



ViPNet Prime Policy Management

Руководство администратора

Версия продукта: 1.11

© АО «ИнфоТеКС», 2026

ФРКЕ.00267-01 32 01

Версия продукта: 1.11

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 Prime Policy Management приведены в Правилах пользования, Лицензионном соглашении с конечным пользователем либо в другой эксплуатационной документации, сопровождающей ViPNet Prime Policy Management.

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.....	6
О документе.....	7
Соглашения документа.....	7
О модуле ViPNet Prime Policy Management.....	8
Что нового в версии 1.11	9
Системные требования	10
Совместимые продукты ViPNet.....	11
Комплект поставки	13
Связанные документы	14
Обратная связь.....	15
 Глава 1. Начало работы.....	16
Лицензирование.....	17
Управление доступом и подключение.....	18
Интерфейс ViPNet Prime Policy Management	19
Порядок работы	21
 Глава 2. Предварительные действия.....	22
Назначение функции управления политиками безопасности	23
Особенности обновления версий	24
Увеличение оперативной памяти при 20000 правил	26
Загрузка классификатора DPI.....	27
Работа с базой данных стран	28
Скачивание базы данных стран с сервера обновлений	28
Проверка электронной подписи базы данных стран с помощью ViPNet PKI Client...28	
Загрузка базы данных стран.....	29
Назначение базы данных стран в организацию.....	30
Импорт политик и правил из Check Point.....	32
Импорт шаблонов политик безопасности из ViPNet Policy Manager	37
Экспорт данных из базы данных ViPNet Policy Manager.....	40
Особенности переноса правил из ViPNet Policy Manager	42
 Глава 3. Работа с политиками безопасности.....	44
О политиках безопасности	46
Создание политики безопасности.....	48

Назначение политики безопасности на устройства	49
Назначение лицензии на устройство	50
Освобождение лицензии на устройства	51
Действия с политиками безопасности	52
Работа со слоями	54
Настройка режима работы ViPNet Coordinator IG	57
Настройка обработки прикладных протоколов	58
Дополнения политики безопасности	60
Разрешение отправки дополнительных параметров функций на целевые устройства	61
Параметры регистрации сессий и IP-пакетов	64
Инспекция политик	68
Работа с отчетом инспекции политики	70
Отправка политик на устройства	72
Настройка отправки результирующих политик	74
Глава 4. Работа с правилами	76
Правила фильтрации трафика	77
Создание правил фильтрации	79
Создание правил фильтрации по пользователям, приложениям и прикладным протоколам	83
Правила фильтрации по странам	86
Создание расписаний	86
Настройка исключений при блокировке пользовательского VPN-трафика	87
Правила трансляции адресов (NAT)	90
Создание правил трансляции адресов	90
Копирование, изменение и удаление правил	93
Просмотр состояний правил	96
Просмотр срабатываний правил	97
Сброс счетчиков срабатываний правил	99
Поиск правил в журнале событий	100
Глава 5. Работа с группами объектов	101
О группах объектов	102
Группы адресов открытой сети	104
Группы протоколов	105
Группы сетевых интерфейсов	107
Группы устройств защищенной сети	109
Группы стран	110
Списки дополнений и исключений для стран	111

Списки блокировки IP-адресов	113
Глава 6. Поиск по правилам и группам	114
Приложение А. Ограничения в названиях объектов	116
Приложение В. Описание ошибок в журнале ошибок импорта из ViPNet Policy Manager	117
Приложение С. Возможные неполадки	125
Неизвестная ошибка	125
Не отображаются счетчики срабатывания правил	125
Длительная инспекция правил	126
Недоступен вход в ViPNet Prime PMM	127
Ошибка импорта шаблона политик из ViPNet Policy Manager	128
После миграции не принимаются политики на координаторе поколения ViPNet 4	128
Приложение D. История версий	130
Что нового в версии 1.10	130
Что нового в версии 1.9.1	131
Что нового в версии 1.9	131
Что нового в версии 1.8	131
Что нового в версии 1.7	133
Что нового в версии 1.6	134
Что нового в версии 1.5.2	135
Что нового в версии 1.5.1	135
Что нового в версии 1.5.0	135
Что нового в версии 1.4	136
Что нового в версии 1.3.1	136
Что нового в версии 1.3	137
Что нового в версии 1.2	139
Что нового в версии 1.1.1	139
Приложение Е. Термины и сокращения	141



Введение

О документе	7
О модуле ViPNet Prime Policy Management	8
Что нового в версии 1.11	9
Системные требования	10
Совместимые продукты ViPNet	11
Комплект поставки	13
Связанные документы	14
Обратная связь	15

О документе

Документ описывает, как управлять политиками безопасности в защищенной сети с помощью ViPNet Prime Policy Management.

Документ предназначен для администраторов ViPNet Prime.

Соглашения документа

Обозначение	Описание
Название	Название элемента интерфейса: окна, вкладки, поля, кнопки, ссылки
Клавиша+Клавиша	Сочетание клавиш: нажмите первую клавишу и, не отпуская её, нажмите вторую
Меню > Команда	Последовательность элементов или действий
Код	Имя файла, путь, фрагмент кода или команда в командной строке



Примечание. В документе могут присутствовать снимки интерфейса из предыдущих версий продукта. Поэтому некоторые элементы интерфейса, которые не влияют на понимание текста, могут выглядеть не так, как в продукте.

О модуле ViPNet Prime Policy Management

ViPNet Prime Policy Management (далее — ViPNet Prime PMM) — модуль системы ViPNet Prime для централизованного управления политиками безопасности устройств в [продуктах ViPNet](#).

В политики безопасности входят:

- правила фильтрации трафика;
- правила трансляции адресов;
- команды по управлению счетчиками срабатывания правил;
- режим работы межсетевого экрана типа «Д» для ViPNet Coordinator IG;
- настройки обработки прикладных протоколов (ALG);
- список дополнений и исключений IP-адресов для корректировки списка IP-адресов выбранных стран;
- список блокировки IP-адресов.

Администратор управляет устройствами в модуле следующим образом:

- 1 Устройство автоматически добавляется в ViPNet Prime PMM, когда на него назначается лицензия в модуле VPN.
- 2 Администратор в модуле ViPNet Prime PMM добавляет устройства в политики и списывает лицензию «Policies nodes». После этого отправляет политики на устройства.
- 3 Устройства получают и применяют политику. На устройствах правила из модуля ViPNet Prime PMM имеют приоритет над правилами, которые заданы локально.

Информация о действиях администраторов в модуле записывается в журнал событий. Подробнее см. «ViPNet Prime. Руководство администратора».

Для использования модуля и управления политиками устройств [требуются лицензии](#).

Что нового в версии 1.11

- **Централизованное управление настройками регистрации IP-пакетов и сессий**

Теперь вы можете задать пользовательские настройки регистрации IP-пакетов или сессий для правил, слоев, политики. Также вы можете оставить системные значения, зависящие от действия правила. Подробнее см. [Параметры регистрации сессий и IP-пакетов](#).

- **Загрузка актуальной базы данных по странам**

Теперь вы можете поддерживать соответствие базы данных по странам на целевых устройствах и в ViPNet Prime Policy Management: загружать актуальную базу в ViPNet Prime Policy Management и назначать ее для использования в организациях. Подробнее см. [Работа с базой данных стран](#).

- **Создание групп стран**

Теперь вы можете [создавать группы стран](#) и использовать их в правилах фильтрации по странам.

- **Защита от отправки правил фильтрации по странам и списков блокировки IP-адресов для устройств, которые не поддерживают работу с ними**

Подробнее см. [Отправка дополнений на целевые устройства](#).

Системные требования

Системные требования см. в «ViPNet Prime. Руководство по установке».

Поддерживается:

- Импорт правил фильтрации и трансляции адресов из ПО Check Point версии R77.30 и ниже.
- Импорт правил фильтрации и трансляции адресов из ViPNet Policy Manager версии 4.5.5.
- Назначение на одно устройство в одной политике безопасности не более 7000 правил.

Совместимые продукты ViPNet

Модуль ViPNet Prime PMM версии 1.11 работает в составе ViPNet Prime 1.9.14 и устанавливается на один компьютер с ним.

- ПО ViPNet поколения 5:
 - ViPNet Coordinator HW 5 версии 5.1.2 и выше.
 - ViPNet Coordinator IG версии 5.1.0 и выше.
 - ViPNet Coordinator KB 5 версии 5.0.0 и выше.
 - ViPNet Client 5 for Linux версии 5.0.0 и выше.



Внимание! ViPNet Client 5 for Linux версии 5.0.0 принимает политики безопасности, если на узле установлена лицензия «Client for Linux» и дистрибутив ключей *.dst.

- ViPNet Client 5 for Windows версии 5.0.0 и выше.
 - ViPNet Client 5 for Android версии 5.2.1 и выше.
 - ViPNet Client 5 for iOS версии 5.0.2 и выше.
 - ViPNet Client 5 for macOS версии 5.0.2 и выше.
 - ViPNet Client 5 для ОС Аврора версии 5.1.0 и выше.
- ПО ViPNet поколения 4:
 - ViPNet xFirewall версии 5.6.2 и выше.



Внимание! В ViPNet Prime PMM нет управления некоторыми настройками устройств, которые автоматически устанавливаются на устройстве при получении политики из ViPNet Prime PMM, например настройки IPS и антивируса.

- ViPNet Coordinator HW версии 4.5.4 и выше.
Не принимаются политики, содержащие правила с действием **Отклонять и отправлять сообщение**.
- ViPNet Coordinator IG версии 4.5.1 и выше.
Не принимаются политики, содержащие правила с действием **Отклонять и отправлять сообщение**.
- ViPNet Coordinator KB 4 версии 4.3.4 и выше.
Не принимаются политики, содержащие правила с действием **Отклонять и отправлять сообщение**.
- ViPNet Client 4U for Android версии 4.0.0 и выше.
- ViPNet Client 4U for iOS версии 4.4.0 и выше.

- ViPNet Client 4U for macOS версии 4.4.0 и выше.
- ViPNet Client 4U for Windows версии 4.14 и выше.
- ViPNet Client for Windows версии 4.5.3 и выше.
- ViPNet Client для ОС Аврора 4.0.1 и выше.
- ViPNet Client 4U for Linux версии 4.15 и выше с ограничениями:
 - Не принимаются политики, содержащие правила с действием **Отклонять и отправлять сообщение**.
 - Поддерживаются только локальные правила защищенной сети.



Примечание. Правила фильтрации локального трафика открытой сети могут применяться на устройствах с ViPNet EndPoint Protection Агент.

Комплект поставки

- Установочные файлы в архиве `pmm.tgz`.

Об установке модуля см. в «ViPNet Prime. Руководство по установке». Модуль устанавливается на одном компьютере с ViPNet Prime.

- Файл для классификатора DPI — `ipoque_PACE2_dpid.xml`.
- Утилита `InfotecsConfwizEnricher.exe` для адаптации правил из Check Point перед импортом в ViPNet Prime PMM.
- Скрипт `export-data-from-vipnet-policy-manager.ps1` для экспорта из базы данных ViPNet Policy Manager. Скрипт расположен в папке `maintenance` в архиве `pmm.tgz`.
- «ViPNet Prime Policy Management. Руководство администратора» в формате PDF.
- Лицензионные соглашения на компоненты сторонних производителей, которые использовались при разработке ViPNet Prime Policy Management, см. в ZIP-архиве «ViPNet Prime Policy Management. Руководство администратора (Приложение)».

Связанные документы

Вы можете дополнительно ознакомиться с документами:

- ViPNet Prime. Руководство по установке.
- ViPNet Prime. Руководство администратора.
- ViPNet Prime Network Visibility System. Руководство администратора.

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

Начало работы

Лицензирование	17
Управление доступом и подключение	18
Интерфейс ViPNet Prime Policy Management	19
Порядок работы	21

Лицензирование

Администратор с учетной записью владельца организации или администратора организации может использовать модуль ViPNet Prime Policy Management только при наличии лицензии «Policy Management module» в файле общей лицензии *.itcslic.

Для управления устройствами в модуле требуется лицензия на количество устройств «Policies nodes». Она позволяет отправлять политики безопасности на устройства защищенной сети.

Проверьте в разделе  **Главная консоль > Лицензии**, что лицензии «Policies nodes» распределены в организацию.

Если лицензии отсутствуют, их количество недостаточно или истек срок действия, а раздел **Лицензии** отсутствует в интерфейсе для вашей учетной записи администратора, обратитесь к суперадминистратору или оператору Prime поставщика услуг ViPNet Prime. Если раздел **Лицензии** доступен, обратитесь в ИнфоТеКС. См. «ViPNet Prime. Руководство администратора», «Управление лицензиями».

Управление доступом и подключение

В модуле ViPNet Prime PMM действуют следующие роли ViPNet Prime:

- Суперадминистратор — имеет доступ ко всем организациям. Подключает модуль к ViPNet Prime, после чего модуль отображается в веб-интерфейсе.
- Владелец организации и администратор организации — имеют доступ только к организациям, в которые назначены. Их полномочия в модуле политик одинаковые.
- Аудитор устройств — просмотр настроек и правил в организациях, в которые назначен.

Об управлении доступом см. «ViPNet Prime. Руководство администратора», раздел «Разграничение полномочий на основе ролей администраторов».

Перед началом работы суперадминистратор в ViPNet Prime подключает модуль. Иначе модуль не будет отображаться в веб-интерфейсе. См. «ViPNet Prime. Руководство администратора», раздел «Подключение модулей к ViPNet Prime».

Для подключения к ViPNet Prime Policy Management:

- 1 В браузере введите:

`https://<доменное имя ViPNet Prime>:<порт>.`

- 2 Введите имя учетной записи и пароль.

- 3 Нажмите **Войти**.

- 4 Слева выберите **Policy Management** .

- 5 Если вы управляете несколькими организациями, выберите организацию.

Интерфейс ViPNet Prime Policy Management

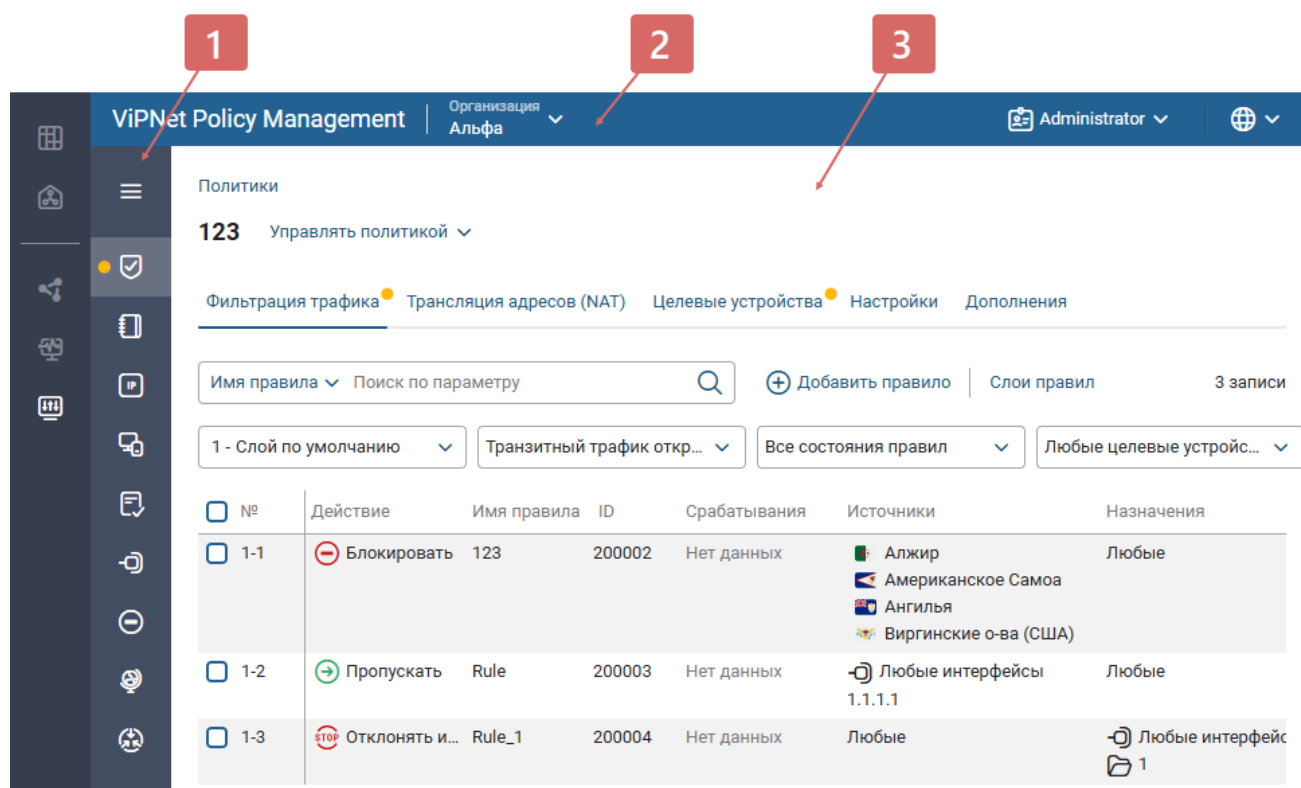


Рисунок 1. Интерфейс ViPNet Prime Policy Management

Цифрами на рисунке обозначены:

1 Панель навигации. Состоит из двух частей:

- Панель переключения между модулями.
- Панель переключения между разделами модуля:
 - **Политики безопасности > Политики** — для создания правил фильтрации трафика и трансляции адресов, просмотра и сброса счётчиков срабатывания правил, изменения режима работы координатора типа «Д», задания настроек прикладных протоколов, добавления списка блокировки IP-адресов и списка дополнений и исключений для стран.
 - **Политики безопасности > Журнал инспекций** — для просмотра и скачивания результатов [проверки правил на согласованность в политике](#).
 - **Группы объектов** — для объединения в группы устройств, их сетевых интерфейсов, адресов открытых устройств и протоколов для использования в правилах фильтрации

и трансляции адресов, стран, создания списков дополнений и исключений для стран и списков блокировки IP-адресов.

- **Сервис > Интеграция** — для импорта правил из Check Point и ViPNet Policy Manager и загрузки файла классификатора [DPI](#).

2 Панель заголовка страницы. Содержит:

- Список организаций, доступных для управления. При выборе организации отображаются все политики безопасности, которые были созданы в ней. Политики безопасности создаются на уровне организации, без возможности создания для конкретного подразделения. Если выбрать подразделение, то отображаются политики для организации.
-  — смена пароля учетной записи администратора и выход из учетной записи администратора. Если администратор был неактивен более 15 минут, сессия завершится автоматически.

3 Содержимое выбранного раздела.

Порядок работы

- 1 В ViPNet Prime назначьте узлу [Control Center](#) функцию управления политиками безопасности.
- 2 В ViPNet Prime PMM [загрузите классификатор DPI](#) (не обязательно).
- 3 Вы можете [импортировать правила из Check Point](#) (не обязательно). Правила импортируются с учетом деления на политики безопасности (секции Check Point).
- 4 Вы можете [импортировать правила из ViPNet Policy Manager](#) (не обязательно). Правила шаблона импортируются в отдельный слой политики безопасности. Все шаблоны ViPNet Policy Manager — в одну политику безопасности в виде отдельных слоев.
- 5 [Создайте политики безопасности](#).
- 6 [Отправьте политики безопасности на устройства](#).

2

Предварительные действия

Назначение функции управления политиками безопасности	23
Особенности обновления версий	24
Увеличение оперативной памяти при 20000 правил	26
Загрузка классификатора DPI	27
Работа с базой данных стран	28
Импорт политик и правил из Check Point	32
Импорт шаблонов политик безопасности из ViPNet Policy Manager	37

Назначение функции управления политиками безопасности

Чтобы управлять политиками безопасности на устройствах поколения ViPNet 4 с помощью ViPNet Prime PMM, назначьте на узел центра управления ViPNet Prime (далее — Control Center) функцию управления политиками безопасности. В результате вы сможете рассылать политики безопасности на устройства поколения ViPNet 4 всех организаций.

Эта настройка определяет, с какого узла устройства поколения ViPNet 4 будут получать политики безопасности. Для поколения ViPNet 5 узлы всегда получают политики от узла Control Center, независимо от того, какой узел выбран в качестве центра управления политиками безопасности.

Если вы выполнили миграцию из ViPNet Administrator, для узлов поколения ViPNet 4 вы можете оставить управление политиками безопасности из ViPNet Policy Manager до переноса шаблонов политик из ViPNet Policy Manager в ViPNet Prime PMM. Для этого вам нужно в качестве центра управления политиками безопасности выбрать узел с ViPNet Policy Manager. В этом случае узлы поколения ViPNet 4 не будут принимать политики, сформированные и отправленные из ViPNet Prime PMM.

Для успешного применения политик безопасности на устройствах с ViPNet Client 4U for Linux установите связи между пользователями узла центра управления политиками безопасности и узлов (с дистрибутивами ключей *.dst), на которые будут рассылаться политики. Подробнее см. в документе «ViPNet Prime. Руководство администратора».

Чтобы назначить [узлу Control Center](#) функцию управления политиками безопасности:

- 1 Войдите в ViPNet Prime как суперадминистратор, владелец организации или администратор организации.
- 2 Если вы управляете несколькими организациями, вверху выберите организацию.
- 3 Выберите **ViPNet VPN**  > **Сервис** > **Сервисные функции**.
- 4 Выберите **Центр управления политиками безопасности**.
- 5 Нажмите .
- 6 Выберите узел Control Center — ViPNet Client 5 for Linux (с дистрибутивом ключей *.dst или *.ds5) (рекомендуется версия 5.1.3 или выше) для управления узлами поколения ViPNet 4 с помощью ViPNet Prime PMM.
- 7 Выберите режим распространения политик безопасности:
 - **Распространять на все устройства сети** — для управления [шлюзами безопасности](#) и другими [поддерживаемыми устройствами](#).
 - **Распространять только на координаторы сети** — для управления только координаторами.
- 8 Нажмите **Сохранить**.

Особенности обновления версий

Обратная совместимость между разными версиями ViPNet Prime не поддерживается, поэтому обновляйте ViPNet Prime Policy Management последовательно с предыдущей версии.

- **1.10 → 1.11**

Обновите ПО модуля только с предыдущей версии.

- **1.9.1 → 1.10**

Обновите ПО модуля только с предыдущей версии.

- **1.9 → 1.9.1 или 1.6 → 1.9.1**

Вы можете обновить ViPNet Prime Policy Management с версии 1.9 или 1.6.

- **1.8 → 1.9 или 1.6 → 1.9**

Вы можете обновить ViPNet Prime Policy Management с версии 1.9 или 1.6.

При обновлении ViPNet Prime PMM происходит обновление СУБД. При обновлении информация о проведенных инспекциях не сохраняется. Статусы **Инспекция пройдена** и **Инспекция не пройдена** зависят от результатов проведенных инспекций, поэтому при обновлении меняются на **Изменена**.

- **1.7 → 1.8**

Если вы импортировали политики из Check Point и требуется сохранить отчет по импорту, скачайте его до обновления модуля ViPNet Prime PMM на версию 1.8.

- **1.6 → 1.7**

Обновите ПО модуля только с предыдущей версии.

- **1.5.2 → 1.6**

Обновите ПО модуля только с предыдущей версии. При отсутствии лицензии «Policy Management module» отобразится сообщение «Лицензия отсутствует. ViPNet Prime Policy Management работает в режиме ограниченной функциональности». Все действия в модуле будут доступны, кроме отправки политики безопасности на устройство.

- **1.5.1 → 1.5.2**

Скачайте журнал ошибок последней загрузки политик из Check Point. После обновления на версию 1.5.2 журнал удалится. Информация о последней загрузке не будет отображаться.

- **1.5.0 → 1.5.1**

- Скачайте журнал ошибок последней загрузки политик из Check Point. После обновления на версию 1.5.1 журнал удалится. Информация о последней загрузке не будет отображаться.
- После обновления заново подтвердите подключение модуля к ViPNet Prime.

См. «ViPNet Prime. Руководство администратора», раздел «Подключение модулей к ViPNet Prime».

- Период расписаний правил ранее 1970 года изменится на период с 01.01.1970 00:00 по 02.01.1970 00:00. Измените расписания и отправьте изменения на устройства.
- 1.2 → 1.5.x или 1.4 → 1.5.x
 - Скачайте журнал ошибок последней загрузки политик из Check Point. После обновления журнал удалится. Информация о последней загрузке не будет отображаться.
 - При переходе с версий 1.2 или 1.4 на версию 1.5.x, после установки версии 1.5.x не запускайте модуль ViPNet Prime PMM.
 - После обновления заново подтвердите подключение модуля к ViPNet Prime.

- 1.3 → 1.3.1 → 1.4

Для обновления на версию 1.4 последовательно установите все предыдущие версии в указанном порядке.

После обновления на версию 1.4 подтвердите подключение модуля к ViPNet Prime.

- 1.2 → 1.3

Перед обновлением с версии 1.2 на версию 1.3 отправьте изменения политик на устройства. Все правила будут перенесены в одну политику безопасности, в слои по умолчанию. В качестве целевых устройств будут перечислены устройства, на которые были назначены правила в версии 1.2.

Если у вас более 20000 правил:

- [увеличьте оперативную память](#) для MongoDB на 1 Гб;
- после обновления убедитесь, что веб-интерфейс модулей ViPNet Prime открывается;
- для уменьшения вычислительной нагрузки на сервер ViPNet Prime разделите политику так, чтобы в новой политике было одно целевое устройство.

Увеличение оперативной памяти при 20000 правил

Увеличьте оперативную память для MongoDB при 20000 правил и более:

- 1 Остановите модуль ViPNet Prime PMM.
- 2 Откройте для редактирования файл `pmm.compose.yaml`.
- 3 В секции `pmm-mongo` увеличьте значение параметра `mem_limit` на 1 Гб и сохраните файл.
- 4 Запустите модуль ViPNet Prime PMM.

Загрузка классификатора DPI

Для фильтрации трафика по содержимому (DPI) загрузите файл классификатора DPI в формате XML.

Классификатор DPI содержит набор приложений и прикладных протоколов. У классификатора есть версия, которая определяет этот набор. Классификатор DPI загружается в организацию и применяется к устройствам этой организации.

В разных организациях вы можете использовать классификаторы DPI разных версий. Если версия классификатора DPI на устройстве и версия, которая загружена в организацию в модуле ViPNet Prime PMM, будут различаться, то отправленная политика:

- на ViPNet xFirewall не будет принята;
- на ViPNet Coordinator HW 5 будет принята и применена частично: трафик будет фильтроваться по приложениям, прикладным протоколам и их группам, которые определяются классификатором DPI из состава ПО координатора (при наличии лицензии на функции DPI).
- на ViPNet Coordinator HW 4 будет принята и применена частично: без настроек DPI в правилах.

Если в политике безопасности, полученной ViPNet Coordinator KB 4, есть классификатор DPI, политика будет принята, но если в правилах используется параметр DPI, политика будет отброшена полностью.

Файл XML входит в комплект поставки ViPNet Prime Policy Management.

Чтобы загрузить классификатор DPI:

- 1 [Войдите в ViPNet Prime как суперадминистратор, владелец организации или администратор организации.](#)
- 2 Выберите организацию.
- 3 Выберите **Интеграция**.
- 4 Выберите вкладку **Классификатор DPI**.
- 5 Выберите **Загрузить классификатор DPI**.
- 6 Для загрузки в другую организацию скачайте ранее загруженный файл классификатора DPI.



Внимание! Если в правилах ViPNet Prime PMM использовались приложения и протоколы из классификатора DPI предыдущей версии, а потом вы загрузили классификатор новой версии, в котором эти приложения и протоколы отсутствуют, то вручную измените правила. Автоматически такие устаревшие протоколы и приложения из правил не удаляются.

Работа с базой данных стран

Чтобы создавать правила по странам, загрузите в ViPNet Prime Policy Management актуальную базу данных по странам:

- 1 Скачайте базу данных стран с сервера обновлений.
- 2 Проверьте электронную подпись файла базы данных стран.
- 3 Загрузите базу данных стран.
- 4 Назначьте базу данных стран в организацию.

Скачивание базы данных стран с сервера обновлений

Вы можете скачать базу данных стран (файл *.zip) и откреплённую электронную подпись (далее — ЭП) (файл *.zip.sig) с сервера обновлений.

Подключение к серверу обновлений выполняется по протоколу HTTPS/TLS с односторонней аутентификацией и шифрованием передаваемых данных. В Windows данный сертификат установлен по умолчанию.

Имя и пароль учётной записи для доступа к серверу обновлений выдает ИнфоТеКС при формировании лицензии.

