

РУКОВОДСТВО АДМИНИСТРАТОРА

НЕТХАБ

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

СОДЕРЖАНИЕ

Содержание.....	2
1 Общие сведения об ИС	4
1.1 Полное наименование системы и ее условное обозначение	4
1.2 Назначение системы	4
1.3 Функциональный состав Системы	4
1.4 Сценарии взаимодействия пользователя с Системой	4
1.5 определения, обозначения, сокращения	4
2 Требования	5
3 Доступ в Веб-интерфейс Нетхаб.....	6
4 Управление лицензиями	8
4.1 Просмотр информации о текущей лицензии.....	8
4.2 Установка лицензии.....	9
5 Управление устройствами	12
5.1 Добавление устройств	12
5.2 Добавление устройства из файла.....	14
5.3 Изменение устройств.....	15
5.4 Удаление устройств	16
6 Анализ.....	17
6.1 Создание и просмотр отчета об анализе	17
7 Настройка параметров системы	18
7.1 Панель администрирования	18
7.2 увеличение дискового пространства.....	18
7.3 Расширение дискового пространства путем монтирования нового диска.....	19
7.4 Расширение дискового пространства путем расширения существующего диска ...	19
7.5 Ручное определение URT	20
7.6 Использование статического метода.....	20
7.7 Использование гибридного метода	21
7.8 Описание других опций.....	22
7.8.1 ПОЛЬЗОВАТЕЛИ/РОЛИ.....	22
7.8.2 ПЛАНИРОВЩИК.....	22
7.8.3 СООТВЕТСТВИЕ.....	23
7.8.4 МОНИТОРИНГ.....	23
8 Добавление устройств.....	25
8.1 Добавление устройств Cisco ASA	25
8.1.1 Стандартный метод	25
8.1.2 Альтернативный метод (ручной)	26
8.1.3 Настройка прав для подключения.....	27
8.2 Cisco Firepower	29
8.2.1 Предварительная настройка	29
8.2.2 Добавление Cisco Firepower.....	30
8.3 Cisco Nexus	32
8.3.1 Права для подключения	32
8.3.2 Добавление Cisco Nexus.....	33
8.4 Добавление устройств Cisco IOS.....	33
8.4.1 Права для подключения	33
8.4.2 Добавление Cisco IOS.....	34
8.5 Добавление устройств Paloalto	34
8.5.1 Настройка прав для подключения.....	35

8.6	Добавление устройства Check Point	35
8.6.1	Сетевые подключения Check Point	35
8.6.2	Настройка прав Check Point	36
8.7	Добавление устройства Check Point Multi-Domain Security Management	37
8.7.1	Установить права пользователя	40
8.8	Добавление SmartCenter/шлюз Check Point	40
8.8.1	Установить права для пользователя Нетхаб	42
8.9	Добавление СМА Check Point	42
8.9.1	Поля и параметры Check Point	44
8.9.2	Включить сбор данных для устройств Check Point	48
8.10	Добавление устройств Huawei USG	67
8.10.1	Установка плагина	68
8.10.2	Настройка фаервола	68
8.10.3	Подключение	69
8.11	Добавление устройств Usergate	70
8.11.1	Установка плагина	71
8.11.2	Подключение	71
8.12	Добавление устройств fortinet	71
8.12.1	Настройка прав для подключения	71
8.12.2	Подключение	73
8.12.3	ActiveChange	74
8.12.4	Сбор и мониторинг логов	74
9	Нетхаб Менеджер	76
9.1	Создание запроса на изменение	76

1 Общие сведения об ИС

1.1 Полное наименование системы и ее условное обозначение

Наименование: Решение(продукт) Нетхаб

Условное обозначение: Нетхаб/Nethub.

1.2 Назначение системы

Продукт Нетхаб, разработанный компанией ООО «Нетхаб», состоит из двух основных модулей: Нетхаб Аналитик и Нетхаб Менеджер. Нетхаб аналитик предназначен для сбора, и анализ конфигурации сетевых устройств. Нетхаб менеджер позволяет управлять конфигурациями сетевых устройств, включая гибкую настройка цепочек согласований (Workflow) и шаблонов заявок.

1.3 Функциональный состав системы

В состав системы входят следующие подсистемы:

- Модуль Аналитик
- Модуль Менеджер

1.4 Сценарии взаимодействия пользователя с Системой

Возможны следующие сценарии начала взаимодействия пользователя с системой:

- С помощью графического интерфейса администратора Нетхсб, загружаемого на удаленном АРМ при помощи веб-браузера.
- С помощью интерфейса командной строки, через протокол ssh.

1.5 Определения, обозначения, сокращения

БАЗА ДАННЫХ (БД) – Структурированное хранилище данных.

МСЭ – межсетевой экран

RAM – оперативно запоминающее устройство

АРМ – автоматизированное рабочее место

2 Требования

Клиентская автоматизированное рабочее место (далее - АРМ) необходимо для управления системой СУПОТОК.

На клиентском АРМ для работы с ОС должен быть установлен клиент для подключения по SSH (например Putty).

На клиентском АРМ рекомендуется использовать разрешение экрана 1920x1080 или выше.

Для работы с веб-интерфейсом Системы необходимо использовать один из следующих поддерживаемых браузеров:

- Firefox 2.0 и выше;
- Google Chrome;
- Internet Explorer 11 и выше;
- Microsoft Edge.

3 Доступ в Веб-интерфейс Нетхаб

Для начала работы с веб-консолью необходимо:

- 1) в одном из поддерживаемых браузеров перейти по адресу `https://<ip> /`, после чего появиться окно с предложением, ввода данных для аутентификации аналогичное рисунку Рисунок 1.

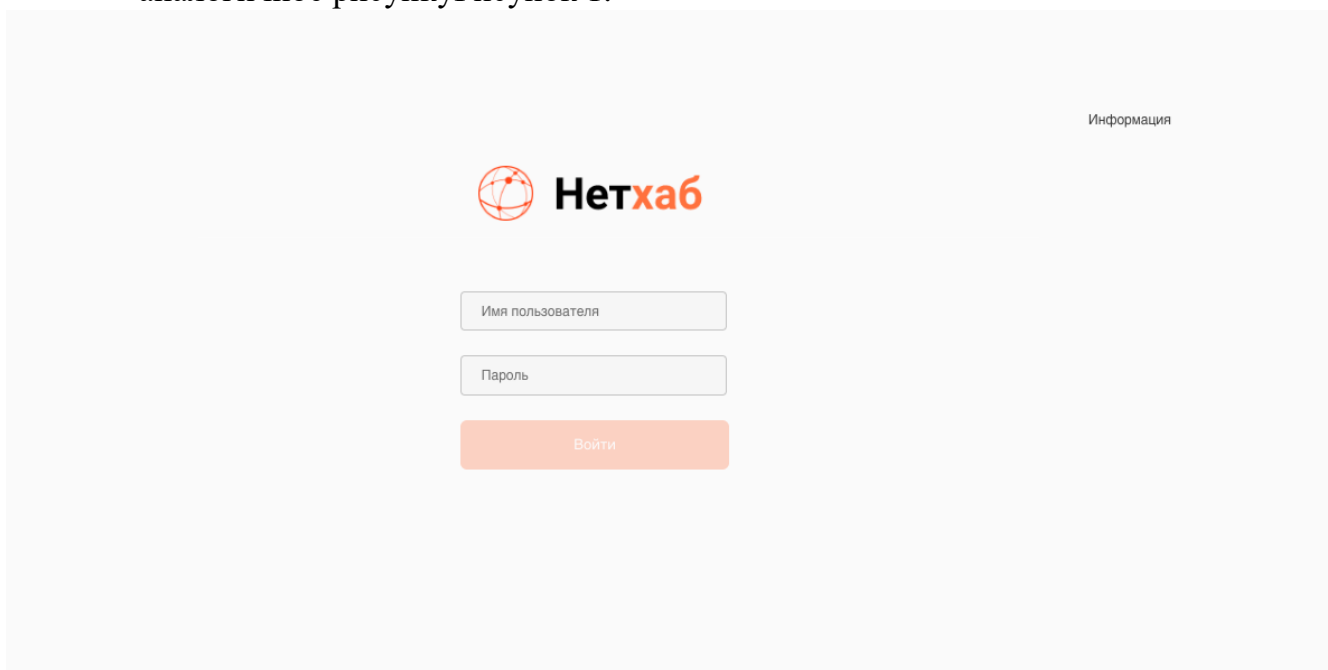


Рисунок 1 Окно аутентификации Нетхаб

- 2) ввести легитимные данные для доступа к веб-консоли. После входа, будет открыта главная страница Нетхаб аналитик (см. Рисунок 2).

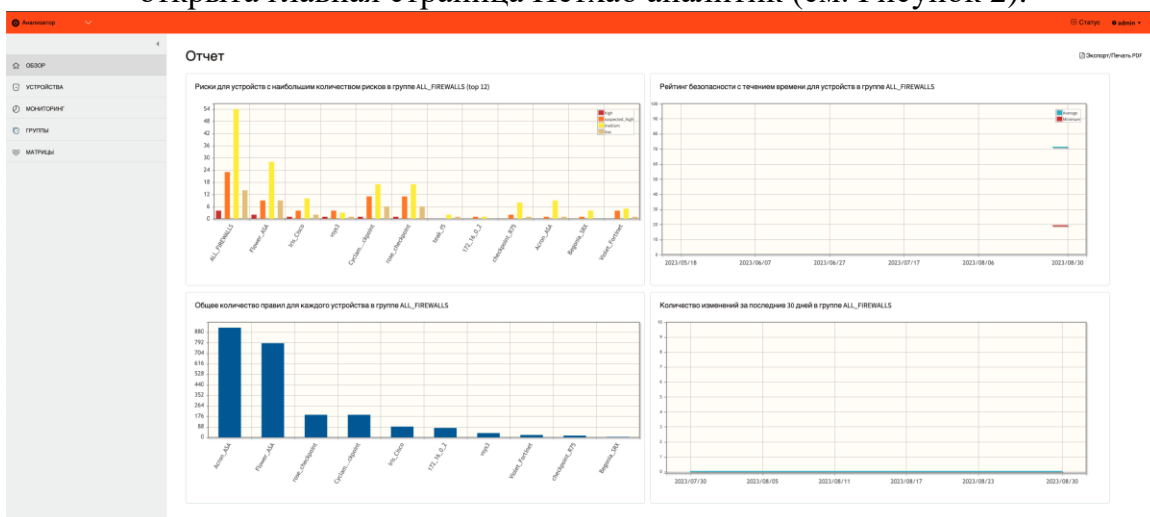


Рисунок 2 Главная страница Нетхаб аналитик

Для выхода из Нетхаб, необходимо нажать на меню пользователя и выбрать «Завершить сессию», аналогично Рисунок 3.

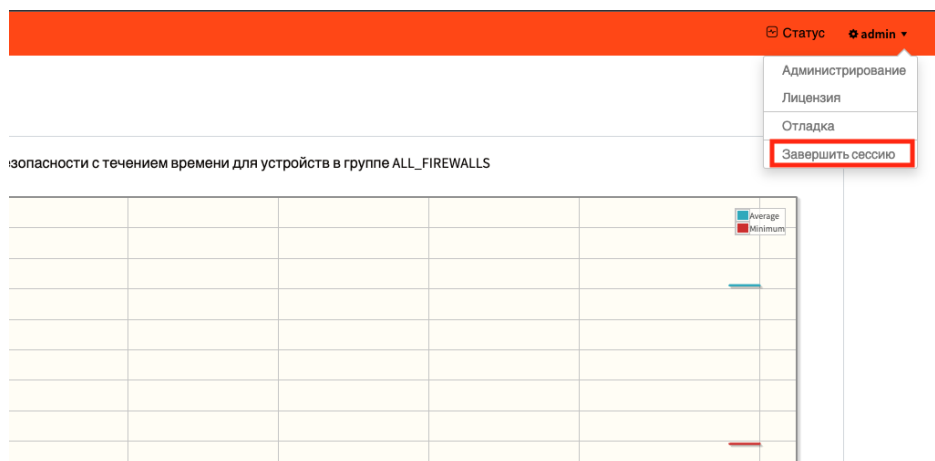


Рисунок 3 Выход из Нетхаб

4 Управление лицензиями

Обновление лицензии необходимо в следующих случаях:

- истек срок действия лицензии;
- превышены ограничения на количество устройств;
- добавление новых модулей Нетхаб.

4.1 Просмотр информации о текущей лицензии

Просмотр информации о лицензии необходим для получения информации о:

- текущем и максимально возможном количестве подключенных межсетевых экранов;
- текущем и максимально возможном количестве подключенных роутеров;
- MAC-адресе;
- ID лицензии.

Для просмотра информации о текущей лицензии:

- 1) подключиться к веб интерфейсу Нетхаб от имени администратора;
- 2) нажать на имя пользователя и выбрать пункт «Лицензия» в выпадающем меню (см. Рисунок 4);

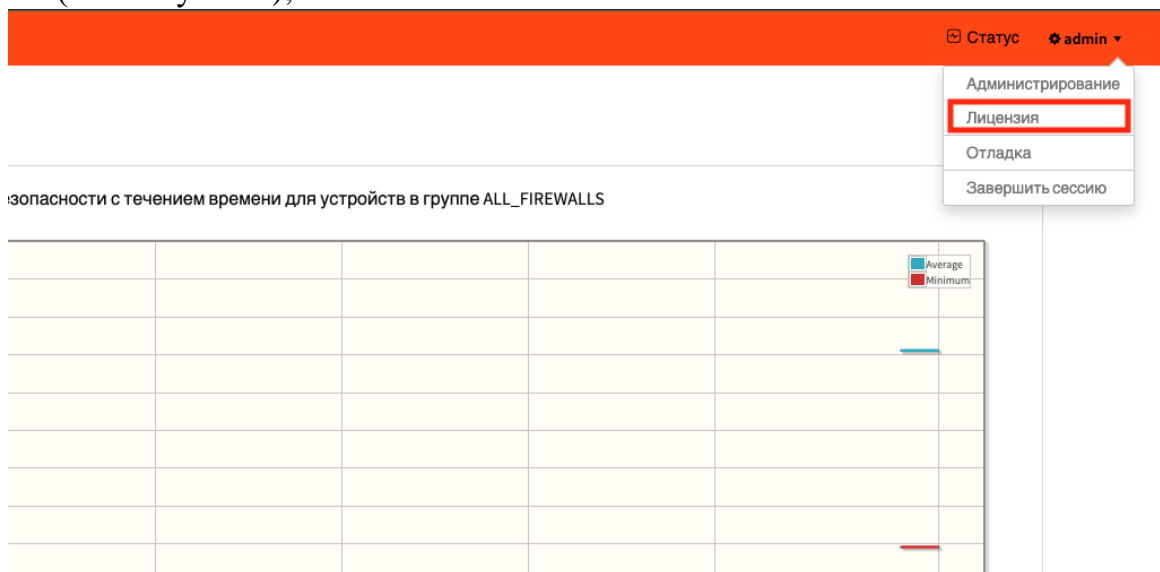


Рисунок 4 Выбор пункта «Лицензия»

Будет открыто окно аналогичное Рисунок 5.

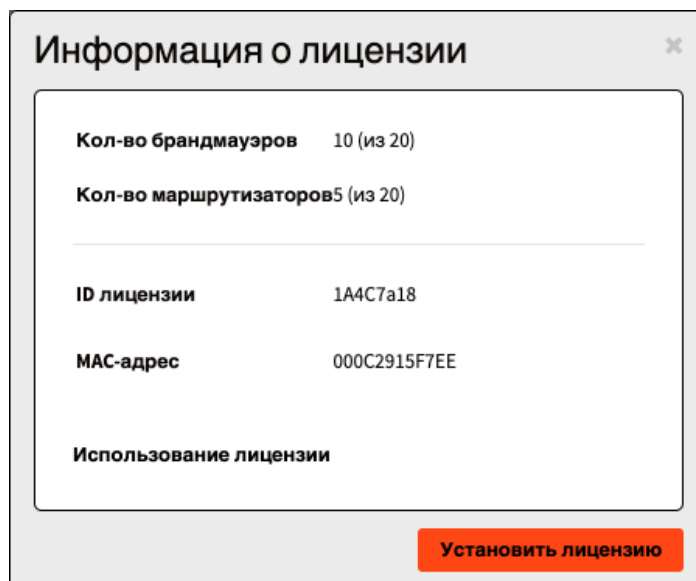


Рисунок 5 Информация о лицензии

4.2 Установка лицензии

1) Через веб интерфейса

Перейти в веб интерфейс из-под пользователя с правами администратора, нажать на имя пользователя и выбрать пункт «Лицензия» (см. Рисунок 4). Будет открыта страница информации лицензии Нетхаб, где необходимо нажать кнопку «Установить лицензию» (откроется страница с пользовательское соглашение аналогично Рисунок 5). Далее открывается окно установки лицензии (Рисунок 7), где нужно указать путь до актуального файла лицензии (с расширение lic), выбрав элемент «Выберете файл», и запустить установку лицензии «Установить».



Рисунок 6 Пользовательское соглашение Нетхаб

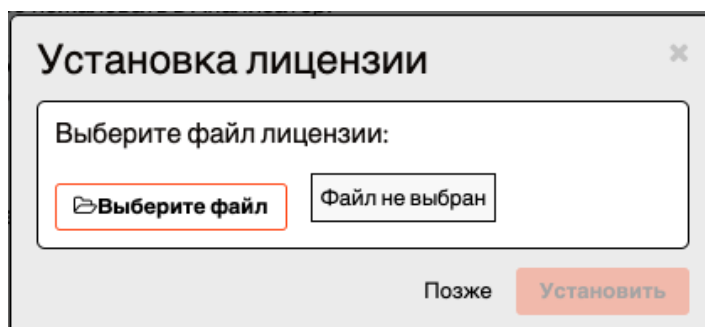


Рисунок 7 Установка лицензии

2) Через интерфейс командной строки

Подключиться к серверу, на котором установлен Нетхаб, через клиент SSH и выполнить команду:

```
nethub_conf
```

Будет открыта консольная утилита для настройки Нетхаб (см. Рисунок 8).

```
Пожалуйста, выберите элемент конфигурации:
1. Настройка IP-адреса
2. Настройка времени и даты
3. Настройка сервера DNS
4. Изменение доменного имени DNS
5. Изменить имя хоста
6. Измените root пароль
7. Измените afa пароль
8. Обновление программного обеспечения
9. Сброс пароля администратора AFA
10. Сброс пароля базы данных
11. Настройка NAS
12. Установить лицензию
13. Настройка HA/DR
14. Конфигурация продукта
15. Конфигурация распределенной архитектуры
16. Перенос узлов Нетхаб
17. Здоровье системы
18. Сбор логов
Q. Выход из системы

Нажмите 'a' для выхода из оболочки
Your choice:
> |
```

Рисунок 8 Консольная утилита для настройки Нетхаб

Далее необходимо ввести «12» и выбрать пункт «Установить лицензию», после чего будет открыто диалоговое окно, в котором необходимо указать путь до файла лицензии (с расширение lic).

