базы вредоносного ПО по расписанию	Выключено
Расписание обновления базы правил IPS и базы вредоносного ПО	Ежедневно, время обновления выбирается случайное
База правил IPS	Из состава дистрибутива
База вредоносного ПО	Не установлена, необходимо установить с сервера обновления или с USB-носителя
Уровень важности событий IPS, регистрируемых в системном журнале	Уровень 3 (информационные)

В дальнейшем вы можете настроить параметры IPS в соответствии с политиками безопасности вашей сети.

Включение и выключение IPS



Внимание! Не рекомендуется выключать IPS без необходимости, поскольку ваша сеть станет потенциально незащищенной от сетевых атак, воздействия сетевых вирусов и попыток эксплуатации уязвимостей в программном обеспечении.

Чтобы выключить автоматический запуск IPS при загрузке ViPNet Coordinator HW, выполните:

```
hostname# service ips mode off

The settings are saved. System must be restarted for the changes to take effect. Restart now? Y/N
```

Чтобы включить автоматический запуск IPS, выполните:

```
hostname# service ips mode on

The settings are saved. System must be restarted for the changes to take effect. Restart now? Y/N
```

Чтобы выключить IPS:

```
hostname# service ips stop
```

Чтобы вновь включить IPS:

```
hostname# service ips start
```

Если IPS запущен, то при наличии действующей лицензии «Обновление Malware Detection» вы можете включить обнаружение вредоносного ПО:

```
hostname# service ips malware on

The settings are saved.
```

Обновление базы правил IPS

База правил IPS публикуется на сервере обновления `https://updateids.infotecs.ru`, или другом, указанном в документе комплекта поставки. В нем же указаны имя пользователя и пароль на доступ к серверу обновления.

По умолчанию установлена база правил IPS из состава дистрибутива ViPNet Coordinator HW. При наличии действующей лицензии «Обновление базы правил IPS» вы можете:

- обновить базу правил IPS с сервера, в том числе настроить обновление по расписанию;
- скачать базу правил IPS с сервера, скопировать её на USB-носитель и обновить вручную.



Внимание! Убедитесь, что сервер обновлений доступен на ViPNet Coordinator HW по доменному имени, иначе добавьте DNS-сервер пересылки (см. Настройка DNS-сервера).

Во время обновления базы работа IPS не прерывается.

Обновление по расписанию

1 Адрес сервера обновления по умолчанию — `updateids.infotecs.ru`. Если необходимо использовать другой сервер, задайте его IP-адрес или доменное имя:

```
hostname# service ips rule update server address <IP-адрес или доменное имя>
```

2 Задайте имя пользователя для доступа к серверу обновления:

```
hostname# service ips rule update server login <имя пользователя>
```

3 Задайте пароль пользователя для доступа к серверу обновления:

```
hostname# service ips rule update server password
```

4 Если политики безопасности вашей компании запрещают подключение к внешним серверам напрямую, вы можете обновлять базу через прокси-сервер в вашей сети:

4.1 Задайте IP-адрес или доменное имя прокси-сервера:

```
hostname# service ips rule update server proxy address <IP-адрес или доменное имя>
```

4.2 По умолчанию используется TCP-порт 3128. При необходимости измените его:

```
hostname# service ips rule update server proxy port <порт>
```

4.3 В зависимости от типа узла прокси-сервера (открытый или защищенный), создайте разрешающий сетевой фильтр (локальный фильтр открытой сети или фильтр защищенной сети), пропускающий трафик от ViPNet Coordinator HW на TCP-порт прокси-сервера.



Примечание. Чтобы вернуться к обновлению базы правил IPS напрямую, выполните:

```
hostname# service ips rule update server proxy address none
```

5 По умолчанию обновление по расписанию выключено. Чтобы настроить расписание и включить обновление:

5.1 Задайте расписание:

```
hostname# service ips rule update schedule <расписание>
```

В расписании вы можете указать время и день:

- `daily at <чч:мм>` — ежедневно в указанное время;
- `weekly on <день недели> at <чч:мм>` — в указанное время определенного дня недели.

5.2 Включите обновление по расписанию:

```
hostname# service ips rule update on
```

6 Принудительно обновите базу правил IPS:

```
hostname# service ips rule update fetch
```

7 Просмотрите сведения о базе правил IPS и проверьте настройки ее обновления:

```
hostname# service ips show update-settings
```

Далее база правил IPS будет обновляться по расписанию.

Обновление с USB-носителя

Если политики безопасности вашей компании запрещают подключение к внешним серверам, вы можете обновить базу правил IPS с USB-носителя вручную:

1 Скачайте с сервера обновления и скопируйте на USB-носитель файлы актуальной базы правил IPS (файл базы формата `*.tgz` и файл ЭП формата `*.tgz.sig`).

2 Обновите базу правил IPS с USB-носителя вручную:

```
hostname# service ips rule update usb
```

Далее отслеживайте актуальность базы правил IPS самостоятельно и обновляйте ее с USB-носителя вручную.

Обновление базы вредоносного ПО

База вредоносного ПО публикуются на сервере обновления `https://updateids.infotecs.ru`, или другом, указанном в документе комплекта поставки. В нем же указаны имя пользователя и пароль на доступ к серверу обновления.

По умолчанию база вредоносного ПО не установлена. При наличии действующей лицензии «Обновление Malware Detection» вы можете:

- обновить базу вредоносного ПО с сервера, в том числе настроить обновление по расписанию;
- скачать базу вредоносного ПО с сервера, скопировать её на USB-носитель и обновить вручную.

Если вы не включили обнаружение вредоносного ПО ранее, включите его сейчас:

```
hostname# service ips malware on
```

Обновление по расписанию

1 Адрес сервера обновления по умолчанию — `updateids.infotecs.ru`. Если необходимо использовать другой сервер, задайте его IP-адрес или доменное имя:

```
hostname# service ips malware update server address <IP-адрес или доменное имя>
```

2 Задайте имя пользователя для доступа к серверу обновления:

```
hostname# service ips malware update server login <имя пользователя>
```

3 Задайте пароль пользователя для доступа к серверу обновления:

```
hostname# service ips malware update server password
```

4 Если политики безопасности вашей компании запрещают подключение к внешним серверам напрямую, вы можете обновлять базу вредоносного ПО через прокси-сервер в вашей сети:

4.1 Задайте IP-адрес или доменное имя прокси-сервера:

```
hostname# service ips malware update server proxy address <IP-адрес или доменное имя>
```

4.2 По умолчанию используется TCP-порт 3128. При необходимости измените его:

```
hostname# service ips malware update server proxy port <порт>
```

4.3 В зависимости от типа узла прокси-сервера (открытый или защищенный), создайте разрешающий сетевой фильтр (локальный фильтр открытой сети или фильтр защищенной сети), пропускающий трафик от ViPNet Coordinator HW на TCP-порт прокси-сервера.

Примечание. Чтобы вернуться к обновлению базы вредоносного ПО напрямую, выполните:

```
hostname# service ips malware update server proxy address none
```

---

5 По умолчанию обновление по расписанию выключено. Чтобы настроить расписание и включить обновление:

5.1 Задайте расписание:

```
hostname# service ips malware update schedule <расписание>
```

В расписании вы можете указать время и день:

- `daily at <чч:мм>` — ежедневно в указанное время;
- `weekly on <день недели> at <чч:мм>` — в указанное время определенного дня недели.

5.2 Включите обновление по расписанию:

```
hostname# service ips malware update on
```

6 Принудительно обновите базу вредоносного ПО:

```
hostname# service ips malware update fetch
```

7 Просмотрите сведения о базе вредоносного ПО и проверьте настройки ее обновления:

```
hostname# service ips show update-settings
```

Далее база вредоносного ПО будет обновляться по расписанию.

Обновление с USB-носителя вручную

Если политики безопасности вашей компании запрещают подключение к внешним серверам, вы можете обновить базу вредоносного ПО с USB-носителя вручную:

1 Скачайте с сервера обновления и скопируйте на USB-носитель файлы актуальной базы вредоносного ПО (файл базы формата `*.tgz` и файл ЭП формата `*.tgz.sig`).

2 Обновите базу вредоносного ПО с USB-носителя вручную:

```
hostname# service ips malware update usb
```

Далее отслеживайте актуальность базы вредоносного ПО самостоятельно и обновляйте ее с USB-носителя вручную.

Просмотр настроек IPS

Чтобы просмотреть текущие настройки IPS, в том числе обнаружения вредоносного ПО, выполните:

```
hostname# service ips show status
```

При этом отображаются:

- состояние IPS:
  - `IPS subsystem is on` — включено;
  - `IPS subsystem is on and updating` — включено и выполняется обновление базы правил IPS;
  - `IPS subsystem is in service mode` — технологический режим;
  - `IPS subsystem is off` — выключено;
- состояние автоматического запуска IPS при перезагрузке:
  - `autostart is on` — включен;
  - `autostart is off` — выключен;
- состояние обнаружения вредоносного ПО:
  - `Malware detection is on` — включено;
  - `Malware detection is off` — выключено;
- уровень важности событий IPS, регистрируемых в системном журнале;
- дата и время создания базы правил IPS;
- дата и время создания базы вредоносного ПО;
- дата и время последнего обновления базы правил IPS;
- дата и время последнего обновления базы вредоносного ПО.

Для просмотра сведений о текущих настройках обновления базы правил IPS и базы вредоносного ПО выполните:

```
hostname# service ips show update-settings
```

При этом по каждой из баз отображаются следующие настройки:

- обновления базы по расписанию (включено или выключено);
- расписание обновления базы (периодичность и время обновления);
- адрес сервера обновления базы;
- имя пользователя для доступа к серверу обновления;
- статус пароля пользователя (установлен или не установлен).
- адрес, порт и статус прокси-сервера;

- дата и время окончания действия лицензии;
- идентификатор лицензии.

Настройка регистрации событий IPS

События, связанные с работой системы предотвращения вторжений IPS, классифицированы по шести уровням (приведены в порядке убывания важности события):

- 0 — критические события;
- 1 — ошибки;
- 2 — предупреждения;
- 3 — информационные события;
- 4 — отладочные события;
- 5 — детализированные отладочные события.

События регистрируются в системном журнале ViPNet Coordinator HW в соответствии с установленным уровнем важности. По умолчанию установлен уровень 3. При этом в системный журнал записываются события с уровнями 0–3: критические события, ошибки, предупреждения и информационные события.

Вы можете изменить текущий уровень важности регистрируемых событий, например для выявления причины неполадок, возникших в работе предотвращения вторжений. В этом случае, для получения детализированных сведений, вы можете установить уровень 4 (отладочные) или 5 (детализированные отладочные). При уровне 5 вы будете получать все сообщения о работе предотвращения вторжений.

Для изменения текущего уровня важности регистрируемых событий системы предотвращения вторжений ViPNet Coordinator HW:

```
hostname# service ips syslog-level <уровень событий>
```

В качестве параметра `<уровень событий>` укажите значение от 0 до 5 .

В некоторых случаях, при изменении уровня важности событий IPS, регистрируемых в системном журнале ViPNet Coordinator HW, требуется перезапуск IPS (подробнее см. «Справочник команд и конфигурационных файлов», раздел «Команды группы service», команда `service ips syslog-level`).

Восстановление базы правил IPS

При возникновении неполадок при обновлении базы правил IPS вы можете восстановить базу правил до версии, поставляемой в составе дистрибутива ViPNet Coordinator HW. Для этого выполните:

```
hostname# service ips rule restore-default
```

После выполнения команды изменятся следующие параметры:

- Настройки обновления базы правил с сервера (адрес сервера обновлений, имя и пароль пользователя, расписание) сохранятся.
- Автоматическое обновление базы правил IPS с сервера будет выключено.
- Настройки правил IPS (действие правила, комментарии и параметры правил) будут установлены в состояние по умолчанию.



8

Настройка параметров безопасности

Управление локальными учетными записями 281

Настройка оповещения об истечении срока действия ключей 288

Просмотр сведений о ключе защиты обновлений и ключах обмена 289

Обновление ключей по истечении срока их действия 291

Перевыпуск ключей локального SSH-сервера 292

Настройка доступа сетевых интерфейсов к оперативной памяти 293

Управление локальными учетными записями

Параметры учетных записей

Таблица 17. Параметры локальных учетных записей

Параметр	Обозначение	Значения
Имя *	`Login`	• допустимые символы: буквы (`A–Z`, `a–z`), цифры (`0–9`), символы `-._()` • длина: 1–63 символа
Пароль *	`Password`	• допустимые символы: буквы (`A–Z`, `a–z`), цифры (`0–9`), символы `(!@#$%^&*()-_+=;:'",.<>/?|\`~[]{}`) • длина: 8–81 символ • пароль не имеет ограничения по сроку действия. Напоминание о необходимости смены пароля выводится через 150 дней после его установки или смены, а предупреждение — через 180 дней
Роль *	`Role`	• `Superadmin` — суперадминистратор • `Administrator` — администратор • `Netadmin` — сетевой администратор • `Auditor` — аудитор
Полное имя	`Full name`	• строка символов UTF-8 • длина строки: не более 80 символов
Описание	`Description`	• строка символов UTF-8 • длина строки: не более 80 символов • `Built-in account` — описание суперадминистратора (неизменяемое)
Состояние *	`Status`	• `active` — учетная запись активна • `blocked` — учетная запись заблокирована

* — обязательный параметр учетной записи.

Полномочия ролей по управлению учетными записями

Роль учетной записи определяет полномочия пользователя по настройке учетных записей, а именно:

- создание учетных записей;
- удаление учетных записей;
- изменение параметров учетных записей;
- просмотр учетных записей и завершение сессий пользователей.

Таблица 18. Полномочия ролей по созданию учетных записей

	Суперадминистратор	Администратор	Сетевой администратор	Аудитор
Создание учетных записей	Да	Да	Нет	Нет
Доступные роли учетной записи при создании новой или изменении существующей	• Administrator • Netadmin • Auditor	• Administrator • Netadmin • Auditor		

Таблица 19. Полномочия ролей по удалению учетных записей

	Суперадминистратор	Администратор	Сетевой администратор	Аудитор
Удаление учетных записей	Да	Да	Нет	Нет
Роли удаляемых учетных записей	• Administrator • Netadmin • Auditor	• Administrator • Netadmin • Auditor		

Таблица 20. Полномочия ролей по изменению параметров учетных записей

Параметр	Суперадминистратор	Администратор	Сетевой администратор	Аудитор
Имя	Да	• Superadmin • Administrator	• Superadmin • Administrator	• Superadmin • Administrator
Роль	Нет	• Superadmin • Administrator	• Superadmin • Administrator	• Superadmin • Administrator
Полное имя	Да	• Superadmin • Administrator	• Superadmin • Administrator	• Superadmin • Administrator
Описание	Нет	Superadmin	Superadmin	• Superadmin • Administrator
Пароль	Да	• Superadmin • Administrator	• Superadmin • Administrator • Netadmin (свой пароль)	• Superadmin • Administrator • Auditor (свой пароль)

Параметр	Суперадминистратор	Администратор	Сетевой администратор	Аудитор
Состояние	Нет	• Superadmin • Administrator	• Superadmin • Administrator	• Superadmin • Administrator

Таблица 21. Полномочия ролей по просмотру учетных записей и завершению сессий

	Суперадминистратор	Администратор	Сетевой администратор	Аудитор
Просмотр списка локальных пользователей и параметров их учетных записей	Да	Да	Да	Нет
Завершение сессий локальных пользователей	• свои сессии • Administrator • Netadmin • Auditor	• свои сессии • Administrator • Netadmin • Auditor	свои сессии	свои сессии

Управление учетными записями

После инициализации на ViPNet Coordinator HW есть только локальная учетная запись admin с ролью суперадминистратора. Пароль для этой учетной записи вы задали в ходе инициализации.

В соответствии с политиками безопасности вашей организации создайте учетные записи с ролями администратора, сетевого администратора и аудитора.

Создание учетной записи

```
hostname# users add <имя учетной записи>
```

Команда выполняется интерактивно (чтобы прервать выполнение, нажмите **Ctrl**+**C**):

1 Выберите роль пользователя.

2 Задайте и подтвердите пароль.

3 Если используется аутентификация по сертификату:

3.1 При появлении сообщения `Disconnect your token, connect user's token, and press <Enter>` отключите свой USB-токен и подключите USB-токен, который будет использоваться для аутентификации нового пользователя на ViPNet Coordinator HW.

3.2 Если необходимо инициализировать USB-токен:

3.2.1 В строке `Do you want to reinitialize token? [Yes/No]` введите `Y` и нажмите **Enter** — для инициализации USB-токена и записи сертификата.

3.2.2 В строке `Enter admin-token pincode` введите PIN-код администратора USB-токена.

3.2.3 В строке `Enter new user-token pincode` задайте PIN-код пользователя USB-токена и подтвердите его, затем нажмите **Enter**.

3.3 Если необходимо использовать существующий сертификат для аутентификации пользователя:

3.3.1 В строке `Do you want to reinitialize token? [Yes/No]` введите `N` и нажмите **Enter**.

3.3.2 В строке `Enter user's pincode` введите PIN-код пользователя USB-токена, затем нажмите **Enter**.

4 Задайте полное имя пользователя. Чтобы пропустить ввод, нажмите **Enter**.

5 Задайте описание. Чтобы пропустить ввод, нажмите **Enter**.

По умолчанию созданная учетная запись активна.

Изменение параметров учетной записи

```
hostname# users edit <имя учетной записи> info
```

Команда выполняется интерактивно (чтобы прервать выполнение, нажмите **Ctrl**+**C**):

1 Чтобы сменить роль локального пользователя:

1.1 В строке `Do you want to change user role [Yes/No]` нажмите `Y`.

1.2 Выберите новую роль пользователя (список доступных ролей зависит от роли пользователя, выполняющего команду).

2 Задайте новое имя пользователя (чтобы пропустить, нажмите **Enter**):

3 Задайте новое полное имя пользователя (чтобы пропустить, нажмите **Enter**);

4 Задайте новое описание (чтобы пропустить, нажмите **Enter**).

При изменении роли, имени или смене пароля все сессии пользователя завершаются.

Смена пароля учетной записи

Для смены пароля текущего пользователя:

```
hostname# users passwd
```

Для смены пароля другого пользователя:

```
hostname# users edit <имя учетной записи> passwd
```

При выполнении команды задайте новый пароль и подтвердите его. После смены пароля все сессии пользователя завершаются.

Установка или замена сертификата аутентификации пользователя

Для установки сертификата текущего пользователя:

```
hostname# users cert
```

1 Подключите USB-токен к ViPNet Coordinator HW.

2 Чтобы инициализировать USB-токен:

2.1 В строке `Do you want to reinitialize token? [Yes/No]` введите `Y`.

2.2 Введите PIN-код администратора USB-токена.

2.3 Задайте и подтвердите новый PIN-код пользователя USB-токена.

3 Чтобы задать существующий сертификат для доступа текущего пользователя:

3.1 В строке `This token is already used by another user. Continue anyway? [Yes/No]` введите `Y`.

3.2 В строке `Do you want to reinitialize token? [Yes/No]` введите `N`.

3.3 Введите PIN-код пользователя USB-токена.

Для установки сертификата другого локального пользователя:

```
hostname# users edit <имя учетной записи> cert
```

- Отключите USB-токен текущего пользователя от ViPNet Coordinator HW, а затем подключите USB-токен локального пользователя, для которого устанавливается сертификат.
- Чтобы инициализировать USB-токен:
  - В строке `Do you want to reinitialize token? [Yes/No]` введите `Y`.
  - Введите PIN-код администратора USB-токена.
  - Задайте и подтвердите новый PIN-код пользователя USB-токена.
- Чтобы задать существующий сертификат для доступа пользователя:
  - В строке `Do you want to reinitialize token? [Yes/No]` введите `N`.
  - Введите PIN-код пользователя USB-токена.
- Отключите USB-токен локального пользователя от ViPNet Coordinator HW, а затем подключите USB-токен текущего пользователя.

После выполнения команды все сеансы пользователя принудительно завершаются.

Просмотр учетных записей

```
hostname# users show
```

По команде отображаются локальные учетные записи пользователей:

- `Block timeout period` — время блокировки учетных записей в минутах;
- `User list` — список и параметры учетных записей:
  - имя пользователя;
  - `Role` — роль:
    - `Superadmin` — суперадминистратор;
    - `Administrator` — администратор;
    - `Netadmin` — сетевой администратор;

        - `Auditor` — аудитор;
    - `Status` — состояние:
        - `Active` — активна;
        - `Blocked (permanent)` — заблокирована постоянно;
        - `Blocked (<чч.мм> left)` — заблокирована после 10-ти неудачных попыток ввода пароля (время до разблокировки `<чч.мм>`);
    - `Full name` — полное имя пользователя;
    - `Description` — описание; для `Superadmin` — указание на встроенную учетную запись (`Built-in account`).
    - Если используется аутентификация по сертификату:
        - `Hardware token` — серийный номер USB-токена;
        - `The validity period of the certificate: <дд-мм-гггг>` — срок действия сертификата пользователя (если срок действия истек, отображается `The certificate expired`).

Блокировка и разблокировка учетной записи

Учетная запись блокируется и разблокируется автоматически для предотвращения подбора пароля. Кроме этого, вы можете заблокировать учетную запись на нужное вам время вручную и разблокировать ее при необходимости:

```
hostname# users edit <имя учетной записи> status {active | blocked}
```

При блокировке учетной записи пользователя все его сессии завершаются.

Удаление учетной записи

```
hostname# users delete <имя учетной записи>
```

При выполнении команды подтвердите удаление локальной учетной записи пользователя.

Завершение сессий пользователей

Пользователи, в соответствии со своей ролью, могут завершать собственные сессии или сессии других пользователей:

```
hostname# users kick user <имя учетной записи>
```

Суперадминистратор может завершать все сессии всех пользователей, кроме своей текущей:

```
hostname# users kick all
```

Предотвращение подбора пароля учетных записей

Для предотвращения подбора пароля локальных учетных записей используется прогрессивная задержка ввода пароля, временная блокировка учетных записей и оповещение о попытках подбора пароля:

- Если имя пользователя указано верно, то каждая неудачная попытка ввода пароля, в том числе совершаемая им в разных сессиях, увеличивает счетчик ошибок аутентификации учетной записи на единицу.
- Если пароль учетной записи введен правильно, счетчик ошибок аутентификации учетной записи сбрасывается. Иначе, после 10-ой неудачной попытки учетная запись пользователя временно блокируется, по умолчанию на 10 минут. По истечении времени блокировки учетная запись автоматически разблокируется. Настроить другое время блокировки (от 10 до 1440 минут), одинаковое для всех локальных пользователей, вы можете командой:

  ```
  hostname# users block-timeout <время блокировки>
  ```

- После трех неудачных попыток ввод пароля станет доступен через 3 секунды. Каждая последующая неудачная попытка ввода пароля увеличивает задержку в два раза по сравнению с предыдущей и считается попыткой подбора пароля. При этом значение счетчика попыток подбора пароля, общего для всех локальных учетных записей, увеличивается на единицу. Уведомление о попытках подбора пароля с указанием значения счетчика отображается при каждой успешной аутентификации любого пользователя:

  ```
  login as: admin
  Password:
  End of keyboard-interactive prompts from server
  ...
  ------------------------------------------------------------------
  Password guessing attempts registered: 5
  ------------------------------------------------------------------
  ...
  Starting the command line interface of Platform: HW1000
  hostname>
  ```

  Уведомление о количество неудачных попыток аутентификации может быть сброшено только вручную суперадминистратором, локальным или централизованным администратором:

  ```
  hostname# admin clear-auth-warning
  Password guessing counter was cleared.
  ```

- Неудачные попытки аутентификации пользователей и попытки подбора пароля регистрируются в журнале СКЗИ.
- Неверное указание имени пользователя также вызывает прогрессивную задержку ввода пароля. После 10-ой попытки идентификации с неверным именем пользователя прогрессивная задержка сбрасывается.

Настройка оповещения об истечении срока действия ключей

По умолчанию период оповещения об истечении срока действия ключей обмена, защиты обновлений узла и закрытого ключа сертификата составляет 30 дней. Оповещение отображается после аутентификации в двух случаях:

- срок действия ключа истек;
- срок действия ключа скоро истечет — разница в днях между датой окончания срока действия и текущей датой меньше периода оповещения.

Например:

```
login as: admin

Password:

End of keyboard-interactive prompts from server

WARNING: Your authentication key expire. Validity period < 7 day(s).

...

Starting the command line interface of Platform: HW1000

hostname>
```

Вы можете изменить период оповещения, указав количество дней из интервала 7-365. Например, чтобы оповещение отображалось за две недели до окончания срока действия:

```
hostname# iplir warning-threshold 14

Key warnings will start displaying in 14 days before expiry date.
```

Подробнее о настройке оповещения см. «Справочник команд и конфигурационных файлов», раздел «Команды группы iplir».

Просмотр сведений о ключе защиты обновлений и ключах обмена

Чтобы просмотреть сведения о ключе защиты обновлений узла и криптодрайвере:

```
hostname# iplir show key-info
NSK information:
        Uid:3E4923748274C62023140A1A46DB4D3C
                Software-specified key ID: 97e35097-c615-4fe9-aa8a-b221004f80b5
                Key algorithm: The Magma key algorithm
                Key expiration date: 2026-01-28
                Key effective date: 2024-11-04
                My network ID: 5ae0
                My host ID: 4
                My host name: VA1000-1
                My host variant: 0
                Message count on NSK: 20
Driver information:
        Support systems:
                ItcsCdCryptSystemGost | status: ItcsCdCryptSystemReady
                ItcsCdCryptSystemFips | status: ItcsCdCryptSystemUnavailable
                ItcsCdCryptSystemCustom | status: ItcsCdCryptSystemUnavailable
        Support crypto suites:
                G28147_CFB_WITH_IMIT
                G28147_CTR_WITH_IMIT_CMACKDF
                ITCS_AES256_CFB_WITH_IMIT
                G28147_CTR_WITH_IMIT (for IPLir 4.1)
                G3412_MAGMA_AEAD
                G3412_KUZNYECHIK_CTR_WITH_CMAC (CTR + CMAC)
                G3412_KUZNYECHIK_AEAD
                G3412_KUZNYECHIK_AEAD_MP
```

В результате будут выведены сведения:

- о ключе защиты обновлений узла:
  - `UID` — идентификатор;
  - атрибуты ключа:
    - `Software-specified key ID` — идентификатор ключа, задаваемый приложением;
    - `Key algorithm` — алгоритм шифрования;
    - `Key expiration date` — дата окончания периода действия ключа;
    - `Key effective date` — дата начала периода действия ключа;
    - `My network ID` — идентификатор собственной сети;
    - `My host ID` — идентификатор собственного узла;
    - `My host variant` — вариант собственного узла;
    - `Message count on NSK` — порядковый номер сообщения на ключе.
- о криптодрайвере:
  - `Support systems` — поддерживаемые системы и их статус;
  - `Support crypto suites` — поддерживаемые алгоритмы шифрования.

Чтобы просмотреть сведения обо всех ключах обмена:

```
hostname# iplir show exchange-keys
|----------|---------|-----------|-------------------------|-----------------|
|   Peer   | Variant | StartDate |        ExpiryDate       |     KeyID       |
|----------|---------|-----------|-------------------------|-----------------|
|0x5ae00002|        0| 2023-11-04|  2024-01-28(  -2  days)|0x0200e0...599971|
|0x5ae00002|        0| 2024-11-04|  2026-01-28(  398 days)|0x0200e0...594170|
|0x5ae00001|        0| 2024-11-04|  2026-01-28(  398 days)|0x0100e0...a04000|
|0x5ae00004|        0| 2024-11-04|  2026-01-28(  398 days)|0x0400e0...6b21e7|
|----------|---------|-----------|-------------------------|-----------------|
Warning starts displaying in 7 days before expiry date.
```



Примечание. Отрицательное значение в поле `ExpiryDate` означает, что ключ обмена более не используется, но ещё не удален в ViPNet Prime.

Чтобы просмотреть сведения о ключах обмена, срок действия которых истек или скоро истечет:

```
hostname# iplir show exchange-keys warning
```

Чтобы просмотреть сведения о ключах обмена с определённым ViPNet-узлом:

```
hostname# iplir show exchange-keys peer <ViPNet ID узла>
```

Обновление ключей по истечении срока их действия

Ключи обмена, ключи защиты обновлений узла и закрытый ключ сертификата пользователя имеют ограниченный срок действия — 15, 15 и 12 месяцев соответственно. Истечение срока действия любого из ключей не накладывает ограничений на работу ViPNet Coordinator HW. Но мы рекомендуем обновить ключи, чтобы гарантировать защиту трафика между узлами сети ViPNet.

При скором истечении срока действия (по умолчанию за 30 дней) или истечении срока действия любого из ключей в командном интерпретаторе и веб-интерфейсе выводится оповещение. Кроме этого, в системном журнале регистрируется событие об оповещении. Администратор сети ViPNet должен сформировать новые ключи и выслать их на ViPNet Coordinator HW.



Внимание! После обновления ключей создайте новую резервную копию конфигурации, так как использовать ранее созданные резервные копии будет невозможно.

Перевыпуск ключей локального SSH-сервера

Удалённое подключение к ViPNet Coordinator HW обеспечивает локальный SSH-сервер. Если вам необходимо заменить ключи SSH-сервера, например в вашей компании изменилась политика безопасности, выполните:

```
hostname# admin ssh reset-key local
```

Старый ключ будет удалён и сгенерирован новый.

Для просмотра информации о ключах локального SSH-сервера, выполните:

```
hostname# admin ssh show-key local
```

Настройка доступа сетевых интерфейсов к оперативной памяти

В некоторых исполнениях ViPNet Coordinator HW на аппаратных платформах поддерживается управление доступом сетевых интерфейсов к оперативной памяти:

- HW100 Q1, Q2;
- HW1000 Q7, Q8, Q9;
- HW2000 Q4, Q5;
- HW5000 Q1, Q2.

По умолчанию доступ не ограничен и сетевые интерфейсы могут использовать произвольную область оперативной памяти. Если ограничение доступа включено, интерфейсы могут обращаться только к изолированной области памяти, предназначенной для них. Это предотвращает атаки, связанные с прямым доступом к оперативной памяти. Ограниченный доступ интерфейсов к оперативной памяти повышает безопасность работы ViPNet Coordinator HW, но снижает его производительность.

При изменении ограничения доступа необходима перезагрузка ViPNet Coordinator HW. Вы можете перезагрузить устройство немедленно или выбрать отложенную перезагрузку.

Чтобы включить ограничение доступа:

```
hostname# machine memory-isolation on

The settings are saved.

A reboot is required to enable memory isolation. You can reboot the system now or later.

Do you want to reboot the system now? (Yes/No): No
```

Чтобы просмотреть настройки ограничение доступа:

```
hostname# machine memory-isolation show

Current memory isolation state: disabled

After a system reboot, the memory isolation state will be changed to: enabled
```



9

Настройка системных параметров

Настройка даты и времени 295

Настройка подключения к веб-интерфейсу 296

Выбор профиля производительности 298

Установка допустимого времени неактивности сессии пользователя 299

Просмотр активных сессий пользователей 300

Перезагрузка ViPNet Coordinator HW 301

Установка серийного номера 302

Просмотр лицензии 303

Использование резервного раздела в исполнениях с двумя накопителями 305

Сброс к заводским настройкам 306

Настройка даты и времени



Внимание! Если системные дата и время заданы неверно, защищённые соединения с другими узлами защищённой сети могут блокироваться. Рекомендуем настраивать синхронизацию системного времени по протоколу NTP (см. Настройка NTP-сервера).

Настройка даты и времени вручную:

1 Посмотрите текущие дату и время:

```
hostname# machine show date
```

2 Чтобы изменить часовой пояс:

```
hostname# machine set timezone {<Континент/Пояс> | <UTC>}
```

Название континента и часового пояса должны начинаться с прописной буквы. Например, чтобы установить часовой пояс Москвы:

```
hostname# machine set timezone Europe/Moscow
```

Чтобы посмотреть список всех часовых поясов, введите команду без параметра.

3 Чтобы изменить дату и время:

```
hostname# machine set date <YYYY-MM-DD> <hh:mm:ss>,
```

где `YYYY` — год, `MM` — месяц, `DD` — день, `hh` — часы, `mm` — минуты, `ss` — секунды.

Например:

```
hostname# machine set date 2026-02-22 12:00:00
Do you really wish to change the date?
Continue? [Yes/No]: Yes
```

Настраивайте системную дату, время и часовой пояс только на активном узле кластера.

Настройка подключения к веб-интерфейсу

По умолчанию для подключения с помощью веб-интерфейса используются протокол HTTPS (TCP-порт 8080) и самоподписанный сертификат, который генерируется при инициализации ViPNet Coordinator HW. Самоподписанный сертификат можно перевыпустить, например, если закончился срок его действия:

```
hostname# webui recreate-cert [bits <длина ключа> digest {sha256 | sha384 | sha512} span <срок действия> [subj <subject>]]
```

Длину ключа, алгоритм хэширования и дополнительные параметры, в том числе IP-адреса сетевых интерфейсов и DNS-имена, по которым вы будете подключаться, задайте в соответствии с политиками безопасности вашей организации. Если вы выполните команду без параметров, будут использоваться значения, как при инициализации:

- длина ключа — 2048 бит;
- алгоритм хэширования — sha256;
- срок действия — 1825 дней;
- имя субъекта — имя узла.

Подробнее см. в документе «Справочник команд и конфигурационных файлов».

Вместо самоподписанного сертификата вы можете использовать сертификат, изданный в УЦ:

1 Создайте запрос на сертификат:

```
hostname# service cert request create name <имя сертификата> bits {2048 | 3072 | 4096} digest {sha256 | sha384 | sha512} [subj <subject>]
```



Примечание. Длину ключа, алгоритм хеширования и дополнительные параметры задайте в соответствии с политиками безопасности вашей организации.

В процессе выполнения команды будут запрошены личные данные, необходимые для создания сертификата (страна, город, организация и т.д.).

После выполнения команды будет создан файл запроса и файл с закрытым ключом.

2 Подключите к ViPNet Coordinator HW USB-носитель и экспортируйте запрос на сертификат:

```
hostname# service cert request export <файл запроса>
```

3 Отправьте файл запроса в УЦ, например, InfoTeCS или др.



Примечание. При издании сертификатов учитывайте:

- Сертификаты должны быть подписаны с использованием алгоритма RSA.
- Поддерживается импорт сертификатов в кодировке DER и Base64.
- УЦ должен использовать алгоритм подписи SHA-2.

4 Получите сертификат из УЦ, скопируйте его на USB-носитель и подключите носитель к ViPNet Coordinator HW.

5 Импортируйте сертификат в локальное хранилище сертификатов:

```
hostname# service cert import
```

6 Установите сертификат для службы `WebUI`:

```
hostname# webui https-cert <имя файла сертификата>
```

7 При необходимости измените TCP-порт 8080, используемый по умолчанию:

7.1 Измените TCP-порт:

```
hostname# webui port <номер TCP-порта>
```

7.2 В фильтре `Allow ViPNet WebGUI` измените номер TCP-порта:

7.2.1 удалите существующий фильтр:

```
hostname# firewall vpn delete tcp dport 8080
```

7.2.2 добавьте новый фильтр:

```
hostname# firewall vpn add rule "Allow ViPNet WebGUI" src <ViPNet ID узла |
группа ViPNet ID узлов> dst @local tcp dport <номер TCP-порта> pass
```

7.3 Перезапустите службу `WebUI`:

```
hostname# webui restart
```

Если на шаге 7 вы изменили TCP-порт по умолчанию — в адресной строке браузера укажите: `https://<IP-адрес ViPNet Coordinator HW>:<номер TCP-порта>`.

Чтобы переключить работу службы `WebUI` на HTTP:

```
hostname# webui protocol http
```

Выбор профиля производительности

Для исполнений ViPNet Coordinator HW на аппаратных платформах HW100 N1, N2, N3, Q1, Q2, HW2000 Q4, Q5, HW5000 Q1, Q2 вы можете выбрать профиль производительности обработки трафика сетевых соединений. По умолчанию установлен профиль стандартного распределения ресурсов, обеспечивающий быструю обработку трафика нескольких сетевых соединений.

При выборе профиля высокой производительности для обработки трафика одного соединения происходит перераспределение ресурсов: все аппаратные прерывания от сетевых адаптеров обрабатываются одним ядром процессора, а шифрование выполняется оставшимися ядрами.



Внимание! Если выбран профиль высокой производительности, а фактическое количество сетевых соединений, обрабатываемых ViPNet Coordinator HW, больше одного, то скорость обработки и передачи защищенного трафика будет снижена.

Чтобы выбрать профиль высокой производительности для одного сетевого соединения:

```
hostname# iplir set performance-mode single
```

Выбранный профиль будет применен после перезагрузки ViPNet Coordinator HW.

Чтобы просмотреть текущий профиль производительности:

```
hostname# iplir show performance-mode
```

Если профиль производительности был изменен, но перезагрузка ViPNet Coordinator HW не выполнена, отображается текущий и выбранный профили.

Чтобы выбрать профиль стандартного распределения ресурсов:

```
hostname# iplir set performance-mode multi
```

Установка допустимого времени неактивности сессии пользователя

Допустимое время неактивности сессии пользователя определяет период, по истечении которого сессия будет завершена, если пользователь не выполнял управляющих запросов. Этот параметр одинаков для сессий всех пользователей и синхронизируется между узлами кластера. Значение по умолчанию — 600 секунд.

Для просмотра допустимого времени неактивности сессии выполните:

```
hostname# machine session-inactivity-timeout show
```

Для изменения допустимого времени неактивности сессии выполните:

```
hostname# machine session-inactivity-timeout set <время>,
```

где `<время>` — время неактивности в интервале 60–54000 секунд.

Просмотр активных сессий пользователей

Чтобы просмотреть текущие сессии пользователей, выполните команду:

```
hostname# who
Interface     IP Address  Role          User         Status   Login time
-------------------------------------------------------------------------------
CLI(tty1)     -           Superadmin    admin (you)  Active   17:15:13 05.07.2024
WebUI(eth2)   192.168.1.1 Auditor       Ivanov.I     Inactive 13:25:23 06.07.2024
WebUI(eth3)   192.168.1.9 Netadmin      Petrov.P     Inactive 13:24:23 06.07.2024
WebUI(wlan0)  172.23.0.1  Administrator K.Vasiliev   Active   12:17:55 06.07.2024
```

Сведения о текущих сессиях обновляются каждые 7 секунд. По каждой из них отображаются:

- `Interface` — тип подключения: `CLI` или `WebUI` (интерфейс подключения: `<имя сетевого интерфейса>` или `<имя консоли>`);
- `IP Address` — IP-адрес сетевого интерфейса;
- `Role` — роль пользователя: `Superadmin`, `Administrator`, `Netadmin`, `Auditor`;



Примечание. Для централизованного пользователя, для учетной записи которого в ViPNet Prime одновременно заданы роли **Сетевой администратор шлюза безопасности** и **Аудитор устройств**, в поле Role отображается `merge_utm-whole-read_utm-net-admin`.

- `User` — имя пользователя:
  - для текущей сессии добавляется постфикс `(you)`;
  - для имени централизованного пользователя добавляется префикс `prime/`;
- `Status` — состояние сессии:
  - `Active` — активна;
  - `Inactive` — неактивна, переходит в это состояние, если нет управляющих запросов;
- `Login time` — время и дата начала сессии.

Сессия автоматически завершается, когда время нахождения в состоянии `Inactive` превышает допустимое время неактивности сессии.

Перезагрузка ViPNet Coordinator HW

Чтобы перезагрузить ViPNet Coordinator HW вручную, выполните:

```
hostname# machine reboot
```

При необходимости вы можете включить и настроить перезагрузку ViPNet Coordinator HW по расписанию:

1 Включите перезагрузку:

```
hostname# machine reboot-schedule on
```

2 Задайте расписание перезагрузки, указав время и день недели:

```
hostname# machine reboot-schedule time <время> [day <день>]
```



Внимание! Выполнение команд `machine self-test`, `admin upgrade software` и `machine backup export` по времени не должно совпадать с перезагрузкой по расписанию. Иначе выполнение команд будет прекращено.

Рекомендуется устанавливать время перезагрузки узлов кластера, различающееся не менее чем на 30 минут.

Чтобы просмотреть текущую настройку перезагрузки по расписанию, выполните:

```
hostname# machine reboot-schedule show
```

Установка серийного номера

Начиная с версии 5.2.0 ПО ViPNet Coordinator HW поддерживает серийный номер устройства для исполнений на аппаратных платформах. Для новых устройств номер устанавливается на производстве и не может быть изменен. Для устройств с ПО, обновленных пользователем, номер рекомендуется установить вручную в соответствии с указанным на этикетке устройства.



Внимание! Если серийный номер не отображается после обновления ПО, необходимо установить его вручную в соответствии с указанным на этикетке устройства.

Длина серийного номера: 4–18 символов. Допустимые символы:

- Прописные и строчные буквы латинского алфавита: `A–Z`, `a–z`.
- Арабские цифры: `0–9`.
- Специальный символ `-` .

Используйте серийный номер:

- При обращении в службу поддержки ИнфоТеКС.
- Для инвентаризации оборудования: серийный номер доступен по SNMP (OID .1.3.6.1.4.1.10812.1.10.1. в VIPNET-MIB).

Чтобы проверить серийный номер:

```
hostname# version

Product: ViPNet Coordinator HW

Platform: HW1000C

Serial number: Not set

License: HW1000C

Software version: 5.1.1-4550
```

Если номера нет, вы можете установить его:

```
hostname# serial <серийный номер на этикетке устройства>
```

Просмотр лицензии

Лицензия определяет функциональные характеристики ViPNet Coordinator HW. Чтобы просмотреть сведения об установленных объектах лицензирования:

```
hostname> license
License object      Version  Status  Expiration date Subscription ID
---------------     -------  ------  --------------- ---------------
Coordinator VA1000  5.99     active  2026-03-10             -
VPN                 5.99     active  2026-03-10             -
Failover            5.99     active  2026-03-10             -
DPI                 5.99     active  2026-03-10             -
DPI update          5.99     active  2026-03-10             -
IPS                 5.99     active  2026-03-10             -
IPS update          5.99     active  2026-03-10      4307158/1:5:1:utm_ips_update_1000
IPS MD update       5.99     active  2026-03-10      4308007/1:2:1:utm_md_update_1000
SSL inspection      5.99     active  2026-03-10             -
URL-category update 5.99     active  2026-03-10             -
```

По команде отображаются:

- `License object` — тип объекта лицензирования:
  - Основной объект в соответствии с исполнением ViPNet Coordinator HW, например `Coordinator VA1000`.
  - `DPI` — DPI;
  - `DPI update` — обновление DPI;
  - `VPN` — VPN;
  - `IPS` — предотвращение вторжений IPS;
  - `Failover` — система защиты от сбоев в режиме кластера;
  - `SSL inspection` — SSL/TLS-инспекция транзитного трафика;
  - `IPS update` — обновление базы правил IPS;
  - `IPS MD update` — обновление базы вредоносного ПО;
  - `URL-category update` — обновление базы URL-категорий.
- `Version` — максимальная версия ПО ViPNet Coordinator HW, поддерживаемая лицензией.
- `Status` — статус объекта лицензирования:
  - `active` — действует.

  - `expired` — не действует.
- `Expiration date` — дата окончания действия объекта лицензирования в формате `YYYY-MM-DD`.
- `Subscription ID` — идентификатор лицензии.

Использование резервного раздела в исполнениях с двумя накопителями



Примечание. Резервный раздел не поддерживается в исполнении HW50 с одним дисковым накопителем.

Критически важные файлы ПО ViPNet Coordinator HW автоматически копируются в резервный раздел (`/mnt/reserv`) незагрузочного диска в следующих случаях:

- Успешная проверка целостности файлов при первоначальной установке ПО, обновлении ПО или загрузке ViPNet Coordinator HW.
- Успешное выполнение команды `machine self-test`.
- Обновление справочников и ключей.
- Изменение пароля локальных пользователей.

Резервные копии файлов используются при восстановлении, если обнаружено нарушение целостности файлов ПО (см. Контроль целостности файлов ПО).

В кластере резервные копии файлов синхронизируются.

Сброс к заводским настройкам

В ряде случаев вы не сможете пройти аутентификацию на ViPNet Coordinator HW, чтобы устранить неисправность, например:

- истек срок действия ключей или лицензии в тот момент, когда нет связи с ViPNet Prime;
- некорректно обновлены справочники и ключи;
- утрачен пароль администратора;
- программный сбой, неправильная настройка ПО или аппаратной платформы;
- замена батарейки на аппаратной платформе.

Для продолжения работы выполните сброс к заводским настройкам, при котором удаляются все пользовательские настройки:

1. Включите ViPNet Coordinator HW (виртуальную машину ViPNet Coordinator VA):
2. В окне загрузки выберите сброс к заводским настройкам:
   - Для ViPNet Coordinator HW в зависимости от консоли:
     - при подключении с помощью монитора и клавиатуры — выберите **Factory reset** и нажмите **Enter**;
     - при подключении через консольный порт — выберите **Factory reset/Serial console** и нажмите **Enter**.

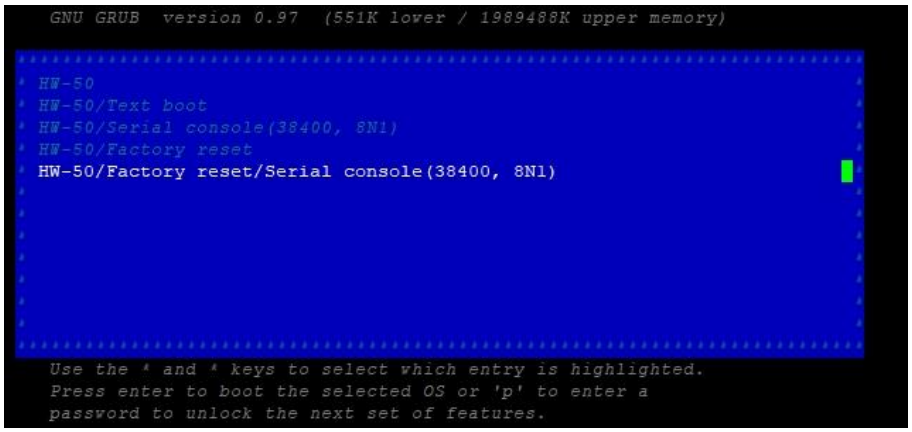


Рисунок 59. Окно загрузки ViPNet Coordinator HW при подключении через консольный порт

   - Для ViPNet Coordinator VA выберите **Factory reset** и нажмите **Enter**.



Рисунок 60. Окно загрузки ViPNet Coordinator VA

3 В строке `Are you sure you want to execute this command and delete key? [Delete/No]` введите `Delete` нажмите **Enter**.

Примечание. Перед сбросом настроек реализована 30-секундная задержка, в течение которой можно отменить сброс, нажав **Ctrl+C**.

4 Нажмите **Enter** для перезагрузки.

После сброса восстановите настройки ViPNet Coordinator HW из резервной копии индивидуальной конфигурации (см. Восстановление из резервной копии индивидуальной конфигурации). Если резервной копии нет, выполните инициализацию ViPNet Coordinator HW (см. «Подготовка к работе», разделы «Инициализация в консольном режиме» или «Инициализация в полноэкранном режиме»).



10

Резервное копирование и восстановление настроек

Управление копиями конфигурации VPN 309

Управление индивидуальной конфигурацией 313

Управление универсальной конфигурацией 318

Управление копиями конфигурации VPN

Копия конфигурации VPN — совокупность настроек ViPNet Coordinator HW. С помощью нее вы можете вернуться к другому состоянию ViPNet Coordinator HW (например, к состоянию до выполнения настроек).

Существуют два вида копий конфигурации VPN:

- частичная — включает в себя конфигурационные файлы ViPNet Coordinator HW: `iplir.conf` и все файлы с именем, соответствующим маске `iplir.conf-<интерфейс или группа интерфейсов>`, `failover.ini`, `mftp.conf`;
- полная — включает в себя все файлы частичной копии конфигурации VPN, а также сетевые фильтры.

Копии конфигурации VPN могут создаваться следующими способами:

- Автоматически (перед обновлением ПО или справочников и ключей). В этом случае по умолчанию создаются частичные копии конфигурации VPN. Вы можете изменить вид копии конфигурации VPN, создаваемой автоматически, или выключить автоматическое создание копий конфигурации VPN, отредактировав значение параметра `confsave` в секции `[upgrade]` в файле `mftp.conf`.

  Максимальное число автоматически созданных копий конфигурации VPN задаётся параметром `maxautosaves` в секции `[upgrade]` (по умолчанию — 10).

  Описание параметров секции `[upgrade]` см. в документе «Справочник команд и конфигурационных файлов», в разделе «Секция [upgrade]».
- Вручную по команде. В этом случае всегда создаётся полная копия конфигурации VPN.

Создание копии конфигурации VPN

Чтобы создать копию текущей конфигурации VPN:

1 Завершите работу служб `iplir`, `failoverd` и `mftpd`:

```
hostname# iplir stop
hostname# failover stop
hostname# mftp stop
```

2 Выполните команду:

```
hostname# vpn config save <имя>
```

и укажите имя копии конфигурации VPN, используя только буквы латинского алфавита, цифры, символы «-» и «_».

3 Если копия конфигурации VPN с выбранным именем уже существует, будет предложено ее перезаписать:

```
Config with name'<имя копии конфигурации VPN>' (version <версия ViPNet Coordinator HW>)
already exists! Overwrite it?
```

   - Чтобы подтвердить перезапись, введите `y` и нажмите **Enter**.
   - Чтобы создать конфигурацию с другим именем, введите `n` и нажмите **Enter**.

4 Запустите службы `iplir`, `failoverd` и `mftpd`:

```
hostname# iplir start
hostname# failover start
hostname# mftp start
```

Просмотр списка копий конфигурации VPN

Чтобы просмотреть список ранее созданных копий конфигурации VPN:

```
hostname# vpn config list
```

Формат отображения списка сохраненных копий: `"Name", Version, Type, saved on Date at Time, loaded at Date-load at Time-load`, где:

- `Name` — имя копии конфигурации VPN.
- `Version` — версия ПО ViPNet Coordinator HW, в которой была создана копия конфигурации VPN (может отсутствовать).
- `Type` — вид копии конфигурации VPN: `full` (полная) или `part` (частичная).
- `Date`, `Time` — дата и время создания копии конфигурации VPN.
- `Date-load`, `Time-load` — дата и время загрузки копии конфигурации VPN.

Если копия конфигурации VPN уже использовалась для восстановления настроек ViPNet Coordinator HW, дата и время использования отображаются после даты и времени создания копии конфигурации VPN (после `loaded`). Если копия конфигурации VPN ни разу не использовалась, после даты и времени создания будет указано `never loaded`.

Восстановление настроек из копии конфигурации VPN

1 Завершите работу служб `failoverd` и `mftpd`:

```
hostname# failover stop
hostname# mftp stop
```

2 Загрузите конфигурацию:

```
hostname# vpn config load <имя копии конфигурации> [<версия ViPNet Coordinator HW>],
```

указав имя копии конфигурации VPN и версию ViPNet Coordinator HW, в которой она была создана. Если имя копии конфигурации VPN состоит из нескольких слов, заключите его в кавычки.

3 Если текущая версия ViPNet Coordinator HW выше версии ViPNet Coordinator HW, в которой была создана выбранная для восстановления настроек копия конфигурации VPN, подтвердите возврат к более ранней версии.

4 Будет предложено сохранить все текущие настройки ViPNet Coordinator HW:

```
Save current configuration?
Continue [Yes/No]?
```

- Чтобы сохранить все текущие настройки, введите `Y` и нажмите **Enter**. Затем укажите имя соответствующей полной копии конфигурации VPN.
- Чтобы не сохранять текущие настройки ViPNet Coordinator HW, введите `n` и нажмите **Enter**.

5 Дождитесь завершения восстановления настроек.

6 Запустите службы `failoverd` и `mftpd`:

```
hostname# failover start
hostname# mftp start
```

Удаление копии конфигурации VPN

Чтобы удалить ненужные копии конфигурации VPN:

```
hostname# vpn config delete <имя копии конфигурации> [<версия ViPNet Coordinator HW>],
```

указав имя копии конфигурации VPN и версию ПО ViPNet Coordinator HW, в которой она была создана.

Чтобы не писать имя копии конфигурации VPN полностью или удалить сразу несколько копий конфигурации VPN, имена которых содержат определенные символы, вместо имени укажите маску имени, используя символ `*`.

Например, чтобы удалить все копии конфигурации VPN, созданные автоматически в августе 2026 года:

```
hostname# vpn config delete rollback-2026-08-*
```

Если несколько копий конфигурации VPN имеют имя, соответствующее указанной маске, то будет отображено количество таких копий конфигурации VPN:

```
<количество копий конфигурации VPN> configs match that pattern. Delete? [Yes/No]
```

Выполните одно из действий:

- Чтобы подтвердить удаление всех копий конфигурации VPN, введите `y` и нажмите **Enter**.
- Чтобы отменить удаление всех копий конфигурации VPN, введите `n` и нажмите **Enter**.

Чтобы удалить копии конфигурации VPN, созданные в определенной версии VPN-компонента ViPNet Coordinator HW, укажите номер этой версии:

```
hostname# vpn config delete rollback-2026-08-* 4.5.2
```

Управление индивидуальной конфигурацией

Индивидуальная конфигурация позволяет осуществлять возврат настроек ViPNet Coordinator HW к состоянию, которое было на момент её создания. Файл индивидуальной конфигурации имеет расширение `ecf` и зашифрован на ключе обмена, который используется для защиты соединения ViPNet Coordinator HW с ViPNet Prime. Чтобы восстановить настройки из файла индивидуальной конфигурации, на ViPNet Coordinator HW должен быть установлен тот же ключ обмена, который использовался при экспорте конфигурации. Если ключ обмена был обновлён на ViPNet Coordinator HW, создайте новую резервную копию индивидуальной конфигурации.

Вы можете использовать копии индивидуальных конфигураций:

- Для восстановления настроек ViPNet Coordinator HW в случае сбоя или некорректного обновления ПО.
- При замене неисправного ViPNet Coordinator HW, в том числе и в кластере (см. Замена неисправного узла кластера).

Индивидуальная конфигурация содержит:

- настройки защищенной сети;
- настройки сетевых интерфейсов;
- настройки маршрутизации и статические маршруты, если такие созданы;
- сетевые фильтры и правила трансляции адресов;
- настройки параметров обработки прикладных протоколов;
- настройки системы защиты от сбоев;
- настройки транспортного сервера MFTP;
- журналы и настройки протоколирования;
- настройки дополнительных служб (DHCP-сервера и других);
- настройки взаимодействия с ИБП;
- настройки туннелирования;
- текущие ключи для соединений по протоколу SSH2.

Резервное копирование индивидуальной конфигурации

Резервное копирование индивидуальной конфигурации может быть выполнено:

- По расписанию — на сервер ViPNet Prime один раз в сутки.
- Вручную — на сервер ViPNet Prime или USB-носитель.

По умолчанию резервное копирование по расписанию включено и выполняется в случайное время из интервала 21.00–23.00. Чтобы настроить расписание, задайте время одним из способов:

- Укажите точное время:

  `hostname# machine backup schedule <время>`

  Время задается в формате: `hh:mm`, где, `hh` — часы (24-часовой формат), `mm` — минуты.

- Укажите интервал времени:

  `hostname# machine backup schedule <начало интервала>-<конец интервала>`

  В этом случае время следующего резервного копирования выбирается случайным образом из указанного диапазона с округлением минут.

Чтобы отключить резервное копирование по расписанию, выполните:

```
hostname# machine backup off
```

Чтобы создать резервную копию на сервере ViPNet Prime или USB-носителе вручную, выполните:

```
hostname# machine backup export {server | usb)
```

Независимо от того, как была создана резервная копия, на сервере ViPNet Prime хранится только последняя копия конфигурации — каждая последующая копия затирает предыдущую.

Примечание. На время резервного копирования создается сетевой фильтр, разрешающий подключение к серверу ViPNet Prime и останавливаются службы `vpn` и `mftp`.

По завершении копирования фильтр будет удален, а службы будут запущены заново.