Чтобы скачать базу данных стран с сервера обновлений:

- 1 Введите в адресной строке браузера: <https://updateids.infotecs.ru>.
- 2 Введите имя пользователя и пароль из письма, которое вы получили при запросе лицензии.
- 3 На панели слева выберите **ViPNet Prime**.
- 4 С помощью фильтра найдите базу данных стран для версии вашего ViPNet Prime Policy Management.
- 5 Нажмите на нужный файл обновления и его ЭП. Начнётся скачивание выбранных файлов.

Проверка электронной подписи базы данных стран с помощью ViPNet PKI Client

Перед загрузкой базы данных стран в ViPNet Prime Policy Management необходимо проверить откреплённую электронную подпись файла.

Для проверки ЭП рекомендуется использовать ViPNet PKI Client. Скачать ViPNet PKI Client и документацию можно с сайта infotecs.ru. Вместе с установочным файлом будет предоставлена демо-лицензия на 6 месяцев.

Чтобы проверить ЭП базы данных стран:

- 1 В главном окне программы ViPNet PKI Client выполните одно из действий:
 - Нажмите **Выбрать файлы** и выберите файл с базой данных стран и файл *.sig (*.detached.sig).
 - Перетащите файл базы данных стран и файл *.sig (*.detached.sig) в главное окно программы.
- 2 Нажмите на значок  напротив имени файла *.sig (*.detached.sig).

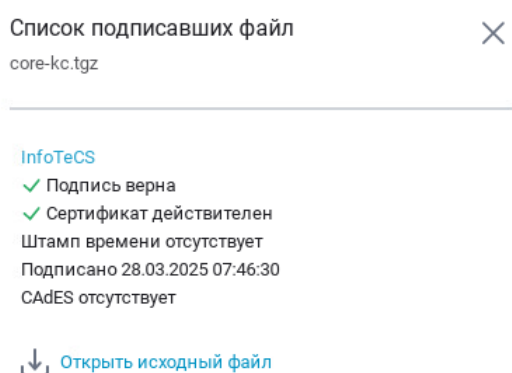


Рисунок 2. Результат проверки ЭП файла

Загрузка базы данных стран

Чтобы получить базу данных стран вам потребуются данные учетной записи для доступа на сервер обновлений, получите их в ИнфоТеКС. При обновлении с ViPNet Prime Policy Management 1.10 останется база данных стран по умолчанию, вы можете загрузить новую.

- 1 [Войдите в ViPNet Prime как суперадминистратор](#).
- 2 Выберите организацию.
- 3 Выберите **Интеграция**.
- 4 Выберите вкладку **База данных стран**.
- 5 Выберите
 - **Загрузить базу данных** — если первый раз загружаете базу данных.
 - **Сменить базу данных** — если обновляете базу данных.
- 6 Выберите файл с базой *.zip и нажмите **Открыть**. Вы можете загрузить файл не более 200 Мбайт.

Начнется загрузка базы данных стран.

После загрузки базы данных у владельцев и администраторов организаций отобразится оповещение о появлении новой базы данных стран.

Если при загрузке базы данных стран появляется ошибка, связанная с содержанием базы данных, обратитесь в ИнфоТеКС.

Если при загрузке базы данных стран в ViPNet Prime Policy Management появляется уведомление, что для некоторых стран отсутствуют названия на одном из языков, названия будут отображаться на том языке, на котором они доступны.

Вы не можете удалить загруженную базу данных стран, но можете загрузить новую.

Назначение базы данных стран в организацию

- 1 Войдите в ViPNet Prime как суперадминистратор, владелец или администратор организации.
- 2 Выберите организацию.
- 3 Выберите **Интеграция**.
- 4 Выберите вкладку **База данных стран**.
- 5 В разделе **Назначение базы данных стран**:
 - в строке организации напротив организации нажмите  **Назначить базу данных стран**.
 - выберите организацию и на панели справа нажмите  **Назначить актуальную базу**.
- 6 Подтвердите назначение.

При назначении базы в организацию выполняется проверка правил, групп и списков дополнений и исключений на соответствие загружаемым кодам.
- 7 Статус, указанный напротив организации, сменится на **Назначена**, будет указана версия базы, дата и время назначения.

Если в новой базе стран нет каких-то используемых кодов стран, при назначении базы в организацию появится сообщение об ошибке. Вы сможете скачать отчет со списком объектов, в которых используются отсутствующие коды стран. Для этого выберите организацию и на панели справа нажмите **Скачать отчет**. Установите другую базу данных стран или удалите эти коды из объектов. Если на целевом устройстве и в ViPNet Prime Policy Management не совпадает список кодов стран, возможны трудности при создании правил из-за отсутствия используемых кодов в одной из баз. Обновите до последней версии базу данных стран на устройстве и в ViPNet Prime PMM.

Чтобы посмотреть информацию о загруженной и используемой базе стран в организации:

- 1 Войдите в ViPNet Prime как суперадминистратор, аудитор, владелец или администратор организации.
- 2 Выберите организацию.

- 3 Выберите **Интеграция**.
- 4 Выберите вкладку **База данных стран**.
- 5 Выберите организацию и посмотрите информацию на панели справа.

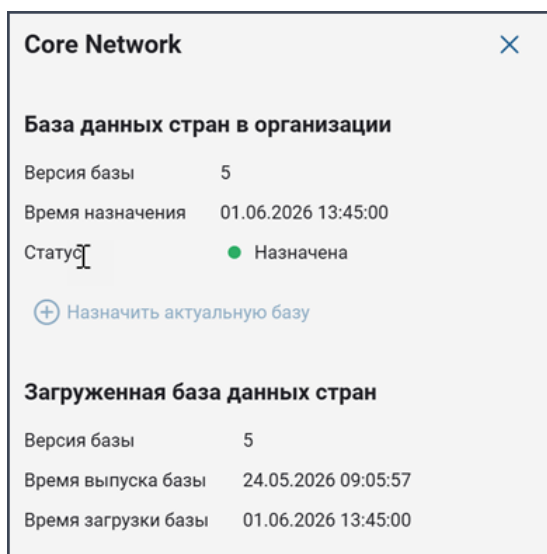


Рисунок 3. Просмотр информации о базе данных стран

Импорт политик и правил из Check Point

При переходе с оборудования Check Point на шлюзы безопасности ViPNet вы можете импортировать в модуль ViPNet Prime Policy Management правила фильтрации трафика и трансляции адресов из ПО Check Point версии R77.30 и ниже. Для этого экспортируйте правила в файлы в формате XML с помощью утилит Check Point (см. в документации Check Point). Общий размер файлов, которые вы можете одновременно загрузить — 200 Мбайт.

Порядок действий перед импортом в ViPNet Prime PMM

- 1 Экспортируйте данные из Check Point с помощью утилиты Check Point Confwiz. Подробнее см. в подразделе «Экспорт данных с помощью утилиты Check Point Confwiz».
- 2 Экспортируйте данные из Check Point с помощью утилиты Check Point Web Visualization Tool. Подробнее см. в подразделе «Экспорт данных с помощью утилиты Check Point Web Visualization Tool».
- 3 С помощью утилиты Confwiz Enricher (входит в комплект поставки) адаптируйте данные экспорта. Подробнее см. в подразделе «Адаптация данных из Check Point с помощью утилиты Confwiz Enricher».

Экспорт данных с помощью утилиты Check Point Confwiz

Экспортируйте файлы:

- `fw_policies.xml` (содержит тег `<table name="fw_policies">`) — правила фильтрации и правила трансляции. Если у нескольких файлов одинаковые теги `<table>`, они все не загрузятся.
- `network_objects.xml` (содержит тег `<table name="network_objects">`) — группы устройств открытой сети.
- `services.xml` (содержит тег `<table name="services">`) — группы протоколов.
- `policies_collections.xml` — выбор отдельных политик для импорта, иначе будут импортированы все политики безопасности.

Экспорт данных с помощью утилиты Check Point Web Visualization Tool

Экспортируйте данные с помощью утилиты Check Point Web Visualization Tool, если в правилах Check Point используются сетевые объекты:

- `cluster_member;`
- `gateway_ckp;`
- `gateway_cluster;`

- `host_ckpt`.

Адаптация данных из Check Point с помощью утилиты Confwiz Enricher

Адаптируйте данные экспорта с помощью утилиты Confwiz Enricher (входит в комплект поставки). Для этого в командной строке Windows введите:

```
Infotecs.ConfwizEnricher.exe --confwiz-dir="имя_папки_с_базой_данных"
--wvt-dir="имя_папки_с_XML-файлами" --out-dir=.\out --disassemble-network-interfaces
--remove-duplicates
```

Где:

- `--confwiz-dir` — обязательный параметр, задает имя папки с данными из Check Point Confwiz. По умолчанию папка `database`. В папке должны присутствовать файлы XML из Check Point Confwiz:
 - o `fw_policies.xml`;
 - o `network_objects.xml`;
 - o `services.xml`;
 - o `policies_collections.xml` (опционально).
 - `--wvt-dir` — обязательный параметр, задает имя папки с файлом XML из Check Point Web Visualization Tool. По умолчанию папка `xml`. В папке должен присутствовать файл `network_objects.xml` с данными сетевых объектов из Check Point Web Visualization Tool.
 - `--out-dir` — обязательный параметр, задает имя выходной папки, в которую будут записаны дополненные XML-файлы для последующей загрузки в модуль ViPNet Prime PMM. По умолчанию папка `out`.
 - `--disassemble-network-interfaces` — поиск сетевых объектов с сетевыми интерфейсами в файле `network_objects.xml` утилиты Check Point Confwiz, чтобы в составе группового объекта указать IP-адреса сетевых интерфейсов объектов Check Point типа `host_plain`.
 - `--remove-duplicates` — удаление дубликатов внутри правила.
 - `--convert-negate-cell` — преобразование параметров правила, в которые добавлено два или более значений и применен параметр «not in»:
 - o В файле `network_objects.xml` добавляется объект `network_object_group_<порядковый номер>_<метка времени unix epoch>` типа `network_object`, содержащий исходные значения из правила.
 - o В файле `services.xml` добавляется объект `Exclusion_service_group_<порядковый номер>_<метка времени unix epoch>` типа `service_group`, содержащий исходные значения из правила.
 - o В файле `fw_policies.xml` исходные значения параметров правила `src`, `dst`, `services` заменяются на добавленные объекты.
- При совпадении значений в параметре правила одна группа может быть использована несколько раз. Если нет группы с необходимыми параметрами, создается новая группа.
- `--help` — показать справку.

Пример:

```
Infotecs.ConfwizEnricher.exe --confwiz-dir="D:\CPConfwiz\database" --wvt-dir="D:\Web  
Visualization Tool\xml" --out-dir=.out --disassemble-network-interfaces  
--remove-duplicates --convert-negate-cell
```

Импорт правил из Check Point

1 Подключитесь к веб-интерфейсу.

2 Выберите организацию.

3 Выберите **Интеграция > Импорт**.

4 Выберите вкладку **Импорт**.

5 Нажмите **Импортировать > Из Check Point**.

6 Нажмите **Загрузить**.

Во время загрузки объекты Check Point преобразуются в [группы объектов ViPNet Prime PMM](#).

7 Выберите файлы с политиками безопасности.

8 Чтобы импортировать правила типа Automatic NAT, выберите **Сохранить правила Check Point типа Automatic NAT в отдельной политике**. После импорта вы сможете изменить их и перенести в основную политику безопасности.

9 Просмотрите выбранные политики безопасности.

Если название объекта в Check Point совпадает с названием существующей группы ViPNet Prime PMM, выберите одно из действий:

- **Создать новую группу PMM** — чтобы преобразовать объекты Check Point в новые группы PMM.
- **Использовать группы PMM** — чтобы не импортировать одноименные объекты Check Point и использовать существующие группы ViPNet Prime PMM.

Если имена совпадают, вы можете использовать существующие группы объектов или создать новые группы. При этом не проверяется, изменялся ли состав объекта Check Point и существующей группы. После импорта политик вы можете просмотреть, как сопоставляются импортированные группы объектов с исходными объектами Check Point.

10 Нажмите **Импортировать**.

Дождитесь окончания импорта. Отобразится информация о количестве импортированных политик безопасности.

11 Если импортированы не все правила — последний импорт имеет статус **Частично импортировано**, просмотрите журнал ошибок. Для этого в строке **Журнал** нажмите **Скачать**.

Скачается файл в формате XLSX, в котором указаны уровень ошибки, имя файла Check Point и номер строки в файле, из-за которой возникла ошибка загрузки файла.

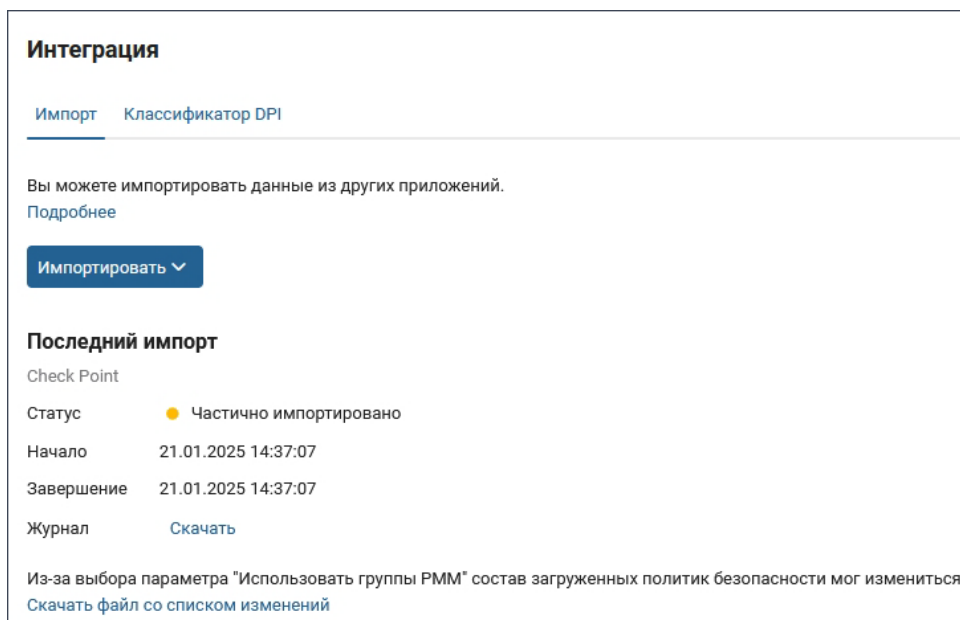


Рисунок 4. Импорт правил

Если статус импорта политики **Не импортировано**, отчет не формируется.

- 12 Чтобы скачать и просмотреть изменения импортированных групп объектов относительно исходных объектов Check Point, нажмите **Скачать файл со списком изменений**. Скачается файл `Group-changes-CP_<дата и время формирования файла (от начала импорта)>`.

- 13 [Назначьте политики на устройства.](#)

- 14 [Инспектируйте правила на согласованность.](#)

- 15 [Отправьте политики на устройства.](#)

После импорта политик вы можете просмотреть в файле `Group-changes-CP_<дата и время формирования файла (от начала импорта)>`, как сопоставляются загруженные группы объектов с исходными объектами ViPNet Prime. Файл содержит таблицу со столбцами:

- **Имя группы (Источник)** — имя исходного объекта из Check Point.
- **Имя группы (PMM)** — имя существующей группы объектов.
- **Тип группы (PMM)** — тип пользовательской группы объектов.
- **Состав (Источник)** — состав исходного объекта из Check Point.
- **Состав (PMM)** — состав существующей группы объектов.
- **Инверсия (Check Point)** — преобразование над объектом правила в Check Point, со значением «все, кроме указанного». В ViPNet Prime PMM преобразуется в групповой объект с составом «любые» и исключением. Например, в Check Point в источнике указано 10.1.1.1 и к нему применен параметр «not in», что означает «все, кроме 10.1.1.1».
- **Исключения (PMM)** — групповой объект с исключением в условии правила. Исключает указанное значение из всех (любых) значений.
- **Исключения (Источник)** — групповой объект с исключением в условии правила. Исключает указанное значение из всех (любых) значений.

Имя группы (Источник)	Имя группы (PMM)	Тип группы (PMM)	Состав (Источник)	Состав (PMM)	Исключения (Источник)	Инверсия (только Check Point)	Исключения (PMM)
CP_SSL_Network_E	CP_SSL_Network_E	Протоколы	TCP: 555-777 -> 0-55	любые		нет	TCP: 555..777 -> 0..5555
MySQL	MySQL	Протоколы	TCP: any -> 3306	TCP: any -> 3306		нет	
HTTP_and_HTTPS	HTTP_and_HTTPS	Протоколы	TCP: any -> 8080	TCP: any -> 8080		нет	
PostgreSQL	PostgreSQL	Протоколы	TCP: 2000 -> 5432	TCP: 2000 -> 5432		нет	
IPSO_Clustering_M	IPSO_Clustering_M	Протоколы	TCP: any -> 1111	TCP: any -> 1111		нет	
FW1	FW1	Протоколы	TCP: any -> 256	TCP: any -> 256		нет	
FW1_log	FW1_log	Протоколы	TCP: any -> 257	TCP: any -> 257		нет	
FW1_clntauth_teln	FW1_clntauth_teln	Протоколы	TCP: any -> 259	TCP: any -> 259		нет	
FW1_clntauth_http	FW1_clntauth_http	Протоколы	TCP: any -> 900	TCP: any -> 900		нет	

Рисунок 5. Журнал изменений импортированных групп объектов из Check Point

Особенности импорта

- Правила фильтрации импортируются в раздел транзитных фильтров открытой сети.
- Если у правила фильтрации Check Point не было названия, ему будет присвоено название `imported rule (N)`, где N — номер правила по порядку в файле импорта.
- Если в правиле фильтрации Check Point были исключения, то создаются группы объектов с исключениями и добавляются в правила фильтрации. Для источников и назначений создаются группы устройств открытой сети с именами `Exclusion <название группы из источника>`.
- При импорте для параметров регистрации сессий и IP-пакетов в правилах фильтрации задаются значения по умолчанию.
- При импорте в описание правил или групповых объектов попадут только первые 1000 символов.

При импорте правил трансляции адресов из Check Point импортируются правила трансляции одного IP-адреса в другой. В параметрах трансляции не поддерживаются значения подсети или диапазона IP-адресов.

Если в правилах используются имена групп, они импортируются как группа устройств открытой сети. Имена групп трансляции источников и назначений не импортируются.

Группа объектов в правилах импортируется, если в ней заданы:

- IP-адрес, диапазон IP-адресов или адрес подсети.
- IP-адрес сетевого интерфейса.

При совпадении имен группа импортируется с именами, где N — номер группы по порядку в файле импорта:

- `Imported host N <имя группы>` — для групп адресов открытой сети;
- `Imported protocol N <имя группы>` — для групп протоколов.

При повторном импорте политик и совпадении имен добавляется индекс, например: (1) `Imported {host | protocol}`, (2) `Imported {host | protocol}` и так далее.

Вы можете одновременно импортировать политики безопасности только в разных организациях. В одной организации одновременно импортировать несколько политик безопасности из Check Point нельзя. Импорт политик может занимать до одного часа.

Импорт шаблонов политик безопасности из ViPNet Policy Manager

Импорт шаблонов политик безопасности из ViPNet Policy Manager — это один из шагов миграции продуктов поколения [ViPNet 4](#) на продукты поколения [ViPNet 5](#). Смена поколения продукта — это не обновление на новую версию, а замена продукта другим. Поэтому после миграции возврат к использованию ViPNet Policy Manager (продукта поколения ViPNet 4) не предусмотрен.

После миграции из ViPNet Administrator в ViPNet Prime вы можете импортировать в ViPNet Prime PMM шаблоны политик безопасности из ViPNet Policy Manager.

Шаблон политики безопасности ViPNet Policy Manager (далее — шаблон) — это набор правил фильтрации, правил трансляции адресов и других настроек, предназначенный для определенной политики безопасности. В ViPNet Policy Manager шаблоны назначаются на узлы и подразделения и используются для формирования результирующих политик безопасности, которые рассылаются на узлы.

Порядок импорта шаблонов:

- 1 Загрузите в ViPNet Prime лицензию на целевые устройства. Лицензии из ViPNet Policy Manager не импортируются.

- 2 Проведите миграцию данных сети из ViPNet Administrator в ViPNet Prime. Подробнее см. в документе «ViPNet Prime Migration Tool. Руководство администратора».

Без миграции данных из ViPNet Administrator вы не сможете импортировать в ViPNet Prime правила фильтрации, использующие объекты защищенной сети, и назначить полученные политики на устройства.

Миграция данных сети из ViPNet Administrator проводится в ViPNet Prime версии 1.9.6, 1.9.10 и 1.9.11.1.

- 3 Экспортируйте шаблоны из ViPNet Policy Manager версии 4.5.5. Если вы используете ViPNet Policy Manager версии ниже, обновите его до версии 4.5.5.

- 4 С помощью скрипта `export-data-from-vipnet-policy-manager.ps1` из комплекта поставки [выгрузите из базы данных ViPNet Policy Manager](#) обязательные файлы:

- `vw_PolicyTemplates.xml` — с выгрузкой из базы данных шаблонов политик;
- `vw_NetworkNodes.xml` — с выгрузкой из базы данных узлов защищённой сети;
- `vw_ManagedObjectTemplates.xml` — с выгрузкой из базы данных назначений шаблонов политик узлам защищённой сети.

Выгружайте эти данные только после экспорта шаблонов (подробнее см. в документации ViPNet Policy Manager).

5 Импортируйте шаблоны в ViPNet Prime PMM и данные из базы данных ViPNet Policy Manager.

Ограничения

- Максимальный уровень вложенности групп при импорте — 10.
- За одну операцию импорта загружайте данные из одного ViPNet Policy Manager. Это требуется, чтобы при импорте избежать логических ошибок и некорректной замены данных, вызванных несогласованностью данных (базы данных, групп и правил) из разных ViPNet Policy Manager. Чтобы импортировать данные из двух и более ViPNet Policy Manager, загружайте данные каждого из них отдельно.
- Если в ранее импортированный шаблон были внесены изменения в ViPNet Policy Manager, чтобы они применились в ViPNet Prime PMM, нужно заново загрузить измененный шаблон. Предварительно удалите ранее загруженные шаблоны.
- У загружаемых шаблонов не должны совпадать имена.
- В ViPNet Prime PMM не добавляйте целевые устройства в пустую политику безопасности, если требуется на время импорта оставить сеть защищенной. После импорта сформируйте в ViPNet Prime PMM политики безопасности, а потом применяйте их на устройствах.
- При импорте шаблонов из ViPNet Prime PMM классификатор DPI не импортируется.
- При импорте для параметров регистрации сессий и IP-пакетов в правилах фильтрации задаются значения по умолчанию.
- Максимальное время импорта — 3 часа, поэтому рекомендуется загружать шаблоны несколькими частями. Через 3 часа импорт прерывается, независимо от того, сколько шаблонов было импортировано. При загрузке шаблонов несколькими частями они будут разнесены по разным политикам.

Особенности импорта политик

- Шаблоны импортируются в одну политику безопасности со стандартным названием `import PM <дата и время>`.
- Каждый загруженный шаблон политики преобразуется в **слой политики безопасности**, который содержит таблицы с правилами. В таблицы правил переносятся правила фильтрации и правила трансляции адресов.
- Шаблоны переносятся в слои без сохранения приоритетов между собой, определенных в ViPNet Policy Manager.
- Пустые слои в таблице правил не создаются. Слой считается пустым, если в нем нет ни одного правила для переноса или они недействительны.
- Если в имени шаблона есть символы, недопустимые в имени слоя, имя слоя заменяется на «Layer_N», где N — порядковый номер импортируемого файла шаблона.
- В слое сохраняются приоритеты правил, заданные в шаблоне.
- Правилам в рамках слоя назначаются новые идентификаторы, свободные для данной организации.

Загрузка шаблонов

- 1 Подключитесь к веб-интерфейсу.
- 2 Выберите организацию.
- 3 Выберите **Интеграция > Импорт**.
- 4 Нажмите **Импортировать > Из Policy Manager**.
- 5 Нажмите **Загрузить**.
- 6 Выберите файлы с шаблонами. Общий объем загружаемых файлов не более 200 Мбайт.

Кроме шаблонов обязательно загрузите файлы `vw_PolicyTemplates.xml`, `vw_NetworkNodes.xml` и `vw_ManagedObjectTemplates.xml`, [экспортированные из ViPNet Policy Manager](#).
- 7 Убедитесь, что все файлы загрузились и нажмите **Далее**.
- 8 Выберите одно из действий:
 - **Создать новую группу PMM** — чтобы преобразовать объекты ViPNet Policy Manager в новые группы ViPNet Prime PMM. К имени группы добавится «Imported».
 - **Использовать группы PMM** — чтобы не загружать одноименные объекты ViPNet Policy Manager и использовать существующие группы ViPNet Prime PMM. Рекомендуется выбирать этот режим при загрузке шаблонов несколькими частями или при повторном импорте одинаковых наборов данных.
- 9 Нажмите **Импортировать**.

Дождитесь окончания импорта. Отобразится информация о количестве импортированных шаблонов.
- 10 Чтобы просмотреть журнал ошибок по результатам импорта, завершившегося со статусами **Частично импортировано** и **Не импортировано**, в разделе **Последний импорт** нажмите **Скачать**. Скачается файл `Import-log-PM_<дата и время формирования файла (от начала импорта)>` в формате XLSX, в котором указаны имена файлов, идентификаторы ViPNet, имена объектов и описание ошибок. Подробнее см. [Описание ошибок в журнале ошибок импорта из ViPNet Policy Manager](#).
- 11 Вы можете скачать и просмотреть изменения загруженных групп объектов относительно исходных объектов, если выбрали режим импорта **Использовать группы PMM**. Для этого после импорта нажмите **Скачать файл со списком изменений**. Скачается файл `Group-changes-PM_<дата и время формирования файла (от начала импорта)>.xlsx`.
- 12 [Распределите слои по политикам безопасности](#).
- 13 [Назначьте политики на устройства](#).
- 14 [Инспектируйте правила на согласованность](#).
- 15 [Отправьте политики на устройства](#).

Вы можете отправить изменения максимум 7000 правил, каждое из которых содержит 11 IP-адресов, на 80 устройств или объем параметров, эквивалентный указанным значениям. Если необходимо отправить большее количество изменений на устройство или появилась ошибка

при отправке изменений, разделите отправку изменений на несколько частей. Например, вы можете уменьшить:

- о количество политик, отправляемых за одну операцию;
- о количество устройств, на которые назначена отправляемая политика.

После импорта шаблонов вы можете просмотреть в файле `Group-changes-PM_<дата и время формирования файла (от начала импорта)>.xlsx`, как сопоставляются загруженные группы объектов с исходными объектами ViPNet Prime. Файл содержит таблицу со столбцами:

- **Имя группы (Источник)** — имя объекта из ViPNet Policy Manager.
- **Имя группы (PMM)** — имя существующей группы объектов.
- **Тип группы (PMM)** — тип пользовательской группы объектов.
- **Состав (Источник)** — состав исходного объекта из ViPNet Policy Manager. Устройства защищенной сети в группе устройств защищенной сети отображаются в виде VPN ID устройства или номера ViPNet-сети в шестнадцатеричном формате. Номер ViPNet-сети состоит из четырех символов, VPN ID — из восьми.
- **Состав (PMM)** — состав существующей группы объектов.
- **Инверсия (Check Point)** — заполняется только для Check Point.
- **Исключения (PMM)** — групповой объект с исключением в условии правила.
- **Исключения (Источник)** — групповой объект с исключением в условии правила. Исключает указанное значение из всех (любых) значений.

Имя группы (Источник)	Имя группы (PMM)	Тип группы (PMM)	Состав (Источник)	Состав (PMM)	Исключения (Источник)	Инверсия (только CheckPoint)	Исключения (PMM)
server	server	Адреса открытой сети	10.0.26.100, 10.0.26.100	10.0.26.100, 10.0.26.100		нет	
All_Internet	All_Internet	Адреса открытой сети	yaya.ru	8.0.0.0-8.255.255.255		нет	
DMZ_admins	DMZ_admins	Адреса открытой сети	33.3.3.3	Ext_NTP		нет	
Net_10.10.10.0	Net_10.10.10.0	Адреса открытой сети	43.24.32.42	10.10.10.0-10.10.10.255		нет	
Net_10.10.20.0	Net_10.10.20.0	Адреса открытой сети	56.65.74.76	10.10.20.0-10.10.20.255		нет	
IP-адреса 5	IP-адреса 5	Адреса открытой сети	host.com, mail.ru, pochta1.ru	host.com, mail.ru, pochta1.ru		нет	pochta1.ru
Протоколы 5	Протоколы 5	Протоколы	TCP: 7 -> 7	TCP: 7 -> 7		нет	
Протоколы 7	Протоколы 7	Протоколы	UDP: 7 -> 7	UDP: 7 -> 7		нет	
Протоколы 9	Протоколы 9	Протоколы	TCP: 1-65535 -> 1-65535	TCP: 1..65535 -> 1..65535		нет	
Протоколы 20	Протоколы 20	Протоколы	All	любые	IP: 16, IP: 19	нет	IP: 16, IP: 19
Протоколы 15	Протоколы 15	Протоколы	ICMP: 12/0	ICMP: 12/0	ICMP: 13, ICMP: 15	нет	ICMP: 13, ICMP: 15

Рисунок 6. Журнал изменений импортированных групп объектов из ViPNet Policy Manager

Экспорт данных из базы данных ViPNet Policy Manager

Скрипт `export-data-from-vipnet-policy-manager.ps1` запускается в Windows PowerShell от имени администратора ОС, у которого должна быть роль `sysadmin` для SQL-сервера, на котором расположена база данных ViPNet Policy Manager. Также вы можете использовать для подключения к базе данных встроенного пользователя «sa». Для подключения с использованием встроенного

пользователя «sa» убедитесь, что на сервере [включена смешанная аутентификация](#), учетная запись включена и для неё задан пароль.

