Настройка двухфакторной аутентификации в Check Point Security Gateway

Общая информация

Check Point Security Gateway – это шлюз безопасности. Он позволяет проверять данные на наличие угроз, безопасно публиковать приложения, а также служит VPN хабом для удаленного доступа сотрудников.

Использование устройства Рутокен для VPN-соединения позволяет сделать процесс подключения более безопасным.

Описание процесса аутентификация в Check Point Security Gateway при помощи сертификата, записанного на Рутокен:

Пользователь соединяется с Check Point Security Gateway Appliance при помощи клиентского приложения Check Point Security Gateway. Пользователь подключает Рутокен, на котором хранится сертификат, и вводит PIN -код. После успешной аутентификации пользователь получает доступ к внутренним ресурсам.

Для настройки двухфакторной аутентификации необходимо:

- Установить и настроить Microsoft Certificate Authority.
- Наличие у пользователя устройства Рутокен с специальным сертификатом.
- Установить Панель управления Рутокен.

Процесс настройки Check Point Security Gateway состоит из следующих шагов:

1) Создание учетной записи пользователя и выпуск регистрационного ключа.

2) Создание группы пользователей.

3) Включение возможности аутентификации для VPN-клиентов.

4) Настройка правил фильтрации для VPN-клиентов.

5) Установка политики.

6) Установка сертификата.

7) Разрешение контроля удаления смарт-карты.

Создание учетной записи пользователя и выпуск регистрационного ключа

Для создания учетной записи пользователя и выпуска регистрационного ключа:

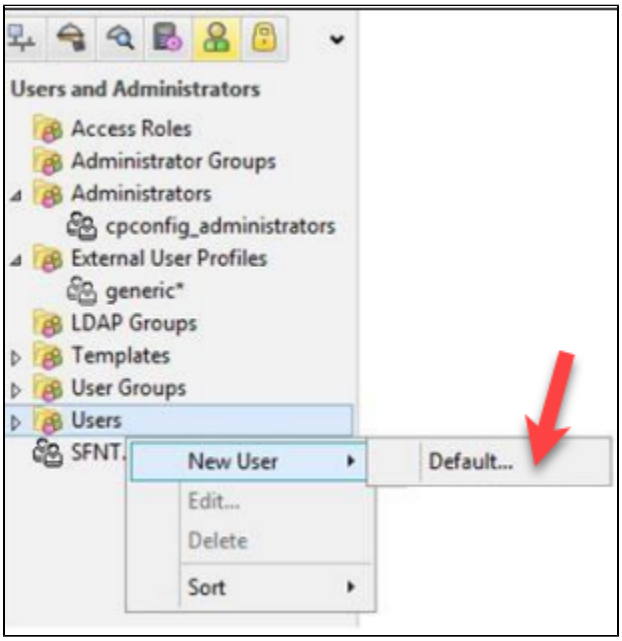
1) Откройте **Check Point SmartDashboard R77**.

2) Введите имя пользователя и пароль.

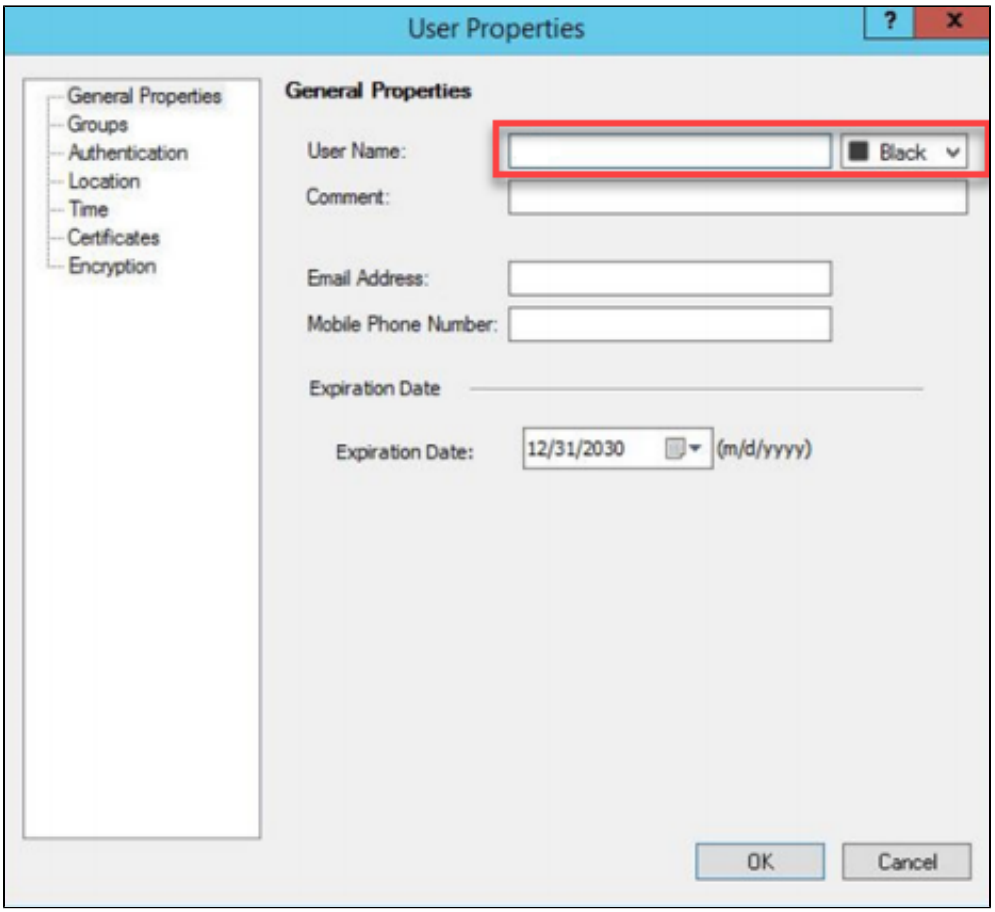
3) В поле **Server IP Address** из раскрывающегося списка выберите имя или IP -адрес сервера, на котором расположен Check Point Security Gateway.

