ASA 8. X: Пример конфигурации регистрации SCEP AnyConnect

Содержание

Введение

Функциональность регистрации SCEP введена в версии 2.4 автономного клиента AnyConnect. В этом процессе вы модифицируете профиль XML AnyConnect, чтобы включать связанную с SCEP конфигурацию и создать определенную групповую политику и профиль подключения для хранилища сертификатов. Когда пользователь AnyConnect соединяется с этой определенной группой, AnyConnect отправляет запрос хранилища сертификатов к серверу CA, и сервер CA автоматически принимает или запрещает запрос.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

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

- Многофункциональные устройства защиты Cisco ASA серии 5500, которые работают под управлением ПО версии 8. x
- Версия VPN 2.4 AnyConnect Cisco

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Условные обозначения

Более подробную информацию о применяемых в документе обозначениях см. в описании условных обозначений, используемых в технической документации Cisco.

Общие сведения

Цель Автоматической регистрации SCEP на AnyConnect состоит в том, чтобы выполнить сертификат клиенту безопасным и масштабируемым способом. Например, пользователи не должны запрашивать сертификат от сервера CA. Эта функциональность интегрирована в клиенте AnyConnect. Сертификаты выполнены клиентам на основе параметров сертификата, упомянутых в файле конфигурации XML.

Обзор требуемых изменений

Функция регистрации SCEP AnyConnect требует, чтобы определенные параметры сертификата были определены в профиле XML. Групповая политика и Профиль подключения созданы на ASA для хранилища сертификатов, и профиль XML привязан к той политике. Клиент AnyConnect соединяется с Профилем подключения, который использует эту определенную политику и отправляет запрос для сертификата с параметрами, которые определены в XML-файле. Центр сертификации (CA) автоматически принимает или запрещает запрос. Если элемент <CertificateSCEP> определен в клиентском профиле, клиент AnyConnect получает сертификаты с Протоколом SCEP.

Аутентификация сертификата клиента должна отказать, прежде чем AnyConnect пытается автоматически получить новые сертификаты, поэтому если вам уже установили подтвержденный сертификат, регистрация не происходит.

Когда пользователи входят определенной группе, они автоматически зарегистрированы. Существует также ручной способ, доступный для извлечения сертификата, в котором пользователям предоставляют кнопку **Get Certificate**. Когда у клиента есть прямой доступ к серверу CA, не через туннель, это только работает.

См. руководство для администратора клиента VPN Cisco AnyConnect, Выпуск 2.4 для получения дополнительной информации.

Параметры настройки XML для активации опции SCEP Anyconnect

Это важные элементы, которые должны быть определены в XML-файле AnyConnect. См. руководство для администратора клиента VPN Cisco AnyConnect, Выпуск 2.4 для получения дополнительной информации.

- <AutomaticSCEPHost> — Задает имя хоста ASA и профиль подключения (туннельная

группа), для которой настроено извлечение сертификата SCEP. Значение должно быть в формате полного доменного имени имени профиля ASA\connection или IP-адреса имени профиля ASA\connection.
- <CAURL> — Определяет SCEP CA сервер.
- <CertificateSCEP> — Определяет, как запрашивают содержание сертификата.
- <DisplayGetCertButton> — Определяет, отображает ли GUI AnyConnect кнопку Get Certificate. Это позволяет пользователям вручную запросить обновление или инициализацию сертификата.

Вот профиль в качестве примера:

```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/AnyConnectProfile.xsd">
<ClientInitialization>
<UseStartBeforeLogon UserControllable="true">false</UseStartBeforeLogon>
<AutomaticCertSelection UserControllable="true">true</AutomaticCertSelection>
<ShowPreConnectMessage>false</ShowPreConnectMessage>
<CertificateStore>All</CertificateStore>
<CertificateStoreOverride>false</CertificateStoreOverride>
<ProxySettings>Native</ProxySettings>
<AutoConnectOnStart UserControllable="true">true</AutoConnectOnStart>
<MinimizeOnConnect UserControllable="true">true</MinimizeOnConnect>
<LocalLanAccess UserControllable="true">false</LocalLanAccess>
<AutoReconnect UserControllable="false">true
<AutoReconnectBehavior UserControllable="false">
     ReconnectAfterResume
   </AutoReconnectBehavior>
</AutoReconnect>
<AutoUpdate UserControllable="false">true</AutoUpdate>
<RSASecurIDIntegration UserControllable="false">
    Automatic
  </RSASecurIDIntegration>
<WindowsLogonEnforcement>SingleLocalLogon</WindowsLogonEnforcement>
<WindowsVPNEstablishment>AllowRemoteUsers</WindowsVPNEstablishment>
<AutomaticVPNPolicy>false</AutomaticVPNPolicy>
<PPPExclusion UserControllable="false">Automatic
<PPPExclusionServerIP UserControllable="false"></PPPExclusionServerIP>
</PPPExclusion>
<EnableScripting UserControllable="false">false</EnableScripting>
<CertificateEnrollment>
<AutomaticSCEPHost>asa2.cisco.com/certenroll</AutomaticSCEPHost>
<CAURL PromptForChallengePW="false">
     http://10.11.11.1/certsrv/mscep/mscep.dll
   </CAURL>
<CertificateSCEP>
<Name_CN>cisco</Name_CN>
<Company_O>Cisco</Company_O>
<DisplayGetCertButton>true</DisplayGetCertButton>
</CertificateSCEP>
</CertificateEnrollment>
</ClientInitialization>
<ServerList>
<HostEntry>
<HostName>asa2.cisco.com</HostName>
</HostEntry>
</ServerList>
</AnyConnectProfile>
```