Вы можете указать необязательные параметры:

- `-t` — "название_таблицы_или_представления" — экспортируемые таблицы и представления. Имена таблиц перечисляйте через запятую. По умолчанию экспортируются таблицы:

- o `vw_NetworkNodes,`
- o `vw_PolicyTemplates,`
- o `vw_ManagedObjectTemplates,`
- o `vw_NamedObjects,`
- o `vw_LinkedNamedObjects,`
- o `vw_LinkedSystemObjects,`
- o `vw_ViPNetData,`
- o `vw_HostData,`
- o `vw_InterfaceData,`
- o `vw_ServiceData,`
- o `vw_ScheduleData,`
- o `vw_Roles,`
- o `vw_UserAccounts,`
- o `vw_UserRoles,`
- o `vw_NetworkGroupPolicyTemplatesProxies,`
- o `vw_NetworkGroups,`
- o `vw_NodesTemplates,`
- o `vw_GroupsTemplates,`
- o `vw_ManagedObjectGroups,`
- o `vw_NodeFiles,`
- o `vw_NodeOptionStatus,`
- o `vw_NodeReceipt,`
- o `vw_NodeSendHistory.`



Внимание! Обязательно экспортируйте таблицы `vw_PolicyTemplates`, `vw_NetworkNodes` и `vw_ManagedObjectTemplates`. Они требуются для импорта шаблонов политик в ViPNet Prime Policy Management.

- `-e` "путь_к_папке" — папка для экспорта, путь может быть относительным или абсолютным. По умолчанию — папка, в которой находится скрипт.
- `-n` "схема_таблиц" — схема экспортируемых таблиц. По умолчанию — "pm".
- `-d` "имя_базы_данных" — имя базы данных, из которой экспортируются таблицы. По умолчанию — "ViPNetPolicyManager".
- `-s` "имя_сервера" — имя сервера, на котором хранится экземпляр SQL Server. По умолчанию — "localhost".

- `-i "имя_SQL_Server"` — имя экземпляра SQL Server, из которого выгружаются таблицы и представления. По умолчанию — `"WINNCCSQL"`.
- `-u "имя_пользователя"` — имя пользователя для подключения к базе данных. Укажите, если используется проверка подлинности SQL Server.
- `-p "пароль_пользователя"` — пароль для подключения к базе данных. Укажите, если используется проверка подлинности SQL Server.

Пример

```
PS>export-data-from-vipnet-policy-manager.ps1 -t vw_PolicyTemplates,
vw_NamedObjects,vw_NetworkNodes, vw_ManagedObjectTemplates -e ".\exportDirectory" -s
"localhost" -i "WINNCCSQL" -u "admin" -p "qwerty" -d "vipnetpolicymanager" -n "pm"
```

Особенности переноса правил из ViPNet Policy Manager

- Если в правиле в источниках или назначениях используется условие по VPN-узлу, необходимо, чтобы указанный узел существовал в модуле VPN.
- Если в правиле есть условия по пользователям, приложениям или прикладным протоколам (DPI), при импорте шаблона такие правила отбрасываются. В журнале ошибок регистрируется ошибка.
- Если в условии указан узел, который не найден в модуле VPN, правило не импортируется. Если в качестве объекта, указан узел, который не найден в модуле VPN, объект исключается из группы, группа импортируется без ненайденного узла.
- Расписание может быть задано только для ежедневного или еженедельного выполнения, или ограничено временным диапазоном. Иначе расписание не задается для правил, содержащих это условие, и правила выполняются всегда.
- Длина имени правила в ViPNet Prime PMM может быть не более 70 символов. Если длина имени импортируемого правила больше 70 символов, у импортированного правила имя будет состоять из первых 70 символов, полное имя будет указано в описании к правилу, но не более 1000 символов.
- Имя группы в ViPNet Prime PMM может быть не более 70 символов. Если имя импортируемой группы больше 70 символов, в ViPNet Prime PMM в имя группы попадут первые 70 символов, в описание группы попадут первые 1000 символов.
- ViPNet Prime PMM не поддерживает значения ICMP-сообщений: 1-Unassigned, 2-Unassigned, 7-Unassigned, 19-Reserved (for Security). Правила с такими значениями не импортируются.
- Пустые пользовательские группы и системная группа **Другие узлы** не импортируются. Правила с такими группами не импортируются.
- В ViPNet Prime PMM нет условия по номеру защищенной ViPNet-сети, доступного в ViPNet Policy Manager. Все устройства одной подсети импортируются в одну пользовательскую группу.

В дальнейшем при добавлении устройств в защищаемую сеть вам потребуется вручную добавлять их в эту группу.

Если устройств больше 1000, они делятся на две и более группы.

- В ViPNet Prime PMM при использовании системного объекта «Целевое устройство», невозможно указать сетевой интерфейс. Если в одном правиле ViPNet Policy Manager был использован сетевой интерфейс и системный объект «Мой узел», интерфейс не фиксируется в условиях правила.
- В ViPNet Prime Policy Management для правил локального трафика открытой сети допустимо указать интерфейс только в источниках или только назначениях правил. При переносе правил фильтрации локального трафика открытой сети с указанием интерфейса в источниках и назначениях:
 - в импортированном правиле заполняется значение интерфейса только для источника;
 - в журнал ошибок записывается ошибка с указанием того, какой интерфейс не был перенесен в назначения.
- Правило исключается из импорта, если не соответствует условиям:
 - Если источник трафика — устройства защищенной сети, его назначением может быть только группа «Целевое устройство» или «Широковещательная рассылка».
 - Если назначение трафика — устройства защищенной сети, его источником может быть только группа «Целевое устройство».
 - В ViPNet Prime Policy Management группа «Целевое устройство» не может быть одновременно источником и назначением трафика.
 - В качестве источника или назначения трафика должна быть указана группа «Целевое устройство» или «Широковещательная рассылка». Невозможно указать значение «любые» и в источнике и в назначении.

Подробнее с информацией об ошибках [можно ознакомиться в журнале ошибок](#)

Import-log-PM_<дата и время формирования файла (от начала импорта)>.

З

Работа с политиками безопасности

О политиках безопасности	46
Создание политики безопасности	48
Назначение политики безопасности на устройства	49
Назначение лицензии на устройство	50
Освобождение лицензии на устройства	51
Действия с политиками безопасности	52
Работа со слоями	54
Настройка режима работы ViPNet Coordinator IG	57
Настройка обработки прикладных протоколов	58
Дополнения политики безопасности	60
Разрешение отправки дополнительных параметров функций на целевые устройства	61
Параметры регистрации сессий и IP-пакетов	64
Инспекция политик	68
Отправка политик на устройства	72

О политиках безопасности

Чтобы управлять правилами фильтрации трафика и правилами трансляции адресов централизованно из ViPNet Prime, создайте политики безопасности (далее — политики).

С помощью политик вы можете:

- группировать наборы правил фильтрации и трансляции, например, по географическому признаку или в зависимости от организационной структуры предприятия;
- назначать правила фильтрации и трансляции на разные типы устройств. ViPNet xFirewall, ViPNet Coordinator HW и другие могут использоваться в одной политике в качестве целевых устройств.

Целевые устройства — устройства, на которые назначается политика. На одно устройство вы можете назначить одну политику.

Политика создается со слоем по умолчанию, вне слоя правила в политике создать нельзя. Слой — это набор правил фильтрации или трансляции в политике. Они помогают логически сгруппировать правила внутри политики. Слои создаются только в политике, но один слой можно добавить в несколько политик. Вы можете использовать слои, чтобы задать несколько уровней защиты в политике безопасности для разных офисов, протоколов сетевой инфраструктуры, аспектов безопасности, применять слои для разных категорий сотрудников, например, задавать более строгие правила для некоторых сотрудников.

Вы можете сгруппировать правила в один слой и назначить его в разные политики безопасности. Такой слой называется общим. Общие слои позволяют использовать одинаковые правила в разных политиках безопасности. Например, **вы можете создать слои** для корпоративных ресурсов, социальных сетей, файлообменников, игровых платформ, сторонних сервисов VPN и так далее и использовать их в разных политиках.

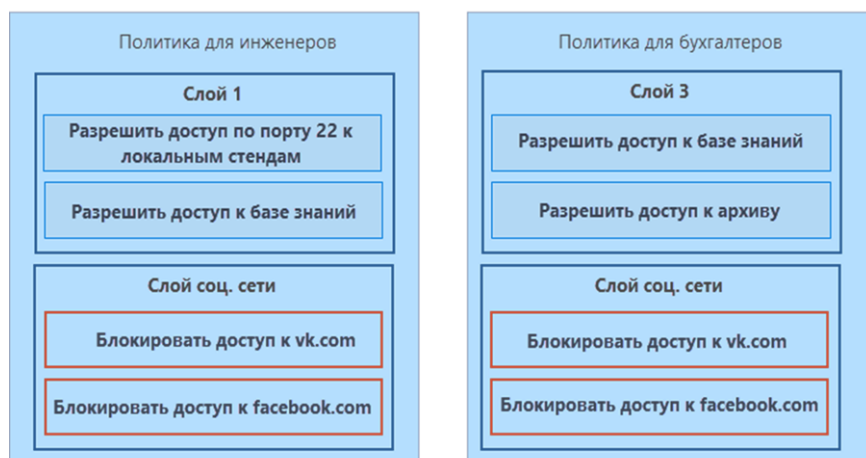


Рисунок 7. Пример использования слоев в политиках безопасности

Правила и слои в политике безопасности применяются с учетом приоритета:

- внутри слоя от высшего приоритета правила к низшему — правила с высшим приоритетом располагаются над правилами с низшим приоритетом;
- в рамках разных слоев от высшего приоритета слоя к низшему — слои с высшим приоритетом располагаются над слоями с низшим приоритетом.

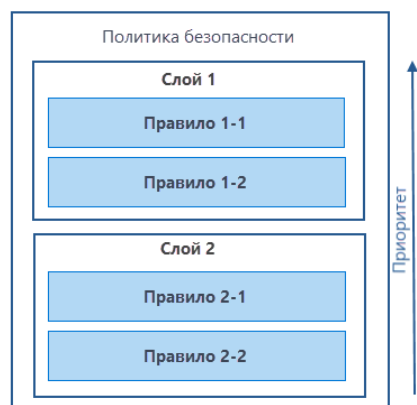


Рисунок 8. Приоритет правил и слоев

Политики безопасности имеют статусы.

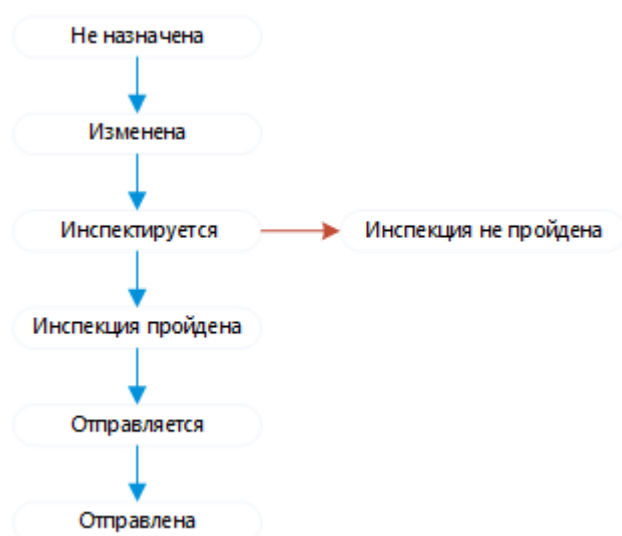


Рисунок 9. Статусы политик безопасности

Если в политике есть неотправленные на устройства изменения, отображается маркер  рядом с именем политики и разделом **Политики**. При отправке политик вы можете для каждого целевого устройства просмотреть результирующую политику безопасности и ее статус.



Внимание! С одной политикой безопасности может работать только один администратор. Иначе изменения, сделанные одновременно, могут не сохраниться или будут не видны для другого администратора.

Создание, переименование и удаление политик и другие действия в модуле вы можете просмотреть в журнале событий ViPNet Prime.

Создание политики безопасности

- 1 Подключитесь к веб-интерфейсу.
- 2 Выберите организацию.
- 3 В разделе **Политики безопасности** > **Политики** нажмите **Добавить политику**.
- 4 Введите название политики.
- 5 Нажмите **Создать**. Политика создается со слоями по умолчанию:
 - для фильтрации трафика;
 - для трансляции адресов.
- 6 Выберите политику.
- 7 Назначьте политику на устройства.
- 8 Назначьте лицензию на управляемые устройства.
- 9 Выберите слой по умолчанию или [создайте новый слой](#), чтобы объединить правила в группу.
- 10 Чтобы быстрее создавать правила, [создайте группы объектов](#).
- 11 Задайте параметры регистрации сессий и IP-пакетов по умолчанию для правил, создаваемых в [политике](#) или [слое](#).
- 12 Создайте [правила фильтрации](#) и [трансляции](#).
- 13 Для правил фильтрации [задайте расписания правил](#).
- 14 Выберите режим работы ViPNet Coordinator IG.
- 15 Чтобы передать на узлы [команду сброса счётчиков срабатывания правил](#), добавьте ее в политику безопасности.
- 16 Настройте обработку прикладных протоколов.
- 17 Разрешите отправку правил и списков на целевые устройства.
- 18 Создайте список блокировки IP-адресов и добавьте его в политику безопасности.
- 19 Создайте список дополнений и исключений для стран и добавьте его в политику безопасности.
- 20 Отправьте политику на устройства.

Назначение политики безопасности на устройства

Чтобы применить правила из политики на устройствах, назначьте политику на целевые устройства. Целевые устройства — устройства защищенной сети, которые выполняют функции межсетевого экранирования.

Вы можете назначить на целевые устройства одну политику безопасности. По умолчанию политики не назначены на целевые устройства.

Политика создается и копируется без назначенных целевых устройств. Статус скопированной политики: **Не назначена**.

Чтобы назначить политику на устройства:

- 1 Перейдите в политику.
- 2 Выберите **Целевые устройства**.
- 3 Нажмите **Добавить устройство**.
- 4 Выберите устройства. В списке отображаются устройства, на которые еще не назначена политика. Чтобы просмотреть все целевые устройства, снимите флажок **Только доступные**.
- 5 Нажмите **Добавить**.
- 6 Для управления устройствами в модуле, [назначьте лицензию на них](#).

Чтобы правила из политики назначить на конкретное целевое устройство, выполните одно из действий:

- Выберите правила и на панели сверху нажмите  > **Назначить на устройства**. Выберите **Избранные целевые устройства**, затем выберите устройства и нажмите **Сохранить**.
- Выберите правило и в столбце **Целевые устройства** нажмите . Выберите **Избранные целевые устройства**, затем выберите устройства и нажмите **Сохранить**.

Чтобы отменить политику на устройствах:

- 1 Выберите политику.
- 2 Выберите **Целевые устройства**.
- 3 Выберите устройства.
- 4 Нажмите .
- 5 Чтобы применить изменения на устройствах, нажмите **Отправить изменения на устройства**.

Назначение лицензии на устройство

Лицензия позволяет управлять устройством в модуле ViPNet Prime PMM, отправлять на устройство политику безопасности.

Чтобы назначить лицензию на управляемые устройства:

- 1 [Добавьте целевые устройства в политику безопасности.](#)
- 2 Выполните одно из действий:
 - В столбце **Лицензия** напротив устройства нажмите .
 - Выберите целевые устройства и нажмите **Управлять лицензией** > **Назначить**.
- 3 [Отправьте изменения на устройства.](#)

Освобождение лицензии на устройства

При удалении целевого устройства из политики безопасности лицензия освобождается автоматически. При необходимости вы можете освободить лицензию с устройства:

- 1 Выберите политику безопасности.
- 2 Выполните одно из действий:
 - В столбце **Лицензия** напротив устройства нажмите .
 - Выберите целевые устройства и нажмите **Управлять лицензией** > **Освободить**.
- 3 [Отправьте изменения на устройства](#).

При освобождении лицензии с устройства политика безопасности остается на устройстве. Чтобы удалить политику безопасности с устройства, [удалите целевое устройство из политики безопасности](#).

Действия с политиками безопасности

Изменение политики безопасности

- 1 Наведите указатель мыши на политику и нажмите .
- 2 Измените название политики и нажмите **Сохранить**.
- 3 Нажмите на политику. Откроется страница с правилами фильтрации трафика и трансляции адресов.
- 4 Измените состав политики.
- 5 [Отправьте изменения на устройства](#).

Копирование политики безопасности

Вы можете использовать политику в качестве шаблона для новых шлюзов безопасности или структурных подразделений организации. Политика копируется без назначенных целевых устройств. Правила в исходной политике остаются без изменения. Списки блокировки IP-адресов и списки дополнений и исключений по странам будут скопированы в новую политику из исходной. Если в исходной политике правила назначены избранным целевым устройствам, то в скопированной политике они будут иметь статус **Не указаны**.

Чтобы скопировать политику безопасности:

- 1 Выберите политику и нажмите .
- 2 Введите название политики и нажмите **Сохранить**.
- 3 Измените состав новой политики.
- 4 [Назначьте политику на устройства](#).

Разделение политики безопасности

Из политики с несколькими устройствами вы можете переместить часть устройств в новую политику. Устройства переместятся в новую политику вместе с правилами, которые назначены на них, при этом:

- В новую политику к новым правилам из исходной политики скопируются правила, назначенные на перемещаемые устройства.
- В новую политику переместятся правила, назначенные только на устройства новой политики.
- Если в исходной политике слой содержит правила только для перемещаемых устройств, то такой слой переместится из исходной политики в новую.

- Правила (или слои с правилами), назначенные на целевые устройства новой и разделяемой политики, скопируются в новую политику.
- Общий слой вместе с правилами будет распределен в новую политику.
- В новую политику скопируются список блокировки IP-адресов и список дополнений и исключений для стран, если они добавлены в политику.

Чтобы разделить политику:

- 1 Убедитесь, что в политике безопасности, которую вы хотите разделить, правила фильтрации и трансляции в слоях назначены на целевые устройства.



Внимание! Во время разделения политики безопасности не выполняйте других действий на компьютере.

- 2 Выберите политику и нажмите .
- 3 Введите название новой политики безопасности.
- 4 Выберите целевые устройства, которые будут перенесены в новую политику:
 - Оставьте в исходной политике хотя бы одно целевое устройство.
 - Выбирайте сначала устройства с наибольшим количеством уникальных правил. Если таких устройств несколько, то выберите сначала устройство с наименьшим количеством правил.
 - Выберите не более двух устройств за одно разделение.



Примечание. Если у вас более 20000 правил, для уменьшения нагрузки на сервер ViPNet Prime Policy Management разделите политику так, чтобы в новой политике было одно целевое устройство.

- 5 Нажмите **Разделить**.
- 6 Для целевых устройств сбросится лицензия. Перейдите в новую политику и **назначьте целевому устройству лицензию**.
- 7 **Отправьте изменения на устройства**. Дождитесь статуса политики безопасности **Отправлена**.

Если одинаковые правила назначены на большое количество целевых устройств:

- 1 Разделите политики с этими устройствами.
- 2 **Объедините одинаковые правила в общий слой**.
- 3 Распределите общий слой в политики.
- 4 Удалите дублирующие правила.

Удаление политики безопасности

Вы можете удалить за один раз только одну политику. Политика удаляется без возможности восстановления.

Чтобы удалить политику, выберите политику и нажмите .

Работа со слоями

При создании политики безопасности создается слой по умолчанию. Правила создаются в этом слое. Чтобы правила в одной политике сгруппировать по признакам, создайте новые слои.

При создании правил вы выбираете слой, к которому относится правило. По умолчанию все правила из слоя применяются ко всем целевым устройствам политики безопасности. Вы можете точно назначить одно правило на целевое устройство политики безопасности. Новое правило в слое создается с наименьшим приоритетом и помещается в конце слоя — оно будет применено последним в слое.

У правила, создаваемого в общем слое, одинаковые настройки параметров регистрации во всех политиках безопасности, в которые распределен слой. При создании правила в общем слое, если установлено значение **Использовать значение, заданное в текущей политике**, для этого правила во всех политиках будут использоваться значения из той политики, в которой создавалось правило. При редактировании правила, если установлено значение **Использовать значение, заданное в текущей политике**, для этого правила во всех политиках будут использоваться значения из той политики, в которой изменялось правило.

Создание слоя

- 1 Выберите организацию.
- 2 В разделе **Политики безопасности** > **Политики** выберите политику.
- 3 Нажмите **Слои правил**.
- 4 Нажмите  **Добавить слой** > **Новый**.
- 5 Задайте имя слоя и пользовательские настройки значений по умолчанию для регистрации IP-пакетов и сессий для правил, создаваемых в этом слое:
 - **Использовать значение, заданное в текущей политике** — настройки слоя будут использовать значения, заданные в политике. Для каждой политики, в которой находится слой, будут использоваться свои значения. Это значение установлено по умолчанию при создании нового слоя.
 - **Регистрация включена**;
 - **Регистрация отключена**.

При выборе для сессий **Регистрация включена**, задайте **Параметры сессий**. При выборе **Расширенные настройки** дополнительно задайте **Состояние сессии** или **Состояние TCP-сессии**.

- 6 Нажмите **Создать**.

Изменение названия слоя

- 1 Выберите организацию.
- 2 Выберите политику.

3 Нажмите **Слои правил**.

4 Наведите указатель мыши на название слоя и нажмите .

5 Введите название слоя и нажмите **Сохранить**.

Изменение настроек регистрации для слоя

1 Выберите организацию.

2 Выберите политику.

3 Нажмите **Слои правил**.

4 В столбце **Регистрация** нажмите .

5 Измените параметры и нажмите **Сохранить**.

Новые настройки будут распространяться только на правила, созданные после изменения настроек.

Изменение приоритета слоя

1 Нажмите **Слои правил**.

2 Выберите один или несколько слоев.

3 Нажмите  (повысить) или  (понизить).

Если вы выбрали несколько слоев, то они перемещаются по списку вместе и располагаются друг за другом.

Добавление слоя в другую политику

1 Убедитесь, что слой назначен на все целевые устройства политики: в столбце **Целевые устройства** имеет значение **Устройства политики**.

2 Нажмите **Слои правил**.

3 Выберите слой.

4 Нажмите  > **Добавить в другую политику**. Правила в общем слое будут отмечены .

Чтобы удалить общие слои из политики, выберите слои и нажмите  > **Отвязать общий слой**.

Чтобы удалить слои из политики или общие слои из всех политик, выберите слои и нажмите .



Внимание! Слои удаляются вместе с правилами.

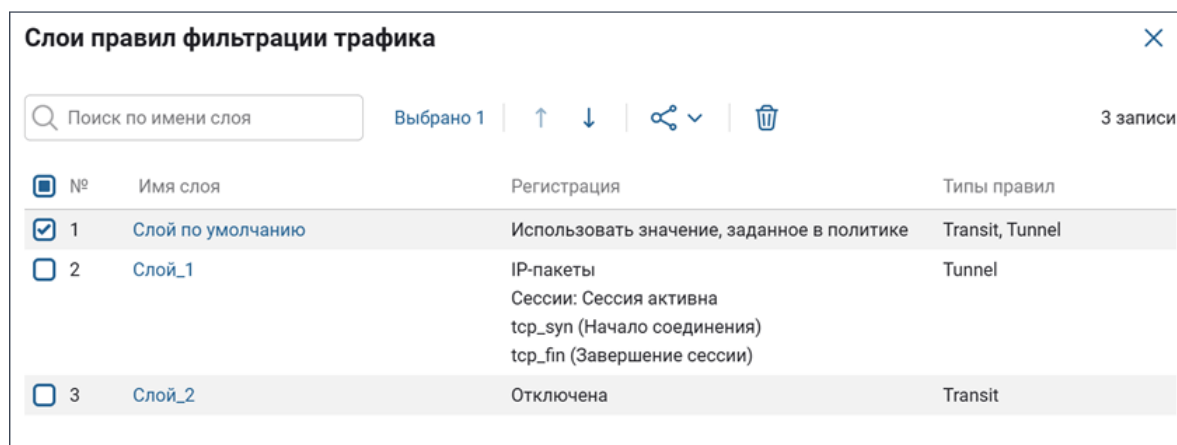


Рисунок 10. Работа со слоями политики безопасности

Добавление слоя из другой политики

- 1 Выберите политику и нажмите **Слои правил**.
- 2 Нажмите  **Добавить слой > Из другой политики**.
- 3 Выберите слой и нажмите **Добавить**.

Настройка режима работы ViPNet Coordinator IG

Вы можете передать в составе политики безопасности настройки устройств. Они отправляются на все целевые устройства политики, но применяются только теми устройствами, которые могут их применить. Такие настройки можно изменить локально на устройстве. Применяются настройки, заданные последними.

При копировании или разделении политики безопасности настройки режима работы не переносятся в новую политику.

Чтобы изменить режим работы межсетевого экрана уровня промышленной сети (тип «Д»):

- 1 [Подключитесь к веб-интерфейсу.](#)
 - 2 Выберите организацию.
 - 3 В модуле VPN убедитесь, что координатор работает в режиме межсетевого экрана уровня промышленной сети (тип «Д»).
- См. «ViPNet Prime. Руководство администратора», «Настройка применения ViPNet Coordinator IG в промышленной сети».
- 4 В разделе **Политики** выберите политику.
 - 5 Перейдите на вкладку **Настройки**.
 - 6 Нажмите **Добавить**.
 - 7 Слева выберите вкладку **Режим работы Coordinator IG**.
 - 8 Включите **Режим работы Coordinator IG**.
 - 9 Выберите режим: **Штатный** (по умолчанию), **Регламентное обслуживание** или **Специальный**.
 - 10 [Создайте правила фильтрации.](#)
 - 11 Просмотрите изменения результирующей политики и [отправьте изменение на устройство](#).

Настройка обработки прикладных протоколов

Прикладные протоколы обеспечивают работу пользовательских сетевых сервисов, таких как IP-телефония, DNS-служба, FTP-служба. Использование этих сервисов может повлиять на доступность сервисов в защищенной сети с виртуальной адресацией или трансляцией адресов, так как IP-адреса передаются в теле IP-пакета. Некоторые прикладные протоколы для передачи данных открывают дополнительные соединения на случайно выбранный порт, номер которого заранее неизвестен. Для таких IP-пакетов невозможно создать разрешающее правило фильтрации, поэтому соединение будет заблокировано. Подробнее см. в документации на ViPNet Client.

Настройки обработки прикладных протоколов отправляются только на целевые устройства поколения [ViPNet 4](#), в том числе на клиенты с дистрибутивом ключей `*.dst`:

- ViPNet Client 5 for Windows 5.2 и выше;
- ViPNet Client 5 for Linux 5.1.3 и выше;
- ViPNet Client 5 for iOS 5.1 и выше;
- ViPNet Client 5 для ОС Аврора 5.1 и выше.

Действие настроек распространяется на все целевые устройства в политике безопасности. Настроить работу протокола для нескольких устройств из списка целевых политики безопасности невозможно.

По умолчанию правил обработки прикладных протоколов в политиках безопасности нет, они добавляются вручную администраторами.

При включении обработки прикладных протоколов по умолчанию устанавливаются порты:

- DNS — 53 (UDP);
- FTP — 21 (TCP);
- H.323 — 1720 (TCP), 1719 (UDP);
- SCCP — 2000 (TCP);
- SIP — 5060, 5080 и 5068 — TCP и UDP.

Вы можете изменить порты для каждого протокола и использовать эти настройки в политиках безопасности:

- 1 [Подключитесь к веб-интерфейсу](#).
- 2 Выберите организацию.
- 3 В разделе **Политики** выберите политику.
- 4 Перейдите на вкладку **Настройки**.
- 5 Нажмите **Добавить**.