4) Нажмите **Login**.

5) В главном окне Check Point SmartDashboard выберите пункт: Users → New User → Default.

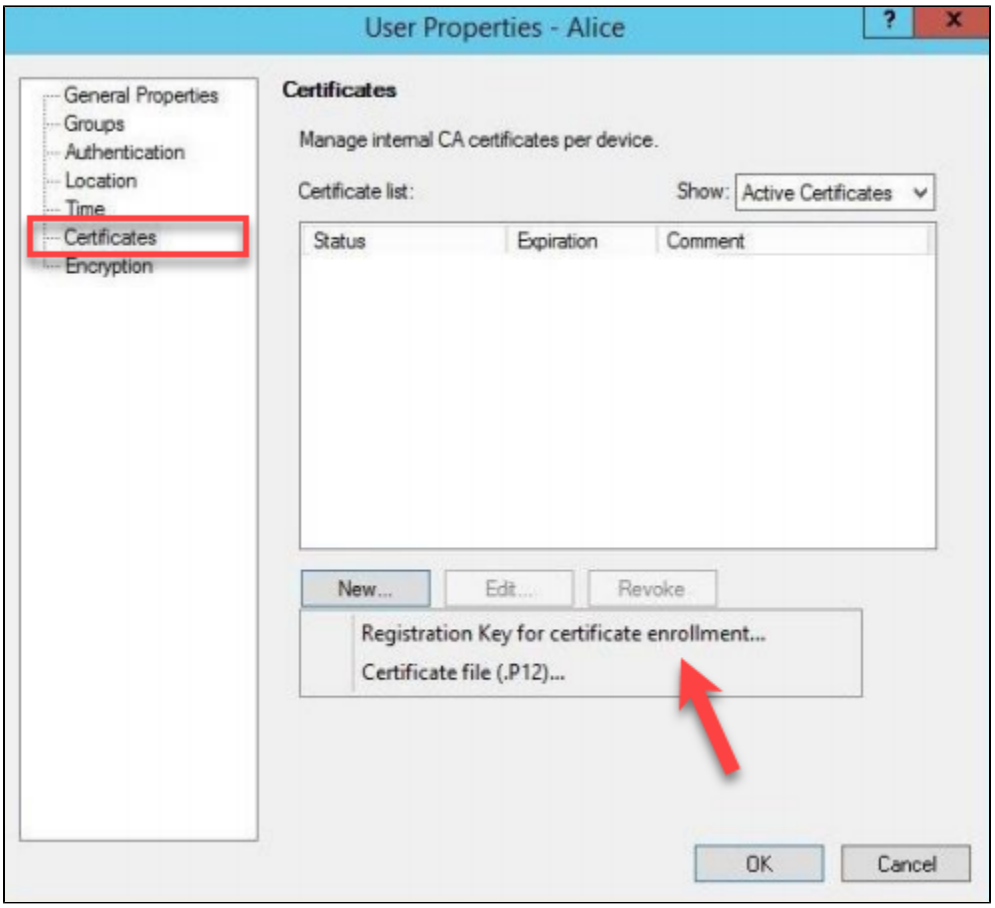


6) В окне **User Properties** в поле **User Name** введите имя пользователя.

