Check Point Security Gateway и JaCarta PKI

Руководство по настройке

Листов: 25

Автор: Timofey Alekseev

Аннотация

Настоящая инструкция содержит сведения о настройке двухфакторной аутентификации в Check Point Security Gateway с использованием электронных ключей JaCarta PKI.

Оглавление

JaCarta Client

Удалённый доступ к ресурсам организации несёт пользу, но и создаёт ряд проблем для IT-департамента. Возможность корректной идентификации пользователей, запрашивающих доступ к информационной системе, достигается за счёт использования комплексных решений контроля доступа.

Внедрение решений для удалённого доступа без строгой аутентификации пользователей равносильно хранению важных данных в сейфовой ячейке, ключ от которой хранится на ближайшем журнальном столике.

Хорошие решения по аутентификации пользователей подразумевают гарантированный доступ к ресурсам компании только авторизованным пользователям.

PKI - эффективный метод аутентификации для систем строгой аутентификации в аспектах функциональности, безопасности и соблюдения зависимостей.

JaCarta Client - программное обеспечение, позволяющее строить инфраструктуру с открытыми ключами с применением ключевых носителей JaCarta PKI. Данное программное обеспечение позволяет применять защищённую передачу информации, основанную на инфраструктуре открытых ключей.

Электронные ключи могут поставляться в различных форм-факторах, включая USB-токены, смарт-карты, в т.ч. с широкими возможностями кастомизации (нанесение логотипа, использование корпоративного стиля и т.д.). Все форм-факторы управляются единым интерфейсом, программным обеспечением JaCarta Client. JaCarta Client имеет унифицированные методы работы, такие, как PKCS#11, CAPI, которые обеспечивают поддержку множества приложений "из коробки", поддерживающих данные интерфейсы. Поддерживаются такие сценарии, как защищённый Web-вход, защищённый вход в систему, шифрование данных, шифрование почты. PKI ключи и сертификаты могут быть созданы, размещены и использованы наиболее безопасным способом при помощи аппаратных либо программных токенов.

JaCarta Management System предлагает Вашей организации комплексную платформу управления жизненным циклом ключей. JMS связывает идентификаторы с пользователями, позволяя контролировать сертификаты, используемые ими. JMS позволяет масштабировать систему без угрозы нарушения работы.

Check Point Security GateWay защищает внутренние и внешние сети, публичные и приватные облака от внутренних и внешних угроз безопасности, защищая виртуальные машины и приложения при помощи полного набора инструментов защиты Check Point Software Blades.

Данный документ подробно описывает шаги по настройке поддержки входа в удалённую сеть по сертификату пользователя при помощи смарт-карты, либо аппаратного токена JaCarta PKI. Документ подразумевает, что Check Point Security GateWay окружение уже настроено на статические пароли пользователей для аутентификации.

Требования к ПО

Информация в документе применима к:

- JaCarta Client — программное обеспечение, управляющее токенами JaCarta производства "Аладдин Р.Д.";
- Check Point Security GateWay.

Окружение

Версии программного обеспечения, которые были использованы для подготовки данной инструкции.

- JaCarta PKI Client
- CheckPoint GAIA
- CheckPoint Endpoint Security Client

Для кого предназначен этот документ

Данный документ предназначен для системных администраторов, знакомых с семейством Check Point Security Gateway и заинтересованных в использовании возможностей многофакторной аутентификации при помощи смарт-карт и токенов JaCarta производства "Аладдин Р.Д.".

Аутентификация при помощи сертификатов с использованием JaCarta PKI Client.
Схема выше демонстрирует сценарий аутентификации по сертификату.

Пользователь соединяется с Check Point Security Gateway Appliance при помощи клиентского приложения Check Point Security Gateway. Пользователь вставляет токен JaCarta PKI, на котором расположен его сертификат, вводит PIN-код токена.

После успешной аутентификации пользователь получает доступ к внутренним сетевым ресурсам.

Предварительные требования

Здесь описываются предварительные требования, которые необходимо удовлетворить прежде, чем приступать к настройке двухфакторной аутентификации по сертификатам для Check Point Security Gateway с использованием JaCarta PKI.

Для использования аутентификации по сертификатам необходимо установить и настроить Microsoft Certificate Authority. В качестве Удостоверяющего центра может быть использован любой УЦ, но в данном документе рассматривается именно Microsoft CA.

Пользователи должны иметь токены JaCarta PKI с выпущенными подходящими сертификатами на них.

JaCarta PKI Client версии 6.30 и выше должно быть установлено на компьютерах пользователей.

Поддерживаемые токены и смарт-карты

USB токены:

- JaCarta PKI;
- JaCarta PKI/Flash;
- JaCarta PKI/ГОСТ;
- JaCarta PKI/ГОСТ/Flash.

Смарт-карты:

- JaCarta PKI;
- JaCarta PKI/ГОСТ.

Для смарт-карт требуется считыватель ASEDriveIII USB.

Настройка Check Point Security Gateway

Check Point SmartDashboard может быть использовано для настройки CheckPoint SSL VPN или IPSec VPN.

Настройка Check Point Security Gateway требует выполнения ряда действий.

1. Создание учётной записи пользователя и выпуск регистрационного ключа.