- 6 Слева выберите вкладку **Прикладные протоколы**.
- 7 Включите  **Прикладные протоколы**.
- 8 Включите  необходимые прикладные протоколы. Включится обработка прикладных протоколов с портами, установленными по умолчанию.
- 9 Чтобы изменить порты для прикладного протокола, в его строке нажмите .

Порты для разных прикладных протоколов должны отличаться. Для одного прикладного протокола разным транспортным протоколам может быть назначен один порт.

- 10 Укажите порты для используемых транспортных протоколов. Несколько портов указывайте через запятую, диапазон портов — с помощью тире.

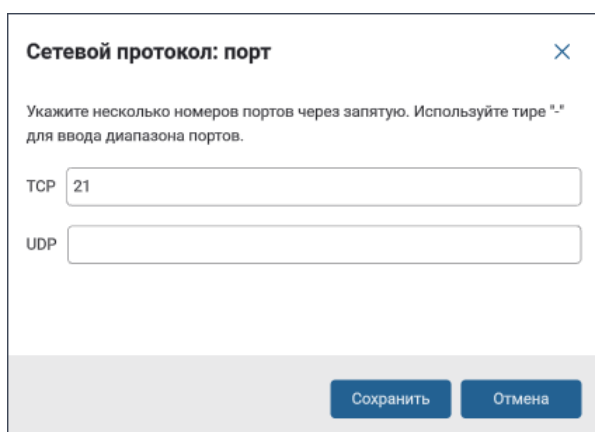


Рисунок 11. Указание портов для прикладного протокола

- 11 Нажмите **Сохранить**.
 - 12 Нажмите **Добавить**.
- Изменится результирующая политика устройства.
- 13 [Просмотрите изменения результирующей политики и отправьте изменение на устройство](#).

Если в политике безопасности есть устройства поколения **ViPNet 5** (с дистрибутивом ключей *.ds5), на них не будут отправлены настройки прикладных протоколов. Вы можете ознакомиться со списком этих устройств.

Чтобы изменить настройки прикладных протоколов:

- 1 На вкладке **Настройки** в разделе с настроенными протоколами нажмите  > **Изменить**.
- 2 Измените настройки и сохраните изменения.

Чтобы вернуться к настройкам по умолчанию, нажмите **Вернуть настройки протоколов по умолчанию**.

Если вы изменили настройки обработки прикладных протоколов и затем отключили их обработку, при повторном включении будут установлены порты по умолчанию.

Чтобы отключить добавление настроек прикладных протоколов, на вкладке **Настройки** в разделе с настроенными протоколами нажмите  > **Отключить**, подтвердите отключение.

Дополнения политики безопасности

В политику безопасности вы можете добавить:

- Список блокировки IP-адресов — предварительно [загрузите файл со списком блокировки IP-адресов](#) в разделе **Блокировка IP-адресов**.
- Список дополнений и исключений для стран — предварительно [создайте список дополнений и исключений IP-адресов](#) в разделе **Страны > Дополнения и исключения для стран**.

Чтобы добавить в политику безопасности список дополнений и исключений для стран или список блокировки IP-адресов:

- 1 [Подключитесь к веб-интерфейсу](#).
- 2 Выберите организацию.
- 3 В разделе **Политики** выберите политику.
- 4 Перейдите на вкладку **Дополнения**.
- 5 Нажмите **Добавить**.
- 6 Выполните одно из действий:
 - Чтобы добавить список дополнений и исключений для стран, на вкладке **Дополнения и исключения для стран** выберите список. Если нет ни одного списка, [создайте его](#).
 - Чтобы добавить список блокировки IP-адресов, на вкладке **Блокировка IP-адресов** выберите список. Если нет ни одного списка, [создайте его](#).
- 7 Нажмите **Добавить**.

На вкладке **Дополнения** появится раздел с информацией о выбранном списке.
- 8 [Разрешите отправку дополнений на целевые устройства](#).

Чтобы выбрать другой список, на панели списка нажмите  > **Изменить**, выберите список и нажмите **Сохранить**.

Чтобы удалить список из политики, на панели списка нажмите  > **Удалить из политики**, подтвердите удаление списка. Также вы можете снять флажок со списка и сохранить изменения.

Если список дополнений и исключений удален из политики безопасности или из него удалены все IP-адреса, на целевом устройстве список дополнений и исключений будет очищен при получении результирующей политики.

Если список блокировки IP-адресов удален из политики безопасности или удалена политика безопасности, на целевом устройстве список будет удален при получении результирующей политики, если на устройство разрешена отправка списка блокировки IP-адресов.

Разрешение отправки дополнительных параметров функций на целевые устройства

На некоторые целевые устройства поколения ViPNet 5 вы можете разрешить отправку:

- правил фильтрации по странам;
- списка блокировки IP-адресов;
- параметров регистрации IP-пакетов;
- параметров регистрации сессий.

Не все управляемые устройства могут принять политику безопасности, содержащую дополнительные параметры функции, что может привести к тому, что политика будет отброшена целиком. Чтобы избежать этого, ViPNet Prime Policy Management запрещает отправлять дополнительные функции на такие устройства. Принять политику с дополнительными параметрами функций, может только ViPNet Coordinator HW 5.

Вы не сможете разрешить отправку дополнительных параметров функций на устройства, которые не поддерживают эту функциональность. Но некоторые версии устройств, на которые можно разрешить отправку, не могут применить политику с дополнительными параметрами.



Внимание! О версиях ПО, поддерживающих дополнительные параметры функции, уточняйте в документации на устройство. Отправка дополнительных параметров функций на устройства, которые их не поддерживают, может привести к неработоспособности устройства.

Если правила фильтрации по странам и список дополнений и исключений были отправлены на устройства, при запрете отправки правил фильтрации по странам список дополнений и исключений остается на устройстве.

Если список блокировки IP-адресов отправлен на устройство, при запрете его отправки список блокировки останется на устройстве.

Чтобы правила фильтрации по странам, список дополнений и исключений IP-адресов, список блокировки IP-адресов, параметры регистрации сессий или IP-пакетов включались в результирующие политики устройств, разрешите отправлять их на целевые устройства:

- 1 Подключитесь к веб-интерфейсу.
- 2 Выберите политику безопасности.
- 3 Выберите **Целевые устройства**.
- 4 Выберите целевые устройства и нажмите **Функции**.

5 Выберите один из пунктов:

- **Отправка правил с фильтрацией по странам** — на устройства будут отправляться правила фильтрации по странам и списки дополнений и исключений IP-адресов. Если в политике безопасности нет правил фильтрации по странам, но есть список дополнений и исключений, он отправится на устройство, если разрешена отправка.
- **Отправка списка блокировки IP-адресов**
- **Отправка параметров регистрации IP-пакетов** — на устройства будут отправляться правила фильтрации с параметрами регистрации IP-пакетов.
- **Отправка параметров регистрации сессий** — на устройства будут отправляться правила фильтрации с параметрами регистрации сессий.

6 Выберите **Разрешить** или **Запретить**.

Разрешить отправку правил фильтрации по странам, списка блокировки IP-адресов, параметры регистрации IP-пакетов и сессий вы можете не на все устройства. ViPNet Prime Policy Management запрещает отправлять дополнительные параметры функций на устройства, которые не смогут их принять. При этом запретить отправку дополнительных параметров функций вы можете для любого устройства. По умолчанию отправка правил с фильтрацией по странам, списка блокировки IP-адресов, параметров регистрации IP-пакетов и сессий на целевые устройства запрещена.

7 Подтвердите, если разрешаете отправку на выбранные целевые устройства.

Если вы выбрали устройства, которые не поддерживают правила фильтрации по странам, список блокировки IP-адресов, параметры регистрации сессий или IP-пакетов, появится уведомление, из которого вы можете перейти к просмотру списка таких устройств, для этого нажмите **Показать список**.

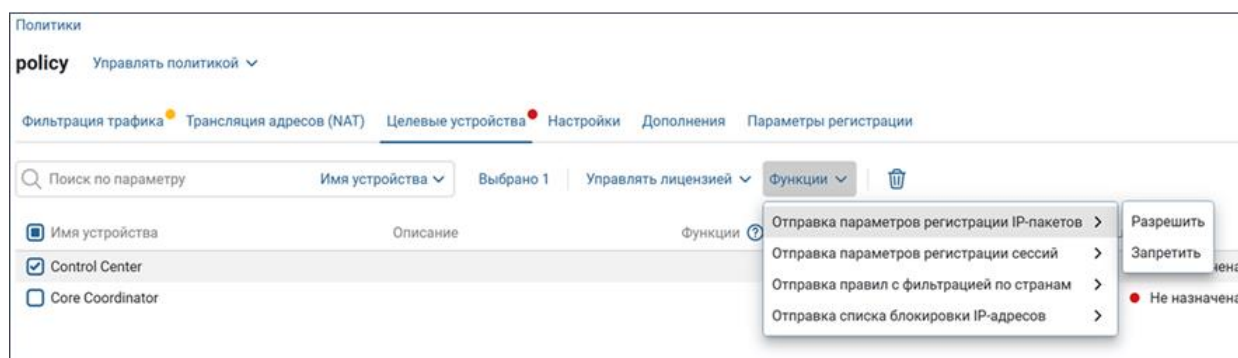


Рисунок 12. Назначение функции на целевое устройство

В столбце **Функции** будет отображаться значок:



— если на целевое устройство разрешена отправка правил фильтрации по странам;



— если на целевое устройство разрешена отправка списка блокировки IP-адресов;



— если на целевое устройство разрешена отправка параметров регистрации сессий;



— если на целевое устройство разрешена отправка параметров регистрации IP-пакетов.

Правила фильтрации по странам, список блокировки IP-адресов, параметры регистрации IP-пакетов и сессий включаются в результирующую политику только тех устройств, на которые разрешена их отправка. Разрешение или запрет отправки правил распространяется на все созданные в организации правила для каждого устройства отдельно.

Когда разделяете политику:

- правила фильтрации по странам и правила с параметрами регистрации IP-пакетов и сессий для правил переносятся в новую политику, если назначены на все переносимые целевые устройства;
- правила фильтрации по странам и правила с параметрами регистрации IP-пакетов и сессий для правил копируются в новую политику, если назначены на часть переносимых целевых устройств;
- параметры регистрации IP-пакетов и сессий для слоя и политики копируются в новую политику;
- список дополнений и исключений и список блокировки IP-адресов добавляется в новую политику, если он был добавлен в политику безопасности.

Параметры регистрации сессий и IP-пакетов

На шлюзах безопасности для каждого правила фильтрации администратор может включить или отключить регистрацию IP-пакетов и сессий в журнале и задать, какое состояние сессии необходимо регистрировать. Настройка параметров регистрации только определенных событий позволяет снизить нагрузку на аппаратные ресурсы шлюзов безопасности и межсетевых экранов и уменьшить объем хранимых данных.

Правила с параметрами регистрации сессий поддерживаются только ViPNet Coordinator HW 5.4 и выше (для сессий только начало и конец сессии) и ViPNet Coordinator KB 5.0.0 и выше.

Нельзя разрешать отправку параметров регистрации сессий на устройства:

- поколения 5:
 - ViPNet Coordinator IG 5.2.0 и выше,
 - ViPNet Client 5,
- поколения 4:
 - ViPNet Client 4,
 - ViPNet xFirewall 5.4 и выше,
 - ViPNet Coordinator HW 4.5.8 и выше,
 - ViPNet Coordinator IG 4.5.1 и выше,
 - ViPNet Coordinator KB 4.3.4 и выше.

Правила с параметрами регистрации IP-пакетов поддерживают устройства поколения 5:

- ViPNet Coordinator HW 5.3.0 и выше,
- ViPNet Coordinator IG 5.2.0 и выше,
- ViPNet Coordinator KB 5.0.0 и выше.

Нельзя разрешать отправку параметров регистрации IP-пакетов на устройства поколения 4:

- ViPNet xFirewall 5.4 и выше,
- ViPNet Coordinator HW 4.5.8 и выше,
- ViPNet Coordinator IG 4.5.1 и выше,
- ViPNet Coordinator KB 4.3.4 и выше.

Чтобы снизить трудозатраты администраторов шлюзов безопасности и межсетевых экранов, ViPNet Prime Policy Management позволяет централизованно настроить для правил параметры регистрации IP-пакетов и сессий. При этом вы можете настроить параметры:

- для всех правил политики безопасности;

- для всех правил слоя;
- для каждого правила при создании или изменении;
- оставить системные значения для правила в зависимости от его действия:
 - для регистрации IP-пакетов — для блокирующих правил значение **Включена**, для пропускающих — **Отключена**;
 - для регистрации сессий — для блокирующих правил значение **Включена**, **Отслеживать начало и конец сессии**, для пропускающих — **Отключена**.

При создании правила фильтрации настройки применяются в соответствии со следующим приоритетом (по убыванию приоритета):

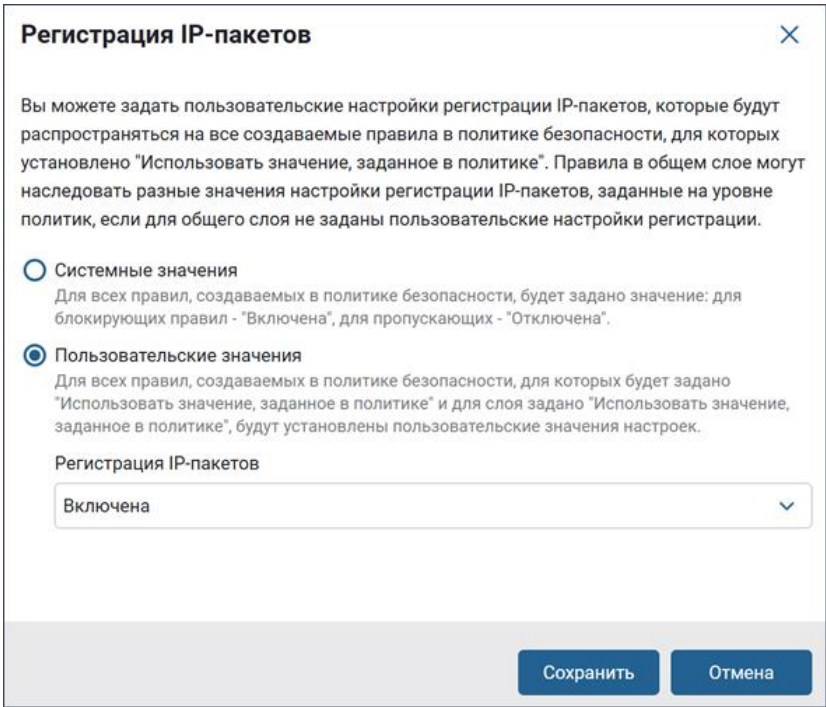
- 1 Настройки, заданные для правила.
- 2 Настройки, заданные для слоя — если в правиле задано использование настроек, заданных для слоя.
- 3 Настройки, заданные для политики — если в правиле задано использование настроек, заданных для политики, и нет настроек, заданных для слоя.
- 4 Системные настройки — если в правиле задано использование настроек, заданных для политики, и нет настроек, заданных для слоя. И при этом не заданы пользовательские настройки для политики.

Особенности и ограничения:

- Параметры регистрации, заданные в слое или политике, распространяются только на создаваемые правила. Если в слое или политике, из которых используются параметры регистрации, изменились заданные значения, они не повлияют на уже созданные правила, а будут подставляться только в создаваемые правила.
- При импорте правил из Check Point или ViPNet Policy Manager правилам назначаются системные значения регистрации IP-пакетов и сессий.
- На шлюзах безопасности и межсетевых экранах есть возможность задать глобальные настройки регистрации IP-пакетов и сессий. В ViPNet Prime Policy Management нет возможности управлять глобальными настройками регистрации. Если на управляемом устройстве отключена регистрация IP-пакетов и сессий, то параметры, настроенные для правил в ViPNet Prime Policy Management, не будут учитываться.
- Для некоторых типов устройств нельзя разрешить отправку параметров регистрации IP-пакетов и сессий.
- При обновлении ViPNet Prime Policy Management с версии, не поддерживающей управление параметрами регистрации IP-пакетов и сессий, на версию, поддерживающую управление параметрами регистрации, для всех правил устанавливаются системные значения параметров регистрации.
- Если для правила установлены системные значения настроек, при редактировании правила при смене действия правила параметры регистрации не изменяются.

Чтобы задать значения параметров регистрации IP-пакетов и сессий для политики:

- 1 Подключитесь к веб-интерфейсу.
- 2 Выберите организацию.
- 3 В разделе **Политики** выберите политику.
- 4 Перейдите на вкладку **Параметры регистрации**.
- 5 На панели регистрации IP-пакетов или сессий нажмите .
- 6 Выберите:
 - **Системные значения** — чтобы использовались системные значения в зависимости от действия правила.
 - **Пользовательские значения** — для всех правил, созданных в политике безопасности после изменения настроек, для которых будет задано **Использовать значение, заданное в политике** и для слоя задано **Использовать значение, заданное в текущей политике**, будут установлены пользовательские значения настроек, заданные для политики. Задайте эти значения.



Регистрация IP-пакетов

Вы можете задать пользовательские настройки регистрации IP-пакетов, которые будут распространяться на все создаваемые правила в политике безопасности, для которых установлено "Использовать значение, заданное в политике". Правила в общем слое могут наследовать разные значения настройки регистрации IP-пакетов, заданные на уровне политик, если для общего слоя не заданы пользовательские настройки регистрации.

☐ Системные значения
Для всех правил, создаваемых в политике безопасности, будет задано значение: для блокирующих правил - "Включена", для пропускающих - "Отключена".

☒ Пользовательские значения
Для всех правил, создаваемых в политике безопасности, для которых будет задано "Использовать значение, заданное в политике" и для слоя задано "Использовать значение, заданное в политике", будут установлены пользовательские значения настроек.

Регистрация IP-пакетов

Включена

Сохранить Отмена

Рисунок 13. Настройка регистрации IP-пакетов для политики

- 7 Если вы выбрали **Пользовательские значения**:
 - 7.1 Для регистрации IP-пакетов выберите **Включена** или **Отключена** и нажмите **Сохранить**.
 - 7.2 Для регистрации сессий:
 - 7.2.1 Выберите **Включена** или **Отключена**.

7.2.2 Если регистрация сессий включена, задайте **Параметры сессий**. При выборе **Расширенные настройки** дополнительно задайте параметры **Состояние сессии** или **Состояние TCP-сессии**.

7.2.3 Нажмите **Сохранить**.

- 8 Убедитесь, что на целевых устройствах, добавленных в политику, включена регистрация IP-пакетов и сессий.

Инспекция политик

В ходе инспекции вы можете убедиться, что правила, созданные в ViPNet Prime PMM, будут работать правильно, что в политике нет несогласованных правил — противоречий и дубликатов. Политика безопасности инспектируется автоматически при отправке на устройства, или вы можете запустить инспекцию вручную.

Проверяются на согласованность:

- правила транзитного и локального трафика открытой сети;
- параметры правил: действие, источники и назначения, целевые устройства и протоколы.

Не проверяются:

- локальные правила, созданные на устройстве;
- правила фильтрации защищенной сети и туннелируемых ресурсов;
- правила трансляции адресов;
- правила фильтрации по странам.

Также не проверяются:

- настройки ViPNet Coordinator IG;
- настройки обработки прикладных протоколов;
- счетчики срабатывания правил;
- параметры правил: названия и описания правил, протоколы DPI, приложения DPI, расписания;
- [системные группы объектов](#);
- список блокировки IP-адресов;
- список дополнений и исключений для стран;
- параметры регистрации IP-пакетов и сессий.

При инспекции учитываются все вложенные группы в правилах.

Правила проверяются на:

- Дубликаты — правила с одинаковым действием полностью совпадают.
- Вхождения одного правила в другое — все параметры правила 1 совпадают с частью параметров правила 2 с таким же действием.

Пример: IP-адреса источника менее приоритетного правила входят в адреса источников более приоритетного правила — 192.168.1.5 входит в подсеть 192.168.1.0/24. Если остальные параметры правила совпадают, то такое правило избыточно и его можно удалить.

- Противоречия — если есть другое правило такого же типа с более высоким приоритетом и один из параметров правила содержится в списке значений другого правила.

Пример: Есть блокирующее и разрешающее правила. Блокирующее правило имеет более высокий приоритет, чем разрешающее правило. Если диапазон адресов из разрешающего правила входит в диапазон блокирующего правила, то разрешающее правило никогда не сработает.

Если в паре правил выявлены несогласованные данные или одинаковые условия срабатывания, это записывается в отчет, который можно скачать в разделе **Журнал инспекции политик**. Отчеты хранятся 7 суток. Если несогласованные правила не выявлены, отчет не создается.

Политики проверяются на согласованность в фоновом режиме. Поддерживается проверка 20 тысяч правил. Если количество правил в политике больше, вы можете отправить политику безопасности на целевые устройства без инспекции правил.

Чтобы вручную запустить инспекцию политик:

Внимание! Чтобы избежать увеличения времени инспекций политик безопасности:

- Не запускайте новую инспекцию политики, пока не завершилась предыдущая.
- Не изменяйте политику, если она находится в статусе **Инспектируется**, до смены статуса.
- Не перезагружайте сервисы ViPNet Prime PMM во время инспекции политик. Перезапуск сервисов не отменяет запущенные инспекции политик. Отменить запущенную инспекцию нельзя. Ожидайте ее завершения.



Инспекция обычно длится несколько минут, но может занимать до 6 часов при повышенной нагрузке на ViPNet Prime или большого размера политики.

1 Подключитесь к веб-интерфейсу.

2 Выберите **ViPNet Prime PMM**  > **Политики**.

3 Выполните одно из действий:

- Чтобы инспектировать все политики в организации, нажмите **Инспектировать политики**.
- Выберите несколько политик и нажмите **Инспектировать политики**.
- Нажмите на название политики, выберите **Управлять политикой** > **Инспектировать политику**.



Примечание. Вы можете инспектировать политику только в статусе **Изменена**.

4 Если в результате инспекции были выявлены несогласованные правила, в разделе **Журнал инспекции политик** скачайте отчет *.xlsx. В зависимости от количества найденных несогласованных правил отчет может скачиваться от нескольких секунд до нескольких минут.

Работа с отчетом инспекции политики

Отчет инспекции — это файл XLSX с результатами проверки правил на наличие дубликатов, противоречий в значениях.

Файл отчета имеет название `Consistency-check-results_<дата и время создания журнала>_RU.xlsx` и не содержит названия организации. Если вы администрируете несколько организаций, отслеживайте принадлежность файла отчета к определенной организации дополнительными мерами.

Максимальное количество несогласованных пар в отчете — 20 тыс.

Для записей в отчете инспекции действуют следующие соглашения:

- «Правило 2» имеет приоритет выше, чем «Правило 1».
- Группа объектов записывается в следующем виде:

- Адреса с исключениями:

<Адреса из состава группы> [<Исключение 1>, <Исключение 2>, <Исключение N>] (<Название группы>).

- Исключения записываются в квадратных скобках как адреса или названия групп объектов.

Если исключение — это группа объектов, то в квадратных скобках отображается название группы, состав группы не перечисляется.

- Название группы записывается в круглых скобках.

Например, записи обозначают:

- 1.1.1.1-1.1.1.9 [Группа_A] (Группа_D) — Группа_A исключается из состава адресов 1.1.1.1-1.1.1.9 группового объекта Группа_D.
 - 1.1.1.11-1.1.1.20 (Группа_D) — адреса 1.1.1.11-1.1.1.20 из состава группового объекта Группа_D.

- Состав «Любые» с исключениями:

Любые [<Исключение 1>, <Исключение 2>, <Исключение N>] (<Название группы>).

Например, записи обозначают:

- Любые [1.1.1.1, 2.2.2.2] (Группа 1) — адреса 1.1.1.1 и 2.2.2.2 исключаются из состава **Любые** группового объекта Группа 1.
 - Любые [1.1.1.1] (Группа 2) — исключение 1.1.1.1 из состава **Любые** группового объекта Группа 2.

- В отчет записываются не все параметры правила, а только те, которые связаны с конфликтом:
 - Если в группе объекта несколько значений адресов исключений, в журнал запишутся только те адреса исключений (отображаются в квадратных скобках), которые влияют на конфликт.

- Если состав имеет несколько адресов или диапазонов адресов, в журнал запишется только тот диапазон, который связан с конфликтом, а не все диапазоны адресов источника или назначения.
- Запись вида <Адреса из состава группы 2> (<Название группы 1> > <Название группы 2>) обозначает, например:
1.1.1.1 (Томск > Офис 1) — адрес 1.1.1.1 из состава группы «Офис 1», которая входит в группу «Томск».
- Если правило 1 содержит один большой диапазон адресов, в который входят значения адресов из правила 2, то эти значения перечисляются через запятую в одной строке, напротив большого диапазона.

Для пары сравниваемых правил в отчет записываются их идентификаторы (RuleID). По номеру идентификатора вы можете найти правило в списке правил.

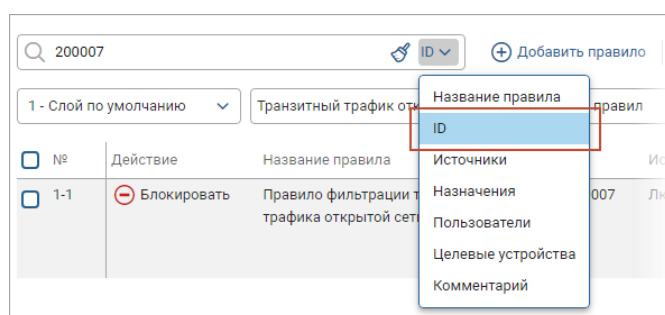


Рисунок 14. Поиск правила по идентификатору

Отправка политик на устройства

При отправке политики на устройства все правила объединяются [с учетом приоритета](#). Вы можете просмотреть их перед отправкой. Информация о слое не отображается и не передается на устройство, как и название политики.

Перед отправкой политики на устройства автоматически [инспектируются все правила в политике](#). Если статус политики **Инспекция не пройдена**, блокируется ее отправка, и она исключается из отправки по умолчанию. Чтобы отправить изменения, сначала устраните конфликты из журнала инспекций, или отправьте политику в статусе **Инспекция не пройдена** принудительно.

Для результирующей политики устройства вы можете просмотреть информацию об изменениях фильтрации трафика, трансляции адресов, [настройках](#).



Примечание. Если вы внесли изменения в политику безопасности, а затем отменили их, результирующая политика все равно останется в статусе **Изменена**.

Чтобы отправить изменения политик на устройства:

- 1 [Подключитесь к веб-интерфейсу](#).
- 2 Выберите организацию.
- 3 Чтобы отправить изменения в выбранных политиках, в разделе **Политики безопасности** > **Политики** выберите политику и нажмите **Отправить изменения на устройства**. Отобразится список устройств, на которые будут отправлены политики.



Примечание. Чтобы отправить изменения, повторите попытку и в открывшемся окне включите **Отправить изменения политик со статусом "Инспекция не пройдена"**.

- 4 Чтобы отправить изменения во всех политиках, нажмите **Отправить изменения на устройства**.
- 5 Чтобы просмотреть результирующую политику безопасности, выберите устройство и нажмите .
- 6 Чтобы принудительно отправить политики, которые не прошли инспекцию, включите **Отправить изменения политик со статусом "Инспекция не пройдена"**.

Отправка изменений на устройства

Поиск

9 записей

Устройство	Описание	Политика	Статус политики	Результирующая политика
GTW-Core-1		Политика индустриал...	Инспекция не пройдена	
Gateway-001				
IG-1		Политика индустриал...	Инспекция не пройдена	

Отправить

Отмена

Рисунок 15. Принудительная отправка политики, которая не прошла инспекцию

7 Нажмите **Отправить**.

В ViPNet Prime Policy Management не отображается статус применения результирующей политики на устройствах.

Особенности при смене поколения клиента и координатора

Если администратор ViPNet Prime изменил поколение клиента или координатора с ViPNet 4 на ViPNet 5, результирующая политика будет отмечена измененной, вы сможете отправить ее вручную на устройство в рабочем порядке. Автоматически результирующая политика не будет отправлена. На устройстве будут действовать правила и настройки, которые были применены до смены поколения.

Не отправляйте результирующую политику на устройства, на которых происходит смена поколения, до установки нового дистрибутива ключей на узле. Иначе результирующая политика не будет доставлена или может быть отправлена неактуальная результирующая политика.

Настройка отправки результатирующих политик

Вы можете управлять поведением модуля при инспекции политики с помощью специального параметра. Он может принимать следующие значения:

- `Allow` — не блокировать отправку изменений несогласованной политики безопасности — политики в статусе **Инспекция не пройдена**. Инспекция при отправке автоматически не производится.
- `AllowOnlyByForce` (по умолчанию) — блокировать отправку изменений несогласованных политик безопасности и включить возможность их принудительной отправки на устройства. Инспекция производится автоматически при отправке.