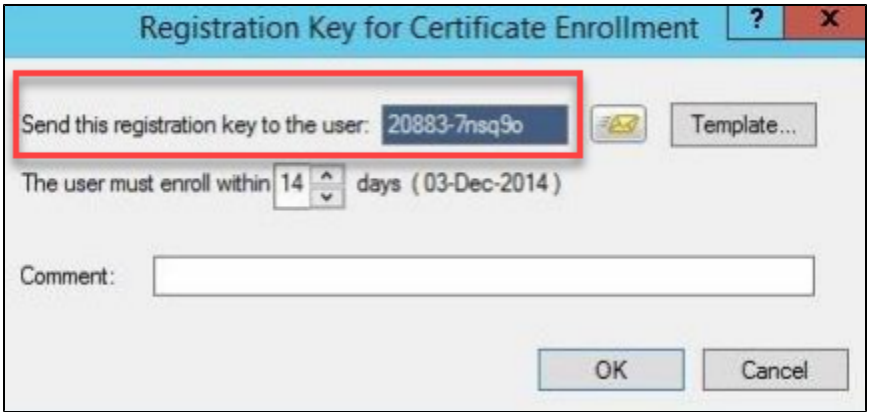


7) В левой части этого окна выберите пункт **Certificates**.

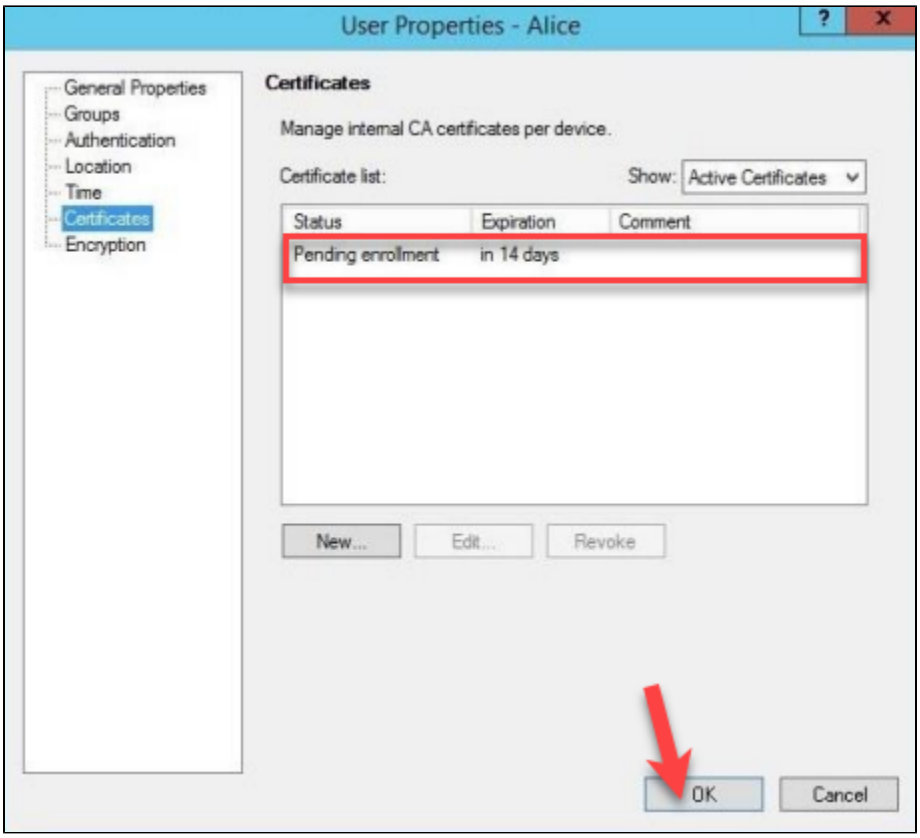
8) Нажмите **New** и выберите пункт **Registration Key for certificate enrollment**. Откроется окно **Registration Key for Certificate Enrollment**.



9) В этом окне скопируйте регистрационный ключ.



10) В окне **User Properties** в списке сертификатов отобразится сертификат. Нажмите **OK**.

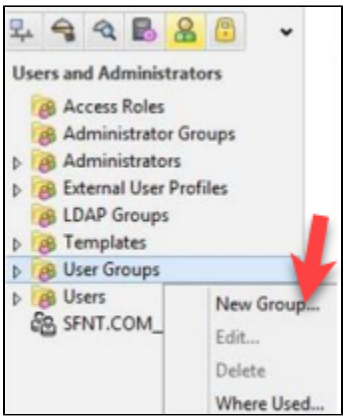


Создание группы пользователей

Check Point Security Gateway не позволяет определять правила для определенных пользователей, но позволяет делать это для групп пользователей.