Настройте ASA для поддержки протокола SCEP для

AnyConnect

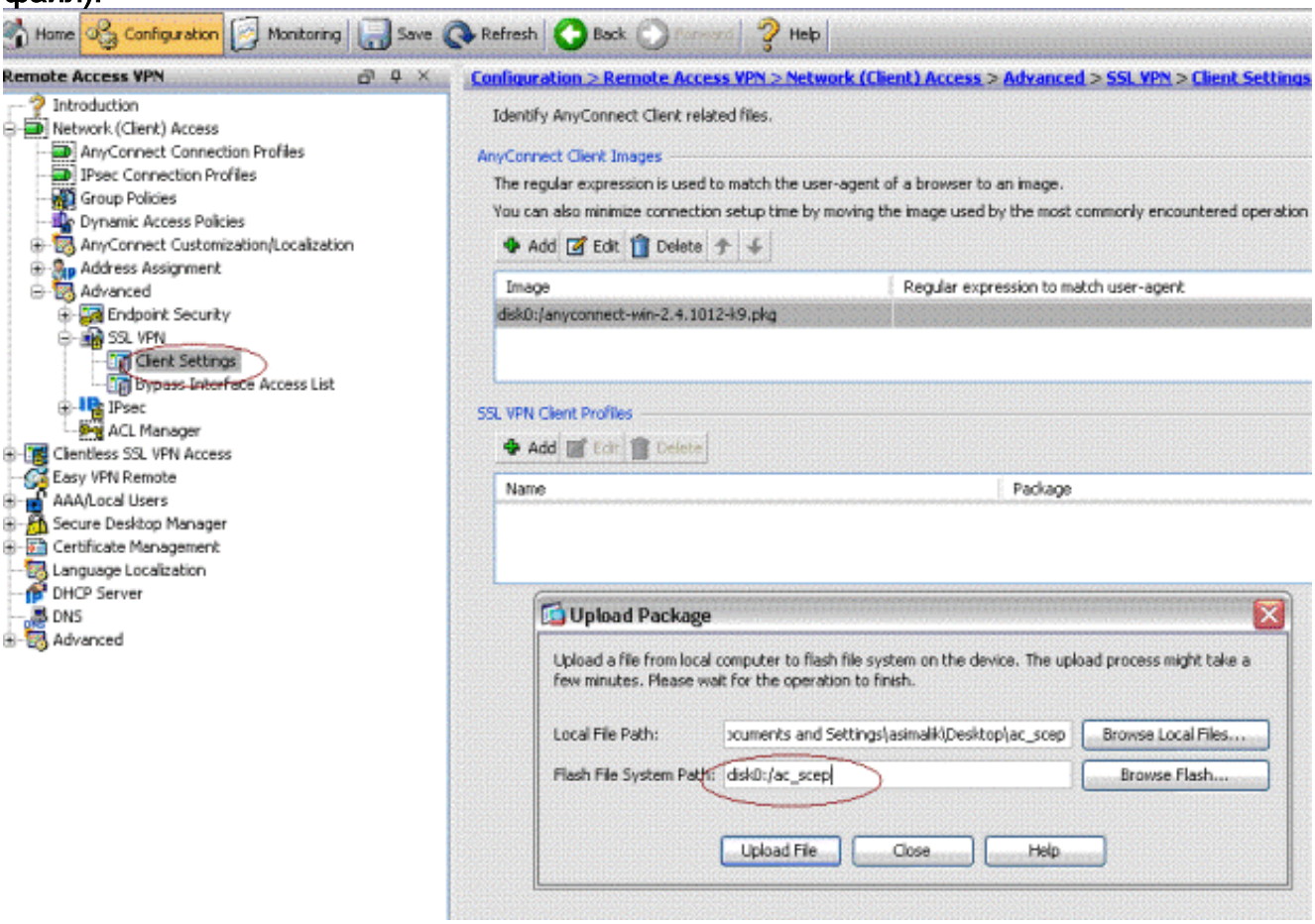
Для обеспечения доступа к частному Центру регистрации (RA) администратор ASA должен создать псевдоним, который имеет ACL, который ограничивает частное сетевое подключение стороны желаемым RA. Для автоматического получения сертификата пользователи соединяются и аутентифицируются на этом псевдониме.

Выполните следующие действия:

1. Создайте псевдоним на ASA для обращения определенной настроенной группе.
2. Задайте псевдоним в элементе <AutomaticSCEPHost> в клиентском профиле пользователя.
3. Подключите клиентский профиль, который содержит <CertificateEnrollment> раздел определенной настроенной группе.
4. Заставьте ACL для определенной настроенной группы ограничивать трафик частной стороной RA.

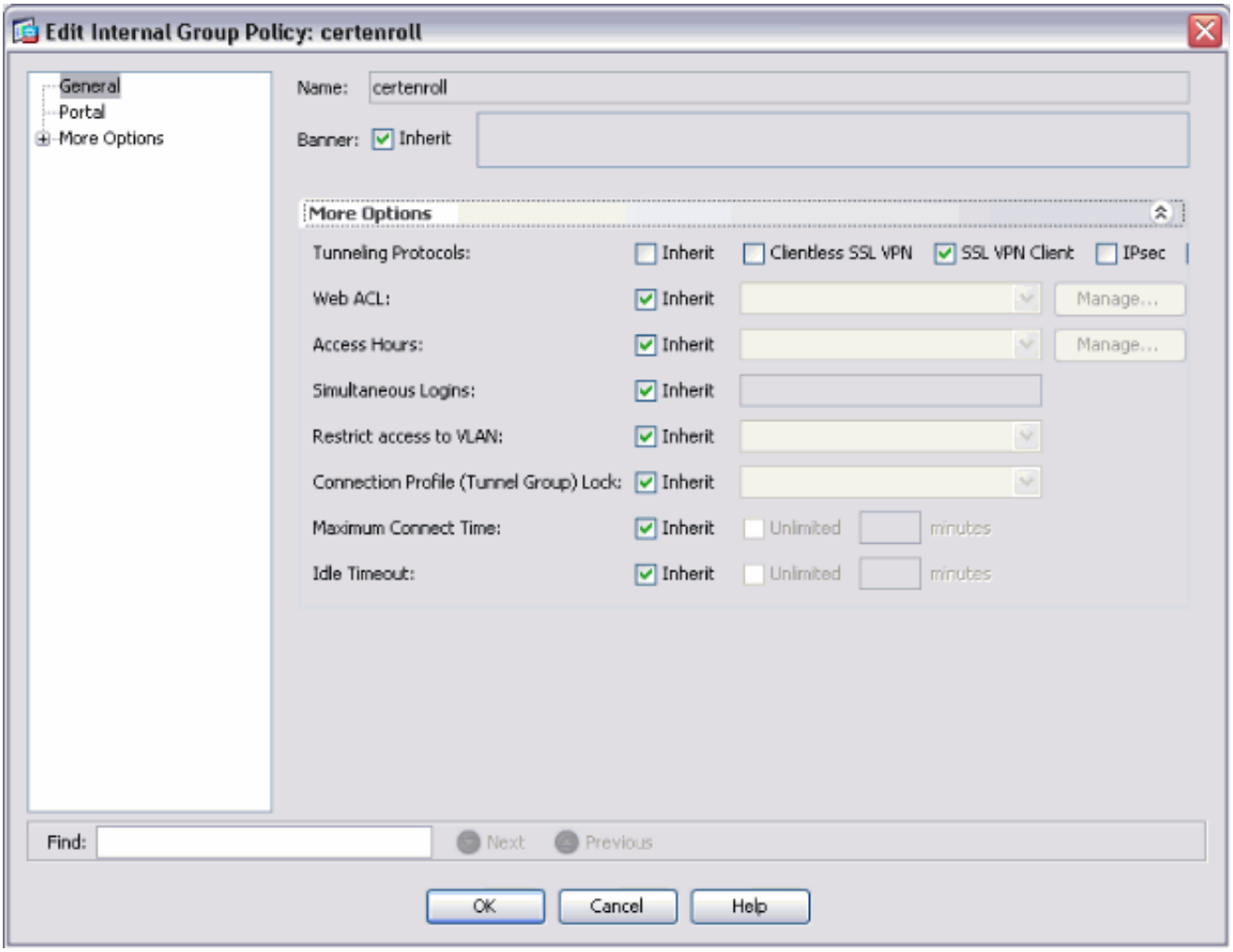
Выполните следующие действия:

1. Загрузите профиль XML к ASA.Выберите **Remote Access VPN> сетевой доступ (клиент)> Усовершенствованный> VPN SSL> Клиентские параметры настройки**.Под профилями VPN-клиента SSL (SVC) **нажмите Add**.Нажмите **Browse Local Files**, чтобы выбрать файл конфигурации и нажать **Browse Flash** для определения названия флэша - файла.**Щелкните Upload File (Загрузить файл).**

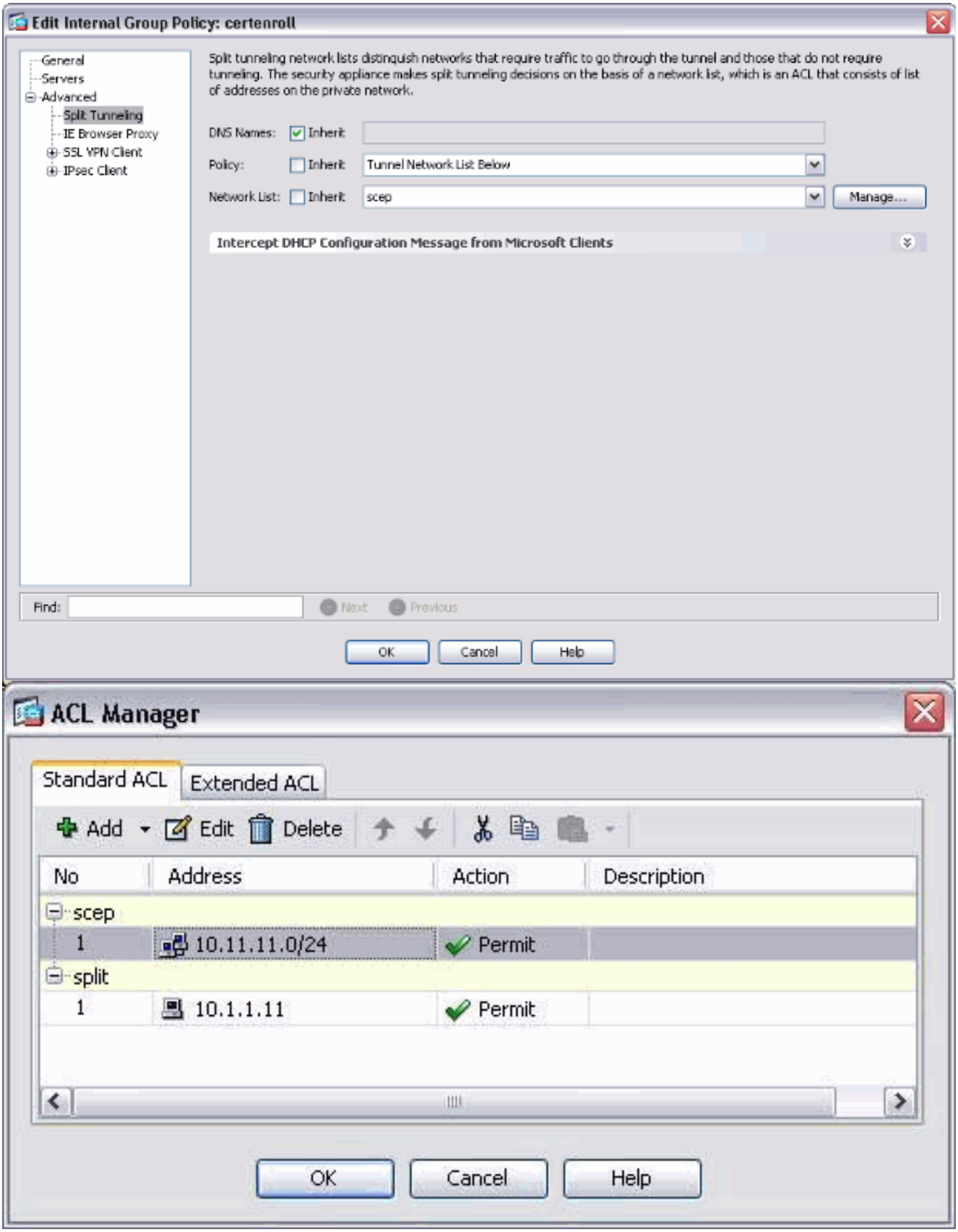


2. Установите **certenroll** групповую политику для хранилища сертификатов.Выберите **Remote access VPN> доступ Клиента сети> Групповая политика** и **нажмите**