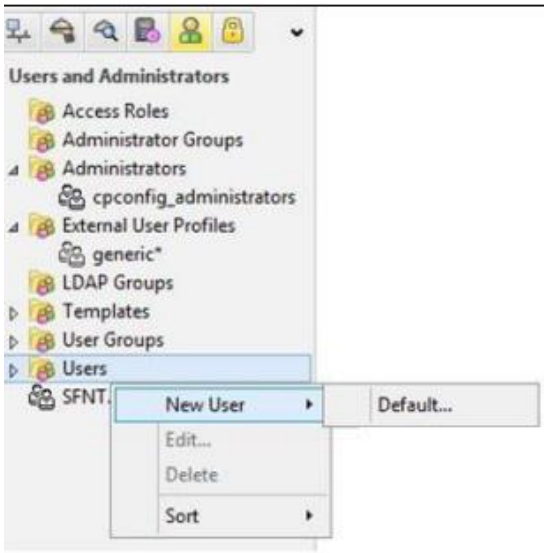
- Создание группы пользователей.
- Разрешение аутентификации для клиентов VPN.
- Установка политики.
- Установка сертификата.
- Разрешение контроля удаления смарт-карты.

Создание пользователя и выпуск ключа регистрации

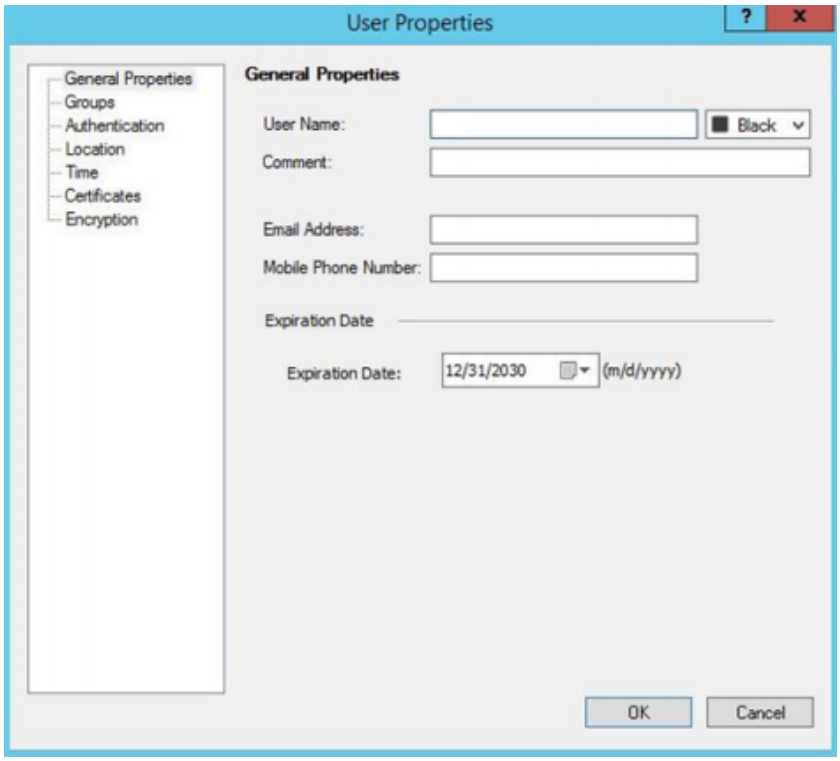
Пользователь создаётся с определённой схемой аутентификации для входа на Check Point Security VPN Client. Затем администратор инициирует процесс выпуска сертификата на Security Management Server и получает ключ регистрации.

- Откройте Check Point SmartDashboard R77.
- На экране логина заполните следующие поля и нажмите "Login".
- Username - введите имя пользователя.
- Password - введите пароль для пользователя.
- Servername or Server IP Adress - выберите имя или IP-адрес сервера, где Check Point Security Gateway расположен.

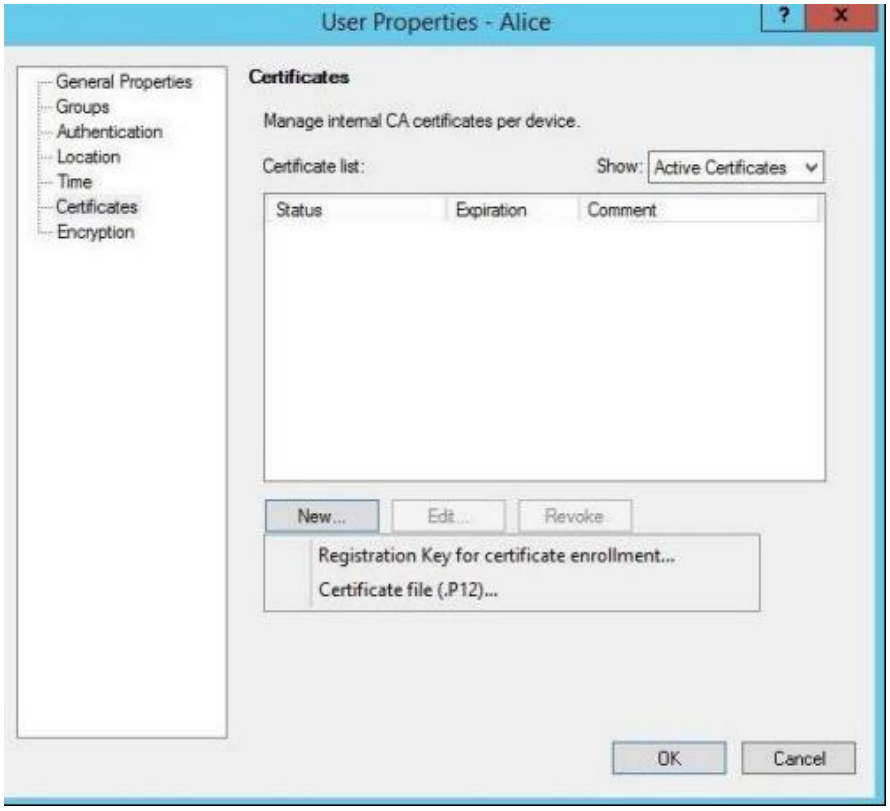
- В главном окне Check Point SmartDashboard, под Check Point SmartDashboard, кликните по Users и затем кликните по New User > Default.