Поэтому нам необходимо создать группу пользователей. Для этого:

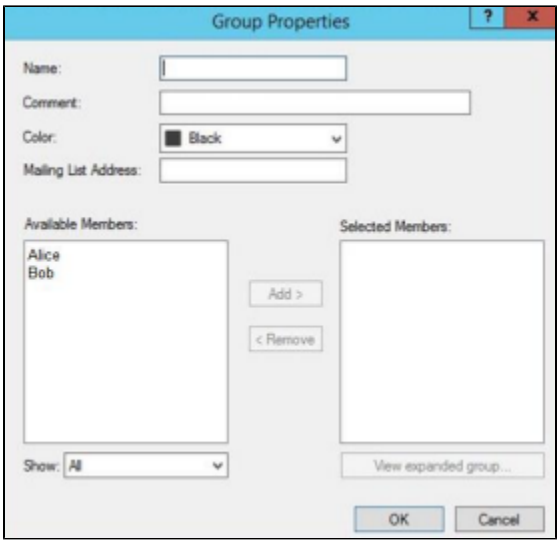
1) В главном окне Check Point SmartDashboard выберите пункт: User Groups → New Group.



2) В окне **Group Properties** в поле **Name** введите название группы (например, VPN_Group).

3) В поле **Available Members** щелкните по необходимым логинам.

4) Нажмите **Add**. В результате пользователи с выбранными логинами добавятся в группу.

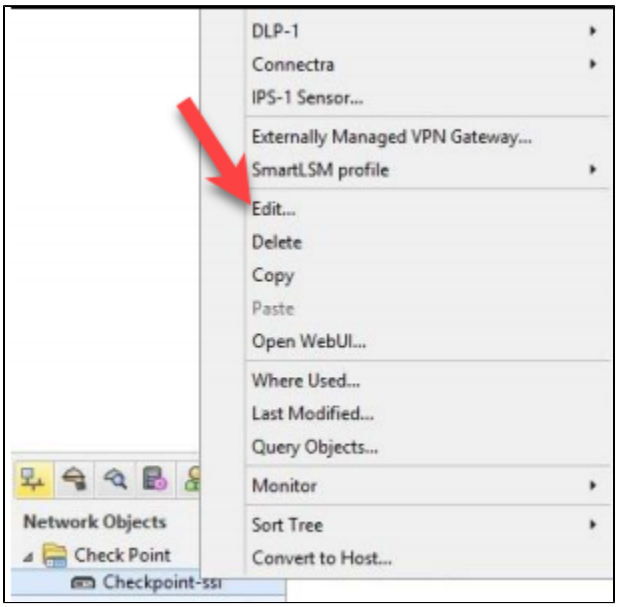


5) Нажмите **OK**. В результате группа будет создана.

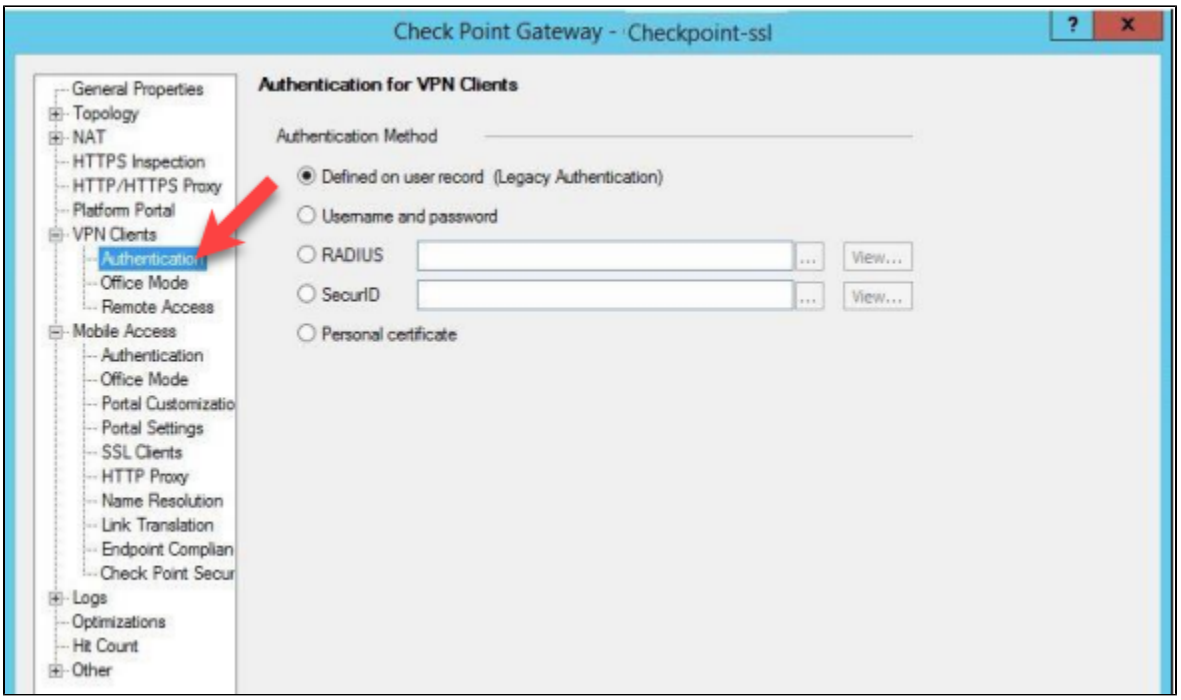
Включение возможности аутентификации для VPN-клиентов

Чтобы включить возможность аутентификации для VPN-клиентов:

1) В главном окне Check Point SmartDashboard выберите пункт: Check Point → Check Point-ssl → Edit.