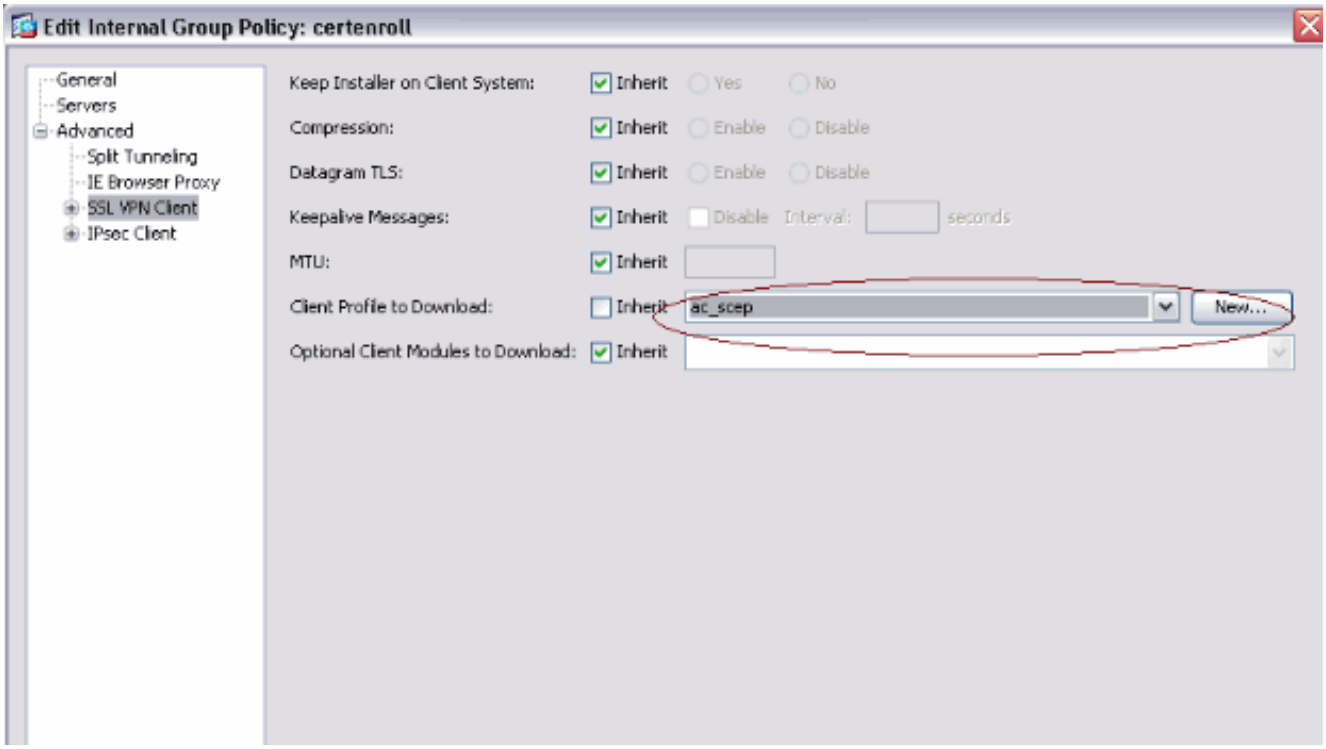
Add.



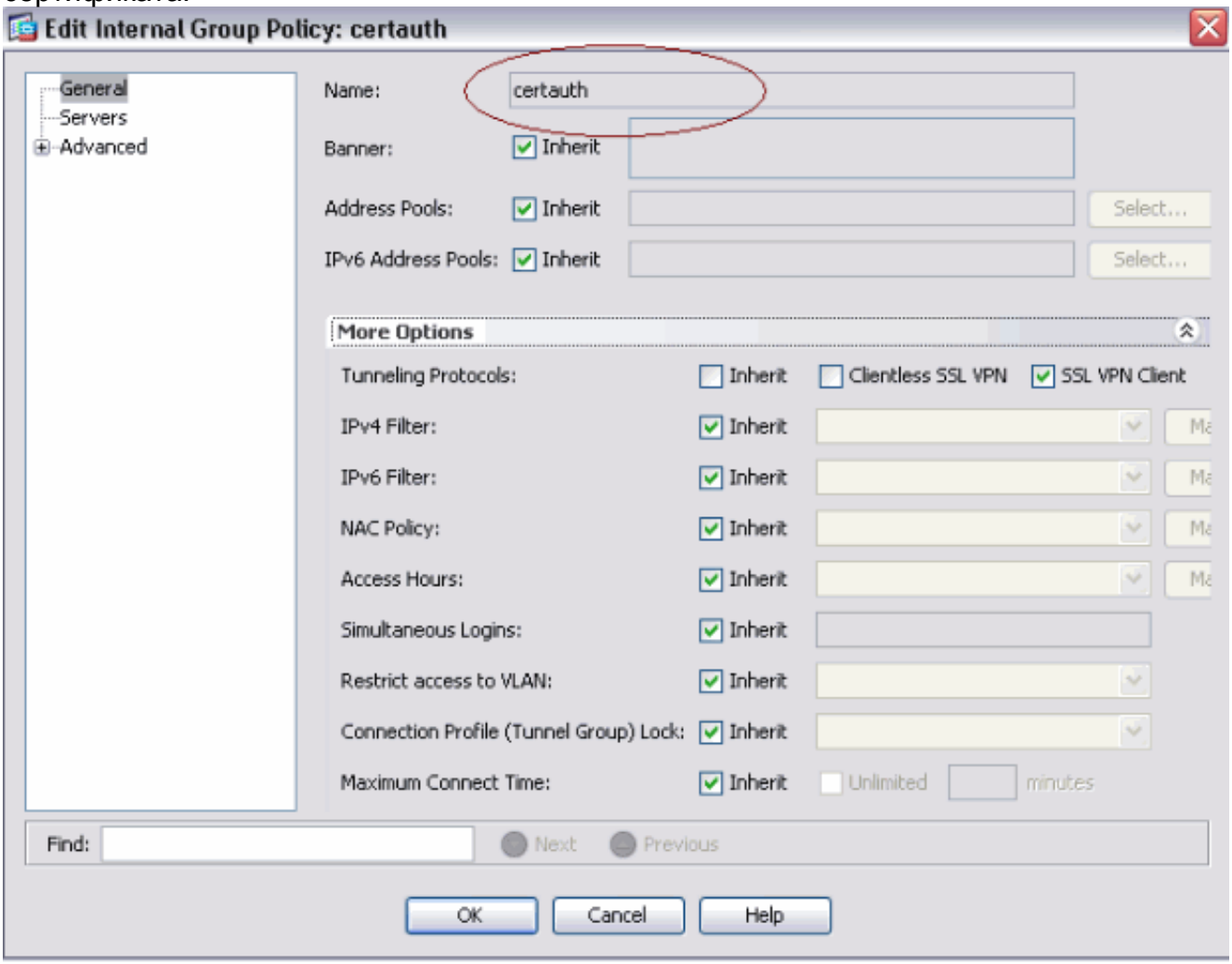
Добавьте разделение туннеля для сервера CA.Разверните **Усовершенствованный**, и затем выберите **Split Tunneling**.Выберите **Tunnel Network List Below** из меню Policy и нажмите **Manage** для добавления списка контроля доступа.