- В окне параметров пользователей в поле имени пользователя введите имя пользователя.

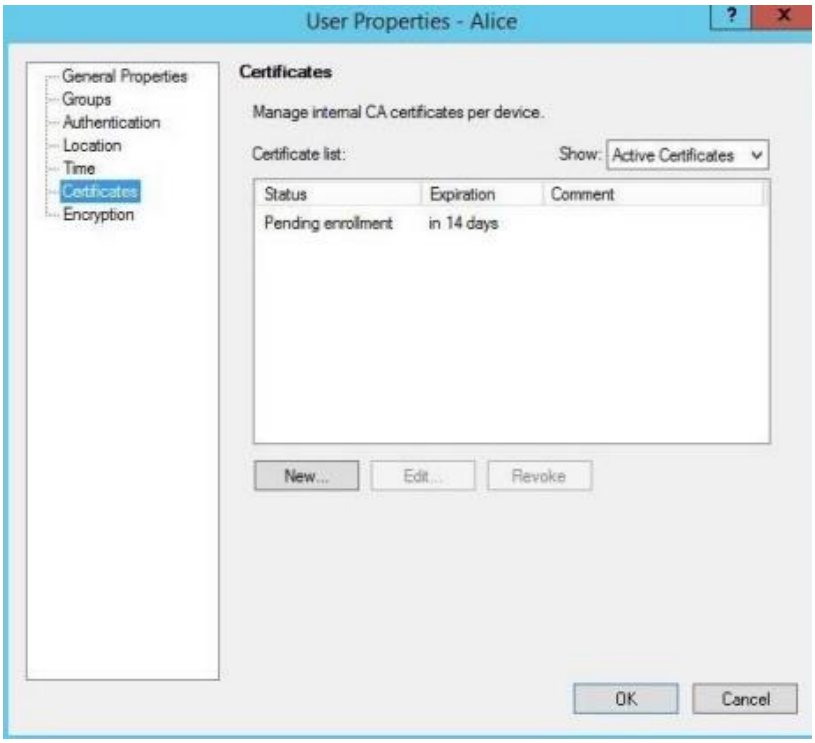


- Кликните по Certificates.



- Кликните по New, затем выберите Registration Key for certificate enrollment.
- В окне Registration Key for Certificate Enrollment отображается ключ регистрации.
- Скопируйте данный регистрационный ключ, сохраните его - он понадобится для дальнейшей регистрации.

- В окне параметров пользователя, в списке сертификатов, добавляется ожидающий установки сертификат. Нажмите ОК.



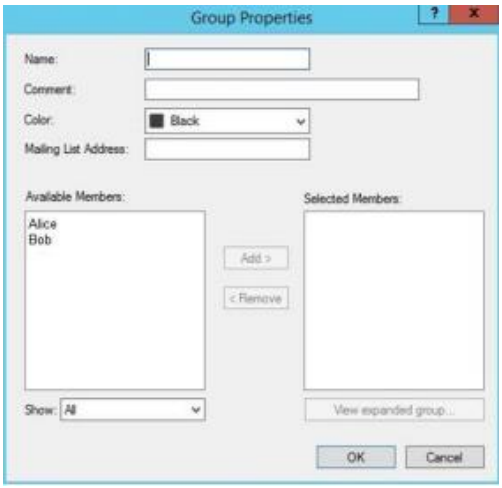
Создание группы пользователей

Пользовательские группы — набор пользователей, имеющих общие задачи, либо обязанности. Группы пользователей, как и отдельные пользователи, могут быть обработаны в политиках безопасности.

Создание групп позволяет Вам назначать задачи определённым пользователям. Шлюз не позволяет Вам определить правила для определённых пользователей, но Вы можете назначать определённые правила группам пользователей.

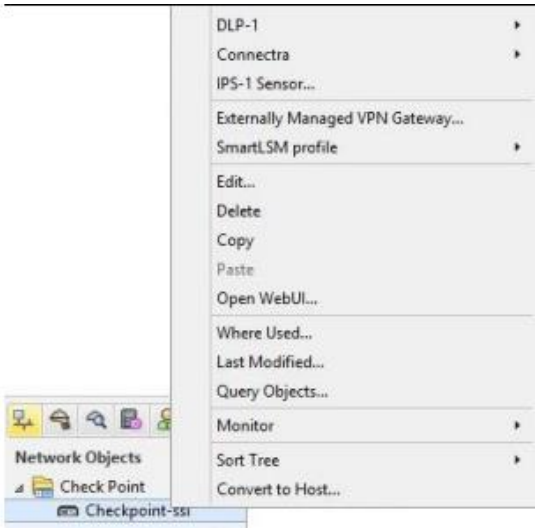
1. В главном окне Check Point SmartDashboard, под Users and Administrators, правый клик по User Groups, а затем New Group.

2. В окне Group Properties заполните следующие поля, а затем кликните ОК.
3. Name - введите имя группы, например, VPN_Group.
4. Available Members/Selected Members - в списке доступных членов выберите членов для добавления в группу, затем кликните Add. Выбранные члены будут перемещены в список Selected Members.