Шаблон имени файла индивидуальной конфигурации: `<имя сетевого узла>-<время создания файла>.ecf`.

Формат времени создания файла: `YYYYMMDDTHHMMSSZ`, где `YYYY` — год, `MM` — месяц, `DD` — день, `HH` — час, `MM` — минуты, `SS` — секунды.

Чтобы просмотреть настройки резервного копирования:

```
hostname> machine show backup
```

На экран будут выведены:

- Статус резервного копирования по расписанию: включено, выключено или недоступно.
- Информация о последнем резервном копировании на сервер ViPNet Prime.
- Время следующего резервного копирования по расписанию.

Восстановление из резервной копии индивидуальной конфигурации



Внимание! Восстановление настроек из резервной копии индивидуальной конфигурации возможно, если с момента создания этой копии на ViPNet Coordinator HW не были обновлены ключи обмена.

Если ViPNet Coordinator HW находится в работоспособном состоянии, вы можете восстановить настройки из резервной копии индивидуальной конфигурации:

1 Запишите копию индивидуальной конфигурации на USB-носитель.

2 Выполните импорт конфигурации:

```
hostname# machine config import
```

2.1 Подключите USB-носитель к ViPNet Coordinator HW.

2.2 Введите номер файл конфигурации из списка и нажмите **Enter**.

3 Отключите USB-носитель и перезагрузите ViPNet Coordinator HW.

Если работоспособность ViPNet Coordinator HW нарушена, восстановите настройки из копии индивидуальной конфигурации в ходе инициализации ViPNet Coordinator HW:

1 Получите у администратора защищённой сети новый дистрибутив ключей для вашего ViPNet Coordinator HW.



Примечание. Если у вас есть старый дистрибутив ключей (полученный ранее), вы можете использовать его, если выполняются условия:

- Дистрибутив ключей был создан после того, как ViPNet Coordinator HW был впервые введён в эксплуатацию и подключён к ViPNet Prime.
- С момента создания этого дистрибутива ключей на ViPNet Coordinator HW не был обновлён ключ обмена для связи с ViPNet Prime и не был изменён способ аутентификации. Дату последней установки (обновления) ключа обмена вы можете просмотреть по команде `iplir show key-info` (см. атрибут `Key effective date`).

2 Запишите на USB-носитель или CD-диск:

2.1 Копию индивидуальной конфигурации.

2.2 Дистрибутив ключей ViPNet Coordinator HW.

3 Удалите ключи ViPNet Coordinator HW:

```
hostname# admin remove keys
```

В строке `Are you sure you want to execute this command? Continue? [Yes/No]` введите `Yes` и нажмите **Enter**.

4 После перезагрузки ViPNet Coordinator HW выполните шаги 1–14 сценария инициализации в одном из режимов (см. документ «Подготовка к работе», разделы «Инициализация в консольном режиме» или «Инициализация в полноэкранном режиме»).

5 На шаге 15 сценария инициализации выберите загрузку конфигурации:

- В строке `Select the setup method` введите `2` и нажмите **Enter**.
- В окне **Please select further setup method** выберите **Load appliance configuration file** и нажмите **Next**.

6 Выберите способ загрузки конфигурации:

- В строке `Would you like to install appliance configuration file from USB or CD storage device? [u/c]` введите:
  - `u` — для загрузки конфигурации с USB-носителя.
  - `c` — для загрузки конфигурации с CD-диска.
- В окне **Would you like to start installing appliance configuration from USB or CD storage device?** выберите способ и нажмите **Next**.

7 Подключите USB-носитель или CD-привод к ViPNet Coordinator HW; вставьте CD-диск в привод.

8 Чтобы найти файлы `ecf`, нажмите **Enter** или **Next**.

- Если на USB-носителе или CD-диске обнаружен только один файл `ecf`, то он будет выбран для загрузки.
- Если обнаружено несколько файлов `ecf`:
  - Введите номер файла из списка `Found several appliance configuration files` и нажмите **Enter**.
  - В окне **Found several appliance initialization files. Please choose one appliance configuration file** выберите файл в списке и нажмите **Next**.

Примечание. В списке указываются имена и идентификаторы узлов сети ViPNet, которым соответствуют файлы `ecf`.

Если в консольном режиме найдено больше 20 файлов, список выводится постранично.

В полноэкранном режиме длинные имена файлов могут быть отображены не полностью. Чтобы просмотреть полное имя, выберите файл в списке — его имя будет отображено под окном мастера.

Дождитесь сообщения о восстановлении индивидуальной конфигурации.

9 Откажитесь от изменения настроек аутентификации (изменения пароля и инициализации USB-токена локального администратора `admin`):

- В строке `Local authentication settings were imported from appliance configuration file. Overwrite them? [Yes/No]` введите `No` и нажмите **Enter**.
- В окне **Local authentication settings were imported from appliance configuration file. Overwrite them?** нажмите **No**.

10 Перезагрузите ViPNet Coordinator HW:

- В строке `For the proper application of the recovered settings, you must reboot HW appliance. Do you want to reboot now? [Yes/No]` введите `y` и нажмите **Enter**.
- В окне **For the proper application of the recovered settings, you must reboot HW appliance** нажмите **Reboot**.

Если при инициализации вы использовали старый дистрибутив ключей, обновление справочников и ключей произойдёт автоматически через несколько минут. Администратор ViPNet Prime также может сделать это вручную.

Управление универсальной конфигурацией

Универсальная конфигурация включает три группы настроек ViPNet Coordinator HW:

- Настройки межсетевого экрана:
  - Сетевые фильтры.
  - Правила трансляции адресов (NAT).
  - Группы объектов.
- Настройки сетевых интерфейсов:
  - Состояние интерфейса (`on`/`off`).
  - Класс интерфейса (`access`, `trunk`, `slave`).
  - IP-адрес и маска сети, или настройки получения IP-адреса и других параметров по DHCP.
  - Дополнительные IP-адреса (`alias`).
  - Режим работы агрегированного интерфейса (`balance-rr`, `balance-xor`, `balance-tlb`, `802.3ad`, `active-backup`, `broadcast`).
  - Настроенные VLAN.
- Настройки маршрутизации:
  - Маршрут по умолчанию.
  - Статические маршруты.
  - Административная дистанция и вес маршрута.
  - Административная дистанция и вес маршрутов, полученных по DHCP.
  - Настройка метрики для маршрутов PPP-протокола.
  - Настройки маршрутизации по протоколу OSPF (состояние службы, области маршрутизации и подсети, приоритет интерфейсов, настройка перераспределения статических маршрутов и динамических маршрутов, полученных по DHCP, идентификатор маршрутизатора, настройки аутентификации).
  - Настройки DGD (состояние, перечень шлюзов и метод проверки доступности, правила переключения политик маршрутизации).
  - Настройки Policy Routing (политики маршрутизации и активная на момент обновления политика).

Кроме этого, универсальная конфигурация содержит сведения о продукте, платформе и версии ПО, например: HW-VA, VA, 5.1.0. Универсальная конфигурация позволяет переносить настройки с ViPNet Coordinator HW различных исполнений и версий ПО (4.3.2 и 4.5.x), а также ViPNet xFirewall

5.x. Файл универсальной конфигурации имеет расширение `vbe` и зашифровывается на пароле при экспорте конфигурации.

Экспорт универсальной конфигурации

Чтобы экспортировать универсальную конфигурацию на USB-носитель:

1. Выполните:

   ```
   hostname# machine config export usb
   ```

2. Добавьте описание конфигурации:

   2.1 В строке `Do you want to add configuration description [Yes/No]` введите `y` и нажмите **Enter**.

   2.2 В строке `Description` введите текст описания (до 512 символов UTF-8) и нажмите **Enter**.

3. В строке `Enter password for encryption` введите пароль, на котором будет зашифрован файл конфигурации, и нажмите **Enter**. Разрешённые символы: `A–Z`, `a–z`, `0–9`, специальные символы. Длина пароля — от 8 до 31 символа.

4. При появлении сообщения `Insert USB drive with at least 1.7 MB free space and press Enter` подключите USB-носитель к ViPNet Coordinator HW и нажмите **Enter**.

5. Дождитесь завершения экспорта и отключите USB-носитель.

Шаблон имени файла универсальной конфигурации: `<имя сетевого узла>-<время создания файла>.vbe`.

Формат времени создания файла: `YYYYMMDDTHHMMSSZ`, где `YYYY` — год, `MM` — месяц, `DD` — день, `HH` — час, `MM` — минуты, `SS` — секунды. Время записывается в системе UTC.

Импорт настроек универсальной конфигурации

Чтобы импортировать настройки универсальной конфигурации:

1. Запишите файл универсальной конфигурации на USB-носитель.

2. Выполните импорт настроек:

   ```
   hostname# machine config import
   ```

   2.1 Подключите USB-носитель к ViPNet Coordinator HW.

   2.2 Введите номер файла конфигурации из списка обнаруженных на USB-носителе и нажмите **Enter**.

   2.3 В строке `Enter configuration password` введите пароль и нажмите **Enter**.

   2.4 Выберите импортируемые настройки универсальной конфигурации и способ их импорта (`append` — добавить или `replace` — заменить):

2.4.1 В строке `Select which settings you want to import: Firewall [y/n]` введите `y` и нажмите **Enter**.

2.4.2 В строке `Append firewall settings or replace them? [a/r]` введите `a` или `r` и нажмите **Enter**.

2.4.3 В строке `Network interface settings [y/n]` введите `y` и нажмите **Enter**.

2.4.4 В строке `Routing settings [y/n]` введите `y` и нажмите **Enter**.

2.4.5 В строке `Append routing settings or replace them? [a/r]` введите `a` или `r` и нажмите **Enter**.

3 Отключите USB-носитель и перезагрузите ViPNet Coordinator HW.

Также вы можете импортировать настройки универсальной конфигурации в ходе инициализации ViPNet Coordinator HW:

1 Получите у администратора защищённой сети новый дистрибутив ключей для вашего ViPNet Coordinator HW.



Примечание. Если у вас есть старый дистрибутив ключей (полученный ранее), вы можете использовать его, если выполняются условия:

- Дистрибутив ключей был создан после того, как ViPNet Coordinator HW был впервые введён в эксплуатацию и подключён к ViPNet Prime.
- С момента создания этого дистрибутива ключей на ViPNet Coordinator HW не был обновлён ключ обмена для связи с ViPNet Prime и не был изменён способ аутентификации. Дату последней установки (обновления) ключа обмена вы можете просмотреть по команде `iplir show key-info` (см. атрибут `Key effective date`).

2 Запишите на USB-носитель или CD-диск:

2.1 Файл универсальной конфигурации.

2.2 Дистрибутив ключей ViPNet Coordinator HW.

3 Выполните шаги 1–14 сценария инициализации в одном из режимов (см. документ «Подготовка к работе», разделы «Инициализация в консольном режиме» или «Инициализация в полноэкранном режиме»).

4 На шаге 15 сценария инициализации выберите загрузку конфигурации:

- В строке `Select the setup method` введите `2` и нажмите **Enter**.
- В окне **Please select further setup method** выберите **Load appliance configuration file** и нажмите **Next**.

5 Выберите способ загрузки конфигурации:

- В строке `Would you like to install appliance configuration file from USB or CD storage device? [u/c]` введите:
  - `u` — для загрузки конфигурации с USB-носителя.
  - `c` — для загрузки конфигурации с CD-диска.

- В окне **Would you like to start installing appliance configuration from USB or CD storage device?** выберите способ и нажмите **Next**.

6 Подключите USB-носитель или CD-привод к ViPNet Coordinator HW; вставьте CD-диск в привод.

7 Чтобы найти файлы `vbe`, нажмите **Enter** или **Next**.

- Если на USB-носителе или CD-диске обнаружен только один файл `vbe`, то он будет выбран для загрузки.
- Если обнаружено несколько файлов `vbe`:
  - Введите номер файла из списка `Found several appliance configuration files` и нажмите **Enter**.
  - В окне **Found several appliance initialization files. Please choose one appliance configuration file** выберите файл в списке и нажмите **Next**.



Примечание. В списке указываются имена и идентификаторы узлов сети ViPNet, которым соответствуют файлы `ecf`.

Если в консольном режиме найдено больше 20 файлов, список выводится постранично.

В полноэкранном режиме длинные имена файлов могут быть отображены не полностью. Чтобы просмотреть полное имя, выберите файл в списке — его имя будет отображено под окном мастера.

8 Введите пароль доступа к выбранной конфигурации:

- В строке `Enter configuration password` введите пароль и нажмите **Enter**.
- В окне **Enter configuration password** введите пароль и нажмите **Enter**.

9 Выберите импортируемые настройки:

9.1 Межсетевого экрана:

- В строке `Firewall [y/n]` введите `y` или `n` и нажмите **Enter**.
- В окне **Would you like to import firewall settings?** выберите **Import** или **Skip** и нажмите **Next**.



Примечание. Особенности импорта настроек МЭ из ViPNet xFirewall версий 5.6.0 и выше см. в примечании на шаге 2.4.1 предыдущего сценария.

9.2 Сетевых интерфейсов:

- В строке `Network interface settings [y/n]` введите `y` или `n` и нажмите **Enter**.
- В окне **Would you like to import network settings?** выберите **Import** или **Skip** и нажмите **Next**.

9.3 Маршрутизации:

- В строке `Routing settings [y/n]` введите `y` или `n` и нажмите **Enter**.
- В окне **Would you like to import routing settings?** выберите **Import** или **Skip** и нажмите **Next**.

10 Задайте пароль суперадминистратора `admin`:

- В строке `Enter new superadmin password` введите и подтвердите пароль, затем нажмите **Enter**.
- В окне **To access the device, set the superadministrator password** введите и подтвердите пароль, затем нажмите **Next**.

11 Дождитесь завершения импорта настроек и перезагрузите ViPNet Coordinator HW:

- В строке `For the proper application of the recovered settings, you must reboot HW appliance. Do you want to reboot now? [Yes/No]` введите `y` и нажмите **Enter**.
- В окне **For the proper application of the recovered settings, you must reboot HW appliance** нажмите **Reboot**.

Если при инициализации вы использовали старый дистрибутив ключей, обновление справочников и ключей произойдёт автоматически через несколько минут. Администратор ViPNet Prime также может сделать это вручную.

11

Обеспечение отказоустойчивости

Настройка системы защиты от сбоев 324

Просмотр информации о работе системы защиты от сбоев 340

Подключение ViPNet Coordinator HW к ИБП 344

Управление режимом производительности 347

Настройка системы защиты от сбоев

Назначение системы защиты от сбоев

Система защиты от сбоев предназначена для контроля работоспособности ПО ViPNet Coordinator HW и создания отказоустойчивого решения на базе двух ViPNet Coordinator HW. Система может работать в одиночном режиме или в режиме кластера.

Параметры работы системы защиты от сбоев задаются в файле `failover.ini`. Подробнее см. «Справочник команд и конфигурационных файлов», раздел «Файл failover.ini».

Работа системы защиты от сбоев в одиночном режиме

По умолчанию система защиты от сбоев работает в одиночном режиме и обеспечивает:

- контроль собственной работоспособности;
- контроль работоспособности запущенных служб и драйверов ViPNet Coordinator HW, ведение статистики использования системных ресурсов;
- контроль сбоев при обработке IP-пакетов VPN-драйвером.

В состав системы защиты от сбоев входят watchdog-драйвер `itcswd` и служба `failoverd`. При загрузке системы сначала запускается watchdog-драйвер, а затем служба `failoverd`, которая запускает остальные службы и драйверы. Watchdog-драйвер `itcswd` и служба `failoverd` работают в фоновом режиме.

Watchdog-драйвер контролирует работоспособность службы `failoverd`. Если в настройках включен механизм регистрации служб и драйверов, `failoverd` периодически посылает драйверу сообщения для подтверждения своей работоспособности. Если по истечении определенного времени от службы не будет получено ни одного сообщения, драйвер инициирует перезагрузку системы. Подробнее см. в документе «Справочник команд и конфигурационных файлов», в описании секции `[misc]` файла `failover.ini`.

Служба `failoverd` контролирует работоспособность остальных служб и драйверов ViPNet Coordinator HW. В процессе своей работы каждая из них периодически посылает службе `failoverd` сообщения для подтверждения своей работоспособности. Если по истечении определенного времени от какой-либо службы не будет получено ни одного сообщения или от VPN-драйвера будет получено сообщение с кодом ошибки обработки IP-пакетов, служба `failoverd` считает, что произошел сбой и пытается завершить работу этой службы. Если завершить работу корректно не удается, служба `failoverd` производит принудительный перезапуск. Если после пяти перезапусков подряд, работу контролируемой службы восстановить не удалось, она считается неработоспособной, и `failoverd` инициирует перезапуск системы.

Работа системы защиты от сбоев в режиме кластера

Система защиты от сбоев позволяет объединить в кластер два ViPNet Coordinator HW или ViPNet Coordinator VA с одинаковой платформой и версией ПО:

- активный узел — выполняет функции ViPNet Coordinator HW;
- пассивный узел — находится в режиме ожидания.

В случае нарушения работоспособности активного узла, пассивный узел переключается в активный режим и выполняет функции сбойного узла, а сбойный узел переходит в пассивный режим.



Внимание! В режиме кластера не поддерживаются модули Wi-Fi и 3G. Отключите их до объединения узлов в кластер.

Интерфейсы кластера:

- Резервируемый интерфейс — сетевой интерфейс узла кластера, который резервируется на другом узле кластера.
- Интерфейс кластера — резервируемый интерфейс активного узла кластера.

  Каждый интерфейс кластера имеет один IP-адрес, по которому кластер доступен для других узлов. Этот IP-адрес всегда принадлежит узлу, работающему в данный момент в активном режиме. Резервируемые интерфейсы узла, работающего в пассивном режиме, не имеют IP-адресов, по которым другие узлы могли бы установить соединение с кластером. При переключении узлов кластера, резервируемые интерфейсы узла, который переходит в активный режим, получают IP-адреса интерфейсов кластера.
- Интерфейс синхронизации — сетевой интерфейс узла кластера, который подключен напрямую к интерфейсу другого узла кластера. Через интерфейс синхронизации передаются данные между узлами кластера:
  - Пакеты синхронизации, содержащие информацию о текущем режиме работы каждого узла кластера. Обмен пакетами синхронизации позволяет избежать ситуации, когда оба узла кластера работают в активном режиме, например, в случае практически одновременного запуска.
  - Копии принятых и готовых к отправке MFTP-конвертов.
  - Копии конфигурационных файлов и журналов. Перечень файлов, подлежащих передаче, задается в секции `[sendconfig]` конфигурационного файла `failover.ini`.
  - Справочники, ключи и лицензии.

  Каждая группа данных передается в открытом виде путем копирования во временный каталог с последующей проверкой, что все файлы группы успешно переданы.

Внимание! Не синхронизируются при переключении узлов кластера:

- сессии, к которым применяется правило трансляции адреса источника;
- журнал IP-пакетов и его настройки;
- BGP-сессии (время восстановления BGP-сессий и построения BGP-маршрутов при переключении узлов кластера составляет от 1 до 3 минут).

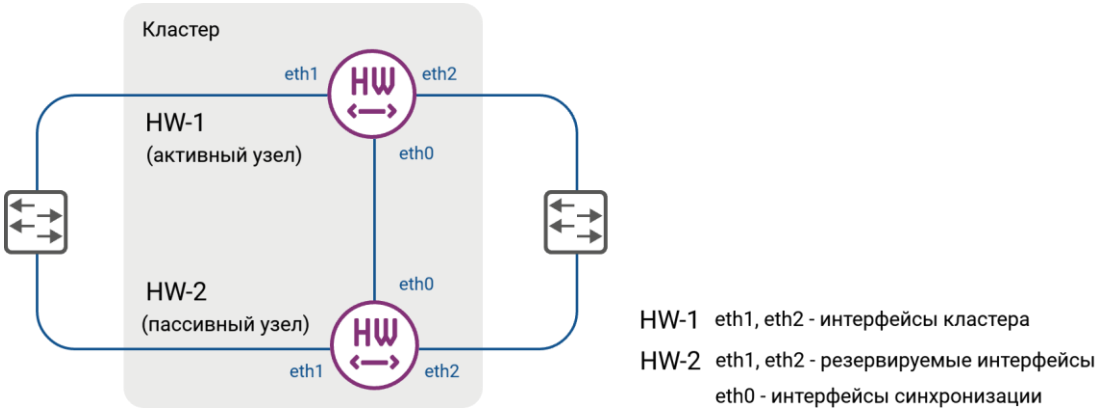


Рисунок 61. Схема кластера

В процессе работы кластера пассивный узел контролирует работоспособность активного узла кластера, а активный узел контролирует работоспособность своих интерфейсов.

Проверка работоспособности активного узла кластера:

1 Пассивный узел периодически посылает ARP-запрос на обнаружение дублирующего IP-адреса в режиме DAD, проверяя присутствует ли в сети интерфейс с IP-адресом активного узла, и ожидает ARP-ответ.

Внимание! Увеличение времени ожидания ответа на ARP-запрос приведет к увеличению времени перехода пассивного узла в активный режим.

2 В случае отсутствия ответа, пассивный узел кластера переключается в активный режим, и каждый его резервируемый интерфейс получает IP-адрес для работы в активном режиме. При этом активный узел кластера переходит в пассивный режим, а на его резервируемых интерфейсах настроенные IP-адреса сбрасываются.

Примечание. Пассивный узел следит за состоянием интерфейса синхронизации. Это позволяет обнаружить потерю питания на активном узле и быстрее переключить кластер.

1 При потере сигнала на интерфейсе синхронизации пассивный узел проверяет присутствие в сети интерфейсов с IP-адресами активного узла кластера.

2 Если ни один из резервируемых интерфейсов активного узла не отвечает, пассивный узел переходит в активный режим сразу, без использования счетчика сбоев.

Проверка работоспособности интерфейсов активного узла кластера:

1 Активный узел периодически анализирует IP-трафик, проходящий через каждый из своих резервируемых интерфейсов.

2 Если за определенный период времени не зафиксировано ни одного отправленного и принятого IP-пакета, производится дополнительная проверка — через каждый интерфейс посылаются эхо-запросы стабильным объектам сети (например, маршрутизаторам).

3 В случае отсутствия ответов на эхо-запросы, счетчик отказов для соответствующего интерфейса увеличивается на единицу. Если получен хотя бы один ответ или зафиксирован трафик на интерфейсе, счетчик отказов сбрасывается.

4 При достижении счетчиком порогового значения интерфейс считается неработоспособным, и активный узел переключается в пассивный режим, а пассивный узел становится активным.



Примечание. Эхо-запросы для контроля работоспособности сетевых интерфейсов активного узла могут посылаться постоянно (подробнее см. в описании конфигурационного файла `failover.ini` в документе «Справочник команд и конфигурационных файлов»).

Для опроса IP-адресов активного узла и обмена данными между активным и пассивным узлом на обоих узлах кластера автоматически создаются разрешающие сетевые фильтры.

Развертывание кластера

1 Убедитесь, что оба ViPNet Coordinator HW кластера имеют одинаковую платформу и версию ПО:

```
hostname# version
```



Примечание. Если вы развертываете кластер на базе ViPNet Coordinator VA, оба узла должны иметь одинаковые параметры эмулируемого аппаратного обеспечения: количество процессоров, ОЗУ и сетевых интерфейсов.

2 Отключите от локальной сети оба ViPNet Coordinator HW.

3 Если на ViPNet Coordinator HW были установлены справочники и ключи, удалите их:

```
hostname# admin remove keys
```

4 Выполните инициализацию обоих ViPNet Coordinator HW, используя один и тот же дистрибутив ключей.

5 На каждом ViPNet Coordinator HW выберите резервируемые интерфейсы и настройте их: задайте статические IP-адреса, установите класс access (см. Настройка сетевых интерфейсов Ethernet) и включите интерфейсы. Назначение IP-адресов по протоколу DHCP не допускается.

6 На каждом ViPNet Coordinator HW выберите интерфейс синхронизации.



Примечание. В качестве интерфейса синхронизации рекомендуется выбирать физические проводные интерфейсы (`eth`) класса `access`.

Соедините интерфейсы синхронизации обоих ViPNet Coordinator HW с помощью Ethernet-кабеля и настройте их: задайте статические IP-адреса и включите интерфейсы. IP-адреса интерфейсов синхронизации должны принадлежать одной сети.



Внимание! IP-адрес интерфейса синхронизации на каждом из узлов кластера не должен совпадать с IP-адресами узлов защищённой сети, иначе трафик, идущий на эти адреса, будет блокироваться. Если необходимо использовать одинаковые адреса, для разрешения конфликта рекомендуется настроить видимость соответствующих узлов защищённой сети по виртуальным адресам (см. Настройка виртуальных IP-адресов).

7 Выберите один или несколько стабильных объектов сети, например, маршрутизатор, которые будут использоваться для проверки работоспособности интерфейсов активного узла кластера.



Внимание! Настройку сетевых служб необходимо выполнять после развертывания кластера и запуска системы защиты от сбоев. Настройка выполняется на активном узле кластера.

На каждом из ViPNet Coordinator HW:

1 Завершите работу службы системы защиты от сбоев:

```
hostname# failover stop
```

2 Откройте файл `failover.ini` для редактирования:

```
hostname# failover config edit
```

3 Для каждого резервируемого интерфейса задайте следующие параметры в секции `[channel]`. Если для нужного интерфейса секция отсутствует, создайте ее:



Внимание! Для каждой пары резервируемых интерфейсов, подключенных к одной сети, значения параметров секции `[channel]` должны совпадать.

- `device` — имя сетевого интерфейса.

  На обоих узлах кластера для доступа к одной и той же сети должны использоваться сетевые интерфейсы с одинаковыми именами.

- `activeip` — IP-адрес с префиксом маски, который присваивается сетевому интерфейсу, когда узел работает в активном режиме.

- `testip` — IP-адрес маршрутизатора или другого стабильного узла сети, находящегося в одной подсети с IP-адресом из параметра `activeip`, к которому будут посылаться эхо-запросы для проверки работоспособности интерфейса.



Примечание. В качестве `testip` не рекомендуется задавать адрес интерфейса «внутренней петли» (loopback), например, `127.0.0.1`, так как в этом случае реальной проверки работоспособности сетевого интерфейса не производится.

Для каждого резервируемого интерфейса вы можете указать несколько параметров `testip`. В этом случае сбоем интерфейса будет считаться ситуация, когда ни от одного из заданных IP-адресов не будет получено ответа.

Например, чтобы эхо-запросы отправлялись на IP-адреса 192.168.10.1 и 192.168.20.1, добавьте строки:

```
testip = 192.168.10.1
testip = 192.168.20.1
```



Внимание! Если в кластере используется L2OverIP и требуется проверять состояние его интерфейса, то в качестве тестового IP-адреса для этого интерфейса необходимо задать адрес из локального сегмента, а также выключить блокирование одноадресных Ethernet-кадров с неизвестным MAC-адресом получателя командой `iplir set l2overip unsolicited-frames broadcast`. Не рекомендуется указывать для рабочего интерфейса L2OverIP тестовый IP-адрес в удаленном сегменте.

- `testdevice` — имя сетевого интерфейса, для которого необходимо контролировать состояние соединения. При потере физического соединения на указанном интерфейсе будет выполнено переключение узлов кластера.

  В качестве сетевого интерфейса в параметре `testdevice` вы можете указать только физический интерфейс. Не допускается задавать виртуальные, агрегированные или VLAN интерфейсы, а также `localhost`. При этом вы можете указать физический интерфейс, который задан как trunk-интерфейс для VLAN.

  Параметр `testdevice` необязательный. В каждой секции `[channel]` вы можете задать только один параметр `testdevice`.



Внимание!

- Не изменяйте значение параметра `testdevice`, когда служба `failoverd` запущена в режиме кластера. Иначе это будет воспринято системой как потеря физического соединения и приведет к переключению узлов кластера.
- В параметре `testdevice` указывайте только те сетевые интерфейсы, состояния которых действительно должны контролироваться для работоспособности кластера.

- `ident` — текстовая строка, идентифицирующая сетевой интерфейс. Для интерфейсов, подключенных к одинаковым сетям, параметры `ident` должны совпадать. По этому параметру система защиты от сбоев определяет интерфейсы, которые выполняют одинаковые функции на узлах кластера.
- `checkonlyidle` — проверка только неактивных резервируемых интерфейсов:
  - `yes` (по умолчанию) — активный узел посылает эхо-запросы на сетевые узлы `testip`, только если за период опроса IP-адресов на резервируемых интерфейсах не было ни входящих, ни исходящих пакетов;
  - `no` — эхо-запросы на узлы `testip` посылаются всегда.

  При `checkonlyidle = yes`:

- снижается нагрузка на активный узел кластера и сетевые узлы `testip`, уменьшается служебный трафик;
- проверяется только сетевая активность на резервируемых интерфейсах, поэтому сетевые узлы `testip` должны быть подключены к резервируемым интерфейсам напрямую, иначе при обрыве соединения на промежуточном коммутационном оборудовании не произойдет переключение узлов кластера.

При `checkonlyidle = no`:

- повышается нагрузка на активный узел кластера и сетевые узлы `testip`, возрастает служебный трафик;
- проверяется доступность сетевых узлов `testip`, а не сетевая активность на резервируемых интерфейсах, поэтому используйте это значение параметра, если между резервируемыми интерфейсами и сетевыми узлами `testip` установлено промежуточное коммутационное оборудование или резервируются агрегированные интерфейсы.

- `usevirtualmac` — использование виртуальных MAC-адресов для сетевых интерфейсов кластера, заданных в данной секции `[channel]`:
  - `yes` — использовать виртуальные MAC-адреса для сетевых интерфейсов;
  - `no` (по умолчанию) — не использовать виртуальные MAC-адреса для сетевых интерфейсов.

  Использование виртуальных MAC-адресов позволяет ускорить восстановление связи с координатором после переключения узлов кластера. Виртуальные MAC-адреса для сетевых интерфейсов кластера генерируются на основе значения параметра `virtualmacprefix` в секции `[network]`.

Примечание. Виртуальные MAC-адреса не могут назначаться для агрегированных (например, `bond1`) и виртуальных (например, eth0:1) сетевых интерфейсов.

---

4 В секции `[misc]` задайте значение параметра `syncconnections`:

- `yes` — синхронизация соединений при работе в кластере включена. В этом случае при переключении узлов кластера соединения, открытые на активном узле до момента переключения, продолжат работу на пассивном узле. При этом не будут синхронизированы следующие типы соединений:
  - открытые сессии разрешения доменных имен;
  - защищенные соединения по TCP-туннелям;
  - локальные соединения (открытые и защищенные соединения, в которых ViPNet Coordinator HW является источником или назначением);
  - соединения, использующие прикладные протоколы.

  После переключения узлов кластера связь по указанным типам соединений может быть прервана.

- `no` (по умолчанию) — синхронизация соединений при работе в кластере выключена.

Для синхронизации соединений параметра `syncconnections` должен иметь значение `yes` на обоих узлах кластера.

5 Для исполнений ViPNet Coordinator HW на аппаратных платформах рекомендуется увеличить значение MTU на интерфейсах синхронизации. Для этого в секции `[misc]` задайте значение параметра `interclustermtu = 9000`.

6 В секции `[sendconfig]` задайте следующие параметры для синхронизации настроек между узлами кластера:

- `device` — имя интерфейса синхронизации;
- `activeip` — IP-адрес интерфейса синхронизации другого узла кластера.

7 Параметры секций `[sendconfig]` и `[network]` по умолчанию обеспечивают оптимальную скорость переключения узлов кластера. Но вы можете изменить, чтобы учесть особенности работы вашей сети.

8 Сохраните изменения (**Ctrl+O**) и закройте редактор (**Ctrl+X**).

9 Переведите систему защиты от сбоев в режим кластера:

```
hostname# failover config mode cluster
```

10 Подключите оба ViPNet Coordinator HW к локальной сети.

11 Настройте коммутационное оборудование, подключаемое к кластеру.

12 Проверьте связь с каждым сетевым узлом `testip`:

```
hostname> inet ping <testip>
```



Внимание! Отсутствие связи со всеми IP-адресами, указанными в параметрах `testip` хотя бы одной секции `[channel]`, может привести к циклическому переключению узлов кластера после запуска системы защиты от сбоев.

---

13 Запустите систему защиты от сбоев:

```
hostname# failover start
```

ViPNet Coordinator HW, на котором служба системы защиты от сбоев будет запущена первым, начнет работать как активный узел кластера. Вы можете принудительно задать режим каждого узла кластера при запуске службы:

```
hostname# failover start {active | passive}
```

Если активный узел кластера уже запущен, перед запуском службы на втором узле кластера, сначала проверьте доступность активного узла:

```
hostname> failover show active-mac-address
```

В случае успешной проверки будет выведен список активных сетевых интерфейсов кластера, заданных параметрами `device` и `activeip` секции `[channel] failover.ini`, и их MAC-адреса, например:

```
Interface IP-address MAC-address
--------------------------------
```

```
eth0 10.0.2.10 38:D5:47:C9:DA:4C
eth1 10.0.3.10 C9:DA:4C:C9:DA:4C
```

Внимание! Не изменяйте параметры сетевых интерфейсов, задействованных в работе кластера (см. Развертывание кластера). Это может вызвать сбои его работы.

После запуска системы защиты от сбоев на обоих узлах кластера, кластер начнет свою работу. При этом на каждом узле кластера будут автоматически созданы нередактируемые сетевые фильтры, необходимые для корректной работы системы защиты от сбоев с выбранными параметрами.

Примечание. Система защиты от сбоев не контролирует работоспособность интерфейса синхронизации. Чтобы проверить его состояние, выполните команду:

```
hostname> failover show info
```

Если на экран выводится информация о состоянии обоих узлов кластера, значит интерфейсы работают исправно. Иначе, проверьте физическое соединение кабеля с интерфейсом.

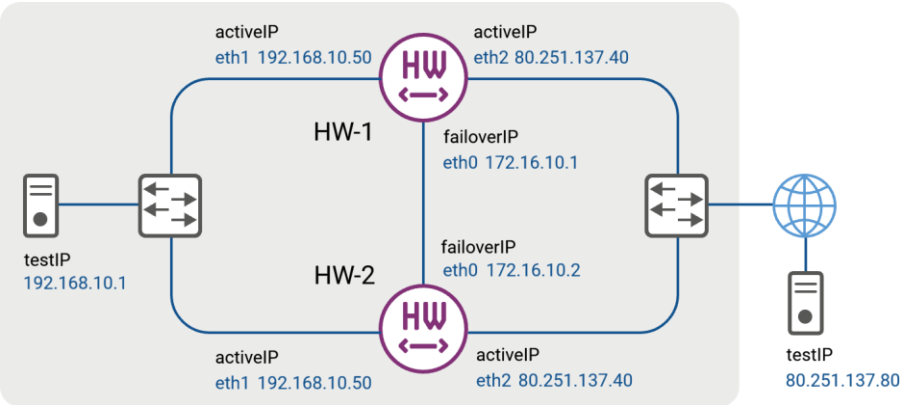


Рисунок 62. IP-адреса интерфейсов кластера и сетевых узлов testIP

Таблица 22. Параметры конфигурационных файлов failover.ini узлов кластера

Узел HW-1	Узел HW-2
[channel]	**[channel]**
`device = eth1`	`device = eth1`
`activeip = 192.168.10.50/24`	`activeip = 192.168.10.50/24`
`testip = 192.168.10.1`	`testip = 192.168.10.1`
`testdevice = eth1`	`testdevice = eth1`
`ident = internal`	`ident = internal`
`checkonlyidle = yes`	`checkonlyidle = yes`
[channel]	**[channel]**
`device = eth2`	`device = eth2`

Узел HW-1	Узел HW-2
`activeip = 80.251.137.40/24`	`activeip = 80.251.137.40/24`
`testip = 80.251.137.80`	`testip = 80.251.137.80`
`testdevice = eth2`	`testdevice = eth2`
`ident = external`	`ident = external`
`checkonlyidle = no`	`checkonlyidle = no`
`usevirtualmac = yes`	`usevirtualmac = yes`
[misc]	**[misc]**
`syncconnections = yes`	`syncconnections = yes`
[network]	**[network]**
`checktime = 10`	`checktime = 10`
`timeout = 2`	`timeout = 2`
`activeretries = 3`	`activeretries = 3`
`channelretries = 3`	`channelretries = 3`
`synctime = 5`	`synctime = 5`
`fastdown = yes`	`fastdown = yes`
`virtualmacprefix = 39`	`virtualmacprefix = 39`
[sendconfig]	**[sendconfig]**
`device = eth0`	`device = eth0`
`activeip = 172.16.10.2` (failoverIP HW-2)	`activeip = 172.16.10.1` (failoverIP HW-1)

Параметры, влияющие на скорость переключения узлов кластера

Активный узел кластера в реальном времени контролирует наличие физического соединения на сетевом интерфейсе, указанном в параметре `testdevice`. В случае потери соединения на этом интерфейсе переключение узлов кластера происходит в течение трех секунд. Одновременно с этим на активном узле:

1. Каждые `checktime` секунд проверяется работоспособность каждого из резервируемых интерфейсов.
2. Если `checkonlyidle = yes`, то анализируется весь сетевой трафик, проходящий через резервируемый интерфейс:
   - **2.1** Если в течение `checktime` через интерфейс не прошло ни одного пакета, через этот интерфейс посылаются эхо-запросы на сетевой узел `testip`, и в течение `timeout` ожидаются ответы на эти запросы.

2.2 Если ни одного ответа не приходит, то счетчик сбоев этого интерфейса увеличивается на единицу, и посылаются новые эхо-запросы. Если на эхо-запрос приходит хотя бы один ответ, то счетчик сбоев интерфейса обнуляется. В случае обнуления счетчиков сбоев всех интерфейсов происходит возврат к началу цикла проверки (ожидание в течение `checktime` и так далее). При достижении счетчиком сбоев какого-либо интерфейса значения `channelretries` интерфейс считается неработоспособным и происходит переключение узлов кластера.

3 Если `checkonlyidle = no`, то эхо-запросы на сетевой узел `testip` посылаются каждые `checktime` секунд.

Максимальное время, необходимое системе защиты от сбоев для определения неработоспособности интерфейса, равно `checktime + (timeout * channelretries)`

На пассивном узле:

1 Каждые `checktime` секунд посылаются ARP-запросы в режиме DAD на узел с адресом `activeip`.

2 По истечении `timeout` проверяется наличие положительного ответа для каждого `activeip` в системной ARP-таблице и делается вывод о работоспособности соответствующего интерфейса активного узла.

3 Если ни от одного интерфейса не был получен ответ, счетчик сбоев (один для всех интерфейсов) увеличивается. Если хотя бы от одного интерфейса был получен ответ, счетчик сбоев обнуляется. В случае достижения счетчиком сбоев значения `activeretries`, производится переход узла в активный режим.

Максимальное время, проходящее с момента неактивности (сбоя, перезагрузки) активного узла до обнаружения пассивным узлом этого факта, равно `checktime + (timeout * activeretries)`

Развертывание кластера совместно с DHCP-сервером и DHCP-relay

1 Разверните кластер (см. Развертывание кластера) с учетом следующего требования: IP-адрес каждого резервируемого интерфейса, на котором должен быть настроен DHCP-сервер или DHCP-relay, должен совпадать с IP-адресом, установленным в параметре `activeip` секции `[channel]` конфигурационного файла `failover.ini` для соответствующего интерфейса кластера.

2 На активном узле настройте параметры работы DHCP-сервера (см. Настройка DHCP-сервера) и DHCP-relay (см. Настройка DHCP-relay).

3 Убедитесь, что параметры DHCP-сервера и DHCP-relay успешно переданы на пассивный узел. Для этого на пассивном узле выполните:

```
hostname> inet show dhcp server
hostname> inet show dhcp relay [<номер копии>]
```

4 Запустите службы DHCP-сервера и DHCP-relay на активном узле:

```
hostname# inet dhcp server start
hostname# inet dhcp relay [<номер копии>] start
```

5 Включите автоматический запуск DHCP-сервера и DHCP-relay:

```
hostname# inet dhcp server mode on
hostname# inet dhcp relay mode on
```

6 Переключите режим работы пассивного узла кластера в активный. Для этого перезагрузите активный узел:

```
hostname> machine reboot
```

7 На узле кластера, ставшем активным, проверьте параметры DHCP-сервера и DHCP-relay:

```
hostname> inet show dhcp server
hostname> inet show dhcp relay [<номер копии>]
```

Запуск и завершение работы системы защиты от сбоев

Чтобы запустить систему защиты от сбоев на одиночном узле:

```
hostname# failover start
```

Чтобы запустить систему защиты от сбоев на узле кластера:

- в режиме активного узла:

  ```
  hostname# failover start active
  ```

- в режиме пассивного узла:

  ```
  hostname# failover start passive
  ```



Внимание! Перед запуском системы защиты от сбоев в активном или пассивном режиме убедитесь в том, что другой узел кластера работает в противоположном режиме. Запуск обоих узлов кластера в активном режиме вызовет конфликт IP-адресов.

Если при запуске системы защиты от сбоев не был указан параметр `active` или `passive`, она будет запущена в том режиме, в котором находилась до завершения работы.

Чтобы завершить работу системы защиты от сбоев:

```
hostname# failover stop
```

Переключение системы защиты от сбоев в одиночный режим

1. На каждом из узлов кластера выполните:

   ```
   hostname# failover config mode single
   ```

2. Отключите один из узлов кластера от локальной сети, чтобы избежать конфликтов при получении справочников и ключей.
3. Убедитесь, что IP-адреса сетевых интерфейсов второго узла кластера заданы верно, так как при переключении системы защиты от сбоев в одиночный режим параметры сетевых интерфейсов в файле `failover.ini` игнорируются.
4. В зависимости от дальнейших планов по использованию кластера:
   - Если вы больше не планируете использовать кластер, удалите ключи с узла, который был отключён от локальной сети:

     ```
     hostname# admin remove keys
     ```

     Если вы хотите в дальнейшем использовать этот ViPNet Coordinator HW как одиночный узел, установите новый дистрибутив ключей.
   - Если вы планируете возобновить работу кластера:
     - Выполните необходимые настройки для развёртывания кластера. В частности, убедитесь, что в конфигурационном файле `failover.ini` заданы IP-адреса всех сетевых интерфейсов кластера.
     - Подключите к локальной сети отключенный узел кластера.

Замена неисправного узла кластера

При обнаружении неисправности активный узел кластера переключается в пассивный режим. Для замены ViPNet Coordinator HW неисправного узла кластера на новый:

1. Выполните резервное копирование конфигурации активного узла кластера (см. Резервное копирование индивидуальной конфигурации).

Примечание. Для настройки нового узла кластера потребуются:

- Дистрибутив ключей активного узла кластера (файл *.ds5).
- IP-адрес интерфейса синхронизации, который был установлен на неисправном узле.
- IP-адрес интерфейса синхронизации активного узла кластера.



IP-адреса вы можете получить на активном узле кластера.

Чтобы узнать IP-адрес интерфейса синхронизации сбойного узла:

```
hostname> failover show config
```

IP-адрес указан в секции `[sendconfig]` в параметре `activeip`.

Чтобы узнать IP-адрес интерфейса синхронизации активного узла:

```
hostname> inet show interface <имя интерфейса>
```

2 Убедитесь, что новый ViPNet Coordinator HW, который будет входить в состав кластера, отключен от локальной сети.

3 Восстановите резервную копию конфигурации активного узла на ViPNet Coordinator HW нового узла кластера (см. Восстановление из резервной копии индивидуальной конфигурации).

4 После перезагрузки нового узла кластера завершите работу службы системы защиты от сбоев:

```
hostname# failover stop
```

5 Задайте IP-адрес интерфейса синхронизации, который был установлен на неисправном узле кластера:

```
hostname# inet ifconfig <интерфейс> address <IP-адрес> netmask <маска>
```

6 Откройте конфигурационный файл `failover.ini` для редактирования:

```
hostname# failover config edit
```

7 Замените значение параметра `activeip` секции `[sendconfig]` на IP-адрес интерфейса синхронизации активного узла кластера.

8 Сохраните изменения (**Ctrl+O**) и закройте редактор (**Ctrl+X**).

9 Если на новом узле кластера включена функция плановой перезагрузки, измените время перезагрузки:

```
hostname# machine reboot-schedule time <время> [day <день>]
```

Время перезагрузки узлов кластера должно отличаться не менее чем на 30 минут.

10 Выключите новый узел кластера:

```
hostname# machine halt
```

11 На активном узле кластера проверьте параметр `activeip` секции `[sendconfig]`:

```
hostname> failover show config
```

Параметр `activeip` должен соответствовать IP-адресу интерфейса синхронизации нового узла кластера.

12 Подключите новый узел кластера к локальной сети, а интерфейсы синхронизации обоих узлов кластера соедините между собой.

13 Включите новый узел кластера.

14 Убедитесь, что новый узел перешел в пассивный режим и стал доступен. Для этого на активном узле кластера выполните:

```
hostname> failover show info
```



Внимание! Допускается эксплуатация кластера только с одним узлом (активным), например на время проведения профилактических работ с пассивным узлом. Если в этот период на активный узел поступят обновления ключей обмена, а затем произойдет сбой активного узла, то при его замене на пассивный узел будет потеряна связь с ViPNet Prime. Чтобы восстановить работоспособность кластера с одним узлом после замены, восстановите узел из резервной копии индивидуальной конфигурации (при восстановлении используйте обновленный дистрибутив ключей).

Работа кластера с коммутационным оборудованием

Настройки коммутационного оборудования (коммутаторы и маршрутизаторы), к которому подключается кластер, могут влиять на его работу. Поэтому при их совместном использовании убедитесь, что на коммутационном оборудовании:

- пропускаются эхо-запросы ICMP с IP-адресов активного узла до всех узлов с IP-адресами, заданными в параметрах `testip` секции `[channel]` конфигурационного файла `failover.ini`, и ответы на них;
- отключена функция Proxy ARP и пропускаются ARP-запросы от пассивного узла до активного узла и ответы на них;
- при использовании виртуальных MAC-адресов:
  - для одного Ethernet-порта разрешены два MAC-адреса;
  - настройки port-security не блокируют смену MAC-адресов сетевых интерфейсов кластера.

Эти рекомендации касаются всех сетевых интерфейсов ViPNet Coordinator HW, для которых в файле `failover.ini` существует секция `[channel]`.

Подключение к пассивному узлу кластера по SSH

В некоторых случаях необходимо удаленно подключиться к пассивному узлу кластера, чтобы просмотреть его состояние, например, если не настроен мониторинг кластера по SNMP (см. Мониторинг кластера):

1. Подключитесь как суперадминистратор, администратор или сетевой администратор к активному узлу по IP-адресу интерфейса кластера (см. Удаленное подключение по SSH).
2. Перейдите в режим настройки:

   ```
   hostname> enable
   ```

3. Подключитесь к пассивному узлу кластера по IP-адресу его интерфейса синхронизации:

   ```
   hostname# inet ssh host <IP-адрес> user <пользователь>] [port <порт>]
   ```

   где пользователь:

   - `admin` — суперадминистратор;
   - другие пользователи с ролями администратора или сетевого администратора.

Просмотр информации о работе системы защиты от сбоев

Текущее состояние системы защиты от сбоев

Просмотр информации о текущем состоянии системы защиты от сбоев :

```
hostname> failover show info
```

По команде отображаются:

- `versions` — версии ПО ViPNet Coordinator HW и системы защиты от сбоев;
- `ID` — идентификатор и имя узла ViPNet;
- `workstation time` — локальное время на узле ViPNet;
- `failover mode` — система защиты от сбоев:
  - `single` — одиночный режим;
  - `active` — режим активного узла кластера;
  - `passive` — режим пассивного узла кластера;
- `failover uptime` — время непрерывной работы системы защиты от сбоев;
- `total cpu` — общая загруженность процессора;
- `total memory` — общий объем памяти;
- `available memory` — объем доступной памяти;
- сведения о текущем состоянии служб failover, iplir, mftp, webgui, uc, controld, aad, external-controld, licd (см. Службы ПО ViPNet Coordinator HW):
  - статус службы:
    - `initializing` — загружается;
    - `works` — работает;
    - `stopped` — работа завершена;
    - `unknown` — неизвестно (например, если произошел сбой в работе службы, была произведена попытка ее перезапуска, и данных о ее состоянии пока нет);
  - сведения о ресурсах процессора, используемых службой.

Примечание. В режиме кластера статистика использования системных ресурсов и текущее состояние служб ViPNet Coordinator HW отображаются для обоих узлов кластера: в столбце `local` — для узла, на котором выполнена команда, в столбце `remote` — для другого узла.

Если служба `failoverd` работает в одиночном режиме:

```
Versions: ViPNet 5.4.2(150), daemon 1.5 (1)
Workstation configured for ID 15EA000B (Coordinator_HW)
The workstation works in a single mode of protection against failures
Workstation time (utc: 1406806848) Wed Jul 31 15:40:48 2026
failover mode       * single
failover uptime           * 0d 0:14
total cpu                 * 3%
total memory              * 2055488 kB
available memory          * 1915324 kB
failover state            * works
failover cpu              * 1%
iplir state               * works
iplir cpu                 * 4%
mftp state                * works
mftp cpu                  * 1%
webgui state              * works
webgui cpu                * 0%
uc state                  * stopped
controld state            * works
controld cpu              * 0%
aad state                 * works
aad cpu                   * 0%
external-controld state   * works
external-controld cpu     * 0%
licd state                * works
licd cpu                  * 0%
```

Если служба `failoverd` работает в режиме кластера:

```
Versions: ViPNet 5.4.2 (30), daemon 1.5 (1)
Workstation configured for ID 29A0022 (Coordinator_HW)
Workstation works in a cluster mode of protection against failures
Workstation time (utc: 1204638024) Thu Jul 27 17:35:30 2026
                          * local             * remote
failover mode       * active            * passive
failover uptime           * 3d  5:26          * 0d  0:00
total cpu                 * 80%               * 0%
total memory              * 2044104 kB  *     2044104 kB
available memory          * 1672360 kB  *     1672360 kB
failover state            * works             * works
```

```
failover cpu              * 7%              * 0%
iplir state               * works           * works
iplir cpu                 * 0%              * 0%
mftp state                * works           * works
mftp cpu                  * 66%             * 0%
webgui state              * works           * stopped
webgui cpu                * 0%              * 0%
uc state                  * stopped         * stopped
controld state            * works           * works
controld cpu              * 0%              * 0%
aad state                 * works           * works
aad cpu                   * 0%              * 0%
external-controld state   * works           * works
external-controld cpu     * 0%              * 0%
licd state                * works           * works
licd cpu                  * 0%              * 0%
```

Если служба `failoverd` остановлена, выводится только информация о его режиме:

```
The failover system is in the single mode
```

Журнал переключений

События о работе системы защиты от сбоев в режиме кластера регистрируются службой `failoverd` в журнале переключений. Среди таких событий:

- `<BOOT>` — запуск службы `failoverd` при загрузке операционной системы;
- `<P_START>` — ручной запуск службы `failoverd` в режиме пассивного узла;
- `<A_START>` — ручной запуск службы `failoverd` в режиме активного узла;
- `<SWITCH>` — переход узла из пассивного в активный (или наоборот).

Чтобы просмотреть записи в журнале переключений узла, выполните:

```
hostname> failover view <дд.мм.гггг[.чч.мм.сс]> <дд.мм.гггг[.чч.мм.сс]>,
```

указав начало и конец интересующего интервала времени. Например:

```
failover view 08.03.2026.00.00.00 23.03.2026.16.37.00
```

Выводится следующая информация:

- версии ПО ViPNet Coordinator HW и службы `failoverd`;
- идентификатор и имя узла;
- указание на работу системы защиты от сбоев в режиме кластера;
- локальные дата и время на узле;
- список записей за выбранный интервал времени (дата, время, идентификатор и описание события).

Данная информация выводится в следующем формате:

```
View journal of failover switching
Versions: ViPNet 5.4.2 (30), daemon 1.5 (1)
Workstation configured for ID 29A0022 (Coordinator_HW)
The workstation works in a cluster mode of protection against failures
Workstation time (utc: 1174916969) Thu Mar 27 17:35:30 2026

09 Mar 2026 12:51:42    <P_START> Start failover daemon in passive mode
22 Mar 2026 12:27:27    <A_START> Start failover daemon in active mode
22 Mar 2026 14:10:35    <A_START> Start failover daemon in active mode
22 Mar 2026 15:30:46    <BOOT> Boot the system
23 Mar 2026 11:09:07    <SWITCH> Switch server from passive mode to active mode
```

Если за указанный интервал времени не произошло ни одного события, выводится сообщение:

```
There are no records in journal of switchings
```

Подключение ViPNet Coordinator HW к ИБП

Внимание! Подключение к ИБП возможно только для аппаратных исполнений ViPNet Coordinator HW. Поддерживаются только ИБП производства APC, подключаемые через USB-порт, например, APC Smart-UPS.

Чтобы обеспечить бесперебойное электропитание ViPNet Coordinator HW, подключите его к ИБП. Тогда при отключении электроэнергии:

1. ViPNet Coordinator HW начинает питаться от аккумуляторной батареи ИБП.
2. Если заряд аккумуляторной батареи достигает критически низкого уровня (этот уровень зависит от следующих параметров, заданных на ИБП: `battery.charge`, `battery.charge.low`, `battery.runtime` и `battery.runtime.low`):
   - 2.1 ИБП взаимодействует с ViPNet Coordinator HW по интерфейсному кабелю и посылает сигнал об истощении батареи.
   - 2.2 ViPNet Coordinator HW получает сигнал и начинает выключаться. При этом на ИБП передается информация о том, что для выключения ViPNet Coordinator HW потребуется не менее 180 секунд. Получив эти данные, ИБП корректирует расход оставшегося заряда батареи таким образом, чтобы ViPNet Coordinator HW успел штатно завершить работу.

     В результате ViPNet Coordinator HW успевает выключиться до полного разряда батареи и потери данных не происходит.
3. Если подача электроэнергии восстанавливается до достижения батареей критически низкого уровня заряда, ViPNet Coordinator HW снова начинает питаться от электросети.

К одному ИБП можно подключить несколько ViPNet Coordinator HW. Устройство, к которому подключен интерфейсный кабель ИБП, является главным (master), остальные — подчиненными (slave). Главное устройство взаимодействует непосредственно с ИБП и отвечает за своевременное оповещение по сети подчиненных устройств. Оно должно быть доступно подчиненным по одному из своих IP-адресов.

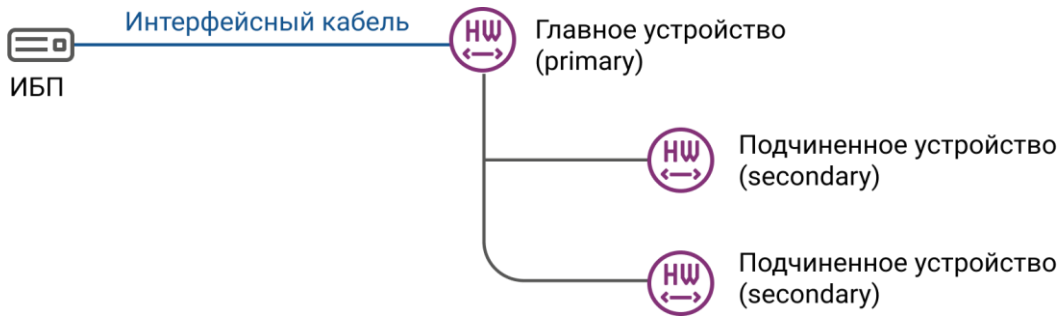


Рисунок 63. Схема подключения ViPNet Coordinator HW к ИБП

Чтобы подключить к ИБП несколько ViPNet Coordinator HW, необходимо настроить каждый из них в соответствии с его ролью (master или slave).

На ViPNet Coordinator HW с ролью master:

1. Подключите к ViPNet Coordinator HW интерфейсный кабель ИБП.
2. Включите взаимодействие ViPNet Coordinator HW с ИБП:

   ```
   hostname# ups set monitoring on
   ```
3. Установите на ViPNet Coordinator HW режим master:

   ```
   hostname# ups set mode master
   ```
4. Запустите взаимодействие ViPNet Coordinator HW с ИБП:

   ```
   hostname# ups start
   ```
5. Проверьте взаимодействие ViPNet Coordinator HW с ИБП:

   ```
   hostname# ups show status
   ```

   Если взаимодействие установлено, отобразится информация о текущем состоянии ИБП.