2) В окне **Check Point Gateway - Checkpoint-ssl** выберите пункт: VPN Client → Authentication.

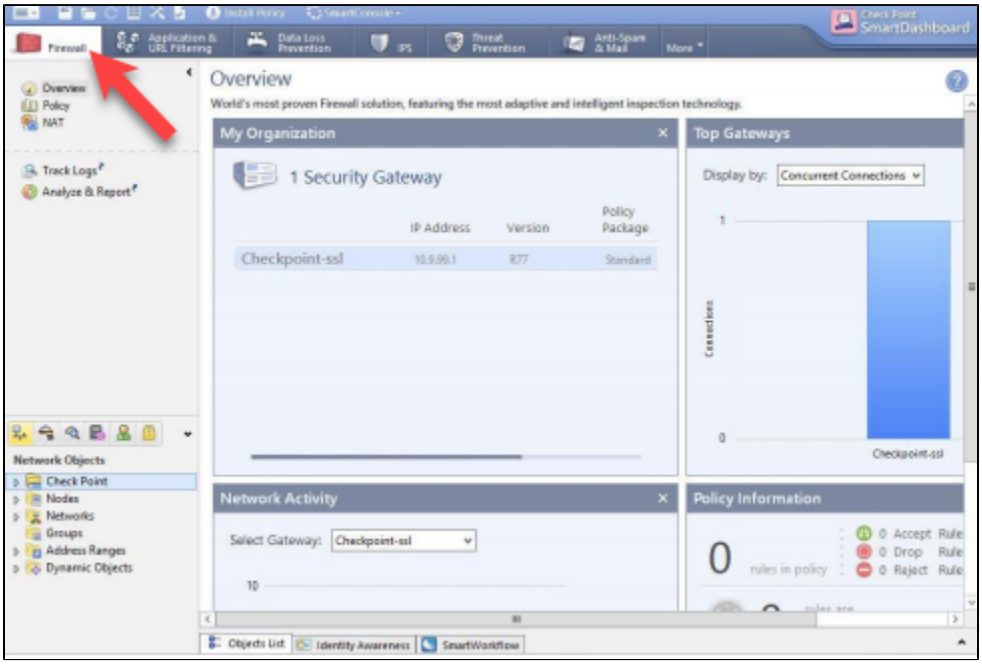


3) В разделе **Authentication Method** установите переключатель **Defined on user record (Legacy Authentication)** и нажмите **OK**.

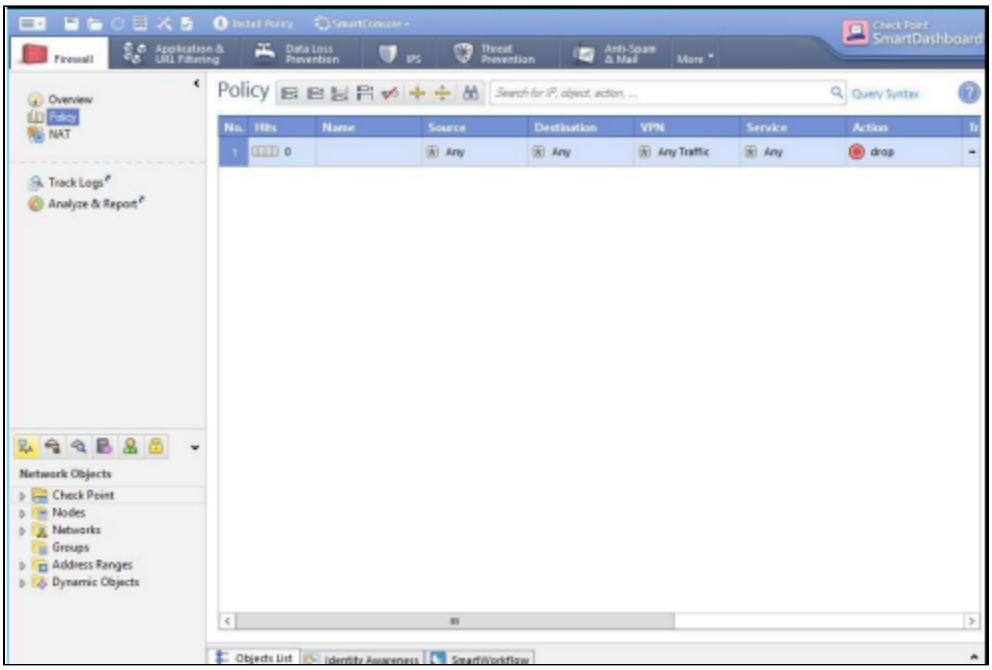
Настройка правил фильтрации для VPN-клиентов

Чтобы настроить правила фильтрации:

1) В главном окне **Check Point SmartDashboard** перейдите на вкладку **Firewall**.