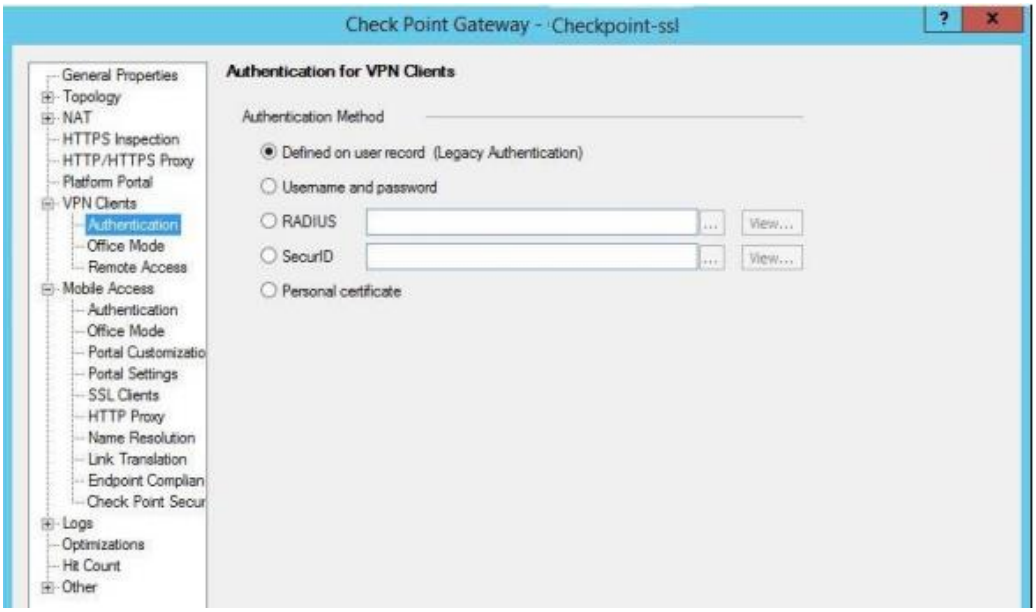


Разрешение аутентификации для клиентов VPN

- В главном окне Check Point SmartDashboard, под Network Objects, раскройте Check Point, правый клик по Вашему устройству, например, Checkpoint-ssl, затем клик по Edit.



- В окне Check Point Gateway – Checkpoint-ssl, раскройте VPN Clients, затем кликните Authentication.



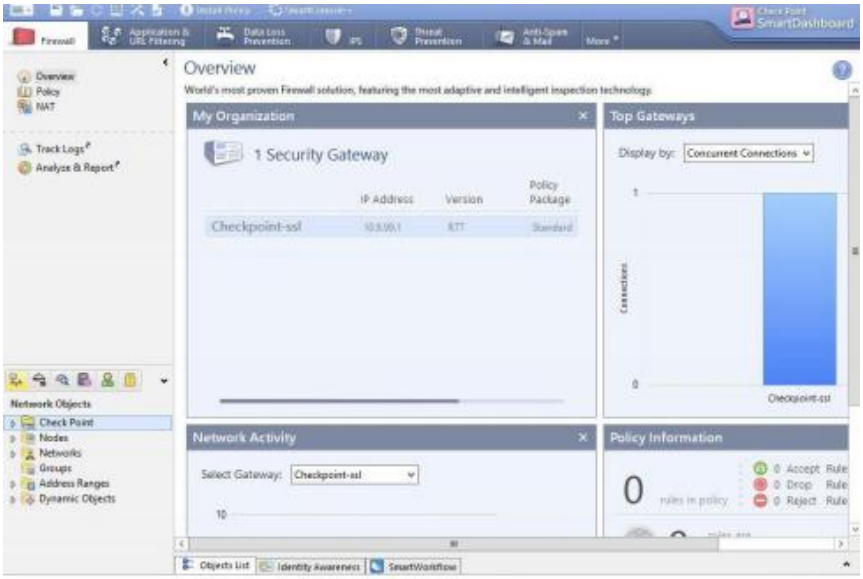
- В Authentication Method выберите Defined on user record (Legacy Authentication) и затем клик по OK.

Настройка правил фильтрации для VPN-клиентов

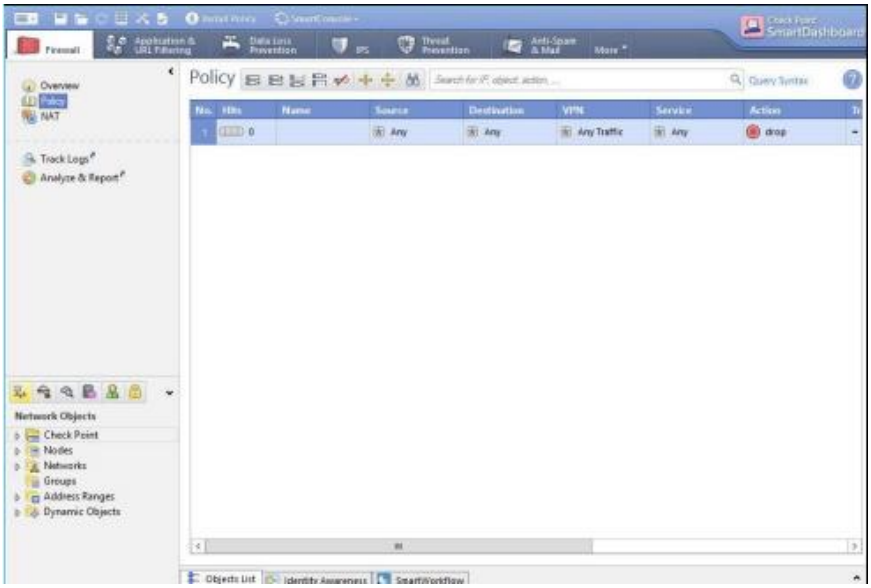
Шлюзы безопасности имеют, по крайней мере, одну аппаратную платформу, которая используется в качестве точки входа в корпоративную сеть.