Внимание! Если вы переподключили интерфейсный кабель ИБП, то для восстановления взаимодействия ViPNet Coordinator HW с ИБП выполните последовательно команды `ups stop` и `ups start`.

На ViPNet Coordinator HW с ролью slave:

1. Включите взаимодействие ViPNet Coordinator HW с ИБП:

   ```
   hostname# ups set monitoring on
   ```
2. Установите на ViPNet Coordinator HW режим slave:

   ```
   hostname# ups set mode slave <master_IP>
   ```

   ViPNet Coordinator HW, выступающий в роли master, должен быть доступен с данного ViPNet Coordinator HW по этому IP-адресу.

   При подключении к ИБП кластера в качестве IP-адреса мастера укажите адрес интерфейса синхронизации узла с этой ролью.
3. Запустите взаимодействие ViPNet Coordinator HW с ИБП:

   ```
   hostname# ups start
   ```
4. Проверьте взаимодействие ViPNet Coordinator HW с ИБП:

   ```
   hostname# ups show status
   ```

   Если взаимодействие установлено, отобразится информация о текущем состоянии ИБП, подключенного к ViPNet Coordinator HW в роли master.

Если к ИБП подключается кластер, то один узел будет главным, а другой — подчиненным. При этом другие устройства к ИБП подключать запрещено.

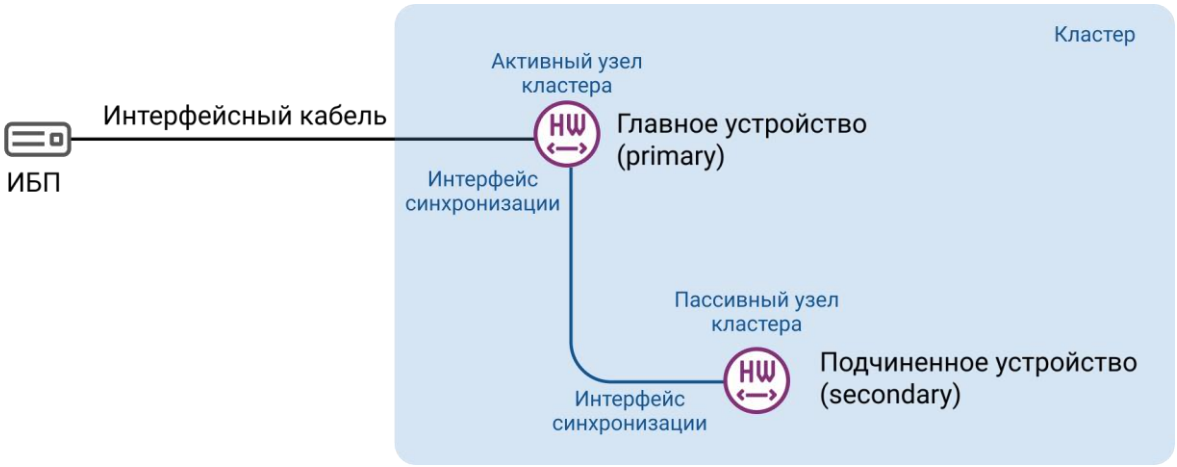


Рисунок 64. Схема подключения кластера к ИБП

Управление режимом производительности

Для соответствия требованиям ФСТЭК к межсетевым экранам в части обеспечения бесперебойного функционирования на аппаратной платформе HW5000 Q2 поддерживается переключение режимов производительности:

- Режим отказоустойчивого управления — режим, при котором одно ядро процессора выделяется только для работы интерфейса управления ViPNet Coordinator HW. Производительность при обработке сетевого трафика может быть снижена.
- Режим полной производительности — режим, при котором для обработки сетевого трафика используются все доступные ядра процессора. Обеспечивает максимальную пропускную способность. Установлен по умолчанию.

Чтобы изменить режим производительности ViPNet Coordinator HW:

1. Выберите режим:

   ```
   hostname# machine performance-mode set {failsafe | full}
   ```

   где:

   - `failsafe` — режим отказоустойчивого управления;
   - `full` — режим полной производительности.

2. Подтвердите выбор режима.
3. Выбранный режим будет установлен после перезагрузки. Чтобы перезагрузить ViPNet Coordinator HW, введите `Yes` и нажмите **Enter**:

   ```
   The settings are saved. System must be restarted for the changes to take effect. Restart now? (Yes/No): Yes
   ```

   Вы можете перезагрузить ViPNet Coordinator HW позже.

Чтобы посмотреть текущий режим производительности:

```
hostname# machine performance-mode show
```

12

Настройка транспортного сервера MFTP

Назначение транспортного сервера MFTP 349

Настройка протоколирования событий транспортного сервера MFTP 350

Настройка транзитного режима 351

Назначение транспортного сервера MFTP

Транспортный сервер MFTP предназначен для передачи транспортных конвертов MFTP между связанными узлами сети ViPNet, поддерживающими работу с дистрибутивом ключей `dst`. Сервер MFTP обеспечивает удаленное обновление на узлах сети:

- Справочников и ключей.
- Программного обеспечения ViPNet.
- Политик безопасности из Policy Management (модуль Prime).

Сервер MFTP реализован службой `mftpd`. Конверты MFTP представляют собой файлы с данными, которыми обмениваются между собой приложения, входящие в состав ПО ViPNet. Размер конверта не может превышать 2 Гбайт. Сервер передает конверты в соответствии с адресами получателей, указанными в заголовках конвертов, по каналу MFTP: узел-отправитель устанавливает TCP-соединение с узлом-получателем, проводится взаимная аутентификация узлов и осуществляется передача конвертов.

Примечание. В исполнении HW50 транспортный сервер MFTP выполняет обновление справочников, ключей, ПО ViPNet и политик безопасности только для собственного узла; конверты MFTP, адресованные другим узлам сети, не обрабатываются.

Поэтому при формировании структуры сети на ViPNet Coordinator HW в исполнении HW50 не должны регистрироваться клиенты ViPNet.

Сервер MFTP ViPNet Coordinator HW версий 5.0 и выше работает в транзитном режиме, обеспечивая передачу конвертов MFTP между узлами ViPNet, поддерживающими работу с дистрибутивом ключей `dst`. Если в сети ViPNet используется ViPNet Coordinator HW любой из версий ниже, чем 4.5.1, необходимо настроить транзитный режим (см. Настройка транзитного режима).

Подробнее о настройке сервера MFTP и ведении его журналов см. документ «Справочник команд и конфигурационных файлов», раздел «Файл mftp.conf».

Настройка протоколирования событий транспортного сервера MFTP

Служба `mftpd` записывает информацию о событиях, происходящих в процессе работы транспортного сервера MFTP, в системный журнал.

Чтобы изменить параметры записи событий:

1. Завершите работу службы `mftpd`:

   ```
   hostname# mftp stop
   ```

2. Откройте файл `mftp.conf` для редактирования:

   ```
   hostname# mftp config
   ```

3. В секции `[debug]` при необходимости измените значения следующих параметров:

   - `debuglevel` — уровень важности событий, записываемых в журнал. Возможные значения: от `-1` до `4` (по умолчанию `3`). Чем выше уровень важности, тем более подробная информация записывается в журнал. Значение параметра `-1` выключает ведение журнала (при этом некоторые важные системные события по-прежнему будут выводиться в журнал).

     Уровень важности `4` используется только для диагностики возможных проблем и должен быть включен по рекомендации специалистов ИнфоТеКС. Не задавайте его для постоянного использования.

   - `debuglogfile` — источник информации, выводимой в журнал, в формате: `syslog:<facility.level>`, где:

     - `facility` — процесс, формирующий информацию. Возможные значения: `kern` (ядро), `user` (пользовательские программы) или `daemon` (службы).
     - `level` — уровень важности информации. Возможные значения: `err` (ошибка), `info` (информационное сообщение) или `debug` (отладочная информация).

     Значение параметра `debuglogfile` по умолчанию — `syslog:daemon.debug`.

4. Сохраните изменения (**Ctrl+O**) и закройте редактор (**Ctrl+X**).

5. Запустите службу `mftpd`:

   ```
   hostname# mftp start
   ```

Настройка транзитного режима

Если в сети ViPNet используется ViPNet Coordinator HW любой из версий ниже, чем 4.5.1, то для корректной передачи транспортных конвертов MFTP в настройках секции `[channel]` файла `mftp.conf` необходимо:

- Для ViPNet Coordinator HW любой из версий ниже, чем 4.5.1 задать `call_timeout = 30`.
- Для ViPNet Coordinator HW версий 5.0 и выше задать `call_flag = no`.

Таблица 23. Параметры секции `[channel]` файлов `mftp.conf`

Настройки HW_1 (версия 5.0 и выше)	**Настройки HW_2 (версия ниже 4.5.1)**
id = <идентификатор HW_2>	id = <идентификатор HW_1>
name = HW_2	name = HW_1
type = mftp	type = mftp
off_flag = no	off_flag = no
call_flag = no	call_flag = yes
ip = <IP-адрес HW_2>	ip = <IP-адрес HW_1>
call_timeout = -1	call_timeout = 30
last_port = 5000	last_port = 5000
last_call = 0	last_call = 0
last_err = 0	last_err = 0

13

Обновление программного обеспечения

Проверка ЭП файла обновления 353

Обновление ПО с версий 4.5.x до версии 5.4.x 359

Обновление ПО с версий 5.1.x, 5.2.x и 5.3.x до версии 5.4.x 364

Обновление ПО в кластере 367

Возврат к ПО версий 4.5.x 369

Возврат к ПО версий 5.1.x, 5.2.x и 5.3.x 372

Локальное обновление DPI 374

Проверка ЭП файла обновления

Примечание. При обновлении ПО с версии 4.5.8 и выше на версию 5.4.2 ручная проверка ЭП файла обновления не требуется. Она выполняется автоматически в ViPNet Coordinator HW. При обновлении ПО до версии 5.4.2 с версии ниже 4.5.8 проверьте ЭП файла обновления согласно данному разделу.

Ниже представлен пример проверки ЭП с помощью модуля File Unit программы ViPNet PKI Client.

Предварительные действия

Подготовьте компьютер, на котором будете проверять ЭП файла обновления:

1. Скопируйте файлы из комплекта поставки той версии ПО ViPNet Coordinator HW, на которую хотите обновиться:
   - файл обновления ПО ViPNet Coordinator HW (`*.lzh`);
   - электронную подпись файла обновления (`*.sig`);
   - корневой сертификат ИнфоТеКСа (`*.cer`).
2. Скачайте актуальный CRL по ссылке http://crl.infotecs.ru/InfoTeCS_TDC_Root_CA.crl.
3. Скачайте ViPNet PKI Client с официального сайта ИнфоТеКСа. Для этого:
   - **3.1** Перейдите по ссылке https://infotecs.ru/downloads/demo/vipnet-pki-client/.
   - **3.2** Нажмите на ссылку с ViPNet PKI Client for Windows.
   - **3.3** Заполните форму заявки на скачивание ViPNet PKI Client и нажмите **Отправить**.
   - **3.4** Скачайте ViPNet PKI Client по ссылке, полученной по электронной почте.
4. Установите ViPNet PKI Client:

Примечание. Если у вас установлен ViPNet PKI Client версии 1.x, сначала удалите её, затем установите новую. При удалении ViPNet PKI Client настройки сохранятся на компьютере.

- **4.1** Запустите установочный файл.
- **4.2** Ознакомьтесь с лицензионным соглашением. Чтобы принять условия лицензионного соглашения, выберите **Я принимаю условия лицензионного соглашения** и нажмите **Далее**.
- **4.3** На шаге **Автоматическое получение настроек приложения из файла** выберите папку пользователя и нажмите **Установить**.
- **4.4** Следуйте указаниям мастера установки.

4.5 Для завершения установки требуется перезагрузка компьютера. Нажмите **Перезагрузить сейчас**.

5 Загрузите и активируйте тестовую лицензию:

5.1 В меню **Пуск** или на рабочем столе запустите **Настройки PKI Client**.

5.2 Выберите  **Лицензия**.

5.3 Нажмите **Выбрать способ активации**.

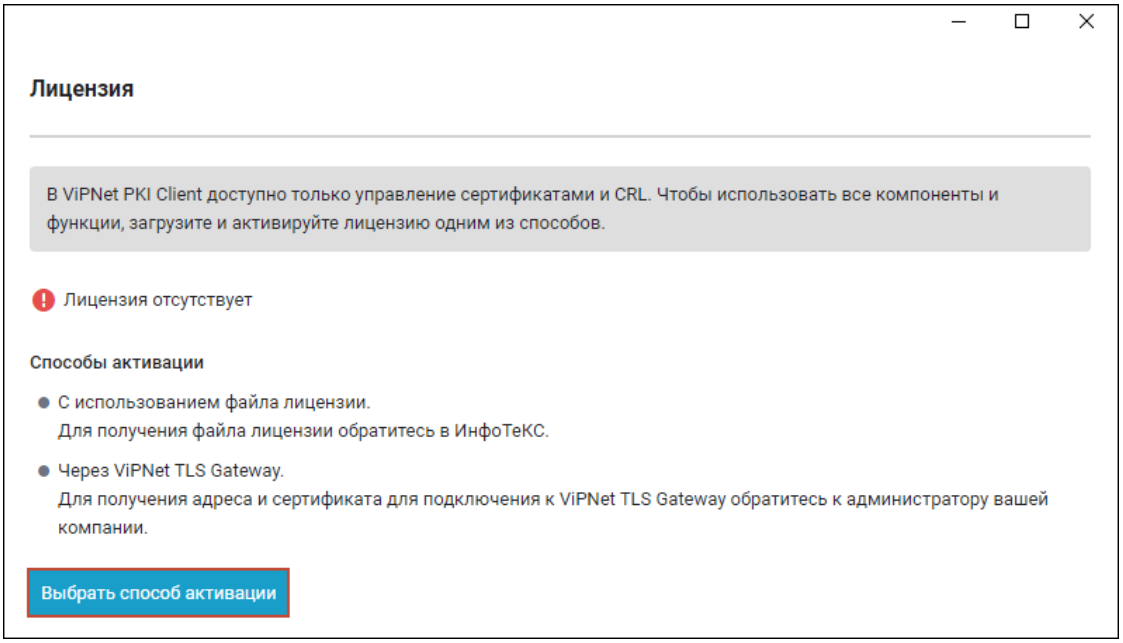


Рисунок 65. Переход к загрузке лицензии

5.4 Выберите **с использованием файла лицензии** и нажмите **Выбрать файл**.

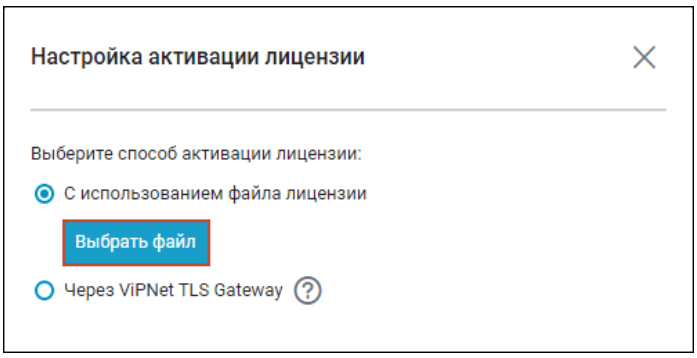


Рисунок 66. Переход к выбору файла лицензии

5.5 Укажите путь к файлу тестовой лицензии и нажмите **Открыть**. Тестовая лицензия (`*.itcslic`) вложена в архив с ViPNet PKI Client.

5.6 Нажмите **Загрузить**.

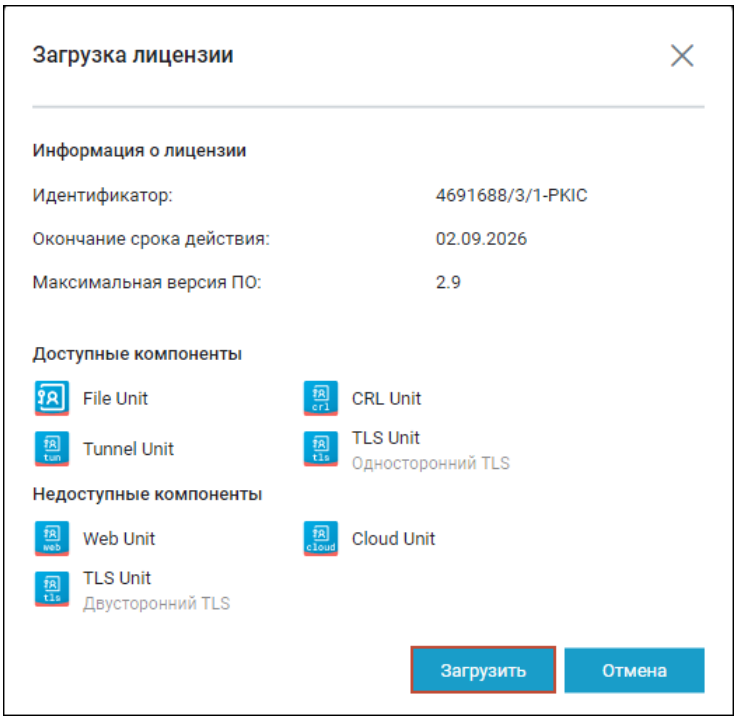


Рисунок 67. Загрузка файла лицензии

5.7 Убедитесь, что лицензия активирована.

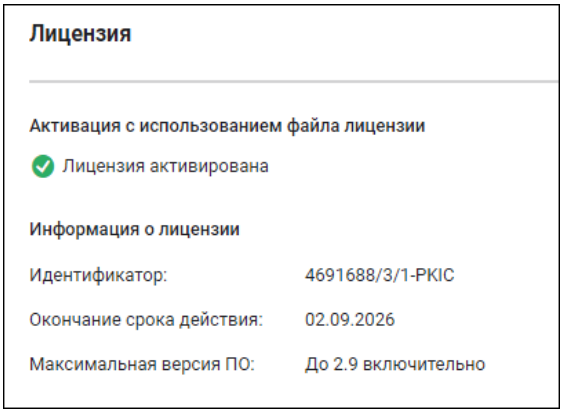


Рисунок 68. Тестовая лицензия активирована

Установка корневого сертификата и CRL

1 В меню **Пуск** запустите **File Unit** из состава ViPNet PKI Client.

2 Нажмите **Настройки**.

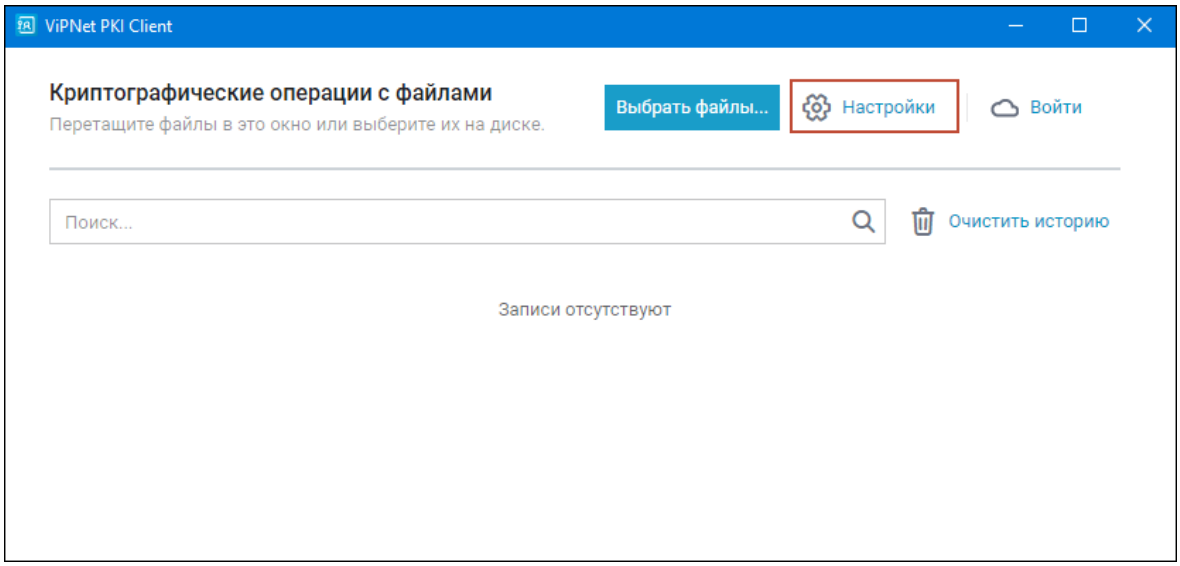


Рисунок 69. Настройка ViPNet PKI Client

3 Перейдите в раздел **Сертификаты**.

4 Добавьте корневой сертификат:

4.1 Нажмите ⊕ **Добавить сертификат или CRL**.

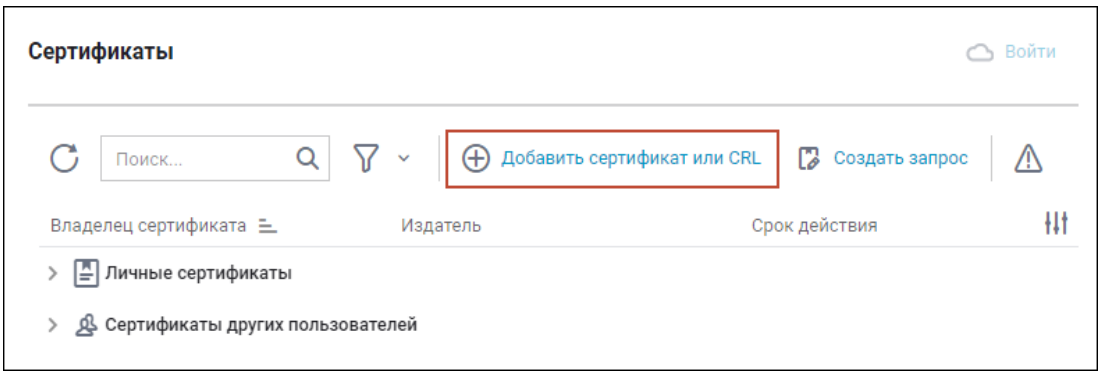


Рисунок 70. Переход к импорту корневого сертификата или CRL

4.2 Укажите путь к файлу корневого сертификата и нажмите **Открыть**.

4.3 Нажмите **Добавить**.

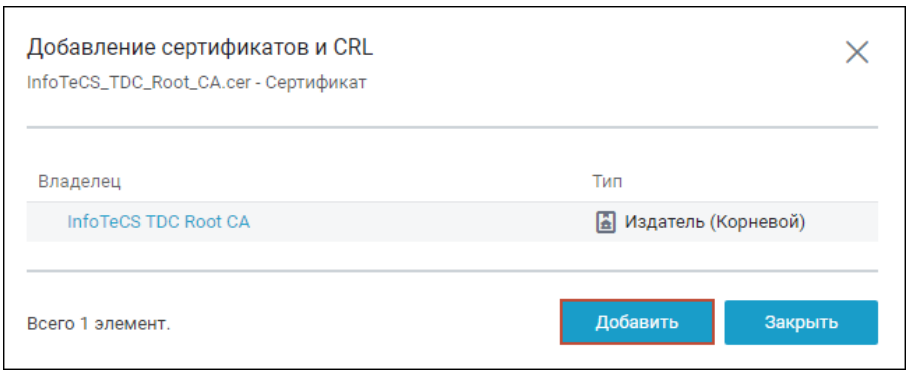


Рисунок 71. Импорт корневого сертификата

4.4 Если появится окно **Предупреждение системы безопасности**, подтвердите установку корневого сертификата.

4.5 Нажмите **Закрыть**.

5 Добавьте CRL:

5.1 Нажмите **Добавить сертификат или CRL**.

5.2 Укажите путь к файлу CRL и нажмите **Открыть**.

5.3 Нажмите **Добавить**.

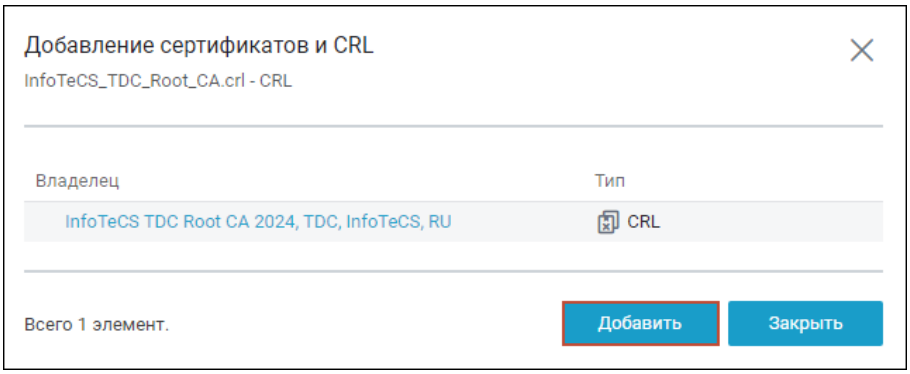


Рисунок 72. Импорт CRL

5.4 Нажмите **Закрыть**.

Установка корневого сертификата и CRL завершена.

Проверка электронной подписи

1 В главном окне программы ViPNet PKI Client выполните одно из действий:

- перетащите файл электронной подписи (`*.sig`) в главное окно программы;
- или нажмите **Выбрать файлы** и выберите файл электронной подписи (`*.sig`).

2 Нажмите **Проверить ЭП**.

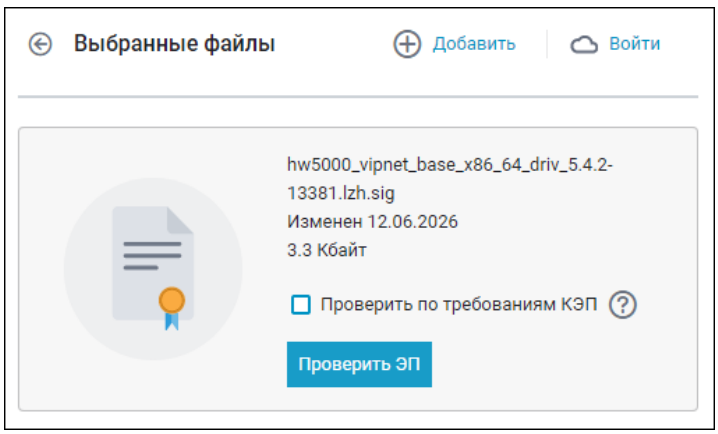


Рисунок 73. Проверка электронной подписи файла обновления

3 Укажите путь к файлу обновления ПО и нажмите **Открыть**.

Если окно выбора файла не появилось, а сразу отобразился результат проверки ЭП, значит файл был найден автоматически.

4 Убедитесь, что подпись действительна:

- **Статус ЭП — Действительна**;
- **Статус сертификата подписанта — Действителен**.

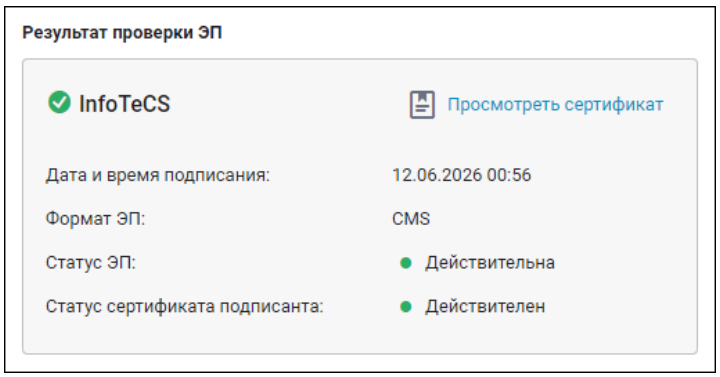


Рисунок 74. Результат проверки электронной подписи файла обновления

Проверка завершена.

Обновление ПО с версий 4.5.x до версии 5.4.x

Обновление ПО до версии 5.4.2 поддерживается с версий 4.5.4–4.5.9 и доступно для исполнений:

- ViPNet Coordinator HW50.
- ViPNet Coordinator HW100.
- ViPNet Coordinator HW1000, ViPNet Coordinator HW1000C, ViPNet Coordinator HW1000D.
- ViPNet Coordinator HW2000.
- ViPNet Coordinator HW5000.
- ViPNet Coordinator VA.

Если установлена версия ниже 4.5.4, обновите ПО последовательно, например: 4.3.2 > 4.5.4 > 5.4.2.

Особенности обновления

- Не сохраняются после обновления:
  - Настройка профиля производительности.
  - Настройка отключения ведения системного журнала.
  - Способ аутентификации пользователей.
  - Если был изменен ViPNet ID узла:
    - Видимость узлов сети ViPNet и туннелируемых узлов.
    - Режим доступа со связанными узлами.
    - Состояние и порт сервера TCP-туннелей.
    - Диапазон туннелируемых адресов.
    - Диапазон присваиваемых виртуальных адресов.
    - L2OverIP (сетевые интерфейсы, номера портов, IP-адреса своего и удаленного координатора, время жизни MAC-адреса).
- Пользовательские фильтры версий 4.5.x (`Allow ViPNet base services` и `Allow ViPNet MFTP`) конвертируются в служебные фильтры (`Allow ViPNet base services in`, `Allow ViPNet base services out`, `Allow ViPNet MFTP in`, `Allow ViPNet MFTP out`).
- В связи с изменением набора прикладных протоколов, приложений и групп, классифицируемых DPI, деактивируются параметры сетевых фильтров, в которых заданы не поддерживаемые в новом наборе прикладные протоколы, приложения и группы. Если все прикладные протоколы, приложения и группы, заданные в сетевом фильтре деактивированы, то деактивируется и сам фильтр.

- Системный журнал версий 4.5.x архивируется; на время обновления включается локальное ведение системного журнала.
- Транспортный сервер MFTP переключается в транзитный режим работы (пересылка транспортных конвертов).
- На аппаратной платформе HW1000 Q8 изменяется нумерация интерфейсов `eth0-eth3` на `eth4-eth7` и наоборот. При этом все настройки, связанные с интерфейсами, автоматически корректируются.
- Обновление ПО ViPNet Coordinator VA с версий 4.5.x не изменяет параметры виртуальной машины. Перед обновлением задайте их в соответствии с рекомендацией для версии версии 5.4.x (подробнее см. документ «Подготовка к работе», раздел «ViPNet Coordinator VA»).
- Локальный администратор `admin` 4.5.x становится суперадминистратором `admin`, пароль сохраняется.
- Локальный пользователь `user` 4.5.x становится локальным аудитором `user`, пароль сохраняется.

Перед обновлением

1 Выполните действия по проверке ЭП файла обновления:

   - При обновлении ПО с версии 4.5.8 и выше необходимо наличие на ViPNet Coordinator HW актуального CRL для проверки ЭП файла обновления. Срок действия CRL — 1 год. Если на момент обновления ПО срок действия CRL уже истечёт, обновление не выполнится.

     Скачайте актуальный CRL по ссылке http://crl.infotecs.ru/InfoTeCS_TDC_Root_CA.crl и на шаге 2 скопируйте файл на USB-носитель.

   - При обновлении ПО с версии ниже 4.5.8 проверьте ЭП вручную (см. Проверка ЭП файла обновления).

2 При локальном обновлении скопируйте на USB-носитель с файловой системой FAT32, ext2, ext3 или ext4:

   2.1 Файл обновления ПО ViPNet Coordinator HW, например, `hw1000_vipnet_base_x86_64_driv_5.4.2-13381.lzh`.

   2.2 Файл дистрибутива ключей `ds5` для инициализации ViPNet Coordinator HW версии 5.4.2.

   2.3 При обновлении ПО с версии 4.5.8 и выше — CRL: `InfoTeCS_TDC_Root_CA.crl`.

> **Примечание.** На один USB-носитель можно записать несколько файлов обновления для различных исполнений ViPNet Coordinator HW, разместив их в разных каталогах. При обновлении будет доступен только файл соответствующего исполнения.

3 При удаленном обновлении скопируйте на USB-носитель файл дистрибутива ключей `ds5` для инициализации ViPNet Coordinator HW версии 5.4.2.

4 Чтобы иметь возможность возврата к ПО версий 4.5.x (см. Возврат к ПО версий 4.5.x), сохраните на USB-носителе:

4.1 Справочники, ключи и настройки:

```
hostname# iplir stop
hostname# mftp stop
hostname# admin export keys binary-encrypted usb
hostname# iplir start
hostname# mftp start
```

4.2 Журнал IP-пакетов (см. Экспорт журнала IP-пакетов на USB-носитель).

Локальное обновление

1. Подключитесь к ViPNet Coordinator HW версии 4.5.x с помощью консоли. При подключении к ViPNet Coordinator VA используйте консоль платформы виртуализации.
2. Перейдите в режим администратора:

   ```
   hostname> enable
   ```

3. При обновлении ПО с версии 4.5.8 и выше импортируйте CRL (файл `InfoTeCS_TDC_Root_CA.crl`):

   ```
   hostname# service cert import
   ```

4. Запустите обновление:

   ```
   hostname# admin upgrade software usb
   ```

5. Подключите USB-носитель с файлами обновления и дистрибутива ключей `ds5` к ViPNet Coordinator HW (виртуальной машине ViPNet Coordinator VA) и нажмите **Enter**:

   ```
   Insert USB flash drive into empty USB slot and press <Enter>
   ```

6. Выберите файл обновления — нажмите `1`:

   ```
   Select file to use for software upgrade:
   1 — /mnt/tmp/sdb1/hw1000_vipnet_base_x86_64_driv_5.4.2-13381.lzh
   Enter file number [1-1] or [q] to cancel: 1
   ```

7. Продолжите без сохранения справочников, ключей и настроек — введите `Yes` нажмите **Enter**:

   ```
   Starting local upgrade... vupgrade - Melted : 000
   Starting sanity check before upgrade...
   Stopping VPN services...
   Shutting down failover daemon
   Shutting down ViPNet Web GUI service
   Shutting down MFTP daemon
   Shutting down IpLir


   Checking integrity of the upgrade file...
   ...
   This is hw1000 platform
   WARNING!
   ```

```
You are going to upgrade software to the version 5.
Downgrade to previous versions is not supported.
The saved software configurations will be deleted.
We strongly recommend to create VBE-backup before proceeding.
In order to create VBE-backup, you need to use the following command:
admin export keys binary-encrypted usb | tftp
Are you sure you want to proceed upgrade? [Yes/No] Yes
```

8 Продолжите без сохранения журнала IP-пакетов — введите `Yes` нажмите **Enter**:

```
WARNING!
Software update deletes the IP packet logs.
To preserve IP packet logs, abort software update and save IP packet logs via CLI or
Web Access.
Continue without saving the logs? [Yes/No] Yes
```

9 Нажмите **Enter**, чтобы перезагрузить ViPNet Coordinator HW.

```
ViPNet Coordinator HW1000 was successfully from 4.5.2 to 5.4.2
Press [Enter] to terminate
```

10 После перезагрузки выполните инициализацию ViPNet Coordinator HW в консольном или полноэкранном режиме (подробнее см. документ «Подготовка к работе», разделы «Инициализация в консольном режиме» и «Инициализация в полноэкранном режиме»).

11 После инициализации:

11.1 Выполните аутентификацию как суперадминистратор.

11.2 Проверьте версию ПО:

```
hostname# version
```

Удаленное обновление

Для обновления необходимо наличие на ViPNet Coordinator HW актуального CRL для проверки ЭП файла обновления. Срок действия CRL — 1 год. Если на момент обновления ПО срок действия CRL уже истечёт, обновление не выполнится.

Скачайте актуальный CRL по ссылке http://crl.infotecs.ru/InfoTeCS_TDC_Root_CA.crl и импортируйте его в хранилище ViPNet Coordinator HW одним из способов:

1 С помощью командного интерпретатора — скопируйте файл на USB-носитель и выполните:

```
hostname# service cert import
```

2 С помощью веб-интерфейса (возможно импортировать удалённо):

2.1 Выберите **Системные настройки** > **Сертификаты** > **Списки отозванных сертификатов (CRL)**.

2.2 Нажмите **Импортировать.**

2.3 Нажмите **Загрузить файл** и выберите CRL.

2.4 Нажмите **Импортировать**.

Удаленное обновление выполняется в ViPNet Prime. Подробнее см. документ «ViPNet Prime. Руководство администратора», раздел «Отправка обновлений на узлы». После автоматического запуска удаленного обновления ПО с версий 4.5.x до версии 5.4.x выполните инициализацию ViPNet Coordinator HW.

Обновление ПО с версий 5.1.x, 5.2.x и 5.3.x до версии 5.4.x

Особенности обновления

- Начиная с ПО версии 5.1.2 не поддерживается совместимость алгоритмов шифрования ГОСТ 34.12–2018 «Магма» и «Кузнечик» версий 5.1.0 и 5.1.1. Чтобы избежать потери связанности между координаторами с ПО версий 5.1.0 и 5.1.1 и координаторами с ПО версий 5.1.2 и выше, планируйте их одновременное обновление.
- Начиная с ПО версии 5.3.1 не поддерживает автоматическое определение видимости узлов и сетей ViPNet. При обновлении такая видимость будет заменена на видимость по реальным или виртуальным IP-адресам в зависимости от текущей. Если доступ к ViPNet-узлу осуществляется по определённому адресу видимости, то перед обновлением задайте эту видимость вручную в секции `[id]` узла файла `iplir.conf` (подробнее см. Настройка видимости узлов).
- Обновление ПО с версии 5.1.0 до версии 5.4.x напрямую не поддерживается. В этом случае обновите ПО последовательно, например 5.1.0 > 5.3.2 > 5.4.x.
- Обновление ПО ViPNet Coordinator VA с версий 5.1.x, 5.2.x и 5.3.x не изменяет параметры виртуальной машины. Перед обновлением задайте их в соответствии с рекомендацией для версии версии 5.4.x (подробнее см. документ «Подготовка к работе», раздел «ViPNet Coordinator VA»).
- После обновления ПО серийный номер может не отображаться. В этом случае необходимо задать серийный номер вручную. Подробнее см. Установка серийного номера.
- В связи с изменением набора прикладных протоколов, приложений и групп, классифицируемых DPI, деактивируются параметры сетевых фильтров, в которых заданы не поддерживаемые в новом наборе прикладные протоколы, приложения и группы. Если все прикладные протоколы, приложения и группы, заданные в сетевом фильтре, деактивированы, то деактивируется и сам фильтр.
- Локальный администратор `admin` становится суперадминистратором `admin`, пароль сохраняется.
- Локальный аудитор `user` остается локальным аудитором `user`, пароль сохраняется, если был задан.

Перед обновлением

1 Необходимо наличие на ViPNet Coordinator HW актуального CRL для проверки ЭП файла обновления. Срок действия CRL — 1 год. Если на момент обновления ПО срок действия CRL уже истечёт, обновление не выполнится.

   Скачайте актуальный CRL по ссылке http://crl.infotecs.ru/InfoTeCS_TDC_Root_CA.crl и на шаге 2 скопируйте файл на USB-носитель.

2 Скопируйте на USB-носитель с файловой системой FAT32, ext2, ext3 или ext4:

2.1 Файл обновления ПО и файл ЭП, например:

- `hw1000_vipnet_base_x86_64_driv_5.4.2-13381.zip`.
- `hw1000_vipnet_base_x86_64_driv_5.4.2-13381.zip.sig`.

2.2 CRL: `InfoTeCS_TDC_Root_CA.crl`.



Примечание. На один USB-носитель можно записать несколько файлов обновления для различных исполнений ViPNet Coordinator HW, разместив их в разных каталогах. При обновлении будет доступен только файл соответствующего исполнения.

3 Для восстановления ViPNet Coordinator HW при сбое локального обновления ПО сохраните резервную копию конфигурации (для кластера — резервные копии обоих узлов). Подробнее см. Управление индивидуальной конфигурацией.

Локальное обновление

1 Подключитесь к ViPNet Coordinator HW с помощью консоли. При подключении к ViPNet Coordinator VA используйте консоль платформы виртуализации.

2 Выполните аутентификацию как локальный администратор `admin`.

3 Импортируйте CRL (файл `InfoTeCS_TDC_Root_CA.crl`):

```
hostname# service cert import
```

4 Запустите обновление:

```
hostname# admin upgrade software
```

5 Подключите USB-носитель с файлами обновления к ViPNet Coordinator HW (виртуальной машине ViPNet Coordinator VA) и нажмите **Enter**:

```
Insert USB flash drive or CD and press <Enter>
Checking integrity and signature of
'hw1000_vipnet_base_x86_64_driv_5.4.2-13381.zip'...
```

6 Выберите файл обновления — нажмите `1`:

```
Select file to use for software upgrade:
1 — /mnt/tmp/sdb1/hw1000_vipnet_base_x86_64_driv_5.4.2-13381.zip
Enter file number [1-1] or [q] to cancel: 1
Starting local upgrade...
```

7 Выполните аутентификацию как суперадминистратор.

8 Проверьте версию ПО:

```
hostname# version
```

Удаленное обновление

Для обновления необходимо наличие на ViPNet Coordinator HW актуального CRL для проверки ЭП файла обновления. Срок действия CRL — 1 год. Если на момент обновления ПО срок действия CRL уже истечёт, обновление не выполнится.

Скачайте актуальный CRL по ссылке http://crl.infotecs.ru/InfoTeCS_TDC_Root_CA.crl и импортируйте его в хранилище ViPNet Coordinator HW одним из способов:

1 С помощью командного интерпретатора — скопируйте файл на USB-носитель и выполните:

```
hostname# service cert import
```

2 С помощью веб-интерфейса (возможно импортировать удалённо):

2.1 Выберите **Системные настройки** > **Сертификаты** > **Списки отозванных сертификатов (CRL)**.

2.2 Нажмите **Импортировать.**

2.3 Нажмите **Загрузить файл** и выберите CRL.

2.4 Нажмите **Импортировать**.

Удаленное обновление выполняется в ViPNet Prime и не требует локального подключения к ViPNet Coordinator HW. Подробнее см. «ViPNet Prime. Руководство администратора», раздел «Отправка обновлений на узлы».

Обновление ПО в кластере

Локальное обновление

1 Убедитесь, что на обоих узлах кластера запущена служба `failoverd`:

```
hostname# failover show info
```

2 Выключите интерфейс синхронизации на обоих узлах:

```
hostname# inet ifconfig <интерфейс> down
```

Затем отсоедините кабель синхронизации от узлов кластера.

3 Обновите ПО на пассивном узле локально:

- Обновление ПО с версий 4.5.x до версии 5.4.x.
- Обновление ПО с версий 5.1.x, 5.2.x и 5.3.x до версии 5.4.x.

4 После обновления перезагрузите пассивный узел и убедитесь в его стабильной работе:

4.1 Проверьте текущее состояние служб ViPNet:

```
hostname# failover show info
```

Все службы должны быть запущены, система защиты от сбоев должна работать в режиме кластера.

4.2 В течение некоторого времени (около 15 минут) понаблюдайте за работой пассивного узла и убедитесь, что он не перезагружается.

5 Переключите активный узел в пассивный режим:

```
hostname# failover stop
hostname# failover start passive
```

В результате пассивный узел, на котором было обновлено ПО, перейдет в активный режим, а узел со старой версией ПО — в пассивный режим.

6 Обновите ПО на пассивном узле (шаг 3).

7 Перезагрузите пассивный узел и убедитесь в его стабильной работе (шаг 4).

8 Соедините оба узла кабелем синхронизации и включите интерфейсы синхронизации:

```
hostname# inet ifconfig <интерфейс> up
```

9 Убедитесь, что синхронизация работает:

9.1 Включите резервирование группы файлов конфигурации в файле `failover.ini` в секции `[sendconfig]`.

9.2 Измените какую-либо настройку в конфигурационном файле на активном узле.

9.3 Через некоторое время проверьте наличие этих же изменений на пассивном узле.

Удалённое обновление

Удалённое обновление ПО выполняется в ViPNet Prime. Подробнее см. «ViPNet Prime. Руководство администратора», раздел «Отправка обновлений на узлы».

Внимание!



- Перед удалённым обновлением ПО убедитесь, что к ViPNet Coordinator HW не подключено ни одно USB-устройство. Иначе это может повлиять на успешность процесса обновления (см. При удалённом обновлении ПО обновился только один узел кластера).
- При обновлении ПО с версий 4.5.x до версии 5.4.x требуется инициализация ViPNet Coordinator HW на узлах кластера, выполняемая локально (подробнее см. «Подготовка к работе», разделы «Инициализация в консольном режиме» и «Инициализация в полноэкранном режиме»).

Возврат к ПО версий 4.5.x

После обновления ПО с версий 4.5.x до версии 5.4.x вы можете вернуться к исходным версиям, например, если возникли проблемы в работе сети ViPNet.

Особенности возврата к исходной версии

- При возврате к исходной версии вы можете:
  - Восстановить конфигурацию ViPNet Coordinator HW из ранее сохраненного файла справочников, ключей и настроек (`.vbe`). Для восстановления конфигурации кластера необходимы файлы справочников, ключей и настроек обоих узлов.
  - Выполнить первичную настройку ViPNet Coordinator HW с помощью файла дистрибутива ключей (`.dst`).
- Журнал IP-пакетов, созданный в версии 5.4.x, не сохраняется.
- На время возврата будет включено ведение локального системного журнала.
- Журналы, используемые только в версии 5.4.x, например журналы сессий, СКЗИ и DNS-запросов, сохраняются; ведение этих журналов будет продолжено в случае обновления ПО до версии 5.4.x.

Перед возвратом к исходной версии

1 Необходимо наличие на ViPNet Coordinator HW актуального CRL для проверки ЭП файла обновления. Срок действия CRL — 1 год. Если на момент обновления ПО срок действия CRL уже истечёт, обновление не выполнится.

   Скачайте актуальный CRL по ссылке http://crl.infotecs.ru/InfoTeCS_TDC_Root_CA.crl и на шаге 2 скопируйте файл на USB-носитель.

2 Скопируйте на USB-носитель с файловой системой FAT32, ext2, ext3 или ext4:

   2.1 Файл обновления ПО исходной версии и файл ЭП, например:

   - `hw1000_vipnet_base_x86_64_driv_4.5.8-1182.lzh`;
   - `hw1000_vipnet_base_x86_64_driv_4.5.8-1182.lzh.sig`.

   2.2 Файл справочников, ключей и настроек, например:

   `hw1000-15ea000b-2025-02-09-12-36-21.vbe`.

   2.3 Файл дистрибутива ключей, например `abn_062b.dst`.

   2.4 CRL: `InfoTeCS_TDC_Root_CA.crl`.

Возврат к исходной версии

1 Подключитесь к ViPNet Coordinator HW с помощью консоли. При подключении к ViPNet Coordinator VA используйте консоль платформы виртуализации.

2 Войдите в режим администратора:

```
hostname# enable
```

3 Импортируйте CRL (файл `InfoTeCS_TDC_Root_CA.crl`):

```
hostname# service cert import
```

4 Запустите возврат к исходной версии:

```
hostname# admin upgrade software
```

5 Подключите USB-носитель к ViPNet Coordinator HW (виртуальной машине ViPNet Coordinator VA) и нажмите **Enter**:

```
Insert USB flash drive or CD and press <Enter>

Checking integrity of 'hw1000_vipnet_base_x86_64_driv_4.5.8-1182.lzh.'...

Checking integrity of 'hw1000-15ea000b-2025-02-09-12-36-21.vbe.'...
```

6 Выберите файл обновления — нажмите `1`:

```
Select file to use for software upgrade:

1 — /mnt/tmp/sdb1/hw1000_vipnet_base_x86_64_driv_4.5.8-1182.lzh

2 — /mnt/tmp/sdb1/hw1000-15ea000b-2025-02-09-12-36-21.vbe

Enter file number [1-2] or [q] to cancel: 1

Starting local upgrade...

...
```

7 В мастере установки дистрибутива ключей выполните одно из действий:

- Восстановление конфигурации ViPNet Coordinator HW из файла `hw1000-15ea000b-2025-02-09-12-36-21.vbe`.
- Первичная настройка ViPNet Coordinator HW с помощью файла дистрибутива ключей `abn_062b.dst`.

Подробнее см. документ «Подготовка к работе» версий 4.5.x, раздел «Первичная настройка ViPNet Coordinator HW».

Возврат к исходной версии в кластере

1 Убедитесь, что на обоих узлах запущена служба `failoverd`:

```
hostname# failover show info
```

2 Выключите интерфейс синхронизации на обоих узлах кластера:

```
hostname# inet ifconfig <интерфейс> down
```

Затем отсоедините кабель синхронизации от узлов кластера.

3 Выполните возврат ПО на пассивном узле (см. предыдущий сценарий «Возврат к исходной версии»).

4 Перезагрузите пассивный узел и убедитесь в его стабильной работе:

- Проверьте текущее состояние служб ViPNet:

```
hostname# failover show info
```

Все службы должны быть запущены, система защиты от сбоев должна работать в режиме кластера.

- В течение некоторого времени (около 15 минут) понаблюдайте за работой пассивного узла и убедитесь, что он не перезагружается.

5 Переключите активный узел в пассивный режим:

```
hostname# failover stop
hostname# failover start passive
```

В результате пассивный узел, на котором был выполнен возврат ПО, перейдет в активный режим, а узел с версией 5.4.x — в пассивный режим.

6 Выполните возврат ПО на пассивном узле (см. предыдущий сценарий «Возврат к исходной версии»).

7 Перезагрузите пассивный узел и убедитесь в его стабильной работе (шаг 4).

8 Соедините оба узла кабелем синхронизации и включите интерфейсы синхронизации:

```
hostname# inet ifconfig <интерфейс> up
```

Возврат к ПО версий 5.1.x, 5.2.x и 5.3.x

Под возвратом ПО понимается установка более ранней версии ПО из файла обновления.

Внимание!

- Возврат к предыдущей версии ПО удалит все ключи и настройки ViPNet Coordinator HW.
- После установки ПО необходимо выполнить инициализацию ViPNet Coordinator HW с помощью нового дистрибутива ключей `*.ds5`.

Перед возвратом к предыдущей версии

1 Экспортируйте конфигурацию ViPNet Coordinator HW в файл `*.ecf`. Это позволит восстановить настройки, если возврат к предыдущей версии ПО пройдёт некорректно. Для этого выполните:

```
hostname# machine backup export usb
```

Примечание. После возврата к предыдущей версии ПО невозможно восстановить настройки из резервной копии конфигурации (`*.ecf` или `*.vbe`), созданной в ViPNet Coordinator HW текущей версии.

2 При необходимости экспортируйте журнал IP-пакетов:

```
hostname# machine logs export network-traffic usb
```

3 Необходимо наличие на ViPNet Coordinator HW актуального CRL для проверки ЭП файла обновления. Срок действия CRL — 1 год. Если на момент обновления ПО срок действия CRL уже истечёт, обновление не выполнится.

Скачайте актуальный CRL по ссылке http://crl.infotecs.ru/InfoTeCS_TDC_Root_CA.crl и на шаге 4 скопируйте файл на USB-носитель.

4 Скопируйте на USB-носитель с файловой системой FAT32, ext2, ext3 или ext4:

- Файл обновления ПО и файл ЭП, например:

  `hw1000_vipnet_base_x86_64_driv_5.3.2-8878.zip`;

  `hw1000_vipnet_base_x86_64_driv_5.3.2-8878.zip.sig`.
- Файл дистрибутива ключей `*.ds5` для инициализации ViPNet Coordinator HW.
- CRL: `InfoTeCS_TDC_Root_CA.crl`.

Возврат к предыдущей версии

1. Подключитесь к ViPNet Coordinator HW с помощью консоли. При подключении к ViPNet Coordinator VA используйте консоль платформы виртуализации.
2. Войдите в режим администратора:

   ```
   hostname# enable
   ```

3. Импортируйте CRL (файл `InfoTeCS_TDC_Root_CA.crl`):

   ```
   hostname# service cert import
   ```

4. Выполните команду обновления ПО:

   ```
   hostname# admin upgrade software
   ```

5. Подключите USB-носитель к ViPNet Coordinator HW и нажмите **Enter**.
6. Введите номер файла обновления из списка и нажмите **Enter**.
7. Подтвердите сброс настроек и установку обновления — введите `Y` и нажмите **Enter**:

   ```
   Warning: You are about to downgrade application software version to 5.3.2-8878.

   Application will be returned to factory settings upon downgrade. It is highly
   recommended to make backup of current settings using commands "machine backup export"
   (*.ecf) or "machine config export" (*.vbe), and journals. Note, backup of current
   settings will not be applicable on downgraded version.

   Continue downgrade [Yes/No]? Y
   ```

8. Дождитесь завершения установки. ViPNet Coordinator HW будет перезагружен автоматически.
9. После перезагрузки выполните инициализацию ViPNet Coordinator HW с помощью дистрибутива ключей `*.ds5`. Подробнее см. в документе «ViPNet Coordinator HW. Подготовка к работе».

Установка ПО в кластере

1. Выключите интерфейсы синхронизации на обоих узлах и отсоедините кабель между ними.
2. На обоих узлах выполните возврат к более ранней версии ПО.
3. Выполните инициализацию с использованием одного дистрибутива ключей `*.ds5` на обоих узлах кластера.
4. После инициализации выполните шаги инструкции по настройке кластера (см. Развертывание кластера).

Локальное обновление DPI

Для поддержания набора классифицируемых приложений, прикладных протоколов и их групп в актуальном состоянии необходимо обновлять DPI. Также вы можете выполнить возврат к версии DPI, вплоть до версии, которая входила в ПО ViPNet Coordinator HW комплекта поставки. В обоих случаях (возврат или обновление) будут деактивированы (см. Деактивация транзитных фильтров открытой сети после обновления ПО) сетевые фильтры, в которых заданы приложения, прикладные протоколы и их группы, отсутствующие в предыдущей версии или не поддерживаемые новой версией.

Перед обновлением

На USB-носитель с файловой системой FAT32, ext2, ext3 или ext4 скопируйте файл обновления DPI и файл ЭП, например:

- `hw1000_vipnet_base_x86_64_5.4_10.0.238_dpi.zip`
- `hw1000_vipnet_base_x86_64_5.4_10.0.238_dpi.zip.sig`

Обновление

1. Подключитесь к ViPNet Coordinator HW с помощью консоли. При подключении к ViPNet Coordinator VA используйте консоль платформы виртуализации.
2. Выполните аутентификацию как суперадминистратор.
3. Перейдите в режим настройки:

   ```
   hostname> enable
   ```

4. Запустите обновление:

   ```
   hostname# service dpi update usb
   ```

5. В строке `During update, firewall will be stopped and all connections will be blocked. Are you sure you want to continue? [Yes/No]:` введите `Y` и нажмите **Enter**.
6. Подключите USB-носитель с файлами обновления к ViPNet Coordinator HW (виртуальной машине ViPNet Coordinator VA) и нажмите **Enter.**
7. Выберите из нумерованного списка найденных файлов обновления DPI файл нужной версии — введите его номер и нажмите **Enter**. После завершения обновления ViPNet Coordinator HW перезагрузится автоматически.

14

Работа с журналами

Журнал IP-пакетов 376

Журнал сессий 386

Журналы аудита и СКЗИ 387

Журнал MFTP 389

Журнал DNS-запросов 390

Системный журнал 391

Экспорт журнала IP-пакетов на USB-носитель 394

Экспорт журналов аудита, СКЗИ, MFTP, DNS-запросов и системного журнала на USB-носитель 396

Экспорт журнала IP-пакетов или журнала сессий по сети в формате CEF 397

Журнал IP-пакетов

Способы регистрации IP-пакетов

ViPNet Coordinator HW может регистрировать IP-пакеты в журнале одним из способов:

- Регистрация по сетевым фильтрам:

  У каждого сетевого фильтра есть параметр `log`, который указывает, регистрировать обработанные им IP-пакеты или нет. По умолчанию этот параметр включён на всех сетевых фильтрах с действием `drop` и `reject`, поэтому регистрируются только заблокированные и отклонённые IP-пакеты. Вы можете включить или отключить регистрацию IP-пакетов на любом настраиваемом сетевом фильтре отдельно (см. Настройка регистрации IP-пакетов и сессий при срабатывании фильтров). Этот способ используется по умолчанию после инициализации ViPNet Coordinator HW.