Повторно отправьте политику безопасности — нажмите **Отправить изменения на устройства** и выберите **Отправить изменения политик со статусом "Инспекция не пройдена"**.

- `Block` — блокировать отправку изменений несогласованных политик безопасности — политик в статусе **Инспекция не пройдена** и отключить возможность их принудительной отправки на устройства. Инспекция производится автоматически при отправке.

По умолчанию в ViPNet Prime Policy Management блокируется отправка политики, которая не прошла инспекцию на согласованность правил.

Чтобы принудительно отправить политику на устройства с несогласованными правилами в ней, если не выбраны режимы `Allow` или `Block`, повторно отправьте изменения на устройства и выберите **Отправить изменения политик со статусом "Инспекция не пройдена"**.

Чтобы изменить поведение при отправке политики безопасности, которая не прошла инспекцию:

1 Остановите Docker-контейнеры модуля:

1.1 На сервере ViPNet Prime перейдите в папку, в которую был распакован архив модуля ViPNet Prime Policy Management.

1.2 Выполните команду:

```
$ sudo ./down.sh
```

2 Из папки `/usr/share/infotecs/pmm` откройте файл `config.env` для изменения.

Для параметра

`PM_Modules__TargetDevicePolicies__Settings__SendingNonConsistentPolicyChangesStrategy` установите одно из значений:

- o `Allow`
- o `AllowOnlyByForce` (по умолчанию)
- o `Block`



Внимание! В синтаксисе параметра

`PM_Modules__TargetDevicePolicies__Settings__SendingNonConsistentPolicyChangesStrategy` используется двойной символ нижнего подчеркивания (`__`) везде, кроме `<PM_Modules>` (используется одинарный символ).

3 Запустите Docker-контейнеры модуля:

```
$ sudo ./up.sh
```

Также этот скрипт остановит и удалит существующие Docker-контейнеры, если их настройки или версии изменились, а затем создаст новые Docker-контейнеры и запустит их.

4

Работа с правилами

Правила фильтрации трафика	77
Правила трансляции адресов (NAT)	90
Копирование, изменение и удаление правил	93
Просмотр состояний правил	96
Просмотр срабатываний правил	97
Сброс счетчиков срабатываний правил	99
Поиск правил в журнале событий	100

Правила фильтрации трафика

Правила фильтрации трафика блокируют или пропускают IP-пакеты в зависимости от условий: источника, назначения, протокола и расписания.

В ПО ViPNet фильтруется:

- Локальный трафик открытой сети — трафик между защищенными и [открытыми устройствами](#).
- Транзитный трафик открытой сети — открытый трафик, проходящий через [шлюзы безопасности](#).
- Трафик туннелируемых ресурсов — трафик между туннелями координатора и устройствами [защищенной сети](#).
- Локальный трафик защищенной сети — трафик, которым устройства защищенной сети обмениваются между собой.

Для всех правил фильтрации:

- Каждому правилу присваивается идентификатор, который уникален в организации.
- При создании правило включено по умолчанию и добавляется в слой, в конец списка.
- Если в составе правила не указаны значения, используются все значения (любые) в источниках, назначениях, пользователях, сервисах и приложениях, расписаниях.

Исключение — правила локального трафика защищенной сети. Для них укажите системную группу **Целевое устройство**, либо **Широковещательная рассылка** для источников или назначений.

- Вы создаете правила в составе политики безопасности и для их применения [отправляете изменения политики безопасности на целевые устройства](#).
- Если вы создаете правило в общем слое, то оно будет создано во всех политиках, в которые был добавлен общий слой.

Приоритет правил и слоев определяет их порядок в [результатирующей политике безопасности](#). Он уменьшается от первого в списке к последнему.

Правила ViPNet Prime Policy Management имеют больший приоритет, чем правила, созданные на управляемом устройстве.

Изменение правил фильтрации записывается в журнал событий ViPNet Prime. Если в условиях правил фильтрации используется [пользователь](#), после удаления пользователя из ViPNet Prime правила фильтрации изменяются. Информация об этом записывается в событие «Удаление пользователя».

Для транзитного трафика открытой сети вы можете задавать правила сетевого и прикладного уровня, для остальных типов трафика — только сетевого. Для фильтрации трафика по приложениям [загрузите классификатор DPI](#).

Локальный трафик открытой сети

Если правила фильтрации локального трафика открытой сети назначены на устройства ViPNet EndPoint Protection, соблюдайте ограничения:

- в качестве источника или назначения поддерживаются только IP-адреса открытой сети (одиночные адреса, диапазоны адресов, группы с такими адресами).
- ViPNet EndPoint Protection Агент не поддерживает:
 - многоадресную рассылку и широковещательные адреса для **системных групп объектов** открытой сети в назначениях;
 - протоколы, которые инкапсулируются в протокол IP (**Код IP-протокола**);
 - действие **Отклонять и отправлять сообщение**.

Трафик туннелируемых ресурсов

Ограничения:

- Системную группу **Туннелируемые адреса устройства** нельзя одновременно добавить в источники и назначения.
- Нельзя одновременно добавить **Сетевой интерфейс** и **Группы сетевых интерфейсов** для туннелируемых ресурсов источников.
- Нельзя одновременно добавить **Сетевой интерфейс** и **Группы сетевых интерфейсов** для туннелируемых ресурсов назначений.
- Условия фильтрации трафика источников и назначений позволяют добавить сетевые интерфейсы только для туннелируемых ресурсов.
- Если источником трафика выбраны устройства защищенной сети, его назначением могут быть только туннелируемые ресурсы. Если назначение трафика — устройства защищенной сети, его источником могут быть только туннелируемые ресурсы.
- Туннелируемые IP-адреса (ресурсы) не создаются как ресурсы для управления в модуле VPN и недоступны для использования как ресурсы в источниках или назначениях правил ViPNet Prime Policy Management.

Рекомендации:

- Отслеживайте изменения IP-адресов ресурсов и координаторов, которые туннелируют эти ресурсы. В источнике и назначении указывайте ресурсы разных координаторов.
- В источниках и назначениях вы можете использовать ресурсы и устройства из своей и доверенных организаций. Но при межсетевом взаимодействии ресурсы доверенных сетей недоступны для использования.
- Чтобы создать правило фильтрации всего входящего трафика к ресурсам, в назначениях добавьте системную группу **Туннелируемые адреса устройства**, а в источниках не задавайте условия фильтрации трафика.

- Чтобы создать правило фильтрации всего исходящего трафика ресурсов, в источниках добавьте системную группу **Туннелируемые адреса устройства**, а в назначениях не задавайте условия фильтрации трафика.

Трафик защищенной сети

- В качестве источника и назначения вы можете задать устройства доверенных организаций: межсетевые экраны ViPNet xFirewall, координаторы, клиенты. Если для устройств разрешено использование функций в доверенных организациях без создания связей с ними, то такие устройства не отображаются в источниках или назначениях.
- Если источник — устройства защищенной сети, его назначением может быть только **Целевое устройство** или **Широковещательная рассылка**.
- Если назначение — устройства защищенной сети, его источником вы можете задать только **Целевое устройство**.

Создание правил фильтрации

Для добавления стран в правило в ViPNet Prime Policy Management [должна быть загружена база по странам](#).



Внимание! Не добавляйте в правило суммарно более 1000 значений. Это может привести к долгому применению политики на устройстве.

- 1 [Подключитесь к веб-интерфейсу](#).
- 2 Выберите политику или [создайте новую политику безопасности](#).
- 3 Выберите **Фильтрация трафика**.
- 4 На панели инструментов выберите тип трафика:
 - **Транзитный трафик открытой сети.**
 - **Трафик туннелируемых ресурсов.**
 - **Локальный трафик открытой сети.**
 - **Локальный трафик защищенной сети.**
- 5 Нажмите  **Добавить правило**. Чтобы задать правилу приоритет при создании:
 - 5.1 Выберите правило из списка.
 - 5.2 Нажмите:
 -  — чтобы создать правило выше,
 -  — чтобы создать правило ниже.
- 6 Введите название правила.

7 Выберите слой.

Если слой выбран на панели инструментов, то в окне создания правила изменить слой нельзя. Чтобы выбрать другой слой, закройте окно и на панели инструментов выберите **Все слои правил**.

Если вы выбирали правило в списке, чтобы задать приоритет создаваемому правилу, правило будет создано в том же слое, что и выбранное из списка правило.

8 Выберите действие правила фильтрации:

-  Пропускать.
-  Блокировать.
-  Отклонять и отправлять сообщение и выберите сообщение, которое будет отправляться межсетевому экрану устройства при срабатывании правила:
 - Сеть назначения недоступна.
 - Устройство назначения недоступно.
 - Порт назначения недоступен.
 - Протокол назначения недоступен.
 - Доступ к сети запрещен.
 - Доступ к устройству запрещен.
 - Связь запрещена.
 - TCP RST.

9 Чтобы задать отправителей и получателей трафика IP-пакетов:

9.1 В разделе **Условия фильтрации трафика > Источники** или **Назначения** нажмите **Добавить**.

9.2 Укажите:

- IP-адреса или доменные имена — в разделе **Адреса открытой сети**.
- Идентификаторы или IP-адреса сетевых интерфейсов — в разделе **Сетевые интерфейсы**.
- **Группы объектов** — в разделах **Адреса открытой сети**, **Сетевые интерфейсы**, **Страны**. Вы можете просмотреть состав группы, для этого нажмите на нее.
- **Страны** — можно добавить только для правил трафика открытой сети: локального или транзитного. Вы можете добавить в правило фильтрации или только страны, или адреса открытой сети и сетевые интерфейсы. При выборе стран вы можете воспользоваться поиском по двухбуквенному коду или названию страны. Одна и та же страна может быть включена и в источники, и в назначения одного правила.

9.3 Нажмите **Сохранить**.

10 Укажите протоколы:

10.1 В разделе **Условия фильтрации трафика > Сервисы и приложения** нажмите **Добавить**.

10.2 В группе **Соединение** укажите:

- **TCP / UDP** и введите порты источника и назначения. Для просмотра часто встречающихся стандартных портов нажмите **Справочник TCP/UDP портов**.
- **ICMP** и тип и код ICMP-сообщения.
- **IP** и код IP-протокола.
- **Группы протоколов** (ddd).

10.3 Нажмите **Сохранить**.

Сервисы и приложения

Соединение

▼ TCP / UDP

Укажите номера портов источника и назначения, отделяя значения запятой. Используйте знак "-" для ввода диапазона портов.

Протокол	Порт источника	Порт назначения
TCP	23	23

[Справочник TCP/UDP портов](#)

> ICMP

> IP

▼ Группы протоколов

- echo-request
- https
- ssh_version_2

Трафик

Для проверки трафика по его содержимому [загрузите классификатор DPI](#) (Deep Packet Inspection).

Сохранить **Отмена**

Рисунок 16. Указание сетевых протоколов

11 Чтобы задать параметры регистрации IP-пакетов для правила:

11.1 В разделе **Регистрация IP-пакетов** нажмите .

11.2 Выберите состояние регистрации: **Включена**, **Отключена**, **Использовать значение, заданное в политике** или **Использовать значение, заданное в слое**.

Использовать значение, заданное в слое — в правило подставится значение, заданное в слое.

Использовать значение, заданное в политике — в правило подставится значение, заданное в политике. Если в политике не задано пользовательское значение, подставится

системное значение. Системное значение задано в политике по умолчанию для правил с выбранным действием.

Значение, используемое по умолчанию, будет зависеть от значений, заданных для слоя.

11.3 Нажмите **Сохранить**.

12 Чтобы задать параметры регистрации сессий для правила:

12.1 В разделе **Регистрация сессий** нажмите .

12.2 Выберите состояние регистрации: **Включена**, **Отключена** или **Использовать значение, заданное в политике** или **Использовать значение, заданное в слое**.

Использовать значение, заданное в слое — в правило подставится значение, заданное в слое.

Использовать значение, заданное в политике — в правило подставится значение, заданное в политике. Если в политике не задано пользовательское значение, подставится системное значение. Системное значение задано в политике по умолчанию для правил с выбранным действием.

Значение, используемое по умолчанию, будет зависеть от значений, заданных для слоя.

12.3 Если вы выбрали **Включена**:

12.3.1 Задайте параметры сессии.

12.3.2 Если в параметрах сессии вы выбрали **Расширенные настройки**, задайте значения для **Состояния сессии** или **Состояния TCP-сессии**.

12.4 Нажмите **Сохранить**.

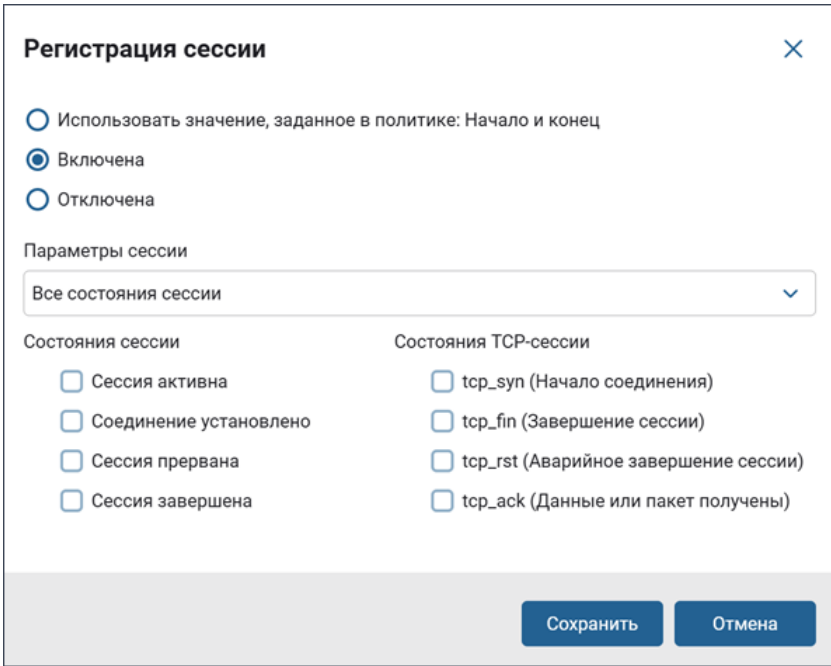


Рисунок 17. Настройка регистрации сессии в правиле

13 Чтобы **создать расписание**, в разделе **Условия фильтрации трафика** > **Расписание** нажмите **Добавить**.

14 Чтобы назначить правило на определенные устройства, а не на все целевые устройства политики (по умолчанию):

14.1 В разделе **Целевые устройства** нажмите .

14.2 Выберите **Избранные целевые устройства политики**.

14.3 Выберите устройства.

14.4 Нажмите **Сохранить**.

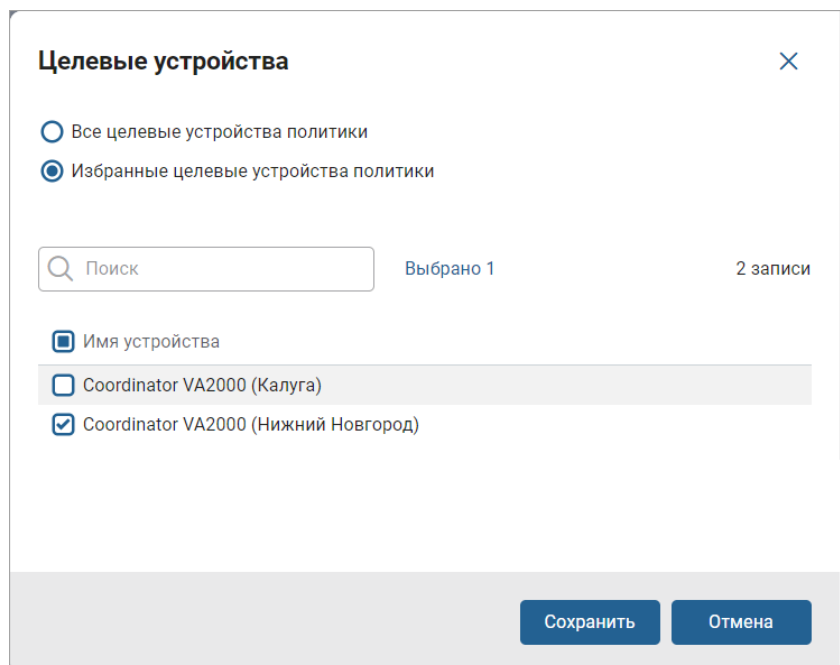


Рисунок 18. Выбор устройств для применения правила

15 Чтобы завершить создание правила, нажмите **Создать**.

Создание правил фильтрации по пользователям, приложениям и прикладным протоколам

Вы можете фильтровать туннелируемый трафик и транзитный трафик открытой сети. В правилах укажите пользователей, которые совпадают с учетными данными Active Directory или Captive Portal. [Имя пользователя в ViPNet Prime задайте латинскими буквами.](#)

Для фильтрации трафика по пользователям вы можете вручную ввести их имена. Такие имена должны совпадать с доменными именами пользователей Active Directory или Captive Portal. Взаимодействие с этими службами настраивается на шлюзе безопасности (см. в документации шлюза безопасности).



Примечание. Если IP-пакет попадает под действие правила фильтрации, в котором задан пользователь, то IP-адрес этого пользователя сопоставляется с адресом источника или назначения IP-пакета. Правило сработает, если адрес источника или назначения IP-пакета совпадет с адресом пользователя Active Directory или Captive Portal.

Для фильтрации трафика по пользователям, приложениям и прикладным протоколам:

- 1 Подключитесь к веб-интерфейсу.
- 2 Для фильтрации трафика по приложениям и прикладным протоколам [загрузите файл классификации DPI](#).
- 3 Выберите политику безопасности.
- 4 Выберите **Фильтрация трафика**.
- 5 На панели инструментов выберите тип трафика:
 - **Транзитный трафик открытой сети.**
 - **Трафик туннелируемых ресурсов.**
- 6 [Создайте правило](#) или измените созданное правило.
- 7 Для фильтрации трафика по пользователям:
 - 7.1 В разделе **Условия фильтрации трафика** > **Пользователи** нажмите **Добавить**.
 - 7.2 Выберите пользователей ViPNet Prime из списка.
 - 7.3 Чтобы добавить пользователей вручную, нажмите  **Новые пользователи** и введите доменные имена пользователей без указания домена. Допустимые символы: латинские буквы, цифры, «-», «_», «.».

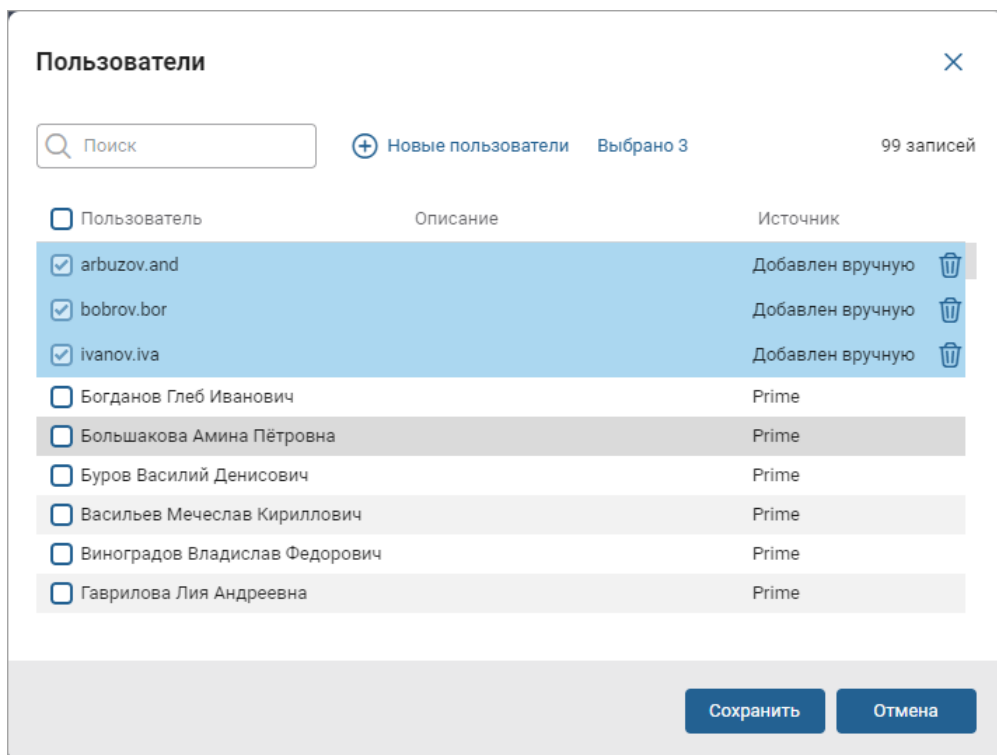


Рисунок 19. Добавление пользователей LDAP в правило DPI

7.4 Нажмите **Сохранить**.

8 Для фильтрации трафика по приложениям или прикладным протоколам:

8.1 Выберите раздел **Условия фильтрации трафика > Сервисы и приложения** и нажмите **Добавить**.

8.2 В группе **Трафик > Приложения** нажмите **Добавить** и выберите приложения.

8.3 В группе **Трафик > Протоколы** выберите прикладные протоколы.

8.4 Нажмите **Сохранить**.

9 Выберите устройства, к которым будет применено правило:

9.1 В разделе **Целевые устройства** нажмите **Добавить**.

9.2 Выберите устройства.

9.3 Нажмите **Сохранить**.

10 Чтобы **создать расписание**, выберите раздел **Условия фильтрации трафика > Расписание** и нажмите **Добавить**.

11 Чтобы завершить создание правила, нажмите **Создать**.

Правила фильтрации по странам

Правила фильтрации по странам — правила открытой сети, в параметрах которых указаны страны. Правила фильтрации по странам разрешают или блокируют трафик с IP-адресами, принадлежащими выбранным странам.

Правила фильтрации по странам поддерживает ViPNet Coordinator HW 5.



Внимание! О версиях ПО, поддерживающих правила фильтрации по странам и списки дополнений и исключений, уточняйте в документации на устройство.

Перед созданием правил фильтрации по странам:

- 1 Загрузите базу в ViPNet Prime Policy Management и назначьте ее в организацию.
- 2 На целевые устройства загрузите базу IP-адресов по странам.

В ViPNet Prime PMM нельзя выполнить поиск и фильтрацию данных в интерфейсе по правилам с фильтрацией по странам.

Создание расписаний

Чтобы правила фильтрации действовали в заданное время, создайте расписания. Если расписание не создано, правило фильтрации действует всегда.

Чтобы создать расписание:

- 1 Выберите политику.
- 2 Выберите **Фильтрация трафика**.
- 3 На панели инструментов выберите тип трафика.
- 4 Выберите правило и в столбце **Расписание** нажмите .
- 5 Выберите одно из действий:
 - Чтобы правило действовало в определенные дни недели, выберите дни недели и укажите временной интервал.

Рисунок 20. Создание расписания

- Чтобы правило действовало в течение периода времени (например, в течение двух недель), выберите **Период** и укажите временной интервал.

6 Для создания еще одного расписания нажмите .

7 Нажмите **Сохранить**.

Настройка исключений при блокировке пользовательского VPN-трафика

Если на устройстве пользователя ViPNet Client 5 с ViPNet EndPoint Protection (EPP) не выполнены политики [Zero Trust Network Access \(ZTNA\)](#) (настраиваются в ViPNet EPP Сервер), ViPNet EPP Агент блокирует пользовательский VPN-трафик.

Если на устройстве пользователя с ViPNet Client 5 не установлен или неработоспособен ViPNet EPP Агент, вы можете настроить блокировку пользовательского VPN-трафика для устройства. Подробнее см. «ViPNet Prime. Руководство администратора», «Блокировка VPN без ViPNet EPP». В этом случае клиент будет блокировать пользовательский VPN-трафик.

Чтобы пропускать трафик от узла к другим узлам [защищенной сети](#), создайте правило фильтрации с типом **Локальный трафик защищенной сети** и названием «Исключения из пользовательского защищенного трафика». Если название правила будет отличаться, оно не сработает на устройстве. Правило должно быть вторым по приоритету в списке правил политики безопасности, при взаимодействии с ViPNet EPP версии 1.7.1, для ViPNet EPP 1.8 правило располагайте первым.

Исключениями из блокировки пользовательского VPN-трафика при работе ZTNA могут выступать:

- ViPNet EPP Сервер.

Если ViPNet EPP Сервер расположен на узле защищенной сети, добавьте его в исключения.

Если ViPNet EPP Сервер расположен в открытой сети, исключения задавать не нужно.

- Исключения для работы ViPNet EPP Агент. Это узлы, с которых можно скачать ПО, обновления ПО, файлы, необходимые для выполнения политик ZTNA, или узлы, с которыми должна быть связь даже при невыполнении политик ZTNA.

Например, если в соответствии с политикой ZTNA на защищаемом устройстве должны быть установлены актуальные базы антивируса, то при блокировке пользовательского VPN-трафика, если базы не установлены, у устройства должен быть доступ к ресурсам с актуальными базами антивируса.

- Исключения при работе в защищенной сети.

Например, корпоративные DNS-серверы, серверы IP-телефонии, терминальные серверы.

Если исключение — клиент защищенной сети, выберите его в качестве назначения трафика, в качестве источника укажите целевое устройство.

Если исключение — туннелируемые координатором ресурсы, выберите координатор в качестве назначения трафика. В этом случае координатор не должен туннелировать другие ресурсы, кроме ресурсов-исключений ZTNA. Это означает, что должен быть отдельный координатор для туннелирования таких ресурсов, иначе правило фильтрации трафика от устройств пользователей к ресурсам не будет обработано.

Блокировка пользовательского VPN-трафика

- 1 При использовании политик ZTNA настройте их в ViPNet EPP Сервер. См. руководство администратора ViPNet EPP.
- 2 В ViPNet Prime VPN для клиентов включите функцию **Блокировка VPN без ViPNet EPP**.

Информация о функции войдет в дистрибутив ключей. Если клиент уже создан, информация о функции отправится на узел автоматически при обновлении справочников и ключей.

- 3 На устройствах пользователей установите:
 - ViPNet Client 5 и дистрибутив ключей;
 - ViPNet EPP Агент.
- 4 В результате пользовательский защищенный VPN-трафик заблокируется, если на устройстве пользователя:
 - не установлен или неработоспособен ViPNet EPP Агент;
 - не выполнены политики ZTNA (если используются).
- 5 Чтобы пропускать трафик от клиента к узлам защищенной сети, создайте правило фильтрации в ViPNet Prime Policy Management, см. ниже.

Настройка исключений из блокировки пользовательского VPN-трафика

- 1 Выберите организацию.
- 2 Выберите политику.
- 3 **Создайте правило фильтрации:**
 - 3.1 Выберите вкладку **Фильтрация трафика**.

- 3.2 На панели инструментов в списке выберите тип **Локальный трафик защищенной сети**.
- 3.3 Нажмите **Добавить правило**.
- 3.4 Введите название правила **Исключения из пользовательского защищенного трафика**.
- 3.5 Выберите действие **Пропускать**.
- 3.6 В качестве источника выберите целевое устройство.
- 3.7 В качестве назначения выберите устройства защищенной сети или группу устройств защищенной сети: клиент или координатор, который туннелирует только ресурсы-исключения. Не выбирайте системные группы:
- Широковещательная рассылка.
 - Многоадресная рассылка.
 - Клиенты.
 - Шлюзы безопасности.
- 3.8 В разделе **Сервисы** оставьте значения прикладных протоколов и приложений пустыми, что означает **Любые**.
- 3.9 В разделе **Расписание** оставьте значение по умолчанию — **Всегда**.
- 3.10 Чтобы пропускать трафик от клиента к исключениям-туннелируемым ресурсам, на координаторе не регистрируйте другие туннелируемые ресурсы.
- 3.11 Настройте для правила приоритет 1.
- 3.12 В качестве целевого устройства выберите клиенты.
- 4 Отправьте изменения политики безопасности на клиенты.

Правила трансляции адресов (NAT)

Правила трансляции сетевых адресов (NAT) обычно применяются на шлюзах безопасности, установленных на границе внутренних и внешних сетей.

При трансляции адреса локальной сети преобразуются в адреса глобальной сети и наоборот. NAT с трансляцией портов преобразует сетевые адреса и порты TCP или UDP в один IP-адрес и номер порта. Также транслируются адреса для пакетов ICMP-сообщений и протокола IP.

В одном правиле вы можете задать как трансляцию источника, так и трансляцию назначения. Если в правиле не указаны протоколы, то оно применяется ко всем протоколам.

Каждому правилу трансляции сетевых адресов присваивается идентификатор, который уникален в организации.

