FlexVPN: удаленный доступ AnyConnect IKEv2 с EAP AnyConnect

Содержание

Введение

Этот документ предоставляет пример конфигурации того, как настроить головной узел IOS/IOS-XE для удаленного доступа с помощью AnyConnect IKEv2 и МЕТОДА АУТЕНТИФИКАЦИИ EAP ANYCONNECT.

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Выпуск 3.15 XE IOS (15.5 (2) S) или позже
- IOS Release 15.5 (2) T или позже
- Версия клиентской части 3.0 AnyConnect или позже

Используемые компоненты

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

- Cisco ASR1002-X рабочий IOS XE 3.15
- Версия клиентской части 3.1.8009 AnyConnect, работающая на Windows 7
- Сервер Cisco ACS 5.3 (дополнительный)

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.

Общие сведения

EAP AnyConnect, также известный как составная аутентификация, позволяет Серверу Flex аутентифицировать клиента AnyConnect использование Cisco составляющий собственность МЕТОД EAP ANYCONNECT. Шифрование / расшифровка базировало методы Протокола EAP, такие как Карта с переменым паролем Общего назначения EAP (EAP-GTC), EAP - Профиль сообщения 5 (EAP-MD5) и так далее, Сервер Flex не работает в режиме прохождения EAP. Вся связь EAP с клиентом завершается на Сервере Flex, и требуемый ключ сеанса, используемый для построения информационного наполнения AUTH, вычислен локально Сервером Flex. **Сервер Flex должен аутентифицировать себя на клиенте, использующем сертификаты как требуется RFC IKEv2.**

Аутентификация локального пользователя теперь поддерживается на Проверке подлинности сервера Flex, и удаленная аутентификация является дополнительной. Это является идеальным для мелкомасштабных развертываний с меньшим количеством количества пользователей удаленного доступа и в средах без доступа к внешней проверке подлинности, Авторизации, и Бухгалтерским (AAA) сервер. Однако для широкомасштабных развертываний и в сценариях, где атрибуты по каждому пользователю желаемы, чтобы было все еще рекомендовано использовать внешний AAA, разъединяют для проверки подлинности и авторизация. РЕАЛИЗАЦИЯ EAP ANYCONNECT разрешает использование Радиуса или TACACS для удаленной аутентификации, авторизации и учета.

Настройка

Authenticating и пользователи Authorizating, использующие Локальную базу данных

> **Примечание:** Для аутентификации пользователей против локальной базы данных на маршрутизаторе EAP должен использоваться. Однако для использования EAP, метод локальной проверки подлинности должен быть rsa-сигналом, таким образом, маршрутизатору нужен надлежащий сертификат, установленный на нем, и это не может быть подписанный сертификат.

Пример конфигурации, который использует аутентификацию локального пользователя, удаленного пользователя и авторизацию группы и удаленный учет.

EAP AnyConnect определенная конфигурация, показанная полужирным

Шаг 1. Включите AAA и настройте списки аутентификации, авторизации и учета (aaa attribute list является дополнительным), и добавьте имя пользователя к локальной базе данных:

```
aaa new-model


!
aaa authentication login a-eap-authen-local local
aaa authorization network a-eap-author-grp local
!
aaa attribute list AAA-attr
attribute type interface-config "ip mtu 1300"
!
username test password cisco12
```

Шаг 2. Настройте точку доверия для получения сертификата ID из сервера CA (маршрутизатор может быть настроен как CA также):

```
crypto pki trustpoint IKEv2-TP
enrollment mode ra
enrollment url http://X.X.X.X:80/certsrv/mscep/mscep.dll
subject-name CN=vpn.example.com,OU=TAC,L=SanJose,C=US
revocation-check none
rsakeypair rsakey
```

Шаг 3. Определите IP local pool для присвоения адресов на Клиентов AnyConnect VPN Client:

```
ip local pool ACPOOL 192.168.10.5 192.168.10.10
```

Шаг 4. . Создайте политику локальной проверки подлинности IKEv2:

```
crypto ikev2 authorization policy ikev2-auth-policy
pool ACPOOL
aaa attribute list AAA-attr
```

Шаг 5. . Создайте желаемое предложение IKEv2 и политику:

```
crypto ikev2 proposal IKEv2-prop1
encryption aes-cbc-256
integrity sha256
group 2
!
crypto ikev2 policy IKEv2-pol
proposal IKEv2-prop1
```

Шаг 6. Создайте профиль IKEv2 для МЕТОДА EAP ANYCONNECT аутентификации клиента:

```
crypto ikev2 profile AnyConnect-EAP
match identity remote key-id *$AnyConnectClient$*
authentication remote anyconnect-eap aggregate
authentication local rsa-sig
pki trustpoint IKEv2-TP
aaa authentication anyconnect-eap a-eap-authen-local
aaa authorization group anyconnect-eap list a-eap-author-grp ikev2-auth-policy
aaa authorization user anyconnect-eap cached
virtual-template 100
```

> **Примечание:** Настройка метод удаленной аутентификации перед методом локальной проверки подлинности будет принят CLI, но может не вступить в силу на версиях кода, на которые влияет CSCva46032. Если вы скопировать/вставить конфигурация от этого документа, гарантируйте, что метод удаленной аутентификации имеет, заражают вступивший в силу и если это не имеет, повторно введите команду.