5 Управление устройствами

5.1 Добавление устройств

Для добавления устройств в Нетхаб нужно:

- 1) Нужно на главной странице Нетхаб Аналитик выбрать панель «УСТРОЙСТВА»:

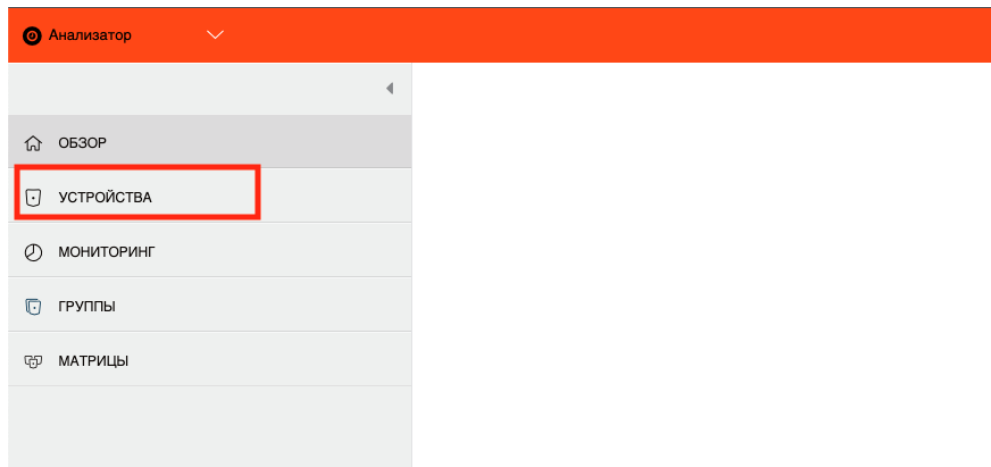


Рисунок 9 Переход на панель УСТРОЙСТВА

- 2) Нажать на иконку ключа рядом с заголовком УСТРОЙСТВА (см. Рисунок 10), для перехода на страницу управления устройствами.

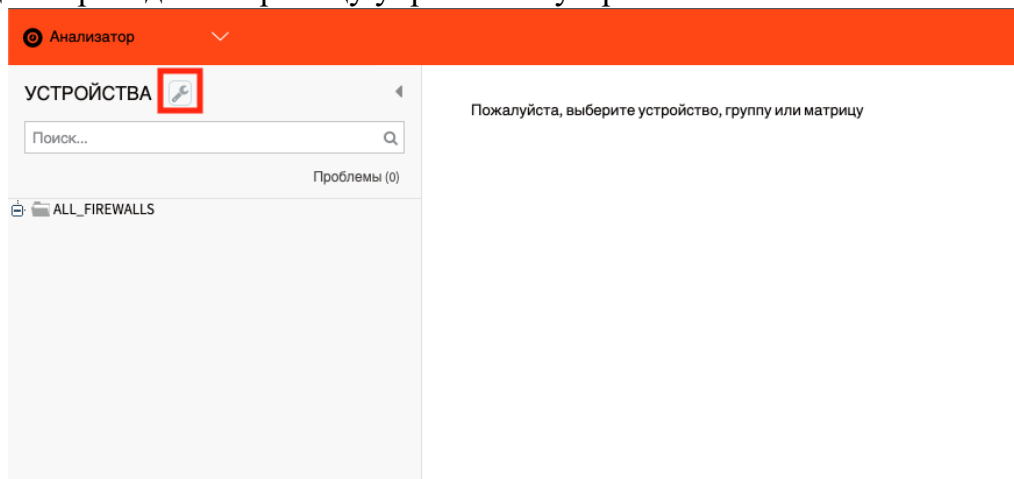


Рисунок 10 Переход на страницу управления устройствами

- 3) В меню управления нажать на выпадающий список «Добавить», далее выбрать опцию «Устройство» (Рисунок 11).

Администрирование

НАСТРОЙКА УСТРОЙСТВ

ПОЛЬЗОВАТЕЛИ/РОЛИ

ПЛАНИРОВАЩИК

СООТВЕТСТВИЕ

ОПЦИИ

МОНИТОРИНГ

АРХИТЕКТУРА

Настройте параметры, необходимые для сбора политик устройства

FIREWALLS
GROUPS
LOG_SERVERS
MATRICES
DR SETS

Добавить ▾

Устройство

Группу

Матрицу

Настройка DR

Разрешения

Большой объем ▾

Рисунок 11 Переход в меню добавления устройств

4) Выбрать нужного производителя сетевого оборудования и конкретную модель из предложенного списка (см. Рисунок 12).

Настройте параметры, необходимые для сбора политик устройства

Check Point	Avaya	
Cisco	Brocade	Amazon
F5	H3C	Microsoft
Fortinet	Linux	
Juniper	Secui	Устройство из файла
Palo Alto Networks	SonicWALL	Элемент маршрутизации
VMware	Symantec	
	Topsec	
	WatchGuard	

Назад

Рисунок 12 Окно выбора производителя сетевого оборудования

5) Следуя инструкциям для каждого конкретного вида устройства (см. раздел 8), указать валидные данные для подключения к устройству для сбора актуальной конфигурации с устройства, аналогично Рисунок 13.

Настройте параметры, необходимые для сбора политик устройства

Информация о доступе

Тип:

Cisco ASA

Хост:

test_host

Имя пользователя:

test_user

Пароль:

Пароль привилегированного пользователя:

Географическое распределение

Устройство, управляемое (?):

Central Manager ▼

Соответствие базовой конфигурации

Профиль соответствия базовой конфигурации:

Cisco - ASA ▼

Возможности удаленного управления

☒ SSH
 ☐ Нестандартный порт

Количество разрешенных ключей шифрования: (?)

безлимитно ▼

☐ SSH (Triple-DES)

☐ SSH (DES)

☐ Telnet

Рисунок 13 Пример заполнения данных

5.2 Добавление устройства из файла

- 1) Перейти в меню добавления устройств (см. Рисунок 12);
- 2) На странице выбора вендора и типа устройства, нажмите «Устройство из файла»;
- 3) В поле имя введите имя вашего устройства;
- 4) Выберите файл, который хотите проанализировать, выбрав один из следующих вариантов:

Загрузить новый	<p>Загрузите файл с вашего компьютера. Найдите и выберите свой файл.</p> <p>Размер файла не должен превышать 20 МБ.</p> <p>Для больших файлов скопируйте файл в каталог /home/afa/nethub/fwfiles и используйте параметр «Существующий на сервере».</p>
Существующий на сервере	<p>Выберите файл, уже сохраненный на сервере Нетхаб, в каталоге /home/afa/nethub/fwfiles.</p>

Выберите файл, который хотите проанализировать, из выпадающего списка.

5) Определите как Нетхаб должен получать информацию о маршрутизации устройства. Выберите один из следующих вариантов:

Автоматический	Автоматически генерировать информацию о маршрутизации устройства при анализе или мониторинге.
Статическая таблица маршрутизации (URT).	Возьмите информацию о маршрутизации устройства из предоставленного вами статического файла.

6) Выберите параметр «Мониторинг изменений в режиме реального времени», чтобы включить оповещение в реальном времени при изменении конфигурации

7) Если в области Опции выбран пункт «Установить права доступа пользователей», появится диалоговое окно редактирование прав пользователей для этого устройства;

8) Нажмите «Добавить». Новое устройство добавлено в дерево устройств.

Настройте параметры, необходимые для сбора политик устройства

Информация о доступе

Тип:

Имя:

Файл: ☒ Загрузить новый ☐ Существует на сервере

Максимальный размер: 20MB (?)

10_46_82_...rew@ll.nxst

Максимум: 20 MB

Коллекция маршрутов

Метод сбора информации о маршруте (?)

☒ Автоматически

☐ Статическая таблица маршрутизации (URT)

Опции

☒ Мониторинг изменений в режиме реального времени

☒ Установить права доступа пользователей

Отмена

Рисунок 14 Пример заполнения данных

5.3 Изменение устройств

Перейти на страницу управления устройствами (см. Рисунок 10). Выбрать нужное устройство из древовидного списка устройств, добавленных в Нетхаб. Далее выбрать опцию «Изменить» для изменения данных и параметров об устройстве (см. Рисунок 13).

Настройте параметры, необходимые для сбора политик устройства

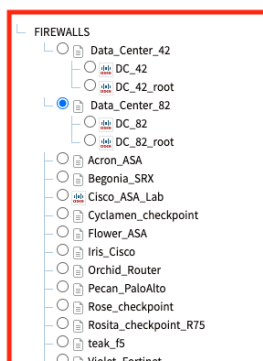


Рисунок 15 Страница управления устройствами

5.4 Удаление устройств

Перейти на страницу управления устройствами (см. Рисунок 10). Выбрать нужное устройство из древовидного списка устройств, добавленных в Нетхаб. Далее выбрать опцию «Удалить» для устройства из Нетхаб (см. Рисунок 15).

6 Анализ

6.1 Создание и просмотр отчета об анализе

Отчет об анализе устройства позволяет получить всю доступную информацию о устройстве и его состоянии.

Для просмотра информации о устройстве необходимо перейти в вкладку «УСТРОЙСТВА» (см. Рисунок 9) и выбрать необходимое устройство из списка слева. Также необходимо убедиться, что иконки «Анализ» и «Мониторинг» имеют зеленую индикацию (см. Рисунок 16) и нажать кнопку Анализ для создания отчета.

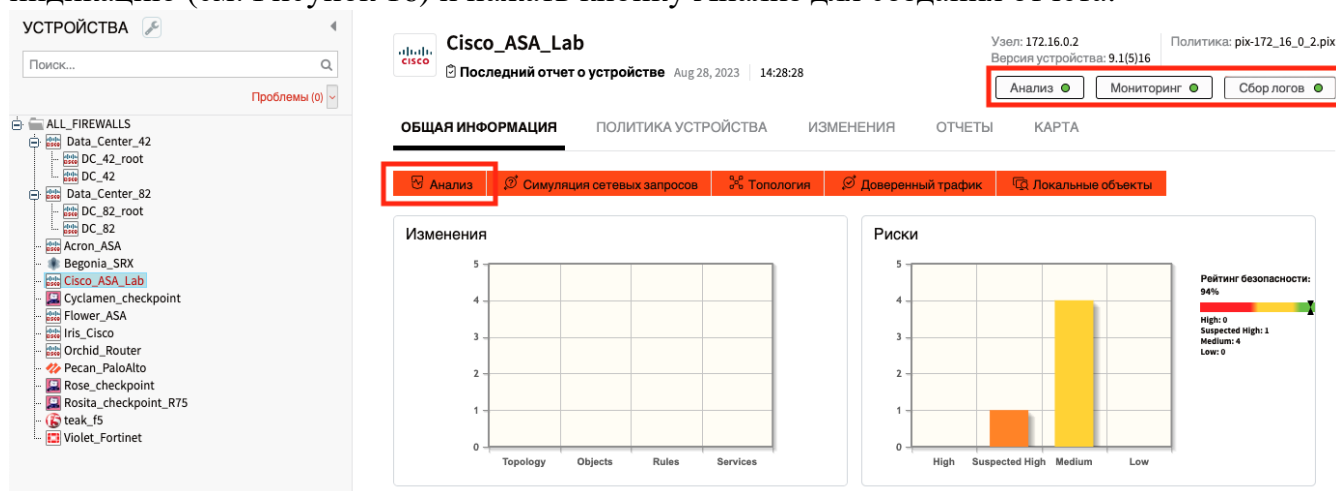


Рисунок 16 Анализ устройства

7 Настройка параметров системы

7.1 Панель администрирования

Большинство настроек Нетхаб выполняется из панели администрирования. Для доступа в панель администрирования, необходимо нажать на меню пользователя и выбрать пункт «Администрирование», аналогично Рисунок 17.

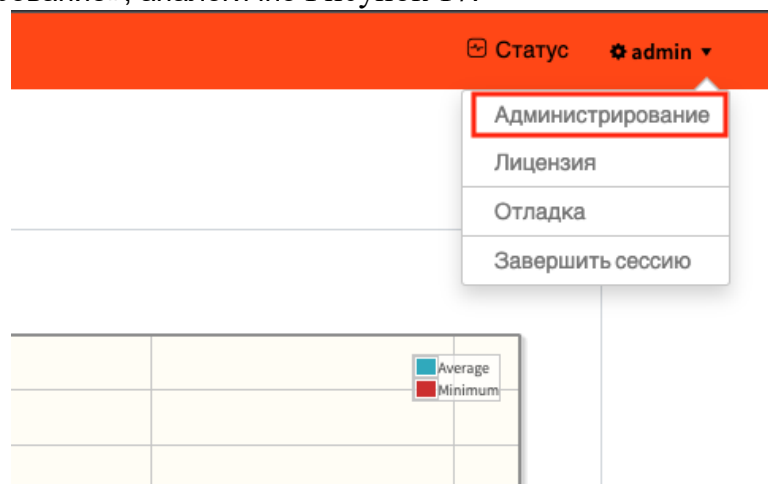


Рисунок 17 Администрирование

Панель администрирования включает следующие вкладки:

НАСТРОЙКА УСТРОЙСТВ	Управление устройствами и группами.
ПОЛЬЗОВАТЕЛИ/РОЛИ	Управление пользователями и ролевым доступом.
ПЛАНИРОВЩИК	Создание и планирование повторяющихся задач (анализ, уведомления).
ПРОВЕРКА НА СООТВЕТСТВИЕ	Настройка профилей рисков и базовых профилей для анализа.
ОПЦИИ	Настройка опций, таких как электронная почта, дисковое пространство, аутентификация, анализ логов, резервное копирование и восстановление и др..
МОНИТОРИНГ	Настройка мониторинга устройств.
АРХИТЕКТУРА	Настройка распределенной архитектуры.

7.2 увеличение дискового простарнтсва

Для просмотра используемого и свободного дискового пространства необходимо в системной консоли ввести команду:

```
df -h
```

Команда `df` отображает для каждого раздела: общий размер (Size), используемое пространство (Used), свободное пространство (Avail), процент использования раздела (Use%) и точку монтирования на файловой системе.

7.3 Расширение дискового пространства путем монтирования нового диска

Для увеличения дискового пространства при помощи монтирования нового диска используется в случае добавления нового диска для виртуальной машины. Для подключения необходимо:

- 1) Проверить смонтированные диски путем ввода команды:
- 2) `«lsblk»`;
- 3) необходимо найти подключаемый диск путем ввода команды `«fdisk -l»`;
- 4) инициализировать диск при помощи команды `«pvcreate /dev/<sda_name>»`, где `<sda_name>` - название подключаемого диска, найденного при выполнении шага 2;
- 5) ввести команду `«vgdisplay»` и скопировать значение переменной «VG Name»;
- 6) увеличить размер логического тома при помощи команды `«vgextend <VGName> /dev/<sdb>»`, где `VGName` - переменная, полученная из 4 шага, а `sdb` – переменная из 2 шага;

7.4 Расширение дискового пространства путем расширения существующего диска

Для увеличения дискового пространства путем расширения существующего диска в виртуальной машине, необходимо:

- 1) удостовериться в наличии актуальной версии резервной копии Нетхаб;
- 2) ввести следующую команду и удостовериться, что дополнительный объем диска был обнаружен:
- 3) `«lsblk»`;
- 4) ввести следующую команду для получения текущего размер раздела данных перед его увеличением:
- 5) `«df -h»`;
- 6) запустить утилиту для работы с дисковым пространством путем ввода следующей команды:
- 7) `«cfdisk»`;
- 8) Разбить существующий виртуальный диск в качестве разделов LVM с использованием `cfdisk`:
- 9) используя `<TAB>` перейти в: New -> Primary -> убедиться, что размер дискового пространства в порядке -> Enter;

- 10) используя <TAB> перейти в: Type -> Введите тип файловой системы -> 8E для Linux LVM;
- 11) используя <TAB> перейти в: Write to save change-> введите «yes»;
- 12) используя <TAB> перейти в: Quit.;
- 13) перезагрузить Nethub Virtual Machine (VM);
- 14) путем ввода «lsblk», проверьте, какие разделы были распознаны после перезагрузки;
- 15) путем ввода «pvcreate /dev/sda3» создайте физический том для этого LVM-диска;
- 16) ввести «vgextend centos /dev/sda3»;
- 17) ввести «pvscan» и проверить корректность заданных индексов и доступного объема;
- 18) для расширения логического тома ввести «lvextend /dev/centos /data /dev/sda3»;
- 19) ввести «resize2fs /dev/centos /data» для увеличения или уменьшения размонтированного дискового пространства;
- 20) ввести «df -h» и убедиться, что доступный размер дискового пространства изменился.

7.5 Ручное определение URT

Нетхаб компилирует данные маршрутизации и топологии, собранные с каждого устройства, в файл единой таблицы маршрутизации (URT), в котором данные хранятся в общем формате Нетхаб. По умолчанию этот файл автоматически обновляется каждый раз, когда устройство отслеживается или анализируется.

Администраторы Нетхаб могут вручную изменить данные маршрутизации и топологии устройства двумя способами:

- 1) **Статический метод:** в файл URT добавляется статическое представление устройства. Впоследствии Нетхаб не будет автоматически восстанавливать обновленные файлы URT для этого устройства. Администратор должен снова вручную обновить файл URT для любых изменений конфигурации.
- 2) **Гибридный метод:** в файл URT для устройства вручную добавляется только настроенная часть информации о маршрутизации (например, дополнительный интерфейс или маршруты). Впоследствии Нетхаб автоматически создаст обновленные файлы URT для этого устройства.

7.6 Использование статического метода

Следуйте следующей инструкции:

- 1) Откройте страницу настройки устройств. Подробнее см. в разделе Доступ к странице НАСТРОЙКА УСТРОЙСТВ;

- 2) В дереве слева выберите устройство или вспомогательное устройство, которое вы хотите изменить, а затем нажмите «Изменить» справа;
- 3) В области Коллекция маршрутов выберите Статическая таблица маршрутизации (URT);
- 4) Если у вас уже есть определенный URT, который вы хотите отредактировать, щелкните. Загрузить текущий файл URT. Чтобы создать новый файл URT, щелкните. Загрузить образец файла;
- 5) Отредактируйте файл с информацией о маршрутизации, которую вы хотите импортировать;
- 6) Снова откройте страницу настройки устройств;
- 7) В дереве слева выберите устройство или вспомогательное устройство, которое вы хотите изменить, а затем нажмите «Изменить» справа;
- 8) В области Коллекция маршрутов выберите Статическая таблица маршрутизации (URT);
- 9) Нажмите «Загрузить новый файл» и выберите отредактированный файл;
- 10) NETXAB проверяет ваш файл и уведомляет вас, если обнаружена какая-либо ошибка синтаксиса или содержимого;
- 11) 10. По завершении нажмите ОК;
- 12) Новая таблица маршрутизации вступит в силу после следующего анализа устройства.

7.7 Использование гибридного метода

Чтобы вручную указать данные маршрутизации в гибридном режиме для устройства сделайте следующее:

- 1) Создайте новые файлы URT, отредактируйте существующий или отредактируйте загруженный образец URT.
- 2) Для одного устройства без дочерних устройств на URT укажите дополнительные маршруты. Если у устройства есть подчиненные устройства, создавайте файлы URT для каждого вспомогательного устройства, а не для родительского устройства. Укажите дополнительные маршруты для дочернего устройства.
- 3) Назовите файл(ы) additionalRoutes.urt (обязательно назовите каждый файл URT точно так. Имя файла чувствительно к регистру).
- 4) Сохраните файл(ы) в папке /home/afa/.fa/firewalls/<deviceTreeName> для одного устройства без подустройств или, если у устройства есть подустройства, сохраните в каждой подпапке /home/afa/.fa/firewalls/<deviceTreeName>/<sub-device name>.
- 5) Проанализируйте устройство.

7.8 Описание других опций

7.8.1 ПОЛЬЗОВАТЕЛИ/РОЛИ

Нетхаб поддерживает аутентификацию через сервер аутентификации LDAP или RADIUS, единый вход (SSO) или локальных пользователей Нетхаб.

