Конфигурация VPN для удаленного доступа AnyConnect на FTD

Содержание

Введение

Этот документ предоставляет пример конфигурации для версии 6.2.2 Защиты угрозы огневой мощи (FTD) и позже, который позволяет VPN для удаленного доступа использовать Transport Layer Security (TLS) и вторую версию протокола Internet Key Exchange (IKEv2). Как клиент, будет использоваться AnyConnect Cisco, который поддерживается на нескольких платформ.

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Основная VPN, TLS и знание IKEv2
- Базовая проверка подлинности, Авторизация, и Бухгалтерский (AAA) и знание RADIUS
- Опыт с центром управления огневой мощи

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Cisco FTD 6.2.2
- AnyConnect 4.5

!--- конфигурацию

1. Preresiquites

Для прохождения через мастера Удаленного доступа в Центре управления Огневой мощи сначала необходимо будет выполнить эти действия:

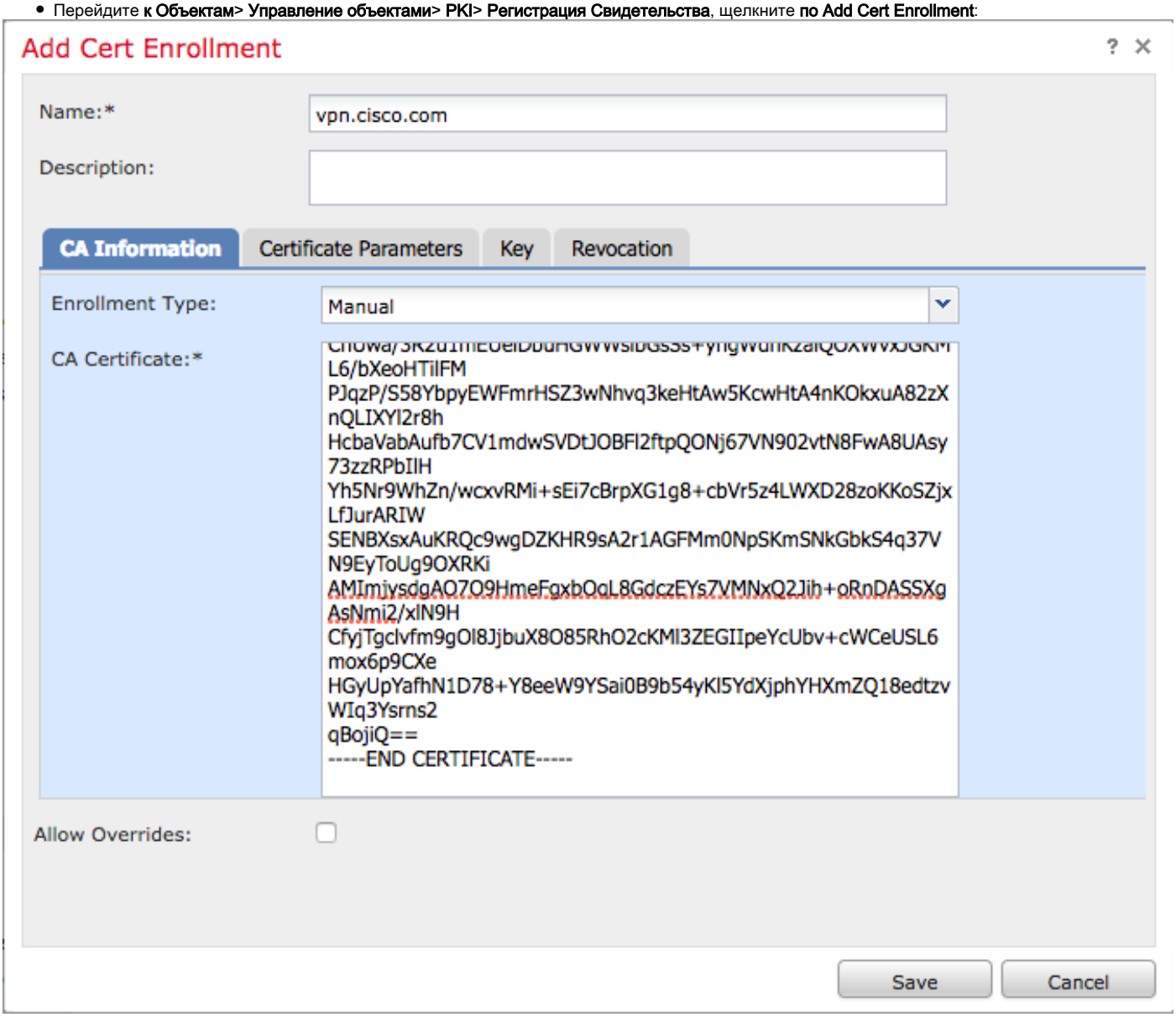
- создайте сертификат, используемый для проверки подлинности сервера,
- настройте RADIUS или Сервер LDAP для проверки подлинности пользователя,
- создайте пул адресов для пользователей VPN,
- AnyConnect загрузки отображает для других платформ.

a) импорт сертификата SSL

Сертификаты важны при настройке AnyConnect. Только RSA базировался, сертификаты поддерживаются в SSL и IPSec. Сертификаты Алгоритма цифровой подписи Эллиптической кривой (ECDSA) поддерживаются в IPSec, но не возможно развернуть новый пакет AnyConnect или профиль XML, когда ECDSA базировался, сертификат используется. Это означает, что можно использовать его для IPSec, но необходимо будет предварительно развернуть пакет AnyConnect и профиль XML каждому пользователю, и любое изменение в профиле XML должно будет быть вручную отражено на каждом клиенте (дефект: CSCtx42595). Дополнительно сертификат должен иметь расширение Альтернативного имени субъекта с именем DNS и/или IP-адресом для предотвращения ошибок в web-браузерах.