Правила шлюза определяют политики разрешений и запретов для шлюза. Правила шлюза строятся на концепции объектов. Для примера, сетевые объекты могут быть использованы в качестве источника и пункта назначения правил.

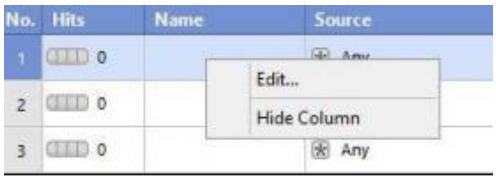
- В главном окне Check Point SmartDashboard кликните по Firewall.



- Кликните по Policy, затем по иконке Add rule at bottom. Строка добавится под меню Policy.

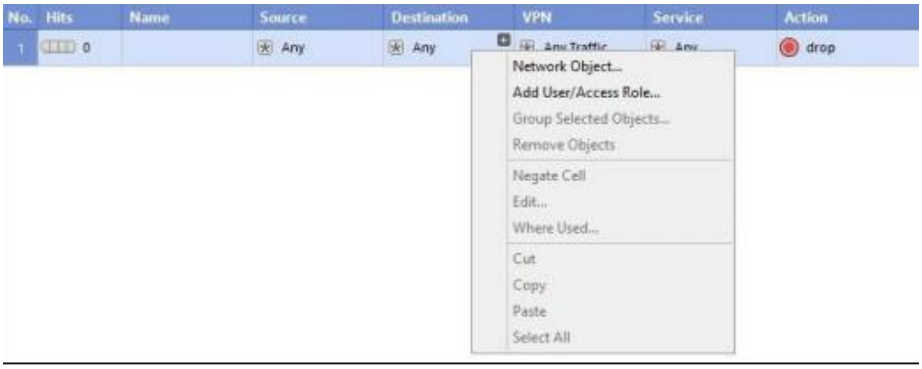


- В колонке Name - правый клик по новой строке и затем Edit.



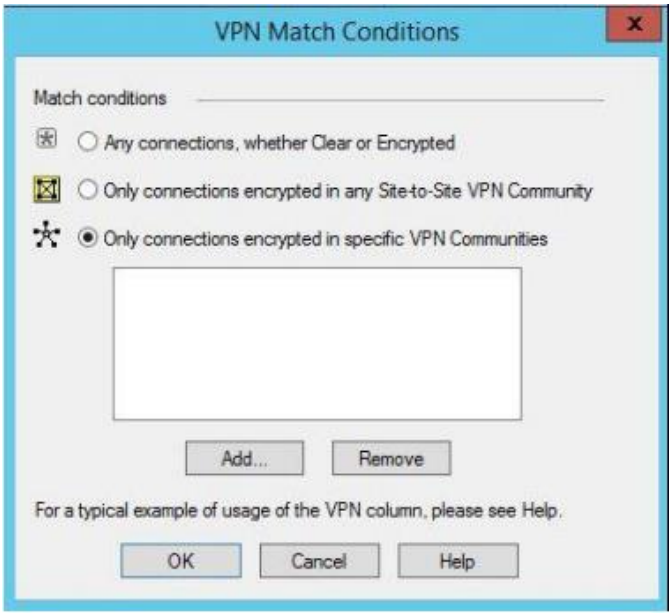
- В окне Rule Name в поле Rule Name добавьте имя для правила, затем кликните по ОК.

- В колонке Destination - правый клик по новой строке, затем клик по Network Object.

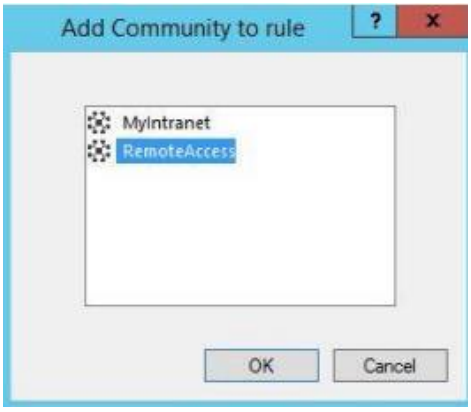


- В окне Add Object выбрать Internal_network. Internal_network - синоним к корпоративной сети предприятия.

- В колонке VPN - правый клик по новой строке, затем Edit Cell.
- В окне VPN Match Conditions выполните следующие шаги и нажмите ОК.
- Выбрать Only connections encrypted in specific VPN communities, нажать ADD.



- В окне Add Community to rule выбрать RemoteAccess и нажать ОК.