Настройка сервера аутентификации или SSO предоставляет дополнительные возможности, например, ассоциирование каждой роли Нетхаб аналитик с определенной группой LDAP. В этом случае пользователям автоматически назначаются роли в соответствии с их принадлежностью к группе LDAP.

Типы пользователей и разрешения:

Администратор	Могут выполнять любые задачи. Например, в дополнение к задачам, которые могут выполнять неадминистративные пользователи, администраторы могут также: - Управлять другими пользователями; - Определять и редактировать контролируемые устройства; - настраивать общие параметры и предпочтения Нетхаб аналитик; - Планировать анализ.
Стандартный пользователь	Может проводить анализ, формировать отчеты, просматривать политики и отчеты, просматривать карту сети и изменения в мониторинге, а также выполнять запросы на моделирование трафика.

7.8.2 ПЛАНИРОВЩИК

В этом разделе описано, как планировать анализы для устройств и групп. Нетхаб может выполнять несколько отчетов параллельно, при этом максимальное количество отчетов, которые могут быть сформированы одновременно, зависит от конфигурации и мощности вашей системы.

Чтобы запланировать новый повторяющийся анализа, в области «Планировщик – Запланировать повторяющийся анализ» нажмите кнопку «Новый».

Запланировать повторяющийся анализ

	Задание	Имя	Время	Устройства/группы	Профиль риска	Изменить
--	---------	-----	-------	-------------------	---------------	----------

Удалить

Новый

Электронная почта панели расписания

	Задание	Имя	Время	Панель управления	Изменить
--	---------	-----	-------	-------------------	----------

Удалить

Новый

Рисунок 18 Обзор планировщика

Появится окно, в котором можно настроить параметры для повторяющегося анализа.

Запланировать повторяющийся анализ

Детали работы

Название задачи:

☐ Основные групповые отчеты по существующим отчетам об устройствах.

☐ Выберите профиль риска: Стандартный ▾

Запустить анализ устройства: Default (только если политика/топология изменилась) ▾ (?)

Выбор устройства/группы

Запланировать задание для устройства/группы: Пожалуйста, выберите устройство или группу

Выбрать устройство / группу

Повторение

☒ Ежедневно

☐ Еженедельно

☐ Ежемесячно

☐ Ежеквартально

☐ Ежегодно

☐ После установки политики

Шаблон повторения

Установить время: 19 ▾ : 30 ▾

Отмена ОК

Рисунок 19 Создание повторяющегося анализа

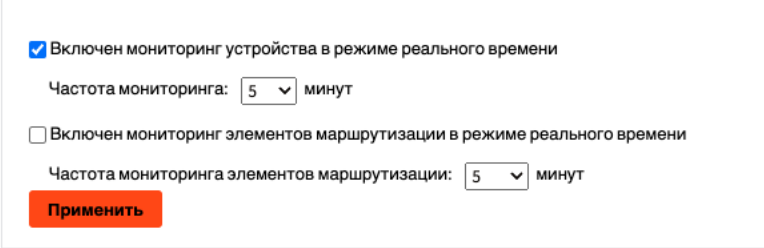
7.8.3 СООТВЕТСТВИЕ

Нетхаб поддерживает множество настроек для работы с рисками и соответствием стандартам. В данном разделе доступен следующий функционал:

- 1) Создание пользовательских профилей риска с помощью встроенных и пользовательских элементов риска;
- 2) Настройка профилей риска;
- 3) Настройка элементов риска;
- 4) Определять новые типы зон в дополнение к предопределенным Внутренняя, Внешняя и DMZ;
- 5) Добавление новых определений групп хостов;
- 6) Добавление новых определений служб;
- 7) Настроить рейтинг безопасности и способ отображения информации о рейтинге безопасности;
- 8) Настроить стандарты соответствия нормативным требованиям, применимые к вашей среде;
- 9) Настроить требования к конфигурации для соответствия базовому уровню.

7.8.4 МОНИТОРИНГ

В Нетхаб предусмотрена возможность мониторинга устройств на предмет изменений в режиме реального времени. Нетхаб будет периодически проверять политики устройств на предмет изменений, и обнаруженные изменения будут отображаться в Web-интерфейсе Нетхаб.



☒ Включен мониторинг устройства в режиме реального времени
Частота мониторинга: 5 минут

☐ Включен мониторинг элементов маршрутизации в режиме реального времени
Частота мониторинга элементов маршрутизации: 5 минут

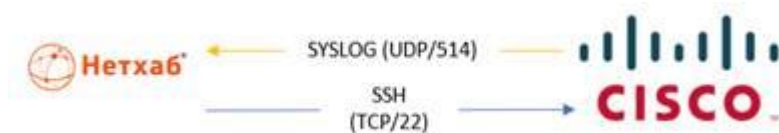
Применить

Рисунок 20 Настройка мониторинга

8 Добавление устройств

8.1 Добавление устройств Cisco ASA

В этом разделе описывается как добавить устройства Cisco в Нетхаб и выполнить нужные настройки. Для подключения сетевого устройства к Нетхаб, необходимо предоставить следующий сетевой доступ:



Создайте нового пользователя:

1. Войдите на устройство Cisco как привилегированный пользователь.
2. Войдите в режим enable.
3. Выполните следующие команды:

Общие команды	<pre> configure terminal username <username> password <password> privilege 5 privilege show level 5 command version privilege show level 5 command mode privilege show level 5 command access-list privilege show level 5 command running-config privilege show level 5 command route privilege configure level 5 command pager </pre>
Устройства ASA с ACL IPV6	<pre> privilege show level 5 command ipv6 </pre>
Устройства ASA с тегами группы безопасности	<pre> privilege configure level 5 command cts sgt-map </pre>
Устройства ASA с контекстом безопасности	<pre> privilege show level 5 command context </pre>

8.1.1 Стандартный метод

- 1) Перейти на страницу добавления устройств (подробнее в разделе 5.1);
- 2) На странице выбора вендора и устройства выберите Cisco > ASA.
- 3) Заполнить необходимые поля для устройства;

Хост	Введите имя хоста или IP-адрес устройства.
------	--

Имя пользователя	Введите имя пользователя, которое будет использоваться для SSH-доступа к устройству.
Пароль	Введите пароль, который будет использоваться для SSH-доступа к устройству.
Пароль привилегированного пользователя	Введите пароль пользователя enable для использования: <ul style="list-style-type: none"> • noenable. Пропустить выполнение команды enable. • Nethub_no_passwd. Пароль пользователя enable пуст. • Пустое поле. Вместо команды enable Нетхаб аналитик выдаст команду login, используя тот же пароль, что и при SSH-соединении.

- 4) Если вы включили ActiveChange, появится диалоговое окно Лицензионное соглашение ActiveChange. Выберите (Согласен) и нажмите кнопку ОК;
- 5) Нажмите кнопку (Добавить). Новое устройство будет добавлено в дерево устройств;
- 6) Если в области Опции выбран пункт «Установить права доступа пользователей», появится диалоговое окно редактирование прав пользователей для этого устройства;
- 7) Появится сообщение об успехе, подтверждающее, что устройство добавлено.

Настройка параметров, необходимых для сбора политик устройства

Информация о доступе

Тип: Cisco ASA

Хост:

Имя пользователя:

Пароль:

Пароль привилегированного пользователя:

Географическое распределение

Устройство, управляемое (1):

Соответствие базовой конфигурации

Профиль соответствия базовой конфигурации:

Возможности удаленного управления

☒ SSH ☒ Настраиваемый порт: Количество разрешенных ключей шифрования:

☐ SSH (Triple-DES)

☐ SSH (DES)

☐ Telnet

Коллекция маршрутов

Метод сбора информации о маршруте (1)

☒ Автоматически

☐ Статическая таблица маршрутизации (SRT)

Просмотр правил

☒ ASDM

☐ CLI

Примечание: некоторые функции доступны только в режиме ASDM (1)

Рисунок 21 Пример добавления Cisco ASA

8.1.2 Альтернативный метод (ручной)

- 1) Подключиться к межсетевому экрану ASA, используя SSH (или Telnet), и записать сеанс в файл;
- 2) Переключиться в режим привилегированного пользователя, введя enable и пароль для привилегированного пользователя.

3) Выполнить следующие команды:

```
show version
show running-config
```

4) Если вы используете динамическую маршрутизацию, выполните:

```
show route
show access-list
exit
```

5) Отредактируйте файл с записью сеанса с помощью текстового редактора.

6) Замените каждую командную строку разделителями, как показано ниже

Что заменять	На что заменять
asafirewall# show access-list	=== show access list ===
asafirewall# show route	=== show route ===

7) Сохранить файл с расширением «.rix»;

8) Добавить устройство из файла (Подробнее в разделе 5.2).

— Добавление устройств Check Point

В этом разделе описывается как добавить устройства Check Point в Нетхаб и выполнить нужные настройки.

На схеме ниже показано сетевое подключение Нетхаб к устройствам Check Point MDSM, CMA или Smart Center и шлюзу Check Point. Версии Check Point R80 и выше имеют дополнительное подключение через HTTP-REST.

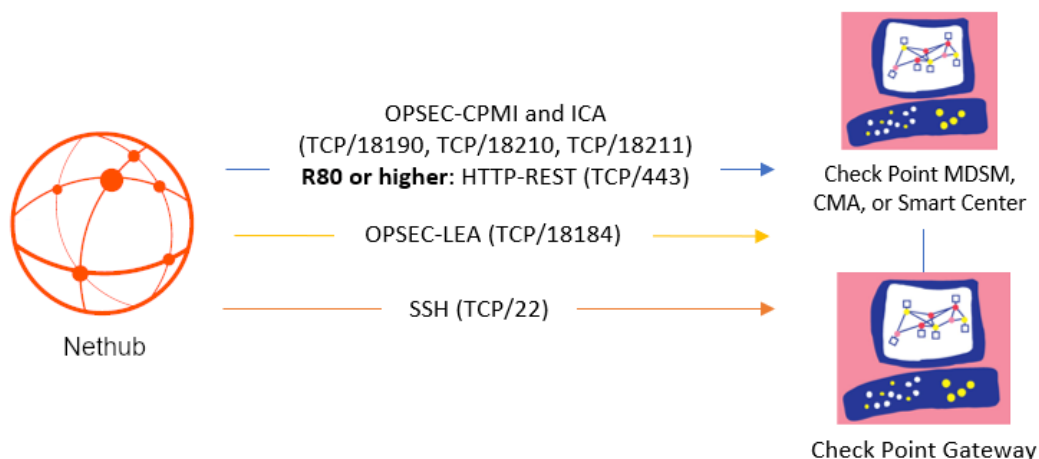


Рисунок 22 Схема сетевого подключения к Check Point

8.1.3 Настройка прав для подключения

Нетхаб может собирать данные и логи через SSH или OPSEC. Для версий Check Point R80 и выше необходимо также определить сбор данных через REST.

Нетхаб требует следующие разрешения для каждого типа подключения к вашим устройствам Check Point:

а) OPSEC

Нетхаб необходимы минимальные права объекта CPMI и LEA OPSEC для подключения к устройствам Check Point и автоматической инициализации сбора логов через определенное соединение LEA.

В интерфейсе Check Point определите права следующим образом:

CPMI	<p>Выберите следующие права CPMI:</p> <ul style="list-style-type: none"> • Разрешить доступ через Management Portal и SmartConsole Applications • Permissions > Read Only All. Чтобы использовать ActiveChange, выберите Read/Write All.
LEA	На вкладке LEA Permissions , в Permissions to Read Logs , выбрать Show all log fields .

б) SSH

Нетхаб должен иметь SSH доступ к соответствующим устройствам управления и регистрации, таким как PV-1, CMA, SmartCenter, внешний лог -сервер или CLM.

- Для **SecurePlatform (SPLAT)** необходимо разрешить Нетхаб переключаться в экспертный режим.
- Для **Solaris/RHEL/IPSO**, Нетхаб должен подключаться от имени пользователя root

Также поддерживается аутентификация с открытым ключом. В таких случаях требуются следующие права:

Read	Нетхаб требует права на чтение папок домена, таких как \$FWDIR/conf или \$FWDIR/log.
Write	<p>Нетхаб записывает пакет, содержащий необходимую конфигурацию, в каталог /tmp или /var/tmp, в зависимости от платформы устройства, например SP или Solaris.</p> <p>Нетхаб аналитик также требует прав на запись в каталоге \$FWDIR/conf для временных файлов логов.</p>

Execute	Нетхаб запускает несколько команд на устройстве управления, включая <code>fwm logexport</code> для логов и <code>crstat</code> для маршрутизации.
----------------	---

в) REST

При использовании устройства Check Point версии R80 или выше, Нетхаб также собирает данные через REST, в дополнение к OPSEC или SSH.

В дополнение к правам OSPEC или SSH, Нетхаб должен иметь права на выполнение вызовов REST к серверу Check Point Security Management Server.

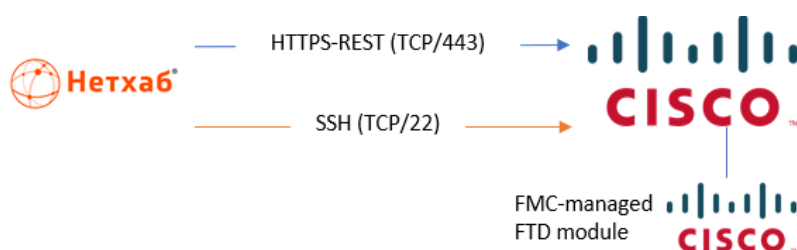
- Минимальные необходимые права Read Only All.
- Когда функция ActiveChange включена, минимальными правами являются Read\Write All.

8.2 Cisco Firepower

В этом разделе описывается как добавить устройства Cisco FTD в Нетхаб и выполнить нужные настройки.

8.2.1 Предварительная настройка

Для подключения сетевого устройства к Нетхаб, необходимо предоставить следующий сетевой доступ:



Нетхаб требует следующих разрешений устройства для подключения к устройствам Cisco Firepower:

Анализ устройства

Система Cisco Firepower включает в себя как межсетевые экраны Firepower Management Center (FMC), так и Firepower Threat Defense (FTD).

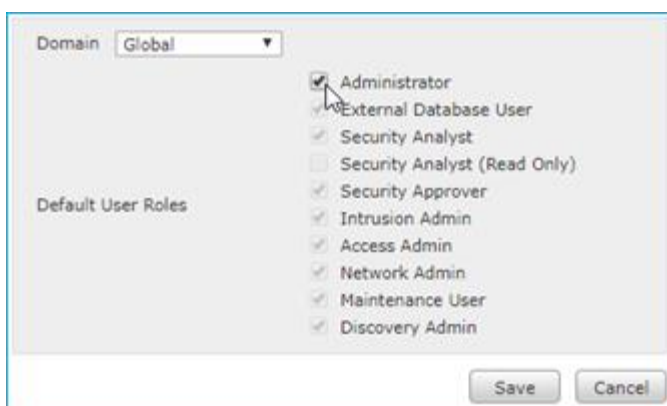
Нетхаб Аналитик напрямую управляет FMC, в основном поддерживая FTD через FMC API. Кроме того, Нетхаб Аналитик собирает данные о маршрутизации и базовом соответствии требованиям непосредственно от FTD через SSH. Следовательно, Нетхаб Аналитик должен иметь оба следующих права доступа:

- API (HTTPS) доступ к FMC
- SSH доступ к FTD. Нетхаб Аналитик не поддерживает прямой доступ к API FDM.

Для подключения к FMC, Нетхаб требуется пользователь с ролью администратора, т.е.:

- Предназначен для Нетхаб. Подключение к устройству с использованием любого другого пользователя может привести к выходу этого пользователя из пользовательского интерфейса Firepower при каждом цикле мониторинга, а также при любых изменениях, внесенных в устройство Firepower через Нетхаб.
- В глобальном домене

Например:



Примечание. Требуется роль уровня администратора из-за ограничений FMC на получение журналов аудита.

Для использования ActiveChange, Нетхаб требует разрешений на чтение и запись. Пользователь должен продолжать сохранять права администратора.

8.2.2 Добавление Cisco Firepower

В этой процедуре описывается, как добавить устройство Cisco Firepower в Нетхаб Аналитик.

Сделайте следующее:

1. Откройте страницу настройки устройств.
2. На странице выбора производителя и устройства выберите **Cisco > Firepower**.
3. При необходимости заполните поля на странице.

Например:

Firepower - Step 1/2

4. Нажмите Next для перехода на страницу **FirePower - Step 2/2**. На этой странице перечислены FTD, которыми управляет Firepower FMC.

Будет открыта страница аналогичная следующему:

Настройте параметры, необходимые для сбора политик устройства

Firepower - Step 2/2

5. Чтобы исключить FTD, снимите его флажок в таблице.

6. Нажмите **Настройка**, чтобы настроить детали для выбранных FTD.

В «Конфигурация прямого доступа», определите Host, User Name, Password, и Baseline Profile для каждого FTD.

Чтобы отключить создание базового отчета о соответствии для этого устройства, выберите **None**.

Нажмите «Тестировать», чтобы проверить соединения с определенными FTD, а затем нажмите «ОК».

Примечание. Необходимо указать учетные данные для каждого FTD, чтобы Нетхаб Аналитик мог собирать данные маршрутизации, необходимые для точного анализа устройства.

7. Если вы включили ActiveChange, появится диалоговое окно Лицензионного соглашения ActiveChange.

Выберите «Я согласен» и нажмите «ОК».

8. Нажмите **Finish**.

Новое устройство добавляется в дерево устройств.

9. Если вы выбрали «Установить права пользователя», появится диалоговое окно «Редактировать пользователей».

В отображаемом списке пользователей выберите одного или нескольких пользователей, чтобы предоставить доступ к отчетам для этой учетной записи.

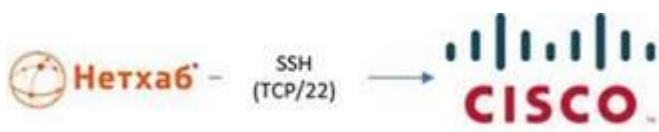
Чтобы выбрать нескольких пользователей, нажмите кнопку CTRL во время выбора.

Нажмите кнопку ОК, чтобы закрыть диалоговое окно.

Появится сообщение об успехе, подтверждающее добавление устройства.

8.3 Cisco Nexus

В этом разделе описывается как добавить устройства Cisco Nexus в Нетхаб и выполнить нужные настройки. Для подключения сетевого устройства к Нетхаб, необходимо предоставить следующий сетевой доступ:



8.3.1 Права для подключения

Для анализа устройств маршрутизатора Cisco Nexus Нетхаб требует возможности запуска следующих команд на устройстве Nexus:

- `show version`
- `show interface`
- `show ip interface`
- `show ip access-list`
- `show running-config`
- `show vdc membership` (Для Nexus 7000 и более поздних версий)

- `show vrf interface | xml`
- `show vrf all interface`
- `show ip route`
- `show ip route vrf all`
- `show vrf all`
- `show bgp vpn4 unicast labels`

Для версий Nexus 7000 и выше у Нетхаб также должны быть разрешения на просмотр всех VDC.