- Регистрация по сетевым интерфейсам:

  - каждый пропущенный и заблокированный локальный IP-пакет отображается в журнале один раз — на том интерфейсе, через который он прошёл, или на том интерфейсе, на котором он был заблокирован;
  - каждый пропущенный транзитный IP-пакет отображается в журнале дважды: первый раз — на интерфейсе, через который он пришёл, второй раз — на интерфейсе, через который он ушёл.

  Этот способ использовался в ViPNet Coordinator HW версий ниже 5.3.0 и будет по умолчанию использоваться после обновления ПО с этих версий до версии 5.4.0. При этом параметр `log` у сетевых фильтров игнорируется.

Для каждого сетевого интерфейса может быть выбран только один из способов регистрации IP-пакетов.

Широковещательные (`registerbroadcast`) и служебные (`registerevents`) IP-пакеты регистрируются только по интерфейсам независимо от способа регистрации других IP-пакетов.

Внимание! Не рекомендуется отключать регистрацию заблокированных IP-пакетов, поскольку это сделает невозможным расследование инцидентов информационной безопасности.

Настройка ведения журнала

Чтобы включить регистрацию событий по фильтрам после обновления ПО ViPNet Coordinator HW с версий ниже 5.3.0 до версии 5.4.0 и выше:

```
hostname# machine logs settings network-traffic <интерфейс> register passed by-rule
```

Чтобы отключить регистрацию IP-пакетов по сетевым фильтрам на одном интерфейсе:

```
hostname# machine logs settings network-traffic <интерфейс> register passed {on | off}
```

- `on` — регистрировать все IP-пакеты на интерфейсе: пропущенные, заблокированные и отклонённые;
- `off` — регистрировать только заблокированные и отклонённые IP-пакеты на интерфейсе.

После выполнения команды параметр `log` в сетевых фильтрах не будет учитываться для IP-пакетов, проходящих через указанный интерфейс.

Другие параметры ведения журнала вы можете настроить в конфигурационном файле `iplir.conf-<интерфейс или группа интерфейсов>` или с помощью команд:

Таблица 24. Команды настройки параметров секции [db]

Параметр	Описание параметра	Команда
maxsize	Максимальный размер журнала IP-пакетов интерфейса	machine logs settings network-traffic maxsize
timediff	Период времени, в течение которого связанные IP-пакеты объединяются в одну запись журнала	machine logs settings network-traffic timediff
omittcpclientport	Регистрацию только порта сервера для TCP-соединений: включена или выключена	machine logs settings network-traffic omit-client-port
registerall	Регистрация пропущенных IP-пакетов в журнале: включена или выключена	machine logs settings network-traffic register
registerbroadcast	Регистрация широковещательных IP-пакетов в журнале: включена или выключена	machine logs settings network-traffic register
registerevents	Регистрация служебных широковещательных IP-пакетов в журнале: включена или выключена	machine logs settings network-traffic register

Таблица 25. Команда просмотра параметров

Параметры	Команда
Секция [db]	machine logs settings show

Просмотр журнала

Журнал IP-пакетов можно просмотреть только на активном узле кластера.

Для просмотра записей журнала выполните команду:

```
hostname# machine logs show network-traffic
```

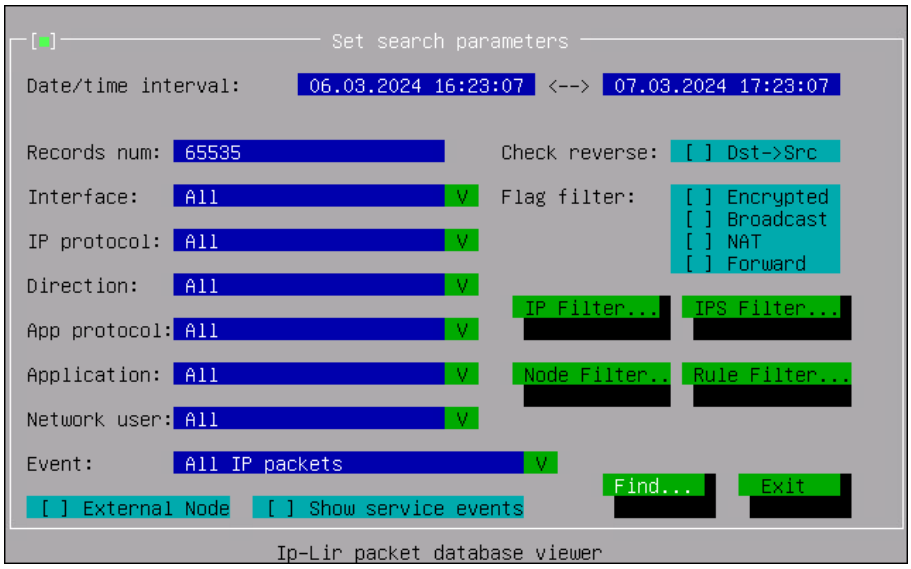


Рисунок 75. Параметры поиска записей в журнале IP-пакетов

По умолчанию предполагается просмотр записей обо всех пакетах, прошедших через сетевые интерфейсы собственного узла за последние 24 часа. Чтобы просмотреть эти записи, нажмите **Find**.

Чтобы просмотреть записи об определенных пакетах, настройте фильтрацию:

1 Укажите параметры IP-пакетов:

- **Date/time interval** — период времени, в который были зарегистрированы пакеты в формате: `YYYY-MM-DD hh:mm:ss <--> YYYY-MM-DD hh:mm:ss`.
- **Records num** — количество записей о зарегистрированных пакетах, которое будет отображено (по умолчанию — 65535). Поле **Records num** задает максимальное количество выводимых записей для каждого сетевого интерфейса. Если в параметрах поиска вы выбрали все сетевые интерфейсы (**All**), то общее количество выводимых записей будет равно сумме всех выводимых записей для каждого интерфейса.
- **Interface** — сетевой интерфейс, на котором были обработаны пакеты. По умолчанию — все доступные интерфейсы (**All**).
- **IP protocol** — IP-протокол, по которому были переданы пакеты:
  - **All** (по умолчанию) — любой протокол;
  - **ICMP** — только протокол ICMP;
  - **TCP** — только протокол TCP;
  - **UDP** — только протокол UDP;
  - **Except TCP, UDP, ICMP** — любой протокол, кроме TCP, UDP и ICMP.
- **Direction** — направление пакетов:
  - **All** (по умолчанию) — входящие и исходящие пакеты;
  - **Incoming** — входящие пакеты;

- **Outgoing** — исходящие пакеты.

- **App protocol —** прикладной протокол. По умолчанию — все прикладные протоколы (**All**).
- **Application** — приложение. По умолчанию — все приложения (**All**).

Примечание.

- Тип прикладного протокола или приложения не всегда определяется по первому IP-пакету (в зависимости от сочетания транспортного и прикладного протоколов). Например, вы создали разрешающее правило для прикладного протокола HTTP. В этом случае для разрешенного HTTP-соединения в журнале IP-пакетов будут отображаться несколько записей о пакетах с транспортным протоколом TCP и неизвестным прикладным протоколом, так как прикладной протокол еще не определен. После того, как прикладной протокол будет определен, в журнале будут отображаться записи о пакетах с транспортным протоколом TCP и прикладным протоколом HTTP.
- При обновлении модуля DPI некоторые прикладные протоколы, приложения и группы приложений могут быть удалены из списка поддерживаемых. Записи в журнале IP-пакетов с такими протоколами или приложениями будут отображать в качестве имени протокола или приложения «Неизвестно/Неизвестен (ID=номер протокола или приложения)».

- **Network user** — имя пользователя сети (см. Пользователь), прошедшего аутентификацию в Active Directory или Captive portal. По умолчанию — все пользователи (**All**).
- **Event** — тип события, которому соответствует IP-пакет (см. Типы событий журнала IP-пакетов). По умолчанию — события всех типов (**All**).
- **Check reverse** — включение в журнал ответных пакетов от получателя отправителю (**Dst -> Src**). Устанавливать этот флажок имеет смысл только, если в качестве отправителя и/или получателя пакетов указаны конкретные IP-адреса (**IP Filter**) или узлы (**Node Filter**).
- **Flag filter** — вид пакетов:
  - **Encrypted** — зашифрованные пакеты;
  - **Broadcast** — широковещательные пакеты;
  - **NAT** — транслированные пакеты;
  - **Forward** — транзитные пакеты.

  Вы можете выбрать один или несколько видов пакетов, установив соответствующие флажки. Транслированные (**NAT**) и транзитные (**Forward**) пакеты следует выбирать только для просмотра записей об IP-пакетах на маршрутизаторе.

2 Чтобы задать IP-адреса, коды стран или порты отправителя или получателя пакетов, нажмите **IP Filter**:

- если в списке **IP protocol** вы выбрали любые протоколы, кроме ICMP, укажите:
  - **Source**:
    - **IP address** — IP-адрес (**Value**) или диапазон IP-адресов (**Range**) отправителей пакетов. По умолчанию — любой адрес (**All**);

- **GeoIP** — код страны (**Value**). По умолчанию — все страны (**All**);

  Примечание. Вы можете задавать коды стран в формате ISO-3166 alpha2, в том числе указать несколько значений через запятую.

- **Port** — порт (**Value**) или диапазон портов (**Range**) отправителей. По умолчанию — все порты (**All**);

- **Destination:**

  - **IP address** — IP-адрес (**Value**) или диапазон IP-адресов (**Range**) получателей пакетов. По умолчанию — любой адрес (**All**);
  - **GeoIP** — код страны (**Value**). По умолчанию — все страны (**All**);
  - **Port** — порт (**Value**) или диапазон портов (**Range**) отправителей. По умолчанию — все порты (**All**);

- если в списке **IP protocol** вы выбрали протокол ICMP, укажите:

  - **Source**:

    - **IP address** — IP-адрес (**Value**) или диапазон IP-адресов (**Range**) отправителей пакетов. По умолчанию — любой адрес (**All**);
    - **GeoIP** — код страны (**Value**). По умолчанию — все страны (**All**);
    - **ICMP type** — тип (**Value**) или диапазон типов (**Range**) ICMP-пакетов;

  - **Destination:**

    - **IP address** — IP-адрес (**Value**) или диапазон IP-адресов (**Range**) получателей пакетов. По умолчанию — любой адрес (**All**);
    - **GeoIP** — код страны (**Value**). По умолчанию — все страны (**All**);
    - **ICMP code** — код (**Value**) или диапазон кодов (**Range**) ICMP-пакетов.

3 Чтобы задать фильтрацию по номеру или группе правил IPS, нажмите **IPS Filter** и укажите:

- **IPS Rule ID** — идентификатор правила IPS.
- **IPS Group** — группа правил IPS.
- **IPS Description** — название правила IPS.

  Если вы указали более одного атрибута правила IPS, то они будут связаны логическим отношением «И».

4 Чтобы задать фильтрацию по номеру сетевого фильтра или по номеру конфигурации сетевых фильтров, нажмите **Rule Filter** и введите номер конфигурации в поле **Rules Set ID** и номер сетевого фильтра в данной конфигурации в поле **Rule ID**. По умолчанию в полях **Rule ID** и **Rules Set ID** установлено значение **All**, что соответствует отображению всех сетевых фильтров всех конфигураций.

Примечание. Номер текущей конфигурации сетевых фильтров устанавливается равным 1 при инициализации ViPNet Coordinator HW и увеличивается при каждом изменении сетевых фильтров, правил трансляции адресов, файлов конфигурации или переключении режимов системы защиты от сбоев.

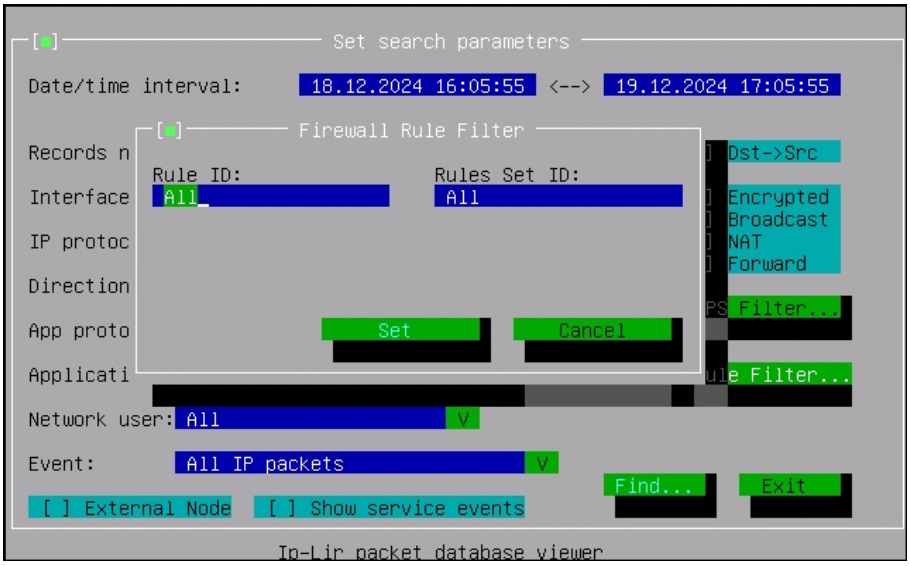


Рисунок 76. Фильтрация по номеру сетевого фильтра и конфигурации

5 Чтобы выбрать узел отправителя или получателя, нажмите **Node Filter**:

5.1 Для выбора узла отправителя нажмите **Select source Node**, для выбора узла получателя — **Select destination Node**.

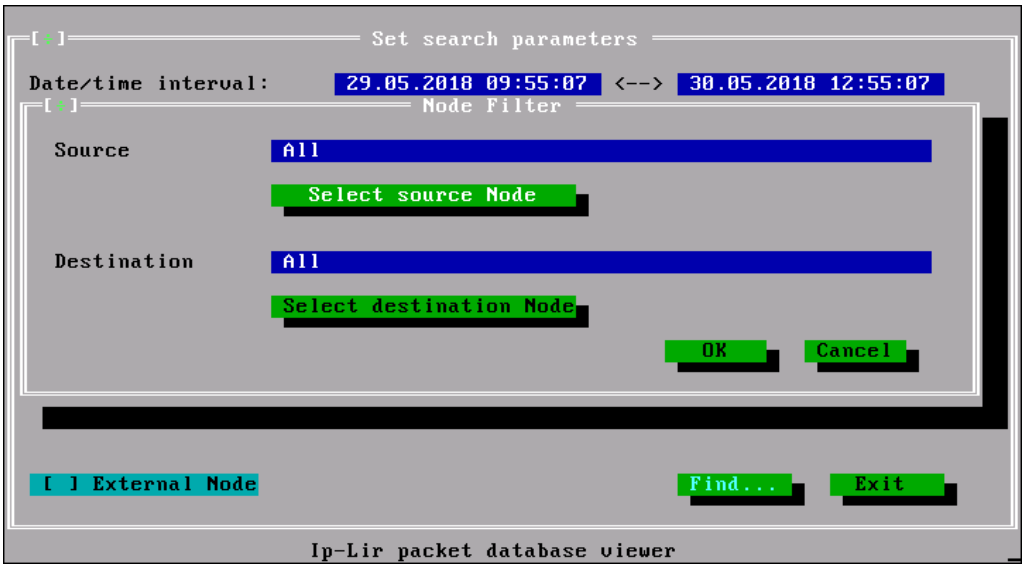


Рисунок 77. Выбор узла отправителя и получателя

В результате откроется таблица со списком узлов ViPNet, с которыми у данного узла есть связь: **ID** — идентификатор узла, **Name** — имя узла.

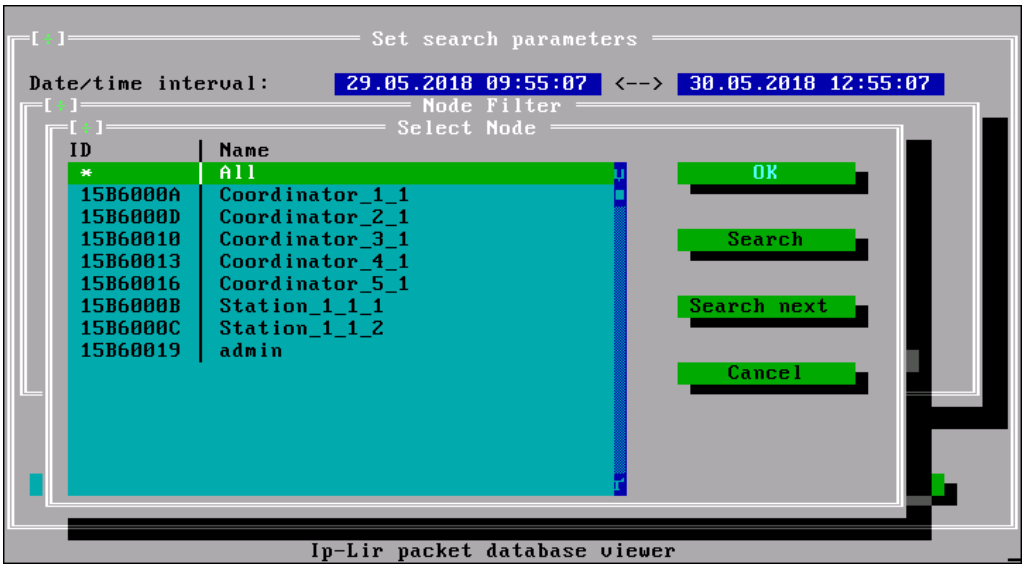


Рисунок 78. Выбор узла отправителя и получателя

5.2 Выберите нужный узел и нажмите **OK**.

Совет. Чтобы быстро найти нужный узел в списке, нажмите **Search**, введите часть идентификатора или имени узла и нажмите **OK**. Курсор будет переведен на строку первого узла, идентификатор или имя которого удовлетворяют условиям поиска. Для перехода к следующему такому узлу нажмите **Search next**.

---

6 Чтобы просмотреть журнал IP-пакетов удаленного узла:

Внимание! При просмотре журнала IP-пакетов удаленного узла действуют следующие особенности и ограничения:

- Удаленный узел должен быть доступен. При необходимости создайте разрешающие фильтры защищенной сети;
- Журнал ViPNet Coordinator HW версий 5.1.0 и выше имеет новый формат БД, поэтому его удаленный просмотр с помощью других продуктов ViPNet (за исключением ViPNet xFirewall версии 5.1 и выше) и ранних версий ViPNet Coordinator HW невозможен.

6.1 Выберите **External Node** и введите пароль администратора узла ViPNet.

6.2 Нажмите **Select** и выберите нужный узел ViPNet из списка.

7 Чтобы просмотреть служебные IP-пакеты, выберите **Show service events**.

8 Нажмите **Find**.

Список отфильтрованных записей журнала отображается в окне **View results**:

- **Date/time** — дата и время регистрации пакета;
- **Dev** — интерфейс, на котором был обработан пакет;
- **Flags** — направление и флаги пакетов:

- < — исходящий пакет;
- > — входящий пакет;
- **C** — зашифрованный пакет;
- **B** — широковещательный пакет;
- **D** — заблокированный пакет;
- **T** — транзитный пакет;
- **R** — пакет, который будет обработан правилами NAT открытой сети;
- **N** — пакет, который был обработан правилами NAT открытой сети;

- **Prot** — протокол, по которому был передан пакет;
- **Source IP** — IP-адрес отправителя пакета;
- **Port** — локальный порт для TCP- и UDP-пакетов или тип для ICMP-пакетов;
- **Destination IP** — IP-адрес получателя пакета;
- **Port** — порт удалённого узла для TCP- и UDP-пакетов или код для ICMP-пакетов.

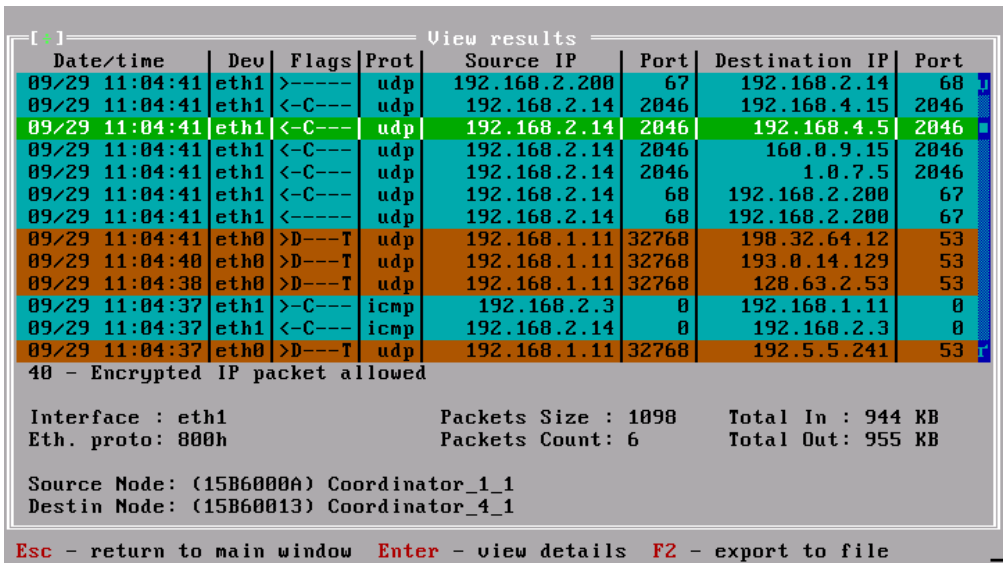


Рисунок 79. Просмотр записей из журнала IP-пакетов

1 Для просмотра краткой информации о пакете выберите его запись в списке. В окне под списком записей отобразятся:

- тип события, которому соответствует IP-пакет (см. Типы событий журнала IP-пакетов);
- **Interface** — интерфейс, на котором был получен IP-пакет;
- **Eth. proto** — шестнадцатеричный идентификатор протокола Ethernet;
- **Packets Size** — суммарный размер пакетов, агрегированных в одной записи;

> **Примечание.** Для зашифрованных пакетов в параметре **Packets Size** отображается размер пакетов со всеми служебными заголовками.

- **Packets Count** — количество пакетов, агрегированных в одной записи;

- **Total In** — суммарный размер всех входящих пакетов, соответствующих критериям поиска;
- **Total Out** — суммарный размер всех исходящих пакетов, соответствующих критериям поиска;



Примечание. Единицы измерения суммарного размера пакетов: **B** — байты, **KB** — килобайты, **MB** — мегабайты.

Символ `*` в поле **Total In** или **Total Out** пакета означает, что этот пакет не учтен в общем объеме входящего или исходящего трафика; `N/A` — отсутствие информации о размере пакетов, соответствующих выбранному типу события.

- **App proto** — тип прикладного протокола (см. Поддерживаемые прикладные протоколы);
- **Application** — тип приложения (см. Поддерживаемые приложения);
- **Network user** — пользователь сети (см. Пользователь).

2 Для просмотра подробной информации о пакете выберите запись и нажмите **Enter**. В окне **Record details** отобразятся:

- **Events** — номер и тип событий, объединенных в одну запись журнала (см. Типы событий журнала IP-пакетов);
- **Interval Begin, End** — начало и конец интервала времени, в течение которого несколько событий были объединены в одну запись журнала IP-пакетов;
- **Source** — IP-адрес и порт отправителя пакетов;
- **Destination** — IP-адрес и порт получателя пакетов;
- **IP protocol** — тип транспортного протокола (TCP/UDP);
- **Count and size** — количество и суммарный размер пакетов, агрегированных в одной записи;
- **Interface** — имя сетевого интерфейса, на котором были зарегистрированы события;
- **Eth. protocol** — шестнадцатеричный идентификатор протокола Ethernet;
- **Direction** — направление пакета (входящий, исходящий);
- **NAT** — флаг транслированного пакета;
- **Drop** — флаг блокировки пакета;
- **Broadcast** — флаг широковещательного пакета;
- **Forward** — флаг транзитного пакета;
- **Encryption** — признак шифрования пакета:
  - **VPN** — пакет зашифрован протоколом ViPNet;
  - **SSL/TLS** — пакет зашифрован протоколами SSL или TLS;
  - **Ignored** — признак шифрования не учитывался при обработке пакета;
- **IPS Rule ID** — идентификатор правила IPS;
- **IPS Description** — название правила IPS;

- **IPS Group** — группа правил IPS;
- **App protocol** — тип прикладного протокола (см. Поддерживаемые прикладные протоколы);
- **Application** — тип приложения (см. Поддерживаемые приложения);
- **Network user** — пользователь сети (см. Пользователь);
- **Source Node** — номер и имя сетевого узла ViPNet (отправителя пакетов);
- **Destin Node** — номер и имя сетевого узла ViPNet (получателя пакетов);
- **Rule UID** — идентификатор сработавшего правила.

Примечание. Для событий 3, 11, 30-32, 34-37, 40, 41 60-63, связанных с обработкой IP-пакета МЭ, в поле **Rule UID** указывается идентификатор сработавшего правила. Для события 40 идентификатор правила может отсутствовать (**0/Unknown**), если причина события не связана с МЭ, например, при декапсуляции входящего зашифрованного IPlir-пакета. Для остальных событий в поле **Rule UID** указывается **0/Unknown**.

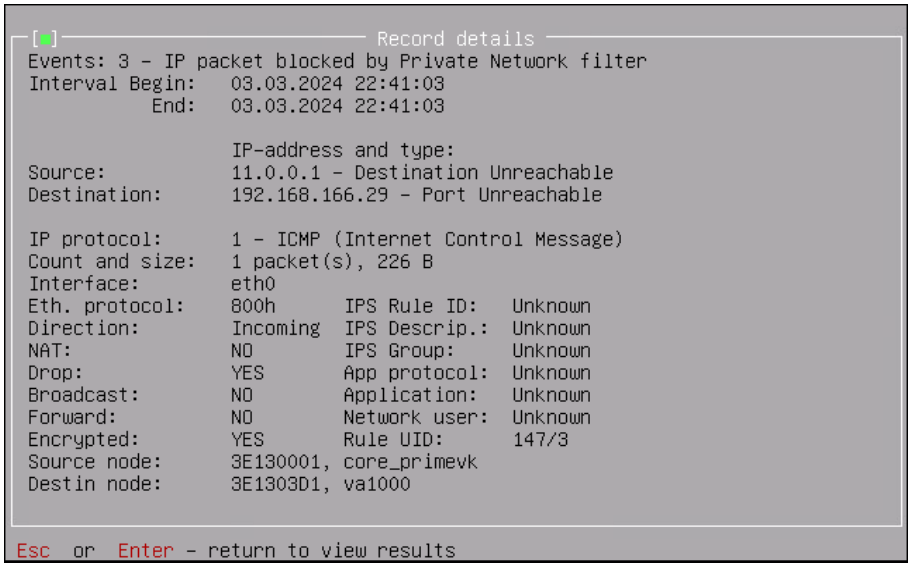


Рисунок 80. Просмотр подробной информации об IP-пакете

3 Для экспорта записей в текстовый файл, например для последующего анализа, нажмите **F2** и укажите файл для экспорта.

Журнал сессий

В журнале регистрируются сетевые сессии. Каждая сессия — непрерывный поток IP-пакетов между двумя сетевыми узлами, который определяется параметрами:

- адрес и порт узла–источника;
- адрес и порт узла–приёмника;
- протокол уровня 3–4 OSI;
- дата и время начала сессии;
- дата и время окончания сессии (для активной сессии — не определено).

Ведение журнала

По умолчанию ведение журнала отключено. Чтобы его включить:

```
hostname# machine logs sessions on
```

Журнал ведётся локально. Чтобы просмотреть процент заполнения журнала, выполните:

```
hostname# machine logs settings show
```

Максимальный размер журнала — 1024 Мбайт. При переполнении журнала старые записи автоматически заменятся новыми.

Просмотр журнала

Просмотр журнала сессий доступен только в веб-интерфейсе. Подробнее см. в документе «Настройка с помощью веб-интерфейса», в разделе «Журнал сессий».

Журналы аудита и СКЗИ

Ведение журнала аудита

В журнале аудита регистрируются события, связанные с выполнением запросов пользователей, в том числе от ViPNet Prime, и служебных запросов ViPNet Coordinator HW. Журнал ведется локально и ротируется. По умолчанию максимальный размер журнала — 50 Мбайт. Чтобы просмотреть текущий максимальный размер журнала и процент его заполнения, выполните:

```
hostname# machine logs setting show
```

При необходимости вы можете изменить максимальный размер журнала:

```
hostname# machine logs settings user-audit size <размер>
```

Минимальное значение — 10 Мбайт, максимальное — зависит от объёма свободной дисковой памяти.

Ведение журнала СКЗИ

В журнале СКЗИ регистрируются события, связанные с выполнением запросов криптографических операций. Журнал ведется локально и не ротируется. По умолчанию максимальный размер журнала — 50 Мбайт. Чтобы просмотреть текущий максимальный размер журнала и процент его заполнения, выполните:

```
hostname# machine logs setting show
```

При необходимости вы можете изменить максимальный размер журнала:

```
hostname# machine logs settings crypto-audit size <размер>
```

Минимальное значение — 10 Мбайт, максимальное — зависит от объёма свободной дисковой памяти.

Просмотр журнала аудита и журнала СКЗИ

Чтобы просмотреть журнал аудита или журнал СКЗИ, выполните:

```
hostname# machine logs show {user-audit | crypto-audit}
```

Подробнее о параметрах команд см. документ «Справочник команд и конфигурационных файлов», раздел «Команды группы machine».

Просмотр событий журнала аудита и журнала СКЗИ на удаленном сетевом узле

Чтобы просматривать события журнала аудита и журнала СКЗИ на удаленном сетевом узле, настройте удаленное протоколирование системного журнала (см. Системный журнал).

Формат событий журнала аудита и журнала СКЗИ в системном журнале:

```
<timestamp> <hostname> <hostname>[<pid>]: <type> [<hostname>] [<failover mode>] <event>
[<result>] [<initiator>] Details: <event details>
```

- `<timestamp>` — дата и время события.
- `<hostname>` — имя узла.
- `<pid>` — ID процесса.
- `<type>` — тип события:
  - `<crypto>` — событие журнала СКЗИ.
  - `<management>` — событие журнала аудита.
- `<failover mode>` — режим работы системы защиты от сбоев:
  - `Single Mode` — одиночный режим.
  - `Active Mode` — активный узел кластера.
  - `Passive Mode` — пассивный узел кластера.
- `<event>` — описание события.
- `<result>` — результат выполнения операции:
  - `success` — успешно.
  - `failed` — ошибка.
- `<initiator>` — инициатор события:
  - Имя учётной записи — имя локальной или централизованной учётной записи пользователя.
  - `System` — служебный запрос.
  - `System.Prime` — запрос ViPNet Prime.
- `<event details>` — дополнительная информация о событии (может отсутствовать).

Например:

```
May 30 14:36:04 2022 va2000 itcs-aad[7375]: <crypto> [va51-3617] [local] [Single Mode]
<admin> logged in. [success] [System] Details: ticket:AAA__4ee13d_6272b0_ab9226_74df7c
```

```
May 30 14:36:04 2022 va2000 webgui-fcgi-server[10369]: <management> [va51-3617] [local]
[Single Mode] Show idle session time-out [success] [admin] Details:
```

Журнал MFTP

Ведение журнала

Транспортный сервер (MFTP) записывает информацию о полностью принятых, отправленных, удаленных и поврежденных транспортных конвертах MFTP в журнал MFTP. Максимальный размер журнала задается в настройках сервера MFTP, при превышении которого наиболее ранние записи перезаписываются новыми. При уменьшении текущего максимального размера журнала MFTP наиболее ранние записи удаляются. Подробнее о настройке журнала MFTP см. документ «Справочник команд и конфигурационных файлов», раздел «Файл mftp.conf. Секция [journal]».

Просмотр журнала

Чтобы просмотреть журнал MFTP, выполните:

```
hostname# machine logs show mftp
```

Подробнее о команде см. документ «Справочник команд и конфигурационных файлов», раздел «Команды группы machine».

Журнал DNS-запросов

Ведение журнала

В журнале DNS-запросов регистрируются события, связанные с обработкой запросов локальным DNS-сервером ViPNet Coordinator HW:

- дата и время запроса;
- IP-адрес и порт, с которого поступил запрос;
- запрошенное доменное имя;
- тип запрошенной DNS-записи.

Журнал ведется локально и ротируется. По умолчанию размер журнала:

- 10 Мбайт — для исполнений с одним дисковым накопителем;
- 50 Мбайт — для исполнений с двумя дисковыми накопителями.

Чтобы просмотреть текущие настройки ведения журнала и статус локального DNS-сервера:

```
hostname# inet show dns
```

При необходимости вы можете изменить размер журнала:

```
hostname# inet dns querylog size <размер>
```

- 1 — 50 Мбайт: для исполнений с одним дисковым накопителем;
- 1 — 200 Мбайт: для исполнений с двумя дисковыми накопителями.



Внимание! Если вы уменьшили размер журнала, а его текущий размер достиг или превышает новое значение, он автоматически будет ротирован.

Чтобы очистить журнал:

```
hostname# machine logs clear dns
```

По умолчанию ведение журнала включено, DNS-запросы регистрируются после запуска DNS-сервера. Чтобы отключить ведение журнала:

```
hostname# inet dns querylog off
```

Просмотр журнала

Чтобы просмотреть все записи журнала:

```
hostname# inet dns querylog show
```

Также вы можете посмотреть записи журнала, содержащие определенный текст:

```
hostname# inet dns querylog show filtered <строка>
```

Системный журнал

Ведение журнала

Все службы ViPNet Coordinator HW записывают информацию о событиях, происходящих в процессе их работы, в системный журнал. Это позволяет контролировать работоспособность ViPNet Coordinator HW, своевременно выявлять и устранять причины сбоев в его работе. Журнал может храниться на ViPNet Coordinator HW (локальное ведение журнала) или на удалённом сетевом узле (удалённое ведение журнала).



Внимание! Во всех исполнениях ViPNet Coordinator HW по умолчанию включено локальное ведение журнала:

- в исполнении с одним дисковым накопителем (HW50) в журнал записывается информация первого уровня важности;
- во всех остальных исполнениях в журнал записывается информация третьего уровня важности.

В случае локального хранения журнала предусмотрена автоматическая ротация файла журнала, выполняемая, когда размер файла журнала достигает:

- 50 Мбайт — для всех исполнений с одним дисковым накопителем;
- 1 Гбайт — для остальных исполнений.

При ротации заполненный файл журнала переименовывается, при этом другой файл журнала, который был переименован раньше остальных, удаляется. Таким образом на ViPNet Coordinator HW всегда хранятся:

- для исполнений с одним дисковым накопителем — три заполненных файла журнала и один текущий файл, в который ведётся запись событий;
- для остальных исполнений — десять заполненных файлов и один текущий файл.

Вы можете установить другие настройки параметров ведения системного журнала:

- Чтобы выбрать место хранения системного журнала:

  ```
  hostname# machine set loghost {<IP-адрес> | <доменное имя> | local}
  ```

  Укажите IP-адрес или доменное имя сетевого узла для удалённого ведения журнала или `local` для локального.

  Особенности настройки удалённого ведение журнала:

  - Если вы выбрали открытый узел для удалённого ведения журнала, на ViPNet Coordinator HW задайте локальный фильтр открытой сети, разрешающий исходящий трафик по протоколу UDP на порт 514 этого открытого узла.
  - При переключении интерфейса ViPNet Coordinator HW, через который передаются события журнала на удалённый узел, в режим получения настроек от DHCP-сервера возможна временная потеря связи с удалённым узлом.

Чтобы избежать потери информации во время отсутствия связи, перед настройкой интерфейса включите локальное ведение журнала:

```
hostname# machine set loghost local
```

После применения настроек снова включите удалённое ведение журнала.

- В кластере не рекомендуется использовать удалённое ведение журнала, так как на удалённый сетевой узел не будут передаваться журналы с пассивного узла (то есть часть информации о работе ViPNet Coordinator HW будет утеряна).

  Если необходимо настроить удалённое ведение журнала в кластере, задайте параметры ведения журнала на обоих узлах кластера, так как они не передаются с активного узла на пассивный.

- Чтобы отключить ведение системного журнала:

  ```
  hostname# machine set loghost null
  ```

- Чтобы изменить уровень важности событий служб, регистрируемых в системном журнал:

  - для `iplircfg` выполните:

    ```
    hostname# iplir option syslog-level <уровень важности>
    ```

  - для `failoverd` и `mftpd` — в секции `[debug]` конфигурационных файлов `failover.ini`, `mftp.conf` настройте параметр `debuglevel`.



Примечание. В большинстве случаев изменять уровень важности, выбранный по умолчанию, не рекомендуется, особенно в исполнении с одним дисковым накопителем (HW50). При повышении уровня необходимо учитывать, что размер файла журнала будет быстро увеличиваться, вследствие чего, будет чаще производиться его ротация при достижении максимального размера (см. Системный журнал).

- Чтобы сообщения о работе службы выводились на консоль командного интерпретатора:

  ```
  hostname# debug on <источник> <уровень важности>
  ```

- Чтобы выключить вывод сообщений на консоль командного интерпретатора, выполните:

  ```
  hostname# debug off.
  ```

Также вы можете настроить ведение журнала так, чтобы следить за работой разных служб на разных терминалах:

- В конфигурационном файле одной из служб в секции `[debug]` задайте нужные параметры, например:

  ```
  [debug]
  debuglogfile = syslog:daemon.debug
  debuglevel = 3
  ```

  И на одном из терминалов выполните команду:

  ```
  hostname# debug on daemon debug
  ```

- В конфигурационном файле другой службы в секции `[debug]` задайте параметры протоколирования, указав другое значение `<источника>`, например:

```
[debug]
debuglogfile = syslog:local0.debug
debuglevel = 3
```

И на другом терминале выполните команду:

```
hostname# debug on local0 debug
```

В результате на первый терминал будут поступать сообщения только от первой службы, на второй терминал — только от второй службы. Чтобы на первом терминале можно было следить за работой обеих служб, на нем в дополнение к первой команде выполните команду:

```
hostname# debug on local0 debug
```



Примечание. Выводимые на консоль командного интерпретатора сообщения о работе служб могут смешиваться с сообщениями самого интерпретатора и командами, набираемыми на консоли. Для просмотра набранной к данному моменту части команды и продолжения её ввода используйте комбинацию клавиш **Ctrl+L**.

Просмотр журнала

Чтобы просмотреть записи системного журнала, выполните:

```
hostname# machine logs show syslog
```

Экспорт журнала IP-пакетов на USB-носитель

1. Откройте журнал IP-пакетов:

   ```
   hostname# machine logs show network-traffic
   ```

2. Задайте параметры для выбора из журнала нужных записей и нажмите **Find**. Подробнее см. Журнал IP-пакетов.
3. В окне **View results** нажмите клавишу **F2**.
4. Введите имя файла, в который вы хотите сохранить журнал, или выберите из списка существующий файл; затем нажмите **Enter**.
5. Завершите просмотр журнала: нажмите клавишу **Esc**, затем **Exit**.
6. Выполните команду экспорта журнала на USB-носитель:

   ```
   hostname# machine logs export network-traffic usb <имя файла>
   ```

   В качестве имени файла укажите имя, которое вы задали при сохранении журнала на шаге 4.
7. Подключите USB-носитель к ViPNet Coordinator HW и нажмите **Enter**.
8. Если подключено несколько USB-носителей, введите номер USB-носителя и нажмите **Enter**.

   Дождитесь завершения экспорта.

Архив с журналом IP-пакетов `<имя файла>.tar.gz` будет сохранён на USB-носителе. Чтобы преобразовать журнал в удобный для чтения вид, распакуйте архив, откройте его с помощью Microsoft Excel и выполните импорт данных, указав в качестве разделителя символ `|`; журнал отобразится в виде таблицы:

- **Time begin** — дата и время начала регистрации пакета;
- **Time end** — дата и время окончания регистрации пакета;
- **Dev** — интерфейс, на котором был обработан пакет;
- **Eth** — шестнадцатеричный идентификатор протокола Ethernet;
- **Flags** — направление и флаги пакета;
- **Prot** — протокол, по которому был передан пакет;
- **Source IP** — IP-адрес отправителя пакета;
- **Port** — локальный порт TCP- и UDP-пакетов или тип для ICMP-пакетов;
- **Destination IP** — IP-адрес получателя пакета;
- **Port** — порт удалённого компьютера для TCP- и UDP-пакетов или код для ICMP-пакетов.
- **Size** — размер пакета (или суммарный размер пакетов, если количество пакетов больше единицы);

- **Cnt** — количество пакетов, относящихся к данному событию;
- **SourceNode** — узел отправителя;
- **DestinNode** — узел получателя;
- **Event** — код и название события, присвоенного пакету;
- **App proto** — прикладной протокол;
- **Application** — приложение;
- **Network user** — пользователь сети;
- **Rule ID** — идентификатор правила IPS, которое сработало на IP-пакет;
- **Rule description** — описание правила IPS, которое сработало на IP-пакет;
- **Rule group** — название группы правила IPS, которое сработало на IP-пакет.

Экспорт журналов аудита, СКЗИ, MFTP, DNS-запросов и системного журнала на USB-носитель

1. Выполните команду:

   ```
   hostname# machine logs export usb
   ```

2. Подключите USB-носитель к ViPNet Coordinator HW и нажмите **Enter**.

Файл архива журналов `logs_<id узла>_<платформа><ревизия>_<версия>_<имя>_<гггг_мм_дд_чч_мм_сс>.tar.gz` будет сохранен на USB-носителе.

Чтобы экспортировать журналы аудита, СКЗИ, MFTP, DNS-запросов и системный журнал на USB-носитель с их последующим удалением на ViPNet Coordinator HW:

1. Выполните команду:

   ```
   hostname# machine logs export-and-clear usb
   ```

2. Подключите USB-носитель к ViPNet Coordinator HW и нажмите **Enter**.

Файл архива журналов `logs-<id узла>_<платформа><ревизия>_<версия>_<имя>_<гггг_мм_дд_чч_мм_сс>.tar.gz` будет сохранен на USB-носителе, а журналы на ViPNet Coordinator HW будут удалены.

Файлы журналов в архиве:

- журнал аудита — `/var/log/audit_user.tar.gz`;
- журнал СКЗИ — `/var/log/audit_crypto.tar.gz`;
- журнал MFTP — `/var/log/mftpenv.log`;
- журнал DNS-запросов — `/var/log/namedlog`;
- системный журнал — `var/log/everything.log` и ротированные архивы.

Экспорт журнала IP-пакетов или журнала сессий по сети в формате CEF

Вы можете настроить экспорт событий журнала IP-пакетов или журнала сессий по сети в формате CEF (далее — сообщения CEF), например в систему управления информационной безопасностью.

Внимание!



- Следует учитывать, что ViPNet Coordinator HW не может отправлять более 6000 событий в секунду. Если количество событий, регистрируемых в секунду в журнале IP-пакетов или журнале сессий, превышает это значение в течение длительного периода, то потеря пакетов на стороне системы управления информационной безопасностью может достигать 1%.
- Экспорт журнала сессий в формате CEF при использовании протокола Syslog не обеспечивает гарантированной доставки событий журнала.

Особенности ведения и экспорта журналов

- Поддерживается одновременное ведение журнала IP-пакетов и журнала сессий.
- Доступна выборочная (по сетевым фильтрам) регистрация IP-пакетов и сессий в журналах.
- Можно настроить экспорт журнала IP-пакетов и (или) журнала сессий как одновременно на один сетевой узел–приемник сообщений CEF, так и параллельно на несколько узлов.

Настройка экспорта журналов

1 Для экспорта событий журнала сессий включите ведение журнала:

```
hostname# machine logs sessions on
```

2 Для экспорта событий журнала IP-пакетов:

2.1 Установите тип формирования сообщений CEF при регистрации IP-пакетов, проходящих через интерфейс:

```
hostname# machine logs settings cef event-type {all | blocked} <интерфейс>
```

где:

- `all` — для всех IP-пакетов;
- `blocked` — для блокированных IP-пакетов или с предупреждением о вторжении (по умолчанию).

2.2 Выберите события, для которых не будут формироваться сообщения CEF:

```
hostname# machine logs settings cef <интерфейс> exclude <события>
```

где `<события>` — номера событий, разделенные запятой.

При экспорте в ViPNet TIAS версии 3.8 и выше рекомендуется исключить все события, кроме 67 и 142.

2.3 При необходимости измените параметр `timediff`, который определяет:

- интервал времени, в течение которого одинаковые события объединяются в одну запись журнала IP-пакетов;
- периодичность отправки сообщений CEF.

Для этого выполните:

```
hostname# machine logs settings network-traffic <интерфейс> timediff <интервал>
```

2.4 Повторите шаги 2.1–2.3 для каждого интерфейса, события которого вы хотите экспортировать.

3 Добавьте сетевой узел–приемник сообщений CEF:

```
hostname# machine logs add cef server <имя> ip <адрес> port <порт>
```



Внимание!

Необходимо обеспечить доверенный канал передачи данных между ViPNet Coordinator HW и внешними системами (в том числе взаимодействующими системами защиты информации других типов), например выделенный физический канал или сеть ViPNet. Допускается осуществлять защиту каналов передачи данных организационными мерами, исключающими возможность утечки или перехвата защищаемых данных, или с помощью сертифицированных средств криптографической защиты информации.

---

4 Выберите журнал и включите экспорт событий на сервер мониторинга:

- Для журнала IP-пакетов:

  ```
  hostname# machine logs settings cef server <имя> on
  ```

- Для журнала сессий:

  ```
  hostname# machine logs settings cef server <имя> sessions on
  ```



Примечание. Чтобы экспортировать оба журнала на один сервер, добавьте новый сервер. При этом задайте такие же адрес и порт, но задайте другое имя сервера.

---

5 Если сетевой узел–приемник сообщений CEF расположен в открытой сети, создайте сетевой фильтр, разрешающий исходящее соединение:

```
hostname# firewall local add src @local dst <IP-адрес> <транспортный протокол> <порт>
pass
```

Для передачи сообщений в ViPNet TIAS задайте порт UDP 5004.

При использовании Syslog:

```
hostname# firewall local add src @local dst <IP-адрес> service @Syslog pass
```

Чтобы удалить сетевой узел–приемник сообщений CEF:

```
hostname# machine logs delete cef server <имя>
```

Просмотр настроек экспорта журналов

Чтобы просмотреть общие настройки экспорта журнала IP-пакетов или журнала сессий в формате CEF:

```
hostname# machine logs settings show
```

При выполнении команды отображаются:

- размеры журналов и процент их заполнения;
- статус ведения журнала сессий;
- список серверов–приемников сообщений CEF.

Чтобы посмотреть настройки удаленного сервера:

```
hostname# machine logs settings show <имя>
```

При выполнении команды отображаются:

- название, IP-адрес и порт сервера;
- выбранный журнал для экспорта:
  - `Sessions: OFF` — экспортируется журнал IP-пакетов;
  - `Sessions: ON` — экспортируется журнал сессий;
- настройки экспорта журнала IP-пакетов по сетевым интерфейсам (если экспортируется журнал пакетов).

Примеры записей журналов

Описание структуры записи журнала IP-пакетов см. в приложении Структура записи журнала IP-пакетов в формате CEF.

Пример записи для экспорта в формате CEF о событии блокировки IP-пакета межсетевым экраном:

```
<38> Dec 19 15:14:54 va100-5a280167 CEF:0|infotecs|HWVA VMWARE|5.4.1-6713|30|Local IP
packet blocked by Public Network filter|10|deviceExternalId=5a280167 start=1766157224000
end=1766157224000 src=172.19.0.1 dst=172.19.0.100 spt=44328 dpt=514 proto=udp cnt=13
dvc=172.19.0.1 out=120900 deviceOutboundInterface=eth0 cn1=800h cn1Label=Eth protocol hex
cs1=NAT no cs2=Drop yes cs3=Broadcast no cs4=Forward no cs5=Encrypted no cs1Label=FlagNAT
cs2Label=FlagDrop cs3Label=FlagBroadcast cs4Label=FlagForward cs5Label=FlagEncrypted
cs6=unknown cs6Label=Application name deviceDirection=1 app=unknown suser= reason=2/21
msg=Block All Traffic dvchost=va100-5a280167 customerURI=http://va100-5a280167:8080
```

Описание структуры записи журнала сессий см. в приложении Структура записи журнала сессий в формате CEF.

Пример записи для экспорта в формате CEF:

```
<38> Apr 02 07:09:56 va100-51de000b CEF:0|infotecs|HWVA VMWARE|5.4.1-6713|40|Encrypted IP
packet allowed|5|cs5Label=Single rule identifier cs5=4000005/14
deviceExternalId=5bdd0f6f cs2Label=Application name cs2=unknown cs4Label=State now
```

```
cs4=REPLIED,ASSURED app=unknown msg=pass-vpn-ssh out=100 in=52 cnt=3 proto=tcp dpt=22
dst=172.18.0.1 src=11.0.0.4 start=1775102915111 spt=43962 cs6Label=SessionID cs6=12
```

15

Мониторинг работы

Мониторинг по SNMP 402

Мониторинг нагрузки 410

Блокировка источников повышенной сетевой нагрузки 412

Просмотр статистики передачи данных 414

Мониторинг по SNMP

С помощью SNMP-агента вы можете удалённо получать информацию о работе ViPNet Coordinator HW, а также настроить автоматическое уведомление о наиболее важных событиях, например, потеря связи с пассивным узлом кластера.

Информация, доступная по протоколу SNMP, представлена в виде набора SNMP-параметров. Каждый параметр имеет уникальный идентификатор (OID). Список доступных SNMP-параметров ViPNet Coordinator HW вы можете просмотреть в приложении Базы управляющей информации (MIB) для протокола SNMP.

Примечание. Все SNMP-параметры доступны только для чтения.

Для получения информации о состоянии ViPNet Coordinator HW вы можете использовать любое ПО мониторинга по протоколу SNMP (SNMP-менеджер), например:

- ViPNet Prime (модуль Network Visibility System).
- Утилита snmpwalk (пакет net-snmp).
- Zabbix.

Сетевой узел с установленным SNMP-менеджером называется сервером мониторинга.

Примечание. В качестве сервера мониторинга мы рекомендуем использовать узел защищённой сети или туннелируемый узел. Если будет использоваться открытый узел, необходимо добавить сетевые фильтры, разрешающие SNMP-трафик:

```
hostname# firewall local add src <IP-адрес сервера мониторинга> dst @local udp dport 161 pass
hostname# firewall local add src @local dst <IP-адрес сервера мониторинга> udp dport 162 pass
```

Протокол SNMP поддерживает следующие способы получения информации:

- Передача параметров по запросу. При этом сервер мониторинга посылает SNMP-запрос на ViPNet Coordinator HW и получает в ответ значения параметров.
- Передача уведомлений. SNMP-агент ViPNet Coordinator HW автоматически отправляет SNMP-уведомления на сервер мониторинга при наступлении определённого события.

Примечание. Чтобы SNMP-запросы обрабатывались корректно, необходимо отправлять их на IP-адрес ViPNet Coordinator HW, который доступен с сервера мониторинга по кратчайшему маршруту.

Если вы включили передачу SNMP-уведомлений, то после включения или перезагрузки ViPNet Coordinator HW доставка первых уведомлений о старте служб `iplircfg`, `mftpd`, `webgui` и `failoverd` на сервер мониторинга не гарантирована. Причина — отсутствие связи с сервером мониторинга во время инициализации сетевой подсистемы.

Если вы импортируете на сервер мониторинга MIB-файлы, поддерживаемые ViPNet Coordinator HW, вы сможете:

- использовать в SNMP-запросах текстовые обозначения параметров вместо числовых (например, `infVipNetHostName` вместо `.1.3.6.1.4.1.10812.1.1.7`);
- получать текстовые обозначения некоторых числовых параметров в ответах на SNMP-запросы (например, при запросе состояния интерфейса, вместо значения `1` или `2`, вы получите значение `up` или `down`);
- получать уведомления от ViPNet Coordinator HW в виде текстовых обозначений параметров вместо числовых (например, `infvpnWebStart` вместо `.1.3.6.1.4.1.10812.1.0.10`).

SNMP-агент ViPNet Coordinator HW поддерживает одновременную работу по протоколам SNMPv1, SNMPv2c и SNMPv3.

Для ограничения доступа к SNMP-параметрам используются следующие подходы:

- В SNMPv1 и SNMPv2c используется параметр community, который является идентификатором и паролем доступа к SNMP-параметрам. ViPNet Coordinator HW ответит на SNMP-запрос, если community в запросе совпадает с любым из community, заданных на ViPNet Coordinator HW.

  Для получения SNMP-уведомлений сервером мониторинга в настройках его SNMP-менеджера, а также в настройках ViPNet Coordinator HW, необходимо задать community для уведомлений.

- В SNMPv3 используются учётные записи пользователей SNMP. ViPNet Coordinator HW ответит на SNMP-запрос, если пользователю разрешён доступ на чтение параметров и данные пользователя в запросе совпадают с данными любого из пользователей, заданных на ViPNet Coordinator HW:
  - имя пользователя;
  - пароль пользователя и алгоритм хэширования пароля;
  - тип аутентификации;
  - ключ и алгоритм шифрования (если заданы).

  Для получения SNMP-уведомлений сервером мониторинга в настройках его SNMP-менеджера укажите данные одного из пользователей SNMP, заданных на ViPNet Coordinator HW. При использовании уведомлений типа TRAP, в настройках SNMP-менеджера дополнительно к учётным данным пользователя укажите параметр `engineID` (OID .1.3.6.1.6.3.10.2.1.1.0).

Настройка SNMP-агента



Внимание! Рекомендуется настраивать SNMP-агент в выключенном состоянии, иначе при задании большого количества параметров увеличится время перезапуска службы SNMP-агента.

По умолчанию SNMP-агент выключен.

1 Для протоколов SNMPv1 и SNMPv2c:

1.1 Добавьте community для чтения SNMP-параметров:

```
hostname# inet snmp community add
```

Длина community — от 6 до 18 символов. Разрешённые символы — прописные и строчные буквы латинского алфавита, цифры и специальные символы: `. * / - : _ ? = @ , & ()`.

Максимальное количество community — 16.

1.2 Задайте адрес сервера мониторинга для отправки SNMP-уведомлений:

```
hostname# inet snmp trapsink add <адрес> [port <номер>] [{v1 | inform}]
```

- `<адрес>` — IP-адрес или доменное имя сервера мониторинга;
- `<номер>` — номер UDP-порта;
- `v1` — отправлять уведомления типа TRAP по протоколу SNMPv1;
- `inform` — отправлять уведомления типа INFORM по протоколу SNMPv2c.

Если порт и тип уведомлений не указан, устанавливаются следующие значения:

- Тип отправляемых уведомлений — TRAP.
- Протокол отправки уведомлений — SNMPv2c.
- Порт, на который отправляются уведомления — UDP 162.

При выполнении команды необходимо ввести community, которое задано на сервере мониторинга для приёма SNMP-уведомлений (trap community).

Вы можете использовать до 16 сетевых узлов в качестве серверов мониторинга.



Внимание! Если задан порт, отличный от UDP 162, необходимо добавить сетевой фильтр, разрешающий передачу SNMP-уведомлений на данный порт:

- для узла защищённой сети: `hostname# firewall vpn add src @local dst <идентификатор узла> udp dport <номер порта> pass`
- для туннелируемого узла: `hostname# firewall tunnel add src @local dst <IP-адрес> udp dport <номер порта> pass`
- для открытого узла: `hostname# firewall local add src @local dst <IP-адрес> udp dport <номер порта> pass`

1.3 Разрешите чтение SNMP-параметров:

```
hostname# inet snmp v2 ro on
```

1.4 Включите отправку SNMP-уведомлений:

```
hostname# inet snmp v2 traps on
```

2 Для протокола SNMPv3:

2.1 Добавьте нового пользователя для доступа к SNMP-параметрам:

```
hostname# inet snmp user add <имя пользователя> [{md5 | sha}]
```

При добавлении пользователя требуется задать пароль и алгоритм хэширования пароля MD5 (по умолчанию) или SHA.

Длина имени пользователя — от 1 до 32 символов. Разрешённые символы — прописные и строчные буквы латинского алфавита и цифры.

Длина пароля — от 8 до 32 символов. Разрешённые символы — прописные и строчные буквы латинского алфавита, цифры и специальные символы: `! @ # $ % ^ & * () - _ + = ; : ' " , . < > / ? \ | ` ~ [ ] { }`.