Выберите **SSL VPN Client** и выберите профиль для certenroll из меню **Client Profile to Download**.

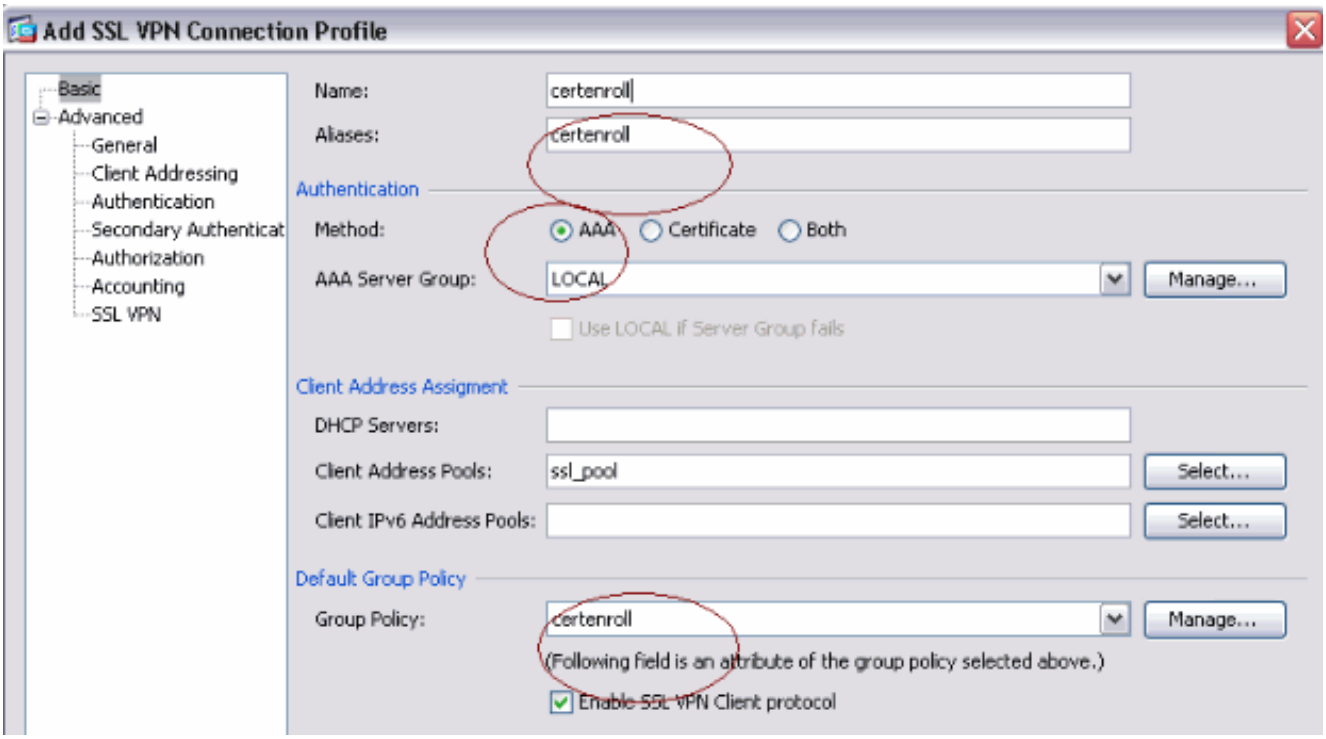


3. Создайте другую группу, названную **certauth** для проверки подлинности сертификата.