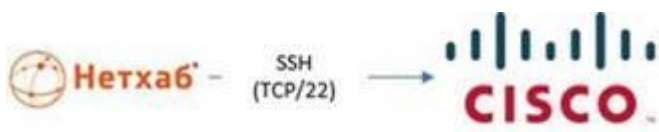
8.3.2 Добавление Cisco Nexus

Перейдите в «Администрирование» → «Настройка устройств» → «Cisco» → «Nexus Router» и заполните следующие поля:

Хост	Введите имя хоста или IP-адрес устройства.
Имя пользователя	Введите имя пользователя, которое будет использоваться для SSH-доступа к устройству.
Пароль	Введите пароль, который будет использоваться для SSH-доступа к устройству.

8.4 Добавление устройств Cisco IOS

В этом разделе описывается как добавить устройства Cisco IOS в Нетхаб и выполнить нужные настройки. Для подключения сетевого устройства к Нетхаб, необходимо предоставить следующий сетевой доступ:



8.4.1 Права для подключения

Для анализа устройств маршрутизатора Cisco IOS, Нетхаб требует возможности запуска следующих команд на устройстве IOS:

- `show version`
- `show interface`
- `show ipv4 vrf all interface`
- `show ip interface`
- `show ipv6 interface`

- `show ip access-list`
- `show ipv6 access-list`
- `show bgp summary`
- `show running-config`
- `show ip route`
- `show bgp vpn4 unicast labels`
- `show ipv4 vrf all interface brief`
- `show ip route vrf`

Примечание. Некоторые команды могут быть актуальны только на устройствах IOS-XE и IOS-XR.

Когда ActiveChange включен, Нетхабу необходимо, чтобы пользователь мог войти в привилегированный режим, используя учетные данные включения (уровень безопасности 15).

8.4.2 Добавление Cisco IOS

Перейдите в «Администрирование» → «Настройка устройств» → «Cisco» → «Маршрутизатор IOS» и заполните следующие поля:

Хост	Введите имя хоста или IP-адрес устройства.
Имя пользователя	Введите имя пользователя, которое будет использоваться для SSH-доступа к устройству.
Пароль	Введите пароль, который будет использоваться для SSH-доступа к устройству.
имя пользователя enable	Введите имя пользователя enable для использования: <ul style="list-style-type: none"> • <code>noenable</code>. Пропустить выполнение команды <code>enable</code>. • Пустое поле. Вместо команды <code>enable</code> Нетхаб аналитик выдаст команду <code>login</code>, используя тот же пароль, что и при SSH-соединении.
Пароль привилегированного пользователя	Пароль привилегированного пользователя

8.5 Добавление устройств Paloalto

В этом разделе описывается как добавить устройства PALOALTO в Нетхаб и выполнить нужные настройки.

Для подключения требуется доступ по следующим портам: TCP/22, TCP/443, UDP/514.

8.5.1 Настройка прав для подключения

Для работы Нетхаб требуется учетная запись Panorama REST API, настроенная с правами Configuration и Operational Requests (см. Рисунок 23).

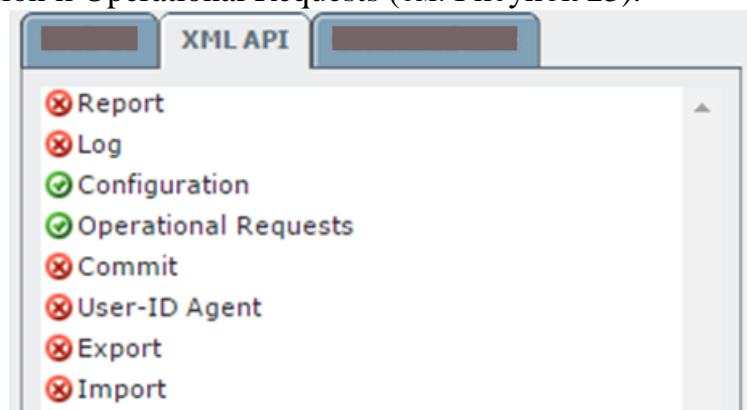


Рисунок 23 Права для REST API

Для подключения к устройствам межсетевого экрана Palo Alto системе Нетхаб требуется один из следующих типов пользователей:

- 1) Суперпользователь (только для чтения)
- 2) Администратор устройства
- 3) Device Admin (только для чтения)

8.6 Добавление устройства Check Point

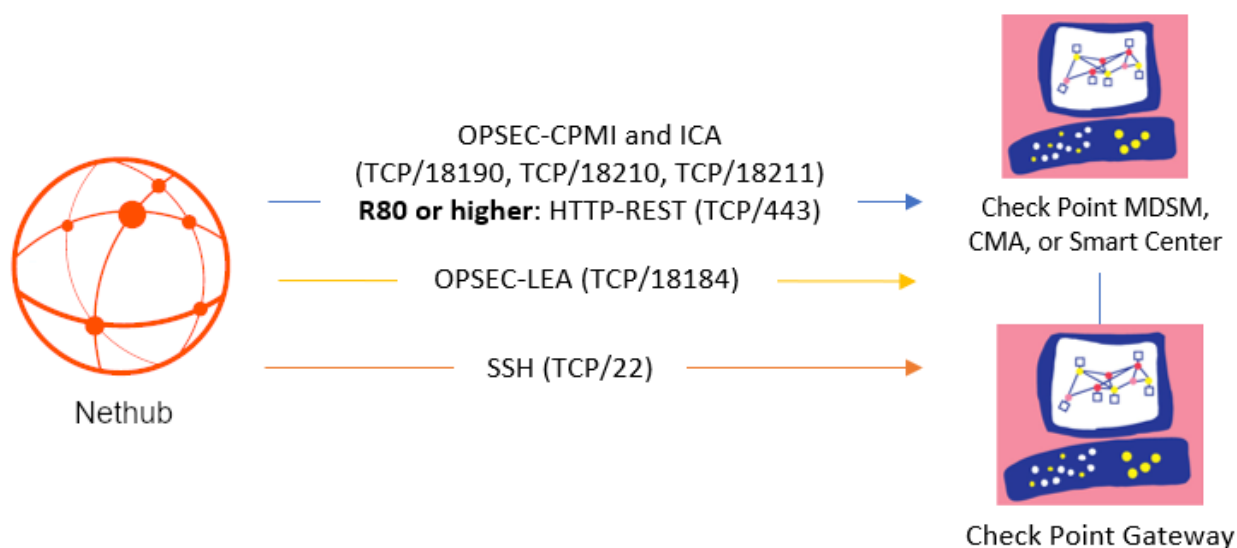
В этом разделе описывается, как добавить устройства Check Point MDSM, SmartCenter/Gateway или СМА, а также поля и параметры, общие для всех этих типов устройств.

Примечание. Вы также должны выполнять изменения в настройках своих устройств в зависимости от того, как вы подключаетесь к устройству из Nethub Analyzer. Подробнее см. в разделе [Включение сбора данных для устройств Check Point](#).

8.6.1 Сетевые подключения Check Point

На следующих схемах показано подключение Nethub к устройству Check Point MDSM, СМА или Smart Center и шлюзу Check Point. Версии Check Point R80 и выше имеют

дополнительное подключение через HTTP-REST.



Примечание. Если ваши серверы логирования CLM/MLM находятся на отдельных хостах, вам потребуется подключаться к ним отдельно.

8.6.2 Настройка прав Check Point

Nethub Analyzer может собирать данные и логи через SSH или OPSEC. Для версий Check Point R80 и выше необходимо также определить сбор данных через REST.

NETHUB требует следующие разрешения для каждого типа подключения к вашим устройствам Check Point:

Соединения через OPSEC (рекомендуется)

NETHUB необходимы минимальные права объекта CPMI и LEA OPSEC для подключения к устройствам Check Point и автоматической инициализации сбора логов через определенное соединение LEA.

В интерфейсе Check Point определите права следующим образом:

CPMI	Выберите следующие права CPMI: <ul style="list-style-type: none"> Разрешить доступ через Management Portal и SmartConsole Applications Permissions > Read Only All. Чтобы использовать ActiveChange, выберите Read/Write All.
LEA	На вкладке LEA Permissions , в Permissions to Read Logs , выбрать Show all log fields .

Примечание. Создайте отдельный объект OPSEC и профиль только для использования в NETHUB. Использование профиля администратора приводит к сбоям из-за настроек Check Point.

Дополнительные сведения см. в разделе [Создание сертификата Check Point OPSEC для устройств Check Point \(R77 и ниже\)](#).

Соединения через SSH

NETHUB должен иметь SSH-доступ к соответствующим устройствам управления и регистрации, таким как PV-1, CMA, SmartCenter, внешний лог-сервер или CLM.

- Для SecurePlatform (SPLAT) необходимо разрешить NETHUB переключаться в экспертный режим.
- Для Solaris/RHEL/IPSO, NETHUB должен подключаться от имени пользователя root

Также поддерживается аутентификация с открытым ключом. В таких случаях требуются следующие права:

Read	Nethub Analyzer требует права на чтение папок домена, таких как \$FWDIR/conf или \$FWDIR/log.
Write	Nethub Analyzer записывает пакет, содержащий необходимую конфигурацию, в каталог /tmp или /var/tmp, в зависимости от платформы устройства, например SP или Solaris. Nethub Analyzer также требует прав на запись в каталоге \$FWDIR/conf для временных файлов логов.
Execute	Nethub Analyzer запускает несколько команд на устройстве управления, включая fwm logexport для логов и cprstat для маршрутизации.

REST-подключение (только для R80 и выше)

При использовании устройства Check Point версии R80 или выше, Nethub Analyzer также собирает данные через REST, в дополнение к OPSEC или SSH.

В дополнение к правам OSPEC или SSH, Nethub должен иметь права на выполнение вызовов REST к серверу Check Point Security Management Server.

- Минимальные необходимые права Read Only All.
- Когда функция ActiveChange включена, минимальными правами являются Read\Write All.

Дополнительные сведения см. в разделе [Включение сбора данных через REST](#).

8.7 Добавление устройства Check Point Multi-Domain Security Management

Check Point Multi-Domain Security Management (MDSM) объединяет несколько сетей с "межсетевым экраном" в единую административную структуру. Эти устройства

объединяют несколько серверов SmartCenter, называемых дополнительными модулями управления клиентами (СМА), на одном хосте.

Nethub Analyzer анализирует политику безопасности модуля фильтрации через защищенное соединение с сервером MDSM.

Примечание: Multi-Domain Security Management, или MDSM, относится к устройствам MDSM и Provider-1.

Сделайте следующее:

1. Перейдите на страницу НАСТРОЙКА УСТРОЙСТВ.
2. На странице выбора вендора и устройства выберите Check Point > Multi Domain Security Management (Provider-1).

Настройте поля и параметры на странице по мере необходимости.

Дополнительные сведения см. в разделе [Поля и параметры Check Point](#).

Примечание: если вы выбрали ActiveChange, появится лицензионное соглашение ActiveChange. Установите флажок Я согласен, а затем нажмите ОК.

3. Нажмите Далее.

Поля на странице Check Point - Multi-Domain Security Management (Provider-1) - Step 2/3 отличаются в зависимости от того, выбрали ли вы подключение к устройству через SSH или OPSEC.

4. Выполните одно из следующих действий:

OPSEC	(Рекомендуется) Введите IP-адрес СМА, который управляет устройствами, которые вы хотите проанализировать.
SSH	Выберите СМА, который управляет устройствами, которые вы хотите проанализировать, щелкнув соответствующую строку.

5. Нажмите Далее.

Появится страница Check Point — Multi-Domain Security Management (Provider-1) — Step 3/3.

На этой странице отображается таблица со списком всех устройств, которыми управляет Check Point MDSM, включая автономные устройства и виртуальные системы.

6. **Необязательно:** настройте Nethub Analyzer для использования логов логирования, созданных управляемым устройством или виртуальной системой.

Совет. Это позволяет Nethub Analyzer обнаруживать определенную информацию об оптимизации политик, например неиспользуемые правила.

Сделайте следующее:

- а. В столбце «Добавить устройство» установите флажок рядом с именем устройства.
- б. В столбце «Метод сбора логов» выберите один из следующих:
 - **None.** Отключает ведение журнала логов
 - **Стандарт.** Включает ведение журнала логов
 - **Обширный.** Включает ведение журнала логов и Intelligent Policy Tuner.
- с. В столбце Сервер логирования нажмите Параметры. Затем выполните одно из следующих действий:
 - Выберите сервер логирования, который вы хотите использовать, из раскрывающегося списка.
 - Выберите «Другое» и введите имя сервера логирования вручную.

Нажмите ОК, по готовности.

- д. **Только SSH:** чтобы изменить определения SSH, выберите Изменить определения SSH.

В диалоговом окне «Настройка SSH Check Point Log Server» выполните следующие действия:

- Укажите, является ли этот сервер логирования частью многодоменного модуля логирования (MLM/CLM) или автономным сервером логирования.
- Заполните поля по мере необходимости. Дополнительные сведения см. в разделе [Поля настройки сервера логов](#).

- е. **Только для OPSEC:** чтобы проверить подключение OPSEC к определенному серверу логирования, нажмите Проверить подключение OPSEC.

Сообщение информирует вас об успешном подключении Nethub Analyzer к серверу логирования.

- ф. Нажмите ОК.

7. **Необязательно:** включите создание базовых отчетов о соответствии и/или разрешите сбор динамической маршрутизации для всех управляемых устройств.

Для этого в области «Прямой доступ к управляемым устройствам» нажмите Настроить.

Отображается диалоговое окно конфигурации прямого доступа.

Заполните необходимые поля и нажмите ОК. Дополнительные сведения см. в разделе [Поля соответствия базовой конфигурации](#).

Примечание. Указание этой информации для устройства запускает прямое SSH-подключение к устройству.

8. При необходимости заполните оставшиеся поля. Дополнительные сведения см. в разделе [Дополнительные параметры Check Point](#).
9. Нажмите **Finish**.

Новое устройство добавлено в дерево устройств.

8.7.1 Установить права пользователя

Если вы выбрали «Установить права пользователя», появится диалоговое окно «Редактировать пользователей».

В отображаемом списке пользователей выберите одного или нескольких пользователей, чтобы предоставить доступ к отчетам для этой учетной записи. Чтобы выбрать нескольких пользователей, нажмите кнопку CTRL во время выбора.

Нажмите ОК, чтобы закрыть диалоговое окно.

8.8 Добавление SmartCenter/шлюз Check Point

Продукты Check Point основаны на распределенной архитектуре, где типичное развертывание Check Point состоит из модуля или устройства фильтрации и сервера SmartCenter.

- **Автономное развертывание** — это самое простое развертывание, при котором сервер SmartCenter и модуль фильтра устанавливаются на одном сервере.
- **Распределенное развертывание** — это более сложное развертывание, при котором модуль фильтра и сервер SmartCenter развернуты на разных серверах.

Nethub Analyzer обеспечивает анализ политики безопасности модуля фильтрации через безопасное соединение с сервером SmartCenter.

Сделайте следующее:

1. Откройте страницу НАСТРОЙКА УСТРОЙСТВ.
2. На странице выбора вендора и устройства выберите **Check Point > Security Management (SmartCenter)**.

Настройте поля и параметры на странице по мере необходимости.

Дополнительные сведения см. в разделе [Поля и параметры Check Point](#).

Примечание. Если вы решите включить ActiveChange, появится лицензионное соглашение ActiveChange. Установите флажок «Я согласен» и нажмите «ОК».

3. Нажмите **Далее**.

Откроется страница Check Point — Управление безопасностью (SmartCenter) — Шаг 2/2, отображающая таблицу со списком всех устройств, которыми управляет Check Point SmartCenter/Gateway, включая автономные устройства и виртуальные системы.

1. **Необязательно:** настройте Nethub Analyzer для использования логов, созданных управляемым устройством или виртуальной системой.

Совет. Это позволяет Nethub Analyzer обнаруживать определенную информацию об оптимизации политик, например неиспользуемые правила.

Сделайте следующее:

- а. В столбце «Добавить устройство» установите флажок рядом с именем устройства.
- б. В столбце «Метод сбора логов» выберите один из следующих:
 - **None.** Отключает ведение журнала логов
 - **Стандарт.** Включает ведение журнала логов
 - **Обширный.** Включает ведение журнала логов и Intelligent Policy Tuner.
- с. В столбце Сервер логирования нажмите «Параметры». Затем выполните одно из следующих действий:
 - Выберите сервер логирования, который вы хотите использовать, из раскрывающегося списка.
 - Выберите «Другое» и введите имя сервера логирования вручную.

Нажмите ОК, по готовности.

- д. **Только SSH:** чтобы изменить определения SSH, выберите «Изменить определения SSH».

В диалоговом окне «Настройка SSH Check Point Log Server» выполните следующие действия:

- Укажите, является ли этот сервер логирования частью многодоменного модуля логирования (MLM/CLM) или автономным сервером логирования.
- Заполните поля по мере необходимости. Дополнительные сведения см. в разделе [Поля настройки сервера логов](#).

- е. **Только для OPSEC:** чтобы проверить подключение OPSEC к определенному серверу логирования, нажмите «Проверить подключение OPSEC».

Сообщение информирует вас об успешном подключении Nethub Analyzer к серверу логирования.

- а. Нажмите ОК.

8. **Необязательно:** включите создание базовых отчетов о соответствии и/или разрешите сбор динамической маршрутизации для всех управляемых устройств.

Для этого в области «Прямой доступ к управляемым устройствам» нажмите Настроить.

Отображается диалоговое окно конфигурации прямого доступа.

Заполните необходимые поля и нажмите ОК. Дополнительные сведения см. в разделе [Поля соответствия базовой конфигурации](#).

Примечание. Указание этой информации для устройства запускает прямое SSH-подключение к устройству.

6. Заполните остальные поля, используя информацию в полях параметров Check Point (см. [Дополнительные параметры Check Point](#)).

7. Добавьте устройство.

Новое устройство добавлено в дерево устройств.

8.8.1 Установить права для пользователя Нетхаб

Если вы выбрали «Установить права пользователя», появится диалоговое окно «Редактировать пользователей».

В отображаемом списке пользователей выберите одного или нескольких пользователей, чтобы предоставить доступ к отчетам для этой учетной записи. Чтобы выбрать нескольких пользователей, нажмите кнопку CTRL во время выбора.

Нажмите ОК, чтобы закрыть диалоговое окно.

8.9 Добавление CMA Check Point

Вы можете добавить отдельные надстройки управления клиентами (CMA), используя описанную ниже процедуру.

Совет: добавьте сразу несколько CMA, добавив Check Point MDSM.

Сделайте следующее:

1. Откройте страницу НАСТРОЙКИ УСТРОЙСТВ.
2. На странице выбора производителя и устройства выберите **Check Point > Single CMA**.

Примечание. Если вы решите включить ActiveChange, появится лицензионное соглашение ActiveChange. Установите флажок «Я согласен» и нажмите «ОК».

3. Нажмите **Next**.

Откроется страница Check Point — Single CMA — Step 2/2, в которой отображается таблица, в которой перечислены все устройства, которыми управляет Check Point CMA, включая автономные устройства и виртуальные системы.

2. **Необязательно:** настройте Nethub Analyzer для использования логов, созданных управляемым устройством или виртуальной системой.

Совет. Это позволяет Nethub Analyzer обнаруживать определенную информацию об оптимизации политик, например неиспользуемые правила.

Сделайте следующее:

- а. В столбце Добавить устройство установите флажок рядом с именем устройства.
- б. В столбце Анализ логов выберите один из следующих:

- **None.** Отключает ведение журнала логов
- **Стандарт.** Включает ведение журнала логов
- **Обширный.** Включает ведение журнала логов и Intelligent Policy Tuner.

с. В столбце Сервер логирования нажмите Параметры. Затем выполните одно из следующих действий:

- Выберите сервер логирования, который вы хотите использовать, из раскрывающегося списка.
- Выберите Другое и введите имя сервера логирования вручную.