Внимание! Не используйте повторяющиеся последовательности символов в пароле. Иначе его хэш может совпасть с хэшем другого пароля. Например, пароли `AbcdAbcd` и `AbcdAbcdAbcd` будут иметь одинаковые хэши.



Примечание. По умолчанию пользователю разрешено чтение SNMP-параметров. Вы можете запретить чтение SNMP-параметров:

```
hostname# inet snmp user set <имя пользователя> read off
```

2.2 Для шифрования SNMP-трафика между сервером мониторинга и ViPNet Coordinator HW (по алгоритму AES-128) создайте ключ шифрования для пользователя:

```
hostname# inet snmp user set <имя пользователя> key
```

Длина ключа шифрования — от 8 до 32 символов. Разрешённые символы — прописные и строчные буквы латинского алфавита, цифры и специальные символы: `! @ # $ % ^ & * () - _ + = ; : ' " , . < > / ? \ | ` ~ [ ] { }`.



Внимание! Не используйте повторяющиеся последовательности символов в ключе шифрования. Иначе его хэш может совпасть с хэшем другого ключа. Например, ключи `AbcdAbcd` и `AbcdAbcdAbcd` будут иметь одинаковые хэши.



Примечание. Если задан ключ шифрования, его необходимо указывать в SNMP-запросах наряду с другими данными пользователя SNMP.

2.3 Разрешите отправку SNMP-уведомлений для пользователя:

```
hostname# inet snmp user set <имя пользователя> trapsess on
```

2.4 Задайте адрес сервера мониторинга для отправки SNMP-уведомлений:

```
hostname# inet snmp user set <имя пользователя> trapsess add <адрес> [port <номер>]
[inform]
```

- `<адрес>` — IP-адрес или доменное имя сервера мониторинга;
- `<номер>` — номер UDP-порта;
- `inform` — отправлять уведомления типа INFORM.

Если порт и тип уведомлений не указан, устанавливаются следующие значения:

- Тип отправляемых уведомлений — TRAP.
- Порт, на который отправляются уведомления — UDP 162.

Внимание!

Если задан порт, отличный от UDP 162, добавьте сетевой фильтр, разрешающий передачу SNMP-уведомлений на данный порт:



- для узла защищённой сети: `hostname# firewall vpn add src @local dst <идентификатор узла> udp dport <номер порта> pass`
- для туннелируемого узла: `hostname# firewall tunnel add src @local dst <IP-адрес> udp dport <номер порта> pass`
- для открытого узла: `hostname# firewall local add src @local dst <IP-адрес> udp dport <номер порта> pass`

Для уведомлений типа INFORM сервер мониторинга должен быть доступен при каждом запуске службы SNMP-агента, иначе SNMP-агент будет недоступен около минуты после каждой отправки уведомления.

2.5 Разрешите чтение SNMP-параметров по протоколу SNMPv3:

```
hostname# inet snmp v3 ro on
```

2.6 Включите отправку SNMP-уведомлений по протоколу SNMPv3:

```
hostname# inet snmp v3 traps on
```

3 По умолчанию SNMP-агент принимает запросы на UDP-порт 161. При необходимости измените номер порта:

```
hostname# inet snmp port <порт>
```



Внимание! При изменении номера порта добавьте соответствующий сетевой фильтр.

4 Включите запуск SNMP-агента при загрузке ViPNet Coordinator HW:

```
hostname# inet snmp autostart on
```

5 По умолчанию SNMP-агент регистрирует в системном журнале события с уровнем важности `error`. При необходимости измените уровень важности:

```
hostname# inet snmp logging <уровень важности>
```

Список возможных значений параметра `<уровень важности>`:

- `off` — регистрация событий выключена;
- `critical` — регистрируются критические ошибки, после которых SNMP-агент не может продолжить работу;
- `error` — регистрируются ошибки, после которых SNMP-агент может продолжать работу;
- `info` — регистрируется полная информация о работе SNMP-агента;
- `debug` — регистрируется служебная информация, используемая при отладке.

6 При необходимости задайте информацию о вашем ViPNet Coordinator HW, которая будет доступна по SNMP при чтении SNMP-параметров:

- Чтобы задать параметр **Контактное лицо** (sysContact OID .1.3.6.1.2.1.1.4.0):

  ```
  hostname# inet snmp system contact
  ```

- Чтобы задать параметр **Имя устройства** (sysName OID .1.3.6.1.2.1.1.5.0):

  ```
  hostname# inet snmp system name
  ```

- Чтобы задать параметр **Местоположение** (sysLocation OID .1.3.6.1.2.1.1.6.0):

  ```
  hostname# inet snmp system location
  ```



Примечание. Параметры **Имя устройства** и **Местоположение** не синхронизируются между узлами кластера.

7 Включите SNMP-агент:

```
hostname# inet snmp start
```

8 Проверьте выполненную настройку SNMP-агента:

```
hostname# inet snmp show
```

Полный список команд по настройке SNMP-агента см. в документе «Справочник команд и конфигурационных файлов».

Мониторинг кластера

Вы можете следить за состоянием обоих узлов кластера по протоколу SNMP. Приём SNMP-запросов и отправку SNMP-уведомлений выполняет активный узел. Для мониторинга пассивного узла кластера активный узел перенаправляет полученные SNMP-запросы на пассивный через интерфейс синхронизации и возвращает ответы отправителю.

Поскольку узлы кластера могут переключаться, SNMP-запрос должен указывать, какой из узлов должен на него ответить. Для этого используются следующие параметры SNMP-агента:

- При использовании SNMPv1 и SNMPv2c для каждого ViPNet Coordinator HW кластера создаётся community для режима кластера. SNMP-запрос с таким community будет адресован конкретному ViPNet Coordinator HW независимо от его текущего режима работы в кластере (активный или пассивный). При переключении системы защиты от сбоев в одиночный режим, community для режима кластера автоматически удаляется.
- При использовании SNMPv3 каждому узлу кластера назначается свой контекст (строка, идентифицирующая ViPNet Coordinator HW в кластере). Контексты создаются автоматически на активном узле в формате `Node<порядковый номер>`, где `<порядковый номер>` — число от 1, которое выбирается по возрастанию в соответствии с IP-адресом интерфейса синхронизации.

Для мониторинга кластера по протоколу SNMP:

1 Настройте SNMP-агент на активном узле кластера (см. Настройка SNMP-агента).

  Настройки будут переданы на пассивный узел при последующей синхронизации.

Примечание. Если на момент развёртывания кластера SNMP-агент уже настроен на одном из ViPNet Coordinator HW, запускайте `failover` в режиме кластера сначала на ViPNet Coordinator HW с настроенным SNMP-агентом. Тогда другой узел кластера получит актуальную конфигурацию SNMP-агента от активного узла. Исходная конфигурация агента на пассивном узле при этом удаляется.

2 Для SNMPv1 и SNMPv2c выполните действия на активном узле кластера:

2.1 Задайте community для мониторинга узла кластера:

```
hostname# inet snmp cluster node <IP-адрес> community
```

где `<IP-адрес>` — IP-адрес интерфейса синхронизации узла кластера.

В ответ на сообщение `Type community:` введите community, отличное от других community. Допустимая длина — от 6 до 18 символов: прописные и строчные буквы латинского алфавита, цифры и специальные символы: `( . * / - : _ ? = @ , &)`.

Примечание. Просмотреть созданные для режима кластера community вы можете:
`hostname# inet snmp cluster show community`

2.2 Разрешите чтение SNMP-параметров узлов кластера по протоколам SNMPv1 и SNMPv2c:

```
hostname# inet snmp cluster v2 on
```

Примечание. Если выводится ошибка: `SNMPv1 and SNMPv2c support is OFF. Please, turn it on first`, выполните действия:

- разрешите чтение SNMP-параметров на активном узле кластера: `hostname# inet snmp v2 ro on`
- повторно разрешите чтение SNMP-параметров: `hostname# inet snmp cluster v2 on`

3 Для SNMPv3 на активном узле кластера:

3.1 Просмотрите контексты, присвоенные узлам кластера, чтобы использовать их в SNMP-запросах:

```
hostname# inet snmp cluster show
```

3.2 Чтобы изменить контекст узла:

```
hostname# inet snmp cluster node <IP-адрес> context <контекст>
```

где `<IP-адрес>` – IP-адрес интерфейса синхронизации узла кластера.

Допустимая длина контекста — от 1 до 32 символов: прописные и строчные буквы латинского алфавита и цифры.

4 На пассивном узле запустите SNMP-агент:

```
hostname# inet snmp start
```

5 В зависимости от версии протокола SNMP используйте созданные community или контексты в SNMP-запросах для получения информации о состоянии конкретного узла кластера (см. руководство по настройке используемого SNMP-менеджера):

- При использовании протоколов SNMPv1 и SNMPv2c отправляйте SNMP-запрос с community соответствующего узла кластера.
- При использовании протокола SNMPv3 отправляйте SNMP-запрос с учётными данными пользователя, созданного с помощью команды `inet snmp user add`, и контекстом соответствующего узла. Если запрос не содержит контекст, ответ будет получен от активного узла кластера.

Мониторинг ViPNet-узлов

Чтобы обнаруживать потерю связи ViPNet Coordinator HW с другими узлами ViPNet, настройте автоматическую отправку SNMP-уведомлений о доступности узлов ViPNet на сервер мониторинга:

1 Настройте SNMP-агент (см. Настройка SNMP-агента).

2 Просмотрите список связанных узлов:

```
hostname# iplir node list
```

3 Включите проверку узла, доступность которого необходимо отслеживать:

```
hostname# iplir node <id узла> availability-monitoring on
```

где `<id узла>` — шестнадцатеричный идентификатор узла ViPNet.

Чтобы просмотреть состояние проверки узла ViPNet и его доступность, выполните команду:

```
hostname# iplir node <id узла> show
```

В строке `Availability monitoring` отобразится состояние проверки:

- `on` — включена; при этом в скобках будет указан текущий статус узла:
  - `available` — узел доступен;
  - `unavailable` — узел недоступен;
- `off` — выключена.

Мониторинг нагрузки

Производительность и пропускная способность ViPNet Coordinator HW зависят от обрабатываемого трафика, а определяются аппаратными характеристиками ViPNet Coordinator HW: центральным процессором (ЦП), оперативной памятью (ОП), дисковой подсистемой и сетевыми интерфейсами, нагрузку на которые вы можете контролировать, а именно:

- `core` — загрузку ЦП в %;
- `loadavg_0`, `loadavg_1`, `loadavg_3` — среднюю нагрузку на ЦП (среднее количество процессов в системной очереди) за последние 1, 5 и 15 минут;
- `mem_free` — количество свободной ОП в %;
- `mem_available` — количество доступной ОП в %;
- по каждому интерфейсу:
  - `PPS` — количество IP-пакетов в секунд;
  - `throughput` — скорость передачи IP-пакетов в битах в секунду;
  - `errps` — количества ошибок в секунду;
- `iopsps_hdd` — быстроту изменения скорости чтения/записи HDD-диска;
- `iopsps_ssd` — быстроту изменения скорости чтения/записи SSD-диска;
- `CPS` — количество новых соединений в секунду.

Значения контролируемых параметров разделены на зоны:

- зеленая — норма, вмешательство не требуется;
- желтая — повышенная нагрузка, при которой следует обратить внимание на возможные источники повышенной сетевой нагрузки;
- красная — критическая нагрузка, существенно влияющая на производительность и стабильность работы ViPNet Coordinator HW, при которой следует незамедлительно принять меры по обнаружению и блокировке источников повышенной сетевой нагрузки.

Пороги перехода значений контролируемых параметров из зоны в зону задаются в секциях `[CPU]`, `[Memory]`, `[Netdev]`, `[Disk]` и `[CPS]` файла `healthmon.ini`. События перехода значений контролируемых параметров из зеленой зоны в желтую, из желтой в красную, а так же при возврате в зеленую зону, регистрируются в системном журнале. Кроме того, вы можете настроить передачу SNMP-оповещений об этих событиях во внешнюю систему мониторинга (подробнее см. VIPNETFWLOAD-MIB).

По умолчанию:

- мониторинг нагрузки остановлен;
- в секциях `[CPU]`, `[Memory]`, `[Netdev]`, `[Disk]` и `[CPS]` разрешена передача SNMP-оповещений.

Чтобы настроить мониторинг нагрузки:

1 Откройте для изменения файл `healthmon.ini`:

```
hostname# healthmond edit
```

2 При необходимости измените границы зон контролируемых параметров в секциях `[CPU]`, `[Memory]`, `[Netdev]`, `[Disk]` и `[CPS]`.

3 Чтобы отправлять SNMP-оповещений во внешнюю систему мониторинга, настройте SNMP-агент ViPNet Coordinator HW (см. Настройка SNMP-агента).



Примечание. По умолчанию в секциях `[CPU]`, `[Memory]`, `[Netdev]`, `[Disk]` и `[CPS]` разрешена отправка SNMP-оповещений. Чтобы запретить отправку, задайте `snmp_enable = 0` в этих секциях.

4 Сохраните изменения — нажмите **Ctrl**+**O**, затем **Ctrl**+**X**.

5 Запустите мониторинг нагрузки:

```
hostname# healthmond start
```

6 Включите автозапуск мониторинга при перезагрузке:

```
hostname# healthmond autostart on
```

7 Просмотрите настройки мониторинга нагрузки и текущее значение контролируемых параметров:

```
hostname# healthmond show
```

Блокировка источников повышенной сетевой нагрузки

Мониторинг нагрузки, кроме контроля использования ресурсов центрального процессора, оперативной памяти, дисковой подсистемы и сетевых интерфейсов, позволяет выявлять и блокировать источники повышенной сетевой нагрузки — сетевые узлы, с которых на ViPNet Coordinator HW поступает большое количество IP-пакетов. Вы можете настроить автоматическую блокировку таких источников, при которой:

- выявляется и временно блокируется трафик от источников повышенной сетевой нагрузки, не попадающий под действие разрешающих фильтров МЭ;
- события блокировки источников повышенной сетевой нагрузки регистрируются в системном журнале;
- во внешнюю систему мониторинга передаются SNMP-оповещения о блокировке IP-адресов.

Параметры настройки автоматической блокировки источников повышенной сетевой нагрузки задаются в секции `[IP_ban]` файла `healthmon.ini`.

Источники повышенной сетевой нагрузки выявляются на основе анализа событий блокировки IP-пакетов (коды 30, 31) в журнале IP-пакетов для интерфейсов (`eth`, `alias eth`, `vlan`, `alias vlan`, `bond`, `alias bond`), заданных в `ifname`. Если количество заблокированных IP-пакетов за `blocking_interval` превышает порог `drops`, то источник попадает в список блокировки на время `ban_time`, по истечении которого удаляется из списка блокировки. Если при этом установлено продление блокировки `ban_again` и количество IP-пакетов, поступающих от источника, находящегося в списке блокировки, превышает порог `count_trigger`, то время блокировки продлевается, а источник остается в списке блокировки еще на время `ban_time`. Блокировка будет продлеваться до тех пор, пока количество IP-пакетов, поступающих от источника, не будет меньше `count_trigger`.

Список блокировки обрабатывается МЭ до применения сетевых фильтров. Если IP-пакет пришел от источника повышенной нагрузки, он блокируется, а обработка сетевыми фильтрами не выполняется, что снижает нагрузку на ViPNet Coordinator HW.

Примечание.

- Выявление источников повышенной сетевой нагрузки может занять до одной минуты. До выявления и блокировки источника трафик продолжает обрабатываться сетевыми фильтрами.
- Максимальное количество источников повышенной сетевой нагрузки — 65535.

Параметры автоматической блокировки источников повышенной нагрузки по умолчанию:

- порог количества заблокированных IP-пакетов `drops` — 10;
- время блокировки в секундах `ban_time` — 1800;

- время подсчета заблокированных IP-пакетов в секундах `blocking_interval` — 65;
- интерфейсы, для которых выявляются источники повышенной нагрузки `ifname` — eth1;
- продление блокировки `ban_again` — 1;
- порог количества IP-пакетов, поступивших от источника, для продления блокировки `count_trigger` — 1000;
- отправка SNMP-оповещения о блокировке источников повышенной нагрузки `snmp_enable` — 1;
- регистрация событий блокировки источников повышенной нагрузки в системном журнале `log_enable` — 1;
- блокировка трафика от источника повышенной нагрузки на всех интерфейсах, пока IP-адрес источника находится в списке блокировки `block_all_ifname` — 1.

Настройка автоматической блокировки источников повышенной сетевой нагрузки

1. Настройте мониторинг нагрузки, если вы не сделали это ранее.
2. Остановите мониторинг нагрузки:

   ```
   hostname# healthmond stop
   ```

3. Откройте файл `healthmon.ini`:

   ```
   hostname# healthmond edit
   ```

4. В секции `[IP_ban]`:

   4.1 Добавьте интерфейсы, для которых будут выявляться источники повышенной нагрузки:

   - `ifname = all` — для всех интерфейсов;
   - `ifname = <список имен интерфейсов, разделенных запятой>` — для указанных интерфейсов;

   4.2 Чтобы блокировать трафик от источника повышенной нагрузки только на интерфейсах `ifname`, пока IP-адрес источника находится в списке блокировки:

   ```
   block_all_ifname = 0
   ```

   4.3 При необходимости измените параметры автоматической блокировки по умолчанию `drops`, `ban_time`, `blocking_interval` и `count_trigger` с учетом трафика вашей сети.

5. Сохраните изменения — нажмите **Ctrl**+**O**, затем **Ctrl**+**X**.
6. Запустите мониторинг нагрузки:

   ```
   hostname# healthmond start
   ```

Просмотреть текущий список блокировки вы можете с помощью команды `healthmond show` или во внешней системе мониторинга (если настроен SNMP-агент ViPNet Coordinator HW).

Просмотр статистики передачи данных

Статистика передачи данных ведется раздельно по всем интерфейсам с момента включения ViPNet Coordinator HW. Статистика учитывает текущую скорость интерфейсов и объем трафика. После запуска команды статистика отображается в режиме реального времени с заданным интервалом обновления (по умолчанию — 3 секунды). Чтобы завершить просмотр статистики, нажмите **Ctrl**+**C**. В кластере просмотр статистики доступен на обоих узлах. После перезагрузки ViPNet Coordinator HW или удаления интерфейса данные статистики сбрасываются. Для ViPNet Coordinator VA статистика может быть сброшена после перезапуска интерфейса.

Чтобы просмотреть статистику передачи данных на всех физических и агрегированных интерфейсах:

```
hostname> inet show traffic

Please wait for 3 sec. Gathering traffic....

Interface             RX speed            TX speed           RX Total         TX Total
----------           ---------           ---------          ---------        ---------
eth0              10,24 Kbit/s        12,37 Kbit/s          456,12 KB        517,37 KB
eth1             999,99  bit/s       634,12  bit/s           12,31 KB          6,27 KB
bond0              1,00 Gbit/s      1000,00 Mbit/s            1,10 TB       1022,12 GB
eth2             512,00 Mbit/s       500,00 Mbit/s          563,20 GB        511,06 GB
eth3             512,00 Mbit/s       500,00 Mbit/s          563,20 GB        511,06 GB


Mon Feb 2 09:55:16 2026
```

Чтобы просмотреть статистику передачи данных виртуального интерфейса `eth2.10` с интервалом обновления 10 секунд:

```
hostname> inet show traffic interface eth2.10 interval 10

Please wait for 10 sec. Gathering traffic....

Interface             RX speed            TX speed           RX Total         TX Total
----------           ---------           ---------          ---------        ---------
eth2.10          500,00 Mbit/s       530,00 Mbit/s          565,25 GB        515,07 GB


Mon Feb 2 09:59:19 2026
```

16

Проверка работоспособности

Контроль целостности файлов ПО 416

Статистический контроль последовательностей случайных чисел 418

Проверка фильтрации транзитного трафика 420

Контроль целостности файлов ПО

Целостность критически важных файлов ПО ViPNet Coordinator HW регулярно проверяется встроенными скриптами. В ходе проверки контролируются:

- Исполняемые и конфигурационные файлы.
- Файлы справочников и ключи.

Указанные файлы защищены контрольными суммами, которые хранятся в файлах с расширением `*.crg`. Проверка целостности заключается в вычислении текущей контрольной суммы файла и ее сравнении с контрольной суммой из файла `*.crg`. Несовпадение контрольных сумм считается нарушением целостности файла.

Каждый файл `*.crg` содержит также собственную контрольную сумму. Проверка контрольной суммы файла `*.crg` выполняется перед проверкой целостности остальных файлов, контрольная сумма которых в нем указана.

Нарушением целостности файлов также считается отсутствие хотя бы одного конфигурационного файла или файла с контрольными суммами.

Проверка целостности файлов выполняется в следующих случаях:

- Установка ПО ViPNet Coordinator HW.
- Обновление ПО ViPNet Coordinator HW.
- Загрузка ПО ViPNet Coordinator HW.
- Периодическая проверка с интервалом 12 часов (в этом случае конфигурационные файлы, а также справочники и ключи не проверяются).



Примечание. При каждой периодической проверке в системный журнал заносится запись, содержащая время и результаты этой проверки. Чтобы просмотреть информацию о последней периодической проверке, выполните:

```
hostname# admin show check integrity status
```

Если команда выполнена до первой периодической проверки целостности файлов, то появится сообщение об отсутствии результатов проверки целостности (`No integrity check information`).

Кроме того, при локальном подключении к ViPNet Coordinator HW вы можете проверить целостность файлов вручную, в рамках регламентного контроля:

```
hostname# machine self-test
```

При несовпадении контрольных сумм в ходе периодической проверки ViPNet Coordinator HW автоматически перезагружается. При несовпадении контрольных сумм в остальных случаях выполняется одно из действий:

- Если для поврежденного файла имеется резервная копия (см. Использование резервного раздела в исполнениях с двумя накопителями), файл автоматически восстанавливается с последующей перезагрузкой ViPNet Coordinator HW.

- Если восстановление поврежденного конфигурационного было неуспешным, ViPNet Coordinator HW перезагружается в режим ограниченного функционирования, в котором локальный администратор `admin` может выполнить следующие действия:
  - Подключиться к ViPNet Coordinator HW с помощью консоли.
  - Просмотреть события журналов для определения причин сбоя.
  - Изменить параметры конфигурационных файлов, за исключением настроек сетевых интерфейсов.
  - Выполнить сброс ViPNet Coordinator HW к заводским настройкам.
  - Перезагрузить ViPNet Coordinator HW.
- Если при загрузке обнаружено нарушение целостности исполняемых файлов ПО ViPNet Coordinator HW, и соответствующая резервная копия не найдена, то загрузка ViPNet Coordinator HW завершается.

Статистический контроль последовательностей случайных чисел

Программный датчик случайных чисел (ПДСЧ) предназначен для генерации последовательностей случайных чисел, используемых в криптографических операциях, например, при работе с сертификатами и ключами. ПДСЧ инициализируется при загрузке ViPNet Coordinator HW. Статистический контроль последовательностей случайных чисел выполняется при генерации каждой новой последовательности и при выполнении команды регламентного контроля `machine self-test`.

Результат статистического контроля регистрируется в журнале СКЗИ (см. Журналы аудита и СКЗИ).

Чтобы выполнить статистический контроль последовательностей случайных чисел:

```
hostname# machine self-test
If you run self-test, then all daemons will be stopped.
Continue?[Yes/No]: Y

Operation may take a long time. Please wait...

>> Self test successfully passed.

>> Imito-protective inserts for modules:

iplircfg >> AEC2F1B4

failoverd >> E29353AE

webgui-fcgi-server >> E2SAS945

webgui-http-server >> 0E64E6FA

vpncrnd >> 35DA5FFC

rvpn_shell >> B77EDA20

vipnetsnrnp >> S133F97C

libidents.so >> 729DEEB0

libpasswd.so >> 415AS0S9

libpwdgen.so >> CE3FF31D

libroulett2.so >> C888289E

libstoredev.so >> D1192E5B
```

Чтобы просмотреть журнал СКЗИ, выполните:

```
hostname# machine logs show crypto-audit
```

```
…
2026-04-04 12:56:08 [HW1000] [Single Mode] Run self-tests [success] [admin]
Details: Command:'machine self-test'
...
```

Проверка фильтрации транзитного трафика

Вы можете проверить правильность фильтрации межсетевым экраном транзитного трафика открытой сети, в том числе связанную с работой DPI и IPS. Проверка выполняется с помощью набора эталонных фильтров. В результате проверки выявляются ошибки двух типов:

- `<имя эталонного фильтра> – Traffic Passed instead of Drop` — фильтр пропустил трафик, который должен быть заблокирован;
- `<имя эталонного фильтра> – Traffic Dropped instead of Pass` — фильтр заблокировал трафик, который должен быть пропущен.

Если в ходе проверки будут обнаружены ошибки:

1. остановите обработку транзитного трафика — в строке `Do you want to stop processing transit traffic? [Yes/No]:` введите `Yes` и нажмите **Enter**);
2. обратитесь в службу поддержки ИнфоТеКС.

Запустите проверку:

```
hostname# firewall self-test

WARNING!

Traffic filtering errors detected.

> Allow traffic for GeoIP – Traffic Dropped instead of Pass

> Block traffic in DPI mode – Traffic Passed instead of Drop

Do you want to stop processing transit traffic? [Yes/No]: Y

Transit traffic processing has been stopped. Please contact the support team.
```

Результат выполнения команды регистрируется в системном журнале и журнале аудита.

A

Сетевые фильтры по умолчанию

Таблица 26. Фильтры защищенной сети (vpn)

Название	Источник	Назначение	Протокол	Действие
Служебные фильтры в режиме кластера				
ViPNet Service in	@any	@local	udp: from 2060 to 2060	pass
ViPNet Service out	@local	@any	udp: from 2060 to 2060	pass
Служебные фильтры				
Block not original udp port	@local	@any	udp: from 0-2045, 2047-63536 to 2046	drop
Allow ViPNet base services in	@any	@local	udp: to 2046, from 2048 to 2048, from 2050 to 2050	pass
Allow ViPNet base services out	@local	@any	udp: to 2046, from 2048 to 2048, from 2050 to 2050	pass
Allow ViPNet MFTP in	@any	@local	tcp: from 5000-5003	pass
Allow ViPNet MFTP out	@local	@any	tcp: from 5000-5003	pass
Allow ViPNet Control services in	ViPNet ID Prime	@local	@any	pass
Allow ViPNet Control services out	@local	ViPNet ID Prime	@any	pass

Настраиваемые фильтры				
ICMP redirect in	@any	@local	icmp: 5	drop
ICMP redirect out	@local	@any	icmp: 5	drop
Allow ICMP Ping in	@any	@local	icmp: 8	pass
Allow ICMP Ping out	@local	@any	icmp: 8	pass
Allow ViPNet DBViewer in	@any	@local	tcp: from 2047	pass
Allow ViPNet DBViewer out	@local	@any	tcp: from 2047	pass
Allow DNS client	@local	@any	tcp/udp: from 53	pass
Allow DNS server	@any	@local	tcp/udp: from 53	pass
Allow NTP client	@local	@any	udp: from 123	pass
Allow NTP server	@any	@local	udp: from 123	pass
Allow DHCP client req	@local	@any	udp: to 68 from 67	pass
Allow DHCP client resp	@any	@local	udp: to 67 from 68	pass
Allow DHCP server req	@local	@any	udp: to 67 from 68	pass
Allow DHCP server resp	@any	@local	udp: to 68 from 67	pass
Allow DHCP-Relay service in	@any	@local	udp: to 67 from 67	pass
Allow DHCP-Relay service out	@local	@any	udp: to 67 from 67	pass
Allow SSH client	@local	@any	tcp: from 22	pass
Allow syslog outgoing	@local	@any	udp: from 514	pass
Allow cef outgoing	@local	@any	udp: from 5001	pass
Allow SNMP	@any	@local	udp: from 161	pass
Allow SNMP traps	@local	@any	udp: from 162	pass
Allow UPS service in (только для аппаратных платформ)	@any	@local	tcp: from 3493	pass
Allow UPS service out (только для аппаратных платформ)	@local	@any	tcp: from 3493	pass
Служебный фильтр по умолчанию				
Default VPN rule	@any	@any	@any	drop

Таблица 27. Фильтры туннелируемых узлов (`tunnel`)

Название	Источник	Назначение	Протокол	Действие
Настраиваемые фильтры				
To all tunnel nodes	@any	@tunneledip	@any	pass
From all tunnel nodes	@tunneledip	@any	@any	pass
Служебный фильтр по умолчанию				
Default tunnel rule	@any	@any	@any	drop

Таблица 28. Локальные фильтры открытой сети (`local`)

Название	Источник	Назначение	Протокол	Действие
Служебные фильтры в режиме кластера				
Failover test IP	@local	<список значений параметров `testip` из `failover.ini`>	icmp	pass
Failover Channel	@local	interface <имя интерфейса синхронизации>	@any	pass
Failover Channel	<IP-адрес интерфейса синхронизации второго узла кластера>	interface <имя интерфейса синхронизации>	@any	pass
Служебные фильтры				
ViPNet Service Common In	@any	@local	tcp/udp: to 2046, 2047, 10096, 5100, 10092	drop
ViPNet Service Common Out	@local	@any	tcp/udp: from 2046	drop
Настраиваемые фильтры				
ICMP redirect in	@any	@local	icmp:5	drop
ICMP redirect out	@local	@any	icmp:5	drop
Block ICMP timestamp response	@local	@any	icmp:14	drop
Allow ICMP Ping	@local	@any	icmp: 8	pass

Allow DNS	@local	@any	tcp/udp: to 53	pass
Allow NTP	@local	@any	udp: to 123	pass
Allow DHCP service req	@any	@local	udp: from 67 to 68	pass
Allow DHCP service resp	@local	@any	udp: from 68 to 67	pass
Allow DHCP-Relay service in	@any	@local	udp: from 67 to 67	pass
Allow DHCP-Relay service out	@local	@any	udp: from 67 to 67	pass
Allow ICMP blackhole response	@local	@any	icmp type 3 code 4	pass
Служебный фильтр по умолчанию				
Default local rule	@any	@any	@any	drop

Таблица 29. Транзитные фильтры открытой сети (`forward`)

Название	Источник	Назначение	Протокол	Действие
Служебный фильтр по умолчанию				
Default transit rule	@any	@any	@any	drop

B

Группы объектов «Протоколы» по умолчанию

Таблица 30. Состав групп объектов «Протоколы»

Имя группы протоколов	Состав группы протоколов
DHCP	UDP:from 67-68 to 67-68
CITRIX	TCP:to 1494
DNS	UDP:to 53
FTP	TCP:to 21
GRE	IP:47
H323	TCP:to 1720
HTTP	TCP:to 80, TCP:to 8080
HTTP-Proxy	TCP:to 3128
HTTPS	TCP:to 443
IGMP	IP:2
IKE	UDP:to 500
IMAP	TCP:to 143
IPSecESP	IP:50
Kerberos	TCP:to 88, TCP:to 749, UDP:to 88, UDP:to 749
L2TP	UDP:to 1701
LDAP	TCP:to 389, UDP:to 389

LotusNotes	TCP:to 1352
MS-SQL	TCP:to 1433-1434, UDP:to 1433-1434
MySQL	TCP:to 3306
NetBIOS-DGM	UDP:from 138 to 138
NetBIOS-NC	UDP:from 137 to 137
NetMeeting	TCP:to 1503
NTP	UDP:to 123
PING	ICMP:8
POP3	TCP:to 110
Postgres	TCP:to 5432
PPTP	TCP:to 1723
RADIUS	UDP:to 1812-1813
RDP	TCP:to 3389
RTSP	TCP:to 554
SCCP	TCP:to 2000
SIP	TCP:to 5060, UDP:to 5060
SMTP	TCP:to 25
SNMP	UDP:to 161
SNMP-Traps	UDP:to 162
SSH	TCP:to 22
Syslog	UDP:to 514
Telnet	TCP:to 23
TFTP	UDP:to 69
UPnP	TCP:to 1900, TCP:to 2869, UDP:to 1900, UDP:to 2869
MFTP	TCP:to 5000-5003
SMCMonitoring	TCP:to 2047, TCP:to 5100, TCP:to 10092
VPNBase	UDP:to 2046, UDP:from 2048 to 2048, UDP:from 2050 to 2050
Cluster	UDP:from 2060 to 2060
ClusterMonitoring	UDP:from 2060 to 2065, UDP:from 2065 to 2060
VNC	TCP:to 5900
OSPF	IP:89



C

База URL-категорий

Таблица 31. Описание URL-категорий

Обозначение	Название	Описание
Advertisements and Pop-Ups	Реклама и всплывающие окна	Сайты, содержащие графическую рекламу (баннеры, всплывающие окна и прочее).
Alcohol and Tobacco	Алкоголь и табак	Сайты, посредством которых реализуется продвижение или продажа алкогольной и табачной продукции.
Anonymizers	Анонимайзеры	Сайты, предоставляющие возможность анонимного посещения других сайтов и ресурсов интернета. Анонимайзеры также могут применяться для обхода средств веб-фильтрации и т.д.
Arts	Искусство	Сайты, посвященные искусству, в том числе различным театрам, музеям, галереям, фотографии, танцевальным коллективам и т.д.
Botnets	Ботнеты	Сайты, которые управляют сетями ботов через командно-контрольные центры.
Business	Бизнес	К данной категории относятся корпоративные веб-сайты, а также интернет-ресурсы, содержащие информацию об услугах и продуктах, необходимых предприятиям любого размера для успешной деятельности.
Chat	Чаты	Сайты, позволяющие осуществлять общение в режиме реального времени.

Обозначение	Название	Описание
Child Abuse Images	Жестокое обращение с детьми	Сайты, содержащие фотографии, иллюстрирующие случаи жестокого обращения с детьми.
Compromised	Заражённые сайты	Сайты, контроль над которыми был захвачен злоумышленниками для распространения вредоносных программ без ведома владельцев. В категорию также входят ресурсы из группы высокого риска заражения.
Computers and Technology	Компьютеры и технологии	Сайты, содержащие обзоры продуктов, новости и информация о компьютерах, программном обеспечении, оборудовании, периферийных устройствах, технологиях и услугах.
Criminal Activity	Преступная деятельность	Сайты, предлагающие советы и рекомендации по совершению противоправных или преступных действий, а также содержащие информацию о том, как скрыть следы преступления. На подобных ресурсах можно узнать о том, как совершить убийство, создать бомбу, взломать замки и т.д. В данную категорию также включены сайты о незаконном использовании электронных устройств, хакерстве, мошенничестве и незаконном распространении программного обеспечения.
Cryptocurrency Mining	Криптомайнеры	Сайты, которые используют технологии майнинга криптовалют без разрешения пользователя.
Cults	Религиозные культы	Сайты, связанные с нетрадиционной религиозной практикой, обычно называемой культами. Подобные движения считаются ложными, неортодоксальными, экстремистскими. Члены культов зачастую живут под руководством харизматического лидера.
Dating and Personals	Сайты знакомств	Сайты, способствующие налаживанию межличностных отношений, таких как знакомства и брак. Категория включает в себя сайты для сватовства, знакомств, ресурсы, предлагающие эскорт-услуги.
Download Sites	Download-архивы	Сайты, которые содержат доступное для скачивания программное обеспечение. Эта категория также включает в себя некоторые Peer-to-Peer сайты.

Обозначение	Название	Описание
Education	Образование	Сайты, поддерживаемые учебными заведениями и школами всех типов, включая дистанционное обучение. Включает в себя общеобразовательные и справочные материалы, такие как словари, энциклопедии, интерактивные курсы, учебные пособия и методические материалы.
Entertainment	Развлечения	Сайты, предлагающие пользователю телеканалы, кино, музыку и видео (в том числе видео по запросу). Категория также включает в себя сайты знаменитостей и развлекательные новости.
Fashion and Beauty	Мода и красота	Сайты о моде, ювелирных изделиях, гламуре, красоте, модельном бизнесе, косметике или связанных со всем перечисленным товарах или услугах. Включает отзывы, сравнения, а также общую информацию, полезную потребителю.
Finance	Финансы	Сайты, связанные с банками, финансами, платежами или инвестициями. В категорию входят интернет-ресурсы банков, брокерских компаний, порталы для онлайн-торговли на бирже. На данных ресурсах также можно узнать котировки акций, информацию об управлении фондами, страховых компаниях, кредитных союзах и т.д.
Forums and Newsgroups	Форумы и новостные ленты	Ленты новостей, форумы, доски объявлений. Категория не включает в себя персональные блоги.
Gambling	Азартные игры	Сайты, связанные с азартными играми, лотереями, казино и букмекерскими агентствами.
Games	Игры	Сайты, связанные с компьютерными или другими видами игр. Ресурсы содержат информацию о разработчиках игр, кодах и читах.
Gay, Lesbian or Bisexual	Нетрадиционная сексуальная ориентация	Сайты, содержащие материалы о геях, лесбиянках, трансгендерах.
General	Общие	Сайты, которые не попадают в другие категории, например, пустые веб-страницы.

Обозначение	Название	Описание
Government	Правительство	Сайты, находящиеся в ведении правительственных или военных организаций, ведомств или учреждений, в том числе отделений полиции, пожарной охраны, таможенных бюро, аварийных служб, гражданской обороны, служб борьбы с терроризмом и больниц.
Greeting cards	Поздравительные открытки	Сайты, которые позволяют людям получать и отправлять поздравительные открытки.
Hacking	Хакерство	Сайты, которые способствуют или содержат рекомендации о том, как получить несанкционированный доступ к компьютерным системам с целью кражи информации, совершения мошеннических действий, советы по созданию вирусов или совершению других видов незаконной деятельности, связанной с кражей цифровой информации.
Hate and Intolerance	Ненависть и нетерпение	Интернет-ресурсы, посвященные вопросу поощрения ущемления прав людей в зависимости от расы, религии, пола, возраста, инвалидности, сексуальной ориентации или национальности.
Health and Medicine	Здоровье и медицина	Сайты, содержащие информацию, относящуюся к поддержанию здоровья, медицинским услугам, фитнесу и благополучию. В данную категорию также включены интернет-ресурсы, связанные с медицинским оборудованием, больницами, аптеками, сестринским делом, медициной, рецептами лекарств, и т.д.
Illegal Drug	Наркотики	Сайты с информацией о приобретении, производстве и использовании незаконных или рекреационных наркотиков, а также злоупотреблении отпускаемыми по рецепту лекарствами.
Illegal Software	Нелегальное ПО	Сайты, которые незаконно распространяют программное обеспечение или защищенные авторским правом материалы, такие как фильмы, музыка, незаконные серийные номера, генераторы ключей.
Image Sharing	Обмен картинками	Порталы для размещения цифровых фотографий и изображений, фотоальбомы и фотообменники.

Обозначение	Название	Описание
Instant Messaging	Сервисы мгновенных сообщений	Сайты, которые позволяют создавать и использовать аккаунт в службах обмена мгновенными сообщениями, таких как ICQ, AOL Instant Messenger, IRC, MSN, Jabber, Yahoo Messenger, и т.п.
Job Search	Поиск работы	Сайты, содержащие списки вакансий, оказывающие помощь в поиске работы. В категорию входят интернет-ресурсы агентств по трудоустройству и рекрутинговых компаний.
Kids sites	Детские сайты	Сайты, ориентированные на детскую аудиторию.
Legal	Юриспруденция	Сайты юридических фирм, обсуждение и анализ юридических вопросов.
Leisure and Recreation	Отдых и оздоровление	Сайты, связанные с рекреационной деятельностью и увлечениями, включая ресурсы, посвященные зоопаркам, центрам общественного отдыха, бассейнам, паркам развлечениям и хобби, таким как садоводство, литература, искусства и ремесла, домашний декор и т.д.
Literature and Books	Литература и книги	Сайты, содержащие опубликованные книги, новеллы, рассказы, включая фантастику, биографии.
Local Information	Местные достопримечательности	Путеводители и информация для туристов, в том числе о ресторанах и местные достопримечательности.
Malware	Вредоносное ПО	Сайты, содержащие нежелательные программы, автоматически загружающиеся и устанавливающиеся на ПК пользователей. Вирусы вносят изменения в систему и позволяют злоумышленникам получить данные с компьютера без ведома и согласия его владельца.
Military	Военные сайты	Информация о военных организациях, военной истории.
Nudity	Нудизм	Ресурсы, содержащие изображение частичной или полной наготы. Категория включает в себя сайты, рекламирующие или продающие нижнее белье, интимную одежду или купальные костюмы.
Nutrition and Diet	Здоровое питание и диеты	Сайты, посвященные правильному питанию, снижению веса, диетам.

Обозначение	Название	Описание
Online training and tools	Онлайн обучение	Дистанционное образование, онлайн-курсы, профессиональное обучение, программы обучения, повышения квалификации.
Parked Domains	Припаркованные домены	К припаркованным доменам относятся URL-адреса с ограниченным контентом, конечные точки перехода с рекламных объявлений. Подобные ресурсы могут приносить прибыль, но, как правило, не несут в себе полезной для пользователя информации. Категория также включает в себя сайты, находящиеся на реконструкции, папки и базовые страницы веб-серверов.
Peer-to-Peer	Пиринговые сети	Сайты, которые позволяют осуществлять прямой обмен файлами между пользователями вне зависимости от центрального сервера.
Personal Sites	Персональные сайты	Персональные сайты, созданные отдельными людьми или группами лиц, блоги.
Personal Storage	Персональные хранилища	Сайты, которые позволяют загружать файлы и резервные копии для удаленного хранения данных.
Pets and Animals	Домашние животные	Сайты, посвященные продуктам и сервисам для домашних и других животных.
Phishing and Fraud	Фишинг и мошенничество	Сайты, которые используются для обмана или в мошеннических целях (например, фишинг), такие как кражи финансовой или другой информации посредством учетной записи пользователя. Эти сайты чаще всего являются искусно выполненной подделкой популярных законных ресурсов, что вводит в заблуждение пользователей.
Politics	Политика	Сайты, посвященные политическим партиям или занимающиеся политической пропагандой, а также предоставляющие информацию о группах интересов, выборах, законодательстве или вопросе лоббирования. Категория включает в себя сайты, которые предлагают сведения о правах и их защите.

Обозначение	Название	Описание
Pornography/Sexually Explicit	Порнография и насилие	Сайты, которые содержат контент сексуального содержания. Категория включает в себя продукцию для взрослых, такую как секс-игрушки, компакт-диски и видео. Сайты из данной группы позволяют заказывать эскорт-услуги, получить сведения о стриптиз-клубах, почитать эротические рассказы и текстовые описания половых актов.
Profanity	Нецензурная лексика	Сайты, содержащие нецензурную лексику
Professional social networks	Профессиональные социальные сети	Подмножество веб-сайтов социальных сетей, которое включает в себя контент, предназначенный исключительно для бизнеса и профессионалов.
Real Estate	Недвижимость	Информация об аренде, покупке или продаже недвижимости или земельных участков. Рекомендации по покупке или продаже жилых помещений. Агентства недвижимости, услуги по аренде, переезду, улучшению жилищных условий.
Reference and Research	Справочная информация	Профессиональные или образовательные справочные материалы, в том числе онлайн-словари, карты, переписи, альманахи, каталоги библиотек, генеалогии, и научной информации.
Religion	Религия	Сайты, посвященные вопросу веры, человеческой духовности и религиозным убеждениям, в том числе сайты церквей, синагог, мечетей и других молитвенных домов.
Restaurants and Dining	Рестораны и еда	Сайты, содержащие списки, обзоры заведений общественного питания. Категория включает в себя сайты с рецептами, инструкциями и советами, продуктами питания и советами по выбору вина.
School Cheating	Школьные мошенничества	Сайты с ответами на различные школьные тесты, написанными эссе, рефератами, исследовательскими или курсовыми работами.
Search Engines and Portals	Поисковые системы и порталы	Сайты, позволяющие осуществлять поиск в интернете по новостям, изображениям, каталогам и другим видам онлайн-контента. Категория включает в себя порталы и каталоги сайтов, такие как белые/желтые страницы.

Обозначение	Название	Описание
Sex Education	Половое воспитание	Сайты, связанные с сексуальным образованием, включая такие темы, как уважение к партнеру, аборты, бисексуальный образ жизни, противозачаточные средства, заболевания, передаваемые половым путем и беременность.
Shopping	Покупки	Интернет-магазины, каталоги, аукционы, рекламные объявления. Категория не включает в себя ресурсы, посвященные товарам и услугам из более узких категорий, таких как здравоохранение и медицина.
Social Networking	Социальные сети	Сайты социальных сетей, пользователи которых могут общаться, взаимодействовать, обмениваться сообщениями, файлами.
Spam Sites	Спам-сайты	Сайты, продвижение которых основано на использовании спам-рассылок.
Sports	Спорт	Сайты команд или спортивных ассоциаций, международные и национальные, спортивные колледжи. Ресурсы, содержащие результаты и расписания игр, спортивные журналы и газеты, виртуальный спорт и спортивные лиги.
Stock trading	Фондовый рынок	Сайты по торговле ценными бумагами и управления инвестиционными активами. Также включает информацию о финансово-инвестиционной стратегии, котировкам и новостям.
Streaming Media and Downloads	Потоковое мультимедиа и загрузки	Сайты, содержащие потоковый контент, например, интернет-радио, интернет-телевидение или MP3-live. Категория включает в себя фан- или официальные сайты музыкантов, групп или звукозаписывающих компаний.
Tasteless	Сайты сомнительного содержания	Сайты с оскорбительным контентом, такого рода как юмор "ниже пояса", ужасный или даже пугающий контент, шокирующие изображения крови, ран или жестокого обращения с животными.
Technical information and documentation	Техническая информация	Сайты, которые предоставляют информацию к технической документации и информации.
Translators	Переводчики	Сайты, на которых возможен онлайн-перевод веб-страниц на другие языки. Данные ресурсы могут использоваться для обхода заданных ограничений, так как просмотр сайтов осуществляется с URL сайта онлайн-переводчика.

Обозначение	Название	Описание
Transportation	Транспорт	Сайты, посвященные автотранспорту и его покупке. Категория включает в себя интернет-ресурсы производителей, дилеров, сайты с обзорами, сообщества, клубы автолюбителей и т.д.
Travel	Путешествия	Авиакомпании, агентства по бронированию авиабилетов, планирование поездок, предварительные заказы, аренда транспортных средств, описания мест назначения, реклама гостиниц и казино.
Unknown	Неизвестная тематика	Сайты без принадлежности к какой-либо категории.
Updates	Обновления	Сайты обновлений программного обеспечения, обновлений операционных систем, обновлений
Violence	Насилие	Сайты, содержащие изображения, текстовые описания и пропаганду физического насилия против людей, животных или организаций\сообществ. Категория включает в себя ресурсы с иллюстрациями ужасов природы, а также сайты, содержащие ненормативную лексику.
Weapons	Оружие	Сайты, содержащие изображения, обзоры и описания оружия. В категории также входят интернет-магазины орудий и оружия, в том числе для занятия спортом.
Web-based Email	Веб-почта	Порталы, позволяющие завести собственные почтовые аккаунты для написания, чтения, отправки и получения электронных писем.

D

Типы событий журнала IP-пакетов

Таблица 32. События блокирования IP-пакетов фильтрами защищенной сети

Номер	Описание события
1	Не найден ключ для передачи IP-пакета сетевому узлу с идентификатором, указанным в IP-пакете
3	Входящий зашифрованный или предназначенный для шифрования исходящий открытый IP-пакет заблокирован фильтром защищенной сети
4	Слишком большой тайм-аут IP-пакета, то есть время его отправки отличается от времени его получения на величину, большую указанной в соответствующей настройке
7	Метод шифрования, код которого указан во входящем IP-пакете, не поддерживается
8	IP-пакет поврежден
9	Неизвестный идентификатор сетевого узла
11	IP-пакет заблокирован фильтром защищенной сети с ICMP- или TCP RST-ответом
13	Превышено максимальное время пребывания IP-пакета в сети
14	Неверный адрес получателя IP-пакета
16	Исчерпана лицензия на количество туннелируемых узлов
17	Неверный IP-адрес получателя
18	Неизвестный IP-адрес получателя
26	Узел с данного координатора недоступен

Таблица 33. События блокирования IP-пакетов локальными фильтрами открытой сети

Номер	Описание события
22	От защищенного узла получен открытый IP-пакет
23	От защищенного узла получен открытый широковещательный IP-пакет
24	На порт, используемый одной из служб ViPNet, получен открытый IP-пакет
30	Локальный IP-пакет заблокирован фильтром открытой сети
31	Транзитный IP-пакет заблокирован фильтром открытой сети
32	Широковещательный IP-пакет заблокирован фильтром открытой сети
33	Пакет заблокирован фильтром антиспуфинга
34	Локальный IP-пакет заблокирован фильтром открытой сети с ICMP или TCP RST ответом
35	Транзитный IP-пакет заблокирован фильтром открытой сети с ICMP или TCP RST ответом
36	IP-пакет заблокирован фильтром для туннелируемых узлов с ICMP или TCP RST ответом
37	Пакет заблокирован фильтром туннелируемых ресурсов

Таблица 34. События блокирования IP-пакетов по другим причинам

Номер	Описание события
28	IP-пакет заблокирован ICAP-сервером
29	IP-пакет заблокирован по причине: включена блокировка трафика, если ICAP-сервер не отвечает
81	Недопустимая версия протокола IP (поддерживается только IPv4)
82	Длина заголовка IP-пакета меньше допустимой
83	Длина IP-пакета меньше указанной в IP-заголовке
84	Значение контрольной суммы в заголовке IP-пакета отличается от ее значения в IP-пакете
85	Размер TCP-заголовка меньше допустимого
86	Размер UDP-заголовка меньше допустимого
90	IP-пакет не был обработан, так как для его обработки недостаточно вычислительных ресурсов
91	IP-пакет получен во время инициализации драйвера ViPNet
92	Размер IP-пакета превышает 48 Кбайт
94	Недостаточно памяти
99	Заблокирован фрагментированный IP-пакет
115	Не удалось найти маршрут для IP-пакета в таблице маршрутизации
116	Не найден сетевой адаптер

118	Ошибка при шифровании исходящего IP-пакета для защищенного узла
119	Получен зашифрованный IP-пакет неизвестного формата, который не может быть расшифрован
131	Ошибка обработки прикладных протоколов: не удалось построить маршрут
135	Ошибка обработки модуля ALG
136	Недостаточно памяти для выполнения трансляции адреса (NAT)
139	Отсутствуют лицензии для туннелирования на узле назначения
142	IP-пакет заблокирован правилом IPS

Таблица 35. События пропуска зашифрованных IP-пакетов

Номер	Описание события
40	Пропущен зашифрованный IP-пакет
41	Пропущен зашифрованный широковещательный IP-пакет
44	Маршрутизация зашифрованного транзитного IP-пакета с подменой адреса получателя
45	Пакет пропущен на туннелирующем координаторе, так как он поступил от туннелируемого узла или предназначен для такого узла

Таблица 36. События пропуска незашифрованных IP-пакетов

Номер	Описание события
60	Пропущен незашифрованный IP-пакет
61	Пропущен незашифрованный широковещательный IP-пакет
62	Пропущен незашифрованный транзитный IP-пакет
67	IP-пакет пропущен с предупреждением IPS

E

Структура записи журнала IP-пакетов в формате CEF

Запись журнала IP-пакетов для экспорта по сети в формате CEF состоит из полей заголовка CEF и полей записи журнала.

Структура записи в режиме `hw`

```
<38> timestamp hostname CEF:Version|Device Vendor|Device Product|Device Version|Device Event Class ID|Name|Severity|Extension
```

где:

- `38` — приоритет;
- `timestamp` — отметка времени;
- `hostname` — имя сетевого узла;
- `Version` — номер версии CEF-нотации;
- `Device Vendor` — производитель устройства (`infotecs`);
- `Device Product` — идентификатор устройства (например, `HW1000`);
- `Device Version` — версия устройства (например, `5.4.1-6703`);
- `Device Event Class ID` — номер события в журнале IP-пакетов (см. Типы событий журнала IP-пакетов);
- `Name` — описание события в журнале IP-пакетов;
- `Severity` — важность события:
  - `5` — IP-пакет пропущен или IP-пакет пропущен с уведомлением IPS;
  - `10` — IP-пакет блокирован;

- `Extension` — набор пар ключ-значение из словаря CEF, разделенных пробелом.

Таблица 37. Описание ключей поля `Extension` для режима `hw`

Ключ словаря CEF	Описание ключа	Название поля в журнале IP-пакетов
cat	Группа правила IPS	Rule group
deviceExternalId	Идентификатор сенсора	
cnt	Число пакетов, соответствующих выбранному типу события	Count
src	IP-адрес отправителя пакетов	Source IP
dst	IP-адрес получателя пакетов	Destination IP
spt	Порт отправителя пакетов	Source port
dpt	Порт получателя пакетов	Destination port
proto	Тип транспортного протокола (TCP или UDP)	IP protocol
externalId	Идентификатор события	
reason	В зависимости от типа события: • идентификатор правила IPS • идентификатор правила МЭ	 • Rule ID • RuleUID
msg	В зависимости от типа события: • описание правила IPS • описание правила МЭ	 • Rule description • Rule description
end	Конец интервала времени UTC, в течение которого несколько событий были объединены в одну запись журнала IP-пакетов	Interval End
dvc	IP-адрес интерфейса, на котором зарегистрировано событие	
dvchost	Сетевое имя устройства	hostname
customerURI	HTTP-ссылка на стартовую страницу управления устройством	
start	Начало интервала времени UTC, в течение которого несколько событий были объединены в одну запись журнала IP-пакетов	Interval Begin
in	Размер входящих пакетов, соответствующих выбранному типу события	size in

out	Размер исходящих пакетов, соответствующих выбранному типу события	size out
deviceInboundInterface	Имя сетевого интерфейса, на котором были зарегистрированы события	Interface
deviceOutboundInterface	Имя сетевого интерфейса, на котором были зарегистрированы события	Interface
cn1	Шестнадцатеричный идентификатор протокола Ethernet	Eth. protocol
cn1Label=Eth protocol hex	Подпись для поля cn1	
deviceDirection	Направление IP-пакета (входящий, исходящий)	Direction
• cs1=NAT {yes|no} • cs2=Drop {yes|no} • cs3=Broadcast {yes|no} • cs4=Forward {yes|no} • cs5=Encrypted {yes|no}	• NAT — флаг транслированного пакета • Drop — флаг блокировки пакета • Broadcast — флаг широковещательного пакета • Forward — флаг транзитного пакета • Encrypted — флаг зашифрованного пакета	
• cs1Label= FlagNAT • cs2Label=FlagDrop • cs3Label=FlagBroadcast • cs4Label=FlagForward • cs5Label=FlagEncrypted	Подпись для полей cs1-cs5	
app	Название прикладного протокола, идентифицированного DPI	App protocol
cs6	Название приложения, идентифицированного DPI	Application
cs6Label=Application name	Подпись для поля cs6	
suser	Имя пользователя сети	Network user
shost	Номер и имя сетевого узла ViPNet	Source node
dhost	Номер и имя сетевого узла ViPNet	Destination node

Структура записи в режиме `ips`

```
timestamp hostname CEF:Version|Device Vendor|Device Product|Device Version|Device Event Class ID|Name|Severity|Extension
```

где:

- `timestamp` — отметка времени;
- `hostname` — имя сетевого узла;
- `Version` — номер версии CEF-нотации;
- `Device Vendor` — производитель устройства (`InfoTeCS`);
- `Device Product` — идентификатор устройства (`IDS-NS`);
- `Device Version` — версия устройства (`3.4`);
- `Device Event Class ID` — идентификатор правила IPS в формате `gid:sid:rev`:
  - `gid` — номер группы правил;
  - `sid` — номер правила;
  - `rev` — версия правила;
- `Name` — описание правила IPS;
- `Severity` — важность события:
  - `5` — IP-пакет пропущен с уведомлением IPS;
  - `10` — IP-пакет блокирован;
- `Extension` — набор пар ключ-значение из словаря CEF, разделенных пробелом.