2) Выберите пункт **Police**, затем нажмите **Add rule at bottom**. В результате добавится новая строка.



3) В столбце **Name** щелкните в новой строке правой кнопкой мыши и выберите **Edit**.

4) В окне **Rule Name** в одноименном поле введите имя правила и нажмите **OK**.

5) В столбце **Destination** в новой строке щелкните правой кнопкой мыши и выберите **Network Object**.

6) В окне **Add Object** щелкните по названию пункта **Internal_network** и нажмите **OK**.

7) В столбце **VPN** в новой строке щелкните правой кнопкой мыши и выберите **Edit Cell**.

8) В окне **VPN Match Conditions** установите переключатель **Only connections encrypted in specific VPN communities** и нажмите **Add**.

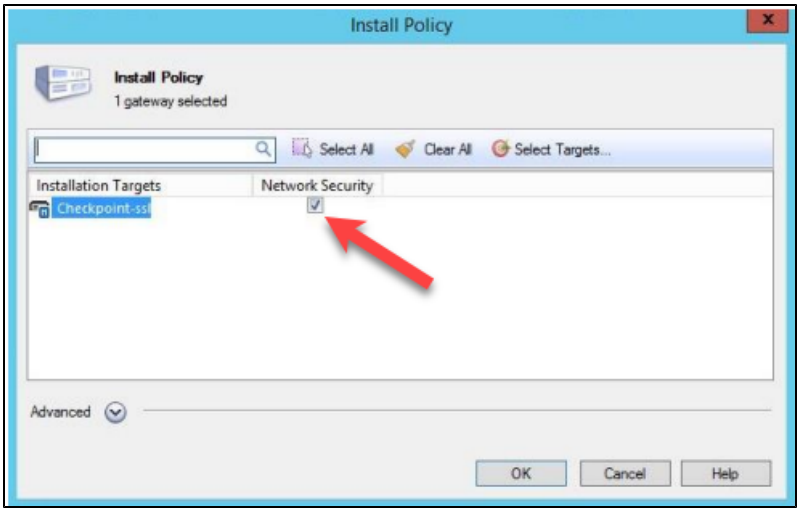
9) В окне **Add Community to rule** выберите пункт **RemoteAccess** и нажмите **OK**.

Установка политики

Чтобы установить политику:

1) В главном окне **Check Point SmartDashboard** щелкните по значку **Install Policy**.

2) В окне **Install Policy** в столбце **Network Security** установите галочку и нажмите **OK**.



3) Дождитесь окончания процесса установки политики и нажмите **Close**.

Установка сертификата

Чтобы установить сертификат:

1) Подключите Рутокен к компьютеру.

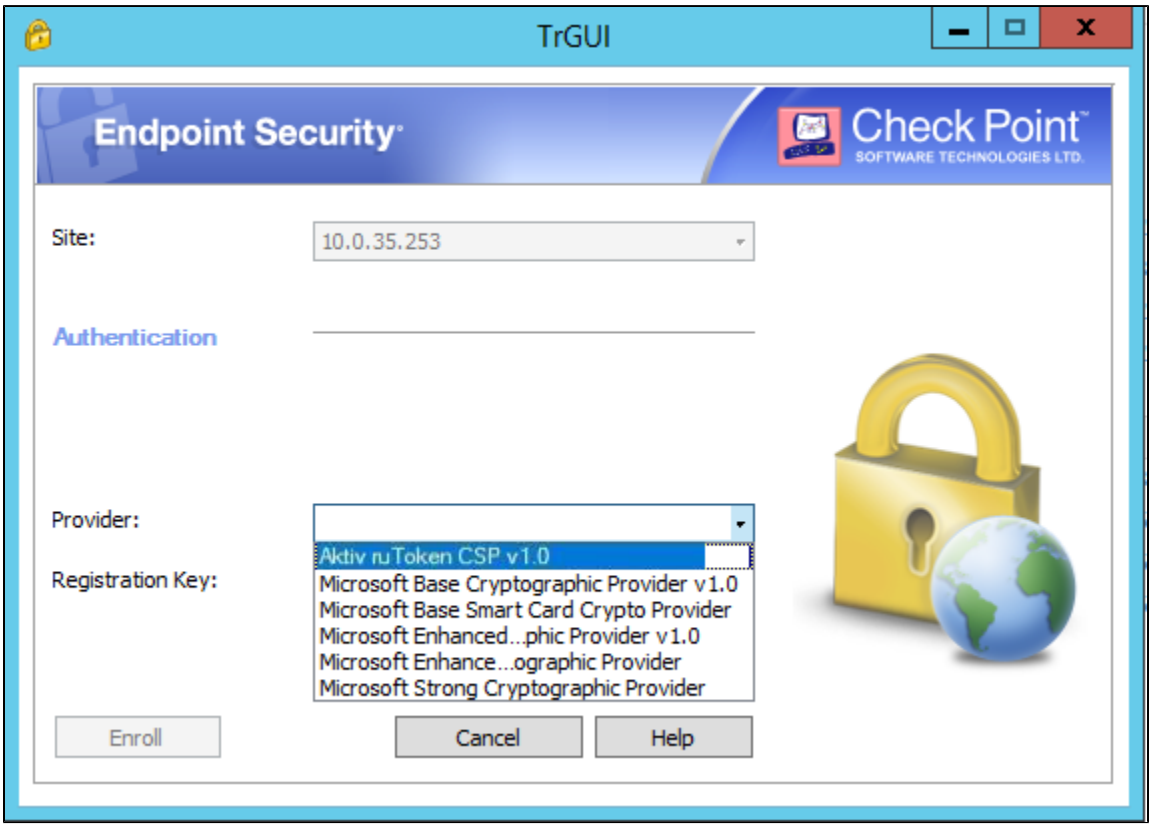
2) Откройте приложение Check Point Endpoint Security.