Нажмите ОК, по готовности.

d. **Только SSH:** чтобы изменить определения SSH, выберите Изменить определения SSH.

В диалоговом окне «Настройка SSH Check Point Log Server» выполните следующие действия:

- Укажите, является ли этот сервер логирования частью многодоменного модуля логирования (MLM/CLM) или автономным сервером логирования.
- Заполните поля по мере необходимости. Дополнительные сведения см. в разделе [Поля настройки сервера логов](#).

e. **Только для OPSEC:** чтобы проверить подключение OPSEC к определенному серверу логирования, нажмите «Проверить подключение OPSEC».

Сообщение информирует вас об успешном подключении Nethub Analyzer к серверу логирования.

a. Нажмите ОК.

9. **Необязательно:** включите создание базовых отчетов о соответствии и/или разрешите сбор динамической маршрутизации для всех управляемых устройств.

Для этого в области Прямой доступ к управляемым устройствам нажмите Настроить.

Отображается диалоговое окно конфигурации прямого доступа.

Заполните необходимые поля и нажмите ОК. Дополнительные сведения см. в разделе [Поля соответствия базовой конфигурации](#).

Примечание. Указание этой информации для устройства запускает прямое SSH-подключение к устройству.

6. Заполните оставшиеся поля, используя информацию в полях параметров Check Point (см. [Дополнительные параметры Check Point](#)).

7. Нажмите Готово. Новое устройство добавлено в дерево устройств.

8. Если вы выбрали «Установить права пользователя», появится диалоговое окно «Редактировать пользователей».

В отображаемом списке пользователей выберите одного или нескольких пользователей, чтобы предоставить доступ к отчетам для этой учетной записи.

Чтобы выбрать нескольких пользователей, нажмите кнопку CTRL во время выбора.

Нажмите ОК, чтобы закрыть диалоговое окно.

Появится сообщение об успешном завершении, подтверждающее добавление устройства.

8.9.1 Поля и параметры Check Point

Устройства Check Point включают следующие типы полей и опций:

8.9.1.1 Информация для доступа

Хост	Введите имя хоста или IP-адрес устройства.
R80 или выше	Выберите эту опцию для устройств версии R80 или выше. Для устройств R80 необходимо настроить параметры API управления устройством для приема вызовов API с IP-адреса сервера Nethub. Дополнительные сведения см. в разделе Включение сбора данных через REST .
Подключиться через	<p>Укажите, как Nethub Analyzer должен подключаться к устройству, выбрав один из следующих вариантов.:</p> <ul style="list-style-type: none"> • SSH: Подключиться через SSH (протокол Secure Shell). Этот параметр недоступен при добавлении одного CMA Check Point. • OPSEC (NGX R60 или выше): Подключиться через OPSEC. (Рекомендуется) <p>Чтобы указать пользовательский порт, выберите «Пользовательский порт» и введите номер порта.</p> <p>Примечание. Для сред Windows поддерживается только OPSEC.</p>
Имя пользователя \ Пароль	<p>Введите имя пользователя и пароль для доступа к устройству.</p> <p>Эти поля появляются только в том случае, если вы выбрали R80 или выше или выбрали SSH в области Подключить через.</p>

Безопасная платформа	<p>Выберите этот параметр, чтобы указать, что на устройстве установлена операционная система Check Point SecurePlatform.</p> <p>Необходимо заполнить поле «Пароль эксперта».</p> <p>Это поле появляется только в том случае, если вы выбрали SSH в области Подключаться через.</p>
Экспертный пароль	<p>Введите экспертный пароль, который открывает доступ ко всем функциям на сервере SmartCenter, необходимым для этого процесса.</p> <p>Это поле появляется только в том случае, если вы выбрали SSH в области Подключиться через.</p>
Solaris / RedHat Linux	<p>Выберите этот параметр, чтобы указать, что на устройстве установлена операционная система Solaris или RedHat Linux.</p> <p>Это поле появляется только в том случае, если вы выбрали SSH в области Подключиться через.</p>
Учетные данные пользователя выше предназначены для пользователя root	<p>Выберите этот параметр, чтобы указать, что имя пользователя и пароль, введенные в полях Имя пользователя и Пароль, являются учетными данными для пользователя root Solaris.</p> <p>Если вы снимите этот флажок, вы должны будете заполнить поле Root пароль.</p> <p>Это поле появляется только в том случае, если вы выбрали SSH в области Подключиться через.</p>
Root пароль	<p>Введите пароль root для Solaris.</p> <p>Это поле появляется только в том случае, если вы выбрали SSH в области Подключаться через.</p>
Высокая доступность	<p>Выберите этот параметр, чтобы настроить высокую доступность для СМА.</p> <p>Важно: Nethub Analyzer подключается к кластеру высокой доступности, используя активный IP-адрес, а не виртуальный IP-адрес. Вы должны настроить правила доступа для каждого устройства в кластере, чтобы разрешить этот трафик.</p> <p>Это поле появляется, только если вы выбрали OPSEC в области Подключиться через. Это не относится к Check Point MDSM.</p>

Вторичное управление безопасностью (SmartCenter)	Введите вторичный СМА. Это поле появляется, только если вы выбрали OPSEC в области Connect via. Это не относится к Check Point MDSM.
---	---

8.9.1.2 Сбор логов

Выберите используемый метод сбора логов.

Если вы выберете SSH, вы должны включить Nethub Analyzer для анализа логирования трафика управления приложениями. Дополнительные сведения см. в разделе [Включение сбора данных через SSH](#). Если вы не выполните этот шаг, информация, связанная с трафиком управления приложениями, не будет отображаться на странице Оптимизация политики отчета об устройстве.

Эта область появляется только в том случае, если вы выбрали OPSEC в области «Подключение через».

8.9.1.3 Настройка OPSEC

В этой области можно указать, какой сертификат использовать для доступа OPSEC к устройству.

Дополнительные сведения см. в разделе [Включение сбора данных через OPSEC](#).

Эта область появляется только в том случае, если вы выбрали OPSEC в области «Подключение через».

8.9.1.4 ActiveChange

Эта область появляется, только если вы выбрали OPSEC в области Connect via.

Выберите «Включить ActiveChange», чтобы включить возможность автоматического внесения изменений для устройства.

Примечание. Этот параметр недоступен для версии R80 и выше.

8.9.1.5 Поля сервера логгирования

Поля сервера логгирования Check Point включают следующее:

Хост (МЛМ)	Введите имя хоста или IP-адрес сервера логгирования.
Имя пользователя	Введите имя пользователя, которое будет использоваться для SSH-доступа к серверу логгирования.
Пароль	Введите пароль, который будет использоваться для доступа SSH к серверу логгирования.

Безопасная платформа	<p>Выберите этот параметр, чтобы указать, что сервер логирования установлен в операционной системе Check Point SecurePlatform.</p> <p>Необходимо заполнить поле «Пароль эксперта».</p>
Экспертный пароль	<p>Введите экспертный пароль, который открывает доступ ко всем функциям на сервере логирования, необходимым для этого процесса.</p>
Solaris	<p>Выберите этот параметр, чтобы указать, что сервер логирования установлен в операционной системе Solaris.</p>
Учетные данные пользователя выше предназначены для пользователя root	<p>Выберите этот параметр, чтобы указать, что имя пользователя и пароль, введенные в поля Имя пользователя и Пароль, являются учетными данными для пользователя root Solaris.</p> <p>Если вы снимите этот флажок, вы должны будете заполнить поле Root Password.</p>
Root пароль	<p>Если вы используете пользователя, отличного от «root», для доступа к ОС Solaris, введите пароль root для Solaris.</p>
Проверить подключение	<p>Нажмите эту кнопку, чтобы проверить подключение к определенному серверу логирования.</p> <p>Сообщение информирует вас об успешном подключении Nethub Analyzer к серверу логирования.</p>

8.9.1.6 Поля соответствия базовой конфигурации

Поля соответствия базовой конфигурации Check Point включают следующее:

IP хоста	Введите IP-адрес устройства.
Имя пользователя	Введите имя пользователя для доступа к устройству.
Пароль	Введите пароль для доступа к устройству.
Платформа	Выберите платформу устройства.

	Это поле появляется только для устройств Check Point.
Дополнительный пароль	Введите пароль, который будет использоваться для выполнения команд ОС на устройстве. Это поле появляется только для устройств Check Point.
Базовый профиль	Выберите базовый профиль соответствия для использования для устройства. Раскрывающийся список включает все базовые профили соответствия в системе. Чтобы отключить создание базового отчета о соответствии для этого устройства, выберите «Нет».
Проверить подключение	Нажмите эту кнопку, чтобы проверить подключение к определенному устройству. Сообщение информирует вас об успешном подключении Nethub Analyzer к устройству.

8.9.1.7 Дополнительные параметры Check Point

Устройства Check Point имеют следующие дополнительные опции:

Мониторинг изменений в режиме реального времени	Выберите, чтобы включить оповещение в режиме реального времени при изменении конфигурации.
Установить права пользователя	Выберите, чтобы установить разрешения пользователя для этого устройства
Сбор журналов аудита из CLM	Выберите для сбора логов аудита из CLM. Примечание. Если этот параметр включен, все модули должны быть настроены на сбор логов из одного и того же CLM.
Частота сбора логов	Введите интервал времени в минутах, через который Nethub Analyzer должен собирать логи для устройства Check Point.

8.9.2 Включить сбор данных для устройств Check Point

Чтобы Nethub Analyzer мог собирать данные с устройства Check Point, необходимо настроить определенные параметры на самом устройстве. Nethub Analyzer собирает

данные с устройств Check Point, используя либо SSH, либо OPSEC, а для версий Check Point R80 и выше Nethub Analyzer собирает данные через REST (наряду с SSH или OPSEC).

Примечание. В дополнение к перечисленным ниже требованиям убедитесь, что пользователь, которого Nethub Analyzer использует для доступа к устройству, имеет необходимые разрешения. Минимальное разрешение, необходимое для чтения только для всех. Когда устройство использует ActiveChange, минимальное разрешение — «Чтение и запись всего». Дополнительные сведения см. в разделе Требуемые разрешения устройства.

Дополнительные сведения см. в разделе [Добавление устройств Check Point](#).

В этой теме:

- [Включить сбор данных через SSH](#).
- [Включить сбор данных через OPSEC](#)
- [Включить сбор данных через REST](#).

8.9.2.1 Включить сбор данных через SSH

Эта процедура описывает, как настроить Nethub Analyzer для обработки логов трафика Check Point.

Nethub Analyzer можно настроить для сбора логов с устройства Check Point через SSH, но на устройстве Check Point требуется специальная настройка. Логирование трафика управления приложениями включают поле `app_rule_id`, и это поле по умолчанию маскируется для пользователя сбора логов SSH, указанного при добавлении устройства в Nethub Analyzer. В результате Nethub Analyzer не может обрабатывать логи, собранные через SSH, а также использовать их для создания информации для области очистки правил управления приложениями на странице «Оптимизация политики» отчета об устройстве.

Чтобы позволить Nethub Analyzer обрабатывать логи трафика управления приложениями, вы должны изменить права для поля `app_rule_id` на устройстве Check Point, как описано в следующей процедуре.

Примечание. Для R80 и выше Nethub Analyzer собирает данные через REST (наряду с SSH или OPSEC). Дополнительные сведения см. в разделе [Включение сбора данных через REST](#).

Сделайте следующее:

1. Запустите GuiDBedit.exe и подключитесь к станции управления устройством Check Point.

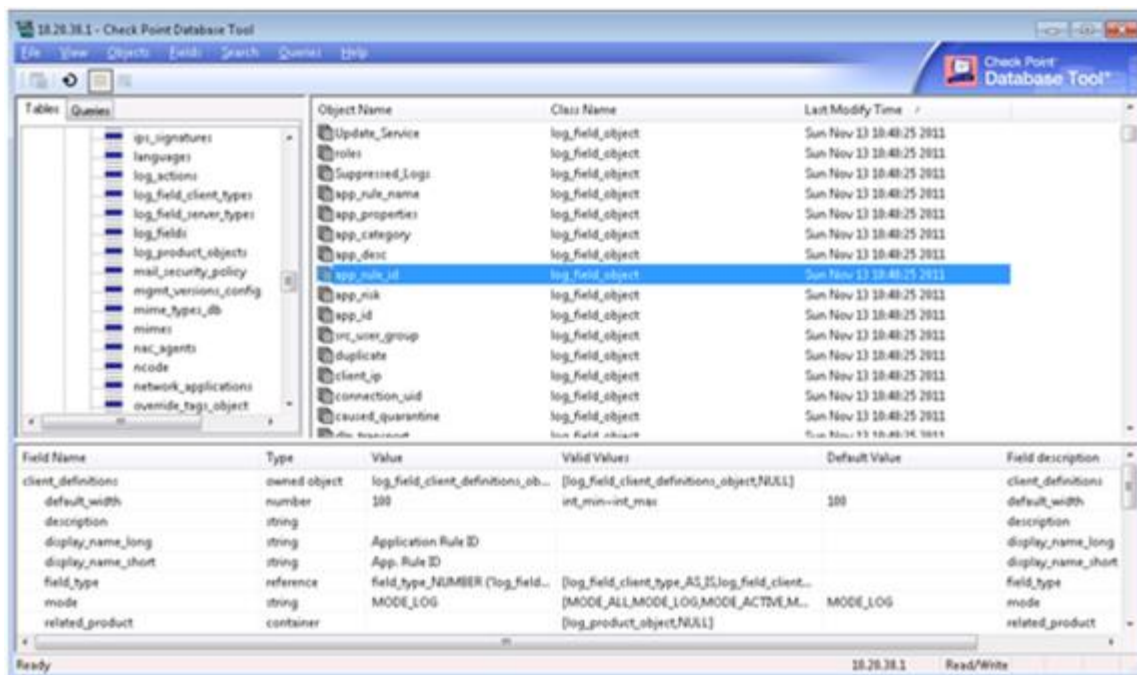
Станция управления обычно находится в папке `C:\Program Files (x86)\CheckPoint\SmartConsole\RXX\PROGRAM`.

где RXX — номер версии.

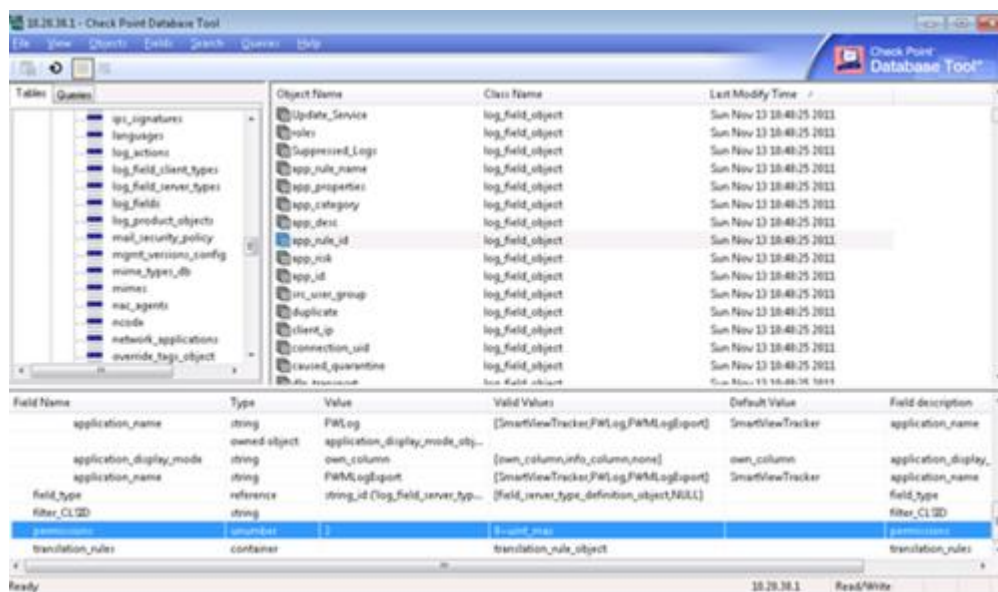
2. На левой панели перейдите к **Other > log_fields**.

3. На правой панели нажмите **app_rule_id**.

На нижней панели отображаются поля, отображаемые для **app_rule_id**.



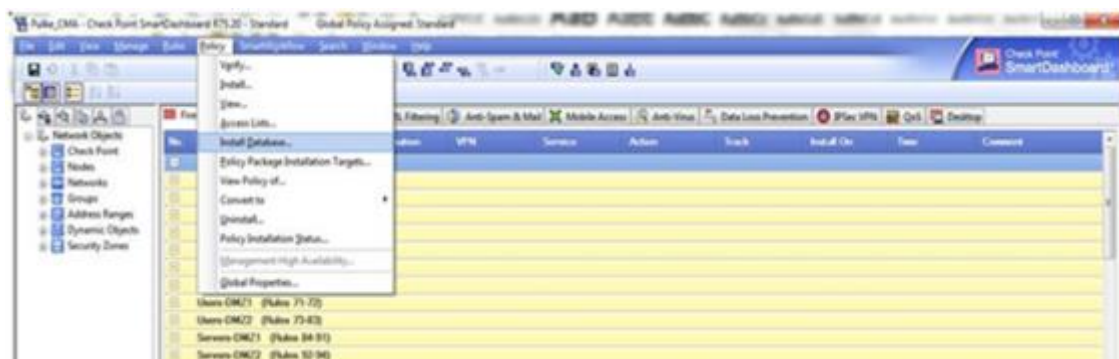
4. В нижней панели дважды нажмите поле **permissions**.



Отображается диалоговое окно редактирования.



5. В поле Value измените значение с 2 на 0.
6. Нажмите OK.
7. Сохраните изменения и выйдите из программы.
8. Если устройство отправляет логи трафика на сервер логгирования, отличный от сервера Nethub (например, CLM или внешний сервер логов), выполните следующие действия:
 - a. Подключитесь к станции управления устройством Check Point через SmartDashboard.
 - b. Переустановите базу данных Check Point на сервере логов, выбрав «Политика», а затем «Install Database» в главном меню.



- c. Выйти из программы.

8.9.2.2 Включить сбор данных через OPSEC

Эта процедура описывает, как указать сертификат доступа OPSEC к устройству Check Point, что необходимо выполнить в Check Point — Multi-Domain Security Management (Provider-1) — Step 1/3 или Check Point — SmartCenter или CMA — Step 1/2 страницы после выбора OPSEC в качестве метода подключения.

Сделайте следующее:

1. Создайте сертификат для вашего устройства. Подробнее см.:
 - [Создание сертификата Check Point OPSEC для MDSM \(R80 и выше\)](#)

- [Создание сертификата Check Point OPSEC для СМА/СМС \(R80 и выше\)](#)
- [Создание сертификата Check Point OPSEC для устройств Check Point \(R77 и ниже\)](#)

2. В Nethub Analyzer в области Настройка OPSEC нажмите Сертификат.

Отобразится диалоговое окно Retrieve a new OPSEC certificate (Получить новый сертификат OPSEC).

Получение нового сертификата OPSEC

После того, как сертификат будет готов, заполните следующее и нажмите «ОК»:

Имя приложения OPSEC:

Одноразовый пароль:

❗ Как создать сертификат Check Point OPSEC?