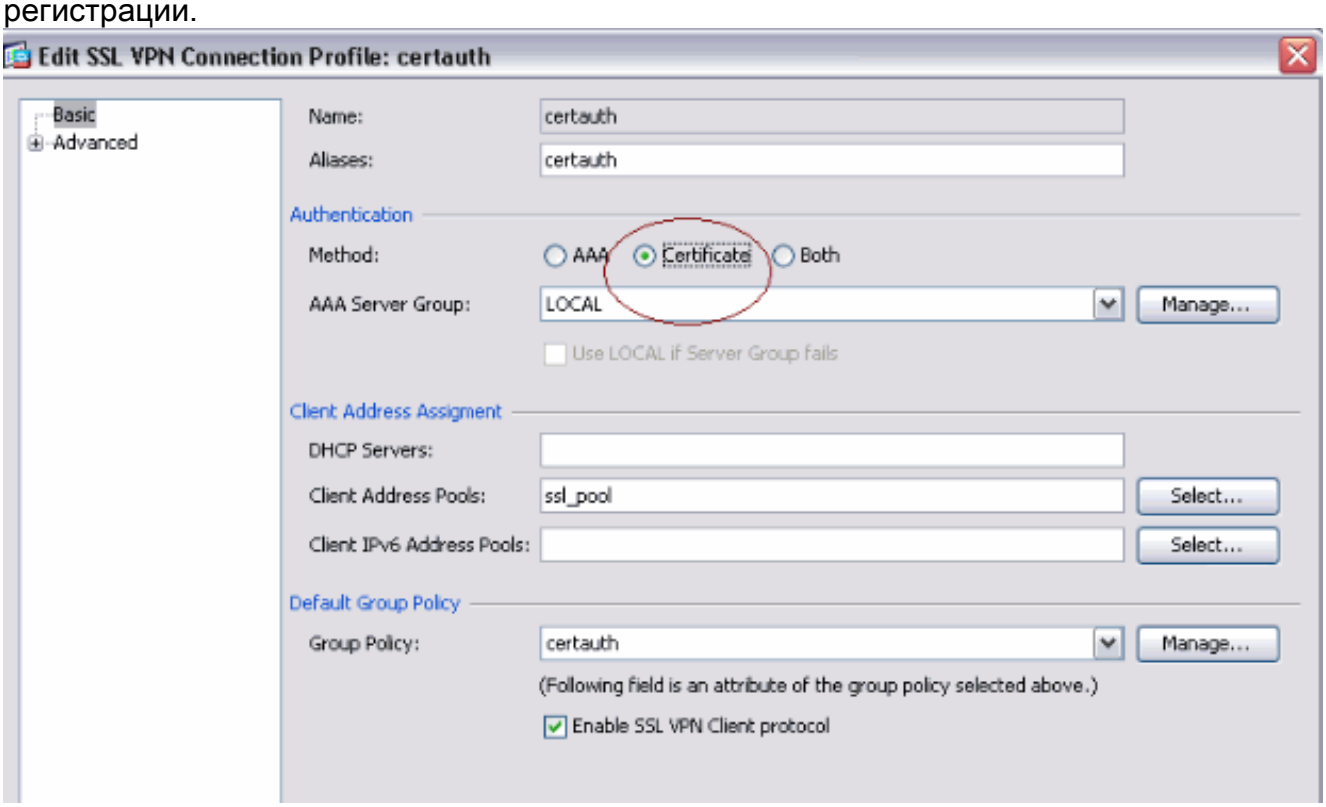


4. Создайте certenroll профиль подключения.Выберите **Remote access VPN> доступ Клиента сети> профили Соединения AnyConnect** и **нажмите Add**.Введите **certenroll** группу в поле Aliases.**Примечание:** Название псевдонима должно совпасть со значением, используемым в профиле AnyConnect под

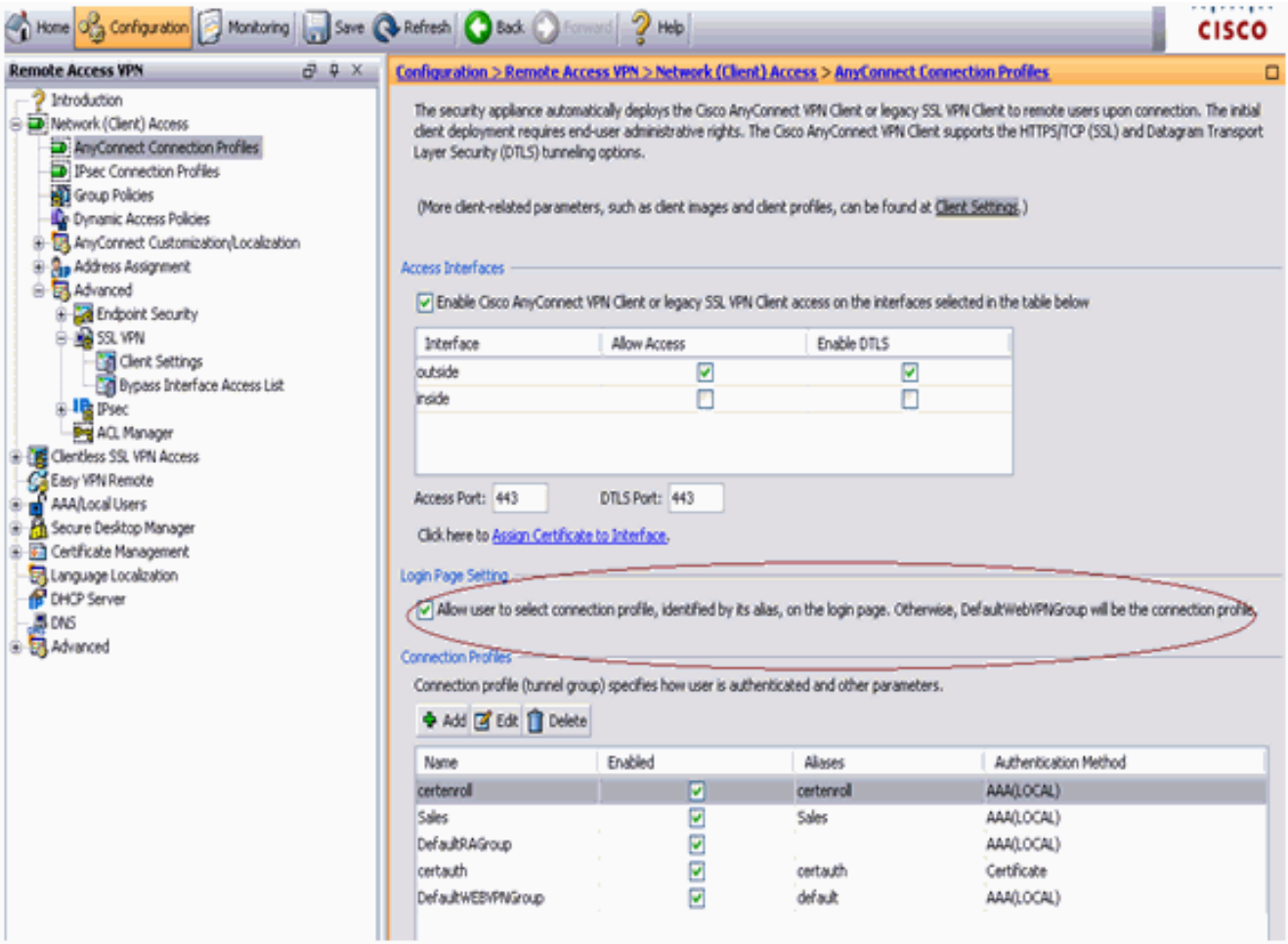
AutomaticSCEPHost.



5. Сделайте другой профиль подключения названным **certauth** с проверкой подлинности сертификата. Это - профиль фактического соединения, который используется после регистрации.