3) В поле **Site** введите IP-адрес.

4) В раскрывающемся списке **Certificate** выберите необходимый сертификат.

5) Нажмите на ссылку **Click here if you don't have a certificate for this site**.

6) В раскрывающемся списке **Provider** выберите значение **Aktiv ruToken CSP v1.0**.



8) В поле **Registration Key** введите регистрационный ключ.

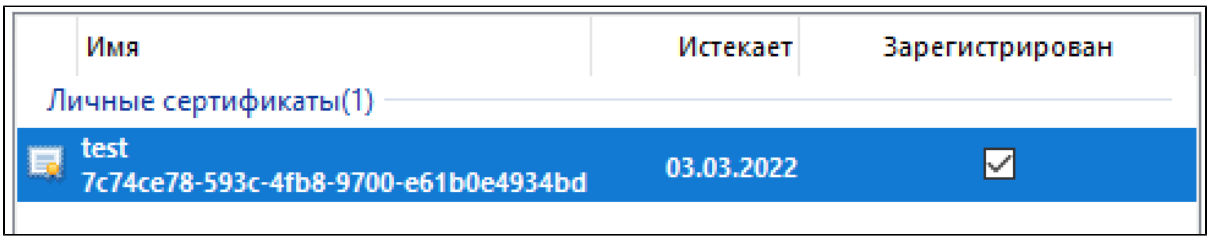
9) Нажмите **Enroll**.

10) В окне **Token Logon** введите PIN-код Рутокена и нажмите **OK**.

11) В окне с сообщением об установке нового корневого сертификата нажмите **Yes**.

12) После завершения процесса установки нажмите **OK**.

13) Откройте **Панель управления Рутокен** и на вкладке **Сертификаты** проверьте, что сертификат сохранился на Рутокене.



Контроль за извлечением смарт-карты

Чтобы настроить контроль за извлечением смарт-карты:

1) Используя редактор **VI**, откройте файл $FWDIR/conf/trac_client_1.ttm.

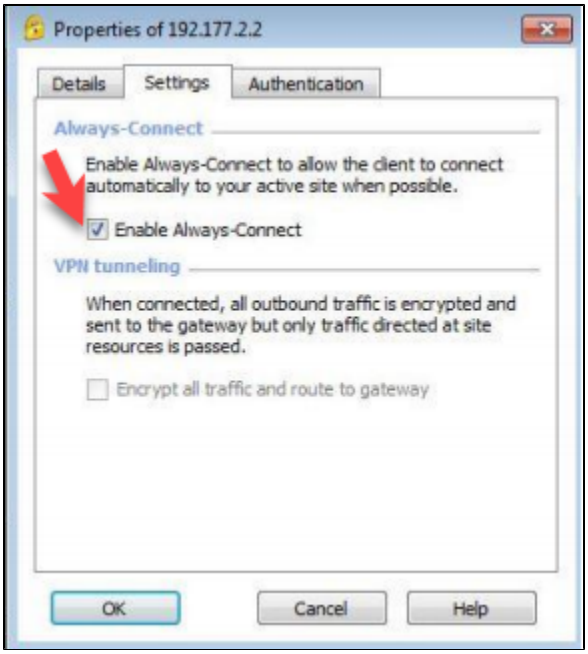
2) Найдите строку disconnect_on_smartcard_removal и выберите необходимое значение параметра:

- true — разрешить детектирование извлечения смарт-карты для текущего шлюза;
- false — запретить детектирование извлечения смарт-карты для текущего шлюза;
- client_deside — разрешить пользователю самостоятельно устанавливать параметр детектирования извлечения смарт-карты для текущего шлюза.