▼ Дополнительно

CPMI Тип авторизации:

CPMI Порт:

LEA Тип авторизации:

LEA Порт:

3. Заполните поля следующим образом:

Имя приложения OPSEC	Введите имя приложения OPSEC, указанное в сертификате OPSEC. Значение по умолчанию - "Nethub".
Одноразовый пароль	Введите одноразовый пароль, указанный в сертификате OPSEC.
Дополнительно	Нажмите для отображения расширенных полей. Появятся поля CPMI Authorization Type, CPMI Port, LEA Authorization Type и LEA Port.

Тип авторизации CPMI	Выберите тип авторизации CPMI.
CPMI Порт	Введите номер порта CPMI. Значение по умолчанию - 18190.
Тип авторизации LEA	Выберите тип авторизации LEA.
Порт LEA	Введите номер порта LEA. Значение по умолчанию - 18184.

4. Нажмите **ОК**, чтобы получить сертификат с сервера Check Point SmartCenter, СМА или MDSM.

После установки сертификата появится окно подтверждения.

5. Нажмите **ОК**.

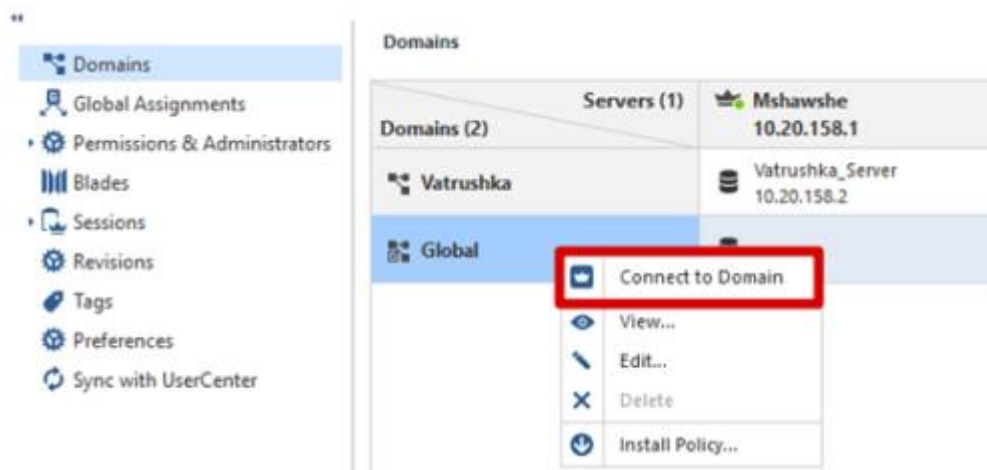
В области Setup OPSEC отображается дата и время создания сертификата.

8.9.2.2.1 Создание сертификата Check Point OPSEC для MDSM (R80 и выше)

Чтобы Nethub Analyzer мог собирать данные с Check Point MDSM через OPSEC, необходимо создать глобальный сертификат для целей аутентификации и безопасности. Сертификат создается с помощью программы Check Point SmartConsole для PV-1.

Сделайте следующее:

1. Подключитесь к SmartConsole, выбрав домен MDS.
2. Щелкните правой кнопкой мыши на **Global** и выберите **Connect to Domain**.

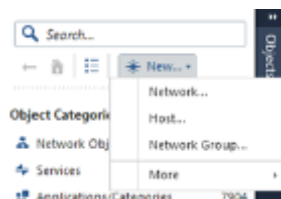


3. Создайте сетевой объект для хоста, на котором запущен Nethub Analyzer

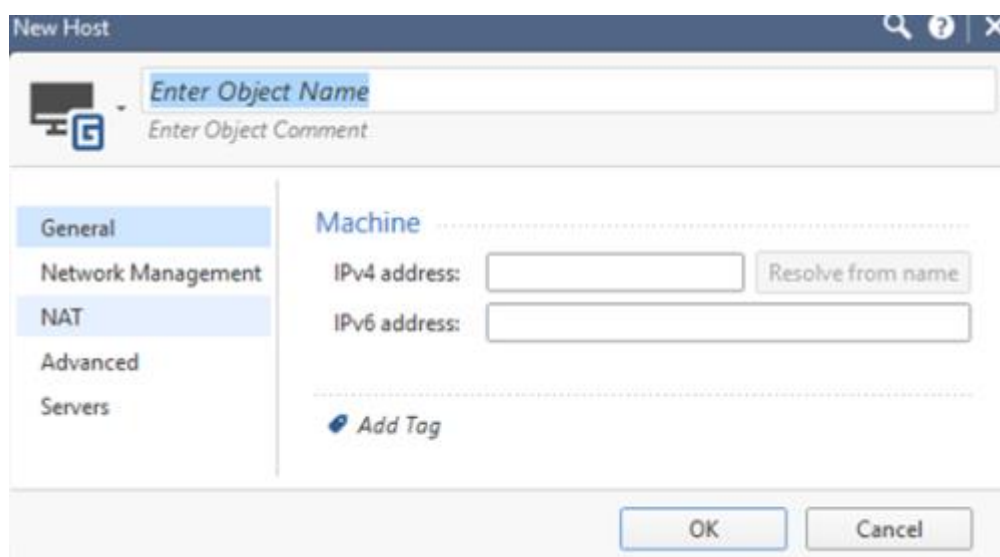
Примечание: Если сетевой объект для хоста уже определен, вы можете пропустить этот шаг.

Сделайте следующее:

- а. Нажмите **New**, а затем **Host**.



Появится окно **New Host**.



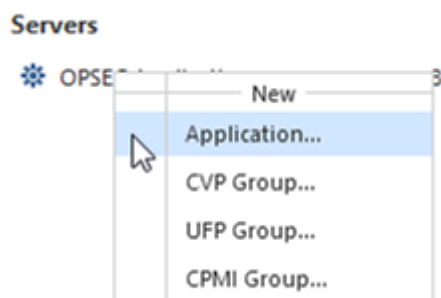
- б. Заполните поля **Object Name** и **IPv4 Address** именем и адресом узла, на котором запущен Nethub Analyzer.
- с. Нажмите **OK**.

4. Создать объект приложения OPSEC для этого сетевого объекта.

Примечание: если объект приложения OPSEC уже определен, вы можете пропустить этот шаг.

Сделайте следующее:

- а. В **Object Categories**, во вкладке **Servers**, выберите **OPSEC Applications > Application**.



Отобразится диалоговое окно **OPSEC Application Properties**.



- b. В диалоговом окне **OPSEC Application Properties** определите следующее:

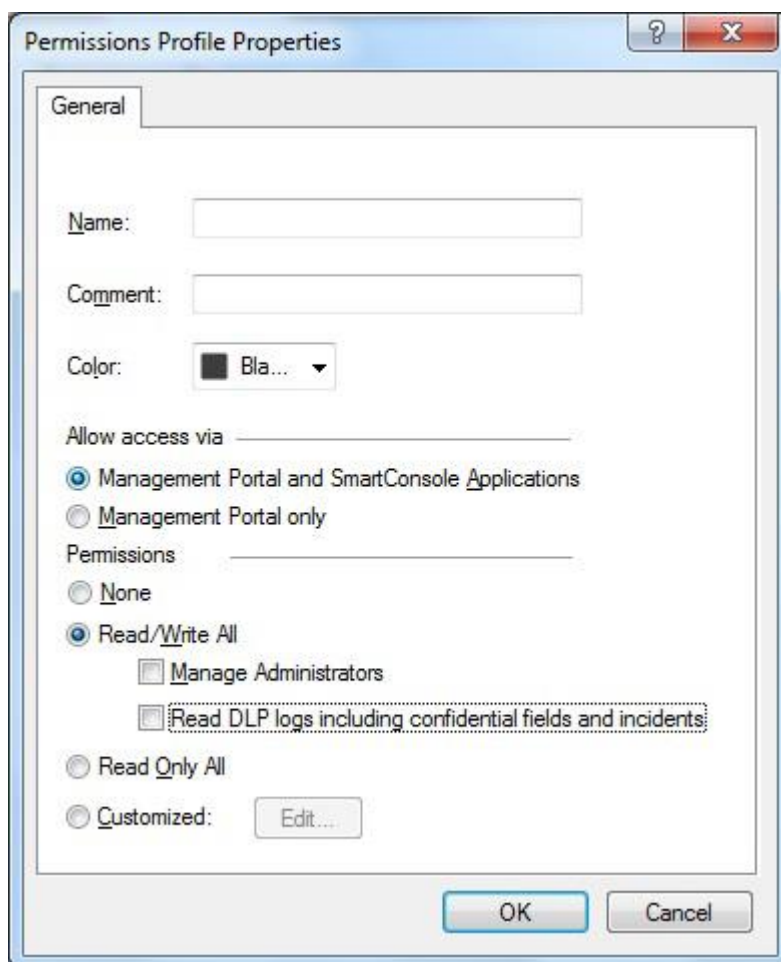
Name	Введите имя приложения OPSEC. Примечание: Запишите введенное вами имя. Вам нужно будет указать это имя в Nethub Analyzer при получении сертификата.
Host	Выберите хост Nethub Analyzer.
Object Entities	Выберите элементы LEA и CPMI.

Появятся вкладки Разрешения LEA и Разрешения CPMI.

- c. На вкладке **CPMI Permissions**, выберите **Permissions Profile**, а затем выполните одно из следующих действий:
- Выберите суперпрофиль в списке или любой другой профиль с необходимыми минимальными правами.
 - Создайте новый профиль разрешений. Для этого нажмите кнопку New (Новый). В диалоговом окне **Permissions Profile Properties** введите имя для нового профиля и выберите необходимые права.

Минимальные права, необходимые для доступа, - Read Only All. Если вы используете ActiveChange, должен быть предоставлен доступ Read/Write All.

Например:



- d. На вкладке **LEA Permissions**, выберите **According to Permissions Profile**, а затем выполните одно из следующих действий:
- Выберите суперпрофиль в списке или любой другой профиль с необходимыми минимальными правами.
 - Создайте новый профиль разрешений. Для этого нажмите кнопку **New (Новый)**. В диалоговом окне **Permissions Profile Properties** введите имя для нового профиля и выберите необходимые права.

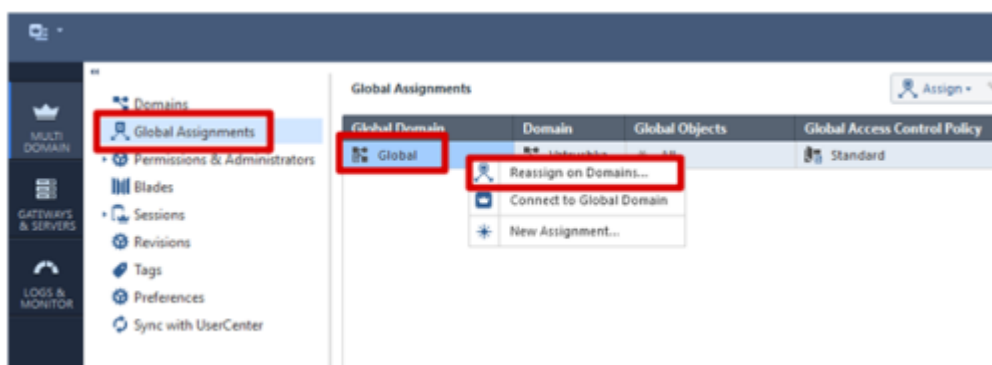
Минимальные необходимые права: **Read Only All**.

- e. Нажмите **OK**. Снова появляется вкладка "General" с дополнительными опциями.
5. Создайте свой сертификат. Сделайте следующее:
- a. Нажмите **Communication**.
 - b. В появившемся диалоговом окне **Communication** введите одноразовый пароль, а затем введите его еще раз для подтверждения.
- Примечание:** Запишите здесь введенный вами пароль. Вам нужно будет указать это имя в **Nethub Analyzer** при получении сертификата.
- c. Нажмите **Initialize**.

Состояние доверия изменится с Uninitialized на Initialized, но доверие не будет установлено. После того, как сертификат будет получен Nethub Analyzer, состояние доверия изменится на Доверенный.

Совет: При необходимости создайте новый сертификат, нажав кнопку Сброс и повторив этот шаг.

6. В верхней части экрана нажмите **Publish**.
7. Подключитесь к консоли MDS (PV-1) и выберите **Global Assignments**.
8. Щелкните правой кнопкой мыши Global и выберите Reassign on Domains (Переназначить на домены).



8.9.2.2.2 Создание сертификата Check Point OPSEC для CMA/SMC (R80 и выше)

Для того чтобы NETHUB ANALYZER мог собирать данные с Check Point CMA или SMC через OPSEC, необходимо создать локальный сертификат для аутентификации и обеспечения безопасности. Сертификат создается с помощью программы Check Point SmartConsole для CMA/SMC.

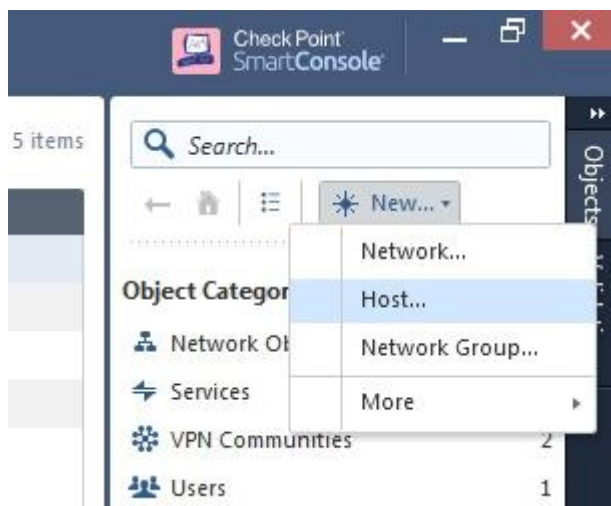
Сделайте следующее:

1. Подключитесь к консоли SmartConsole.
2. Создайте сетевой объект для хоста, на котором запущен Nethub Analyzer.

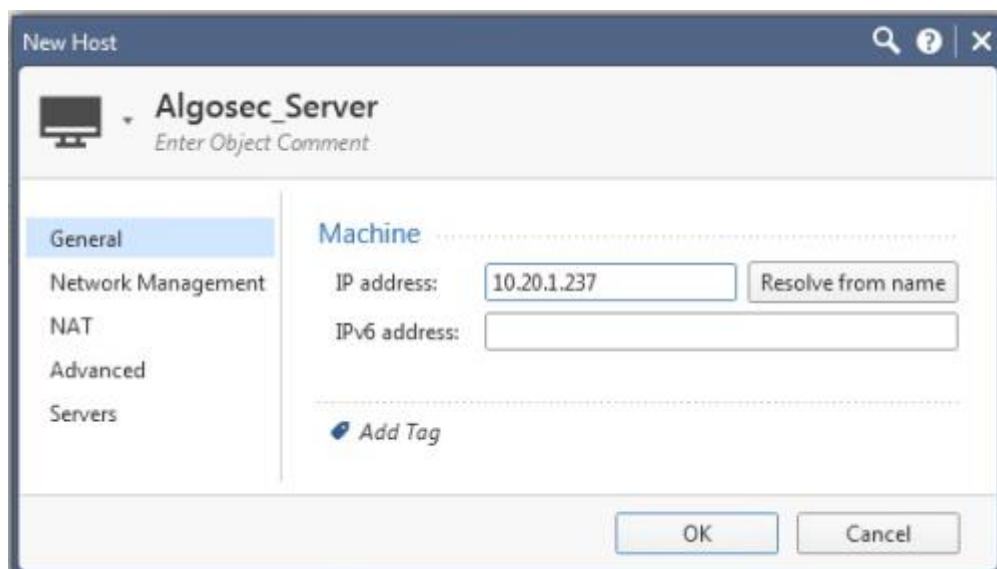
Примечание: Если сетевой объект для хоста уже определен, вы можете пропустить этот шаг.

Сделайте следующее:

- а. В правой панели нажмите кнопку New и выберите Host.




- б. В диалоговом окне «New host» введите имя и IP-адрес хоста, на котором будет запущен Nethub Analyzer, и нажмите ОК.

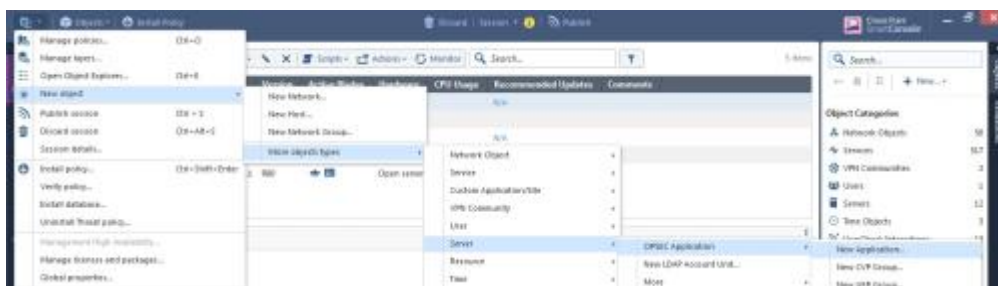


3. Создайте объект приложения OPSEC для этого сетевого объекта.

Примечание: Если объект приложения OPSEC уже определен, вы можете пропустить этот шаг.

Сделайте следующее:

- а. Нажмите  в верхней левой части экрана и выберите:
New object > More object types > Server > OPSEC Application > New Application.



б. В диалоговом окне **OPSEC Application Properties** определите следующее:

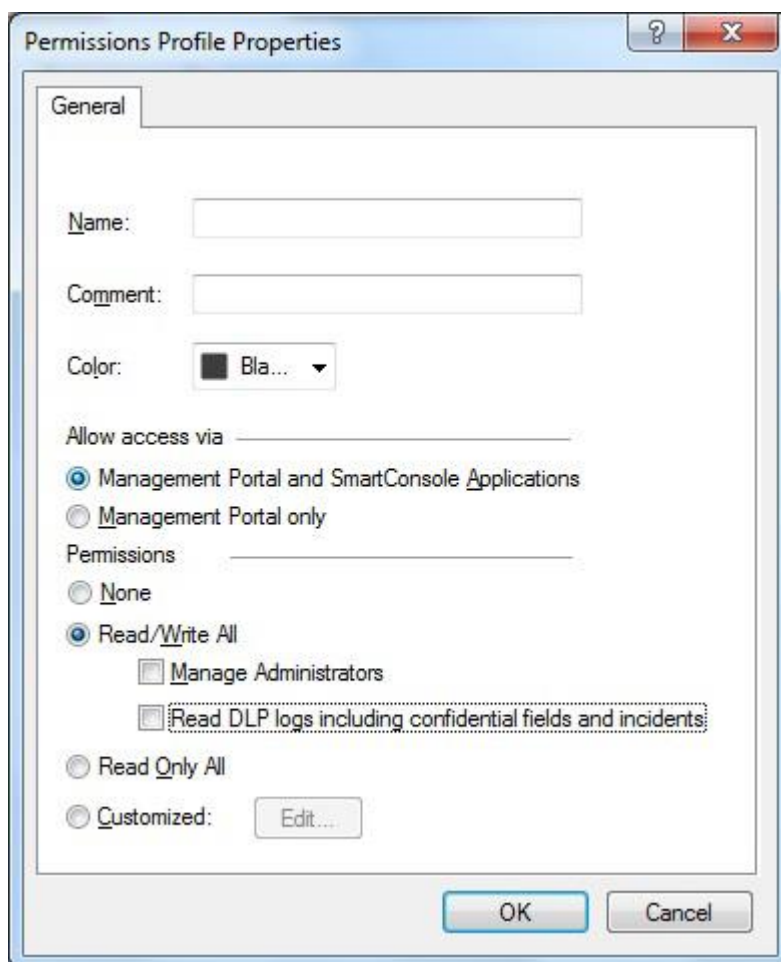
Name	Введите имя приложения OPSEC. Примечание: Запишите здесь введенное вами имя. Вам нужно будет указать это имя в Nethub Analyzer при получении сертификата.
Host	Выберите хост Nethub Analyzer.
Object Entities	Выберите элементы LEA и CPMI.