6. Чтобы удостовериться, что использование псевдонима включено, проверка **Позволяют пользователю выбирать профиль подключения, определенный его псевдонимом, на странице входа. В противном случае DefaultWebVPNGroup является профилем подключения.**



Тестовый SCEP AnyConnect

Воспользуйтесь данным разделом для проверки правильности функционирования вашей конфигурации.

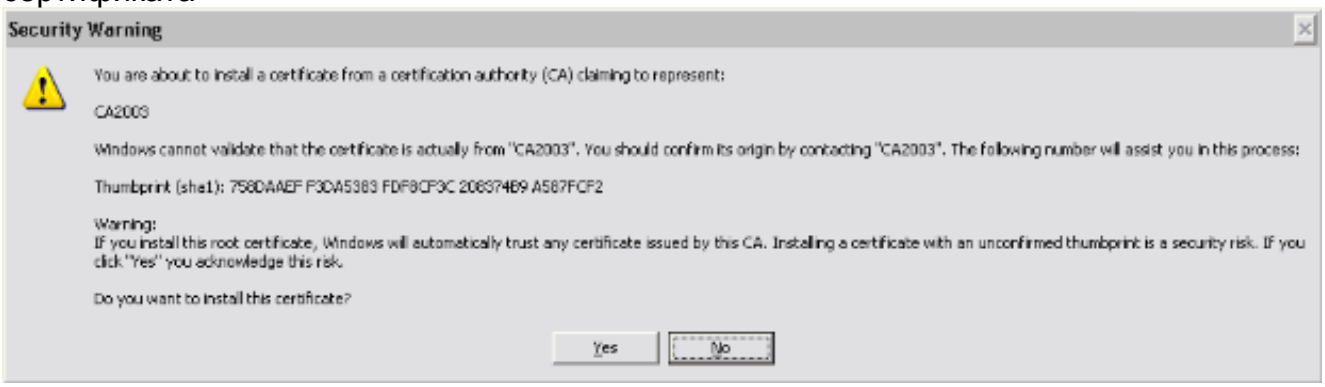
1. Запустите клиента AnyConnect и соединитесь с профилем

certenroll. AnyConnect передает запрос регистрации к серверу CA через

SCEP. Если кнопка **Get Certificate** используется, AnyConnect передает запрос регистрации непосредственно и

не проходит туннель.

2. Это предупреждение появляется. Нажмите **Yes** для установки пользователя использования и корневого сертификата

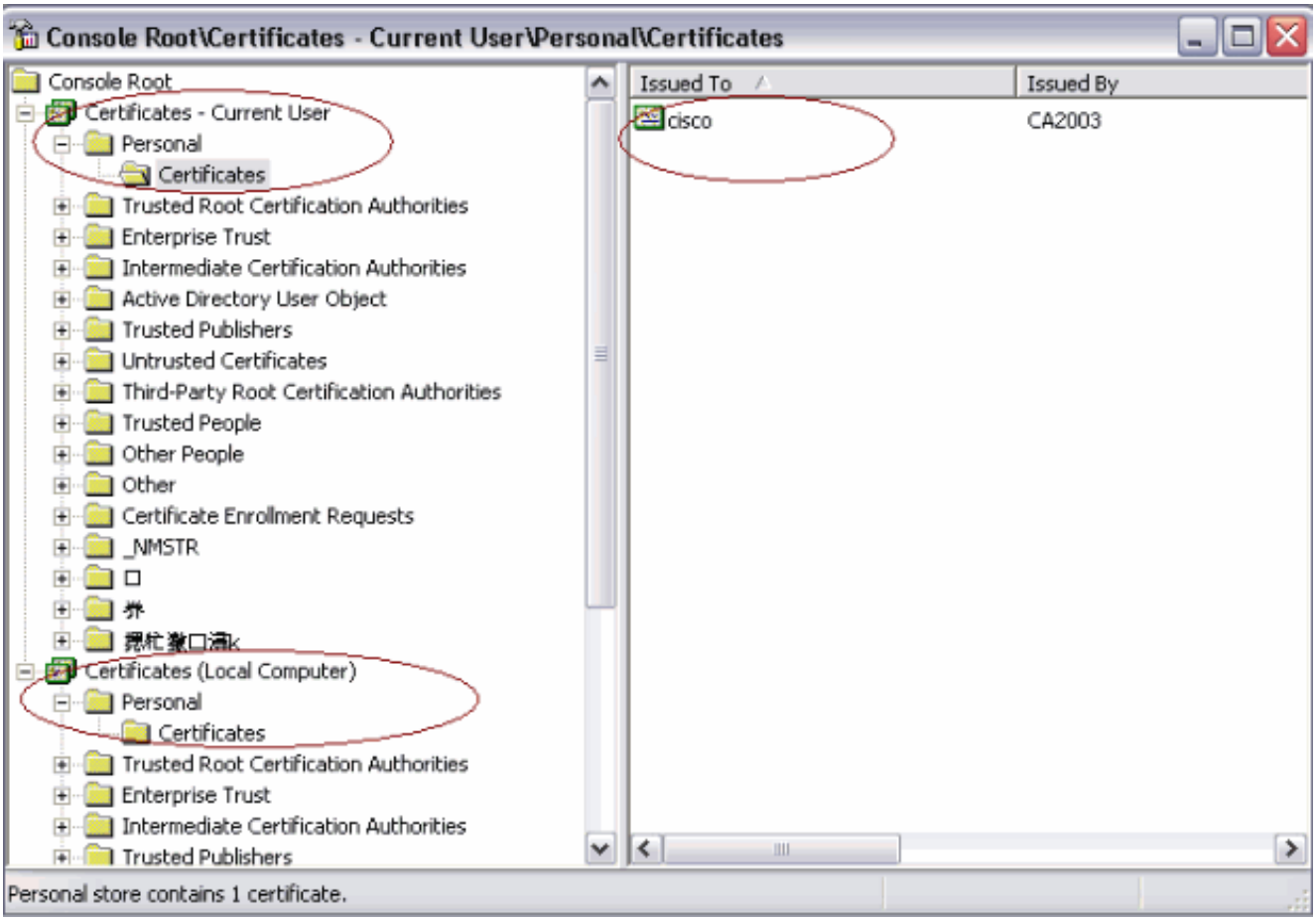


3. Как только сертификат зарегистрирован, подключение к профилю **certauth**.