Таблица 38. Описание ключей поля `Extension` для режима `ips`

Ключ CEF IDS-NS	Описание ключа в ViPNet TIAS	Название поля в журнале IP-пакетов
cat	Категория события (всегда Traffic analysis)	
deviceExternalId	Уникальный идентификатор отправителя события (SensorID)	
cnt	Счетчик событий с заданным идентификатором (сколько раз наблюдалось событие)	Count
src	IP-адрес источника в IPv4 сети	Source IP
dst	IP-адрес узла назначения	Destination IP
spt	Номер порта источника	Source port
dpt	Номер порта назначения	Destination port
proto	Идентификатор транспортного протокол	IP protocol

externalId	Идентификатор события (ID) в базе данных сенсора	
rt	Метка времени события по часам IDS	Interval End

F

Структура записи журнала сессий в формате CEF

Запись журнала сессий для экспорта по сети в формате CEF состоит из полей заголовка CEF и полей записи журнала:

```
<38> timestamp hostname CEF:Version|Device Vendor|Device Product|Device Version|Device Event Class ID|Name|Severity|Extension
```

где:

- `38` — приоритет;
- `timestamp` — отметка времени;
- `hostname` — имя сетевого узла;
- `Version` — номер версии CEF-нотации;
- `Device Vendor` — производитель устройства (`infotecs`);
- `Device Product` — идентификатор устройства (например, `HW1000`);
- `Device Version` — версия устройства (например, `5.4.1-6703`);
- `Device Event Class ID` — номер события в журнале IP-пакетов (см. Типы событий журнала IP-пакетов);
- `Name` — описание события в журнале IP-пакетов;
- `Severity` — важность события:
  - `8-10` — высокая;
  - `5-7` — средняя;
  - `2-4` — низкая;

- `0–1` — очень низкая;

- `Extension` — набор пар ключ-значение из словаря CEF, разделенных пробелом.

Таблица 39. Описание ключей поля `Extension`

Ключ словаря CEF	Описание ключа	Название поля в журнале сессий
• cs6 • cs6Label=SessionID	Идентификатор сессии	id
start	Дата и время начала сессии	time_begin
end	Дата и время завершения сессии	time_end
src	IP-адрес узла–источника сессии	src_ip
dst	IP-адрес узла–приемника сессии	dst_ip
spt	Порт узла–источника сессии	src_port
dpt	Порт узла–приемника сессии	dst_port
proto	Протокол уровня 3–4 OSI	protocol
cnt	Количество отправленных и полученных пакетов в рамках сессии	packet_send_recv
• in • out	Текущее значение отправленных и полученных данных в рамках сессии (в Мбайтах)	mbyte_send_recv
app	Прикладной протокол	app_protocol
• cs2 • cs2Label=Applicaiton name	Приложение	application
suser	Пользователь сети	user_name
• cs4 • cs4Label=State now	Текущее состояние сессии	state_now
• cs5 • cs5Label= Single rule identifier	Единый идентификатор правила	rule_uuid
msg	Описание правила	msg
deviceExternalId	Уникальный идентификатор узла, через который проходит трафик от источника к приемнику	dev_id

G

Базы управляющей информации (MIB) для протокола SNMP

MIB-II System

MIB-II System (.1.3.6.1.2.1.1) включает в себя объекты, предназначенные для получения информации о системных параметрах сетевого узла (например, имя узла, ОС, количество и параметры сетевых интерфейсов, статистика по SNMP-сообщениям). Подробнее см. в RFC 1213.

Примечание. Количество и индексы сетевых интерфейсов ViPNet Coordinator HW могут различаться для разных групп OID в описывающих их таблицах. При настройке мониторинга по протоколу SNMP рекомендуется вместо индексов использовать имена интерфейсов.

ПО ViPNet использует следующие объекты, для которых возможно только чтение данных:

Таблица 40. SNMP-параметры. MIB-II System

OID	Описание
.1.3.6.1.2.1.1.1.0	Информация о сетевом узле (имя узла, информация об ОС).
.1.3.6.1.2.1.1.2.0	OID SNMP-агента.
.1.3.6.1.2.1.1.3.0	Время работы SNMP-агента с последнего запуска (sysUpTime).

OID	Описание
.1.3.6.1.2.1.1.4.0	Контактная информация администратора. Задается командой `inet snmp system contact`. Если информация не задана, параметр отсутствует.
.1.3.6.1.2.1.1.5.0	Имя, назначенное сетевому узлу. Задается командой `inet snmp system name`. Если имя не задано, параметр равен `hostname`.
.1.3.6.1.2.1.1.6.0	Место расположения сетевого узла. Задается командой `inet snmp system location`. Если не задано, параметр отсутствует.
.1.3.6.1.2.1.1.7.0	Число, означающее наличие сетевых служб на определённых уровнях модели OSI. Для каждого уровня, для которого на узле есть службы, число 2 возводится в степень (L-1) и добавляется к общей сумме. Пример для координатора: 2^(4-1)+2^(7-1)=72 – узел работает на транспортном и прикладном уровне.
.1.3.6.1.2.1.1.8.0	Значение sysUpTime с момента последнего изменения состояния или значения столбца .1.3.6.1.2.1.1.9.1.2.A из таблицы .1.3.6.1.2.1.1.9.1.
Таблица поддерживаемых MIB (.1.3.6.1.2.1.1.9.1):	
A — индекс таблицы	
.1.3.6.1.2.1.1.9.1.1.A	Индекс таблицы.
.1.3.6.1.2.1.1.9.1.2.A	OID для MIB, с которыми работает SNMP-агент.
.1.3.6.1.2.1.1.9.1.3.A	Текстовое описание MIB.
.1.3.6.1.2.1.1.9.1.4.A	Время с момента подключения MIB.
ARP-таблица (.1.3.6.1.2.1.3.1.1):	
B — индекс интерфейса, присвоенный сетевым узлом	
E — IP-адрес сетевого узла	
.1.3.6.1.2.1.3.1.1.1.B.1.E	Индекс интерфейса, для которого видна связка IP-MAC.
.1.3.6.1.2.1.3.1.1.2.B.1.E	MAC-адрес.
.1.3.6.1.2.1.3.1.1.3.B.1.E	IP-адрес, соответствующий MAC-адресу.
Таблица описания маршрутов (.1.3.6.1.2.1.4.21.1):	
E — IP-адрес сетевого узла или сети	
.1.3.6.1.2.1.4.21.1.1.E	IP-адрес назначения маршрутов (маршрут по умолчанию 0.0.0.0).
.1.3.6.1.2.1.4.21.1.2.E	Индекс интерфейса (1.3.6.1.2.1.2.2.1.1), через который будет производится маршрутизация.
.1.3.6.1.2.1.4.21.1.3.E	Основная метрика протокола маршрутизации (если не используется, передается значение 1).
.1.3.6.1.2.1.4.21.1.4.E	Дополнительная метрика протокола маршрутизации (если не используется, передается значение 1).

OID	Описание
.1.3.6.1.2.1.4.21.1.5.E	Дополнительная метрика протокола маршрутизации (если не используется, передается значение 1).
.1.3.6.1.2.1.4.21.1.6.E	Дополнительная метрика протокола маршрутизации (если не используется, передается значение 1).
.1.3.6.1.2.1.4.21.1.7.E	IP-адрес следующего маршрутизатора по маршруту (Next Hop).
.1.3.6.1.2.1.4.21.1.8.E	Тип маршрута: • 1 (other) — другое, не может быть причислено к другим категориям; • 2 (invalid) — некорректный; • 3 (direct) — маршрут к подключённой сети; • 4 (indirect) — маршрут к удалённой сети.
.1.3.6.1.2.1.4.21.1.9.E	Механизм маршрутизации, через который был получен маршрут: • 1 (other) — другое, не может быть отнесен к остальным группам; • 2 (local) — статический маршрут, заданный в конфигурации, • 3 (netmgmt) — протокол SNMP; • 4 (icmp) — протокол ICMP (Redirect); • 5 (egp) — протокол EGP; • 6 (ggp) — протокол GGP; • 7 (hello) — протокол Hello; • 8 (rip) — протокол RIP; • 9 (is-is) — протокол IS-IS; • 10 (es-is) — протокол ES-IS; • 11 (ciscoIgrp) — протокол cisco IGRP; • 12 (bbnSpfIgp) — протокол BBNSPFIGP; • 13 (ospf) — протокол OSPF; • 14 (bgp) — протокол BGP.
.1.3.6.1.2.1.4.21.1.10.E	Время жизни маршрута с последнего обновления (в секундах).
.1.3.6.1.2.1.4.21.1.11.E	Маска маршрута.
.1.3.6.1.2.1.4.21.1.12.E	Дополнительная метрика протокола маршрутизации.
.1.3.6.1.2.1.4.21.1.13.E	Информация о протоколе маршрутизации, с помощью которого был получен маршрут. Если эта информация не представлена, параметр равен 0.0.
.1.3.6.1.2.1.11.1.0	Количество полученных сообщений SNMP.
.1.3.6.1.2.1.11.2.0	Количество отправленных сообщений SNMP.
.1.3.6.1.2.1.11.3.0	Количество полученных сообщений SNMP неподдерживаемой версии.

OID	Описание
.1.3.6.1.2.1.11.4.0	Количество полученных сообщений SNMP, адресованных неизвестному сообществу.
.1.3.6.1.2.1.11.5.0	Количество полученных сообщений SNMP, содержащих операцию, не разрешенную на сетевом узле для сообщества.
.1.3.6.1.2.1.11.6.0	Количество ошибок ASN.1 или BER при разборе SNMP-сообщений.
.1.3.6.1.2.1.11.8.0	Количество входящих SNMP PDU, для которых значение поля error-status – «tooBig».
.1.3.6.1.2.1.11.9.0	Количество входящих SNMP PDU, для которых значение поля error-status – «noSuchName».
1.3.6.1.2.1.11.10.0	Количество входящих SNMP PDU, для которых значение поля error-status – «badValue».
.1.3.6.1.2.1.11.11.0	Количество входящих SNMP PDU, для которых значение поля error-status – «readOnly».
.1.3.6.1.2.1.11.12.0	Количество входящих SNMP PDU, для которых значение поля error-status – «genErr».
.1.3.6.1.2.1.11.13.0	Количество успешно полученных MIB объектов с использованием Get-Request и Get-Next.
.1.3.6.1.2.1.11.14.0	Количество успешно записанных MIB объектов с использованием Set-Request.
.1.3.6.1.2.1.11.15.0	Количество успешно обработанных SNMP Get-Request PDUs.
.1.3.6.1.2.1.11.16.0	Количество успешно обработанных SNMP Get-Next PDUs.
.1.3.6.1.2.1.11.17.0	Количество успешно обработанных SNMP Set-Request PDUs.
.1.3.6.1.2.1.11.18.0	Количество успешно обработанных SNMP Get-Response PDUs.
.1.3.6.1.2.1.11.19.0	Количество успешно обработанных SNMP Trap PDUs.
.1.3.6.1.2.1.11.20.0	Количество исходящих SNMP PDU, для которых значение поля error-status – «tooBig».
.1.3.6.1.2.1.11.21.0	Количество исходящих SNMP PDU, для которых значение поля error-status – «noSuchName».
.1.3.6.1.2.1.11.22.0	Количество исходящих SNMP PDU, для которых значение поля error-status – «badValue».
.1.3.6.1.2.1.11.24.0	Количество исходящих SNMP PDU, для которых значение поля error-status – «genErr».
.1.3.6.1.2.1.11.25.0	Количество успешно сгенерированных исходящих SNMP Get-Request PDUs.
.1.3.6.1.2.1.11.26.0	Количество успешно сгенерированных исходящих SNMP Get-Next PDUs.

OID	Описание
.1.3.6.1.2.1.11.27.0	Количество успешно сгенерированных исходящих SNMP Set-Request PDUs.
.1.3.6.1.2.1.11.28.0	Количество успешно сгенерированных исходящих SNMP Get-Response PDUs.
.1.3.6.1.2.1.11.29.0	Количество успешно сгенерированных исходящих SNMP Trap PDUs.
.1.3.6.1.2.1.11.30.0	Возможность отправки authenticationFailure traps: • 1 — разрешено; • 2 — запрещено.
.1.3.6.1.2.1.11.31.0	Количество параметров отброшенных SNMP без уведомлений в связи с несоответствием параметров агента и сервера.
.1.3.6.1.2.1.11.32.0	Количество параметров отброшенных SNMP без уведомлений в связи с проблемами proxy.

IF-MIB

IF-MIB (.1.3.6.1.2.1.2) включает в себя объекты, предназначенные для получения информации о параметрах сетевых интерфейсов сетевого узла (например, тип сетевого интерфейса, физический адрес, пропускная способность). Подробнее см. в RFC 2863.

Примечание. Количество и индексы сетевых интерфейсов ViPNet Coordinator HW могут различаться для разных групп OID в описывающих их таблицах. При настройке мониторинга по протоколу SNMP вместо индексов используйте названия (логические имена) сетевых интерфейсов.

ПО ViPNet использует следующие объекты, для которых возможно только чтение данных:

Таблица 41. SNMP-параметры. IF-MIB

OID	Описание
.1.3.6.1.2.1.2.1.0	Количество сетевых интерфейсов (физических, виртуальных, включая loopback).
Таблица объектов, описывающих сетевые интерфейсы (.1.3.6.1.2.1.2.2.1):	
A — индекс интерфейса	
.1.3.6.1.2.1.2.2.1.1.A	Индекс сетевого интерфейса (A).
.1.3.6.1.2.1.2.2.1.2.A	Описание интерфейса (производитель, название и версия оборудования или ПО).

OID	Описание
.1.3.6.1.2.1.2.2.1.3.A	Тип сетевого интерфейса: • 6 — ethernet; • 24 — localhost. Остальные значения можно посмотреть здесь.
.1.3.6.1.2.1.2.2.1.4.A	MTU (в байтах).
.1.3.6.1.2.1.2.2.1.5.A	Максимальная пропускная способность (бит/сек).
.1.3.6.1.2.1.2.2.1.6.A	MAC-адрес.
.1.3.6.1.2.1.2.2.1.7.A	Назначенное состояние интерфейса: • 1 (up) — включен; • 2 (down) — выключен; • 3 (testing) — состояние тестирования, указывает, что никакие рабочие пакеты не могут быть переданы.
.1.3.6.1.2.1.2.2.1.8.A	Текущее рабочее состояние интерфейса: • 1 (up) — включен; • 2 (down) — выключен; • 3 (testing) — состояние тестирования. Никакие рабочие пакеты не могут быть переданы; • 4 (unknown) — неизвестно; • 5 (dormant) — интерфейс ожидает внешних действий (таких как последовательная линия, ожидающая входящее соединение); • 6 (notPresent) — в интерфейсе отсутствуют компоненты (обычно аппаратные); • 7 (lowerLayerDown) — не работает из-за состояния интерфейса нижнего уровня.
.1.3.6.1.2.1.2.2.1.9.A	Время работы SNMP-агента с начала его запуска (sysUpTime) до момента перехода интерфейса в его текущее состояние.
.1.3.6.1.2.1.2.2.1.10.A	Количество полученных байт (октетов).
.1.3.6.1.2.1.2.2.1.11.A	Количество полученных одноадресных (unicast) пакетов.
.1.3.6.1.2.1.2.2.1.12.A	Количество полученных широковещательных (broadcast) и многоадресных (multicast) пакетов.
.1.3.6.1.2.1.2.2.1.13.A	Количество отклоненных пакетов.
.1.3.6.1.2.1.2.2.1.14.A	Количество пакетов, отклоненных из-за ошибок.
.1.3.6.1.2.1.2.2.1.15.A	Количество пакетов, которые были отклонены из-за неизвестного или не поддерживаемого протокола.
.1.3.6.1.2.1.2.2.1.16.A	Количество отправленных байт (октетов).
.1.3.6.1.2.1.2.2.1.17.A	Количество отправленных одноадресных (unicast) пакетов.

OID	Описание
.1.3.6.1.2.1.2.2.1.18.A	Количество отправленных широковещательных (broadcast) и многоадресных (multicast) пакетов.
.1.3.6.1.2.1.2.2.1.19.A	Количество отклоненных отправленных пакетов.
.1.3.6.1.2.1.2.2.1.20.A	Количество отправленных пакетов, отклоненных из-за ошибок.
.1.3.6.1.2.1.2.2.1.21.A	Количество исходящих пакетов в очереди на отправку.

Таблица статистики дополнительных параметров сетевых интерфейсов (.1.3.6.1.2.1.31.1.1.1):

A — индекс интерфейса из таблицы 1.3.6.1.2.1.2.2.1

.1.3.6.1.2.1.31.1.1.1.1.A	Имя интерфейса.
.1.3.6.1.2.1.31.1.1.1.2.A	Количество входящих многоадресных (multicast) пакетов.
.1.3.6.1.2.1.31.1.1.1.3.A	Количество входящих широковещательных (broadcast) пакетов.
.1.3.6.1.2.1.31.1.1.1.4.A	Количество исходящих многоадресных (multicast) пакетов.
.1.3.6.1.2.1.31.1.1.1.5.A	Количество исходящих широковещательных (broadcast) пакетов.
.1.3.6.1.2.1.31.1.1.1.6.A	Количество байт (октетов), принятых интерфейсом (64-разрядный счетчик).
.1.3.6.1.2.1.31.1.1.1.7.A	Количество входящих одноадресных (unicast) пакетов (64-разрядный счетчик).
.1.3.6.1.2.1.31.1.1.1.8.A	Количество входящих многоадресных (multicast) пакетов (64-разрядный счетчик).
.1.3.6.1.2.1.31.1.1.1.9.A	Количество входящих широковещательных (broadcast) пакетов (64-разрядный счетчик).
.1.3.6.1.2.1.31.1.1.1.10.A	Количество байт (октетов), отправленных интерфейсом (64-разрядный счетчик).
.1.3.6.1.2.1.31.1.1.1.11.A	Количество исходящих одноадресных (unicast) пакетов (64-разрядный счетчик).
.1.3.6.1.2.1.31.1.1.1.12.A	Количество исходящих многоадресных (multicast) пакетов (64-разрядный счетчик).
.1.3.6.1.2.1.31.1.1.1.13.A	Количество исходящих широковещательных (broadcast) пакетов (64-разрядный счетчик).
.1.3.6.1.2.1.31.1.1.1.14.A	Необходимость отправки trap на события linkUp/linkDown: • 1 — отправлять trap; • 2 — не отправлять trap.
.1.3.6.1.2.1.31.1.1.1.15.A	Максимальная скорость интерфейса (Мегабит/сек).
.1.3.6.1.2.1.31.1.1.1.16.A	Режим работы интерфейса: • 1 (true) — принимает все пакеты; • 2 (false) — принимает только пакеты, адресованные сетевому узлу.

OID	Описание
.1.3.6.1.2.1.31.1.1.1.17.A	Наличие физического коннектора у интерфейса: • 1 (true) — есть коннектор (для ethernet); • 2 (false) — нет коннектора (для localhost).
.1.3.6.1.2.1.31.1.1.1.18.A	Имя интерфейса, заданное администратором. Для координатора всегда равно 0.
.1.3.6.1.2.1.31.1.1.1.19.A	Время работы SNMP-агента с последнего запуска (sysUpTime) до появления разрыва в подсчете счетчиков на интерфейсе.
.1.3.6.1.2.1.31.1.5.0	Время работы SNMP-агента с последнего запуска (sysUpTime) до последнего добавления или удаления записи в таблице статистики дополнительных параметров сетевых интерфейсов.

IP-MIB

IP-MIB (.1.3.6.1.2.1.4) включает в себя объекты, предназначенные для получения информации о работе сетевого узла по протоколу IP (например, параметры сетевых интерфейсов, статистика для IP-трафика, таблица IP-адресов). Подробнее см. в RFC 4293.

ПО ViPNet использует следующие объекты, для которых возможно только чтение данных:

Таблица 42. SNMP-параметры. IP-MIB

OID	Описание
.1.3.6.1.2.1.4.1.0	Указывает, является ли сетевой узел маршрутизатором: • 1 — является (координатор всегда работает в данном режиме); • 2 — не является.
.1.3.6.1.2.1.4.2.0	TTL по умолчанию для IP-пакетов.
.1.3.6.1.2.1.4.3.0	Общее количество IP-пакетов, принятых сетевым узлом, включая пакеты с ошибками.
.1.3.6.1.2.1.4.4.0	Количество входящих IP-пакетов, отклоненных сетевым узлом по причине ошибок в заголовке пакета.
.1.3.6.1.2.1.4.5.0	Количество входящих IP-пакетов, отклоненных сетевым узлом по причине ошибок в адресе.
.1.3.6.1.2.1.4.6.0	Количество IP-пакетов, переданных на следующий шлюз.
.1.3.6.1.2.1.4.7.0	Количество IP-пакетов, отклонённых по причине неизвестного или неподдерживаемого протокола.
1.3.6.1.2.1.4.8.0	Количество отклоненных пакетов по причине недостатка буфера.
.1.3.6.1.2.1.4.9.0	Количество успешно доставленных IP-пакетов.

OID	Описание
.1.3.6.1.2.1.4.10.0	Количество IP-пакетов, отправленных сетевым узлом (не включая .1.3.6.1.2.1.4.6.0).
.1.3.6.1.2.1.4.11.0	Количество IP-пакетов, отклонённых по причине недостатка буфера.
.1.3.6.1.2.1.4.12.0	Количество IP-пакетов, отклоненных к дальнейшей передаче по причине отсутствия маршрута.
.1.3.6.1.2.1.4.13.0	Максимальное количество секунд ожидания сборки фрагментов.
.1.3.6.1.2.1.4.14.0	Количество принятых IP-фрагментов.
.1.3.6.1.2.1.4.15.0	Количество успешных сборок IP-пакетов из фрагментов.
.1.3.6.1.2.1.4.16.0	Количество ошибок сборок IP-пакетов из фрагментов.
.1.3.6.1.2.1.4.17.0	Количество успешно фрагментированных исходящих IP-пакетов.
.1.3.6.1.2.1.4.18.0	Количество ошибок при фрагментации исходящих IP-пакетов.
.1.3.6.1.2.1.4.19.0	Количество фрагментов IP-пакетов, сгенерированных данным сетевым узлом.

Таблица IP-адресов сетевого узла для протокола IPv4 (.1.3.6.1.2.1.4.20.1.):

E — IP-адрес

.1.3.6.1.2.1.4.20.1.1.E	IP-адрес.
.1.3.6.1.2.1.4.20.1.2.E	Указатель на интерфейс, которому присвоен этот IP-адрес (A - из таблицы .1.3.6.1.2.1.2.2.1).
.1.3.6.1.2.1.4.20.1.3.E	Маска сети.
.1.3.6.1.2.1.4.20.1.4.E	Значение наименее значимого бита в широковещательном (broadcast) IP-адресе.

Таблица разрешения IP-адресов в физические адреса (ARP-таблица) (.1.3.6.1.2.1.4.22.1.):

A — индекс интерфейса из таблицы 1.3.6.1.2.1.2.2.1.1 IF-MIB

E — IP-адрес

.1.3.6.1.2.1.4.22.1.1.A.E	Индекс интерфейса, для которого видна связка IP-MAC.
.1.3.6.1.2.1.4.22.1.2.A.E	MAC-адрес.
.1.3.6.1.2.1.4.22.1.3.A.E	IP-адрес.
.1.3.6.1.2.1.4.22.1.4.A.E	Тип маппинга: • 1 — другое; • 2 — некорректный; • 3 — динамический; • 4 — статический.
.1.3.6.1.2.1.4.23.0	Количество отклоненных маршрутов.

OID	Описание
.1.3.6.1.2.1.4.31.1.1.	Таблица, содержащая статистику (счетчики) IP-трафика различных версий на сетевом узле для всех интерфейсов.
.1.3.6.1.2.1.4.31.2.0	Значение sysUpTime в момент добавления/удаления столбцов в таблицу .1.3.6.1.2.1.4.31.1.1.

Таблица префиксов IP-адресов (.1.3.6.1.2.1.4.32.1.):

A — индекс интерфейса из таблицы 1.3.6.1.2.1.2.2.1.1 IF-MIB

B — тип адреса:

- **значение 0 — неизвестно;**
- **значение 1 — ipv4;**
- **значение 2 — ipv6;**
- **значение 3 — ipv4z;**
- **значение 4 — ipv6z;**
- **значение 16 — dns.**

C — префикс (адрес сети)

D — длина префикса

.1.3.6.1.2.1.4.32.1.5.A.B.C.D	Источник префикса: • 1 — другое; • 2 — вручную; • 3 — общеизвестный префикс; • 4 — dhcp; • 3 — routeradv (значение получено от роутера).
.1.3.6.1.2.1.4.32.1.6.A.B.C.D	Указывает, может ли префикс использоваться как маршрут: • 1 — может; • 2 — не может.
.1.3.6.1.2.1.4.32.1.7.A.B.C.D	Указывает, может ли префикс использоваться для автоматической конфигурации адреса: • 1 — может; • 2 — не может.
.1.3.6.1.2.1.4.32.1.8.A.B.C.D	Время (в секундах), в течение которого префикс будет оставаться предпочтительным. Значение 4294967295 означает бесконечность.
.1.3.6.1.2.1.4.32.1.9.A.B.C.D	Время (в секундах), в течение которого префикс будет существовать. Значение 4294967295 означает бесконечность.

OID	Описание
Таблица адресной информации по интерфейсам (.1.3.6.1.2.1.4.34.1):	
B — тип адреса: • **значение 0 — неизвестно;** • **значение 1 — ipv4;** • **значение 2 — ipv6;** • **значение 3 — ipv4z;** • **значение 4 — ipv6z;** • **значение 16 — dns.**	
E — IP-адрес	
.1.3.6.1.2.1.4.34.1.3.B.E	Индекс сетевого интерфейса.
.1.3.6.1.2.1.4.34.1.4.B.E	Тип адреса: • 1 (unicast) — одноадресный; • 2 (anycast) — к ближайшему узлу; • 3 (broadcast) — широковещательный.
.1.3.6.1.2.1.4.34.1.5.B.E	Ссылка на строку таблицы префиксов.
.1.3.6.1.2.1.4.34.1.6.B.E	Происхождение адреса: • 1 (other) — другое; • 2 (manual) — назначен вручную; • 4 (dhcp) — назначен по dhcp; • 5 (linklayer) — назначен механизмом автоконфигурации протокола IPv6 (SLAAC); • 6 (random) — назначен случайным образом.
.1.3.6.1.2.1.4.34.1.7.B.E	Статус адреса: • 1 (preferred) — предпочтительный; • 2 (deprecated) — устарел; • 3 (invalid) — недействителен; • 4 (inaccessible) — недоступен; • 5 (unknown)— неизвестен; • 6 (tentative) — предварительный; • 7 (duplicate) — дублированный; • 8 (optimistic) — оптимистичный.
.1.3.6.1.2.1.4.34.1.8.B.E	Время работы SNMP-агента после запуска (sysUpTime) до момента создания записи.
.1.3.6.1.2.1.4.34.1.9.B.E	Время работы SNMP-агента после запуска (sysUpTime) до момента изменения записи.

OID	Описание
.1.3.6.1.2.1.4.34.1.10.B.E	Статус строки: • 1 (active) — строка доступна для использования; • 2 (notInService) — строка недоступна для использования; • 3 (notReady) — отсутствует информация для использования; • 4 (createAndGo) — создание строки и перевод ее в статус active; • 5 (createAndWait) — создание строки и перевод ее в статус notInService; • 6 (destroy) — удаление.
.1.3.6.1.2.1.4.34.1.11.B.E	Механизм хранения строки: • 1 (other) — другое; • 2 (volatile) — изменяемая; • 3 (nonvolatile) — энергонезависимая; • 4 (permanent) — постоянная; • 5 (readOnly) — только для чтения.

Таблица трансляции MAC IP (.1.3.6.1.2.1.4.35.1):

A — индекс интерфейса из таблицы .1.3.6.1.2.1.2.2.1.1 MIB-II

B — тип адреса:

- **0 — неизвестно;**
- **1 — ipv4;**
- **2 — ipv6;**
- **3 — ipv4z;**
- **4 — ipv6z;**
- **16 — dns.**

E — IP-адрес

.1.3.6.1.2.1.4.35.1.4.A.B.E	Транслируемый MAC-адрес.
.1.3.6.1.2.1.4.35.1.5.A.B.E	Время работы SNMP-агента с момента последнего запуска (sysUpTime) до момента изменения MAC-адреса.
.1.3.6.1.2.1.4.35.1.6.A.B.E	Тип маппинга: • 1 (other) — другое; • 2 (invalid) — недопустимое значение; • 3 (dynamic) — динамическое; • 4 (static) — статическое; • 5 (local) — предоставляется для собственного адреса интерфейса объекта.

OID	Описание
.1.3.6.1.2.1.4.35.1.7.A.B.E	Статус маппинга: • 1(reachable) — подтвержден; • 2 (stale) — не подтвержден; • 3 (delay) — ожидание; • 4 (probeprobe) — активное; • 5 (invalid) — недействителен; • 6 (unknown) — не определен; • 7 (incomplete) — выполняется разрешение адреса.
.1.3.6.1.2.1.4.35.1.8.A.B.E	Статус строки: • 1 (active) — строка доступна для использования; • 2 (notInService) — строка недоступна для использования; • 3 (notReady) — отсутствует информация для использования; • 4 (createAndGo) — создание строки и перевод ее в статус active; • 5 (createAndWait) — создание строки и перевод ее в статус notInService; • 6 (destroy) — удаление.
.1.3.6.1.2.1.5.1.0	Общее число ICMP-запросов, полученных сетевым узлом.
.1.3.6.1.2.1.5.2.0	Число ICMP-запросов с ошибкой, полученных сетевым узлом.
.1.3.6.1.2.1.5.3.0	Количество сообщений о недоступности заданного сетевого узла, полученных данным сетевым узлом.
.1.3.6.1.2.1.5.4.0	Количество сообщений об истечении времени ожидания ответа, полученных сетевым узлом.
.1.3.6.1.2.1.5.5.0	Количество полученных сообщений ICMP Parameter Problem.
.1.3.6.1.2.1.5.6.0	Количество полученных сообщений ICMP Source Quench.
.1.3.6.1.2.1.5.7.0	Количество полученных сообщений ICMP Redirect messages.
.1.3.6.1.2.1.5.8.0	Количество полученных сообщений ICMP Echo (request).
.1.3.6.1.2.1.5.9.0	Количество полученных сообщений ICMP Echo Reply.
.1.3.6.1.2.1.5.10.0	Количество полученных сообщений ICMP Timestamp (request).
.1.3.6.1.2.1.5.11.0	Количество полученных сообщений ICMP Timestamp Reply.
.1.3.6.1.2.1.5.12.0	Количество полученных сообщений ICMP Address Mask Request.
.1.3.6.1.2.1.5.13.0	Количество полученных сообщений ICMP Address Mask Reply.
.1.3.6.1.2.1.5.14.0	Количество ICMP сообщений, отправленных сетевым узлом.
.1.3.6.1.2.1.5.15.0	Количество ICMP сообщений, которые сетевой узел не смог отправить из-за проблем с ICMP.
.1.3.6.1.2.1.5.16.0	Количество отправленных сообщений ICMP Destination Unreachable.

OID	Описание
.1.3.6.1.2.1.5.17.0	Количество отправленных сообщений ICMP Time Exceeded.
.1.3.6.1.2.1.5.18.0	Количество отправленных сообщений ICMP Parameter Problem.
1.3.6.1.2.1.5.19.0	Количество отправленных сообщений ICMP Source Quench.
1.3.6.1.2.1.5.20.0	Количество отправленных сообщений ICMP Redirect.
1.3.6.1.2.1.5.21.0	Количество отправленных сообщений ICMP Echo (request).
.1.3.6.1.2.1.5.22.0	Количество отправленных сообщений ICMP Echo Reply.
.1.3.6.1.2.1.5.23.0	Количество отправленных сообщений ICMP Timestamp (request).
.1.3.6.1.2.1.5.24.0	Количество отправленных сообщений ICMP Timestamp Reply.
.1.3.6.1.2.1.5.25.0	Количество отправленных сообщений ICMP Address Mask Request.
.1.3.6.1.2.1.5.26.0	Количество отправленных сообщений ICMP Address Mask Reply.
.1.3.6.1.2.1.5.29.1	Таблица счетчиков ICMP сообщений с указанием версии протокола IP.
.1.3.6.1.2.1.5.30.1	Таблица счетчиков входящих-исходящих ICMP пакетов с указанием версии протокола IP.

IP-FORWARD-MIB

IP-FORWARD-MIB (.1.3.6.1.2.1.4.24) включает в себя объекты, предназначенные для получения информации о параметрах маршрутизации сетевого узла. Подробнее см. в RFC 4292.

ПО ViPNet использует следующие объекты, для которых возможно только чтение данных:

Таблица 43. SNMP-параметры. IP-FORWARD-MIB

OID	Описание
Таблица маршрутизации сетевого узла (.1.3.6.1.2.1.4.24.4.1):	
.1.3.6.1.2.1.4.24.4.1.1.A.B.C.D	Адрес назначения маршрута (A).
.1.3.6.1.2.1.4.24.4.1.2.A.B.C.D	Маска адреса назначения маршрута (B).
.1.3.6.1.2.1.4.24.4.1.3.A.B.C.D	Параметр, обозначающий значение поля IP TOS Field (C).
.1.3.6.1.2.1.4.24.4.1.4.A.B.C.D	Адрес следующего маршрутизатора в маршруте (D).
.1.3.6.1.2.1.4.24.4.1.5.A.B.C.D	Индекс интерфейса, для которого задан маршрут из таблицы .1.3.6.1.2.1.2.2.1 IF-MIB.

OID	Описание
.1.3.6.1.2.1.4.24.4.1.6.A.B.C.D	Тип маршрута: • 1 (other) — другое, не может быть отнесен к остальным группам, • 2 (reject) — недостижимый, • 3 (local) — маршрут, в котором адрес следующего маршрутизатора является адресом назначения, • 4 (remote) — маршрут, в котором адрес следующего маршрутизатора не является адресом назначения.
.1.3.6.1.2.1.4.24.4.1.7.A.B.C.D	Механизм маршрутизации, с помощью которого был получен маршрут: • 1 (other) — другое, не может быть отнесен к остальным группам, • 2 (local) — статический маршрут, заданный в конфигурации, • 3 (netmgmt) — протокол SNMP, • 4 (icmp) — протокол ICMP (Redirect), • 5 (egp) — протокол EGP, • 6 (ggp) — протокол GGP, • 7 (hello) — протокол Hello, • 8 (rip) — протокол RIP, • 9 (is-is) — протокол IS-IS, • 10 (es-is) — протокол ES-IS, • 11 (ciscoIgrp) — протокол cisco IGRP, • 12 (bbnSpfIgp) — протокол BBNSPFIGP, • 13 (ospf) — протокол OSPF, • 14 (bgp) — протокол BGP, • 15 (idpr) — протокол IDRP, • 16 (ciscoEigrp) — протокол cisco EIGRP.
.1.3.6.1.2.1.4.24.4.1.8.A.B.C.D	Время жизни маршрута с последнего обновления (в секундах).
.1.3.6.1.2.1.4.24.4.1.9.A.B.C.D	Информация о протоколе маршрутизации, с помощью которого был получен маршрут. Если эта информация не представлена, параметр равен 0.0.
.1.3.6.1.2.1.4.24.4.1.10.A.B.C.D	Номер AS, к которой относится следующий маршрутизатор в маршруте. Если неизвестен или если для маршрутизации не используется, параметр равен 0.
.1.3.6.1.2.1.4.24.4.1.11.A.B.C.D	Основная метрика маршрута. Если метрика не используется, параметр равен -1.
.1.3.6.1.2.1.4.24.4.1.12.A.B.C.D	Дополнительная метрика маршрута. Если метрика не используется, параметр равен -1.
.1.3.6.1.2.1.4.24.4.1.13.A.B.C.D	Дополнительная метрика маршрута. Если метрика не используется, параметр равен -1.

OID	Описание
.1.3.6.1.2.1.4.24.4.1.14.A.B.C.D	Дополнительная метрика маршрута. Если метрика не используется, параметр равен -1.
.1.3.6.1.2.1.4.24.4.1.15.A.B.C.D	Дополнительная метрика маршрута. Если метрика не используется, параметр равен -1.
.1.3.6.1.2.1.4.24.4.1.16.A.B.C.D	Статус строки таблицы: • 1 (active) — строка доступна для использования, • 2 (notInService) — строка недоступна для использования, • 3 (notReady) — отсутствует информация для использования, • 4 (createAndGo) — создание строки и перевод ее в статус active, • 5 (createAndWait) — создание строки и перевод ее в статус notInService, • 6 (destroy) — удаление
1.3.6.1.2.1.4.24.6.0	Количество текущих корректных маршрутов из таблицы .1.3.6.1.2.1.4.24.7.1
Таблица маршрутизации сетевого узла с указанием версии протокола IP (.1.3.6.1.2.1.4.24.7.1):	
.1.3.6.1.2.1.4.24.7.1.7	Индекс интерфейса, для которого задан маршрут из таблицы .1.3.6.1.2.1.2.2 IF-MIB.
.1.3.6.1.2.1.4.24.7.1.8	Тип маршрута: • 1 (other) — другое, не может быть отнесен к остальным группам, • 2 (reject) — недостижимый, • 3 (local) — маршрут, в котором адрес следующего маршрутизатора является адресом назначения, • 4 (remote) — маршрут, в котором адрес следующего маршрутизатора не является адресом назначения, • 5 (blackhole) — маршрут, по которому пакеты теряются без сообщений об ошибках.

OID	Описание
.1.3.6.1.2.1.4.24.7.1.9	Механизм маршрутизации, с помощью которого был получен маршрут: • 1 (other) — другое, не может быть отнесен к остальным группам, • 2 (local) — статический маршрут, заданный в конфигурации, • 3 (netmgmt) — протокол SNMP, • 4 (icmp) — протокол ICMP (Redirect), • 5 (egp) — протокол EGP, • 6 (ggp) — протокол GGP, • 7 (hello) — протокол Hello, • 8 (rip) — протокол RIP, • 9 (is-is) — протокол IS-IS, • 10 (es-is) — протокол ES-IS, • 11 (ciscoIgrp) — протокол cisco IGRP, • 12 (bbnSpfIgp) — протокол BBNSPFIGP, • 13 (ospf) — протокол OSPF, • 14 (bgp) — протокол BGP, • 15 (idpr) — протокол IDRP, • 16 (ciscoEigrp) — протокол cisco EIGRP.
.1.3.6.1.2.1.4.24.7.1.10	Время жизни маршрута с последнего обновления (в секундах).
.1.3.6.1.2.1.4.24.7.1.11	Номер AS, к которой относится следующий маршрутизатор в маршруте. Если неизвестен или если для маршрутизации не используется, параметр равен 0.
.1.3.6.1.2.1.4.24.7.1.12	Основная метрика маршрута. Если метрика не используется, параметр равен -1.
.1.3.6.1.2.1.4.24.7.1.13	Дополнительная метрика маршрута. Если метрика не используется, параметр равен -1.
.1.3.6.1.2.1.4.24.7.1.14	Дополнительная метрика маршрута. Если метрика не используется, параметр равен -1.
.1.3.6.1.2.1.4.24.7.1.15	Дополнительная метрика маршрута. Если метрика не используется, параметр равен -1.
.1.3.6.1.2.1.4.24.7.1.16	Дополнительная метрика маршрута. Если метрика не используется, параметр равен -1.

OID	Описание
.1.3.6.1.2.1.4.24.7.1.17	Статус строки таблицы: • 1 (active) — строка доступна для использования, • 2 (notInService) — строка недоступна для использования, • 3 (notReady) — отсутствует информация для использования, • 4 (createAndGo) — создание строки и перевод ее в статус active, • 5 (createAndWait) — создание строки и перевод ее в статус notInService, • 6 (destroy) — удаление.

Ethernet-Like MIB

Ethernet-Like MIB (1.3.6.1.2.1.10) включает в себя объекты, предназначенные для получения статистической информации о работе интерфейсов сетевого узла. Подробнее см. в RFC 3635.

ПО ViPNet использует следующие объекты, для которых возможно только чтение данных:

Таблица 44. SNMP-параметры. Ethernet-Like MIB

OID	Описание
Таблица статистики Ethernet-интерфейсов (.1.3.6.1.2.1.10.7.2.1): **A — индекс интерфейса из таблицы 1.3.6.1.2.1.2.2.1.1 IF-MIB**	
.1.3.6.1.2.1.10.7.2.1.1.A	Индекс интерфейса из таблицы 1.3.6.1.2.1.2.2.1.1 IF-MIB.
.1.3.6.1.2.1.10.7.2.1.2.A	Количество ошибок на интерфейсе.
.1.3.6.1.2.1.10.7.2.1.3.A	Количество FCS ошибок на интерфейсе.
.1.3.6.1.2.1.10.7.2.1.4.A	Количество фреймов, вовлечённых в SingleCollision на интерфейсе.
.1.3.6.1.2.1.10.7.2.1.5.A	Количество фреймов, вовлечённых в MultiplyCollision на интерфейсе.
.1.3.6.1.2.1.10.7.2.1.6.A	Количество ошибок SQE TEST ERROR на интерфейсе.
.1.3.6.1.2.1.10.7.2.1.7.A	Количество фреймов, для которых первая попытка отправки была отложена на интерфейсе.
.1.3.6.1.2.1.10.7.2.1.8.A	Количество обнаружения коллизий на интерфейсе, при котором коллизия обнаружена позднее одного slotTime.
.1.3.6.1.2.1.10.7.2.1.9.A	Количество фреймов, которые не удалось передать в связи с коллизиями.
.1.3.6.1.2.1.10.7.2.1.10.A	Количество фреймов, которые не удалось передать в связи с проблемами MAC уровня.
.1.3.6.1.2.1.10.7.2.1.11.A	Количество ошибок передачи в связи с потерей carrier sense condition на интерфейсе.

OID	Описание
.1.3.6.1.2.1.10.7.2.1.13.A	Количество фреймов, принятых на интерфейсе, размер которых превышал максимально допустимый.
.1.3.6.1.2.1.10.7.2.1.16.A	Количество фреймов, которые не удалось принять на интерфейсе в связи с ошибками MAC уровня.
.1.3.6.1.2.1.10.7.2.1.17.A	Идентификатор чипа, который реализует Ethernet-интерфейс.
.1.3.6.1.2.1.10.7.2.1.18.A	Количество ошибок.
.1.3.6.1.2.1.10.7.2.1.19.A	Текущий режим дуплекса на интерфейсе: • 1 — unknown, • 2 — halfDuplex, • 3 — fullDuplex. Для неподключённых интерфейсов параметр равен 1.
1.3.6.1.2.1.10.7.2.1.20.A	Возможность контроля скорости передачи на интерфейсе: • 1 — разрешено, • 2 — запрещено.
.1.3.6.1.2.1.10.7.2.1.21AA	Статус контроля скорости передачи на интерфейсе: • 1 — выключен, • 2 — включен, • 3 — неизвестно.

TCP-MIB

TCP-MIB (.1.3.6.1.2.1.6) включает в себя объекты, предназначенные для получения информации о работе сетевого узла по протоколу TCP (например, количество отправленных сегментов, активных соединений). Подробнее см. в RFC 4022.

ПО ViPNet использует следующие объекты, для которых возможно только чтение данных:

Таблица 45. SNMP-параметры. TCP-MIB

OID	Описание
.1.3.6.1.2.1.6.1.0	Алгоритм определения таймаута для повторной передачи неопознанных октетов.
.1.3.6.1.2.1.6.2.0	Минимальное допустимое значение таймаута для повторной передачи (в миллисекундах).
.1.3.6.1.2.1.6.3.0	Максимальное допустимое значение таймаута для повторной передачи (в миллисекундах).
.1.3.6.1.2.1.6.4.0	Максимальное количество TCP-соединений. При динамическом определении, параметр равен -1.

OID	Описание
.1.3.6.1.2.1.6.5.0	Количество прямых переходов TCP-соединений из состояния CLOSED в состояние SYN-SENT.
.1.3.6.1.2.1.6.6.0	Количество прямых переходов TCP-соединений из состояния LISTEN в состояние SYN-RCVD.
.1.3.6.1.2.1.6.7.0	Количество прямых переходов TCP-соединений в состояние CLOSED из состояния SYN-SENT или SYN-RCVD, а также прямых переходов в состояние LISTEN из состояния SYN-RCVD.
.1.3.6.1.2.1.6.8.0	Количество переходов TCP-соединений в состояние CLOSED из состояния ESTABLISHED или CLOSE-WAIT.
.1.3.6.1.2.1.6.9.0	Количество TCP-соединений, находящихся в состоянии ESTABLISHED или CLOSE-WAIT.
.1.3.6.1.2.1.6.10.0	Количество полученных сегментов, в том числе с ошибками. Включает только количество полученных сегментов на соединениях, установленных в настоящий момент.
.1.3.6.1.2.1.6.11.0	Количество отправленных сегментов.
.1.3.6.1.2.1.6.12.0	Общее количество повторно отправленных сегментов.

Таблица TCP-соединений для протокола IPv4 (.1.3.6.1.2.1.6.13.1):

A - локальный IP-адрес

B - локальный порт

C - удалённый IP-адрес

D - удалённый порт

OID	Описание
.1.3.6.1.2.1.6.13.1.1.A.B.C.D	Состояние TCP-соединения: • 1 (closed) — закрыто, • 2 (listen) — ожидание запроса на соединение со стороны чужих портов и программ TCP, • 3 (synSent) — ожидание парного запроса на установление соединения, • 4 (synReceived) — ожидание подтверждения после того, как запрос соединения уже принят и отправлен, • 5 (established) — установлено, • 6 (finWait1) — ожидание запроса от программы TCP или подтверждения ранее отправленного запроса на закрытие соединения, • 7 (finWait2) — ожидание запроса на закрытие соединения со стороны программы TCP, • 8 (closeWait) — ожидание запроса на закрытие соединения со стороны своего клиента, • 9 (lastAck) — ожидание запроса на закрытие соединения, ранее отправленного программе TCP, • 10 (closing) — ожидание подтверждения со стороны программы TCP запроса о закрытии соединения, • 11 (timeWait) — ожидание, когда программа TCP получила подтверждение своего запроса на закрытие соединения, • 12 (deleteTCB) — удаление буфера управления передачей (TCB) для подключения TCP.
.1.3.6.1.2.1.6.14.0	Количество сегментов с ошибками.
.1.3.6.1.2.1.6.15.0	Количество отправленных сегментов с флагом RST.
Таблица TCP-соединений для протоколов IPv4 и IPv6 (.1.3.6.1.2.1.6.19.1): **V1 — версия протокола IP для локального адреса,** **A — локальный IP-адрес,** **B — локальный порт,** **V2 — версия протокола IP для удалённого адреса,** **C — удалённый IP-адрес,** **D — удалённый порт**	
.1.3.6.1.2.1.6.19.1.7.V1.4.A.B.V2.C.D	Состояние TCP-соединения: • 1 (closed) — закрыто, • 2 (listen) — ожидание запроса на соединение со стороны чужих портов и программ TCP, • 3 (synSent) — ожидание парного запроса на установление соединения, • 4 (synReceived) — ожидание подтверждения после

OID	Описание
	того, как запрос соединения уже принят и отправлен, • 5 (established) — установлено, • 6 (finWait1) — ожидание запроса от программы TCP или подтверждения ранее отправленного запроса на закрытие соединения, • 7 (finWait2) — ожидание запроса на закрытие соединения со стороны программы TCP, • 8 (closeWait) — ожидание запроса на закрытие соединения со стороны своего клиента, • 9 (lastAck) — ожидание запроса на закрытие соединения, ранее отправленного программе TCP, • 10 (closing) — ожидание подтверждения со стороны программы TCP запроса о закрытии соединения, • 11 (timeWait) — ожидание, когда программа TCP получила подтверждение своего запроса на закрытие соединения, • 12 (deleteTCB) — удаление буфера управления передачей (TCB) для подключения.
.1.3.6.1.2.1.6.19.1.8.V1.4.A.B.V2.C.D	Системный идентификатор процесса, связанного с этим соединением. Если такого процесса нет, параметр равен 0.
Таблица открытых TCP-портов (.1.3.6.1.2.1.6.20.1): **V1 — версия протокола IP для локального адреса,** **A — локальный IP-адрес,** **B — локальный порт**	
.1.3.6.1.2.1.6.20.1.4.V1.4.A.B	Системный идентификатор процесса, использующего порт. Если такого процесса нет, параметр равен 0.

UDP-MIB

UDP-MIB (.1.3.6.1.2.1.7) включает в себя объекты, предназначенные для получения информации о различных характеристиках работы сетевого узла по протоколу UDP (например, общее количество полученных и отправленных датаграмм). Подробнее см. в RFC 4113.

ПО ViPNet использует следующие объекты, для которых возможно только чтение данных:

Таблица 46. SNMP-параметры. UDP-MIB

OID	Описание
.1.3.6.1.2.1.7.1.0	Количество входящих UDP-датаграмм.
.1.3.6.1.2.1.7.2.0	Количество входящих UDP-датаграмм, для которых нет открытого порта.

OID	Описание
.1.3.6.1.2.1.7.3.0	Количество входящих UDP-датаграмм, для которых нет открытого порта.
.1.3.6.1.2.1.7.4.0	Количество исходящих UDP-датаграмм.
Таблица открытых UDP-портов для протокола IPv4 (.1.3.6.1.2.1.7.5.1): **A — IP-адрес локального порта,** **B — номер локального порта.**	
.1.3.6.1.2.1.7.5.1.1.A.B	IP-адрес локального порта.
.1.3.6.1.2.1.7.5.1.2.A.B	Номер порта.
Таблица открытых UDP-соединений (.1.3.6.1.2.1.7.7.1): **V1 — версия IP-протокола для локального адреса,** **A — IP-адрес локального порта,** **B — номер локального порта,** **V2 — версия IP-протокола для удалённого адреса,** **C — IP-адрес удалённого порта,** **D — номер удалённого порта.**	
.1.3.6.1.2.1.7.7.1.8.V1.4.A.B.V2.C.D	Системный идентификатор процесса, использующего порт. Если такого процесса нет, параметр равен 0.

HOST-RESOURCES-MIB

HOST-RESOURCES-MIB (.1.3.6.1.2.1.25) включает в себя объекты, предназначенные для получения информации о системных параметрах и оборудовании сетевого узла. Подробнее см. RFC 2790.

ПО ViPNet использует следующие объекты, для которых возможно только чтение данных:

Таблица 47. SNMP-параметры. HOST-RESOURCES-MIB

OID	Описание
.1.3.6.1.2.1.25.1.1.0	Время работы системы с момента последнего запуска.

OID	Описание
.1.3.6.1.2.1.25.1.2.0	Системное время на сетевом узле (значение передается в виде строки байт): • 1-2 байт — год, • 3 байт — месяц, • 4 байт — день, • 5 байт — часы, • 6 байт — минуты, • 7 байт — секунды, • 8 байт — десятые секунды, • 9 байт — «направление» от UTC (соответствующие коды символов ascii), • 10 байт — часы от UTC, • 11 байт — минуты от UTC. Если часовой пояс неизвестен, то последние 3 байта отсутствуют.
1.3.6.1.2.1.25.1.3.0	Индекс устройства из таблицы .1.3.6.1.2.1.25.3.2.1, с которого загружается сетевой узел.
.1.3.6.1.2.1.25.1.4.0	Параметры при загрузке сетевого узла (в том числе название аппаратной платформы — для координатора).
.1.3.6.1.2.1.25.1.5.0	Количество сессий пользователя.
.1.3.6.1.2.1.25.1.6.0	Количество процессов загруженных или исполняемых на сетевом узле.
.1.3.6.1.2.1.25.1.7.0	Максимальное поддерживаемое сетевым узлом количество процессов. Если количество не ограничено, параметр равен 0.
1.3.6.1.2.1.25.2.2.0	Объем оперативной памяти (в килобайтах).
Таблица локальных логических хранилищ сетевого узла (.1.3.6.1.2.1.25.2.3.1):	
A — индекс хранилища	
.1.3.6.1.2.1.25.2.3.1.1.A	Идентификатор, присвоенный сетевым узлом (A).
.1.3.6.1.2.1.25.2.3.1.2.A	OID, присвоенный данному типу хранилища: 1.3.6.1.2.1.25.2.1 + • 1 — устройство не может быть причислено к какой-либо другой категории, • 2 — RAM, • 3 — виртуальная память, временное хранилище, SWAP, • 4 — не извлекаемые НЖМД, • 5 — извлекаемые НЖМД.
.1.3.6.1.2.1.25.2.3.1.3.A	Описание хранилища.

OID	Описание
.1.3.6.1.2.1.25.2.3.1.4.A	Размер в байтах объектов (размеры секторов/блоков/буферов/пакетов), размещенных в данном хранилище.
.1.3.6.1.2.1.25.2.3.1.5.A	Общее количество секторов/блоков/буферов/пакетов в хранилище.
.1.3.6.1.2.1.25.2.3.1.6.A	Количество использованных секторов/блоков/буферов/пакетов в хранилище.
.1.3.6.1.2.1.25.2.3.1.7.A	Количество ошибок операций записи по причине недостатка места.

Таблица устройств сетевого узла (.1.3.6.1.2.1.25.3.2.1):

B — индекс устройства

.1.3.6.1.2.1.25.3.2.1.1.B	Идентификатор, присвоенный сетевым узлом (B).
.1.3.6.1.2.1.25.3.2.1.2.B	OID, присвоенный данному типу устройства: 1.3.6.1.2.1.25.3.1 + • 1 — применяется, если не может быть отнесено к другой группе, • 2 — применяется, если устройство не опознано, • 3 — процессор (ядра), • 4 — сетевой интерфейс, • 5 — принтер, • 6 — жесткий диск (HDD, SSD), • 10 — видеоустройство, • 11 — аудиоустройство, • 12 — сопроцессор, • 13 — клавиатура, • 14 — модем, • 15 — параллельный порт, • 16 — манипулятор типа мышь, • 17 — последовательный порт, • 18 — ленточное хранилище, • 19 — часы, • 20 — энергозависимая память, • 21 — энергонезависимая память.
.1.3.6.1.2.1.25.3.2.1.3.B	Описание устройства.
.1.3.6.1.2.1.25.3.2.1.4.B	ID продукта.

OID	Описание
.1.3.6.1.2.1.25.3.2.1.5.B	Текущий статус устройства: • 1 — статус неизвестен (unknown), • 2 — работает (running), • 3 — предупреждение (warning), • 4 — проверка (testing), • 5 — не работает (down).
.1.3.6.1.2.1.25.3.2.1.6.B	Счетчик количества ошибок на устройстве.

Таблица загрузки процессоров сетевого узла (.1.3.6.1.2.1.25.3.3.1):

B — индекс устройства из таблицы .1.3.6.1.2.1.25.3.2.1

.1.3.6.1.2.1.25.3.3.1.1.B	ID продукта.
.1.3.6.1.2.1.25.3.3.1.2.B	Средняя нагрузка на ядро за последнюю минуту.

Таблица сетевых устройств (.1.3.6.1.2.1.25.3.4.1):

B — индекс устройства из таблицы .1.3.6.1.2.1.25.3.2.1

.1.3.6.1.2.1.25.3.4.1.1.B	Индекс интерфейса из таблицы 1.3.6.1.2.1.2.2.1.1 IF-MIB.

Таблица дисков сетевого узла (.1.3.6.1.2.1.25.3.6.1):

B — индекс устройства из таблицы .1.3.6.1.2.1.25.3.2.1

.1.3.6.1.2.1.25.3.6.1.1.B	Доступ к диску: • 1 — чтение и запись, • 2 — чтение.
.1.3.6.1.2.1.25.3.6.1.2.B	Тип устройства: • 1 — применяется, если не может быть отнесено к другой группе, • 2 — неизвестен, • 3 — жесткий диск, • 4 — дискета, • 5 — оптический диск ROM, • 6 — оптический диск WORM, • 10 — оптический диск RW, • 11 — RAM диск.
.1.3.6.1.2.1.25.3.6.1.3.B	Возможность извлечения диска: • 1 — Разрешено, • 2 — Запрещено.
.1.3.6.1.2.1.25.3.6.1.4.B	Размер диска (в килобайтах). Если диск извлекаемый и он извлечен, параметр равен 0.