с. На вкладке **CPMI Permissions**, выберите **Permissions Profile**, а затем выполните одно из следующих действий:

- Выберите суперпрофиль в списке или любой другой профиль с необходимыми минимальными правами.
- Создайте новый профиль разрешений. Для этого нажмите кнопку New (Новый). В диалоговом окне **Permissions Profile Properties** введите имя для нового профиля и выберите необходимые права.

Минимальные права, необходимые для доступа, - Read Only All. Если вы используете ActiveChange, должен быть предоставлен доступ Read/Write All.

Например:



d. На вкладке Permissions LEA выберите **According to Permissions Profile**, а затем выполните одно из следующих действий:

- Выберите суперпрофиль в списке или любой другой профиль с необходимыми минимальными правами.
- Создайте новый профиль разрешений. Для этого нажмите кнопку New (Новый). В диалоговом окне **Permissions Profile Properties** введите имя нового профиля и выберите необходимые права.

Требуются следующие минимальные права **Read Only All**.

e. Нажмите OK. Снова появляется вкладка "Global" с дополнительными опциями.

4. Создайте свой сертификат. Сделайте следующее:

- a. Нажмите **Communication**.
- b. В появившемся диалоговом окне Communication введите одноразовый пароль, а затем введите его еще раз для подтверждения.

Примечание: Запишите здесь введенный вами пароль. Вам нужно будет указать это имя в Nethub Analyzer при получении сертификата.

c. Нажмите **Initialize**.

Состояние доверия изменится с Uninitialized на Initialized, но доверие не будет установлено. После того, как сертификат будет получен Nethub Analyzer, состояние доверия изменится на Доверенный.

Совет: При необходимости создайте новый сертификат, нажав кнопку Сброс и повторив этот шаг.

5. Переустановите базу данных Check Point на всех существующих серверах логов, включая CLM или внешние серверы логов.

Сделайте следующее:

- a. В верхней части экрана нажмите **Publish**.
- b. В левом верхнем углу нажмите  и выберите **Install database**.
- c. В диалоговом окне **Install database** данных убедитесь, что выбран ваш СМА, и нажмите Установить.

8.9.2.2.3 Создание сертификата Check Point OPSEC для устройств Check Point (R77 и ниже)

Чтобы собрать политику и таблицу маршрутизации с модуля Check Point FireWall-1, Nethub Analyzer может использовать OPSEC API. Для того чтобы это произошло, необходимо создать сертификат для аутентификации и обеспечения безопасности.

Сертификат создается на сервере SmartCenter с помощью утилиты Check Point SmartDashboard или на сервере MDSM с помощью утилиты Check Point Global SmartDashboard.

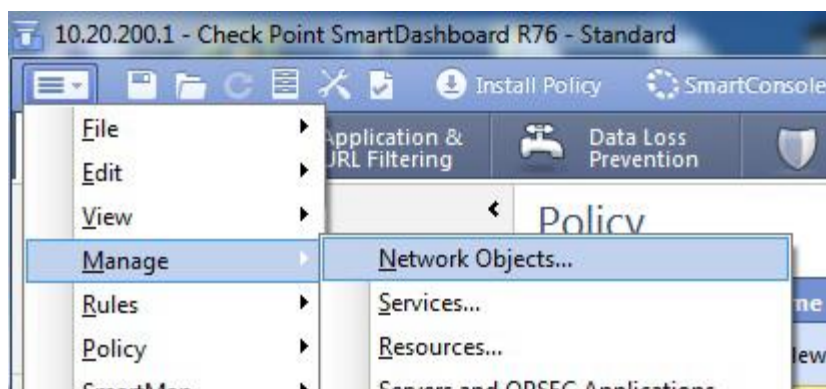
Сделайте следующее:

1. Создайте сетевой объект для хоста.

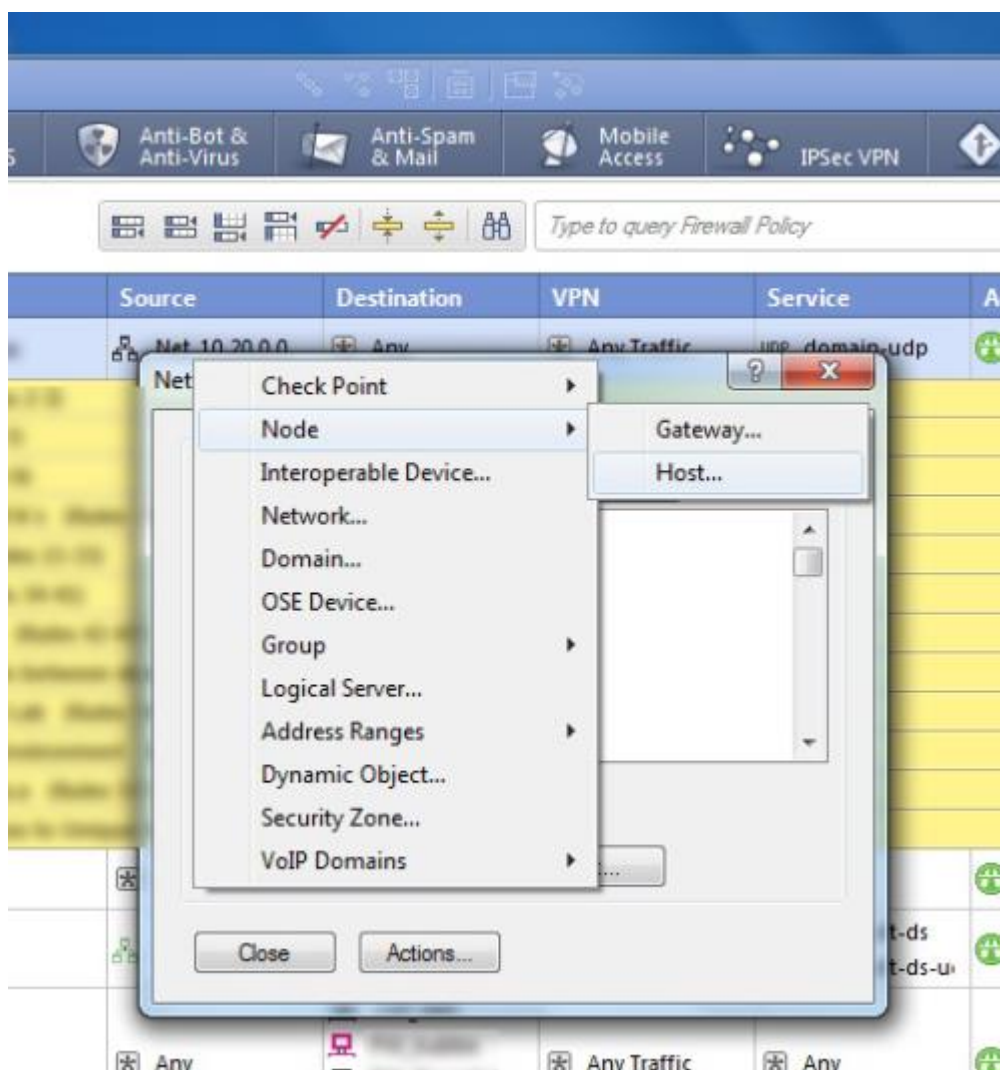
Примечание: Если сетевой объект для хоста, на котором запущен Nethub Analyzer, уже определен, этот шаг можно пропустить.

Сделайте следующее:

- a. На панели главного меню SmartDashboard выберите **Manage > Network Objects**.



- b. Нажмите **New > Node > Host**.



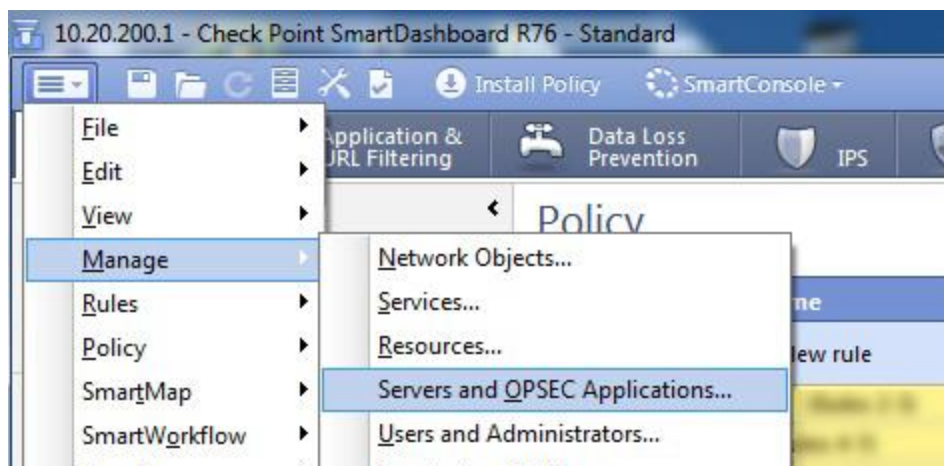
с. В диалоговом окне Host Node введите имя и IP-адрес узла, на котором будет запущен Nethub Analyzer, а затем нажмите ОК.

2. Создайте объект приложения OPSEC для этого сетевого объекта.

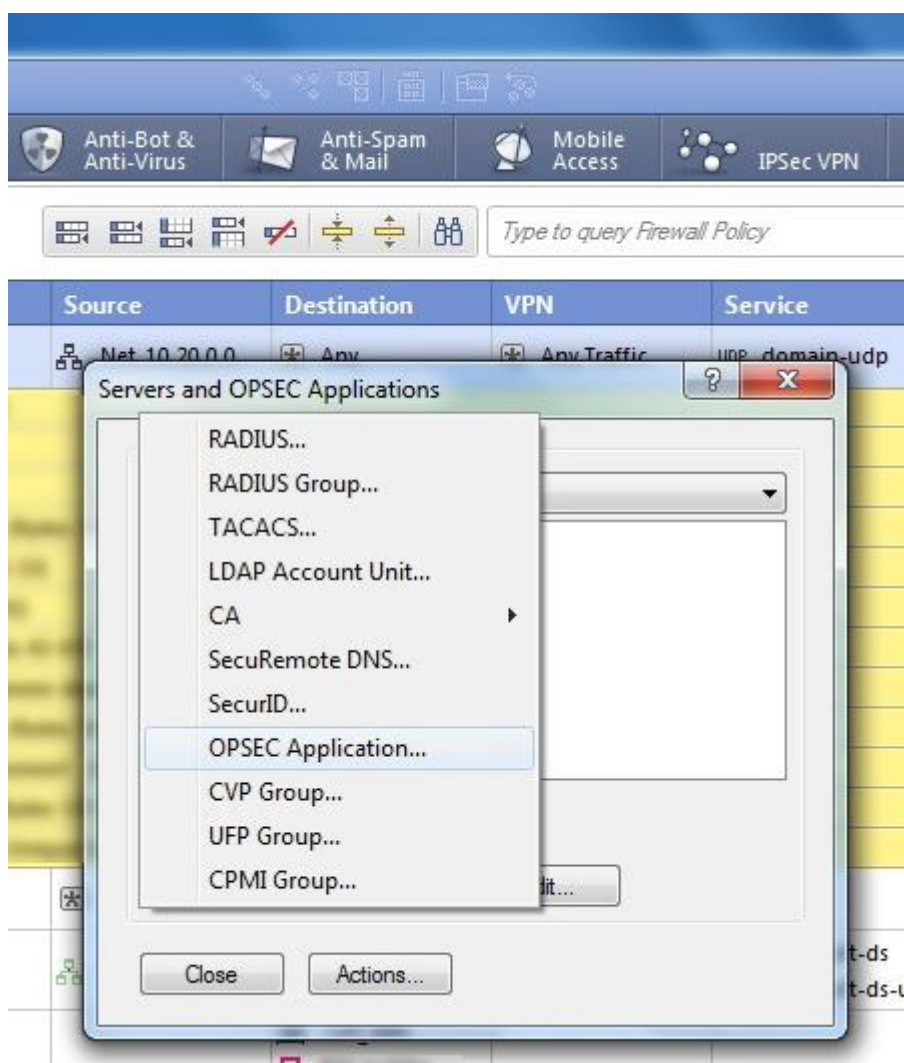
Примечание: Если объект приложения OPSEC уже определен, вы можете пропустить этот шаг.

Сделайте следующее:

а. В главном меню SmartDashboard выберите **Manage**, а затем **Servers and OPSEC Applications**.



- b. В диалоговом окне **Servers and OPSEC Applications** нажмите кнопку **New > OPSEC Application**.



- c. В диалоговом окне **OPSEC Application Properties** определите следующее:

Name	Введите имя приложения OPSEC. Примечание: Запишите введенное вами имя. Вам нужно будет указать это имя в Nethub Analyzer при получении сертификата.
Host	Выберите хост Nethub Analyzer.
Object Entities	Выберите элементы LEA и CPMI.

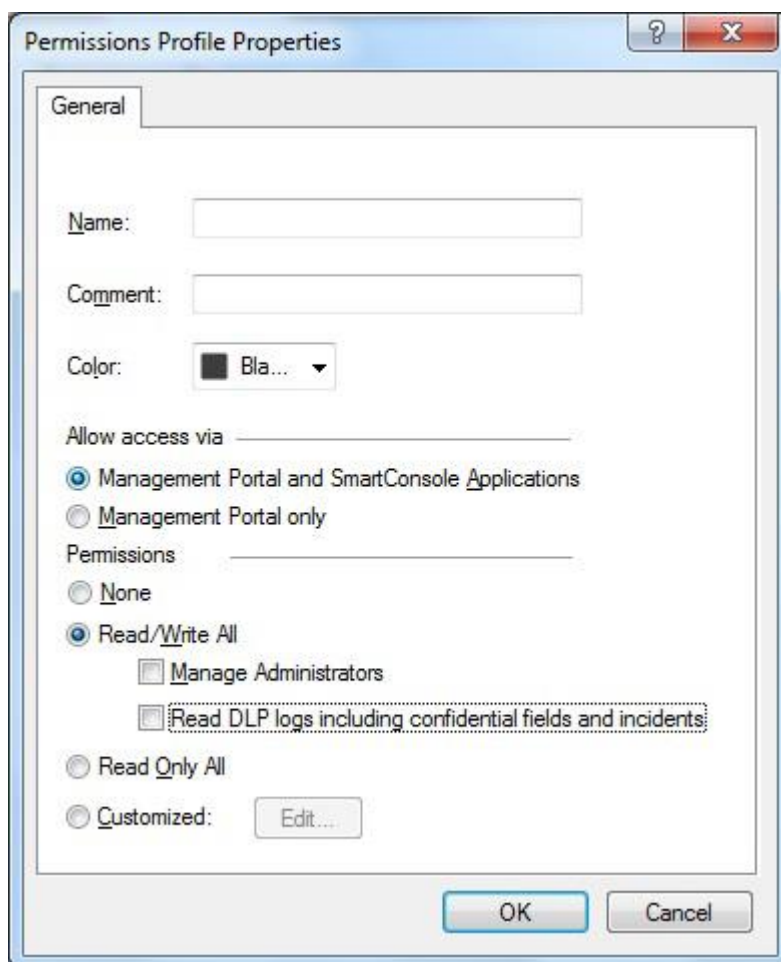
d. На вкладке **CPMI Permissions**, выберите **Permissions Profile**, а затем выполните одно из следующих действий:

- Выберите суперпрофиль в списке или любой другой профиль с необходимыми минимальными правами.
- Создайте новый профиль разрешений. Для этого нажмите кнопку New (Новый). В диалоговом окне **Permissions Profile Properties** введите имя для нового профиля и выберите необходимые права.

Минимальные необходимые права: Read All

Если вы используете ActiveChange, должен быть предоставлен доступ Read/Write All.

Например:



- е. Для Check Point версии R76 или выше, на вкладке Права LEA выберите **According to Permissions Profile**.

Затем выполните одно из следующих действий:

- Выберите суперпрофиль в списке или любой другой профиль с необходимыми минимальными правами.
- Создайте новый профиль разрешений. Для этого нажмите кнопку New (Новый). В диалоговом окне Свойства профиля разрешений введите имя нового профиля и выберите необходимые права.

Минимальные необходимые права: **Read Only All**.

- ф. Нажмите ОК. Снова появляется вкладка "**General**" с дополнительными опциями.
3. Создайте свой сертификат. Сделайте следующее:
- а. Нажмите **Communication**.
 - б. В появившемся диалоговом окне **Communication** введите одноразовый ключ активации, а затем введите его еще раз для подтверждения.

Примечание: Запишите введенный ключ. Вам нужно будет указать его в Nethub Analyzer при подключении сертификата.

с. Нажмите **Initialize**.

Состояние доверия изменится с Uninitialized на Initialized, но доверие не будет установлено. После того как сертификат будет получен Nethub Analyzer, состояние доверия изменится на Доверенный.

Совет: При необходимости создайте новый сертификат, нажав кнопку Сброс и повторив этот шаг.

4. Переустановите базу данных Check Point на всех существующих серверах логов, включая CLM или внешние серверы логгирования. Нажмите Сохранить, а затем выберите в главном меню пункт «Политика и установка базы данных».

8.9.1 Включить сбор данных через REST

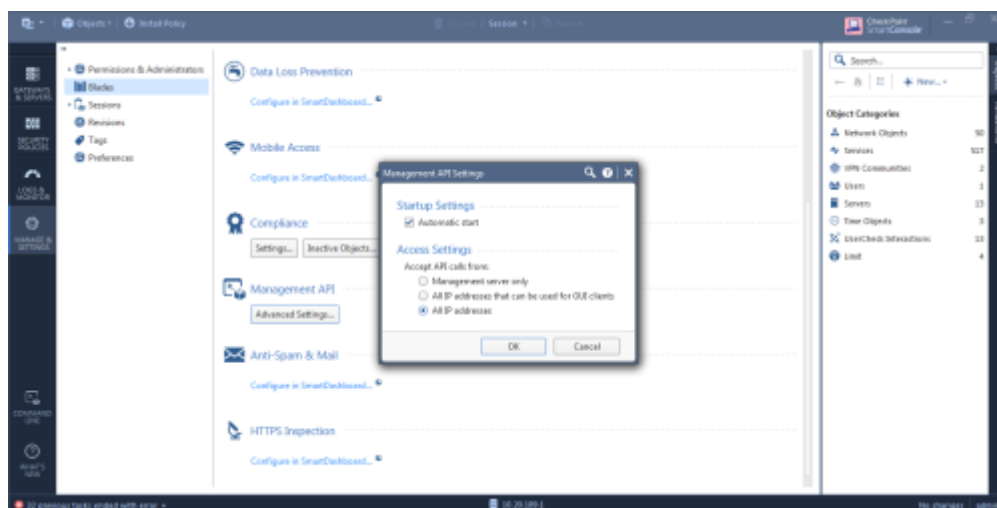
Эта процедура описывает, как включить вызовы REST к серверу управления безопасностью.

Примечание: Для версий R80 и выше Nethub Analyzer собирает данные через REST, наряду с SSH или OPSEC. В дополнение к включению REST, вы также должны включить SSH или OPSEC.

Сделайте следующее:

1. Откройте SmartConsole.
2. В левой панели перейдите к пункту **Manage & Settings > Blades > Management API > Advanced Settings**.