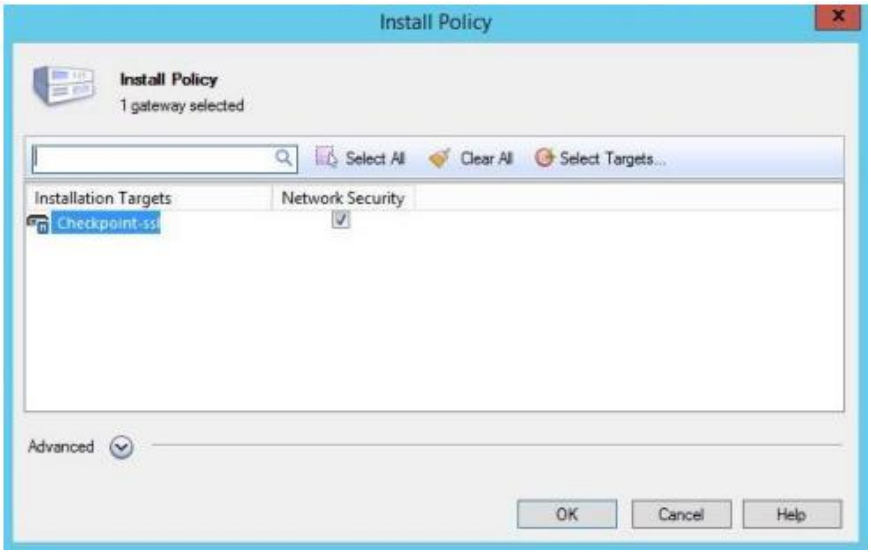


Новая политика создана.

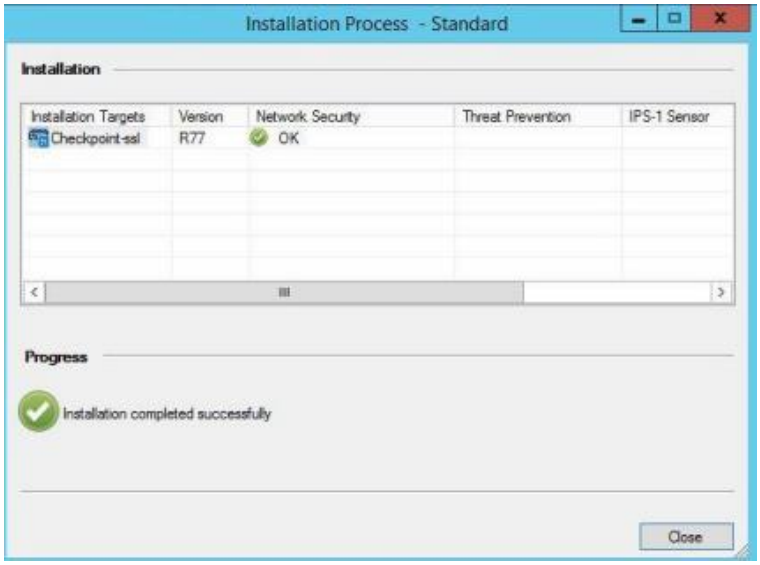
Установка политики

- Процесс установки политики приведён ниже.
- Провести эвристическую проверку правил для того, чтобы убедиться в совместимости и в неизбыточности правил.
- Подтвердить, что каждый шлюз безопасности, к которому будет применено правило, обеспечивает соблюдение, по крайней мере, одного правила.
- Преобразование Политики безопасности в скрипт контроля и скомпилировать этот скрипт в инспекционный код.
- Доставить инспекционный код на все выбранные объекты для доставки.
- В главном окне Check Point SmartDashboard - клик по Install Policy сверху (в меню).

- В окне Install Policy в колонке Network Security выбрать опции для требуемого устройства и кликнуть ОК.



- Когда политика установится, нажать Close.