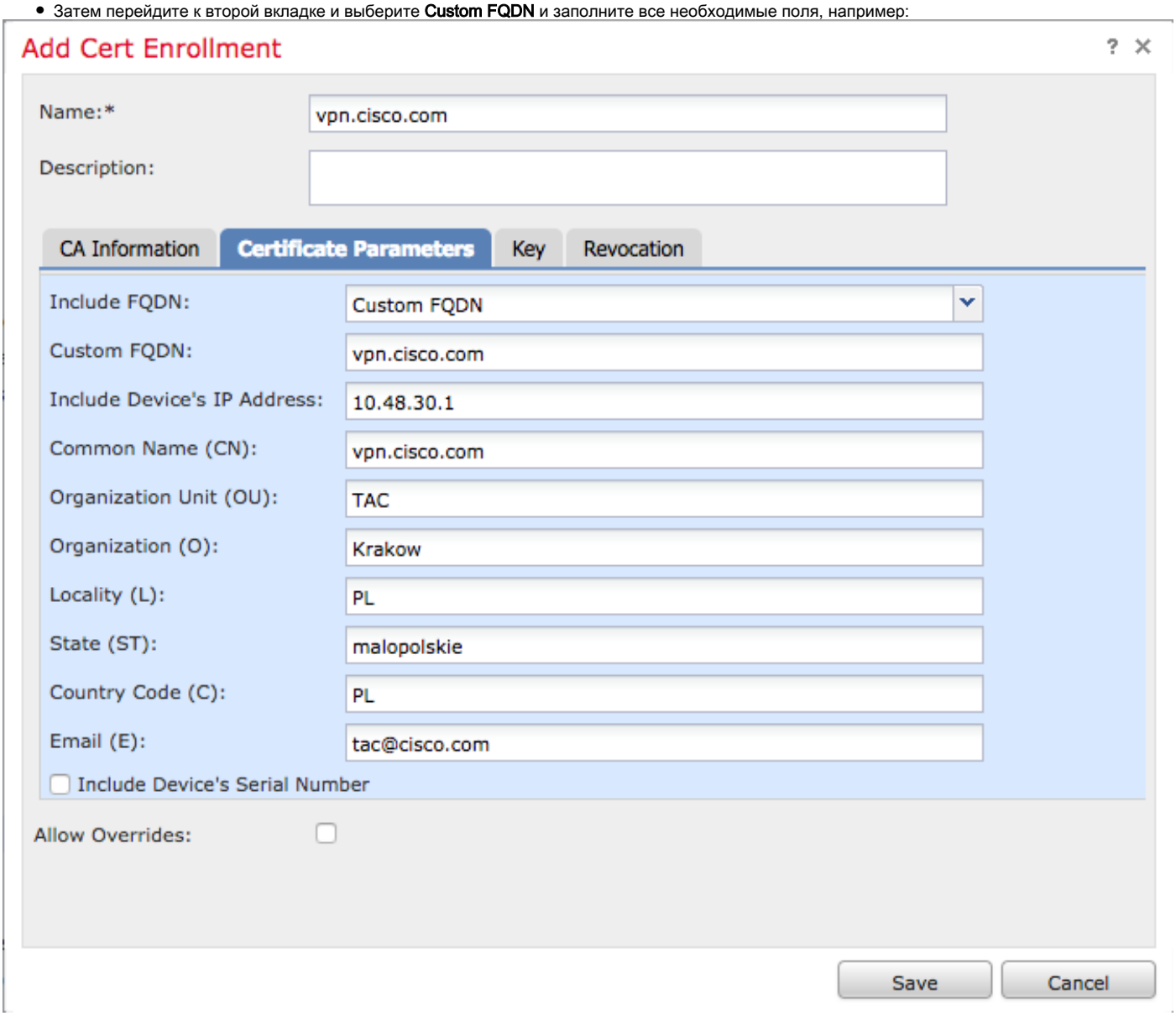
Существует несколько методов для получения сертификата на устройстве FTD, но безопасный и легкий должен создать Запрос подписи сертификата (CSR), подписать его и затем сертификат импорта, выполненный для открытого ключа, который был в CSR. Вот то, как сделать это:

- Перейдите **к Объектам> Управление объектами> PKI> Регистрация Свидетельства**, щелкните **по Add Cert Enrollment**:

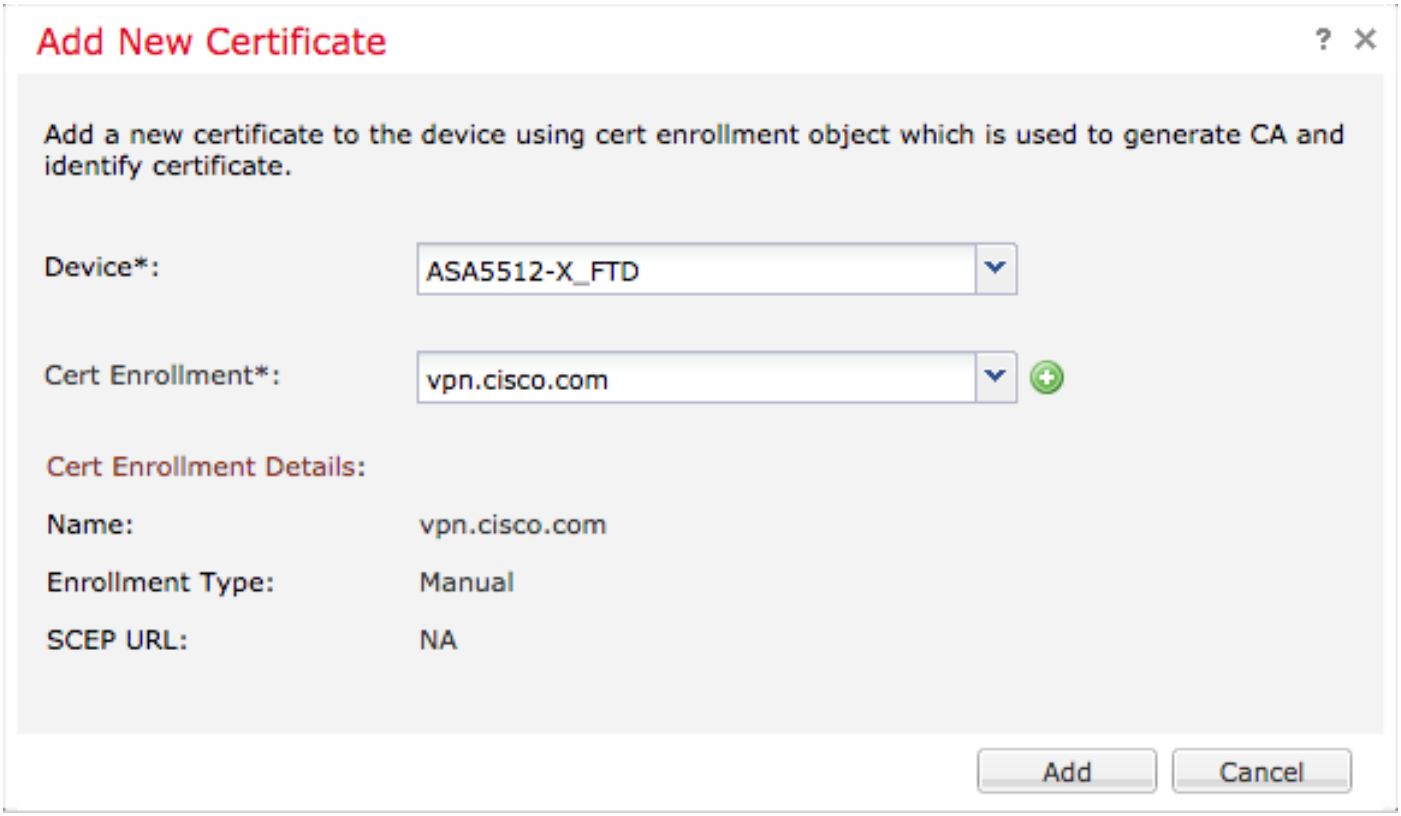


- Выберите **Enrollment Type** и вставьте сертификат Центра сертификации (CA),

- Затем перейдите к второй вкладке и выберите **Custom FQDN** и заполните все необходимые поля, например:



- На третьей вкладке выберите ключевой тип, выберите название и размер. Для RSA 2048 байтов минимальны.
- Нажмите сохраняют и переходят **к Устройствам>, Сертификаты> Добавляют> Новый Сертификат**. Затем выберите **Device,** и в соответствии со **Свидетельством Регистрация** выбирает и точка доверия, которую вы просто создали, **нажмите Add**:



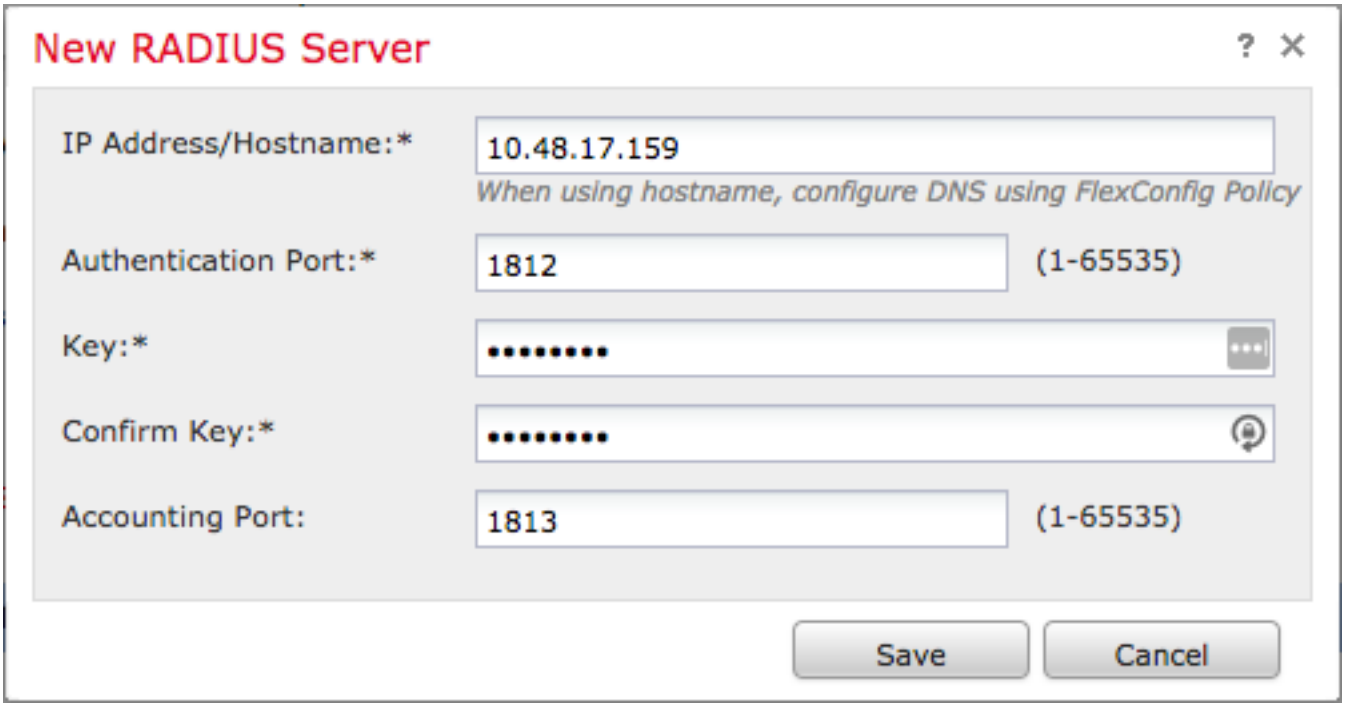
- Позже, рядом с названием точки доверия, щелкните по значку, тогда **Да** и после того CSR копии к CA и подпишите его. Сертификат должен иметь атрибуты как обычный сервер HTTPS.
- После получения сертификата от CA в формате base64 выберите его от диска и нажмите **Import**. Когда это успешно выполняется, необходимо видеть:

Name	Enrollment Type	CA Certificate	Identity Certificate
ASA5512-X_FTD			
vpn.cisco.com	Manual	Available	Available

b) настройте сервер RADIUS

На FTD platftorm, не может использоваться база локальных пользователей, таким образом, вам нужны RADIUS или Сервер LDAP для проверки подлинности пользователя. Настраивать RADIUS:

- Перейдите **к Объектам> Управление объектами> RADIUS Server Group> Add RADIUS Server Group**.
- Заполните название и добавьте IP-адрес наряду с общим секретным ключом, нажмите **Save**:

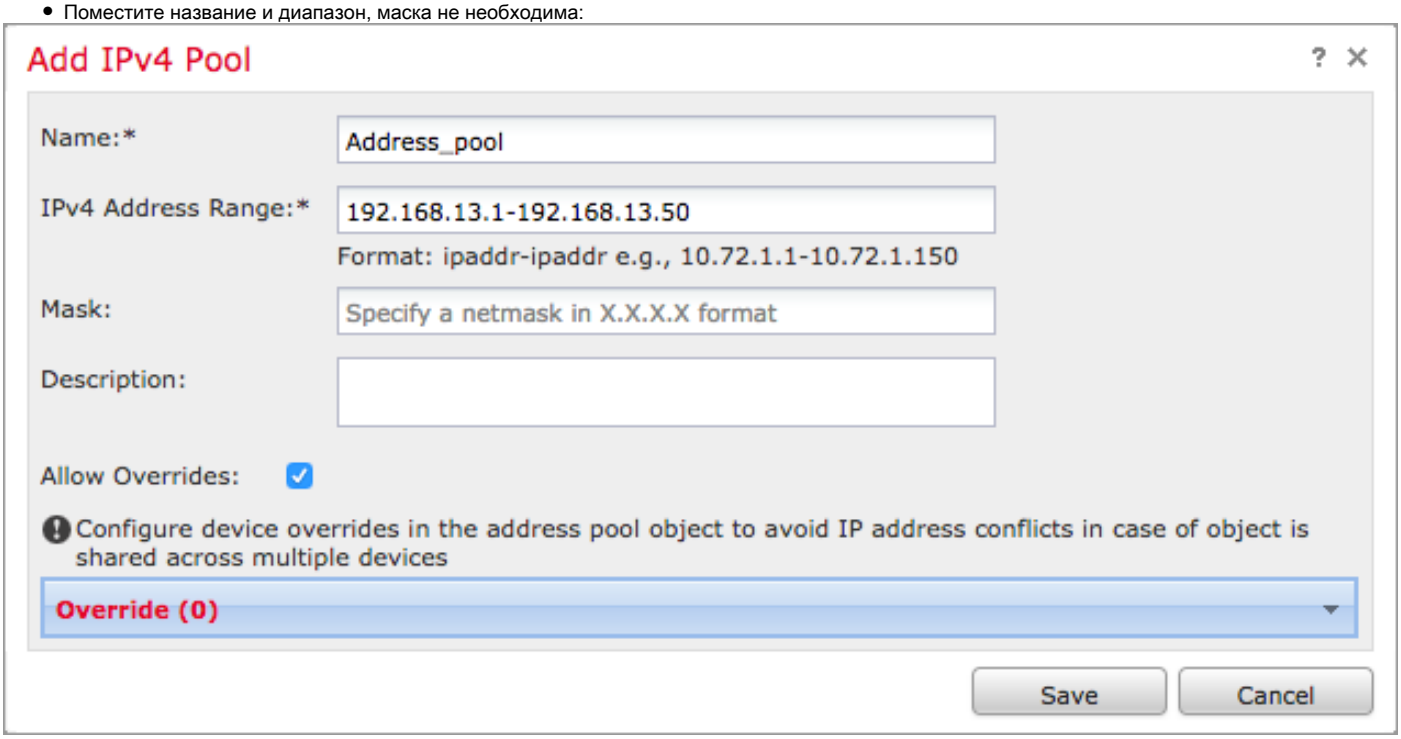


- После этого необходимо видеть сервер в списке:

Name	Value	Override
ISE	1 Server	✖

c) создание пула адресов для пользователей VPN

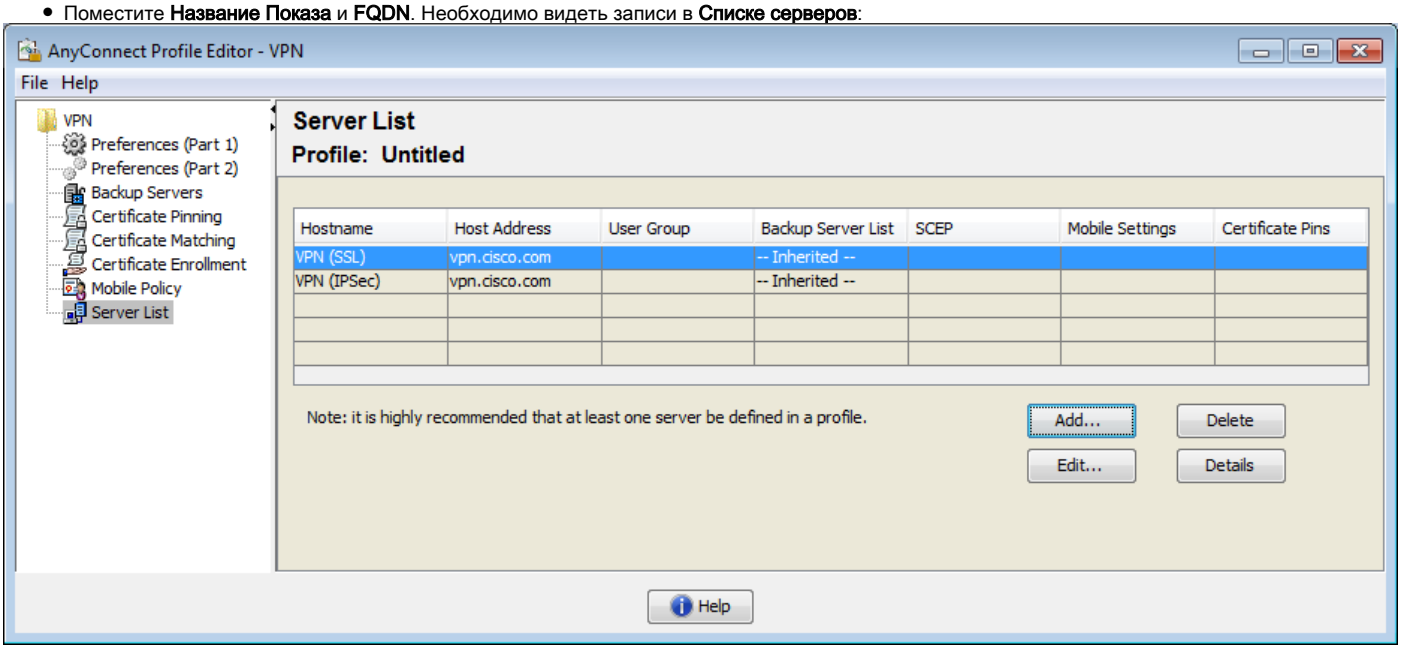
- Перейдите **к Объектам> Управление объектами>, Пулы адресов> Добавляют Пулы IPv4**:
- Поместите название и диапазон, маска не необходима:



d) создание профиля XML

- Редактор Профиля загрузки от узла Cisco и открытый это.
- Перейдите **к Списку серверов>, Добавляют...**

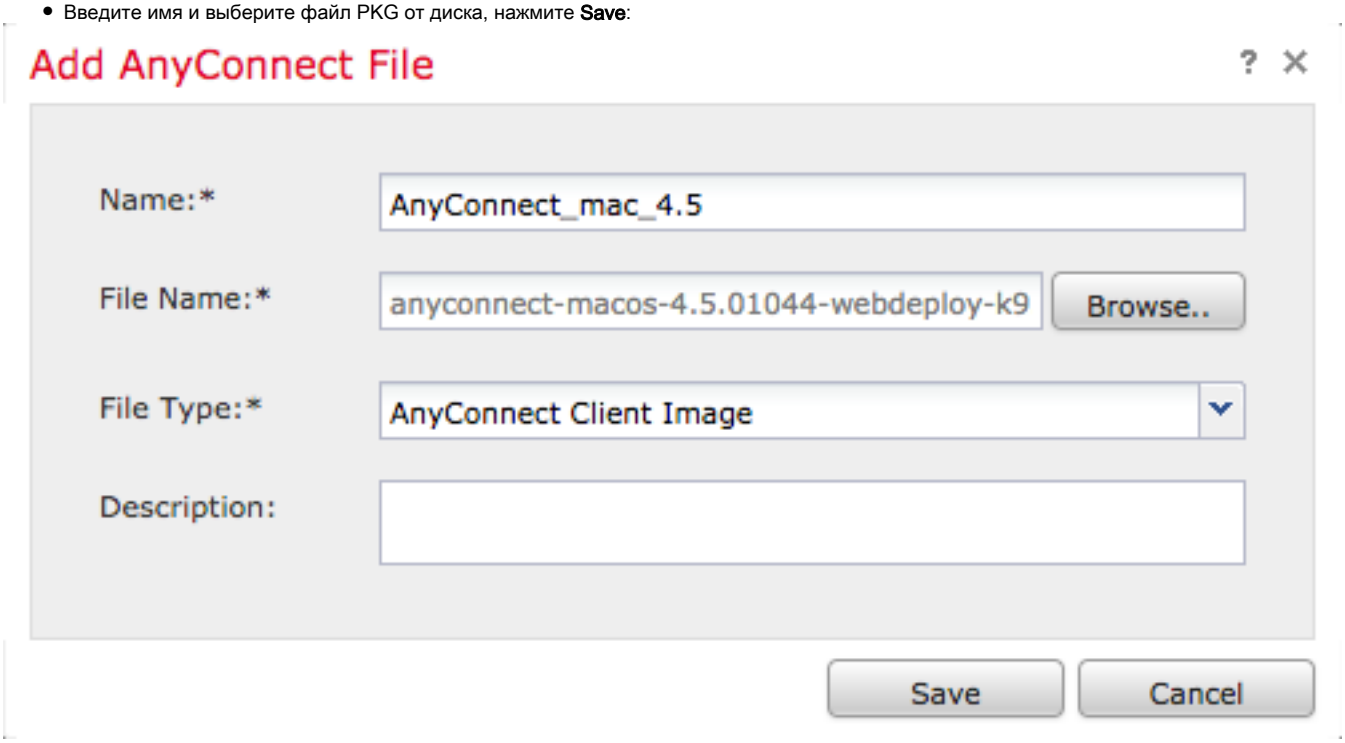
- Поместите **Название Показа** и **FQDN**. Необходимо видеть записи в **Списке серверов**:



- Нажмите **OK** и **File> Save as...**

e) загрузка образов AnyConnect

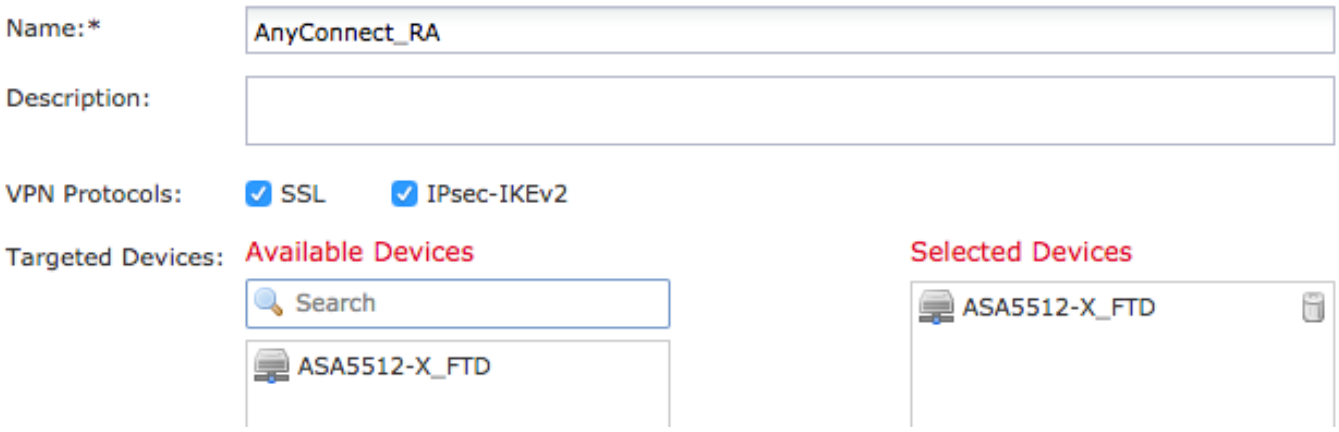
- Загрузите образы pkg от узла Cisco.
- Перейдите **к Объектам> Управление объектами> VPN>, Файл AnyConnect> Добавляет Файл AnyConnect**.
- Введите имя и выберите файл PKG от диска, нажмите **Save**:



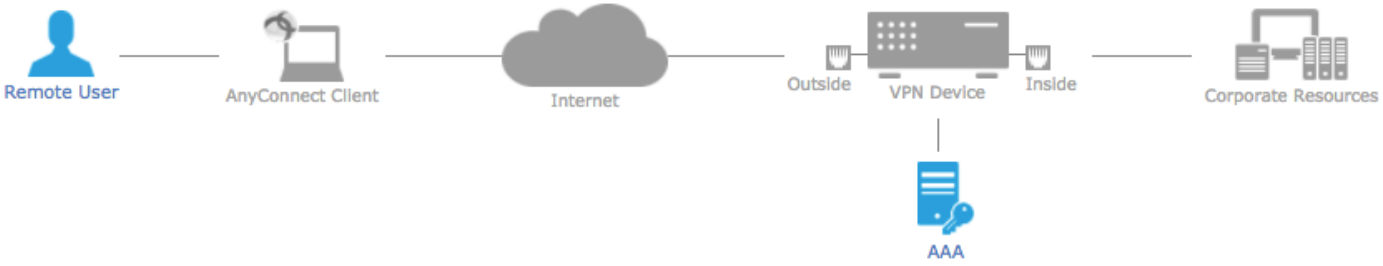
- Добавьте больше пакетов в зависимости от своих требований.

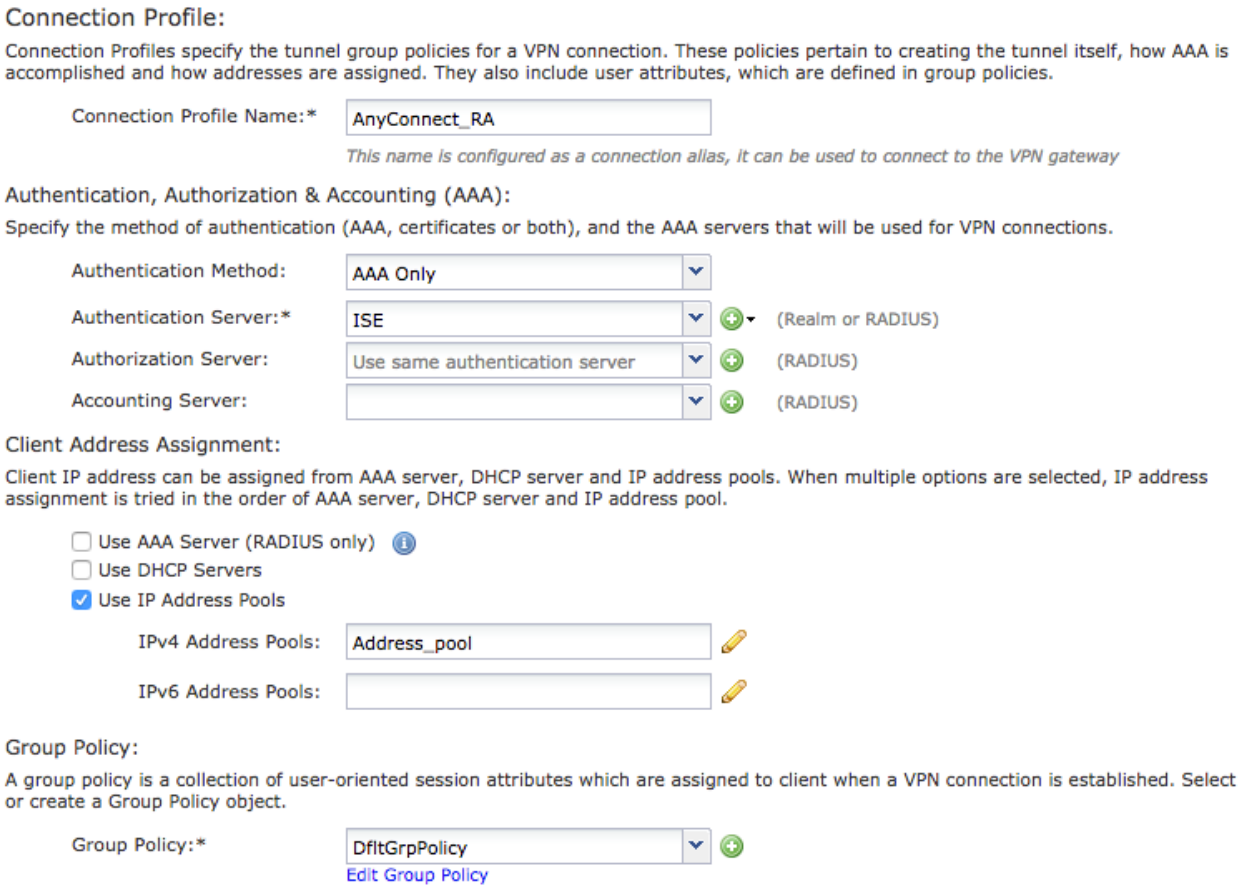
2. Мастер удаленного доступа:

- Перейдите **к Устройствам> VPN>, Удаленный доступ> Добавляет новую конфигурацию**.
- Назовите профиль согласно своим потребностям, выберите устройство FTD:

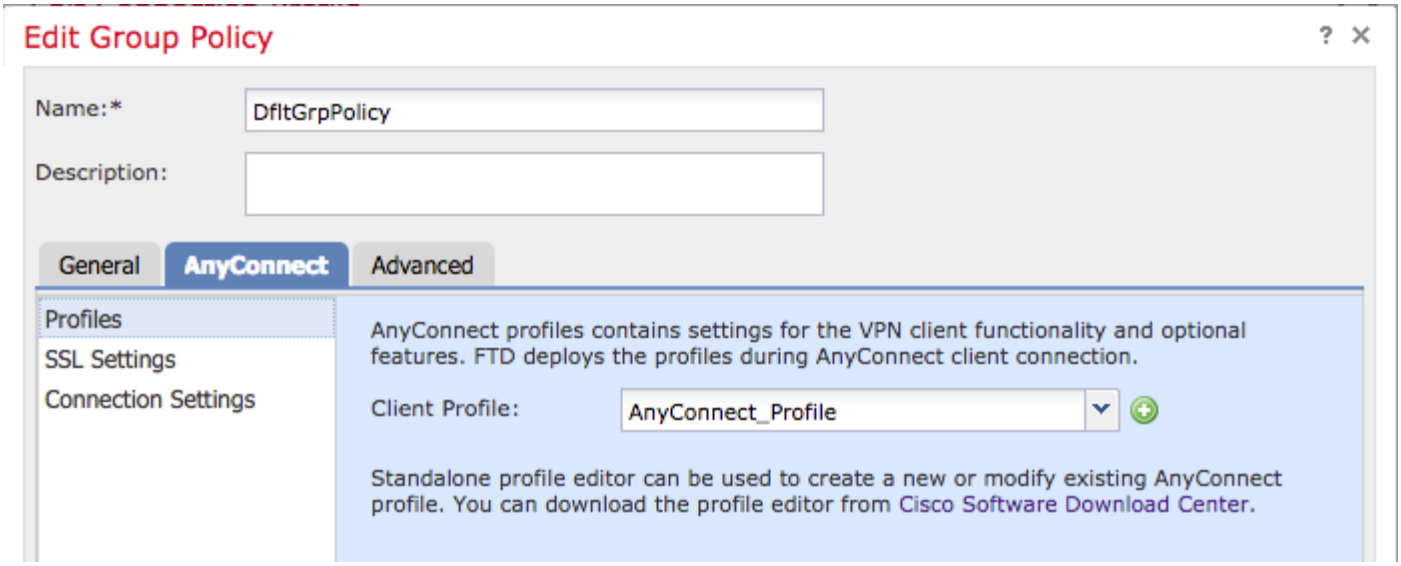


- В **Профиле подключения** шага введите **Имя Профиля подключения**, выберите **Authentication Server** и **Address Pools**, который вы создали ранее:

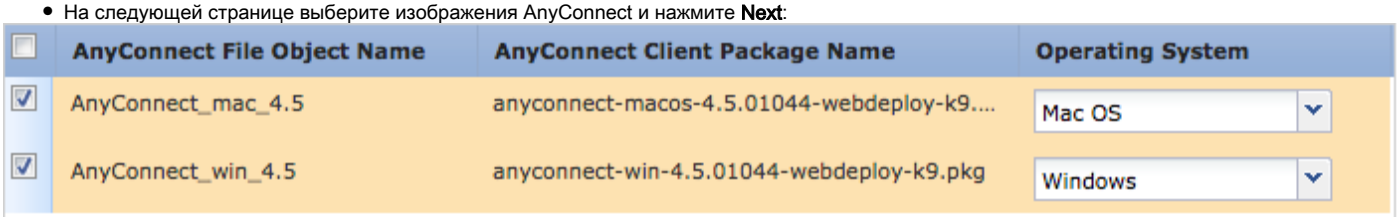




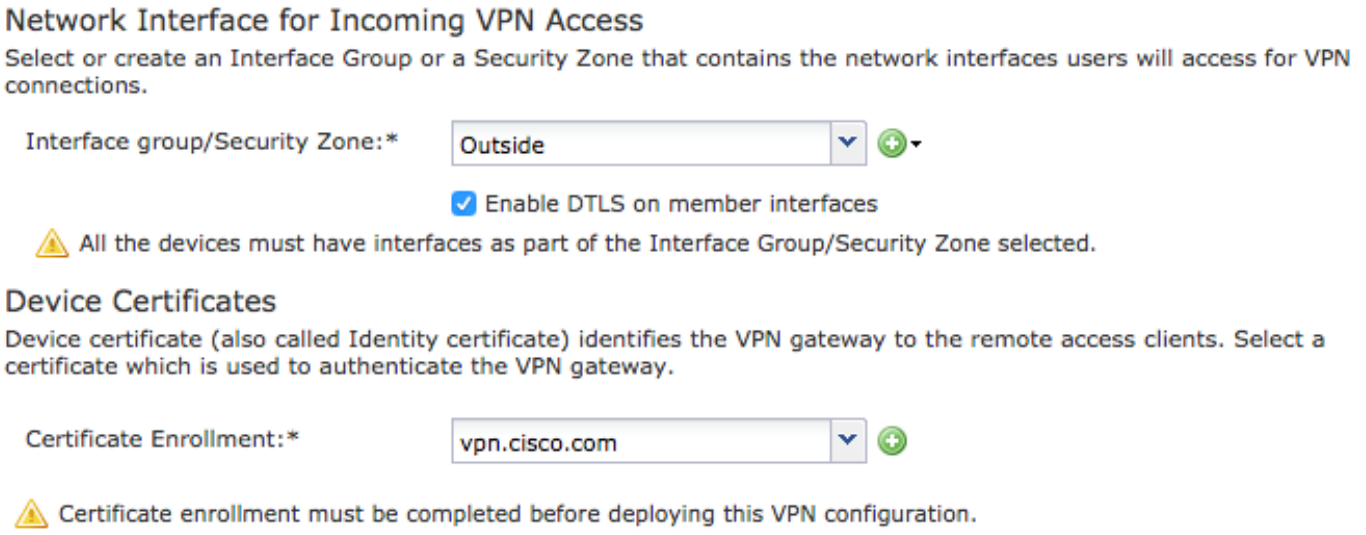
- Щелкните **по Edit Group Policy** и на **вкладке AnyConnect**, выберите **Client Profile**, затем нажмите **Save**:



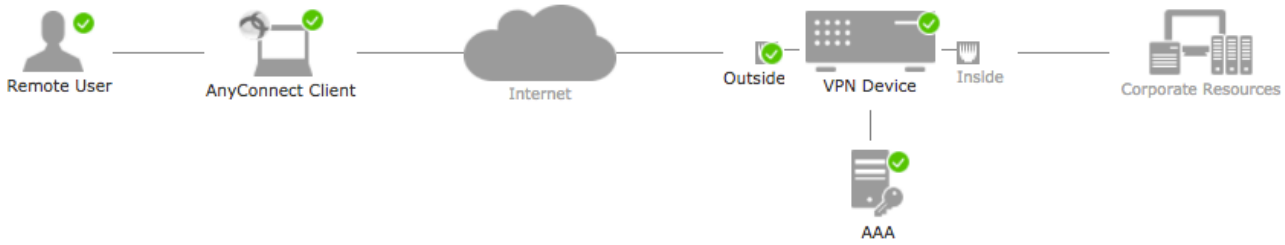
- На следующей странице выберите изображения AnyConnect и нажмите **Next**:



- На следующем экране выберите **Network Interface** и **DeviceCertificates**:



- Когда все настроено правильно, можно нажать **Finish** и затем **Развернуться**:



Remote Access VPN Policy Configuration

Firepower Management Center will configure an RA VPN Policy with the following settings

Name:	AnyConnect_RA
Device Targets:	ASA5512-X_FTD
Connection Profile:	AnyConnect_RA
Connection Alias:	AnyConnect_RA
AAA:	
Authentication Method:	AAA Only
Authentication Server:	ISE
Authorization Server:	ISE
Accounting Server:	–
Address Assignment:	
Address from AAA:	–
DHCP Servers:	–
Address Pools (IPv4):	Address_pool
Address Pools (IPv6):	–
Group Policy:	DfltGrpPolicy
AnyConnect Images:	AnyConnect_mac_4.5 AnyConnect_win_4.5
Interface Objects:	Outside
Device Certificates:	vpn.cisco.com

Additional Configuration Requirements

After the wizard completes, the following configuration needs to be completed for VPN to work on all device targets.

Access Control Policy Update
An *Access Control* rule must be defined to allow VPN traffic on all targeted devices.

NAT Exemption
If NAT is enabled on the targeted devices, you must define a *NAT rule* to exempt VPN traffic.

DNS Configuration
To resolve hostname specified in AAA Servers or CA Servers, configure DNS using *FlexConfig Policy* on the targeted devices.

Network Interface Configuration
Make sure to add interface from targeted devices to SecurityZone object 'Outside'

Device Identity Certificate Enrollment
Make sure to install identity certificate on targeted devices using PKI Cert object 'vpn.cisco.com'

- Это скопирует целую конфигурацию наряду с сертификатами и пакетами AnyConnect к устройству FTD.

Соединение

Для соединения с FTD, необходимо открыть браузер, ввести имя DNS или IP-адрес, указывающий на внешний интерфейс, в данном примере *https://vpn. cisco . com*. Необходимо будет тогда войти с помощью учетных данных, сохраненных в сервере RADIUS, и следовать инструкциям на экране. Как только AnyConnect устанавливает, тогда необходимо поместить тот же адрес в окно AnyConnect и нажать **Connect**.

Ограничения

В настоящее время неподдерживаемый на FTD, но доступный на ASA:

- Двойная аутентификация AAA (проверка подлинности, авторизация и учет)
- Политика динамического доступа
- Просмотр хоста
- Положение ISE
- Балансировщик загрузки VPN
- Локальная проверка подлинности (Усовершенствование: CSCvf92680)
- Карта атрибутов LDAP
- Маркерная аутентификация RSA
- Кастомизация AnyConnect
- Сценарии AnyConnect

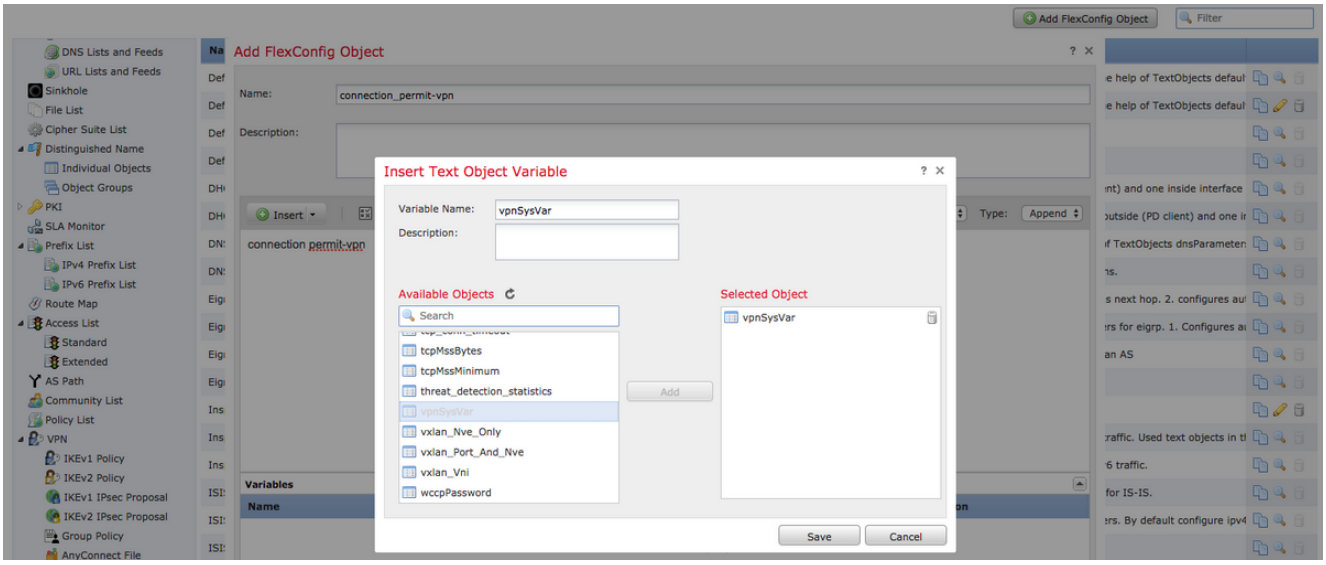
- Локализация AnyConnect
- VPN на приложение
- Прокси SCEP
- Интеграция WSA
- SSO SAML
- Одновременная динамическая криптокарта IKEv2 для RA и VPN L2L