Появится окно Настройки API управления.



3. Чтобы автоматически запускать сервер API при запуске Security Management Server, установите флажок Automatic Start (Автоматический запуск).
4. Выберите IP-адреса, с которых сервер API принимает запросы:

Все IP-адреса, которые могут быть использованы для клиентов GUI	Сервер API будет принимать сценарии и запросы веб-служб от тех же устройств, которым разрешен доступ к серверу управления безопасностью. Убедитесь, что сервер Nethub Analyzer находится в этом списке.
Все IP-адреса	Сервер API будет принимать сценарии и запросы веб-сервисов с любого устройства

5. Нажмите **ОК**.

В появившемся сообщении о перезапуске API управления нажмите кнопку **ОК**.



6. В верхней части нажмите **Publish**.

7. В Management Check Point Server CLI выполните команду `api restart`, а затем выйдите из системы.

8.10 Добавление устройств Huawei USG

В этом разделе описывается как добавить устройства Huawei в Нетхаб и выполнить нужные настройки. Для подключения сетевого устройства к Нетхаб, необходимо предоставить следующий сетевой доступ:



Коннектор к Huawei поставляется в формате отдельного устанавливаемого плагина. Плагин и его обновления поставляются вендором по запросу.

Этот плагин, основанный на общей интеграции устройств, не входит в стандартный инстанс Нетхаб и должен быть установлен вручную.

Этот плагин поддерживает:

- Анализ
- Монитор
- Логи аудита – изменения.

- Логи трафика – Оптимизация политики, включая неиспользуемые правила и IPT.

Плагин не поддерживает: Нетхаб Менеджер, автоматическое внесение изменений.

Плагин поддерживает следующие модели устройств Huawei:

- Межсетевой экран USG6680
- Межсетевой экран USG6680
- Межсетевой экран USG9560
- Межсетевой экран USG6620

Другие модели межсетевых экранов Huawei не тестировались.

Большинство функций брандмауэра Huawei поддерживаются Нетхаб Менеджер, в том числе:

- Несколько VSYS
- Глобальные объекты
- NAT

8.10.1 Установка плагина

1. загрузить zip-файл в систему Нетхаб (консоль Linux)
2. распаковать zip-файл.
3. выполнить «python deploy.py» в консоли Linux

По окончании установки плагина необходимо выполнить релогин в веб-интерфейсе.

8.10.2 Настройка фаервола

1 Требуется один пользователь-администратор, который может получить доступ к FW с помощью ssh или telnet:

1.1 Создайте администратора с типом службы ssh или telnet. Например, чтобы Нетхаб подключался к FW, используя пользователя администратор с именем «ssh_admin», необходимо выполнить эти команды на консоли FW:

```
[system] aaa
```

```
[system-aaa] manager-user ssh_admin
```

```
[system-aaa-manager-user-ssh_admin] service-type ssh
```

1.2 включите службу sTelnet на FW:

```
[system] stelnet server enable
```

1.3 включить доступ SSH на интерфейсе, который подключается к Нетхаб. Например, если необходимо, чтобы Нетхаб подключался к FW по интерфейсу GigabitEthernet1/0/0, необходимо выполнить эти команды в консоли FW:

```
[system] interface GigabitEthernet 1/0/0
```

```
[system-GigabitEthernet1/0/0] service-manage ssh permit
```

2 Если требуется пересылка логов на сервер Нетхаб, вам следует:

2.1 включить 2 типа логов, отправляемых на сервер Нетхаб — лог соответствия политик (трафик) и лог изменений конфигурации (аудит).

```
[system] info-center source POLICY channel loghost log level informational
```

```
[system] info-center source CONFIG channel loghost log level notification
```

2.2 включить создание логов политик. Например, если вы хотите, чтобы фиксировался трафик, соответствующий политике безопасности rule_1, вам необходимо выполнить следующие команды в консоли FW.

```
[system] security-policy
```

```
[system-policy-security] rule name rule_1
```

```
[system-policy-security-rule-rule_1] policy logging
```

2.3 включить создание логов изменений конфигурации. [system] snmp-agent trap enable feature-name config_change

2.4 настроить сервер Нетхаб в качестве хоста сбора логов

```
[system] info-center loghost 10.101.12.8 local-time
```

```
[system] undo dataflow enable
```

2.5 Примечание. FW должен отправлять только 2 типа журналов в Нетхаб:

Policy matching log——Mar 29 2017 16:23:39 USG6600

%%01POLICY/6/POLICYPERMIT(1):vsys=abc, protocol=17, source-ip=63.1.1.8, source-port=137, destination-ip=63.1.1.255, destination-port=137, time=2017/3/30 01:23:39, sourcezone=untrust, destination-zone=untrust, rule-name=eeee

Configuration change log——May 22 2017 03:17:19 USG6000V2

CONFIG/5/CONFIGCHANGE:OID 1.3.6.1.4.1.2011.6.122.83.1.2.1 The configuration has been changed.(UserName=root, TerminalIp=4.1.88.77, VsysName=aa, ModuleType=SecurityPolicy, ModuleObject=abc, Action=ADD, TargetObject=)

8.10.3 Подключение

- 1) Перейти на страницу добавления устройств (подробнее в разделе 5.1);
- 2) На странице выбора вендора и устройства выберите Huawei.
- 3) Заполните поля по мере необходимости (см. таблицу ниже).

Хост	Введите имя хоста или IP-адрес устройства.
Имя пользователя	Введите имя пользователя, которое будет использоваться для доступа к устройству.

Пароль	Введите пароль, который будет использоваться для доступа к устройству.
Нестандартный порт	Чтобы указать пользовательский порт, выберите этот параметр и введите порт. Эта опция актуальна только при выборе REST.

Если требуется сбор логов, системное имя FW необходимо ввести в поле «Дополнительные идентификаторы брандмауэра». Обратите внимание, что FW должны иметь разные идентификаторы, чтобы Нетхаб мог идентифицировать логи, принадлежащие каждому FW (пример Рисунок 24).

Сбор и мониторинг журналов

Метод сбора логов:

Syslog-ng сервер:

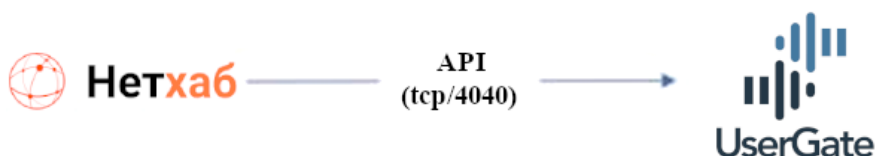
Дополнительные идентификаторы брандмауэра:

(?) Частота сбора журнала (минуты):

Рисунок 24 Пример заполнения поля "Дополнительные идентификаторы брандмауэра"

8.11 Добавление устройств Usergate

В этом разделе описывается как добавить устройства Usergate в Нетхаб и выполнить нужные настройки. Для подключения сетевого устройства к Нетхаб, необходимо предоставить следующий сетевой доступ:



Коннектор к Usergate поставляется в формате отдельного устанавливаемого плагина. Плагин и его обновления поставляются вендором по запросу. Этот плагин, основанный на общей интеграции устройств, не входит в стандартный инстанс Нетхаб и должен быть установлен вручную.

Плагин разработан для версии UserGate старше 6.1.9.

8.11.1 Установка плагина

Для установки необходимо выполнить следующие команды:

```
unzip usergate-connector_230629.zip
```

```
cd release/
```

```
python3.4 deploy.py
```

После установки необходимо перезайти в веб интерфейс системы.

8.11.2 Подключение

- 4) Перейти на страницу добавления устройств (подробнее в разделе 5.1);
- 5) На странице выбора вендора и устройства выберите Huawei.
- 6) Заполните поля по мере необходимости (см. таблицу ниже).

Хост	Введите имя хоста или IP-адрес устройства.
Имя пользователя	Введите имя пользователя, которое будет использоваться для доступа к устройству.
Пароль	Введите пароль, который будет использоваться для доступа к устройству.
Нестандартный порт	Чтобы указать пользовательский порт, выберите этот параметр и введите порт. Эта опция актуальна только при выборе REST.

8.12 Добавление устройств fortinet

Примечание: Версии FortiManager до 5.2.3 не поддерживаются.

Для версий 5.2.3 и выше подключение через SSH/SOAP больше не поддерживается. Вы должны перейти на REST(TCP/443).

8.12.1 Настройка прав для подключения

Для подключения к устройству FortiManager Нетхаб Аналитик требуется учетная запись пользователя с правами Restricted_User.

Достаточно разрешения только на чтение, как показано на Рисунок 25.

System Settings ▾

Dashboard | **Edit Profile**

All ADOMs

Profile Name: Restricted_User

Description: Restricted user profiles have no System Privileges enabled, and have read-only access for all Device Privileges

Type: ☒ System Admin ☐ Restricted Admin

☐ Read-Write ☐ Read-Only ☐ None

System Settings	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Administrative Domain	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
FortGuard Center	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
License Management	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Advanced	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Device Manager	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Add/Delete/Edit Devices/Groups	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Retrieve Configuration from Devices	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Revert Configuration from Revision History	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Terminal Access	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Manage Device Configurations	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Provisioning Templates	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
SD-WAN	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Policy & Objects	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Global Policy Packages & Objects	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Assignment	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Policy Package & Objects	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Policy Check	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Install Policy Package or Device Configuration	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Import Policy Package	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Interface Mapping	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
AP Manager	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
FortiClient Manager	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
FortiSwitch Manager	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
VPN Manager	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>

Рисунок 25 Права необходимые для подключения устройства Fortinet

Примечание: FortiManager v5.2.3 и выше с REST доступом должен иметь разрешения на `rpc-permit (set rpc-permit read)`, используя FortiManager CLI или системные настройки веб-интерфейса для администратора, установите JSON API ACCESS на Read.

Если же используется ActiveChange, Нетхаб Аналитик требует учетную запись пользователя с правами Super_User с правами чтения-записи (см. Рисунок 26).

	System Admin	Read-Write	Read-Only	None
System Settings	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Administrative Domain	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
FortiGuard Center	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
License Management	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Firmware Management	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Advanced	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Device Manager	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Add/Delete/Edit Devices/Groups	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Retrieve Configuration from Devices	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Revert Configuration from Revision History	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Terminal Access	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Manage Device Configurations	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Provisioning Templates	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
SD-WAN	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Policy & Objects	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Global Policy Packages & Objects	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Assignment	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Policy Package & Objects	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Policy Check	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Install Policy Package or Device Configuration	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Import Policy Package	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Interface Mapping	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
AP Manager	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
FortiClient Manager	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
FortiSwitch Manager	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
VPN Manager	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Рисунок 26 Права необходимые для подключения устройства Fortinet с ActiveChange

8.12.2 Подключение

- 1) Перейти на страницу добавления устройств (подробнее в разделе 5.1);
- 2) На странице выбора вендора и устройства выберите Fortinet.
- 3) Заполните поля по мере необходимости (см. таблицу ниже).

Хост	Введите имя хоста или IP-адрес устройства.
Имя пользователя	<p>Введите имя пользователя, которое будет использоваться для доступа к устройству.</p> <p>Это имя пользователя должно быть именем суперпользователя.</p> <p>Если используются административные домены (ADOM):</p> <p>Чтобы проанализировать только устройства под конкретным ADOM, укажите учетные данные администратора конкретного ADOM.</p> <p>Чтобы проанализировать все устройства под всеми ADOM, укажите учетные данные глобального администратора.</p>

	При анализе устройств в качестве глобального администратора никаких других действий не требуется. В противном случае может потребоваться ручная настройка.
Пароль	Введите пароль, который будет использоваться для доступа к устройству.
Подключение через	Для FortiManager версии 5.2.3 и выше выберите REST. (SSH/SOAP больше не поддерживается). Версии FortiManager ранее 5.2.3 не поддерживаются. Вы должны включить соответствующую веб-службу на самом устройстве. Для получения дополнительной информации см. раздел Включение соответствующего API в устройстве FortiNet FortiManager.
Нестандартный порт	Чтобы указать пользовательский порт, выберите этот параметр и введите порт. Эта опция актуальна только при выборе REST.

8.12.3 ActiveChange

Выберите «Включить ActiveChange», чтобы разрешить Нетхаб Менеджеру внесения изменений на устройстве.

8.12.4 Сбор и мониторинг логов

Чтобы Нетхаб Аналитик обрабатывал логи с устройств, управляемых добавляемым устройством FortiManager, вам может потребоваться указать дополнительные идентификаторы устройств.

Это актуально, когда дочернее устройство представлено несколькими или нестандартными идентификаторами устройства. Например, это может быть актуально для кластеров брандмауэров или нестандартных настроек логгирования.

Метод сбора логов	Укажите, должен ли Нетхаб Менеджер собирать логи для устройства, выбрав один из следующих вариантов: None: Не собирать логи. Стандарт: Включение сбора логов. Обширный: Включение сбора логов и Intelligent Policy Tuner. Значение по умолчанию - Обширный.
Сервер Syslog-ng	Если в поле Метод сбора логов, вы выбрали Стандартный или Расширенный, необходимо указать сервер syslog-ng.

Частота
сбора логов

Введите интервал времени в минутах, через который Нетхаб Менеджер должен собирать логи для устройства.

9 Нетхаб Менеджер

Нетхаб менеджер автоматизирует жизненный цикл изменения политики безопасности, начиная с момента подачи запроса на изменение и заканчивая аудитом внесенных изменений. Использование Нетхаб менеджера для внесения изменений в политики безопасности гарантирует, что изменения в устройствах будут одобрены, проверены и реализованы так, как задумано.

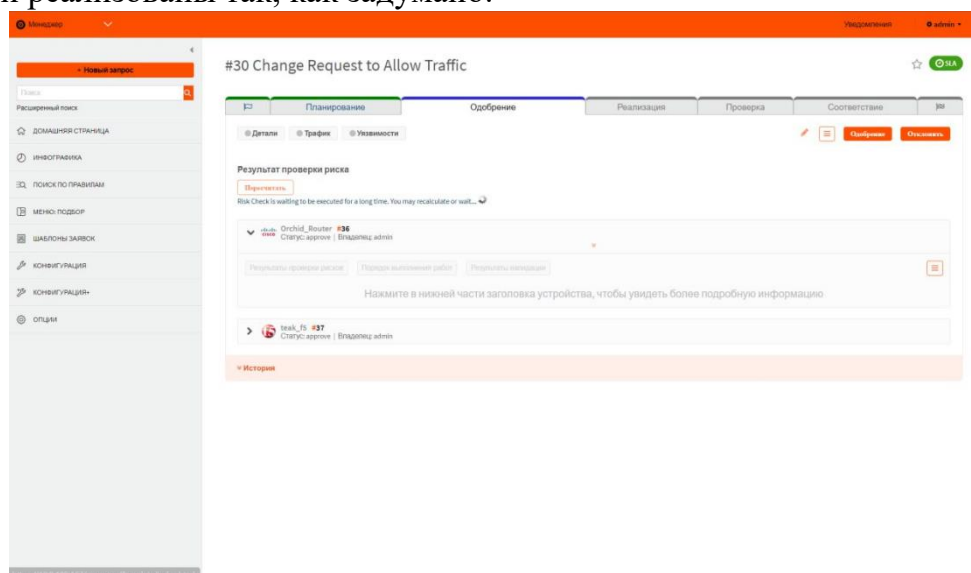


Рисунок 27 Нетхаб менеджер

Нетхаб менеджер анализирует запрос на изменение политики и все связанные с ним устройства, маршрутизаторы и VPN, чтобы убедиться в том, что изменение действительно необходимо.

9.1 Создание запроса на изменение

Данная операция предназначена для внесения в систему Нетхаб данных о запрошенных изменениях сетевых доступов. Для создания запроса необходимо выполнить следующие действия:

- 1) В левом верхнем углу страницы перейти в модуль **Менеджер**, для этого нужно нажать символ «V» и в выпадающем списке выбрать **Менеджер**.

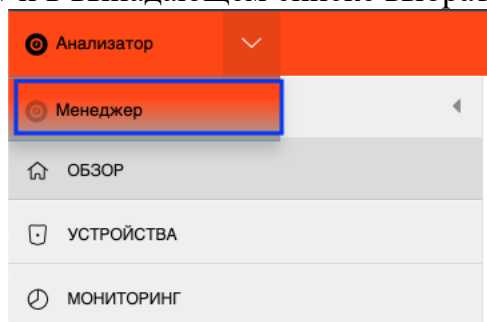


Рисунок 28 Выбор Нетхаб менеджер

2) Для перехода в режим создание запроса нужно нажать кнопку **+ Новый запрос**.

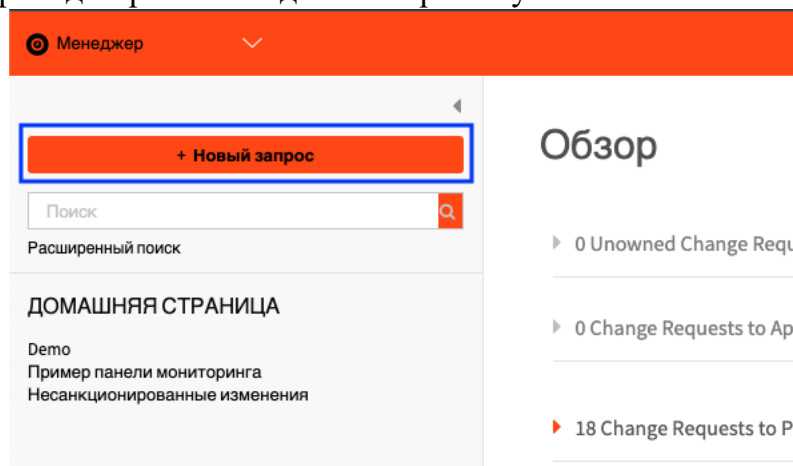


Рисунок 29 Создание запроса

3) Далее необходимо выбрать советующий шаблон запроса из списка;
Создайте новый запрос на изменение

Загрузить черновик

Выберите шаблон запроса:

Шаблон	Описание
Standard	Создайте запрос на изменение для запроса трафика
110: Запрос на множественное подтверждение	Создайте запрос на изменение трафика, который требует нескольких утверждений
115: Automatic Traffic Change Request	Create a traffic change request that progresses automatically
120: Generic request	Create a generic change request
130: Object Change Request	Создайте запрос на изменение объекта (добавление/удаление/редактирование сетевых и сервисных объектов)
140: Rule Removal Request	Create a change request for removing a device rule
145: Rule Modification Request	Create change request for editing a device rule
150: Parallel-Approval Request	Create a traffic change request which requires parallel approvals
160: Web Filter-Change Request (Blue Coat)	Create a web-filter change request
170: Traffic Change Request (IPv6)	Create a request for IPv6 traffic change in Cisco devices
180: Traffic Change Request (Multicast)	Create a request for Multicast traffic change in Cisco devices
190: Verbatim Rule Addition	Create a traffic change request for bulk rules addition exactly as specified
Basic Change Traffic Request	Create a basic change traffic request

Рисунок 30 Выбор шаблона

4) Заполнить необходимые поля и отправить заявку.

Создайте новый запрос на изменение

Назад **Создать черновик** **Создать**

General

Subject:

Change request justification:

Due:

Attachments: [Add files...](#)

Owner:

Requestor:

Expires:

Device Name:

Traffic

Установить значение трафика

1 Source: Destination: Service: Action:

Requested Source Group Name: Requested Destination Group Name: Requested Service Group Name:

Access Lists:

Import traffic from csv

Рисунок 31 Заполнение заявки