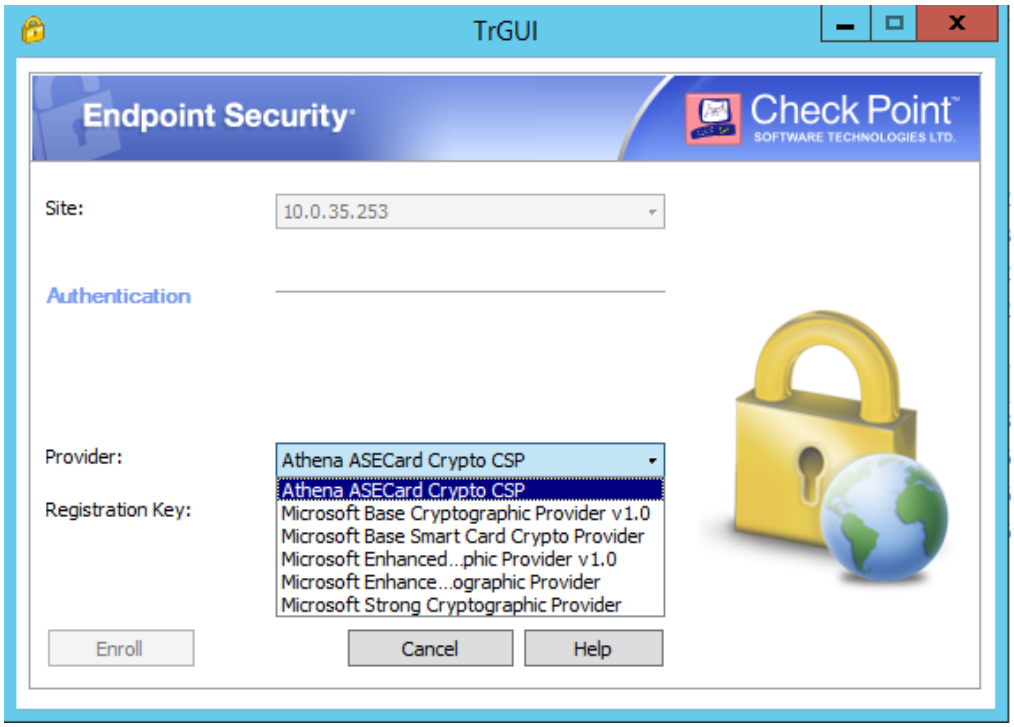


Установка сертификата

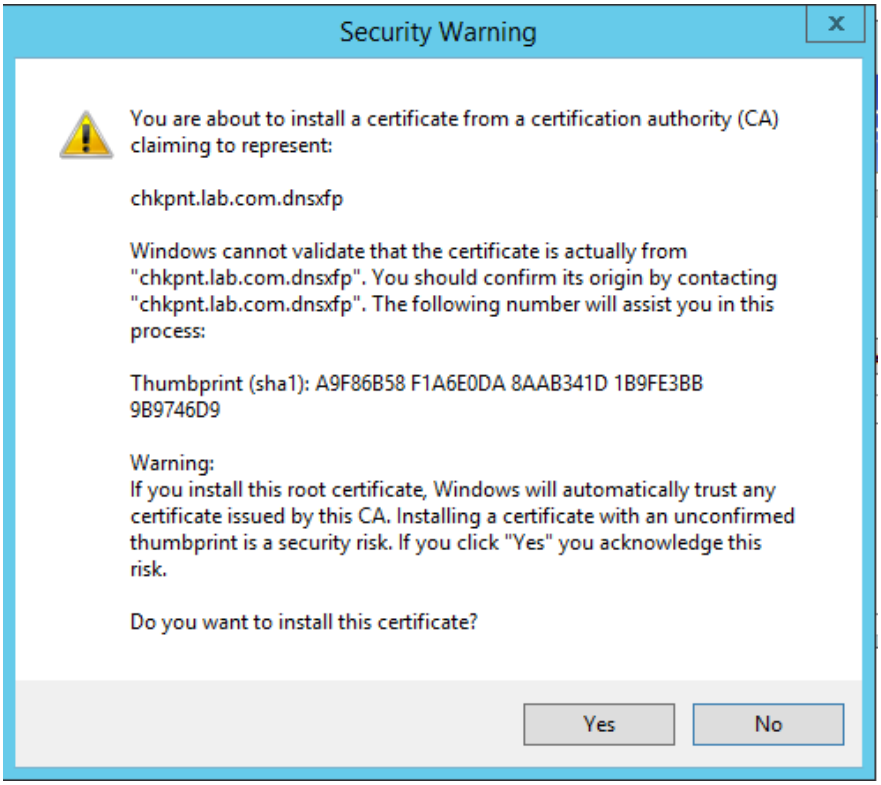
Клиент устанавливает защищённое соединение с внутренним Удостоверяющим центром Check Point, запрашивает сертификаты с помощью ключа регистрации. Запрашивая сертификат пользователя впервые, предоставьте ключ регистрации и установите сертификат на токен.

- Вставьте JaCarta PKI в слот USB, затем откройте приложение Check Point Endpoint Security.
- IP-адрес в поле Site тот же, что был введён в ходе установки. Также в ходе установки в качестве опции аутентификации были выбраны сертификаты. Клик по ссылке Click here if you don't have a certificate for this site.

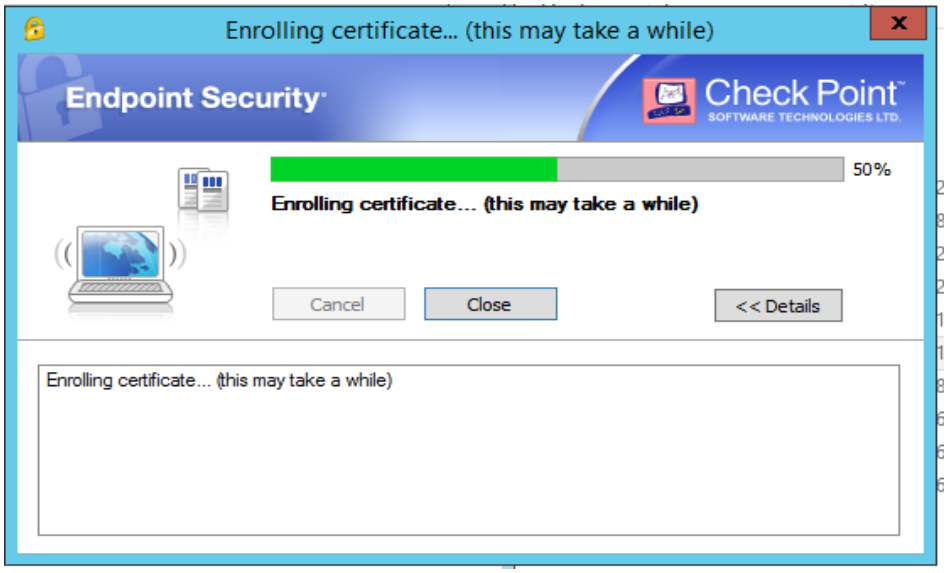
- В поле Provider выберите Athena Smart Card CSP.