Устаревшие опции

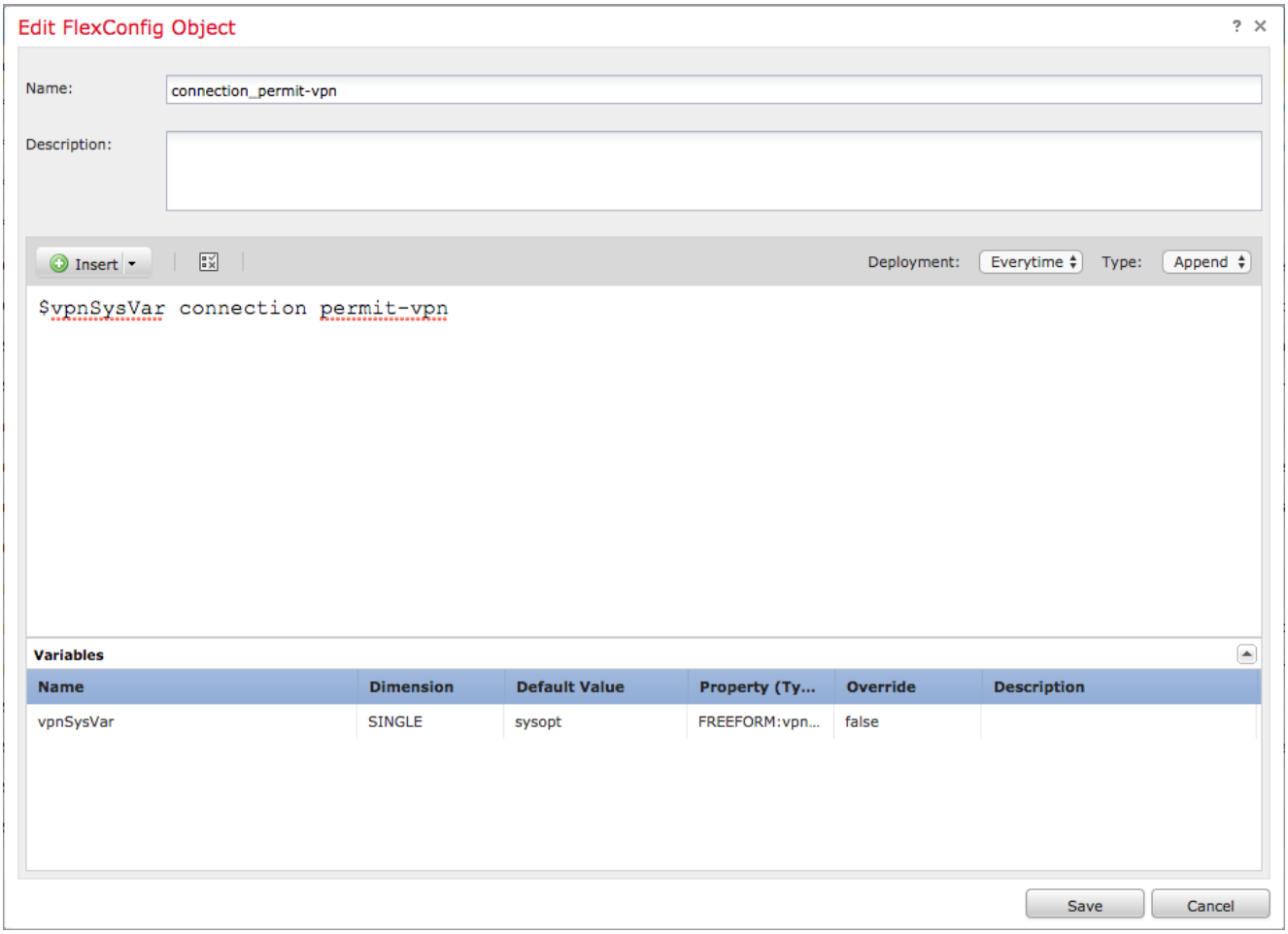
Необходимо помнить, что по умолчанию, отключена опция sysopt connection permit-vpn. Это означает, что необходимо позволить трафик , прибывающий из пула адресов на внешнем интерфейсе с помощью Политики контроля доступа. Несмотря на то, что правило предварительного фильтра или контроля доступа добавлено, намереваясь позволить трафик VPN только, если трафик открытого текста, оказывается, совпадает с критериями правила, это ошибочно разрешено.

Можно все еще включить опцию sysopt connection permit-vpn:

1. Перейдите **к Объектам> Управление объектами> FlexConfig>, Текстовый объект> Добавляет Текстовый объект**.
2. Создайте переменную текстового объекта, например: `vpnSysVar` одиночная запись со значением `"sysopt"`
3. Перейдите **к Объектам > Управление объектами > FlexConfig > , Объект FlexConfig > Добавляет Объект FlexConfig**.
4. Создайте объект FlexConfig с CLI `"vpn разрешения соединения"`:
5. Вставьте переменную текстового объекта в объект flexconfig в начале CLI как `"vpn разрешения соединения $vpnSysVar"`, нажимает **Save:**



6. Примените объект FlexConfig, как **Добавляют** и выбирают развертывания к **Каждый раз**:



7. Перейдите **к Устройствам> FlexConfig** и отредактируйте существующую политику или создайте новую с **Новой кнопкой Policy**.
8. Добавьте просто создал FlexConfig, нажмите **Save**.
9. Разверните конфигурацию для инициализации команды "sysopt connection permit-vpn" на устройстве.

Это, однако, удалит возможность использовать Политику контроля доступа для осмотра трафика, прибывающего от пользователей. Можно все еще использовать фильтр VPN или загружаемый список ACL для фильтрации трафика пользователя.