Создание правил трансляции адресов

- 1 Подключитесь к веб-интерфейсу.
- 2 Выберите политику или [создайте новую политику безопасности](#).
- 3 Для удобства [создайте группы](#), в которых могут быть:
 - IP-адреса и диапазоны IP-адресов;
 - группы протоколов;
 - адреса подсетей.
- 4 Выберите **Трансляция адресов (NAT)**.
- 5 Нажмите  **Добавить правило**. Если вы хотите задать правилу приоритет при создании:
 - 5.1 Выберите правило из списка.
 - 5.2 Нажмите , чтобы создать правило выше, или , чтобы создать правило ниже.
- 6 Введите название правила.
- 7 Чтобы транслировать адреса отправителей пакетов:
 - 7.1 В разделе **Условия трансляции адресов > Источники** нажмите **Добавить**.
 - 7.2 В разделе **Исходные источники**:
 - задайте IP-адреса или доменные имена открытой сети;
 - выберите группы адресов открытой сети.

8 Чтобы задать трансляцию адресов отправителей, в разделе **Транслированный источник** выберите **Заменять исходный адрес источника**:

- **IP-адрес исходящего интерфейса** — адрес отправителя будет заменяться на адрес внешнего интерфейса шлюза безопасности, который определяется автоматически.
- **другой IP-адрес** и введите IP-адрес сетевого интерфейса шлюза безопасности.

9 Чтобы транслировать адреса получателей пакетов:

9.1 В разделе **Условия трансляции адресов > Назначения** нажмите **Добавить**.

9.2 В разделе **Исходные назначения**:

- задайте IP-адреса или доменные имена открытой сети;
- выберите группы адресов открытой сети.

Назначения

Исходные назначения

✓ Адреса открытой сети

IP-адрес или DNS-имя

203.0.113.200/32

Отделяйте значения запятой или переводом на новую строку. Используйте знак "." для диапазона IP-адресов и знак "/" для маски подсети.

✓ Группы адресов открытой сети

Транслированное назначение

☒ Заменять исходный адрес назначения на

* IP-адрес Порт

192.168.1.200

Сохранить Отмена

Рисунок 21. Задание назначения трансляции адресов

10 Чтобы задать трансляцию адреса получателя:

10.1 В разделе **Транслированное назначение** выберите **Заменять исходный адрес назначения на**.

10.2 Введите IP-адрес.

11 Для трансляции порта назначения:

11.1 В разделе **Условия трансляции адресов > Сервисы** нажмите **Добавить**.

11.2 Задайте протокол TCP или UDP одним из следующих способов:

- В разделе **TCP / UDP** выберите протокол.
Введите порты источника и назначения. Для просмотра часто встречающихся стандартных портов нажмите **Справочник TCP/UDP портов**.
- В разделе **IP** выберите код протокола 6 (TCP) или 17 (UDP).

11.3 Задайте порт, на который будет транслироваться трафик:

11.3.1 В разделе **Условия трансляции адресов > Назначения** нажмите **Добавить**.

11.3.2 В разделе **Транслированное назначение** выберите **Заменять исходный адрес назначения**.

11.3.3 Введите порт.

11.4 Нажмите **Сохранить**.

12 Для преобразования адресов пакетов ICMP-сообщений:

12.1 В разделе **Условия трансляции адресов > Сервисы** нажмите **Добавить**.

12.2 В разделе **ICMP** задайте тип и код ICMP-сообщения.

12.3 Нажмите **Сохранить**.

13 Чтобы назначить правило на отдельные устройства из политики:

13.1 В разделе **Целевые устройства** нажмите .

13.2 Выберите **Избранные целевые устройства политики**. По умолчанию правило назначается на все целевые устройства политики.

13.3 Выберите устройства.

13.4 Нажмите **Сохранить**.

14 Чтобы завершить создание правила, нажмите **Создать**.

Копирование, изменение и удаление правил

- 1 Выберите организацию.
- 2 Выберите политику.
- 3 Для удобства поиска правила выберите слой, тип трафика и другие параметры поиска: идентификатор, название, источники, назначения, пользователи, целевые устройства, комментарий, состояние правил.
- 4 Выберите правила флажками.
- 5 Чтобы скопировать правила внутри слоя, нажмите  > **Копировать**. Копии правил будут иметь префикс *Copy* и расположены с приоритетом ниже исходных правил.
- 6 Чтобы переместить правила в другой слой, нажмите  > **Переместить в другой слой**. Правила будут перемещены с наименьшим приоритетом, в конец слоя.
- 7 Чтобы скопировать правила в другую политику:
 - 7.1 Нажмите  > **Копировать в**.
 - 7.2 Выберите политику.
 - 7.3 Выберите слой. Правила будут скопированы с наименьшим приоритетом, в конец слоя.
- 8 Чтобы изменить приоритет правил, нажмите  или . Если вы выбрали несколько правил, то они перемещаются по списку вместе и располагаются друг за другом.

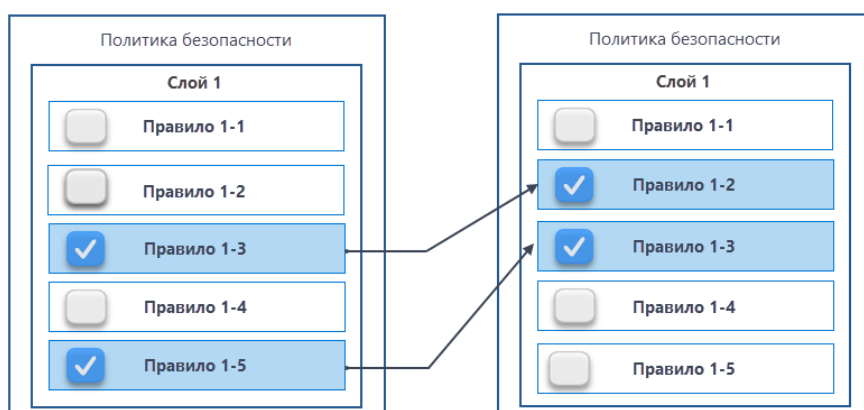


Рисунок 22. Повышение приоритета нескольких правил

- 9 Чтобы изменить один из параметров правила, наведите указатель мыши и нажмите .
- 10 Чтобы исключить правила из результирующей политики, нажмите  > **Изменить состояние** > **Отключить**. Правила в списке примут неактивный вид.
- 11 Чтобы изменить список целевых устройств, на которые назначены правила:

11.1 Нажмите  > **Назначить на устройство.**

11.2 Выберите

- **Все целевые устройства политики** — чтобы назначить на все устройства,
- **Избранные целевые устройства политики** > выберите устройства, на которые назначить правила.

12 Чтобы изменить настройки регистрации IP-пакетов или сессий для правил:

12.1 Нажмите  > **Изменить настройки регистрации.**

12.2 Выберите состояние регистрации IP-пакетов: **Включена**, **Отключена**, **Использовать значение, заданное в слое** или **Использовать значение, заданное в политике**. Если вы выбрали несколько правил, вы можете только включить или отключить параметры регистрации IP-пакетов.

При выборе **Использовать значение, заданное в слое** в правило подставится значение, заданное в данный момент для слоя. Если для слоя не задано значение, подставится значение, заданное для политики.

При выборе **Использовать значение, заданное в политике** в правило подставится значение, заданное в данный момент для политики. Если и в политике не задано пользовательское значение, подставится системное значение. Системное значение задано по умолчанию для правил с выбранным действием.

12.3 Выберите состояние регистрации сессии: **Включена**, **Отключена** или **Использовать значение, заданное в слое** или **Использовать значение, заданное в политике**. Если вы выбрали несколько правил, вы можете только включить или отключить параметры регистрации сессии.

При выборе **Использовать значение, заданное в слое** в правило подставится значение, заданное в данный момент для слоя. Если для слоя не задано значение, подставится значение, заданное для политики.

При выборе **Использовать значение, заданное в политике** в правило подставится значение, заданное в данный момент для политики. Если и в политике не задано пользовательское значение, подставится системное значение. Системное значение задано по умолчанию для правил с выбранным действием.

12.4 Если вы выбрали **Включена**:

12.4.1 Задайте параметры сессии.

12.4.2 Если в параметрах сессии вы выбрали **Расширенные настройки**, задайте значения для **Состояния сессии** или **Состояния TCP-сессии**.

12.5 Нажмите **Сохранить**.

Вы можете изменить параметры регистрации только IP-пакетов, только сессий или оба сразу.

13 Чтобы удалить правила:

13.1 Нажмите  > **Удалить**.

13.2 Подтвердите удаление. Правила из общего слоя удаляются из всех политик, в которые добавлен общий слой.

14 Нажмите **Управлять политикой** > **Отправить изменения на устройства**.

Если в общем слое вы изменяете приоритет правила, удаляете правило, включаете или отключаете правило, то это повлияет на все политики, в которых этот слой используется.



Примечание. Сообщения об этом отображаются однократно за сессию браузера.

Просмотр состояний правил

- 1 Выберите политику.
- 2 Выберите **Фильтрация трафика** или **Трансляция адресов (NAT)**.
- 3 В списке состояния правил выберите одно из значений:
 - **Новое** — чтобы отобразить правила, которые были назначены, но еще не отправлены на устройства:
 - новые правила, которые ни разу не отправлялись ни на одно устройство политики, в том числе скопированные правила и правила из общего слоя;
 - правила, которые были созданы в выключенном состоянии;
 - правила, которые были выключены, и после этого была отправлена политика на устройства.
 - **Отключено** — чтобы найти неактивные правила, которые были отключены.

Просмотр срабатываний правил

Чтобы оптимизировать правила или выявить аномалии в сети, отслеживайте количество срабатываний правил на шлюзах безопасности ViPNet Coordinator HW 5 версии 5.3 и выше и ViPNet xFirewall версии 5.7.5 и выше.

Правила, которые срабатывают чаще других, располагайте в начале списка. Это позволит экономить вычислительные ресурсы шлюза безопасности.

Порядок передачи информации о срабатывании правил с шлюза безопасности в ViPNet Prime PMM:



Примечание. Описание приведено для ViPNet Coordinator HW версии 5.3 и выше и ViPNet Prime NVS версии 1.6 и выше.

1 Шлюз ViPNet Coordinator HW:

- собирает информацию о срабатывании правил межсетевого экрана;
- получает информацию о подключении к ViPNet Prime NVS из дистрибутива ключей;
- отправляет информацию о срабатывании правил в ViPNet Prime NVS по защищенному каналу VPN.



Внимание! Для работы счетчиков в ViPNet Prime PMM могут потребоваться дополнительные действия.

На ViPNet Coordinator HW версии ниже 5.3.2 может потребоваться установить справочник `nvs.info` вручную. См. «ViPNet Prime Network Visibility System. Руководство администратора», раздел «Настройка передачи значений со счетчиков срабатывания правил межсетевого экрана».

Для ViPNet xFirewall версии 5.7.5 и 5.7.6 необходимо принудительно отправить справочники и ключи после установки дистрибутива ключей на узле.

- 2 ViPNet Prime NVS получает данные от шлюза безопасности. Модуль ViPNet Prime PMM запрашивает данные у ViPNet Prime NVS.
- 3 ViPNet Prime NVS отправляет информацию в ViPNet Prime PMM.
- 4 Администратор просматривает информацию о срабатывании правил в ViPNet Prime PMM.

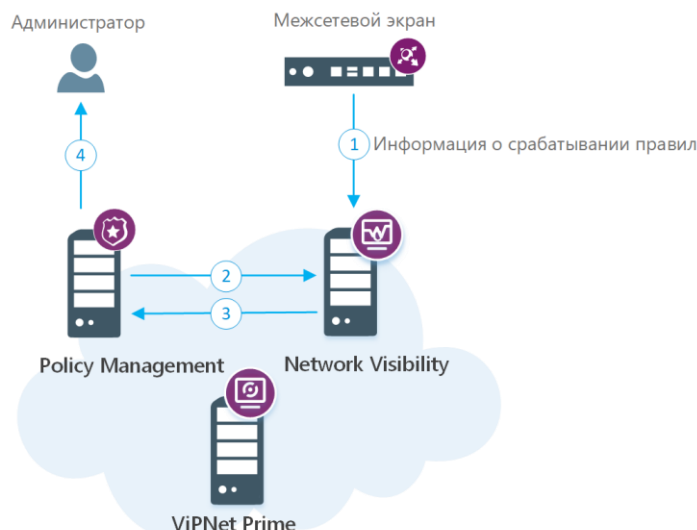


Рисунок 23. Получение информации о срабатывании правил

Чтобы просмотреть срабатывания правил:

- 1 Выберите политику безопасности, тип правил.
- 2 В столбце **Срабатывания** просмотрите значение.

Если устройство не поддерживает отправку информации о срабатывании правил, то для него количество срабатываний не отображается.

Если устройство не добавлено в перечень устройств, за которыми осуществляется мониторинг ViPNet Prime NVS, количество срабатываний счётчиков не отображается. Для работы счётчиков распределите лицензию `monitoring_nodes` на узел и отправьте новые справочники и ключи.



Примечание. Если на сервере ViPNet Prime NVS на жестком диске осталось менее 10% свободного места, то новые данные мониторинга не сохраняются. Для счетчика срабатываний правил отображается **Нет данных**.

Счетчики срабатываний обновляются каждый час. Чтобы вручную обновить счетчики срабатываний правил:

- 1 Выберите политику безопасности.
- 2 Нажмите **Управлять политикой** и выберите **Обновить счетчики срабатываний правил**.

Вы можете использовать информацию о срабатывании правил, чтобы повысить скорость фильтрации трафика на устройствах. Для этого:

- У правил, которые срабатывают чаще других, повысьте приоритет ↑.
- Удалите или отключите неиспользуемые правила или уменьшите их приоритет ↓. У правил, которые не используются, отсутствуют срабатывания правил — в столбце **Срабатывания** значение 0.

Сброс счетчиков срабатываний правил

Когда вы изменяете правила, счетчики срабатываний не сбрасываются автоматически, они продолжают суммироваться с предыдущими значениями.

Чтобы собрать актуальные данные с текущего момента, сбросьте счетчики срабатываний правил и просмотрите статистику срабатываний с момента сброса.

Чтобы сбросить значения счетчика:

- 1 Выберите политику безопасности.
- 2 Нажмите **Управлять политикой > Сбросить счетчики при отправке изменений**.
- 3 Нажмите **Подтвердить**.

Политика безопасности примет статус **Изменена**. При необходимости нажмите **Отменить сброс счетчиков**.

- 4 Чтобы применить изменения на целевых устройствах, нажмите **Управлять политикой > Отправить на устройства**.

Счетчики срабатываний правил сбросятся на целевых устройствах только [после отправки изменений](#).

Поиск правил в журнале событий

Правилам фильтрации трафика и трансляции адресов назначаются идентификаторы (ID) — номера правил, которые уникальны в рамках одной организации и имеют значения от 200 001 до 4 000 000 (не включительно). Информация об идентификаторе правила записывается в журнал событий при следующих действиях с правилом: удаление правил, удаление слоев, создание нового правила.

Если правило было удалено, вы все равно сможете найти его в **Главная консоль**  > **Журнал событий**. Это может быть полезно при расследовании событий информационной безопасности, когда нужно узнать, какое правило сработало и привело к определенному событию на шлюзе безопасности.

Удаление правила фильтрации транзитного трафика открытой сети ✕
Успешно завершено

Информация о событии

Название	Удаление правила фильтрации транзитного трафика открытой сети
Идентификатор	d334bcd6-d969-4c72-9e2a-466e08deced2
Статус	Успешно завершено
Дата и время	17.10.2024 18:06:14.163

Объект события

Имя	Web
Идентификатор	5439b8d4-3af3-408e-8c06-e10078ef70f1

Дополнительные данные

Слой

Идентификатор	4449f19c-dcc1-4e18-bc49-f40692facab6
Наименование	Слой по умолчанию

Политика безопасности

Идентификатор	16e49812-1219-44e7-afb0-a70a28e640ea
Наименование	Политика 3

Идентификатор	5439b8d4-3af3-408e-8c06-e10078ef70f1
Название	Web
Тип	Транзитный фильтр открытой сети
Действие	Блокировать
Состояние	Включено
DPI условия	Любые
Идентификатор правила (ID)	318749
Пользователи	Любые
Источники	
Устройства	

Рисунок 24. Просмотр события удаления правила в журнале событий

5

Работа с группами объектов

О группах объектов	102
Группы адресов открытой сети	104
Группы протоколов	105
Группы сетевых интерфейсов	107
Группы устройств защищенной сети	109
Группы стран	110
Списки дополнений и исключений для стран	111
Списки блокировки IP-адресов	113

О группах объектов

Группы объектов упрощают создание правил фильтрации трафика и трансляции адресов. Они объединяют несколько значений одного типа и могут быть заданы при настройке параметров правил фильтрации вместо отдельных объектов.

Существуют следующие виды групп:

- Системные группы объектов.
- Пользовательские группы объектов.

Системные группы объектов — встроенные объекты с фиксированными именами. Вы можете использовать их в правилах фильтрации для задания отправителей и получателей IP-пакетов, а также в пользовательских группах объектов. Системные группы объектов нельзя изменить или удалить.

В ViPNet Prime Policy Management отсутствуют системные группы объектов PrivateNetworkIP, HttpProxyUsers, InternetIP и возможность их использования при настройке правил фильтрации.

Таблица 1. Системные группы объектов

Имя группы объектов	Значение
Клиенты	Все клиенты. Группа используется в качестве источника или назначения в правилах фильтрации локального трафика защищенной сети и трафика туннелируемых ресурсов
Шлюзы безопасности	Все координаторы и межсетевые экраны ViPNet xFirewall
Широковещательная рассылка	Все широковещательные адреса. Используются при создании правил фильтрации широковещательных пакетов
Многоадресная рассылка	Групповой (multicast) IP-адрес из диапазона 224.0.0.0-239.255.255.255
Целевое устройство	Устройства сети ViPNet, на которые назначаются правила фильтрации
Туннелируемые адреса устройства	Все IP-адреса, туннелируемые координатором

Пользовательские группы объектов — группы объектов, создаваемые администратором. Из групп вы можете исключать объекты. В группы и исключения из групп вы можете добавить другие группы объектов того же типа или некоторые системные группы объектов. Максимальный уровень вложенности групп — 10, кроме групп стран, у которых максимальный уровень вложенности — 1.

Пользовательские группы объектов делятся на:

- Устройства защищенной сети — группа устройств сети ViPNet. Используется в правилах фильтрации локального трафика защищенной сети и трафика туннелируемых ресурсов.

- Адреса открытой сети — IP-адрес, диапазон IP-адресов или доменное имя устройств открытой сети. Используется в правилах трансляции адресов и правилах фильтрации, за исключением правил фильтрации локального трафика защищенной сети.
- Сетевые интерфейсы — любая комбинация сетевых интерфейсов или IP-адресов интерфейсов. Используется в правилах фильтрации, за исключением правил фильтрации локального трафика защищенной сети.
- Протоколы — любая комбинация протоколов и портов. Используется во всех типах правил фильтрации трафика и в правилах трансляции адресов.
- Страны — группа стран, которая используется в правилах фильтрации по странам.

Также вы можете использовать групповые объекты для политики безопасности:

- Блокировка IP-адресов — список IP-адресов, который добавляется в политику безопасности и используется для блокировки трафика с IP-адресов на целевых устройствах.
- Список дополнений и исключений IP-адресов для стран — расположен в разделе **Страны**. Список IP-адресов, который добавляется в политику безопасности, чтобы изменить списки IP-адресов, относящиеся к странам.

Группы адресов открытой сети

Чтобы создать группу:

- 1 На панели слева выберите **Адреса открытой сети**.
- 2 Нажмите  **Добавить группу**.
- 3 Введите имя группы.
- 4 Добавьте в группу IP-адреса и доменные имена. Повторяющиеся значения будут выделены цветом. Если значения не указаны, в состав группы будут включены все адреса открытой сети.
- 5 Чтобы добавить в группу созданные ранее группы открытой сети:
 - 5.1 Нажмите **Добавить**.
 - 5.2 Выберите группу.
 - 5.3 Нажмите **Сохранить**.
- 6 Чтобы исключить из группы IP-адреса, доменные имена или вложенные группы, в разделе **Исключения** введите значения.
- 7 Нажмите **Создать**.

Чтобы изменить группу, в столбце **Группа** или **Состав** нажмите .

Чтобы удалить группы:

- 1 Выберите группы и нажмите .
- Нельзя удалить группы, которые используются в правилах.
- 2 Подтвердите удаление.

Группы протоколов

Чтобы создать группу:

- 1 На панели слева выберите **Протоколы**.
- 2 Нажмите **Добавить группу**.
- 3 Введите имя группы.
- 4 Чтобы добавить протокол TCP или UDP с номером порта источника и назначения, в разделе **Состав > TCP / UDP** выберите протокол и укажите номера портов.

Протокол	Порт источника	Порт назначения		
TCP				
TCP	20-21	20-21		

[Справочник TCP/UDP портов](#)

Рисунок 25. Задание сетевого порта TCP или UDP

- 5 Чтобы добавить протокол ICMP, в разделе **Состав > ICMP** выберите тип и код ICMP-сообщения.
- 6 Чтобы для протокола ICMP задать все типы и все коды сообщений, в разделе **Состав > IP** добавьте протокол ICMP.
- 7 Чтобы добавить другие протоколы, в разделе **Состав > IP** выберите протокол или введите его код. Чтобы добавить еще один протокол, нажмите .

Новая группа протоколов

✕

▼ ICMP

Тип ICMP-сообщения

Код ICMP-сообщения

30 - Traceroute

8 - Echo

3 - Destination Unreachable

3 - Port Unreachable

🗑️

🗑️

🗑️

+

▼ IP

Код IP-протокола

241 - ViPNet - ViPNet protected protocol

6 - TCP - Transmission Control

2 - IGMP - Internet Group Management

1 - ICMP - Internet Control Message

🗑️

🗑️

🗑️

🗑️

+

> Группы протоколов

Исключения

> TCP / UDP

> ICMP

> IP

Создать

Отмена

Рисунок 26. Добавление сетевых протоколов в группу

- 8 Чтобы добавить в состав группы созданные ранее группы протоколов:
 - 8.1 Нажмите **Добавить**.
 - 8.2 Выберите группу.
 - 8.3 Нажмите **Сохранить**.
- 9 Чтобы исключить из группы протоколы или вложенные группы, в разделе **Исключения** укажите объекты.

Чтобы изменить группу, в столбце **Группа** или **Состав** нажмите .

Чтобы удалить группы:

- 1 Выберите группы и нажмите .
- Нельзя удалить группы, которые используются в правилах.
- 2 Подтвердите удаление.

Группы сетевых интерфейсов

Чтобы создать группу:

- 1 На панели слева выберите **Сетевые интерфейсы**.
- 2 Нажмите **Добавить группу**.
- 3 Введите имя группы.
- 4 Укажите идентификаторы или IP-адреса сетевых интерфейсов.

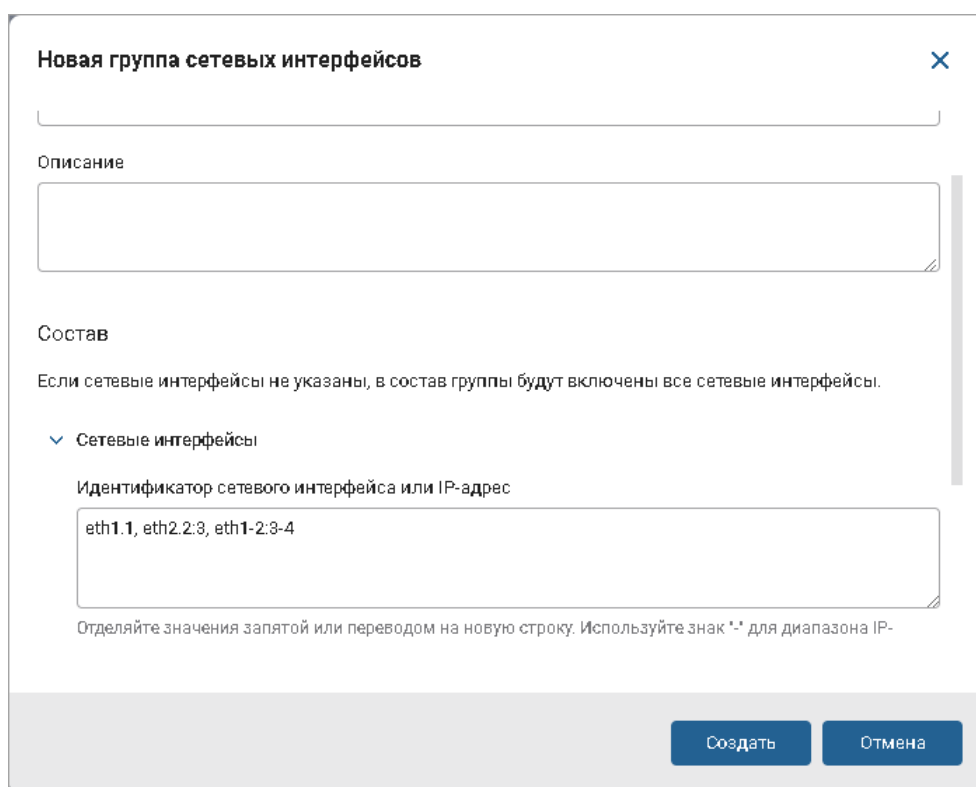


Рисунок 27. Добавление сетевых интерфейсов устройств

- 5 Чтобы добавить в состав группы созданные ранее группы сетевых интерфейсов:
 - 5.1 Нажмите **Добавить**.
 - 5.2 Выберите группу.
 - 5.3 Нажмите **Сохранить**.
- 6 Чтобы исключить идентификаторы или IP-адреса сетевых интерфейсов из заданного диапазона, в разделе **Исключения** > **Сетевые интерфейсы** задайте значения.
- 7 Нажмите **Создать**.

Чтобы изменить группу, в столбце **Группа** или **Состав** нажмите .

Чтобы удалить группы:

- 1 Выберите группы и нажмите .

Нельзя удалить группы, которые используются в правилах.

- 2 Подтвердите удаление.

Группы устройств защищенной сети

Чтобы создать группу:

- 1 На панели слева выберите **Устройства защищенной сети**.
- 2 Нажмите  **Добавить группу**.
- 3 Введите имя группы.
- 4 Добавьте в состав группы устройства сети ViPNet. Если устройства не указаны, в состав группы войдут все устройства защищенной сети организации или подразделения.
- 5 Чтобы добавить в состав группы созданные ранее группы:
 - 5.1 Нажмите **Добавить**.
 - 5.2 Выберите группу.
 - 5.3 Нажмите **Сохранить**.
- 6 Чтобы добавить в группу устройства с именем по шаблону, в разделе **Состав > Шаблоны имен устройств защищенной сети** введите имя с использованием шаблона:
 - o * — любое количество символов;
 - o ? — одиночный символ.
- 7 Чтобы исключить из группы устройства или вложенные группы, в разделе **Исключения** укажите объекты.
- 8 Нажмите **Создать**.

Чтобы изменить группу, в столбце **Группа** или **Состав** нажмите .

Чтобы удалить группы:

- 1 Выберите группы и нажмите .
- Нельзя удалить группы, которые используются в правилах.
- 2 Подтвердите удаление.

Группы стран

Чтобы создать группу:

- 1 На панели слева выберите **Страны**.
- 2 На вкладке **Группы стран** нажмите **Добавить группу**.
- 3 Укажите имя группы и описание.
- 4 В разделе **Страны** нажмите **Добавить**.
- 5 Выберите страны и нажмите **Сохранить**.

При выборе стран вы можете воспользоваться поиском по двухбуквенному коду или названию страны.

Вы можете добавить до 1000 значений в состав групп стран. При задании имени группы учитывайте, что в ViPNet Prime Policy Management все групповые объекты, в том числе разных типов, должны иметь уникальные имена.

Чтобы изменить список группы, рядом с заголовком **Страны** нажмите  и измените список.

- 6 Нажмите **Сохранить**.

Чтобы изменить группу стран:

- 1 На панели слева выберите **Страны**.
- 2 На вкладке **Группы стран** в строке выбранной группы нажмите .
- 3 Измените состав группы и нажмите **Сохранить**.

Чтобы удалить группу стран:

- 1 На панели слева выберите **Страны**.
- 2 На вкладке **Группы стран** выберите одну или несколько групп и на панели сверху нажмите .

Вы не можете удалить группу стран, если она используется в правилах.

- 3 Вы можете просмотреть, в каких правилах используется группа, для этого в предупреждении о невозможности удаления нажмите **Подробнее** и в строке группы нажмите **Правила**.

Списки дополнений и исключений для стран

Вы можете создать список дополнений или исключений IP-адресов страны, из которых разрешено или запрещено обмениваться трафиком с защищенной сетью. Список используется в политике безопасности, чтобы корректировать список IP-адресов стран, заданных в базе стран. Список дополнений и исключений используется только с правилами, которые отправляются на устройства из ViPNet Prime. С правилами, созданными на устройствах, список дополнений и исключение не используется.