Таблица разделов сетевого узла (.1.3.6.1.2.1.25.3.7.1):

B — индекс устройства из таблицы .1.3.6.1.2.1.25.3.2.1

D — индекс устройства из таблицы .1.3.6.1.2.1.25.3.7.1

OID	Описание
.1.3.6.1.2.1.25.3.7.1.1.B.D	Индекс устройства (D).
.1.3.6.1.2.1.25.3.7.1.2.B.D	Описание раздела.
.1.3.6.1.2.1.25.3.7.1.3.B.D	ID раздела в операционной системе — октетная строка.
.1.3.6.1.2.1.25.3.7.1.4.B.D	Размер раздела (в килобайтах).
.1.3.6.1.2.1.25.3.7.1.5.B.D	Файловая система, используемая в разделе. Если файловой системы нет, параметр равен 0.

Таблица файловых систем сетевого узла (.1.3.6.1.2.1.25.3.8.1):

E — индекс устройства из таблицы .1.3.6.1.2.1.25.3.7.1

.1.3.6.1.2.1.25.3.8.1.1.E	Индекс устройства (E).
.1.3.6.1.2.1.25.3.8.1.2.E	Корневая папка файловой системы (точка монтирования).
.1.3.6.1.2.1.25.3.8.1.3.E	Описание удалённого сервера, с которого смонтирована файловая система. Может включать корневую папку файловой системы (точка монтирования) на удалённом сервере. Для локальных файловых систем параметр содержит пустую строку.

OID	Описание
.1.3.6.1.2.1.25.3.8.1.4.E	OID, присвоенный данному типу файловой системы: 1.3.6.1.2.1.25.3.9 + • 1 — Применяется, если не может быть отнесена к другой группе, • 2 — Если тип файловой системы неизвестен, • 3 — BFFS, • 4 — System V, • 5 — DOS FAT, • 6 — OS/2 HPFS, • 7 — MHFS, • 8 — MFS, • 9 — NTFS, • 10 — VNode File System, • 11 — Journaled File System, • 12 — ISO 9660 File System for CD, • 13 — RockRidge File System for CD, • 14 — NFS File System, • 15 — Netware File System, • 16 — Andrew File System, • 17 — OSF DCE Distributed File System, • 18 — AppleShare File System, • 19 — RFS File System, • 20 — Data General DGCFS, • 21 — SVR4 Boot File System, • 22 — Windows FAT32, • 23 — Linux EXT2 File System.
.1.3.6.1.2.1.25.3.8.1.5.E	Права доступа к файловой системе: • 1 — запись, чтение, • 2 — чтение.
.1.3.6.1.2.1.25.3.8.1.6.E	Возможность запуска с файловой системы: • 1 — возможно, • 2 — невозможно.
.1.3.6.1.2.1.25.3.8.1.7.E	Указывает на связь файловой системы и хранилищ.
.1.3.6.1.2.1.25.3.8.1.8.E	Дата последнего полного резервного копирования файловой системы. Октетная строка. Если данные отсутствуют, параметр равен: 00 00 01 01 00 00 00 00.

OID	Описание
.1.3.6.1.2.1.25.3.8.1.9.E	Дата последнего частичного резервного копирования файловой системы. Октетная строка. Если данные отсутствуют, параметр равен: 00 00 01 01 00 00 00 00.
Таблица ПО, запущенного на сетевом узле (.1.3.6.1.2.1.25.4.2.1):	
F — индекс ПО	
.1.3.6.1.2.1.25.4.2.1.1.F	Индекс запущенного ПО (F).
.1.3.6.1.2.1.25.4.2.1.2.F	Наименование запущенного ПО.
.1.3.6.1.2.1.25.4.2.1.3.F	ID ПО производителя.
.1.3.6.1.2.1.25.4.2.1.4.F	Папка, из которой запущено ПО.
.1.3.6.1.2.1.25.4.2.1.5.F	Параметры, с которыми запущено ПО.
.1.3.6.1.2.1.25.4.2.1.6.F	Тип программного обеспечения: • 1 — неизвестно, • 2 — ОС, • 3 — драйвер устройства, • 4 — приложение.
.1.3.6.1.2.1.25.4.2.1.7.F	Текущее состояние ПО: • 1 — запущено (running), • 2 — работоспособно (runnable), • 3 — неработоспособно (notRunnable), • 4 — работает некорректно (invalid).
Таблица с потреблением каждого ПО ЦПУ и ОЗУ (.1.3.6.1.2.1.25.5.1.1):	
F — индекс ПО из таблицы .1.3.6.1.2.1.25.4.2.1	
.1.3.6.1.2.1.25.5.1.1.1.F	Количество процессорного времени, выделенного ПО, в сантисекундах (0,01 с).
.1.3.6.1.2.1.25.5.1.1.2.F	Количество занимаемой оперативной памяти (в килобайтах).

LM-SENSORS-MIB

LM-SENSORS-MIB (.1.3.6.1.4.1.2021) включает в себя объекты, предназначенные для получения информации от различных датчиков, которые установлены в оборудовании сетевого узла.

ПО ViPNet использует следующие объекты, для которых возможно только чтение данных:

Таблица 48. SNMP-параметры. LM-SENSORS-MIB

OID	Описание
Таблица температурных датчиков сетевого узла (.1.3.6.1.4.1.2021.13.16.2.1):	
A — индекс температурного датчика	
.1.3.6.1.4.1.2021.13.16.2.1.1.A	Индекс температурного датчика (A).
.1.3.6.1.4.1.2021.13.16.2.1.2.A	Имя температурного датчика.
.1.3.6.1.4.1.2021.13.16.2.1.3.A	Температура (в м°C).
Таблица датчиков скорости вращения вентиляторов (.1.3.6.1.4.1.2021.13.16.3.1):	
B — индекс датчика скорости вращения вентилятора	
.3.6.1.4.1.2021.13.16.3.1.1.B	Индекс датчика скорости вращения вентилятора (B).
.3.6.1.4.1.2021.13.16.3.1.2.B	Имя датчика скорости вращения вентилятора.
.3.6.1.4.1.2021.13.16.3.1.3.B	Скорость вращения вентилятора (в оборотах в минуту). Если вентилятор не подключен, параметр равен 0.

NOTIFICATION-LOG-MIB

NOTIFICATION-LOG-MIB (.1.3.6.1.2.1.92) включает в себя объекты, предназначенные для получения информации о журналах событий. Подробнее см. в RFC 3014.

ПО ViPNet использует следующие объекты, для которых возможно только чтение данных:

Таблица 49. SNMP-параметры. NOTIFICATION-LOG-MIB

OID	Описание
.1.3.6.1.2.1.92.1.1.1.0	Максимальное количество записей, которое может хранить таблица журналов .1.3.6.1.2.1.92.1.3.1.1 (таблица не поддерживается в ViPNet Coordinator HW). Если ограничений нет, параметр равен 0.
.1.3.6.1.2.1.92.1.1.2.0	Время, в течение которого SNMP-агент должен хранить уведомления (в минутах). Если время не ограничено, параметр равен 0.
.1.3.6.1.2.1.92.1.2.1.0	Количество записей в таблице журналов .1.3.6.1.2.1.92.1.3.1.1 (таблица не поддерживается ViPNet Coordinator HW).
.1.3.6.1.2.1.92.1.2.2.0	Количество записей, отброшенных из-за необходимости освобождения места под новые, или по причине превышения значений параметров .1.3.6.1.2.1.92.1.1.1.0 или 1.3.6.1.2.1.92.1.1.3.1.3. Не включает в себя количество записей, удалённых в связи с истечением времени .1.3.6.1.2.1.92.1.1.2.0.

UCD-SNMP-MIB

UCD-SNMP-MIB (.1.3.6.1.4.1.2021) включает в себя объекты, предназначенные для получения информации о характеристиках и состоянии оборудования сетевого узла (например, состояние оперативной памяти и жесткого диска). Подробнее см. на веб-ресурсе.

ПО ViPNet использует следующие объекты, для которых возможно только чтение данных:

Таблица 50. SNMP-параметры. UCD-SNMP-MIB

OID	Описание
.1.3.6.1.4.1.2021.4.1.0	Фиктивный индекс, всегда равен 0.
.1.3.6.1.4.1.2021.4.2.0	Фиктивное имя, всегда равно объему виртуальной памяти.
.1.3.6.1.4.1.2021.4.3.0	Объем виртуальной памяти (swap) на сетевом узле (в кибибайтах).
.1.3.6.1.4.1.2021.4.4.0	Объем доступной виртуальной памяти (в кибибайтах).
.1.3.6.1.4.1.2021.4.5.0	Объем физической памяти (RAM) на сетевом узле (в кибибайтах).
.1.3.6.1.4.1.2021.4.6.0	Объем доступной физической памяти (в кибибайтах).
.1.3.6.1.4.1.2021.4.7.0	Объем виртуальной памяти, выделенный для текстовых страниц (в кибибайтах).
.1.3.6.1.4.1.2021.4.9.0	Объем физической памяти (RAM), выделенный для текстовых страниц (в кибибайтах). Не выводится, если операционная система не выделяет текстовые страницы от других используемых в RAM.
.1.3.6.1.4.1.2021.4.11.0	Общий объем доступной памяти (RAM + swap) (в кибибайтах).
.1.3.6.1.4.1.2021.4.12.0	Минимальный объем свободной виртуальной памяти (в кибибайтах).
.1.3.6.1.4.1.2021.4.13.0	Общий объем памяти (в кибибайтах), выделенный под разделяемую память (shared memory).
.1.3.6.1.4.1.2021.4.14.0	Общий объем памяти (в кибибайтах), который выделен для использования в качестве буфера обмена.
.1.3.6.1.4.1.2021.4.15.0	Общий объем памяти (в кибибайтах), который выделен для использования в качестве кешированной памяти.
.1.3.6.1.4.1.2021.4.16.0	Объем виртуальной памяти, занятый текстовыми страницами (в кибибайтах).
.1.3.6.1.4.1.2021.4.17.0	Объем физической памяти (RAM), занятый текстовыми страницами (в кибибайтах). Не выводится если операционная система не выделяет текстовые страницы от других используемых в RAM.
.1.3.6.1.4.1.2021.4.18.0	Объем виртуальной памяти на сетевом узле (в кибибайтах). 64-битный аналог .1.3.6.1.4.1.2021.4.3.0.

OID	Описание
.1.3.6.1.4.1.2021.4.19.0	Объем доступной виртуальной памяти (в кибибайтах). 64-битный аналог .1.3.6.1.4.1.2021.4.4.0.
.1.3.6.1.4.1.2021.4.20.0	Объем физической памяти на сетевом узле (в кибибайтах). 64-битный аналог .1.3.6.1.4.1.2021.4.5.0.
.1.3.6.1.4.1.2021.4.21.0	Объем свободной физической памяти (в кибибайтах). 64-битный аналог .1.3.6.1.4.1.2021.4.6.0.
.1.3.6.1.4.1.2021.4.22.0	Общий объем доступной памяти (RAM + swap) (в кибибайтах). 64-битный аналог .1.3.6.1.4.1.2021.4.11.0.
.1.3.6.1.4.1.2021.4.23.0	Минимальный объем свободной виртуальной памяти (в кибибайтах). 64-битный аналог .1.3.6.1.4.1.2021.4.12.0.
.1.3.6.1.4.1.2021.4.24.0	Общий объем памяти (в кибибайтах), выделенный под разделяемую память (shared memory). 64-битный аналог .1.3.6.1.4.1.2021.4.13.0.
.1.3.6.1.4.1.2021.4.25.0	Общий объем памяти (в кибибайтах), который выделен для использования в качестве буфера обмена. 64-битный аналог .1.3.6.1.4.1.2021.4.14.0.
.1.3.6.1.4.1.2021.4.26.0	Общий объем памяти (в кибибайтах), который выделен для использования в качестве кешированной памяти. 64-битный аналог .1.3.6.1.4.1.2021.4.15.0.
.1.3.6.1.4.1.2021.4.27.0	Объем доступной памяти (в кибибайтах), доступный для запуска новых приложений без вымещения данных в swap.
.1.3.6.1.4.1.2021.4.100.0	Признак, что объем виртуальной памяти меньше минимально установленного значения.
.1.3.6.1.4.1.2021.4.101.0	Сообщение о том, что доступный объем виртуальной памяти меньше минимально установленного значения.

Таблица сведений о разделах (.1.3.6.1.4.1.2021.9.1)

B — индекс диска, присвоенный сетевым узлом

.1.3.6.1.4.1.2021.9.1.1.B	Индекс раздела (B).
.1.3.6.1.4.1.2021.9.1.2.B	Точка монтирования раздела.
.1.3.6.1.4.1.2021.9.1.3.B	Устройство (или tmpfs), на котором находится раздел.
.1.3.6.1.4.1.2021.9.1.4.B	Минимальный объем свободного места на разделе (в килобайтах) до появления флага ошибки.
.1.3.6.1.4.1.2021.9.1.5.B	Минимальный объем свободного места на разделе (в процентах) от общего до появления флага ошибки.
.1.3.6.1.4.1.2021.9.1.6.B	Общий объём раздела (в килобайтах).
.1.3.6.1.4.1.2021.9.1.7.B	Свободное место в разделе (в килобайтах).
.1.3.6.1.4.1.2021.9.1.8.B	Занятое место в разделе (в килобайтах).
.1.3.6.1.4.1.2021.9.1.9.B	Занятое место в разделе (в процентах).

OID	Описание
.1.3.6.1.4.1.2021.9.1.10.B	Процент использования инодов в разделе.
.1.3.6.1.4.1.2021.9.1.100.B	Флаг ошибки, сигнализирующий о том, что свободного места в разделе осталось меньше заданного значения .1.3.6.1.4.1.2021.9.1.4.B или .1.3.6.1.4.1.2021.9.1.5.B: • 0 — нет ошибки, • 1 — есть ошибка.
.1.3.6.1.4.1.2021.9.1.101.B	Сообщение об ошибке. Если параметр .1.3.6.1.4.1.2021.9.1.10.B равен 0, сообщение пустое.
.1.3.6.1.4.1.2021.9.1.11.B	Общий объем раздела, представленный в формате 64 бит. Параметр равен 1-32 бит числа. Если раздел менее 2ТБайт, параметр равен .1.3.6.1.4.1.2021.9.1.6.B.
.1.3.6.1.4.1.2021.9.1.12.B	Общий объем раздела, представленный в формате 64 бит. Параметр равен 33-64 бит числа. Если раздел менее 2ТБайт, параметр равен 0.
.1.3.6.1.4.1.2021.9.1.13.B	Общий объем свободного места раздела, представленный в формате 64 бит. Параметр равен 1-32 бит числа. Если свободно менее 2ТБайт, параметр равен .1.3.6.1.4.1.2021.9.1.7.B.
.1.3.6.1.4.1.2021.9.1.14.B	Общий объем свободного места раздела, представленный в формате 64 бит. Параметр равен 33-64 бит числа. Если свободно менее 2ТБайт, параметр равен 0.
.1.3.6.1.4.1.2021.9.1.15.B	Общий объем занятого места раздела, представленный в формате 64 бит. Параметр равен 1-32 бит числа. Если занято менее 2ТБайт, параметр равен .1.3.6.1.4.1.2021.9.1.8.B.
.1.3.6.1.4.1.2021.9.1.16.B	Общий объем занятого места раздела, представленный в формате 64 бит. Параметр равен 33-64 бит числа. Если занято менее 2ТБайт, параметр равен 0.

Таблица информации о средней загрузке системы за 1, 5, 15 минут (1.3.6.1.4.1.2021.10.1)

C — индекс, присвоенный сетевым узлом (постоянный):

- **1 — значение для 1 минуты,**
- **2 — значение для 5 минут,**
- **3 — значение для 15 минут**

.1.3.6.1.4.1.2021.10.1.1.C	Индекс значения средней загрузки: • 1 — 1 минута, • 2 — 5 минут, • 3 — 15 минут
.1.3.6.1.4.1.2021.10.1.2.C	Имя загрузки (по умолчанию: Load-1, Load-5, Load-15).
.1.3.6.1.4.1.2021.10.1.3.C	Средняя загрузка системы в процентах (в виде строки).
.1.3.6.1.4.1.2021.10.1.4.C	Пороговое значение загрузки системы в процентах (в виде строки).
.1.3.6.1.4.1.2021.10.1.5.C	Загрузка системы в процентах (в виде целого числа).

OID	Описание
.1.3.6.1.4.1.2021.10.1.6.C	Загрузка системы в процентах (в виде числа с плавающей точкой).
.1.3.6.1.4.1.2021.10.1.100.C	Флаг, сигнализирующий о превышении средней загрузки порогового значения.
.1.3.6.1.4.1.2021.10.1.101.C	Сообщение о превышении порогового значения.
.1.3.6.1.4.1.2021.10.1.0	Фиктивный индекс, всегда равен 1.
.1.3.6.1.4.1.2021.10.2.0	Фиктивное имя, всегда равно systemStats.
.1.3.6.1.4.1.2021.11.3.0	Среднее количество информации (в килобайтах), записанное на диск за минуту.
.1.3.6.1.4.1.2021.11.4.0	Среднее количество информации (в килобайтах), прочитанное с диска за минуту.
.1.3.6.1.4.1.2021.11.5.0	Среднее количество информации (в блоках данных), записанное на диск за минуту.
.1.3.6.1.4.1.2021.11.6.0	Среднее количество информации (в блоках данных), прочитанное с диска за минуту.
.1.3.6.1.4.1.2021.11.7.0	Среднее количество системных прерываний за минуту.
.1.3.6.1.4.1.2021.11.8.0	Среднее количество переключений контекста за минуту.
.1.3.6.1.4.1.2021.11.9.0	Процент времени, занятого пользовательскими процессами (за минуту).
.1.3.6.1.4.1.2021.11.10.0	Процент времени, когда процессор занят системными процессами (за минуту).
.1.3.6.1.4.1.2021.11.11.0	Процент времени, когда процессор не занят процессами (за минуту).
.1.3.6.1.4.1.2021.11.50.0	Количество тиков процессорного времени, затраченного на исполнения user-level code.
.1.3.6.1.4.1.2021.11.51.0	Количество тиков процессорного времени, затраченного на исполнение reduced-priority code.
.1.3.6.1.4.1.2021.11.52.0	Количество тиков процессорного времени, затраченного на исполнение system-level code.
.1.3.6.1.4.1.2021.11.53.0	Количество тиков процессорного времени, проведенного в состоянии idle.
.1.3.6.1.4.1.2021.11.54.0	Количество тиков процессорного времени, затраченного на исполнение ожидания ввода-вывода.
.1.3.6.1.4.1.2021.11.55.0	Количество тиков процессорного времени, затраченного на исполнение kernel-level code.
.1.3.6.1.4.1.2021.11.56.0	Количество тиков процессорного времени, затраченного на исполнение аппаратных прерываний.
.1.3.6.1.4.1.2021.11.57.0	Количество блоков, отправленное блочному устройству (диску).

OID	Описание
.1.3.6.1.4.1.2021.11.58.0	Количество блоков, полученное блочным устройством (диском).
.1.3.6.1.4.1.2021.11.59.0	Количество обработанных аппаратных прерываний.
.1.3.6.1.4.1.2021.11.60.0	Количество выполненных переключений контекста.
.1.3.6.1.4.1.2021.11.61.0	Количество тиков процессорного времени, затраченного на исполнение программных прерываний.
.1.3.6.1.4.1.2021.11.62.0	Количество блоков, помещенных в виртуальную память.
.1.3.6.1.4.1.2021.11.63.0	Количество блоков, извлеченных из виртуальной памяти.
.1.3.6.1.4.1.2021.11.64.0	Количество тиков процессорного времени, затраченного кодом гипервизора (если узел работает в виртуальной среде).
.1.3.6.1.4.1.2021.11.65.0	Количество тиков процессорного времени, затраченного на виртуальные процессоры в гипервизоре.
.1.3.6.1.4.1.2021.11.66.0	Количество тиков процессорного времени, затраченного на виртуальные процессоры в гипервизоре с пониженным приоритетом.
.1.3.6.1.4.1.2021.11.67.0	Количество ядер процессоров.
.1.3.6.1.4.1.2021.100.1.0	Фиктивный индекс, всегда равен 0.
.1.3.6.1.4.1.2021.100.2.0	Ключевое слово CVS.
.1.3.6.1.4.1.2021.100.3.0	Строка времени из ключевого слова RCS.
.1.3.6.1.4.1.2021.100.4.0	Строка времени из ctime.
.1.3.6.1.4.1.2021.100.5.0	Идентификатор из ключевого слова RCS.
.1.3.6.1.4.1.2021.100.6.0	Опции конфигурации SNMP-агента.
.1.3.6.1.4.1.2021.101.1.0	Фиктивный индекс, всегда равен 0.
.1.3.6.1.4.1.2021.101.2.0	Фиктивная строка, всегда равная snmp.
.1.3.6.1.4.1.2021.101.100.0	Признак ошибки SNMP-агента.
.1.3.6.1.4.1.2021.101.101.0	Описание ошибки SNMP-агента.

UCD-DISKIO-MIB

UCD-DISKIO-MIB (.1.3.6.1.4.1.2021.13.15) включает в себя объекты, предназначенные для получения информации о состоянии памяти и дискового пространства сетевого узла. Подробнее см. на веб-ресурсе.

ПО ViPNet использует следующие объекты, для которых возможно только чтение данных:

Таблица 51. SNMP-параметры. UCD-DISKIO-MIB

OID	Описание
Таблица значений текущих параметров оперативной памяти, виртуальной памяти, дискового пространства и их загрузки (.1.3.6.1.4.1.2021.13.15.1.1.)	
A — индекс таблицы	
.1.3.6.1.4.1.2021.13.15.1.1.1.A	Индекс таблицы (A).
.1.3.6.1.4.1.2021.13.15.1.1.2.A	Описание устройства, полученное от ОС. Для координатора принимает значения: ram0-ram15 loop0-loop7 sda, sda1, sda2, sdb1, sdb2, sdb3
.1.3.6.1.4.1.2021.13.15.1.1.3.A	Количество байт, считанных с устройства с момента запуска.
.1.3.6.1.4.1.2021.13.15.1.1.4.A	Количество байт, записанных на устройство с момента запуска.
.1.3.6.1.4.1.2021.13.15.1.1.5.A	Количество операций доступа к устройству на чтение.
.1.3.6.1.4.1.2021.13.15.1.1.6.A	Количество операций доступа к устройству на запись.
.1.3.6.1.4.1.2021.13.15.1.1.9.A	Средняя загрузка устройства за 1 минуту (в процентах).
.1.3.6.1.4.1.2021.13.15.1.1.10.A	Средняя загрузка устройства за 5 минут (в процентах).
.1.3.6.1.4.1.2021.13.15.1.1.11.A	Средняя загрузка устройства за 15 минут (в процентах).
.1.3.6.1.4.1.2021.13.15.1.1.12.A	Количество операций доступа к устройству на чтение. 64-разрядный параметр.
.1.3.6.1.4.1.2021.13.15.1.1.13.A	Количество байт, записанных на устройство с момента запуска. 64-разрядный параметр.
.1.3.6.1.4.1.2021.13.15.1.1.14.A	Время использования диска с момента запуска (в микросекундах).

NET-SNMP-MIB

NET-SNMP-MIB (1.3.6.1.4.1.8072) включает в себя объекты, предназначенные для получения служебной информации о работе SNMP-агента.

ПО ViPNet использует следующие объекты, для которых возможно только чтение данных:

Таблица 52. SNMP-параметры. NET-SNMP-MIB

OID	Описание
Таблица, содержащая все OID, зарегистрированные MIB-модулями в SNMP-агенте (.1.3.6.1.4.1.8072.1.2.1.1):	

OID	Описание
A – имя MIB-модуля	
B – OID MIB-модуля	
C – приоритет MIB-модуля	
.1.3.6.1.4.1.8072.1.2.1.1.4.A.B.C	Имя модуля, который зарегистрировал OID.
.1.3.6.1.4.1.8072.1.2.1.1.5.A.B.C	Биты, означающие режим работы OID.
.1.3.6.1.4.1.8072.1.2.1.1.6.A.B.C	Таймаут для модуля.
Таблица заскриптованных расширений (.1.3.6.1.4.1.8072.1.3.2.2.1):	
D – идентификатор расширения	
.1.3.6.1.4.1.8072.1.3.2.2.1.2.D	Путь к бинарному файлу или скрипту для запуска.
.1.3.6.1.4.1.8072.1.3.2.2.1.3.D	Аргументы для команды.
.1.3.6.1.4.1.8072.1.3.2.2.1.4.D	Стандартные вводные для команды.
.1.3.6.1.4.1.8072.1.3.2.2.1.5.D	Продолжительность времени, в течение которого результат выполнения команды кешируется (секунд).
.1.3.6.1.4.1.8072.1.3.2.2.1.6.D	Механизм запуска команды: • 1 — fork-and-exec, • 2 — run via a sub-shell.
.1.3.6.1.4.1.8072.1.3.2.2.1.7.D	Механизм исполнения команды: • 1 — run-on-read, • 2 — run-on-set, • 3 — run-command.
.1.3.6.1.4.1.8072.1.3.2.2.1.20.D	Тип хранилища: • 1 (other) — другое, • 2 (volatile) — изменяемый, • 3 (nonvolatile) — неизменяемый, • 4 (permanent) — постоянный, • 5 (readOnly) — только для чтения.
.1.3.6.1.4.1.8072.1.3.2.2.1.21.D	Статус строки таблицы: • 1 (active) — строка доступна для использования, • 2 (notInService) — строка недоступна для использования, • 3 (notReady) — отсутствует информация для использования, • 4 (createAndGo) — создание строки и перевод ее в статус active, • 5 (createAndWait) — создание строки и перевод ее в статус notInService, • 6 (destroy) — удаление.

OID	Описание
Таблица результатов выполнения скриптов (.1.3.6.1.4.1.8072.1.3.2.3.1):	
D – идентификатор расширения	
.1.3.6.1.4.1.8072.1.3.2.3.1.1.D	Первая строка в результате запуска команды.
.1.3.6.1.4.1.8072.1.3.2.3.1.2.D	Полный результат запуска команды одной строки.
.1.3.6.1.4.1.8072.1.3.2.3.1.3.D	Количество строк в результате запуска команды.
.1.3.6.1.4.1.8072.1.3.2.3.1.4.D	Значение, возвращенное командой.
Таблица результатов выполнения команды построчно (.1.3.6.1.4.1.8072.1.3.2.4.1):	
D – идентификатор расширения	
E – номер строки (с единицы)	
.1.3.6.1.4.1.8072.1.3.2.4.1.D.E	Единичная строка вывода команды.
.1.3.6.1.4.1.8072.1.5.1.0	Время, на которое кешируется значение OID по умолчанию (в секундах), если оно не задано в параметре .1.3.6.1.4.1.8072.1.5.3.1.2.F.
.1.3.6.1.4.1.8072.1.5.2.0	Статус кеширования: • 1 — включено, • 2 — выключено.
Таблица кешированных OID (.1.3.6.1.4.1.8072.1.5.3.1):	
F – OID, значение которого кешировано	
.1.3.6.1.4.1.8072.1.5.3.1.2.F	Время, на которое кешируется значение OID (в секундах).
.1.3.6.1.4.1.8072.1.5.3.1.3.F	Статус записи: • 1 (enabled) — включена, • 2 (disabled) — выключена, • 3 (empty) — пустая, • 4 (cached) — кешированная, • 5 (expired) — истекла.
1.3.6.1.4.1.8072.1.7.1.1.0	Статус режима debug SNMP-агента: • 1 — включен, • 2 — выключен.
.1.3.6.1.4.1.8072.1.7.1.2.0	Переключатель вывода для debug: • 1 — вывод всех значений, • 2 — фильтрация вывода. Для работы переключателя параметр .1.3.6.1.4.1.8072.1.7.1.1.0 должен быть равен 1.
.1.3.6.1.4.1.8072.1.7.1.3.0	Переключатель вывода сырого дампа пакетов: • 1 — включен, • 2 — выключен.

OID	Описание
Таблица результатов debug (.1.3.6.1.4.1.8072.1.7.1.4.1):	
G – префикс идентификатора	
.1.3.6.1.4.1.8072.1.7.1.4.4.G	Статус строки таблицы: • 1 (active) — строка доступна для использования, • 2 (notInService) — строка недоступна для использования, • 3 (notReady) — отсутствует информация для использования, • 4 (createAndGo) — создание строки и перевод ее в статус active, • 5 (createAndWait) — создание строки и перевод ее в статус notInService, • 6 (destroy) — удаление.
Таблица форм вывода сообщений SNMP-агента (.1.3.6.1.4.1.8072.1.7.2.1.1):	
H – уровень важности событий: **0 – emergency** **1 – alert** **2 – critical** **3 – error** **4 – warning** **5 – notice** **6 – info** **7 – debug**	
I – идентификатор журнала	
.1.3.6.1.4.1.8072.1.7.2.1.1.3.H.I	Форма вывода сообщений для данной строки: • 1 — stdout, • 2 — stderr, • 3 — file, • 4 — syslog, • 5 — callback.
.1.3.6.1.4.1.8072.1.7.2.1.1.4.H.I	Максимальное значение, для которого применима данная строка: • 0 — emergency, • 1 — alert, • 2 — critical, • 3 — error, • 4 — warning, • 5 — notice, • 7 — debug.

OID	Описание
.1.3.6.1.4.1.8072.1.7.2.1.1.5.H.I	Статус строки таблицы: • 1 (active) — строка доступна для использования, • 2 (notInService) — строка недоступна для использования, • 3 (notReady) — отсутствует информация для использования, • 4 (createAndGo) — создание строки и перевод ее в статус active, • 5 (createAndWait) — создание строки и перевод ее в статус notInService, • 6 (destroy) — удаление.
VACM таблица доступа сетевого узла (.1.3.6.1.4.1.8072.1.9.1.1.): **J – имя группы:** **K – префикс контекста доступа** **L – модель безопасности доступа** **M – уровень безопасности доступа** **N – способ аутентификации**	
.1.3.6.1.4.1.8072.1.9.1.1.2.J.K.L.M.N	Механизм выбора совпадений в VACM: • 1 — exact (полное совпадение), • 2 — prefix (совпадает префикс).
.1.3.6.1.4.1.8072.1.9.1.1.3.J.K.L.M.N	Значение секции ViewName.
.1.3.6.1.4.1.8072.1.9.1.1.4.J.K.L.M.N	Тип хранилища: • 1 (other) — другое, • 2 (volatile) — изменяемый, • 3 (nonvolatile) — неизменяемый, • 4 (permanent) — постоянный, • 5 (readOnly) — только для чтения.
.1.3.6.1.4.1.8072.1.9.1.1.5.J.K.L.M.N	Статус строки таблицы: • 1 (active) — строка доступна для использования, • 2 (notInService) — строка недоступна для использования, • 3 (notReady) — отсутствует информация для использования, • 4 (createAndGo) — создание строки и перевод ее в статус active, • 5 (createAndWait) — создание строки и перевод ее в статус notInService, • 6 (destroy) — удаление.

SNMP-MPD-MIB

SNMP-MPD-MIB (.1.3.6.1.6.3.11) включает в себя статистическую информацию об SNMP-пакетах.

ПО ViPNet использует следующие объекты, для которых возможно только чтение данных:

Таблица 53. SNMP-параметры. SNMP-MPD-MIB

OID	Описание
.1.3.6.1.6.3.11.2.1.1.0	Количество полученных SNMP-пакетов, заблокированных по причине неподдерживаемой или неизвестной модели безопасности.
.1.3.6.1.6.3.11.2.1.2.0	Количество полученных SNMP-пакетов, заблокированных по причине ошибок в SNMP-сообщении.
.1.3.6.1.6.3.11.2.1.3.0	Количество полученных SNMP-пакетов, заблокированных по причине несоответствия pduType.

SNMP-TARGET-MIB

SNMP-TARGET-MIB (.1.3.6.1.6.3.12) включает в себя статистическую информацию об SNMP-пакетах.

ПО ViPNet использует следующие объекты, для которых возможно только чтение данных:

Таблица 54. SNMP-параметры. SNMP-TARGET-MIB

OID	Описание
.1.3.6.1.6.3.12.1.1.0	Параметр для совместной работы нескольких SNMP-менеджеров, для одновременной работы с таблицами данного MIB.
.1.3.6.1.6.3.12.1.4.0	Количество полученных SNMP-пакетов, заблокированных по причине недоступного контекста.
.1.3.6.1.6.3.12.1.5.0	Количество полученных SNMP-пакетов, заблокированных по причине неизвестного контекста.

SNMP-USER-BASED-SM-MIB

SNMP-USER-BASED-SM-MIB (.1.3.6.1.6.3.15) включает в себя объекты, предназначенные для получения информации о параметрах и событиях безопасности SNMP-агента.

ПО ViPNet использует следующие объекты, для которых возможно только чтение данных:

Таблица 55. SNMP-параметры. SNMP-USER-BASED-SM-MIB

OID	Описание
.1.3.6.1.6.3.15.1.1.1.0	Количество заблокированных SNMP-пакетов по причине запроса неизвестного или недоступного уровня безопасности.
.1.3.6.1.6.3.15.1.1.2.0	Количество заблокированных SNMP-пакетов по причине появления вне определённого (доверенного) SNMP-агентом окна.
.1.3.6.1.6.3.15.1.1.3.0	Количество заблокированных SNMP-пакетов по причине использования неизвестного SNMP-агенту имени пользователя.
.1.3.6.1.6.3.15.1.1.4.0	Количество заблокированных SNMP-пакетов по причине обращения к неизвестному SNMP-агенту snmpEngineID.
.1.3.6.1.6.3.15.1.1.5.0	Количество заблокированных SNMP-пакетов по причине отсутствия ожидаемого значения digest value.
.1.3.6.1.6.3.15.1.1.6.0	Количество заблокированных SNMP-пакетов по причине невозможности их расшифровки.
.1.3.6.1.6.3.15.1.2.1.0	Параметр для совместной работы нескольких SNMP-менеджеров с таблицей .1.3.6.1.6.3.15.1.2.2.1.
Таблица параметров безопасности пользователя (.1.3.6.1.6.3.15.1.2.2.1):	
A – EngineID пользователя	
B – имя пользователя	
.1.3.6.1.6.3.15.1.2.2.1.3.A.B	Имя пользователя в формате модели безопасности.
.1.3.6.1.6.3.15.1.2.2.1.4.A.B	Ссылка на другую строку таблицы, в которой создана копия пользователя из текущей строки.
.1.3.6.1.6.3.15.1.2.2.1.5.A.B	Тип протокола аутентификации пользователя.
.1.3.6.1.6.3.15.1.2.2.1.8.A.B	Тип протокола конфиденциальности пользователя.
.1.3.6.1.6.3.15.1.2.2.1.11.A.B	Параметр для определения факта смены ключей пользователя.
.1.3.6.1.6.3.15.1.2.2.1.12.A.B	Тип хранилища: • 1 (other) — другое, • 2 (volatile) — изменяемый, • 3 (nonvolatile) — неизменяемый, • 4 (permanent) — постоянный, • 5 (readOnly) — только для чтения.

OID	Описание
.1.3.6.1.6.3.15.1.2.2.1.13.A.B	Статус строки таблицы: • 1 (active) — строка доступна для использования, • 2 (notInService) — строка недоступна для использования, • 3 (notReady) — отсутствует информация для использования, • 4 (createAndGo) — создание строки и перевод ее в статус active, • 5 (createAndWait) — создание строки и перевод ее в статус notInService, • 6 (destroy) — удаление.

SNMP-VIEW-BASED-ACM-MIB

SNMP-VIEW-BASED-ACM-MIB (.1.3.6.1.6.3.16) включает в себя объекты, предназначенные для получения информации о правах доступа к SNMP-параметрам.

ПО ViPNet использует следующие объекты, для которых возможно только чтение данных:

Таблица 56. SNMP-параметры. SNMP-VIEW-BASED-ACM-MIB

OID	Описание
Таблица доступных контекстов сетевого узла (.1.3.6.1.6.3.16.1.1): **A – строка контекста**	
.1.3.6.1.6.3.16.1.1.1.A	Строка контекста.
Таблица групп доступа (.1.3.6.1.6.3.16.1.2.1): **B – модель безопасности** **C – имя безопасности**	
.1.3.6.1.6.3.16.1.2.1.3.B.C	Имя группы
.1.3.6.1.6.3.16.1.2.1.4.B.C	Тип хранилища: • 1 (other) — другое, • 2 (volatile) — изменяемый, • 3 (nonvolatile) — неизменяемый, • 4 (permanent) — постоянный, • 5 (readOnly) — только для чтения.

OID	Описание
.1.3.6.1.6.3.16.1.2.1.5.B.C	Статус строки таблицы: • 1 (active) — строка доступна для использования, • 2 (notInService) — строка недоступна для использования, • 3 (notReady) — отсутствует информация для использования, • 4 (createAndGo) — создание строки и перевод ее в статус active, • 5 (createAndWait) — создание строки и перевод ее в статус notInService, • 6 (destroy) — удаление.
Таблица прав доступа к группам (.1.3.6.1.6.3.16.1.4.1): **D – имя группы** **E – контекст доступа** **F – модель безопасности** **G – уровень безопасности**	
.1.3.6.1.6.3.16.1.4.1.4.D.E.F.G	Формат совпадения: • 1 (exact) — полное совпадение, • 2 (prefix) — совпадает префикс.
.1.3.6.1.6.3.16.1.4.1.5.D.E.F.G	Имя view на просмотр.
.1.3.6.1.6.3.16.1.4.1.6.D.E.F.G	Имя view на запись.
.1.3.6.1.6.3.16.1.4.1.7.D.E.F.G	Имя view для уведомлений.
.1.3.6.1.6.3.16.1.4.1.8.D.E.F.G	Тип хранилища: • 1 (other) — другое, • 2 (volatile) — изменяемый, • 3 (nonvolatile) — неизменяемый, • 4 (permanent) — постоянный, • 5 (readOnly) — только для чтения.
.1.3.6.1.6.3.16.1.4.1.9.D.E.F.G	Статус строки таблицы: • 1 (active) — строка доступна для использования, • 2 (notInService) — строка недоступна для использования, • 3 (notReady) — отсутствует информация для использования, • 4 (createAndGo) — создание строки и перевод ее в статус active, • 5 (createAndWait) — создание строки и перевод ее в статус notInService, • 6 (destroy) — удаление.
.1.3.6.1.6.3.16.1.5.1.0	Параметр для совместной работы нескольких SNMP-менеджеров с таблицами данного MIB.

OID	Описание
Таблица с параметрами view для семей поддеревьев (.1.3.6.1.6.3.16.1.5.2.1.): **H – имя view** **I – поддерево**	
.1.3.6.1.6.3.16.1.5.2.1.3.H.I	Маска, заданная для view.
.1.3.6.1.6.3.16.1.5.2.1.4.H.I	Тип view: • 1 — included, • 2 — excluded.
.1.3.6.1.6.3.16.1.5.2.1.5.H.I	Тип хранилища: • 1 (other) — другое, • 2 (volatile) — изменяемый, • 3 (nonvolatile) — неизменяемый, • 4 (permanent) — постоянный, • 5 (readOnly) — только для чтения.
.1.3.6.1.6.3.16.1.5.2.1.6.H.I	Статус строки таблицы: • 1 (active) — строка доступна для использования, • 2 (notInService) — строка недоступна для использования, • 3 (notReady) — отсутствует информация для использования, • 4 (createAndGo) — создание строки и перевод ее в статус active, • 5 (createAndWait) — создание строки и перевод ее в статус notInService, • 6 (destroy) — удаление.

SNMP-FRAMEWORK-MIB

SNMP-FRAMEWORK-MIB (.1.3.6.1.6.3.10) включает в себя объекты, предназначенные для получения служебной информации о работе SNMP-агента. Подробнее см. на веб-ресурсе.

ПО ViPNet использует следующие объекты, для которых возможно только чтение данных:

Таблица 57. SNMP-параметры. SNMP-FRAMEWORK-MIB

OID	Описание
.1.3.6.1.6.3.10.2.1.1.0	Идентификатор SNMP-engine.
.1.3.6.1.6.3.10.2.1.2.0	Количество инициализаций SNMP-engine после создания идентификатора.
.1.3.6.1.6.3.10.2.1.3.0	Время, прошедшее с последнего изменения количества инициализаций SNMP-engine (в секундах).

OID	Описание
.1.3.6.1.6.3.10.2.1.4.0	Максимальная длина входящего и исходящего SNMP-сообщения (в байтах).

VIPNET-MIB

VIPNET-MIB (.1.3.6.1.4.1.10812) включает в себя объекты, предназначенные для получения информации о параметрах сетевых узлов ViPNet. Для получения этой информации используется ветвь: `.iso.org.dod.internet.private.enterprises.infotecs.vipnet` (.1.3.6.1.4.1.10812.1).

ПО ViPNet использует следующие объекты, для которых возможно только чтение данных:

Таблица 58. SNMP-параметры. VIPNET-MIB

OID	Описание
.1.3.6.1.4.1.10812.1.1.1.0	Шестнадцатеричный идентификатор сети ViPNet.
.1.3.6.1.4.1.10812.1.1.2.0	Шестнадцатеричный идентификатор сетевого узла ViPNet.
.1.3.6.1.4.1.10812.1.1.3.0	Имя пользователя узла ViPNet.
.1.3.6.1.4.1.10812.1.1.4.0	Время работы ViPNet Coordinator HW (сбрасывается каждый раз при перезапуске службы iplircfg).
.1.3.6.1.4.1.10812.1.1.5.0	Шестнадцатеричный идентификатор, включающий в себя идентификаторы узла ViPNet и сети ViPNet.
.1.3.6.1.4.1.10812.1.1.7.0	Имя узла ViPNet.
.1.3.6.1.4.1.10812.1.2.1	Количество сетевых интерфейсов.
Таблица объектов, описывающих сетевые интерфейсы (.1.3.6.1.4.1.10812.1.2.2):	
.1.3.6.1.4.1.10812.1.2.2.1.1.X	Номер сетевого интерфейса X , где X — индекс интерфейса.
.1.3.6.1.4.1.10812.1.2.2.1.2.X	Имя сетевого интерфейса X.
.1.3.6.1.4.1.10812.1.2.2.1.3.X	Устаревший параметр, всегда равен 0.
.1.3.6.1.4.1.10812.1.2.2.1.4.X	Количество пропущенных входящих незашифрованных пакетов.
.1.3.6.1.4.1.10812.1.2.2.1.5.X	Количество блокированных входящих незашифрованных пакетов.
.1.3.6.1.4.1.10812.1.2.2.1.6.X	Количество пропущенных исходящих незашифрованных пакетов.
.1.3.6.1.4.1.10812.1.2.2.1.7.X	Количество блокированных исходящих незашифрованных пакетов.
.1.3.6.1.4.1.10812.1.2.2.1.8.X	Количество пропущенных входящих зашифрованных пакетов.
.1.3.6.1.4.1.10812.1.2.2.1.9.X	Количество блокированных входящих зашифрованных пакетов.
.1.3.6.1.4.1.10812.1.2.2.1.10.X	Количество пропущенных исходящих зашифрованных пакетов.
.1.3.6.1.4.1.10812.1.2.2.1.11.X	Количество блокированных исходящих зашифрованных пакетов.

OID	Описание
Таблица объектов, описывающих состояние служб iplircfg, failoverd, mftpd, webgui-fcgi-server, remote_management (.1.3.6.1.4.1.10812.1.7.1):	
.1.3.6.1.4.1.10812.1.7.1.1.2.Y	Индекс службы с индексом Y: • 1 — failoverd, • 2 — iplircfg, • 3 — mftpd, • 4 — webgui-fcgi-server, • 5 — external-controld.
.1.3.6.1.4.1.10812.1.7.1.1.3.Y	Состояние службы с индексом Y: • 0 (unknown) — состояние неизвестно, • 1 (shutdown) — работа службы завершена, • 2 (running) — служба работает.
.1.3.6.1.4.1.10812.1.7.1.1.4.Y	Время работы службы с индексом Y.
.1.3.6.1.4.1.10812.1.8.1.0	Режим работы службы failoverd: • 0 (single) — одиночный, • 1 (cluster passive) — режим кластера, узел работает в пассивном режиме, • 2 (cluster active) — режим кластера, узел работает в активном режиме, • 3 (cluster switch) — режим кластера, узел меняет режим работы в текущий момент.
.1.3.6.1.4.1.10812.1.8.2.0	Время последнего переключения службы failover в текущий режим работы.
.1.3.6.1.4.1.10812.1.8.3.0	IP-адрес интерфейса синхронизации другого узла кластера.
.1.3.6.1.4.1.10812.1.8.4.0	Количество сетевых соединений, находящихся в кеше узла кластера.
.1.3.6.1.4.1.10812.1.8.5.0	Системное имя интерфейса синхронизации.
Таблица доступности соединений в канале между узлами кластера (.1.3.6.1.4.1.10812.1.8.6): **X – индекс таблицы**	
.1.3.6.1.4.1.10812.1.8.6.1.1.X	Индекс таблицы.
.1.3.6.1.4.1.10812.1.8.6.1.2.X	IP-адрес интерфейса синхронизации.
.1.3.6.1.4.1.10812.1.8.6.1.3.X	Статус доступности узла: • 1 — доступен, • 2 — недоступен.
Таблица сведений о ViPNet Coordinator HW (.1.3.6.1.4.1.10812.1.10.1):	
.1.3.6.1.4.1.10812.1.10.1.1.1.X	Индекс строки.
.1.3.6.1.4.1.10812.1.10.1.1.2.X	Serial number — имя параметра.

OID	Описание
.1.3.6.1.4.1.10812.1.10.1.1.3.X	Значение параметра Serial number.

SNMP-агент ViPNet Coordinator HW может отправлять уведомления:

Таблица 59. SNMP-уведомления. VIPNET-MIB

OID	Описание
.1.3.6.1.4.1.10812.1.0.1	Запуск службы iplircfg.
.1.3.6.1.4.1.10812.1.0.2	Остановка службы iplircfg.
.1.3.6.1.4.1.10812.1.0.3	Запуск службы mftpd.
.1.3.6.1.4.1.10812.1.0.4	Остановка службы mftpd.
.1.3.6.1.4.1.10812.1.0.7	Запуск службы failoverd.
.1.3.6.1.4.1.10812.1.0.8	Остановка службы failoverd.
.1.3.6.1.4.1.10812.1.0.9	Переключение службы failoverd из пассивного режима в активный.
.1.3.6.1.4.1.10812.1.0.10	Запуск службы webgui.
.1.3.6.1.4.1.10812.1.0.11	Остановка службы webgui.
.1.3.6.1.4.1.10812.1.0.12	Потеря связи с пассивным узлом кластера.
.1.3.6.1.4.1.10812.1.0.13	Восстановление связи с пассивным узлом кластера.
.1.3.6.1.4.1.10812.1.0.14	Запуск службы external-controld.
.1.3.6.1.4.1.10812.1.0.15	Остановка службы external-controld.

VIPNETHW-MIB

VIPNETHW-MIB (.1.3.6.1.4.1.10812.13) включает в себя объекты, предназначенные для получения информации о службе внешнего управления remote_management. Для получения этой информации используется ветвь:
`.iso.org.dod.internet.private.enterprises.infotecs.infvipnetPolicy` (.1.3.6.1.4.1.10812.13).

ПО ViPNet использует следующие объекты, для которых возможно только чтение данных:

Таблица 60. SNMP-параметры. VIPNETHW-MIB

OID	Описание
.1.3.6.1.4.1.10812.13.1	Последовательность объектов, описывающих политики в очереди.
.1.3.6.1.4.1.10812.13.1.1	Объекты, описывающие политики.
.1.3.6.1.4.1.10812.13.1.1.1.X	SNMP-индекс политики.

.1.3.6.1.4.1.10812.13.1.1.2.X	Тип политики: • Software; • License; • Firewall; • VPN; • DPI; • Services.
.1.3.6.1.4.1.10812.13.1.1.3.X	Время формирования политики в ViPNet Prime.
.1.3.6.1.4.1.10812.13.1.1.4.X	Время планового применения политики.

VIPNETFWLOAD-MIB

VIPNETFWLOAD-MIB (.1.3.6.1.4.1.10812.16) содержит объекты, предназначенные для мониторинга нагрузки ViPNet Coordinator HW.

SNMP-агент ViPNet Coordinator HW может отправлять оповещения типа TRAP:

Таблица 61. SNMP-оповещения. VIPNETFWLOAD-MIB

OID	Описание
.1.3.6.1.4.1.10812.16.0.1	Нагрузка на ЦП — повышенная
.1.3.6.1.4.1.10812.16.0.2	Нагрузка на ЦП — критическая
.1.3.6.1.4.1.10812.16.0.3	Нагрузка на ЦП — норма
.1.3.6.1.4.1.10812.16.0.4	Использование ОП — повышенное
.1.3.6.1.4.1.10812.16.0.5	Использование ОП — критическое
.1.3.6.1.4.1.10812.16.0.6	Использование ОП — норма
.1.3.6.1.4.1.10812.16.0.7	Количество активных сессий — повышенное
.1.3.6.1.4.1.10812.16.0.8	Количество активных сессий — критическое
.1.3.6.1.4.1.10812.16.0.9	Количество активных сессий — норма
.1.3.6.1.4.1.10812.16.0.10	Количество новых сессий в секунду — повышенное
.1.3.6.1.4.1.10812.16.0.11	Количество новых сессий в секунду — критическое
.1.3.6.1.4.1.10812.16.0.12	Количество новых сессий в секунду — норма
.1.3.6.1.4.1.10812.16.0.13	Количество IP-пакетов в секунду — повышенное
.1.3.6.1.4.1.10812.16.0.14	Количество IP-пакетов в секунду — критическое
.1.3.6.1.4.1.10812.16.0.15	Количество IP-пакетов в секунду — норма

OID	Описание
.1.3.6.1.4.1.10812.16.0.16	Объем трафика через МЭ — повышенный
.1.3.6.1.4.1.10812.16.0.17	Объем трафика через МЭ — критический
.1.3.6.1.4.1.10812.16.0.18	Объем трафика через МЭ — норма
.1.3.6.1.4.1.10812.16.0.19	Отношение объема трафика через МЭ к количеству IP-пакетов в секунду — повышенное
.1.3.6.1.4.1.10812.16.0.20	Отношение объема трафика через МЭ к количеству IP-пакетов в секунду — критическое
.1.3.6.1.4.1.10812.16.0.21	Отношение объема трафика через МЭ к количеству IP-пакетов в секунду — норма
.1.3.6.1.4.1.10812.16.0.22	Количество SYN-запросов TCP в секунду — повышенное
.1.3.6.1.4.1.10812.16.0.23	Количество SYN-запросов TCP в секунду — критическое
.1.3.6.1.4.1.10812.16.0.24	Количество SYN-запросов TCP в секунду — норма
.1.3.6.1.4.1.10812.16.0.25	Количество ICMP-запросов — повышенное
.1.3.6.1.4.1.10812.16.0.26	Количество ICMP-запросов — критическое
.1.3.6.1.4.1.10812.16.0.27	Количество ICMP-запросов — норма
.1.3.6.1.4.1.10812.16.0.28	Количество UDP-соединений со статусом UNREPLIED — повышенное
.1.3.6.1.4.1.10812.16.0.29	Количество UDP-соединений со статусом UNREPLIED — критическое
.1.3.6.1.4.1.10812.16.0.30	Количество UDP-соединений со статусом UNREPLIED — норма
.1.3.6.1.4.1.10812.16.0.31	Количество ошибок приема/передачи IP-пакетов — повышенное
.1.3.6.1.4.1.10812.16.0.32	Количество ошибок приема/передачи IP-пакетов — критическое
.1.3.6.1.4.1.10812.16.0.33	Количество ошибок приема/передачи IP-пакетов — норма
.1.3.6.1.4.1.10812.16.0.34	Количество отброшенных IP-пакетов — повышенное
.1.3.6.1.4.1.10812.16.0.35	Количество отброшенных IP-пакетов — критическое
.1.3.6.1.4.1.10812.16.0.36	Количество отброшенных IP-пакетов — норма
.1.3.6.1.4.1.10812.16.0.37	Нагрузка на HDD/SSD —повышенная
.1.3.6.1.4.1.10812.16.0.38	Нагрузка на HDD/SSD —критическая
.1.3.6.1.4.1.10812.16.0.39	Нагрузка на HDD/SSD —норма
.1.3.6.1.4.1.10812.16.0.40	Средняя нагрузка на ЦП (loadavg) — повышенная
.1.3.6.1.4.1.10812.16.0.41	Средняя нагрузка на ЦП (loadavg) — критическая
.1.3.6.1.4.1.10812.16.0.42	Средняя нагрузка на ЦП (loadavg) — норма
.1.3.6.1.4.1.10812.16.0.43	Загрузка свободной ОП — повышенная
.1.3.6.1.4.1.10812.16.0.44	Загрузка свободной ОП — критическая

OID	Описание
.1.3.6.1.4.1.10812.16.0.45	Загрузка свободной ОП — норма
.1.3.6.1.4.1.10812.16.0.46	Уровень доступной ОП — повышенный
.1.3.6.1.4.1.10812.16.0.47	Уровень доступной ОП — критический
.1.3.6.1.4.1.10812.16.0.48	Уровень доступной ОП — норма
.1.3.6.1.4.1.10812.16.0.52	Обнаружен источник повышенной сетевой нагрузки

VIPNETVPN-MIB

VIPNETVPN-MIB (.1.3.6.1.4.1.10812.90) включает в себя объекты, предназначенные для получения информации о доступности связанных узлов ViPNet.

ПО ViPNet использует следующие объекты, для которых возможно только чтение данных:

Таблица 62. SNMP-параметры. VIPNETVPN-MIB

OID	Описание
Таблица узлов ViPNet, связанных с ViPNet Coordinator HW (.1.3.6.1.4.1.10812.90.1): **X — номер сетевого узла в таблице**	
.1.3.6.1.4.1.10812.90.1.1.2.X	Имя узла
.1.3.6.1.4.1.10812.90.1.1.3.X	Идентификатор узла в сети ViPNet
.1.3.6.1.4.1.10812.90.1.1.4.X	Статус доступности узла: • 0 — узел недоступен; • 1 — узел доступен

SNMP-агент ViPNet Coordinator HW может отправлять уведомления:

Таблица 63. SNMP-уведомления. VIPNETVPN-MIB

OID	Описание
.1.3.6.1.4.1.10812.90.0.1	Узел ViPNet недоступен
.1.3.6.1.4.1.10812.90.0.2	Узел ViPNet доступен

MonitoringAgent-MIB

MonitoringAgent-MIB (.1.3.6.1.4.1.10812.4) включает в себя объекты, предназначенные для получения информации о характеристиках SNMP-агента (например, версия, уникальный идентификатор).

ПО ViPNet использует следующие объекты, для которых возможно только чтение данных:

Таблица 64. SNMP-параметры. MonitoringAgent-MIB

OID	Описание
.1.3.6.1.4.1.10812.4.3.1.0	Версия агента мониторинга.
.1.3.6.1.4.1.10812.4.3.2.0	Идентификатор инсталляции агента мониторинга.
.1.3.6.1.4.1.10812.4.4	Таблица плагинов агента мониторинга.
.1.3.6.1.4.1.10812.4.5	Таблица функциональных возможностей агента мониторинга.

System-MonitoringAgent-MIB

System-MonitoringAgent-MIB (.1.3.6.1.4.1.10812.4.20) включает в себя объекты, предназначенные для получения информации об устройстве, на котором запущен SNMP-агент.

ПО ViPNet использует следующие объекты, для которых возможно только чтение данных:

Таблица 65. SNMP-параметры. System-MonitoringAgent-MIB

OID	Описание
.1.3.6.1.4.1.10812.4.20.5.0	Идентификатор устройства в HEX-формате.
.1.3.6.1.4.1.10812.4.20.9.0	Уникальный идентификатор устройства в виде строки.