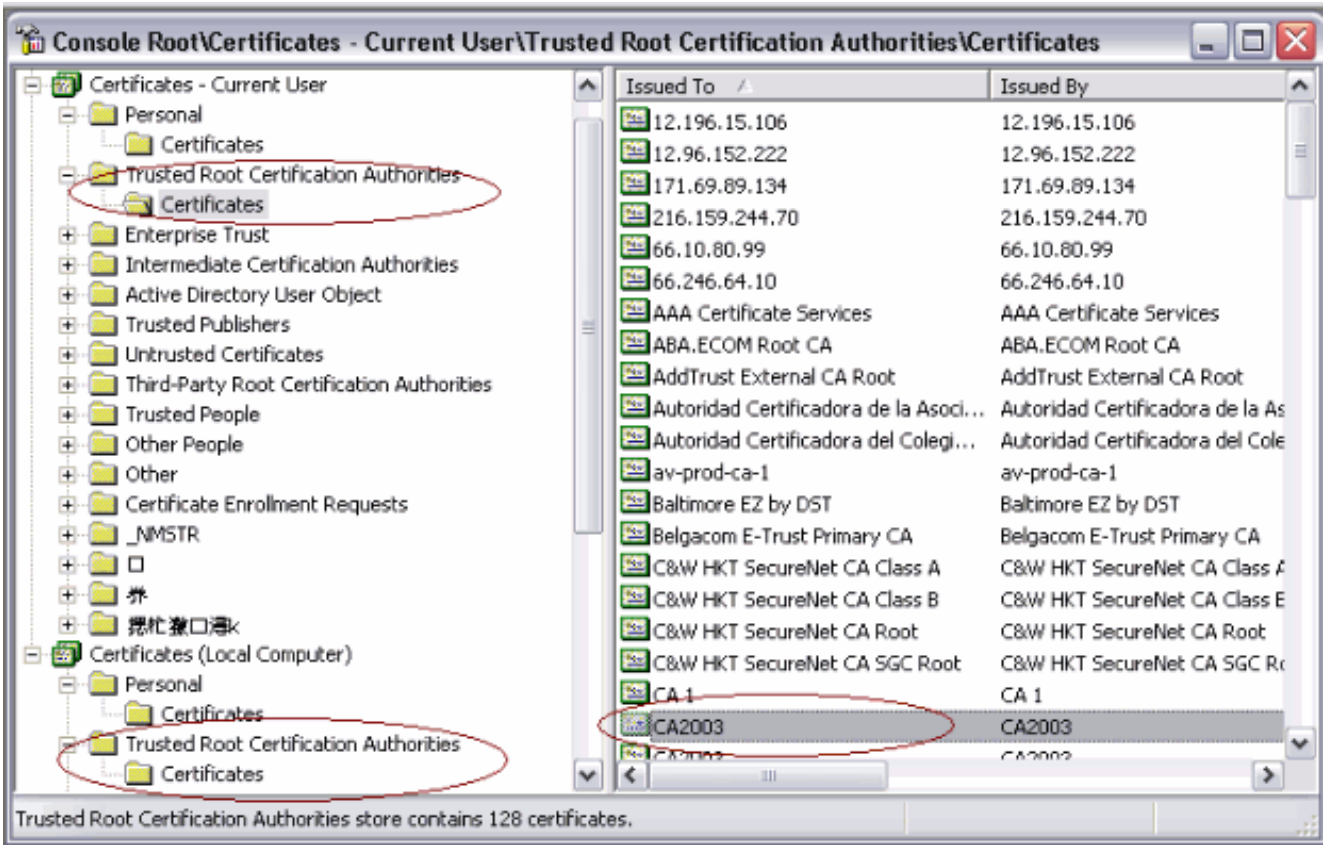
Хранилище сертификата на Microsoft Windows после Запроса SCEP

Выполните следующие действия:

1. Нажмите **Пуск> Выполнить> mmc**.
2. Нажмите **моментальный снимок Add/remove в**.
3. **Нажмите Add** и выберите **сертификаты**.
4. Добавьте **Мою учетную запись пользователя** и сертификаты **учетной записи компьютера**.Этот образ показывает сертификат пользователя, установленный в хранилище сертификата
   Windows:



   Этот образ показывает сертификат CA, установленный в хранилище сертификата
   Windows:



Устранение неполадок

В этом разделе описывается процесс устранения неполадок конфигурации.

- Когда проверка подлинности сертификата отказывает, регистрация SCEP AnyConnect только работает. Если это не регистрируется, проверьте хранилище сертификата. Если сертификаты уже установлены, удаляют их и тестируют снова.
- Регистрация SCEP не работает, пока не используется **команда ssl certificate-authentication interface outside port 443**.См. эти идентификаторы ошибок Cisco для получения дополнительной информации:Идентификатор ошибки Cisco CSCtf06778 (только зарегистрированные клиенты) — SCEP AnyConnect регистрируется, не работает с На Аутентификацию Свидетельства Группы 2Идентификатор ошибки Cisco CSCtf06844 (только зарегистрированные клиенты) — Регистрация SCEP AnyConnect, не работающая с ASA На Аутентификацию Свидетельства Группы
- Если сервер CA за пределами ASA, удостоверьтесь, что позволили прикрепление с **командой same-security-traffic permit intra-interface**. Также добавьте nat снаружи и команды access-list как показано в данном примере:`nat (outside) 1 access-list natoutside extended permit ip 172.16.1.0 255.255.255.0 host 171.69.89.87`Где 172.16.1.0 пул AnyConnect, и 171.69.89.87 IP-адрес сервера CA.
- Если сервер CA находится на внутренней части, удостоверьтесь, что включали его в список доступа разделения туннеля для **certenroll** групповой политики. В этом документе предполагается, что сервер CA находится на внутренней части.`group-policy certenroll attributes`
```
split-tunnel-policy tunnelspecified
 split-tunnel-network-list value scep

access-list scep standard permit 171.69.89.0 255.255.255.0
```

Дополнительные сведения

- Руководство для администратора клиента VPN Cisco AnyConnect, выпуск 2.4
- Cisco Systems – техническая поддержка и документация