Чтобы создать список дополнений и исключений:

- 1 На панели слева выберите **Страны**.
- 2 Выберите вкладку **Дополнения и исключения для стран**.
- 3 Нажмите **Добавить список**.
- 4 Укажите имя группы и описание.
- 5 В разделе **Страны** нажмите **Добавить**.
- 6 Выберите страну.
- 7 В поле **Дополнения** укажите IP-адреса, которые нужно добавить к IP-адресам выбранной страны.

Максимальное количество значений в дополнениях для одной страны — 1000. В рамках одной страны нельзя добавить пересекающиеся IP-адреса и диапазоны IP-адресов.

- 8 В поле **Исключения** укажите IP-адреса, которые нужно исключить из перечня IP-адресов выбранной страны.

Максимальное количество значений в исключениях для одной страны — 1000. В рамках одной страны нельзя добавить пересекающиеся IP-адреса и диапазоны IP-адресов. Нельзя добавлять в дополнения и исключения одной страны пересекающиеся IP-адреса.

- 9 Нажмите **Сохранить**.

В один список вы можете добавить несколько стран с дополнениями и исключениями.

Чтобы изменить список дополнений и исключений IP-адресов страны, в разделе с этой страной нажмите  > **Изменить** и измените списки IP-адресов.

Чтобы удалить список дополнений и исключений IP-адресов страны, в разделе с этой страной нажмите  > **Удалить**.

- 10 Сохраните список.

Чтобы просмотреть состав списка, нажмите на него.

Чтобы изменить список дополнений и исключений для стран:

1 Нажмите на список и выполните одно из действий:

- на панели справа нажмите  напротив страны;
- нажмите  > **Изменить** и в разделе со страной нажмите  > **Изменить**.

2 Внесите изменения в список и сохраните его.

Чтобы удалить список:

1 Выберите списки и нажмите .

Нельзя удалить списки, которые используются в политиках.

2 Подтвердите удаление.

Чтобы скопировать список, выберите список и на панели сверху нажмите . В перечне списков появится новый список с префиксом *Сору*. Вы можете копировать только по одному списку.

В одной организации вы можете создать не более 65 535 списков дополнений и исключений для стран.

Списки блокировки IP-адресов

Вы можете управлять блокировкой трафика на целевых устройствах с помощью создания списков IP-адресов, с которыми требуется блокировать трафик. Списки отправляются из ViPNet Prime PMM на устройства. Список блокировки IP-адресов добавить или обновить в ViPNet Prime Policy Management может только администратор, обновлять его из указанной точки публикации нельзя.

У списка блокировки IP-адресов приоритет выше приоритета любых правил: если IP-адрес указан в списке блокировки, не получится разрешить обмен трафиком с IP-адресом с помощью правил.

Чтобы добавить список блокировки:

1 Подготовьте файл со списком блокировки:

- Формат — CSV или TXT.
- Кодировка — UTF-8.
- Объем — не более 50 Мбайт.
- IP-адреса в формате IPv4, могут содержать маску подсети в нотации CIDR или указываться в виде диапазона. В качестве разделителя IP-адресов в файле можно использовать пробел, табуляцию, запятую, точку с запятой или переход на новую строку.
- Количество записей — не более 2 миллионов. Если в списке какие-то записи не соответствуют формату, они отбросятся при загрузке списка.

Если в строке несколько записей указаны через разделитель, после загрузки файла в списке останется только запись, указанная до разделителя, если она соответствует формату.

```
1.1.1.1
1.1.1.2-1.1.1.5
1.1.1.4
1.1.1.10
1.1.1.25
1.1.1.26
1.1.1.24-1.1.1.31
0.0.0.0-255.255.255.255
84.252.86.87
84.252.86.206
84.252.87.198
192.168.0.0-192.168.0.255
192.168.1.0-192.168.1.255
```

Рисунок 28. Пример списка блокировки IP-адресов

2 На панели слева выберите **Блокировка IP-адресов**.

3 Нажмите **Добавить список**.

4 Введите имя списка и комментарий.

Имя должно быть уникальным в рамках всех имен групповых объектов организации.

5 Загрузите файл: рядом с полем **Файл** нажмите и выберите файл со списком IP-адресов, трафик с которых необходимо блокировать на целевых устройствах.

6 Нажмите **Сохранить**.

В разделе **Блокировка IP-адресов** появится панель с информацией о загруженном списке.

Для одной организации вы можете загрузить до 10 списков блокировки.

Чтобы изменить список блокировки IP-адресов:

- 1 На панели списка нажмите  > **Изменить**.
- 2 Загрузите новый файл со списком IP-адресов.
- 3 Нажмите **Сохранить**.

Чтобы скачать список блокировки IP-адресов, на панели списка нажмите  > **Скачать**. Список блокировки IP-адресов сохранится в файл `<имя_списка>-YYYY-MM-DD-hh-mm.txt`

Чтобы удалить список блокировки IP-адресов:

- 1 На панели списка нажмите  > **Удалить**. Нельзя удалить списки, которые используются в политиках.
- 2 Подтвердите удаление списка.

Поиск по правилам и группам

Вы можете выполнить поиск по значениям параметров правил или групп. Для этого:

- 1 На панели слева выберите:
 - **Политики** и выберите политику — чтобы выполнить поиск по значениям параметров правил.
 - Группу объектов — чтобы выполнить поиск по значениям параметров групп.
- 2 Слева от поля **Поиск** нажмите  и выберите параметр, по которому требуется поиск.

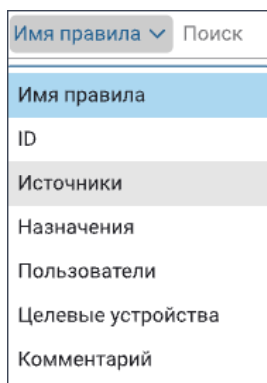


Рисунок 29. Выбор параметра правила для поиска

В правилах фильтрации вы можете искать по имени, ID, источникам, назначениям, пользователям, целевым устройствам, комментариям. В правилах трансляции — по имени правила, ID, исходным источникам и назначениям, целевым устройствам и комментариям. В группах вы можете искать по имени группы, составу и исключениям, описанию.

3 Для поиска введите от 1 до 1000 символов. Регистр на поиск не влияет.

4 Нажмите  или клавишу **Enter**.

Отобразится результат поиска — правила и группы, которые содержат значение, введенное в строку поиска.

Поиск осуществляется до 10 уровня вложенности групп. Максимальное время поиска — 10 минут.

После поиска по группам вы можете перейти к просмотру состава группы и изменить ее состав. Также вы можете изменить параметры найденных правил.

Также вы можете выполнить поиск по параметрам групп и правил при удалении группы: в окне просмотре списка групп и правил, где используется удаляемая группа.



Ограничения в названиях объектов

В именах пользователей, устройств или названий организаций в системе управления ViPNet Prime Policy Management запрещено использовать:

- специальные символы: \ / : * ? < > | &
- знаки абзаца и другие знаки форматирования, кроме пробелов.

Если использовать указанные символы или зарезервированные слова в качестве имени объекта, возникнет ошибка создания объекта.

Чтобы с помощью модуля ViPNet Prime PMM фильтровать трафик по пользователям, имена пользователей должны быть заданы латинскими буквами.

В

Описание ошибок в журнале ошибок импорта из ViPNet Policy Manager

При импорте в ViPNet Prime Policy Management шаблонов политик безопасности, экспортированных из ViPNet Policy Manager могут появляться ошибки, которые фиксируются в журнале ошибок. В таблице приведено описание некоторых ошибок, предупреждений и действия по их устранению.

Ошибка	Описание
Ошибки, при которых импорт будет остановлен до начала обработки файлов с шаблонами	
The file vw_PolicyTemplates.xml is missing.	Отсутствует обязательный файл vw_PolicyTemplates.xml, выгруженный из базы данных ViPNet Policy Manager. Экспортируйте таблицу из базы данных ViPNet Policy Manager и повторите импорт
The file vw_NetworkNodes.xml is missing.	Отсутствует обязательный файл vw_NetworkNodes.xml, выгруженный из базы данных ViPNet Policy Manager. Экспортируйте таблицу из базы данных ViPNet Policy Manager и повторите импорт
The file vw_ManagedObjectTemplates.xml is missing.	Отсутствует обязательный файл vw_ManagedObjectTemplates.xml, выгруженный из базы данных ViPNet Policy Manager. Экспортируйте таблицу из базы данных ViPNet

Ошибка	Описание
	Policy Manager и повторите импорт
The file vw_PolicyTemplates.xml is invalid or corrupt.	Файл vw_PolicyTemplates.xml недействителен или поврежден. Повторите экспорт таблиц из базы данных и загрузите новый файл
The file vw_NetworkNodes.xml is invalid or corrupt.	Файл vw_NetworkNodes.xml недействителен или поврежден. Повторите экспорт таблиц из базы данных и загрузите новый файл
The file vw_ManagedObjectTemplates.xml is invalid or corrupt.	Файл vw_ManagedObjectTemplates.xml недействителен или поврежден. Повторите экспорт таблиц из базы данных и загрузите новый файл
Failed to create new PMM security policy.	Не удалось создать политику безопасности «import PM дата время». Повторите импорт шаблона, который не импортировался
Ошибки, при которых весь шаблон не будет импортирован, процесс импорта не прерывается	
Data at the root level is invalid. Line 1, position 1.	Файл шаблона не соответствует формату XML. Повторно экспортируйте шаблон из ViPNet Policy Manager и импортируйте его в ViPNet PMM
Root XML element namespace does not match http://www.infotecs.ru/2007/ViPNet.	Файл шаблона не соответствует актуальной схеме rules.xsd. Исправьте импортируемый шаблон вручную в соответствии со схемой или повторно экспортируйте шаблон из ViPNet Policy Manager и импортируйте его в ViPNet PMM
Policy template does not contain any valid rules to import.	Шаблон политики не может быть импортирован, так как все правила в нем недействительны. Проверьте правила в ViPNet Policy Manager в соответствии с ограничениями ViPNet PMM и повторно импортируйте шаблоны
Ошибки, связанные с группами	
Named object contains reference(s) to a missing named object with ID 73. Invalid reference(s) will be removed.	Именованный объект использует несуществующий объект во включениях или исключениях. Повторно экспортируйте шаблон из ViPNet Policy Manager и импортируйте его в ViPNet PMM
IpObject with id 1436 and name Novserv10.cloud.local cannot be converted to PMM group because it does not have any Inclusion specified and such composition will mean any value.	Не удалось импортировать группу узлов открытой сети без состава, потому что пустой список будет означать любое значение (any). Создайте группу вручную

Ошибка	Описание
InterfaceObject with id 1436 and name Novserv10.cloud.local cannot be converted to PMM group because it does not have any Inclusion specified and such composition will mean any value.	Не удалось импортировать группу сетевых интерфейсов без состава, потому что пустой список будет означать любое значение (any). Создайте группу вручную
VpnObject with id 1436 and name Novserv10.cloud.local cannot be converted to PMM group because it does not have any Inclusion specified and such composition will mean any value.	Не удалось импортировать группу узлов защищенной сети без состава, потому что пустой список будет означать любое значение (any). Создайте группу вручную
ServiceObject with id 1436 and name Novserv10.cloud.local cannot be converted to PMM group because it does not have any Inclusion specified and such composition will mean any value.	Не удалось импортировать группу сетевых протоколов и сервисов без состава, потому что пустой список будет означать любое значение (any). Создайте группу вручную
IpObject with id 34 and name Kuggs-dev cannot be converted to PMM group because it has any value in Exclusion.	Не удалось импортировать группу узлов открытой сети, в исключениях которого присутствует системный объект «All». Удалите системный объект «All» в ViPNet Policy Manager из исключений группы или создайте группу вручную
InterfaceObject with id 34 and name Kuggs-dev cannot be converted to PMM group because it has any value in Exclusion.	Не удалось импортировать группу интерфейсов с ID 34, с системным объектом «All» в исключениях. Удалите системный объект «All» из исключений группы в ViPNet Policy Manager или создайте группу вручную
VpnObject with id 34 and name Kuggs-dev cannot be converted to PMM group because it has any value in Exclusion.	Не удалось импортировать группу узлов защищенной сети с ID 34, с системным объектом «All» в исключениях. Удалите системный объект «All» из исключений группы в ViPNet Policy Manager или создайте группу вручную
ServiceObject with id 34 and name Kuggs-dev cannot be converted to PMM group because it has any value in Exclusion.	Не удалось импортировать группу сетевых протоколов и сервисов с ID 34, с системным объектом «All» в исключениях. Удалите системный объект «All» из исключений группы в ViPNet Policy Manager или создайте группу вручную

Ошибка	Описание
Ip system object AllCoordinators cannot be converted to host condition.	Системный объект «Координаторы», используемый в составе или исключениях группы узлов открытой сети, не поддерживается. Системный объект «Координаторы» можно использовать только в условиях по узлам защищенной сети. Удалите системный объект из состава группы в ViPNet Policy Manager и повторите импорт шаблона
VPN system object OtherHost cannot be converted to host condition.	Системный объект «Другие узлы», используемый в составе или исключениях именованного объекта узлов защищённой сети, не поддерживается. Удалите системный объект из состава группы в ViPNet Policy Manager и повторите импорт шаблона
Service system object BroadCast cannot be converted to service condition.	Системный объект «Широковещательная рассылка», используемый в составе или исключениях группы протоколов, не поддерживается. Удалите системный объект из состава группы в ViPNet Policy Manager и повторите импорт шаблона
Interface system object Multicast cannot be converted to interface condition.	Системный объект «Многоадресная рассылка», используемый в составе или исключениях группы сетевых интерфейсов, не поддерживается. Удалите системный объект из состава группы в ViPNet Policy Manager и повторите импорт шаблона
Schedule system object TunneledIP cannot be converted to schedule condition.	Системный объект «Туннелируемые адреса», используемый в составе или исключениях группы расписаний, не поддерживается. Удалите системный объект из состава группы в ViPNet Policy Manager и повторите импорт шаблона
Failed to create new PMM group.	Не удалось создать группу. Проверьте правильность данных в ViPNet Policy Manager или создайте группу вручную
A set of interface objects contain duplicating ID(s).	В группах сетевых интерфейсов встречаются дубликаты. Шаблон не соответствует актуальной схеме rules.xsd. Повторно экспортируйте шаблон из ViPNet Policy Manager и импортируйте его в ViPNet PMM
A set of ip objects contain duplicating ID(s).	В группах узлов открытой сети встречаются дубликаты. Шаблон не соответствует актуальной схеме rules.xsd. Повторно экспортируйте шаблон из ViPNet Policy Manager и импортируйте его в ViPNet PMM

Ошибка	Описание
A set of service objects contain duplicating ID(s).	В группах протоколов встречаются дубликаты. Шаблон не соответствует актуальной схеме rules.xsd. Повторно экспортируйте шаблон из ViPNet Policy Manager и импортируйте его в ViPNet PMM
A set of VPN objects contain duplicating ID(s).	В группах защищённой сети встречаются дубликаты. Шаблон не соответствует актуальной схеме rules.xsd. Повторно экспортируйте шаблон из ViPNet Policy Manager и импортируйте его в ViPNet PMM
A set of interface objects does not contain description of every nested included or excluded referenced interface object.	В группах сетевых интерфейсов присутствуют связи не всех объектов, которые используются в составе и исключениях. Шаблон не соответствует требованиям ViPNet PMM
A set of ip objects does not contain description of every nested included or excluded referenced ip object.	В группах узлов открытой сети присутствуют связи не всех объектов, которые используются в составе и исключениях. Шаблон не соответствует требованиям ViPNet PMM
A set of service objects does not contain description of every nested included or excluded referenced service object.	В группах протоколов присутствуют связи не всех объектов, которые используются в составе и исключениях. Шаблон не соответствует требованиям ViPNet PMM
A set of VPN objects does not contain description of every nested included or excluded referenced VPN object.	В группах узлов защищённой сети присутствуют связи не всех объектов, которые используются в составе и исключениях. Шаблон не соответствует требованиям ViPNet PMM
Named object does not contain any condition in inclusions.	Группа без состава. Шаблон не соответствует требованиям ViPNet PMM. Создайте группу вручную
Invalid ICMP condition is omitted.	Недействительное условие по протоколу ICMP исключается из импортируемой группы с протоколами. В ViPNet Policy Manager проверьте, что нет условий по неподдерживаемым протоколам ICMP в правилах, или удалите их. ViPNet PMM не поддерживает значения ICMP-сообщений: 1-Unassigned, 2-Unassigned, 7-Unassigned, 19-Reserved (for Security). Правила с такими значениями не импортируются
Detected apply condition by unavailable VPN node with identifier 578D000A. The condition is excluded.	Группа использует в составе узел, не существующий в модуле VPN. Проведите миграцию из ViPNet Administrator в ViPNet Prime. Необходимо, чтобы узел мигрировал в модуль VPN

Ошибка	Описание
Schedule named object with specified exclusion has been omitted.	Группа расписаний, содержащая исключения, пропущена. Расписание может быть задано только для ежедневного или еженедельного выполнения, или ограничено временным диапазоном. Иначе расписание не задается для правил, использующих эту группу, и правила выполняются всегда. Приведите расписания в ViPNet Policy Manager к виду ViPNet PMM
Private network identifier condition has been substituted by set of private node conditions.	Правило, использующее в условиях идентификатор защищенной сети, заменено на правило с группой узлов защищенной сети. В ViPNet PMM нет условия по номеру защищенной ViPNet-сети, которое есть в ViPNet Policy Manager. Все устройства одной подсети импортируются в одну пользовательскую группу

Ошибки, связанные с правилами

An error found while checking Rule with ID 200002. Rule contains reference(s) to missing named object with ID 998.	Правило ссылается на несуществующую группу. Создайте правило вручную
ICMP condition of type 1 cannot be converted to service condition.	В правиле используется недействительное условие по протоколу ICMP. Проверьте в ViPNet Policy Manager, что в правилах нет условий по неподдерживаемым протоколам ICMP, или удалите их. ViPNet PMM не поддерживает значения ICMP-сообщений: 1-Unassigned, 2-Unassigned, 7-Unassigned, 19-Reserved (for Security). Правила с такими значениями не импортируются
Detected apply condition by unavailable VPN node with identifier 578D000A.	В правиле используется условие по несуществующему узлу в модуле VPN. Проведите миграцию из ViPNet Administrator в ViPNet Prime. Необходимо, чтобы узел мигрировал в модуль VPN
Ip system object AllCoordinators cannot be converted to host condition.	В правиле используется условие с неподдерживаемым системным объектом. Удалите системный объект из состава группы в ViPNet Policy Manager и повторите импорт шаблона
Interface system object Multicast cannot be converted to interface condition.	
Service system object AllClients cannot be converted to service condition.	
VPN system object OtherHost cannot be converted to host condition.	

Ошибка	Описание
Rule uses DPI conditions.	В правиле используется условие DPI. Такие правила не импортируются. Удалите правило в ViPNet Policy Manager и создайте его вручную в ViPNet PMM или отредактируйте правило в ViPNet Policy Manager правило и загрузите повторно
Rule uses users conditions.	В правиле используется условие по пользователям. Такие правила не импортируются. Удалите правило в ViPNet Policy Manager и создайте вручную в ViPNet PMM или отредактируйте в ViPNet Policy Manager правило и загрузите повторно
Rule that does not meet specific PMM requirements for VpnHost conditions was omitted with following reason: If destination contains VPN nodes, then source must be LocalHost.	Если назначение трафика — устройства защищённой сети, его источником может быть только группа «Целевое устройство». Отредактируйте правило в ViPNet Policy Manager, экспортируйте шаблоны и импортируйте их в ViPNet PMM повторно
Rule that does not meet specific PMM requirements for VpnHost conditions was omitted with following reason: If source contains VPN nodes, then destination must be either LocalHost or BroadCast.	Если источник трафика — устройства защищённой сети, его назначением может быть только группа «Целевое устройство» или «Широковещательная рассылка». Отредактируйте правило в ViPNet Policy Manager, экспортируйте шаблоны и импортируйте их в ViPNet PMM повторно
Rule that does not meet specific PMM requirements for VpnHost conditions was omitted with following reason: System object LocalHost cannot be used both for source and destination.	Группа «Целевое устройство» не может быть одновременно источником и назначением трафика. Отредактируйте правило в ViPNet Policy Manager, экспортируйте шаблоны и импортируйте их в ViPNet PMM повторно
Rule that does not meet specific PMM requirements for VpnHost conditions was omitted with following reason: At least LocalHost or BroadCast must be specified as source or destination of a VPN rule.	В источниках или назначениях трафика должна быть указана группа «Целевое устройство» или «Широковещательная рассылка». Невозможно указать значение апу и в источниках, и в назначениях
Network interfaces have been used both in source and destination. Destination network interface is omitted.	Сетевой интерфейс задан одновременно в источниках и назначениях. Отредактируйте правило в ViPNet Policy Manager и загрузите повторно
Network interface has been used with LocalHost system object. Interfaces are omitted.	Сетевой интерфейс был использован вместе с системным объектом «Целевое устройство». Отредактируйте правило в ViPNet Policy Manager и загрузите повторно

Ошибка	Описание
Hybrid schedule has been omitted.	Условие по гибриднему расписанию было исключено. Настройте расписание для правила в ViPNet PMM
Failed to create new PMM layer of security policy.	Не удалось создать слой в политике безопасности. Повторите импорт шаблонов
Failed to create new PMM rule in layer of security policy. Target node or broadcast group is required.	Не удалось создать правило в слое в политике безопасности. Укажите в ViPNet Policy Manager целевое устройство или группу «Широковещательная рассылка». Или создайте правило вручную



Возможные неполадки

Неизвестная ошибка

При возникновении неизвестной ошибки на компьютере с ViPNet Prime перейдите в папку с модулем ViPNet Prime PMM и пересоздайте Docker-контейнеры модуля ViPNet Prime PMM:

```
$ sudo ./down.sh
```

```
$ sudo ./up.sh
```

Если неизвестная ошибка отобразилась при разделении политики безопасности и повторилась снова, то вместо разделения политики используйте другие действия, которые приведут вас к тому же результату, например:

- удалите целевое устройство из исходной политики безопасности;
- создайте новую политику безопасности;
- назначьте целевое устройство в новую политику безопасности;
- скопируйте правила;
- распределите слой в другую политику.

Не отображаются счетчики срабатывания правил

Это происходит, когда между созданием узла для ViPNet Coordinator HW версии 5.3.0 и выше и созданием дистрибутива ключей прошло менее 3 минут. Тогда справочник `nvs.info` еще не добавляется в дистрибутив ключей.

Чтобы устранить проблему, установите файл `nvs.info` на шлюз безопасности. Это позволит ему подключиться к ViPNet Prime NVS и передать информацию о срабатывании в модуль ViPNet Prime PMM. См. «ViPNet Prime Network Visibility System. Руководство администратора», раздел «Установка справочника на устройство, опрашиваемое по SNMP».

Для устранения проблемы не устанавливайте новый дистрибутив ключей, так как это приведет к потере локальных настроек и правил фильтрации и трансляции на шлюзе безопасности. Кроме этого, если создать и не устанавливать новый дистрибутив ключей, то на шлюзе безопасности поколения ViPNet 5 вы не сможете использовать старые резервные копии файла индивидуальной конфигурации `*.ecf` и единую аутентификацию Single Sign-On с помощью ViPNet Prime. Это связано с тем, что при создании нового дистрибутива ключей изменяются секреты для аутентификации. Дождитесь автоматического обновления справочников и ключей на шлюзе безопасности.

Если ViPNet Prime Policy Management не получает счетчики срабатывания правил от координатора:

- 1 На координаторе включите службу DNS:

```
inet dns mode on
inet dns start
```

- 2 Если ViPNet Prime NVS установлен на отдельном компьютере, разрешите трафик от координатора до сервера ViPNet Prime NVS по порту 4222 (порт протокола NATS по умолчанию), например:

```
firewall vpn add src @local dst 0x52ee0002 tcp dport 4222 pass
```

где `0x52ee0002` — ViPNet-идентификатор узла, на котором установлен сервер ViPNet Prime NVS.

Если ViPNet Prime NVS установлен на одном компьютере с ViPNet Prime, то это правило не требуется, так как для клиента Control Center по умолчанию разрешен весь трафик.

Убедитесь, что правило добавлено:

```
firewall vpn show
```

См. «ViPNet Prime Network Visibility System. Руководство администратора», раздел «Установка справочника на устройство, опрашиваемое по SNMP».

Длительная инспекция правил

При большом количестве правил от 4500 до 7000 (максимальное количество правил для одного устройства — 7000), назначенных одному устройству, а также большом объеме каждого правила (максимальное количество элементов в правиле 1000 для источников, назначений, сервисов и расписаний) и общем количестве правил для организации 20000 и выше, инспекция политик не завершается длительное время.

При этом в журналах модуля ViPNet Prime PMM присутствует ошибка:

```
$ sudo journalctl CONTAINER_NAME=pmm-worker | grep System.OutOfMemoryException
```

Для устранения проблемы увеличьте оперативную память до 4 Гб для службы `worker-service`:

1 Остановите модуль ViPNet Prime PMM:

```
$ sudo /usr/share/infotecs/prime/deployment/pmm/down.sh
```

2 Откройте для редактирования файл `pmm.compose.yaml`.

3 В секции `pmm-worker` увеличьте значение параметра `mem_limit` до 4 Гб и сохраните файл:

```
mem_limit: 4096m
```

4 Запустите модуль ViPNet Prime PMM:

```
$ sudo /usr/share/infotecs/prime/deployment/pmm/up.sh
```

Недоступен вход в ViPNet Prime PMM

После перезагрузки компьютера или завершения работы ViPNet Client 5 for Linux недоступен вход в раздел  **Policy Management** в веб-интерфейсе ViPNet Prime Policy Management. Отображается бесконечная загрузка. В модуле VPN не отправляются справочники.

1 Откройте журнал контейнера `pmm-core`:

```
$ sudo journalctl CONTAINER_NAME=pmm-core
```

2 В журналах контейнера `pmm-core`:

```
2022-07-05 10:38:22.311 [INF] Module configuration sent
2022-07-05 10:38:22.311 [INF] Module in SMP initialized
2022-07-05 10:38:22.764 [INF] Notifications dispatcher was started
2022-07-05 10:38:22.769 [INF] "PolicyRulesCleanerBackgroundService" started
2022-07-05 10:38:22.773 [INF] "ResultantPoliciesSenderBackgroundService" started
2022-07-05 10:38:22.778 [INF] initialization done
2022-07-05 10:38:22.781 [INF] "VpnSynchronizationBackgroundService" started
2022-07-05 10:41:05.043 [ERR] Error returned from introspection endpoint: Resource temporarily unavailable (prime.cactus.mngmob:443)
2022-07-05 10:41:05.051 [ERR] Error returned from introspection endpoint: Resource temporarily unavailable (prime.cactus.mngmob:443)
2022-07-05 10:41:05.056 [INF] "Bearer" was not authenticated. Failure message: "Error returned from introspection endpoint: Resource temporarily unavailable (prime.cactus.mngmob:443)"
2022-07-05 10:41:05.057 [INF] "Bearer" was not authenticated. Failure message: "Error returned from introspection endpoint: Resource temporarily unavailable (prime.cactus.mngmob:443)"
2022-07-05 10:41:11.741 [ERR] Error returned from introspection endpoint: Resource temporarily unavailable (prime.cactus.mngmob:443)
2022-07-05 10:41:11.741 [INF] "Bearer" was not authenticated. Failure message: "Error returned from introspection endpoint: Resource temporarily unavailable (prime.cactus.mngmob:443)"
2022-07-05 10:41:11.762 [INF] AuthenticationScheme: "Bearer" was challenged.
```

Рисунок 30. Ошибка входа в ViPNet Prime PMM

Возможные причины

Дистрибутив ключей был установлен под одним пользователем ОС, а вход в ОС был выполнен под другим пользователем.

Устранение проблемы

1 Войдите в ОС как пользователь, для которого был установлен дистрибутив ключей устройства Control Center. Чтобы проверить, установлен ли дистрибутив ключей для данного пользователя:

```
$ vipnetclient info
```

2 Убедитесь, что в ViPNet Client 5 for Linux включено VPN-соединение:

```
$ vipnetclient start
```

См. документацию на ViPNet Client 5 for Linux.

3 Повторите попытку входа в модуль.

Если это не помогло, переустановите дистрибутив ключей от имени суперпользователя `root`. В результате ViPNet Client 5 for Linux будет запускаться сразу после перезапуска ОС.

Ошибка импорта шаблона политик из ViPNet Policy Manager

Импорт шаблона политик из ViPNet Policy Manager выполняется более 3 часов и имеет статус **В процессе**.