H

Службы ПО ViPNet Coordinator HW

Службы ViPNet:

- `aad` — скрипт управления службой аутентификации и авторизации;
- `bonding` — скрипт управления модулем агрегирования сетевых интерфейсов;
- `conntrackd_tracker` — служба синхронизации сессий межсетевого экрана;
- `itcs_controld` — служба обработки запросов;
- `dgd` — скрипт управления службой `dgdd`;
- `drviplir` — драйвер перехвата сетевого трафика;
- `frr` — скрипт управления службой динамической маршрутизации `zebra`;
- `itcs-external-controld` — служба взаимодействия с ViPNet Prime;
- `failover` — скрипт управления службой `failoverd`;
- `failoverd` — служба системы защиты от сбоев;
- `healthmond` — служба мониторинга нагрузки;
- `l2overip` — драйвер прозрачного соединения сегментов сети на уровне L2;
- `iplircfg` — служба настройки драйвера перехвата сетевого трафика, ведения журнала IP-пакетов, обновления справочно-ключевой информации;
- `iplirpasswd` — утилита проверки паролей аудитора и администратора;
- `itcscrpt` — драйвер шифрования IP-пакетов;
- `itcskrniface` — драйвер перехвата сетевого трафика;
- `itcswd` — драйвер службы мониторинга системы;

- `mftp` — скрипт управления службой `mftpd`;
- `mftpd` — служба транспортного сервера MFTP;
- `network_journald` — служба работы с журналами IP-пакетов и сессий;
- `ntp_service` — скрипт управления службой NTP;
- `rvpn_shell` — командный интерпретатор ViPNet;
- `session_watcher` — служба, отслеживающая сессии пользователей ViPNet;
- `uc` — служба идентификации пользователей сети;
- `unmerge` — утилита распаковки дистрибутива справочников и ключей;
- `urlcatd` — служба управления URL-категориями;
- `vipnetsnmp` — служба SNMP;
- `vupgrade` — утилита обновления ПО ViPNet Coordinator HW;
- `webgui` (`webgui_captive_portal`, `webgui-fcgi-server`, `webgui_php`, `webgui_frontend`) — служба веб-интерфейса.

Службы Linux:

- `acpid` — служба обработки ACPI-событий;
- `crond` — служба запуска задач по расписанию;
- `conntrackd` — служба работы с сессиями межсетевого экрана;
- `dgdd` — служба проверки состояния удаленных шлюзов (DGD);
- `dhcpd` — служба DHCP-сервера;
- `dhcrelay` — служба агента-ретранслятора DHCP-запросов;
- `icap` — служба работы с ICAP-серверами;
- `licd` — служба лицензирования;
- `login` — служба аутентификации и открытия сессий;
- `named` — служба DNS;
- `ntpd` — служба NTP;
- `pcscd` — служба работы с токенами;
- `pppd` — службы управления соединениями точка-точка (только в исполнениях HW50 и HW100);
- `snmpd` — служба SNMP;
- `snort` — служба IPS/DPI;
- `sshd` — служба SSH;
- `sslsplit` — служба SSL/TLS-инспекции;
- `syslogd` — служба системного журнала;
- `ospfd` — служба OSPF-маршрутизации;

- `udhcpc` — служба DHCP-клиента;
- `upslog`, `upssched` — службы мониторинга и управления ИБП;
- `watchfrr` — служба управления службой динамической маршрутизации `frr`;
- `watchquagga` — служба управления службой динамической маршрутизации `quagga`;
- `vmunix` — ядро Linux;
- `xinetd` — служба запуска сетевых серверных процессов;
- `zebra` — динамической маршрутизации;
- `zdhcpd` — служба протокола DHCP для динамической маршрутизации.

Поддерживаемые приложения

Эти приложения вы можете указать в параметре `dpiapp <название приложения>` транзитного фильтра.

1 - 9

123VPN, 1kxun

A

AccuWeather, Activision Blizzard, AdobeConnect, Adult Content, Advertisement, Analytics and Tracking, AI Search, AirBnB, Akamai Cloud, Alibaba, AliExpress, AliPay, Amazon, Amazon Alexa, Amazon API Gateway, Amazon Cloud, Amazon Cloudfront, Amazon EC2, Amazon Prime Video, Amazon S3, Among Us, Ankama, AnyDesk, APNS, Apple Music, Apple Services, Apple Siri, Apple TV, Apteka.ru, Atlassian, Avast DNS, Avira Phantom VPN, Avito

B

Badoo, Blacknut, Bloomberg, Bluesky, Boosteroid, Brightcove, Browsec VPN, Bumble

C

CacheFly, CactusVPN, Canonical, CDNetworks, CDNvideo, Channel One, character.ai, ChatGPT, Citilink, Citrix, Claude, ClickHouse, Cloud Mail / VK WorkDisk, Cloudera Platform, Cloudflare, Cloudflare WARP, Cloudinary, CNN, CopyMonkey, Crashlytics, Criteo, CrossFire, Cybersec

D

Dailymotion, DashScope, DataSaver, DAZN, DeepSeek, Deezer, DigitalOcean, DingTalk, DirecTV, Discord, Disney Plus, DNS Shop, DNSCrypt, DoH/DoT, Dota 2, DotVPN, Dropbox

E

EA Games, eBay, Edgecast CDN, Elastic Search Cloud, Epic Games, Erstream, ESPN, ETM, Evernote

F

Facebook, Facebook Reels and Stories, Facebook VoIP, Fastly, Fortinet, FusionBrain, Fuze Meeting

G

GearUp Booster, Gemini, Genprokuratura, Gerwin, GigaChat, GigaCode, GitHub, GitLab, Gold Apple, Google, Google AI Studio, Google Analytics, Google Chat, Google Classroom, Google Cloud, Google Docs, Google Drive, Google Mail, Google Maps, Google Meet, Google Photos, Google Play, Google Shared Services, Google Trust Services, GoToMeeting, Guild Wars 2

H

HBO Now, Huawei Mobile Cloud, Huawei Services, Hugging Face, Hulu

I

iCloud, iFlix, iHeartRadio, Instagram, iOS App Store, Iqiyi, iTunes, Ivi-Ru

J

Jasper, Joom

K

Kakaotalk, Kaspersky Services, KeyCDN, Kick, Kinopoisk, Kontur Talk, Kuper

L

LagoFast, Lamoda, Last-fm, Leonardo.Ai, Life-Ru, Line, LinkedIn, LitRes-Ru, Livestream, LoL Wild Rift, Lumen Technologies, Lustre

M

M.Video-Eldorado, Maestro, Magnit Market, Mail-Ru, Mastodon, MAX, MCHS, MediaNova CDN, Megamarket, Messenger, Meta AI, Microsoft Azure, Microsoft Outlook, Microsoft Services, Microsoft Teams, MidJourney, Minimax Chat, Mining, mos.ru, Mozilla, MTS Link, MTS Services, MTS TV, Mudfish, Mullvad VPN, Mumble, MyOffice

N

Naver, NBC News, NBC Sports, Nest, NetEase Games, NetFlix, Nexon, NGenix, Nintendo Network, NoMachine, NordVPN, NotebookLM, Notion, Ntop, Nvidia GeForce NOW, Nvidia Services

O

OCS, Odnoklassniki, Office 365, Ollama, OneDrive, Ookla, OpenAI, OpenDNS, Opera VPN, Oracle Cloud Infrastructure (OCI), Oracle Services, Ozon

P

Paltalk, Pandora, Paramount Plus, Pastebin, Path of Exile, Pay-Rw, Perplexity, Petrovich, Pinterest, PlayStation Network, Pluralsight, Pochta Rossii, POPS, Private Internet Access, Proton VPN

Q

QQ, Qwen Chat

R

Rackspace Cloud, Radmin, reddit, Roblox, RoboGPT, Rockstar Games, Rudalle, Rumble, RUTUBE

S

Salesforce, Samokat, Samsung Max Privacy VPN, SberDisk, SecureVPN, SecureVPN-Pro, Shedevrum, Shein, Showtime, Signal, Signal VoIP, Sima-Land, Sina, Sina Weibo, SiriusXM, Slack, SMTPS, Snapchat, Snapchat Call, SoftEther, Sonos, SoundCloud, Speakchat, Spotify, Stability AI, Steam, Surfshark

T

Tailscale, Taobao, TeamViewer, Telegram, Temu, Tencent, Tencent Games, Tencent Video, Tesla Services, The Elder Scrolls Online, Threads, Tidal, TikTok, TOR, TrueConf Online, Tumblr, TuneIn Radio, TunnelBear, TurboText, Twitch

U

Ubiquity, unknown

V

Viber, Vimeo, ViPNet, Visper, Vivox, VK, VK Messenger, VK Teams, VK Video, VkusVill, Vse Instrumenty, Vudu

W

Wangsu CDN, Waze, Webex, WeChat, WhatsApp, WhatsApp Call, WhatsApp Files, Wikipedia, Wildberries, Windows Update, Windscribe, World of Warcraft

X

X (Twitter), X5 Services, XBOX, Xiaomi Services

Y

Yahoo Services, Yandex Alice, Yandex Browser Telemetry, Yandex Cloud, Yandex Direct, Yandex Disk, Yandex Docs, Yandex Eda-Delivery, Yandex Foundation Models, Yandex Lavka, Yandex Mail, Yandex Market, Yandex Messenger, Yandex Metrika, Yandex Music, Yandex Services, Yandex Telemost, Yandex Tracker, Youla, YouTube, YouTube Upload

Z

Zattoo, ZOOGVPN, Zoom

J

Поддерживаемые прикладные протоколы

Эти протоколы вы можете указать в параметре `dpiprotocol <название протокола>` транзитного фильтра.

A

AFP, Agora, AH IPSec, AliCloud Server, AMQP, Apache JServ, Apache Kafka, Armagetron, ATG, Avast Services

B

BACNET, Beckhoff ADS, BFCP, BFD, BGP, Bitcoin, BitTorrent, BJNP

C

Call of Duty Mobile, CAN, CAPWAP, Cassandra, Ceph, Check_MK, CNP over IP, CoAP, Collectd, Common Industrial Protocol, Corba, CPHA, CryNetwork

D

DCE RPC, DHCP, DHCPv6, Diameter, DICOM, DLEP, DNP3, DNS, DRDA, DTLS

E

EAQ, EasyWeather, eDonkey, EGD, EGP, Elasticsearch, ERSPAN, ESP IPSec, Ether-S-Bus, Ethereum, EtherNetIP, EtherSIO

F

FastCGI, FINS, FIX, FLUTE, FTP, FTP Data, FTPS

G

Gaijin Entertainment, Gearman, Geneve, Genshin Impact, Git, GLBP, Gnutella, Google Call, GRE, GTP

H

H323, Hamachi, HAProxy, HART-IP, HCL Notes, Heroes of the Storm, HiSLIP, HL7, HLS, HP VM Group Management, HSRP, HTTP, HTTP Connect, HTTP Proxy, HTTP/2

I

i3D, IAX, ICMP, ICMPv6, IEC 62056 (DLMS/COSEM), IEEE 1703, IEEE C37.118 Synchrophasor Protocol, IGMP, IMAP, IMAPS, IP in IP, IPlir4, IPlir6, IPP, IPsec, IRC, ISO 9506-1-2003 MMS

J

Jabber, Java RMI, JSON-RPC

K

KakaoTalk Voice, KCP, Kerberos, Kismet, KNXnet IP

L

LDAP, LDP, Line Call, Link-Local Multicast, LISP

M

Megaco, MELSEC, Memcached, Meraki Cloud, MGCP, Microsoft Delivery Optimization, Microsoft Teams Call, MikroTik NDP, Modbus, Monero, MongoDB, MPEG, MPEG-DASH, MPLS, MQTT, MS SQL TDS, MS-RPCH, MulticastDNS, Munin, MySQL

N

Nano, NAT-PMP, NATS, NetBIOS, NetFlow, New Office Environment, NFS, NTP

O

OCSP, OICQ, OPC UA, OpenFlow, OpenVPN, OpenWire, Oracle Database, OSPF

P

PFCP, PGM, PIM, POP, PostgreSQL, PPTP, Protocol Buffers, PTPv2

Q

QUIC

R

RADIUS, RAFT, RakNet, RDP, RESP, Riot Games, RIPE Atlas, RMCP, Roughtime, RSH, Rsync, RTCP, RTMP, RTP, RTPS, RTSP, Rx

S

S7comm, S7comm Plus, Samsung SDP, SCADA, SCTP, sFlow, SIP, Skinny, SLP, SMB v2/3, SMB/CIFS, SMPP, SMTP, SNMP, SOAP, Socks, SOME/IP, Source Engine, SSDP, SSH, SSL, STOMP, STUN, Syncthing, Syslog

T

TeamSpeak, Telegram Call, Telnet, Teredo, TFTP, Threema, Thrift, Tinc, TivoConnect, Toca Boca, TP-Link SHP, TRDP, TriStation, TrueConf, Tuya LAN, TZSP

U

UBNTAC2, UFTP, UMAS, unknown, Usenet

V

Valve SDR, Viber Call, VNC, VPN Kontinent, VRRP, VXLAN

W

Warcraft 3, WebDAV, WebSocket, WHOIS, WireGuard, WS-Discovery

X

XDMCP

Y

Yojimbo

Z

Z39.50, Zabbix, Zug

К

Поддерживаемые группы приложений

Эти группы приложений вы можете указать в параметре `dpigroup <группа приложений>` транзитного фильтра (см. Группа приложений).

Advertisement and Analytic Services

Приложения в группе:

`Advertisement, Analytics And Tracking, Criteo, Google Analytics, Yandex Browser Telemetry, Yandex Direct, Yandex Metrika`

App-Stores and OS Updates

Приложения в группе:

`Google Play, iOS App Store, Windows Update`

Связанные протоколы:

`Microsoft Delivery Optimization`

Artificial Intelligence

Приложения в группе:

`AI Search, Amazon Alexa, Apple Siri, character.ai, ChatGPT, Claude, CopyMonkey, DashScope, DeepSeek, FusionBrain, Gemini, Gerwin, GigaChat, GigaCode, Google AI Studio, Hugging Face, Jasper, Leonardo.Ai, Maestro, Meta AI, MidJourney, Minimax Chat, NotebookLM, Ollama, OpenAI, Perplexity, Qwen Chat, RoboGPT, Rudalle, Shedevrum, Stability AI, TurboText, Visper, Yandex Alice, Yandex Foundation Models`

Audio Entertainment

Приложения в группе:

Apple Music, Deezer, iHeartRadio, Last-fm, Pandora, SiriusXM, Sonos, SoundCloud, Spotify, Tidal, TuneIn Radio, Yandex Music

Books and Magazines

Приложения в группе:

LitRes-Ru

Browsers

Приложения в группе:

Mozilla

Business

Приложения в группе:

Atlassian, Evernote, Google Docs, Google Trust Services, MyOffice, Notion, Nvidia Services, Office 365, Yandex Docs, Yandex Tracker

Связанные протоколы:

DICOM, HL7, Zug

Cloud and CDN Services

Приложения в группе:

Akamai Cloud, Amazon API Gateway, Amazon Cloud, Amazon Cloudfront, Amazon EC2, Amazon S3, Brightcove, CacheFly, Canonical, CDNetworks, CDNvideo, Cloudera Platform, Cloudflare, Cloudinary, DigitalOcean, Edgecast CDN, Erstream, Fastly, Google Cloud, Huawei Mobile Cloud, KeyCDN, Lumen Technologies, MediaNova CDN, Microsoft Azure, NGenix, Oracle Cloud Infrastructure (OCI), Oracle Services, Rackspace Cloud, Wangsu CDN, Yandex Cloud

Связанные протоколы:

Ceph

Conference

Приложения в группе:

AdobeConnect, Discord, Fuze Meeting, Google Meet, GoToMeeting, Kontur Talk, Microsoft Teams, MTS Link, Slack, Speakchat, TrueConf Online, Webex, Yandex Telemost, Zoom

Связанные протоколы:

BFCP, HCL Notes, TrueConf

Cryptocurrency

Приложения в группе:

Mining

Связанные протоколы:

Bitcoin, Ethereum, Monero, Nano

Database

Приложения в группе:

ClickHouse, Elastic Search Cloud

Связанные протоколы:

Cassandra, DRDA, Elasticsearch, Memcached, MongoDB, MS SQL TDS, MySQL, Oracle Database, PostgreSQL

Development Tools and Services

Приложения в группе:

Crashlytics, GitHub, GitLab, Salesforce

Связанные протоколы:

Apache Kafka

Device Security

Приложения в группе:

Avast DNS, Cybersec, Kaspersky Services

Связанные протоколы:

Avast Services

E-Commerce

Приложения в группе:

AliExpress, Amazon, Apteka.ru, Avito, Citilink, DNS Shop, eBay, ETM, Gold Apple, Joom, Kuper, Lamoda, M.Video-Eldorado, Magnit Market, Megamarket, Ozon, Petrovich, Samokat, Shein, Sima-Land, Taobao, Temu, VkusVill, Vse Instrumenty, Wildberries, X5 Services, Yandex Eda-Delivery, Yandex Lavka, Yandex Market, Youla

Education

Приложения в группе:

Google Classroom, Pluralsight, Wikipedia

Encrypted

Связанные протоколы:

DTLS, QUIC, SSL

Enterprise Services

Приложения в группе:

Alibaba, Apple Services, Citrix, Google Shared Services, Huawei Services, Microsoft Services, MTS Services, Tesla Services, Xiaomi Services, Yandex Services

Filetransfer

Приложения в группе:

Cloud Mail / VK WorkDisk, Dropbox, Google Drive, Google Photos, iCloud, Lustre, OneDrive, Pastebin, SberDisk, WhatsApp Files, Yandex Disk

Связанные протоколы:

AFP, FLUTE, FTP, FTP Data, FTPS, NFS, Rsync, SMB v2/3, SMB/CIFS, Syncthing, TFTP, UFTP, WebDAV

Finance

Приложения в группе:

Pay-Rw

Связанные протоколы:

FIX

Gaming

Приложения в группе:

Activision Blizzard, Among Us, Ankama, Blacknut, Boosteroid, CrossFire, Dota 2, EA Games, Epic Games, GearUp Booster, Guild Wars 2, LagoFast, LoL Wild Rift, NetEase Games, Nexon, Nintendo Network, Nvidia GeForce NOW, Path of Exile, PlayStation Network, Roblox, Rockstar Games, Steam, Tencent Games, The Elder Scrolls Online, World of Warcraft, XBOX

Связанные протоколы:

Armagetron, Call of Duty Mobile, CryNetwork, Gaijin Entertainment, Genshin Impact, Heroes of the Storm, i3D, RakNet, Riot Games, Source Engine, Toca Boca, Valve SDR, Warcraft 3, Yojimbo

Generic

Приложения в группе:

unknown

Связанные протоколы:

unknown

Government

Приложения в группе:

Genprokuratura, MCHS, mos.ru, Pochta Rossii

Industrial

Связанные протоколы:

BACNET, Beckhoff ADS, CAN, CNP over IP, Common Industrial Protocol, DNP3, EGD, Ether-S-Bus, EtherNetIP, EtherSIO, FINS, HART-IP, IEC 62056 (DLMS/COSEM), IEEE 1703, IEEE C37.118 Synchrophasor Protocol, ISO 9506-1-2003 MMS, KNXnet IP, Modbus, RTPS, S7comm, S7comm Plus, SCADA, UMAS

M2M and IoT

Приложения в группе:

Nest

Связанные протоколы:

AMQP, ATG, CoAP, EasyWeather, MELSEC, MQTT, NATS, OPC UA, OpenWire, TP-Link SHP, TRDP, TriStation, Tuya LAN

Mail

Приложения в группе:

Google Mail, Mail-Ru, Microsoft Outlook, POPS, SMTPS, Yandex Mail

Связанные протоколы:

IMAP, IMAPS, POP, SMTP

Messaging

Приложения в группе:

APNS, DingTalk, Google Chat, Kakaotalk, Line, MAX, Messenger, Paltalk, QQ, Signal, Snapchat, Telegram, Viber, VK Messenger, VK Teams, WeChat, WhatsApp, Yandex Messenger

Связанные протоколы:

IRC, Jabber, OICQ, SMPP, STOMP, Threema, Usenet

Navigation

Приложения в группе:

2Gis, Google Maps, Waze

Network Management

Приложения в группе:

DNSCrypt, DoH/DoT, Ntop, Ookla, OpenDNS, Ubiquity

Связанные протоколы:

AliCloud Server, Apache JServ, BFD, BGP, BJNP, CAPWAP, Check_MK, Collectd, Corba, CPHA, DHCP, DHCPv6, Diameter, DLEP, DNS, EGP, FastCGI, Git, GLBP, HP VM Group Management, HSRP, ICMP, ICMPv6, IGMP, IPP, KCP, Kerberos, Kismet, LDAP, LDP, Link-Local Multicast, LISP, Megaco, Meraki Cloud, MikroTik NDP, MulticastDNS, Munin, NAT-PMP, NetBIOS, NetFlow, NTP, OCSP, OpenFlow, OSPF, PFCP, PGM, PIM, Protocol Buffers, PTPv2, RADIUS, RAFT, RESP, RIPE Atlas, Roughtime, RSH, Rx, Samsung SDP, SCTP, sFlow, SLP, SNMP, SOME/IP, SSDP, Syslog, Thrift, Tinc, TivoConnect, UBNTAC2, VRRP, VXLAN, WHOIS, WS-Discovery, Z39.50, Zabbix

News

Приложения в группе:

AccuWeather, Bloomberg, CNN, Life-Ru, NBC News

Peer to Peer

Связанные протоколы:

BitTorrent, eDonkey, Gnutella

Pornography

Приложения в группе:

Adult Content

Remote Control

Приложения в группе:

AnyDesk, NoMachine, Radmin, TeamViewer

Связанные протоколы:

DCE RPC, Gearman, HiSLIP, Java RMI, JSON-RPC, MS-RPCH, RDP, RMCP, SOAP, SSH, Telnet, VNC, XDMCP

Social

Приложения в группе:

Badoo, Bluesky, Bumble, Facebook, Facebook Reels and Stories, Instagram, LinkedIn, Mastodon, Odnoklassniki, Pinterest, reddit, Sina, Sina Weibo, Threads, TikTok, Tumblr, VK, X (Twitter)

Streaming

Приложения в группе:

1kxun, Amazon Prime Video, Apple TV, Channel One, Dailymotion, DAZN, DirecTV, Disney Plus, ESPN, HBO Now, Hulu, iFlix, Iqiyi, iTunes, Ivi-Ru, Kick, Kinopoisk, Livestream, MTS TV, NBC Sports, NetFlix, OCS, Paramount Plus, Rumble, RUTUBE, Showtime, Tencent Video, Twitch, Vimeo, VK Video, Vudu, YouTube, YouTube Upload, Zattoo

Связанные протоколы:

Agora, HLS, MPEG, MPEG-DASH, RTCP, RTMP, RTP, RTSP

Travel and Transportation

Приложения в группе:

AirBnB

Tunnel

Приложения в группе:

123VPN, Avira Phantom VPN, Browsec VPN, CactusVPN, Cloudflare WARP, DotVPN, Fortinet, Mudfish, Mullvad VPN, NordVPN, Opera VPN, Private Internet Access, Proton VPN, Samsung Max Privacy VPN, SecureVPN, SecureVPN-Pro, SoftEther, Surfshark, Tailscale, TOR, TunnelBear, ViPNet, Windscribe, ZOOGVPN

Связанные протоколы:

AH IPSec, ERSPAN, ESP IPSec, Geneve, GRE, GTP, Hamachi, HTTP Connect, HTTP Proxy, IP in IP, IPlir4, IPlir6, IPsec, MPLS, OpenVPN, PPTP, Socks, Teredo, TZSP, VPN Kontinent, WireGuard

Voice over IP

Приложения в группе:

Facebook VoIP, Mumble, Signal VoIP, Snapchat Call, Vivox, WhatsApp Call

Связанные протоколы:

EAQ, Google Call, H323, IAX, KakaoTalk Voice, Line Call, MGCP, Microsoft Teams Call, New Office Environment, SIP, Skinny, STUN, TeamSpeak, Telegram Call, Viber Call

Wallet

Приложения в группе:

AliPay

Web

Приложения в группе:

DataSaver, Google, Naver, Tencent, Yahoo Services

Связанные протоколы:

HAProxy, HTTP, HTTP/2, WebSocket



Особенности фильтрации по приложениям и прикладным протоколам

Для ряда приложений и прикладных протоколов, которые вы можете задать при создании транзитных фильтров, существуют следующие особенности:

- Фильтр с заданным протоколом MySQL обрабатывает трафик для версии MySQL 5.6 и выше.
- Чтобы разрешить трафик Aliexpress, создайте разрешающий фильтр с указанием приложений Aliexpress и Alibaba.
- Запрещающий фильтр по приложению Alibaba также будет блокировать трафик сайта Aliexpress.
- Приложение Kontur Talk использует в своей работе Yandex Services. Поэтому в разрешающий фильтр для приложения Kontur Talk также добавляйте приложение Yandex Services.

  Если вы хотите разрешить трафик Kontur Talk и запретить трафик одного из приложений Яндекс, создайте:

  - разрешающий фильтр для приложения Kontur Talk;
  - запрещающий фильтр для приложения Яндекс;
  - разрешающий фильтр для Yandex Services.
- Чтобы разрешить трафик любого из приложений Яндекс, создайте разрешающий фильтр для самого приложения Яндекс и для приложения Yandex Services.
- Чтобы разрешить трафик любого из приложений Google, создайте разрешающий фильтр для самого приложения Google и для приложения Google Services.

- Для корректной работы программ и сервисов из группы приложений Gaming, создайте разрешающий фильтр для этой группы и для группы Cloud and CDN Services.
- Чтобы разрешить трафик VK Video, создайте разрешающий фильтр для приложений VK Video, VK и Odnoklassniki.
- Чтобы разрешить трафик VK Messenger, создайте разрешающий фильтр для приложений VK Messenger и VK.
- Чтобы разрешить трафик Cloud Mail / VK WorkDisk, создайте разрешающий фильтр для приложений Cloud Mail / VK WorkDisk, VK и Mail-Ru.
- Чтобы разрешить трафик VK Teams, создайте разрешающий фильтр для приложений VK Teams, VK и Mail-Ru.

M

Поддерживаемые MIME-типы

- **Application — Внутренний формат прикладной программы**
  - application/atom+xml: Atom
  - application/EDI-X12: EDI X12 (RFC 1767)
  - application/EDIFACT: EDI EDIFACT (RFC 1767)
  - application/json: JavaScript Object Notation JSON (RFC 4627)
  - application/javascript: JavaScript (RFC 4329)
  - application/octet-stream: двоичный файл без указания формата (RFC 2046)
  - application/ogg: Ogg (RFC 5334)
  - application/pdf: Portable Document Format, PDF (RFC 3778)
  - application/postscript: PostScript (RFC 2046)
  - application/soap+xml: SOAP (RFC 3902)
  - application/font-woff: Web Open Font Format
  - application/xhtml+xml: XHTML (RFC 3236)
  - application/xml-dtd: DTD (RFC 3023)
  - application/xop+xml: XOP
  - application/zip: ZIP
  - application/gzip: Gzip
  - application/x-bittorrent: BitTorrent

- application/x-tex: TeX

- **audio — Аудио**
  - audio/basic: mulaw аудио, 8 кГц, 1 канал (RFC 2046)
  - audio/L24: 24-bit Linear PCM аудио, 8-48 кГц, 1-N каналов (RFC 3190)
  - audio/mp4: MP4
  - audio/aac: AAC
  - audio/mpeg: MP3 или др. MPEG (RFC 3003)
  - audio/ogg: Ogg Vorbis, Speex, Flac или др. аудио (RFC 5334)
  - audio/vorbis: Vorbis (RFC 5215)
  - audio/x-ms-wma: Windows Media Audio
  - audio/x-ms-wax: Windows Media Audio перенаправление
  - audio/vnd.rn-realaudio: RealAudio
  - audio/vnd.wave: WAV (RFC 2361)
  - audio/webm: WebM
- **image — Изображение**
  - image/gif: GIF (RFC 2045 и RFC 2046)
  - image/jpeg: JPEG (RFC 2045 и RFC 2046)
  - image/pjpeg: JPEG
  - image/png: Portable Network Graphics (RFC 2083)
  - image/svg+xml: SVG
  - image/tiff: TIFF (RFC 3302)
  - image/vnd.microsoft.icon: ICO
  - image/vnd.wap.wbmp: WBMP
- **message — Сообщение**
  - message/http: (RFC 2616)
  - message/imdn+xml: IMDN (RFC 5438)
  - message/partial: E-mail (RFC 2045 и RFC 2046)
  - message/rfc822: E-mail; EML файлы, MIME файлы, MHT файлы, MHTML файлы (RFC 2045 и RFC 2046)
- **model — Для 3D моделей**
  - model/example: (RFC 4735)
  - model/iges: IGS файлы, IGES файлы (RFC 2077)
  - model/mesh: MSH файлы, MESH файлы (RFC 2077), SILO файлы

- model/vrml: WRL файлы, VRML файлы (RFC 2077)
- model/x3d+binary: X3D ISO стандарт для 3D компьютерной графики, X3DB файлы
- model/x3d+vrml: X3D ISO стандарт для 3D компьютерной графики, X3DV VRML файлы
- model/x3d+xml: X3D ISO стандарт для 3D компьютерной графики, X3D XML файлы

- **multipart — Составные файлы**
  - multipart/form-data: MIME Webform (RFC 2388)
  - multipart/signed: (RFC 1847)
  - multipart/encrypted: (RFC 1847)
  - multipart/mixed: MIME E-mail (RFC 2045 и RFC 2046)
  - multipart/alternative: MIME E-mail (RFC 2045 и RFC 2046)
  - multipart/related: MIME E-mail (RFC 2387 и используемое MHTML (HTML mail))
- **text — Текст**
  - text/cmd: команды
  - text/css: Cascading Style Sheets (RFC 2318)
  - text/csv: CSV (RFC 4180)
  - text/html: HTML (RFC 2854)
  - text/javascript (Obsolete): JavaScript (RFC 4329)
  - text/plain: текстовые данные (RFC 2046 и RFC 3676)
  - text/php: Скрипт языка PHP
  - text/xml: Extensible Markup Language (RFC 3023)
- **video — Видео**
  - video/mpeg: MPEG-1 (RFC 2045 и RFC 2046)
  - video/mp4: MP4 (RFC 4337)
  - video/ogg: Ogg Theora или другое видео (RFC 5334)
  - video/quicktime: QuickTime
  - video/webm: WebM
  - video/x-ms-wmv: Windows Media Video
  - video/x-flv: FLV
  - video/3gpp: .3gpp .3gp
  - video/3gpp2: .3gpp2 .3g2
- **vnd — Вендорные файлы**
  - application/vnd.oasis.opendocument.text: OpenDocument
  - application/vnd.oasis.opendocument.spreadsheet: OpenDocument

- application/vnd.oasis.opendocument.presentation: OpenDocument
- application/vnd.oasis.opendocument.graphics: OpenDocument
- application/vnd.ms-excel: Microsoft Excel файлы
- application/vnd.openxmlformats-officedocument.spreadsheetml.sheet: Microsoft Excel 2007 файлы
- application/vnd.ms-powerpoint: Microsoft Powerpoint файлы
- application/vnd.openxmlformats-officedocument.presentationml.presentation: Microsoft Powerpoint 2007 файлы
- application/msword: Microsoft Word файлы
- application/vnd.openxmlformats-officedocument.wordprocessingml.document: Microsoft Word 2007 файлы
- application/vnd.mozilla.xul+xml: Mozilla XUL файлы
- application/vnd.google-earth.kml+xml: KML файлы (например, для Google Earth)

- **x — Нестандартные файлы**
  - application/x-www-form-urlencoded: Form Encoded Data
  - application/x-dvi: DVI
  - application/x-latex: LaTeX файлы
  - application/x-font-ttf: TrueType (незарегистрированный MIME-тип, но наиболее часто используемый)
  - application/x-shockwave-flash: Adobe Flash
  - application/x-stuffit: StuffIt
  - application/x-rar-compressed: RAR
  - application/x-tar: Tarball
  - text/x-jquery-tmpl: jQuery
  - application/x-javascript
- **x-pkcs — PKCS**
  - application/x-pkcs12: p12 файлы
  - application/x-pkcs12: pfx файлы
  - application/x-pkcs7-certificates: p7b файлы
  - application/x-pkcs7-certificates: spc файлы
  - application/x-pkcs7-certreqresp: p7r файлы
  - application/x-pkcs7-mime: p7c файлы
  - application/x-pkcs7-mime: p7m файлы
  - application/x-pkcs7-signature: p7s файлы



N

Использование ViPNet Coordinator HW в качестве МЭ типа А четвертого класса защиты

Рекомендации по использованию ViPNet Coordinator HW в качестве межсетевого экрана типа «А» четвертого класса защиты:

- Запретите трафик от нежелательных приложений. Для этого создайте сетевые фильтры, запрещающие передачу данных через порты, которые используют эти приложения.

  Разрешите трафик от доверенных приложений. Для этого создайте сетевые фильтры, разрешающие передачу данных через порты, которые используют эти приложения.

- Для ассоциации пользователей сети и IP-адресов:
  - для каждого сетевого узла задайте статический IP-адрес;
  - занесите в специальный журнал ФИО физических лиц, имеющих учётные записи на сетевых узлах;
- организуйте фиксацию времени работы пользователей на сетевых узлах, где зарегистрировано несколько учётных записей, в специальном журнале.



Возможные неполадки

Блокирование медиа-сессии SIP-соединения при завершении сигнальной сессии по таймауту

В SIP-клиентах некоторых производителей сигнальная сессия SIP-соединения может завершаться через 300 сек. при отсутствии активности. В этом случае ViPNet Coordinator HW блокирует медиа-сессию установленного SIP-соединения. Чтобы избежать блокирования медиа-сессии, установите в настройках SIP-клиента отправку сообщений `Keep Alive` каждые 30 сек. У разных производителей SIP-клиентов этот параметр может называться `re-INVITE`, `OPTIONS`, `INFO` или `NOTIFY`.

Неполадки в работе сервисов IP-телефонии, видео- и аудиоконференций после переключения кластера

Если в вашей сети используются сервисы IP-телефонии, видео- и аудиоконференций, которые работают по протоколам H.323, SCCP, SIP и устанавливают TCP-соединения, то после переключения узлов кластера возможны неполадки в их работе. В этих случаях пользователям сервисов необходимо сделать вызов заново или перезапустить клиента, например SIP-телефон.

Не отображаются активные пользователи при настройке взаимодействия с Active Directory

При взаимодействии ViPNet Coordinator HW с Active Directory на видимость активных пользователей влияет параметр групповой политики **Аудит входа в систему**. По умолчанию этот параметр не определен, поэтому после настройки взаимодействия с контроллером домена в журнале безопасности Active Directory могут не фиксироваться события с кодом 4624. Это приводит к тому, что активные пользователи не отображаются в списке пользователей ViPNet Coordinator HW.

Для устранения проблемы на контроллере домена:

1. Запустите редактор групповой политики `gpedit.msc`.
2. Выберите **Конфигурация компьютера** > **Конфигурация Windows** > **Параметры безопасности** > **Конфигурация расширенной политики аудита** > **Политики аудита системы** - **Объект локальной групповой политики**.
3. В категории **Вход/Выход** выберите **Аудит входа в систему**.
4. На вкладке **Политика** установите флажки **Настроить следующие события аудита** и **Успех**.
5. Нажмите **OK**.

После обновления групповой политики активные пользователи контроллера домена будут отображаться в списке пользователей ViPNet Coordinator HW.

Пропадает связь с контроллером Active Directory

Установленные по умолчанию параметры групповых политик Windows Server обеспечивают его доступность при настройке взаимодействия ViPNet Coordinator HW с Active Directory. Установка значений, отличных от заданных по умолчанию, может привести к нарушению связи ViPNet Coordinator HW с контроллером домена.

Чтобы избежать проблем при взаимодействии ViPNet Coordinator HW с Active Directory установите рекомендованные значения групповых политик, относящихся к параметрам безопасности домена:

1. Запустите редактор групповой политики `gpedit.msc`.
2. Выберите **Конфигурация компьютера** > **Конфигурация Windows** > **Параметры безопасности** > **Локальные политики** и установите параметры, указанные в таблице ниже.

Таблица 66. Рекомендованные значения параметров политик безопасности

Политика безопасности	Условия на значение
DCOM: Ограничения компьютера на доступ в синтаксисе SDDL (Security Descriptor Definition	Не допускается явный запрет на удалённый доступ для технологического пользователя или группы

Политика безопасности	Условия на значение
Language)	«Пользователи DCOM»
DCOM: Ограничения компьютера на запуск в синтаксисе SDDL (Security Descriptor Definition Language)	Не допускается явный запрет на удалённый запуск и активацию для технологического пользователя или группы «Пользователи DCOM»
Сетевая безопасность: минимальная сеансовая безопасность для клиентов на базе NTLM SSP (включая безопасный RPC)	Параметр «Требовать сеансовую безопасность NTLMv2» должен быть отключен
Сетевая безопасность: уровень проверки подлинности LAN Manager	Должен быть установлен параметр по умолчанию «Не определено», либо выбран параметр политики «Отправлять только NTLMv2-ответ. Отказывать LM»
Сетевая безопасность: не хранить хэш-значения LAN Manager при следующей смене пароля	«Не определено» или «Отключен»

3 Проверьте настройки политик безопасности, перечисленные в таблице ниже. Если они отличаются от значений по умолчанию, убедитесь, что они не препятствуют сетевой аутентификации ViPNet Coordinator HW в вашем домене.

Таблица 67. Политики сетевой аутентификации NTLM

Политика безопасности	Значение по умолчанию
Сетевая безопасность: ограничения NTLM: аудит проверки подлинности NTLM в этом домене	«Не определено»
Сетевая безопасность: ограничения NTLM: входящий трафик NTLM	«Не определено»
Сетевая безопасность: ограничения NTLM: добавить исключения для серверов в этом домене	«Не определено»
Сетевая безопасность: ограничения NTLM: добавить удалённые серверы в исключения проверки подлинности NTLM	«Не определено»
Сетевая безопасность: ограничения NTLM: исходящий трафик NTLM к удалённым серверам	«Не определено»
Сетевая безопасность: ограничения NTLM: проверка подлинности NTLM в этом домене	«Не определено»

После обновления базы правил IPS отображается неправильный статус

В ряде случаев изменение статуса службы обновления IPS может происходить с задержкой. Такое происходит, когда изменения не затрагивают текущее состояние базы правил IPS.

Например, если при настройке службы обновления IPS был установлен неправильный пароль сервера обновлений, то при отображении статуса службы командой `service ips show status` выведется сообщение об ошибке:

```
IPS rules database failed to download: Authentication fail. Server send error: 102
```

Если база правил IPS находится в актуальном состоянии, ввод правильного пароля не повлияет на ошибочно выводимый статус службы. Статус службы будет обновлен при следующем успешном обновлении базы правил IPS.

После настройки системного времени недоступна аутентификация пользователей

После настройки системного времени в некоторых случаях становится недоступной аутентификация пользователей.

Чтобы устранить проблему, перезагрузите ViPNet Coordinator HW.

Ошибка обновления справочников, ключей и лицензий

- Отдельные команды, связанные с системными процессами, вызывают глобальную блокировку управляющих запросов, которая накладывает ограничения на работу ViPNet Coordinator HW. В частности, обновление справочников, ключей и лицензий, поступившее из ViPNet Prime во время глобальной блокировки, не будет применено. Дождитесь завершения глобальной блокировки и повторно отправьте обновление из ViPNet Prime.
- Применение обновления справочников, ключей и лицензий по времени может совпасть с переключением узлов кластера. В этом случае обновление не будет применено. Поэтому повторно отправьте из ViPNet Prime обновление справочников и ключей.

Ошибка обновления ПО, справочников, ключей и лицензий

Ошибка обновления ПО, справочников, ключей и лицензий на узлах, связанных с ViPNet Coordinator HW, может быть связана с отсутствием доступа последнего к транспортному серверу ViPNet Prime:

1 Определите IP-адрес доступа к ViPNet Prime. Для этого откройте конфигурационный файл `iplir.conf`:

```
hostname# iplir show config
```

IP-адрес доступа указан в секции `[id]` узла `Control Center` в параметре `accessip`:

```
...
[id]
id= 0x3e130002
name= Control Center                                    VPN-15891
ip= 7.0.0.2, 11.0.0.2
accessip= 11.0.0.2
port= 55777
...
```

2 Проверьте, что IP-адрес доступа к ViPNet Prime соответствует его доменному имени:

```
hostname# machine hosts show
127.0.0.1 va1000 localhost localhost.localdomain
11.0.0.2 prime.vk
```

3 Иначе добавьте в файл `hosts` запись о соответствии IP-адреса доступа к ViPNet Prime и доменного имени ViPNet Prime:

```
hostname# machine hosts add <IP-адрес доступа к ViPNet Prime> <доменное имя ViPNet Prime>
```

Ошибка локального обновления ПО ViPNet Coordinator VA

При ошибке локального обновления ПО ViPNet Coordinator VA, связанной с целостностью обновляемых файлов, проверьте тип контроллера USB-носителя. Тестирование показало, что ошибка происходит при использовании USB-носителя с контроллером Alcor 0xF500. В этом случае замените USB-носитель и выполните обновление повторно.

Ошибка обновления ПО версий 4.5.1/4.5.2 до версии 5.1.0

Ошибка локального или удаленного обновления ПО версий 4.5.1/4.5.2 до версии 5.1.0 может возникнуть после перехода управления сетью ViPNet с ViPNet ЦУС на ViPNet Prime. Подробнее о причине ошибки и способе ее устранения см. «ViPNet Prime. Руководство главного администратора», раздел «Обновление ViPNet Coordinator HW 4.5.x до версии 5.1.0».

При удалённом обновлении ПО обновился только один узел кластера

Отправьте обновление ПО из ViPNet Prime на ViPNet Coordinator HW повторно или выполните локальное обновление узла кластера (см. Обновление ПО с версий 5.1.x, 5.2.x и 5.3.x до версии 5.4.x).

Ошибка создания резервной копии индивидуальной конфигурации на ViPNet Prime

Одной из причин ошибки, возникающей при создании резервной копии индивидуальной конфигурации на ViPNet Prime, может быть выпуск нового дистрибутива ключей ViPNet Coordinator HW:

- Если вы создавали резервную копию в командном интерпретаторе, на эту причину указывает строка `error: Make sure that you are using the latest appliance initialization file for this appliance` в выводе команды.
- Если вы создавали резервную копию в веб-интерфейсе, на эту причину указывает событие системного журнала, содержащее текст `Make sure that you are using the latest appliance initialization file for this appliance`.

Для устранения причины обновите в ViPNet Prime справочники и ключи ViPNet Coordinator HW.

Низкая скорость обработки трафика на интерфейсах 1G исполнения ViPNet Coordinator HW5000

Если на исполнении ViPNet Coordinator HW5000 включены IPS и/или DPI, то скорость обработки трафика на интерфейсах 1G будет ниже, чем на интерфейсах 10G. Падение скорости обработки обусловлено особенностями сетевого адаптера 1G аппаратных платформ HW5000 Q1 и HW5000 Q2. Для подключения ViPNet Coordinator HW5000 к коммутационному оборудованию сети рекомендуется использовать интерфейсы 10G:

- HW5000 Q1 — интерфейсы eth2, eth3, eth6, eth7.
- HW5000 Q2 — интерфейсы eth4 - eth11.

Сбои в работе агрегированного канала

Сбои в работе агрегированного канала могут быть вызваны неполадками в работе подчинённых интерфейсов, например:

- Неисправностью сетевого оборудования.
- Несогласованностью скоростных режимов работы интерфейсов.
- Неисправностью физического тракта.

Чтобы выяснить причины неполадок в работе подчинённого интерфейса:

1 Проверьте работоспособность интерфейса:

1.1 Просмотрите информацию об интерфейсе:

```
hostname# inet show interface <интерфейс>
```

1.2 Проверьте вывод в строке `Link detected`:

Если в строке отображается `no`, интерфейс неработоспособный.

2 Проверьте режим работы смежного устройства, с которым осуществляется связь по агрегированному интерфейсу. Режимы работы должны совпадать на обоих устройствах.

Циклическая перезагрузка ViPNet Coordinator HW

Циклической считается перезагрузка ViPNet Coordinator HW, произошедшая более трех раз подряд в течение 10 минут. При этом локальный администратор не может пройти аутентификацию. Событие циклической перезагрузки регистрируется в системном журнале. Причинами циклической перезагрузки могут быть:

- ошибки в системных файлах;
- неисправность аппаратной платформы;
- ошибки обновления ПО;
- некорректная установка дистрибутива ключей;
- некорректная настройка ViPNet Coordinator HW.

Чтобы выяснить причину циклической перезагрузки:

1 Подключитесь к ViPNet Coordinator HW с помощью консоли.

2 Дождитесь сообщения `If you want to start ViPNet later, press ENTER or VPN services will start after 5 seconds` и нажмите **Enter**, чтобы отложить запуск служб VPN на 10 минут,

3 Пока службы VPN не запущены, войдите как локальный администратор.

4 Выполните экспорт журналов на USB-носитель.

5 Самостоятельно проанализируйте системный журнал или передайте его в службу технической поддержки ИнфоТеКС.

Особенности добавления объектов лицензирования DPI и IPS

Объекты лицензирования DPI и IPS могут быть добавлены на ViPNet Coordinator HW в любое время. Если в момент добавления на ViPNet Coordinator HW были открыты сессии в веб-интерфейсе или командном интерпретаторе, то функционал DPI и IPS будет в них недоступен. В этом случае перезапустите сессии.

Особенности увеличения объёма оперативной памяти виртуальной машины ViPNet Coordinator VA

При увеличении объёма оперативной памяти виртуальной машины ViPNet Coordinator VA автоматически не изменяется максимальное количество одновременно устанавливаемых соединений МЭ (параметр `max-connections`). Поэтому после запуска виртуальной машины установите его вручную в соответствии с вариантом исполнения ViPNet Coordinator VA:

```
hostname# firewall settings max-connections <значение>
```

Подробнее см. «Справочник команд и конфигурационных файлов», раздел «Команды группы firewall».

Нарушена связь ViPNet Coordinator HW с узлами защищенной сети

Одной из причин нарушения связи ViPNet Coordinator HW с узлами защищенной сети может быть расхождение времени между отправкой и приемом IP-пакета. Время может различаться не более, чем на величину, задаваемую командой `iplir option maxtimedif` (по умолчанию — 2 часа).

Другой причиной нарушения связи может быть рассинхронизация времени более чем на 12 часов как вперед, так и назад. Чтобы уточнить причину и решения проблемы:

- Для исполнений на аппаратных платформах проверьте работоспособность батарейки системной платы. В случае ее неисправности:
  - замените батарейку;

- установите время вручную.

- Если ViPNet Coordinator HW синхронизируется с выделенным NTP-сервером, который не используется другими узлами защищенной сети, проверьте его работоспособность. В случае неисправности используйте другой NTP-сервер.

Особенности передачи трафика между ViPNet Coordinator HW версий 4.5.x–5.2.1 и 5.3.x

Если на пути передачи трафика между ViPNet Coordinator HW версий 5.3.x расположен ViPNet Coordinator HW версий 4.5.x–5.2.1, настройте на нем разрешающие транзитные фильтры открытой сети:

```
hostname# firewall forward src <IP-адрес ViPNet узла 5.3.x_1> dst <IP-адрес ViPNet узла 5.3.x_2> pass
```

```
hostname# firewall forward src <IP-адрес ViPNet узла 5.3.x_2> dst <IP-адрес ViPNet узла 5.3.x_1> pass
```

Иначе транзитный трафик между ViPNet Coordinator HW версий 5.3.x будет заблокирован на ViPNet Coordinator HW версий 4.5.x–5.2.1.

Особенности работы ViPNet Coordinator HW 5.3.1 с ViPNet Prime 1.9.5

После обновления ViPNet Prime с версии 1.7.2 до версии 1.9.5 или подключения нового ViPNet Coordinator HW 5.3.1 к защищенной сети под управлением ViPNet Prime 1.9.5, связь ViPNet Coordinator HW 5.3.1 с модулем ViPNet NVS будет потеряна. Для восстановления отправьте обновление справочников и ключей на ViPNet Coordinator HW 5.3.1.

При подключении к сети Wi-Fi сетевой интерфейс не получает IP-адрес от DHCP-сервера

Ошибка проявляется на устройствах MikroTik и может быть вызвана несовместимостью протоколов шифрования между маршрутизатором и ViPNet Coordinator HW. Для устранения ошибки на маршрутизаторе установите значения параметров при настройке Security Profile для интерфейса:

- Для сети WPA:
  - Authentication Types — WPA PSK;

    - Unicast Ciphers и Group Ciphers — tkip.
- Для сети WPA2:
    - Authentication Types — WPA2 PSK;
    - Unicast Ciphers и Group Ciphers — aes ccm.

P

Термины и сокращения

ViPNet Prime

ПО для централизованного управления решениями ViPNet. Позволяет управлять конфигурацией сети (включая устройства, пользователей и лицензии), централизованно обновлять ПО ViPNet и выполнять мониторинг состояния сети ViPNet.

Включает в себя основные функциональные модули:

- ViPNet VPN — модуль управления топологией сети, регистрирует защищаемые устройства и задаёт связи между ними.
- ViPNet Network Visibility System — модуль мониторинга состояния сети ViPNet и входящих в неё устройств.
- ViPNet Policy Management — модуль централизованного управления политиками безопасности узлов сети ViPNet.

ViPNet TIAS

Система ViPNet TIAS (Threat Intelligence Analytics System) анализирует события информационной безопасности, поступающие от различных источников: ViPNet IDS NS, ViPNet IDS HS, ViPNet xFirewall, ViPNet EPP; автоматически выявляет инциденты информационной безопасности на основании потока этих событий и оперативно информирует заинтересованных лиц о произошедших инцидентах.

Администратор сети ViPNet

Лицо, отвечающее за управление сетью ViPNet, создание и обновление справочников и ключей для сетевых узлов ViPNet, настройку межсетевого взаимодействия с доверенными сетями.

Базовый виртуальный адрес

Является точкой отсчета при назначении виртуальных адресов для каждого из реальных адресов узла. Если в данный момент узел виден по виртуальному адресу, его адресом доступа считается либо базовый виртуальный адрес, либо вторичный виртуальный адрес, соответствующий первому в списке реальному адресу.

Виртуальная защищенная сеть

Технология, позволяющая создать логическую сеть, чтобы обеспечить множественные сетевые соединения между компьютерами или локальными сетями через существующую физическую сеть. Уровень доверия к такой виртуальной сети не зависит от уровня доверия к физическим сетям благодаря использованию средств криптографии (шифрования, аутентификации) и средств персонального и межсетевого экранирования.

Виртуальный IP-адрес

IP-адрес, который приложения на сетевом узле ViPNet (А) используют для обращения к ресурсам сетевого узла ViPNet (Б) или туннелируемых им узлов вместо реального IP-адреса узла. Виртуальные IP-адреса узлу ViPNet (Б) назначаются непосредственно на узле А. На других узлах узлу ViPNet (Б) могут быть назначены другие виртуальные адреса. Узлу ViPNet (Б) назначается столько виртуальных адресов, сколько реальных адресов имеет данный узел. При изменении реальных адресов у узла Б выделенные ему виртуальные адреса не изменяются. Виртуальные адреса туннелируемых узлов привязываются к реальным адресам этих узлов и существуют, пока существует данный реальный адрес. Использование виртуальных адресов позволяет избежать конфликта реальных IP-адресов в случае, если сетевые узлы ViPNet работают в локальных сетях с пересекающимся адресным пространством, а также использовать эти адреса для аутентификации удалённых узлов в приложениях ViPNet.

Дистрибутив ключей

Набор симметричных ключей обмена с защищенными узлами сети ViPNet. Формируется в ViPNet Prime на основе заданных связей между узлами.

В ViPNet Coordinator HW версии 5.0 и выше используется дистрибутив ключей `ds5`. Содержит справочники, ключи и лицензии, необходимые для инициализации и работы ViPNet Coordinator HW.

В ViPNet Coordinator HW версий 4.4.x, ViPNet xFirewall и ViPNet Client используется дистрибутив ключей `dst`.

Доверенная сеть

Сеть ViPNet, с узлами которой узлы собственной сети ViPNet осуществляют защищенное взаимодействие.

Защищенный интернет-шлюз (открытый интернет)

Технология, реализованная в программном обеспечении ViPNet. При подключении к интернету узлы локальной сети изолируются от защищенной сети, а при работе в защищенной сети — от интернета, что обеспечивает защиту от возможных сетевых атак извне без физического отключения компьютеров от локальной сети.

Защищенный узел

Сетевой узел, на котором установлено программное обеспечение ViPNet с функцией шифрования трафика на сетевом уровне.

Клиент (ViPNet-клиент)

Сетевой узел ViPNet, который является начальной или конечной точкой передачи данных. В отличие от координатора клиент не выполняет функции маршрутизации трафика и служебной информации.

Ключи защиты обновлений

Ключи защиты обновлений обеспечивают безопасное удаленное обновление ключей обмена из ключевого центра ViPNet Prime и их хранение в ViPNet Coordinator HW.

Ключи обмена

На ключах обмена защищается канал передачи данных между двумя связанными узлами сети ViPNet.

Командный интерпретатор

Командная оболочка, предназначенная для администрирования программного обеспечения ViPNet Coordinator HW с помощью ряда специальных команд.

Координатор (ViPNet-координатор)

Сетевой узел ViPNet, представляющий собой компьютер с установленным программным обеспечением координатора (ViPNet Coordinator) или программно-аппаратный комплекс. В сети ViPNet-координатор выполняет серверные функции, а также маршрутизацию трафика и служебной информации.

Межсетевое взаимодействие

Информационное взаимодействие, организованное между сетями ViPNet. Позволяет узлам различных сетей ViPNet обмениваться информацией по защищенным каналам. Для организации взаимодействия между узлами различных сетей ViPNet администраторы этих сетей обмениваются межсетевой информацией.

Метрика адреса доступа

Определяет задержку (в миллисекундах) отправки тестовых пакетов при выполнении опроса узла для определения доступности адреса. Предназначена для задания приоритета использования каналов связи.

Открытый узел

Узел без ПО ViPNet с функцией шифрования трафика на сетевом уровне, расположенный в сети «за координатором».

Сервер IP-адресов

Функциональность координатора, обеспечивающая регистрацию, рассылку и предоставление информации о состоянии защищенных узлов.

Сервер соединений

Функциональность координатора, обеспечивающая соединение клиентов друг с другом в случае, если они находятся в разных подсетях и не могут соединиться напрямую. Для каждого клиента функцию сервера соединений выполняет координатор, назначенный сервером IP-адресов.

Сетевой узел ViPNet

Сетевой узел с ПО ViPNet, зарегистрированный в ViPNet Prime VPN.

Сеть ViPNet

Логическая сеть, организованная с помощью программного обеспечения ViPNet и представляющая собой совокупность защищённых узлов ViPNet. Сеть ViPNet имеет наложенную маршрутизацию, обеспечивающую взаимодействие узлов сети. Каждая сеть ViPNet имеет свой уникальный номер.

Справочники и ключи

Настройки узла ViPNet, ключи защиты обновлений, ключи обмена и ключи пользователя.

Транспортная квитанция

Файл, оповещающий отправителя о невозможности доставки транспортного конверта MFTP.

Транспортный конверт

Зашифрованная информация служб или приложений, доставляемая на защищенные узлы ViPNet транспортным сервером MFTP.

Транспортный сервер MFTP

Компонент координатора, обеспечивающий маршрутизацию транспортных конвертов MFTP между узлами сети ViPNet.

Туннелирование

Технология для защиты соединений между устройствами локальных сетей, которые связаны через интернет или другие публичные сети. Шифрование трафика устройств выполняется координаторами, установленными на границах локальных сетей.

Туннелируемый узел

Узел, на котором не установлено программное обеспечение ViPNet с функцией шифрования трафика на сетевом уровне, но его трафик на потенциально опасном участке сети зашифровывается и расшифровывается на координаторе, за которым он стоит.

Туннелирующий координатор

Координатор, который осуществляет туннелирование.

Шлюзовой координатор

Координатор, через который происходит обмен транспортными конвертами между сетями ViPNet, установившими межсетевое взаимодействие. Шлюзовые координаторы назначаются в ViPNet Prime каждой сети при организации взаимодействия между двумя различными сетями ViPNet.

Электронная подпись (ЭП)

Откреплённая CMS-подпись, сформированная по Р 1323565.1.025–2019 и ГОСТ 34.10-2012 (512 бит).