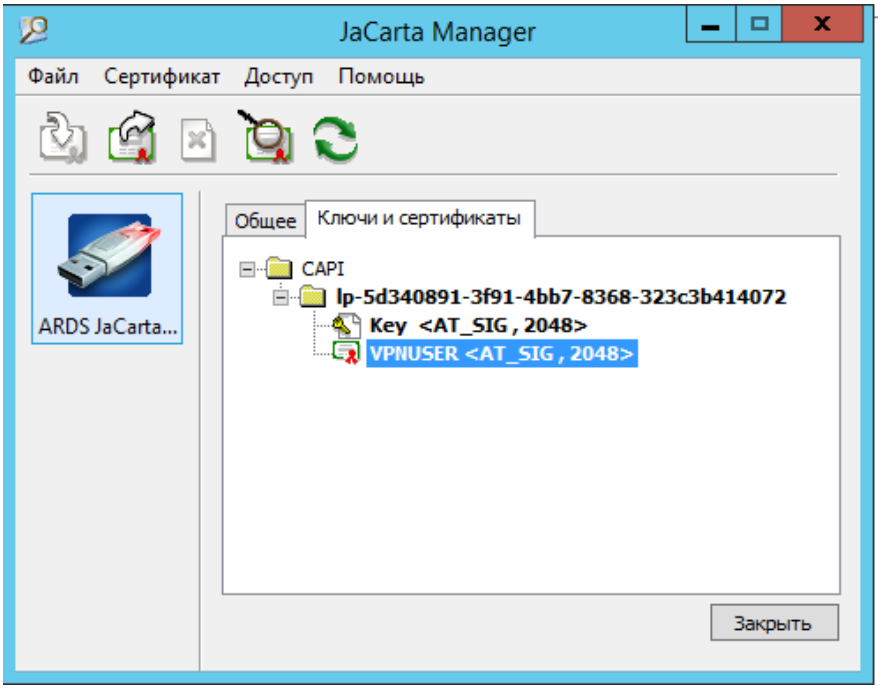
- В поле Registration Key введите сохранённый ранее ключ регистрации, нажмите Enroll.
- В окне Token Logon в поле Token Password введите PIN-код пользователя от используемой JaCarta PKI, затем нажмите ОК.
- Сообщение системы безопасности предложит установить новый корневой сертификат, нажмите YES. Данный сертификат принадлежит Удостоверяющему центру Check Point Internal.



- Когда установка завершится, нажмите ОК.



- Откройте JaCarta PKI Client и убедитесь в том, что сертификат был успешно выпущен.



Контроль за извлечением смарт-карты

- На шлюзе Check Point Gateway необходимо отредактировать файл

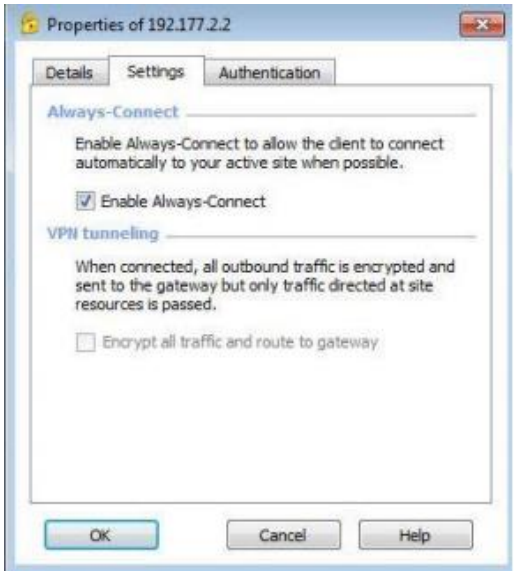
$FWDIR/conf/trac_client_1.ttm, используя редактор VI либо любой другой.

- Далее необходимо найти строку disconnect_on_smartcard_removal.

```
*:disconnect_on_smartcard_removal (
gateway (
 :default (true)
)
)*
```

- Изменить параметры по умолчанию в соответствии с требованиями:
  - 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.

- Далее необходимо сохранить файл и выйти из режима редактирования.
- Установить политику, используя Smart DashBoard.
- На компьютере, являющимся клиентским, откройте окно параметров Check Point Endpoint Security и поставьте галку напротив Enable always-connect.



Вход на шлюз

Откройте приложение Check Point Endpoint Security.

- Вставьте JaCarta PKI. Сертификаты на токене будут отображаться в поле Certificate. Нажмите Connect.

- В окне Token Logon в поле Password введите PIN-код от токена и нажмите OK.
- В панели задач кликните иконку VPN для просмотра статуса подключения. Когда аутентификация проходит успешно, статус соединения становится Connected.

Контакты, техническая поддержка

Офис (общие вопросы)

Адрес: 129226, Москва, ул. Докукина, д. 16, стр. 1, компания "Аладдин Р.Д."

Телефоны: +7 (495) 223-00-01 (многоканальный), +7 (495) 988-46-40

Факс: +7 (495) 646-08-82

E-mail: aladdin@aladdin-rd.ru (общий)

Web: www.aladdin-rd.ru

Время работы: ежедневно с 10:00 до 19:00, кроме выходных и праздничных дней.

Техподдержка

Служба техподдержки принимает запросы только в письменном виде через Web-сайт:

www.aladdin-rd.ru/support/index.php

Для оперативного решения Вашей проблемы укажите используемый Вами продукт, его версию, подробно опишите условия и сценарии применения, по возможности, снабдите сообщение снимками экрана, примерами исходного кода.

Регистрация изменений

Версия	Изменения
1.0	Исходная версия документа

Лицензии ФСТЭК России № 0037 и № 0054 от 18.02.03, № 2874 от 18.05.12
Лицензии ФСБ России № 12632 Н от 20.12.12, № 24530 от 25.02.14
Система менеджмента качества компании соответствует требованиям стандарта ISO/ИСО 9001-2011
Сертификат СМК ГОСТ Р ИСО 9001-2011 № РОСС RU.ИС72.К00082 от 10.07.15
Apple Developer

Тел. +7 (495) 223-00-01 Email: aladdin@aladdin-rd.ru Web: www.aladdin-rd.ru