3) Сохраните файл.

4) Установите политику.

5) Откройте окно параметров **Check Point Endpoint Security** и установите галочку **Enable always-connect**.



6) Нажмите **OK**.

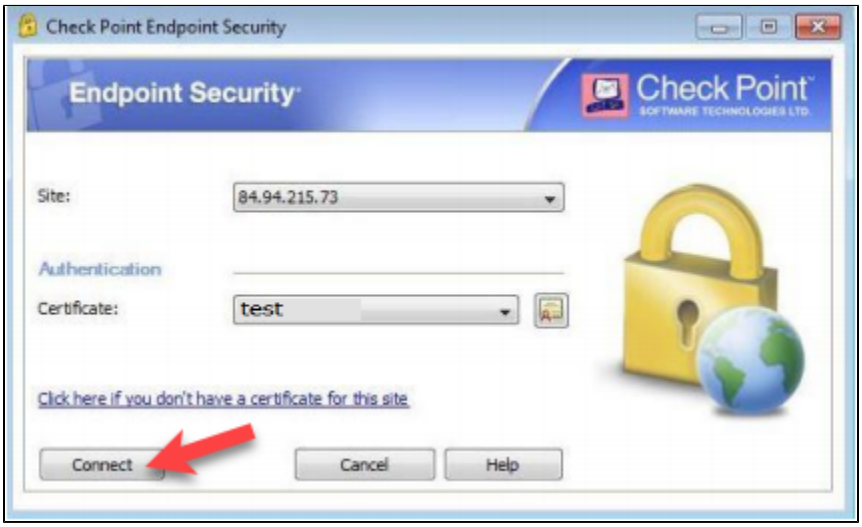
Вход на шлюз

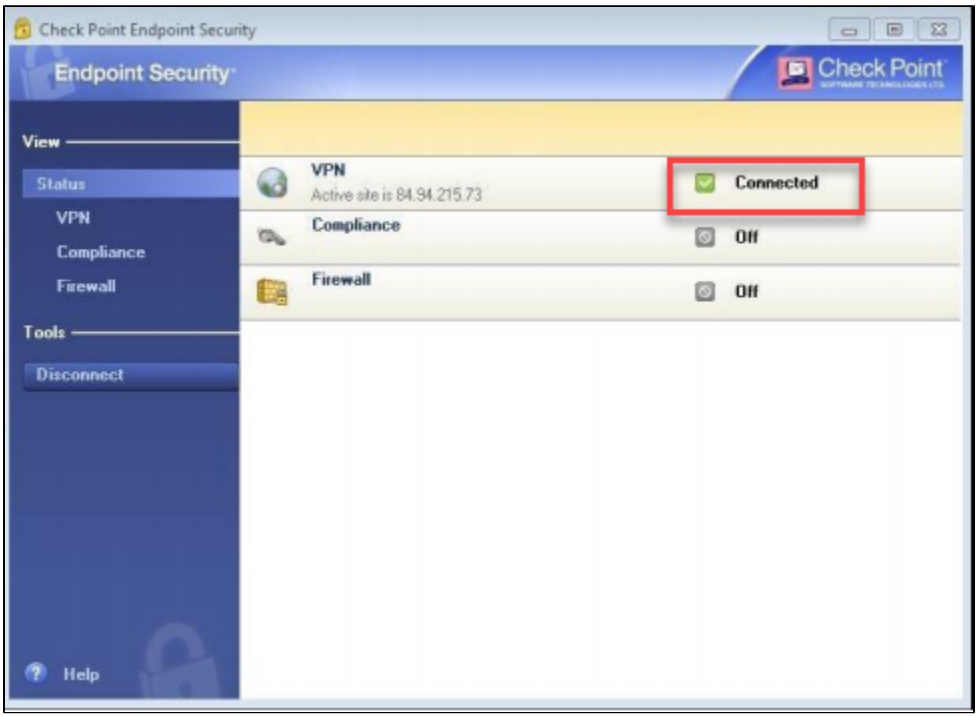
Чтобы войти на шлюз:

1) Откройте приложение Check Point Endpoint Security.

2) Подключите Рутокен к компьютеру.

3) Нажмите **Connect**.



4) В окне **Token Logon** в поле **Password** введите PIN-код Рутокена и нажмите **OK**.

5) На панели задач щелкните по иконке VPN. Если аутентификация прошла успешно, то статус соединения **Connected**.