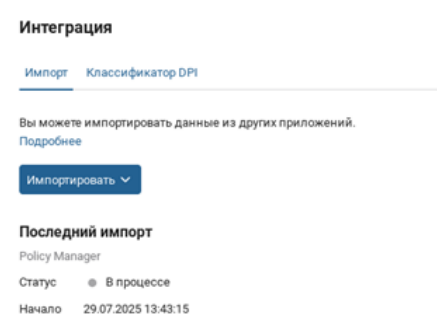


Рисунок 31. Статус импорта политик

Возможные проблемы

Импорт завершился с ошибкой. Журнал событий содержит соответствующую запись.

▼	29.07.2025 13:43:15	Запрос на импорт
	29.07.2025 13:43:15.507	Запрос на импорт
	29.07.2025 13:43:20.549	Окончание импорта

Рисунок 32. Ошибка импорта политики в ViPNet Prime Policy Management

Устранение проблемы

Перезапустите ViPNet Prime Policy Management.

После миграции не принимаются политики на координаторе поколения ViPNet 4

На координаторе поколения ViPNet 4 не принимается политика безопасности, в журнале транспортных конвертов MFTP статус **Поврежден**, задача указывается некорректно.

16:37:10, 15 Окт 2025	00000000	00000000	Почта	mu~3vii~.ctl	0.77	Поврежден	MFTP
16:37:10, 15 Окт 2025	00000000	00000000	Почта	m0)3vii~.ctl	0.78	Поврежден	MFTP

Рисунок 33. Статус конверта с политиков в журнале транспортных конвертов

Возможные причины

При установке ViPNet Prime Policy Management указан неверные ViPNetID узла центра управления.

Устранение проблемы

Повторно установите модуль ViPNet Prime PMM и укажите верный ViPNetID узла центра управления.



История версий

Что нового в версии 1.10

- **Управление списком блокировки IP-адресов**

Теперь вы можете создать список с нежелательными IP-адресами, трафик которых должен всегда блокироваться на целевом устройстве. Список блокировки необходимо добавить в политику безопасности. Вы можете запретить отправку списка на отдельные устройства. Подробнее см. в разделах [Списки блокировки IP-адресов](#), [Дополнения политики безопасности](#) и [Отправка дополнений на целевые устройства](#).

- **Параметры фильтрации по странам**

- **Выбор стран в параметрах фильтрации правила**

Правила фильтрации по странам отправляются на устройства в составе политики безопасности. Вы можете запретить отправку таких правил на отдельные устройства. Подробнее см. в разделах [Правила фильтрации трафика](#) и [Отправка дополнений на целевые устройства](#).

- **Изменение списка IP-адресов, относящегося к стране**

Теперь вы можете добавлять или исключать IP-адреса из списка IP-адресов, относящихся к странам, индивидуально для каждой политики безопасности. Подробнее см. в разделах [Списка дополнений и исключений для стран](#), [Дополнения политики безопасности](#) и [Отправка дополнений на целевые устройства](#).

- **Изменение в интерфейсе**

- Теперь адрес подсети в группе адресов открытой сети будет отображаться в виде диапазона IP-адресов. Например, 192.168.1.0/24 после обновления на версию 1.10 станет отображаться в виде 192.168.1.0-192.168.1.255.
- Теперь каждая группа объектов расположена в отдельном разделе на панели слева.

Что нового в версии 1.9.1

- Отображается номер доверенной сети устройств при просмотре или изменении списка устройств защищенной сети в группах и правилах



Устройство	Номер сети	Организация
Coordinator 2 (4gen)	24479	Test
Coordinator 1 (4gen)	24479	Test

Рисунок 34. Отображение номера доверенной сети

- После смены поколения координатора результирующая политика будет отмечена измененной, вы сможете отправить её на устройство. Результирующая политика, которая была применена на устройстве до смены поколения, продолжит работать

Подробнее см. [Отправка политик на устройства](#).

Что нового в версии 1.9

- Поддержка ViPNet Client 5 для ОС Аврора версии 5.1.0 и выше

Теперь вы можете централизованно управлять правилами фильтрации на клиентах ViPNet Client 5 для ОС Аврора версии 5.1.0 и выше.

- Улучшение внутренней функциональности

Что нового в версии 1.8

- Импорт шаблонов политик безопасности из ViPNet Policy Manager

Вы можете перенести шаблоны политик безопасности из ViPNet Policy Manager после миграции сети из ViPNet Administrator в ViPNet Prime. Подробнее см. [Импорт шаблонов политик безопасности из ViPNet Policy Manager](#).

- Настройка обработки прикладных протоколов

Вы можете задать порты, по которым работают прикладные протоколы, и использовать эти настройки в политиках безопасности. Подробнее см. [Настройка обработки прикладных протоколов](#).

- IP-адреса и доменные имена в правилах фильтрации туннелируемых ресурсов

Раньше в правилах фильтрации трафика туннелируемых ресурсов вы могли использовать в качестве источника и назначения только ресурсы координатора своей или доверенной организации из модуля VPN. Теперь в источниках и назначениях правил фильтрации трафика туннелируемых ресурсов вы можете:

- задать IP-адреса, диапазоны IP-адресов, подсети и доменные имена туннелей координатора;

- добавить пользовательские группы адресов открытой сети.

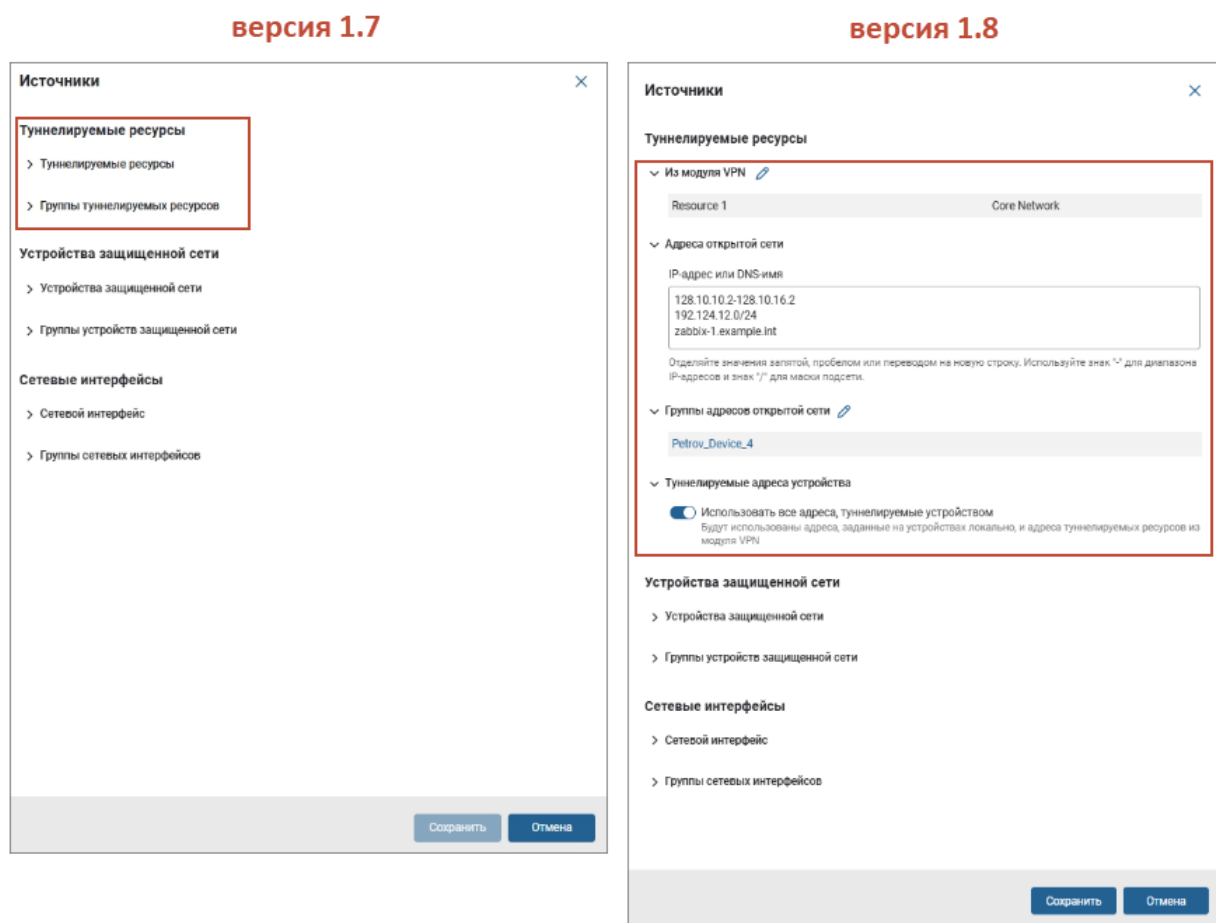


Рисунок 35. Изменения при создании правил фильтрации трафика туннелируемых ресурсов

Подробнее см. [Правила фильтрации трафика](#).

- **Доработана утилита Confwiz Enricher**

Теперь при адаптации данных Check Point с помощью утилиты Confwiz Enricher вы можете преобразовать параметры правила, заданные в виде исключений, для загрузки в ViPNet Prime PMM. Подробнее см. [Импорт политик и правил из Check Point](#).

- **Доработана отправка политик на устройства с ViPNet Client for Windows версии 4.5.5**

Теперь при получении нескольких политик они применяются на устройстве в правильном порядке.

- **Внутренние изменения**

Переименовали сервисы:

- `pmm_pmm-core_1` в `pmm-core`
- `pmm_pmm-worker_1` в `pmm-worker`
- `mongo` в `pmm-mongo`

Переименовали файл `docker-compose.pm.yml` в `pmm.compose.yaml`

- **Поддержка ViPNet Client for Windows версии 4.5.5**

Теперь с помощью ViPNet Prime и модуля ViPNet Prime PMM вы можете централизованно управлять правилами фильтрации на клиентах ViPNet Client for Windows версии 4.5.5.

Что нового в версии 1.7

- **Отображение идентификатора правила (RuleID)**

Чтобы однозначно идентифицировать правила на устройствах и в управляющем приложении, теперь для каждого правила фильтрации и трансляции адресов отображается идентификатор — уникальный номер правила. Он имеет значения от 200 001 до 4 000 000 и уникален внутри одной организации.

☐ №	Действие	Название правила	ID	Источники
☐ 1-1	Блокировать	Правило фильтрации транзитного трафика открытой сети 1	200007	Любые
☐ 1-2	Блокировать	Правило фильтрации транзитного трафика открытой сети 2	200010	Любые

Рисунок 36. Идентификатор правила

По идентификатору правила вы можете легко его найти.

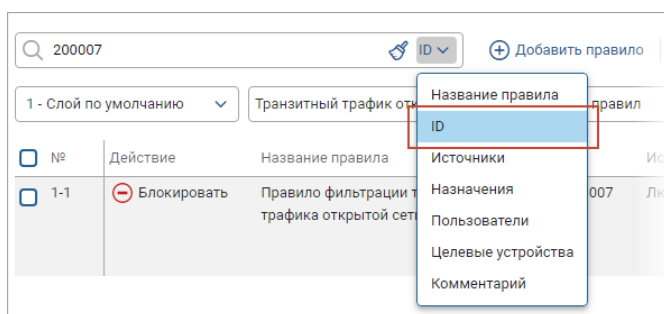


Рисунок 37. Поиск правила по идентификатору

Идентификатор и другие атрибуты правила записываются в [журнал событий ViPNet Prime](#) при действиях с правилом.

- **Повышение информативности отчета инспекции политик**

- Раньше отчет содержал номер правила в слое по порядку, например 1–15 (правило 15 в слое 1), а теперь — идентификатор правила в организации, по которому вы можете найти правило на шлюзе безопасности и в ViPNet Prime.
- Теперь отчет содержит конфликтующий параметр из правила: его название и значение в правиле 1 и правиле 2. См. [Работа с отчетом инспекции политики](#).
- Раньше отчет выгружался в формате CSV, теперь для читаемости — только в XLSX.

№	Тип конфликта	Тип правила	Название правила 1	ID 1	Название правила 2	ID 2	Совпадающий параметр	Значение правила 1	Значение правила 2
1	Вхождение	Transit	Новое правило	200003	Сору Новое правило	200004	Источники	1.1.1.1, 1.1.1.3 2.1.1.3 168.132.1.75 32.13.32.13	1.1.1.0-1.1.1.5 (Группа 1) 2.1.1.0-2.1.1.5 (Группа 2) 168.132.1.1-168.132.1.255 (Офис Уфа) 32.13.32.13
							Назначения	1.1.1.1, 1.1.1.3 2.1.1.3 168.132.1.75	1.1.1.0-1.1.1.5 (Группа 1) 2.1.1.0-2.1.1.5 (Группа 2) 2.1.1.0 - 168.132.1.168 (Офис Уфа)
							Сервисы и приложения	TCP: 3 -> 4 IP: 14	TCP: 0..65535 -> 4 IP: 14

Рисунок 38. Пример записи в отчете инспекции

- **Изменения в документации**

- Добавлен раздел [Настройка исключений при блокировке пользовательского VPN-трафика](#).

Пользовательский VPN-трафик может блокироваться, если:

- конечное защищаемое устройство (клиент) с ViPNet EndPoint Protection не соответствует политикам Zero Trust Network Access (ZTNA).
- на конечном защищаемом устройстве (клиенте) не установлен или неработоспособен ViPNet EndPoint Protection.

Чтобы пользователь имел доступ в защищенную сеть при блокировке VPN-трафика, создайте правило фильтрации с типом «Локальный трафик защищенной сети» и названием «Исключения из пользовательского защищенного трафика».

- Добавлен раздел [Настройка отправки результирующих политик](#). Теперь вы можете управлять поведением инспекции политик при отправке изменений на устройства.

- **Внутренние изменения**

- Переименовали сервис pmm_pmm_nginx_1 в pmm_pmm-edge-server_1.
- Улучшили интерфейс. Теперь вы можете найти правила только по состоянию **Новое** или **Отключено**. См. [Просмотр состояний правил](#).

Что нового в версии 1.6

- **Переключение режимов ViPNet Coordinator IG**

Позволяет из управляющего ПО переключить режим работы на координаторе: «Штатный», «Регламентный», «Специальный» в соответствии с требованиями ФСТЭК к межсетевым экранам типа «Д».

- **Лицензирование модуля и количества управляемых устройств**

Чтобы использовать ViPNet Prime Policy Management, теперь требуется лицензия на него и на количество устройств в защищенной сети, для которых разрешено использовать функции ViPNet Prime Policy Management.

- **Изменения в интерфейсе**

При загрузке политик безопасности из Check Point в ViPNet Prime Policy Management возможность выбрать сохранение правил типа Automatic NAT в отдельную политику перенесена в первый шаг мастера загрузки.

- **Работа ViPNet Prime Policy Management в режиме замкнутой программной среды на Astra Linux SE**

Что нового в версии 1.5.2

Просмотр изменений загруженных и исходных объектов при загрузке правил из Check Point

Вы можете скачать файл с изменениями, чтобы проверить корректность загрузки групп объектов Check Point в ViPNet Prime PMM.

Что нового в версии 1.5.1

- **Улучшена загрузка правил из Check Point:**

- **Выбор политик безопасности**

Теперь вы можете выбрать, какие политики загружать из Check Point. Для этого загрузите файл `policies_collections.xml` [вместе с остальными файлами из Check Point](#).

- **Выбор параметров загрузки**

При загрузке одноименных групп объектов Check Point вы можете выбрать, использовать существующие группы или создать новые группы объектов.

- **Загрузка правил Automatic NAT в отдельную политику безопасности**

- **Ограничение на период расписаний правил**

Введено ограничение на период в расписаниях правил — нельзя указать расписание ранее 1970 года.

Что нового в версии 1.5.0

- **Использование узлов из доверенных сетей и организаций**

Шлюзы безопасности и клиенты, к которым в модуле VPN был предоставлен доступ для связей в доверенных организациях и сетях, вы можете использовать в составе:

- правил фильтрации локального трафика защищенной сети;
 - правил фильтрации трафика туннелируемых ресурсов;
 - групп объектов устройств защищенной сети.

Вы можете использовать узлы из доверенных сетей под управлением ViPNet Prime или ViPNet Administrator. Но использование туннелей координатора из доверенной сети под управлением ViPNet Administrator и ресурсов из ViPNet Prime недоступно. Также недоступно использование узлов, которые предоставлены в совместный доступ только для использования сервисных функций в доверенных организациях.

О том, как разрешить создавать связи с узлом из доверенной организации, см. «ViPNet Prime. Руководство администратора», «Связи с объектами доверенных организаций».

- **Проверка целостности ПО**

Если нарушена целостность сервиса модуля Policy Management, сервис блокируется. Запись об этом отображается в журнале аудита.

См. «ViPNet Prime. Руководство по установке», разделы «Нарушение целостности и работы ПО» и «Просмотр журналов аудита».

- **Улучшение внутренней функциональности**

Поддержана новая версия протокола для управления политиками безопасности на узлах поколения ViPNet 5.

Что нового в версии 1.4

- **Счетчики срабатывания правил**

Для каждого правила фильтрации и трансляции на шлюзах безопасности поколения 5, таких как ViPNet Coordinator HW 5, вы можете [просмотреть количество срабатываний правил](#). Это поможет оптимизировать правила, чтобы обрабатывать их быстрее, или выявить аномалии в сети.

- **Инспекция правил в политиках безопасности**

Вы можете проверить правила фильтрации транзитного и локального трафика открытой сети на согласованность, чтобы автоматически [найти конфликтующие правила и их дубликаты в политике безопасности](#). Например, вы можете автоматически найти перекрывается ли разрешающее правило другим разрешающим или блокирующим правилом более высокого приоритета.

- **Отправка изменений только для выбранной политики**

Теперь вы можете выбрать политику и отправить изменения на устройства только этой политики.

- **Удобство использования**

- Нумерация слоев в выпадающих списках
- Удаление единственной записи порта TCP / UDP
- Просмотр имен политик безопасности в окне просмотра результирующей политики
- Фильтрация по нескольким слоям

Что нового в версии 1.3.1

- **Разделение политик безопасности**

Теперь вы можете автоматически переиспользовать ранее созданные правила для устройств из одной политики безопасности в другой политике или применить их на новые устройства. Для этого [разделите политику безопасности на две](#). При этом целевые устройства с их правилами автоматически переместятся в новую политику. Воспользуйтесь этим и разделите

политики на несколько в зависимости от устройства, если после обновления с версии ViPNet Prime PMM 1.2 в одной политике безопасности получилось большое количество правил.

- **Улучшение интерфейса**

- **Постраничная навигация**

Теперь при большом количестве групп объектов они отображаются постранично, и вы можете настраивать количество записей на странице от 50 до 250 с шагом 50. По умолчанию отображается 100 записей.

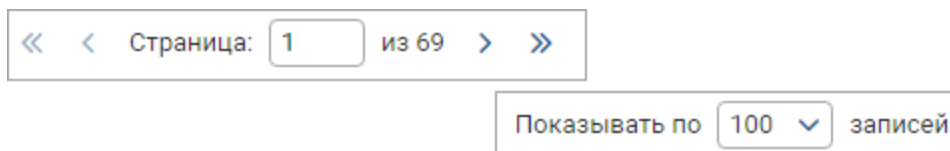


Рисунок 39. Постраничное отображение объектов

- **Просмотр состава групп объектов в правилах**

Раньше вы переходили в раздел **Группы объектов**, чтобы просмотреть состав группы. Теперь вы можете просмотреть состав групп в правилах сразу из политики.

Что нового в версии 1.3

- **Политики безопасности**

Теперь вместо работы с каждым правилом фильтрации и трансляции в отдельности вы работаете с наборами правил — политиками безопасности и назначаете их на устройства. Это позволит быстрее управлять новыми устройствами при большом количестве правил на них.

- **Многоуровневые политики безопасности**

- **Слои**

Группируйте правила в слои, например, в зависимости от организационной структуры предприятия и управляйте их приоритетом.

- **Общие слои**

Используйте одинаковые группы правил в разных политиках безопасности. См. [Работа со слоями](#).

- **Статусы политик безопасности**

Просматривайте актуальную информацию о политиках безопасности: **Не назначена**, **Изменена**, **Отправляется**, **Актуальна**.

- **Статусы результирующих политик безопасности**

Просматривайте статусы результирующих политик безопасности для каждого управляемого устройства: **Актуальна**, **Отправляется**, **Изменена**.

- **Состояния правил**

См. [Просмотр состояний правил](#).

- **Пользователи из внешних источников в правилах фильтрации трафика**

Раньше, чтобы в правилах транзитного трафика открытой сети и трафика туннелируемых ресурсов указать LDAP-имена пользователей Active Directory и Captive Portal, вы создавали таких пользователей в ViPNet Prime. Теперь этого не требуется, и вы можете в правилах указать пользователей без создания их в ViPNet Prime. Вы добавляете их вручную в [условия правил](#).

- **Версионирование результирующей политики безопасности**

Теперь изменения результирующей политики для целевого устройства версионированы. Идентификатор результирующей политики устройства используется в составных идентификаторах таблицы правил, отдельного правила. Это может быть полезно при анализе трафика, чтобы идентифицировать, каким было правило до изменения. Версия результирующей политики отображается в разделе **Главная консоль**  > **Журнал событий** для событий **Отправка политики**. Идентификация таблицы правил и отдельного правила на момент обработки IP-пакета межсетевым экраном целевого устройства поддерживается ViPNet Coordinator HW версии 5.2 и выше.

- **Улучшение взаимодействия с интерфейсом**

- **При удалении групп объектов**

Теперь перед удалением групп объектов отображается предупреждение, и вы можете ознакомиться с группами объектов и правилами, на которые повлияет это удаление. Запрещено удаление групп объектов, которые используются в правилах.

- **При загрузке классификатора DPI**

Раньше вы загружали два файла для классификатора DPI — XML и XSD. Теперь вам требуется загружать только XML-файл для классификатора DPI.

- **Просмотр информации об импорте правил из CheckPoint**

Раньше в ViPNet Prime Policy Management вы не могли посмотреть статус загрузки. Если при ошибке импорта вы пропустили сообщение со ссылкой на скачивание журнала загрузки `import-log.txt`, вы не могли скачать его снова. Теперь, чтобы просмотреть правила, которые не импортировались, вы можете всегда скачать журнал последнего импорта. Также вы можете просмотреть статус, дату и время начала и завершения импорта. Сообщение о завершении импорта правил с ошибками теперь отображается при переходе в другие разделы интерфейса.

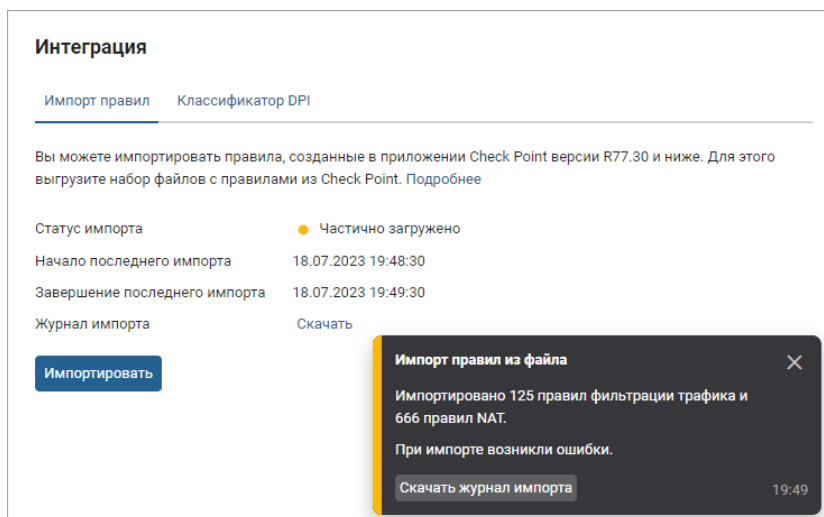


Рисунок 40. Просмотр информации об импорте правил CheckPoint

- **Скачивание ранее загруженного файла классификатора DPI**

Раньше, если вы пропустили всплывающее уведомление при загрузке классификатора DPI, вы не могли его скачать. Теперь вы можете скачать классификатор DPI в любой момент, чтобы загрузить его в другую организацию.

Что нового в версии 1.2

- **Фильтрация трафика по пользователям, приложениям и прикладным протоколам**

Теперь вы можете фильтровать трафик:

- по приложениям и прикладным протоколам [DPI](#);
- по учетным записям пользователей из службы каталогов AD или LDAP-сервера.

Фильтрация применяется к транзитному трафику открытой сети и трафику туннелируемых ресурсов.

- **Правила трансляции сетевых адресов (NAT)**

Теперь вы можете управлять правилами NAT на шлюзах безопасности.

- **Импорт правил NAT из Check Point**

Теперь вы можете импортировать правила NAT из [оборудования Check Point](#).

Что нового в версии 1.1.1

- **Поддержка ViPNet Coordinator HW версии 4.5.1**

Теперь с помощью ViPNet Prime и модуля ViPNet Prime PMM вы можете централизованно управлять правилами фильтрации на координаторах ViPNet Coordinator HW версии 4.5.1.

- **Поддержка ViPNet Coordinator HW версии 5**

Теперь вы можете управлять правилами фильтрации на координаторах ViPNet Coordinator HW версии 5.x.



Термины и сокращения

DPI (Deep Packet Inspection)

Технология расширенной инспекции содержимого сетевого трафика на уровнях 2 — 7 модели OSI и накопления статистики. На основании анализа полученных данных идентифицируются приложения и прикладные протоколы.

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.

Zero Trust Network Access (ZTNA)

Технология сетевого доступа с нулевым доверием, основанная на принципах модели безопасности "Zero Trust", при которой каждый пользователь, устройство и сетевой ресурс перед получением доступа к ресурсам внутренней сети подвергаются проверке на основе детализированных правил контроля доступа. ZTNA позволяет повысить безопасность и защиту сетевых ресурсов.

Доверенная организация

Организация, с которой установлено взаимодействие для обмена информацией по защищенным каналам VPN.

Защищённое устройство

Узел [защищённой сети](#), на котором установлено программное обеспечение ViPNet с функцией шифрования трафика.

Клиент (ViPNet-клиент)

Защищённое устройство ViPNet, которое является начальной или конечной точкой передачи данных. В отличие от координатора клиент не выполняет функции маршрутизации трафика и служебной информации.

Координатор (ViPNet-координатор)

Защищённое устройство ViPNet, которое в сети ViPNet VPN выполняет серверные функции, маршрутизацию трафика и служебной информации.

Организация (ViPNet-организация)

Объект управления, подчинённые объекты которого логически изолированы от объектов других организаций. Представляет собой часть сети ViPNet, к управлению которой может быть предоставлен отдельный доступ в веб-интерфейсе ViPNet Prime.

Открытое устройство

Устройство без ПО ViPNet с функцией шифрования трафика на сетевом уровне, расположенное в сети «за координатором».

Открытый трафик

Поток незашифрованных IP-пакетов.

Поколение ViPNet 4

Поколение продуктов ViPNet с централизованным управлением из ViPNet Administrator или ViPNet Prime и передачей транспортных конвертов по MFTR. Использует дистрибутивы ключей *.dst.

Поколение ViPNet 5

Поколение продуктов ViPNet с централизованным управлением из ViPNet Prime и передачей транспортных сообщений по HTTP/HTTPS. Использует дистрибутивы ключей *.ds5.

Политика безопасности

Набор правил фильтрации трафика и правил трансляции IP-адресов, настроек устройств, которые регулируют безопасность устройств [защищенной сети](#).

Поставщик услуг

Компания, которая владеет серверной частью системы управления ViPNet Prime и лицензиями на продукты ViPNet и предоставляет доступ к ViPNet Prime по ссылке другим компаниям.

Результирующая политика безопасности

Политика безопасности для отдельного защищенного устройства, полученная в результате объединения (с учетом приоритета) правил фильтрации трафика и правил NAT, настроек, назначенных устройству.

Ресурс

Отдельное сетевое устройство или целая подсеть, трафик с которыми шифруется не самими устройствами, а координатором, установленным в той же маршрутизируемой сети, с помощью [туннелирования](#) трафика при передаче данных через интернет или другие открытые сети.

Сеть ViPNet

Защищённая сеть, организованная с помощью программного обеспечения ViPNet и представляющая собой совокупность сетевых узлов. Узлы обмениваются информацией с помощью наложенной маршрутизации. Каждая сеть имеет свой уникальный номер.

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. Устройства могут не быть узлами сети ViPNet. Такие устройства называются [ресурсами](#).

Целевое устройство

Устройства защищенной сети, которые выполняют функции межсетевого экранирования.

Центр управления

Обязательное устройство сети ViPNet, связанное с устройствами всех организаций. Обеспечивает отправку обновлений об изменении свойств объектов, связей между объектами, лицензионных ограничений, ключей на защищённые устройства ViPNet. Это устройство функционирует как ViPNet-клиент. Имя по умолчанию — Control Center.

Шлюзы безопасности

Координаторы и устройства ViPNet xFirewall.