Шаг 7. Отключите основанный поиск сертификата HTTP URL:

```
crypto ikev2 profile AnyConnect-EAP
```

```
match identity remote key-id *$AnyConnectClient$*
authentication remote anyconnect-eap aggregate
authentication local rsa-sig
pki trustpoint IKEv2-TP
aaa authentication anyconnect-eap a-eap-authen-local
aaa authorization group anyconnect-eap list a-eap-author-grp ikev2-auth-policy
aaa authorization user anyconnect-eap cached
virtual-template 100
```

Шаг 8. Определите шифрование, и алгоритмы хэширования использовали защищать данные

```
crypto ikev2 profile AnyConnect-EAP
match identity remote key-id *$AnyConnectClient$*
authentication remote anyconnect-eap aggregate
authentication local rsa-sig
pki trustpoint IKEv2-TP
aaa authentication anyconnect-eap a-eap-authen-local
aaa authorization group anyconnect-eap list a-eap-author-grp ikev2-auth-policy
aaa authorization user anyconnect-eap cached
virtual-template 100
```

> **Примечание:** *Обратитесь* этот документ подтвердить, поддерживают ли ваши оборудования маршрутизатора алгоритмы шифрования NGE (например, приведенный выше пример имеет алгоритмы NGE). В противном случае установка КОНТЕКСТА БЕЗОПАСНОСТИ IPSEC на аппаратных средствах откажет на последней стадии согласования.

Шаг 9. Создайте Профиль IPSEC:

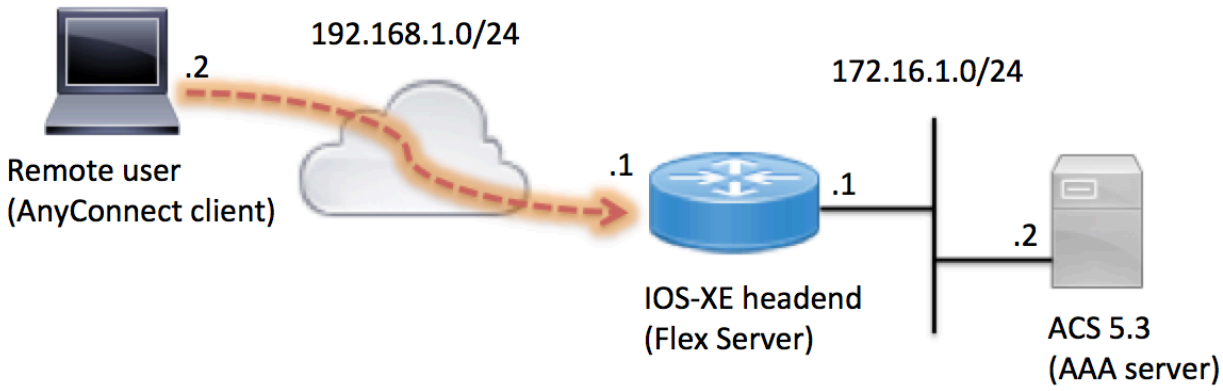
```
crypto ikev2 profile AnyConnect-EAP
match identity remote key-id *$AnyConnectClient$*
authentication remote anyconnect-eap aggregate
authentication local rsa-sig
pki trustpoint IKEv2-TP
aaa authentication anyconnect-eap a-eap-authen-local
aaa authorization group anyconnect-eap list a-eap-author-grp ikev2-auth-policy
aaa authorization user anyconnect-eap cached
virtual-template 100
```

Шаг 10. Настройте virtual-template (привяжите шаблон в профиле IKEv2),

```
crypto ikev2 profile AnyConnect-EAP
match identity remote key-id *$AnyConnectClient$*
authentication remote anyconnect-eap aggregate
authentication local rsa-sig
pki trustpoint IKEv2-TP
aaa authentication anyconnect-eap a-eap-authen-local
aaa authorization group anyconnect-eap list a-eap-author-grp ikev2-auth-policy
aaa authorization user anyconnect-eap cached
virtual-template 100
```

Аутентификация, авторизация и учет с помощью удаленного AAA-сервера

Схема сети



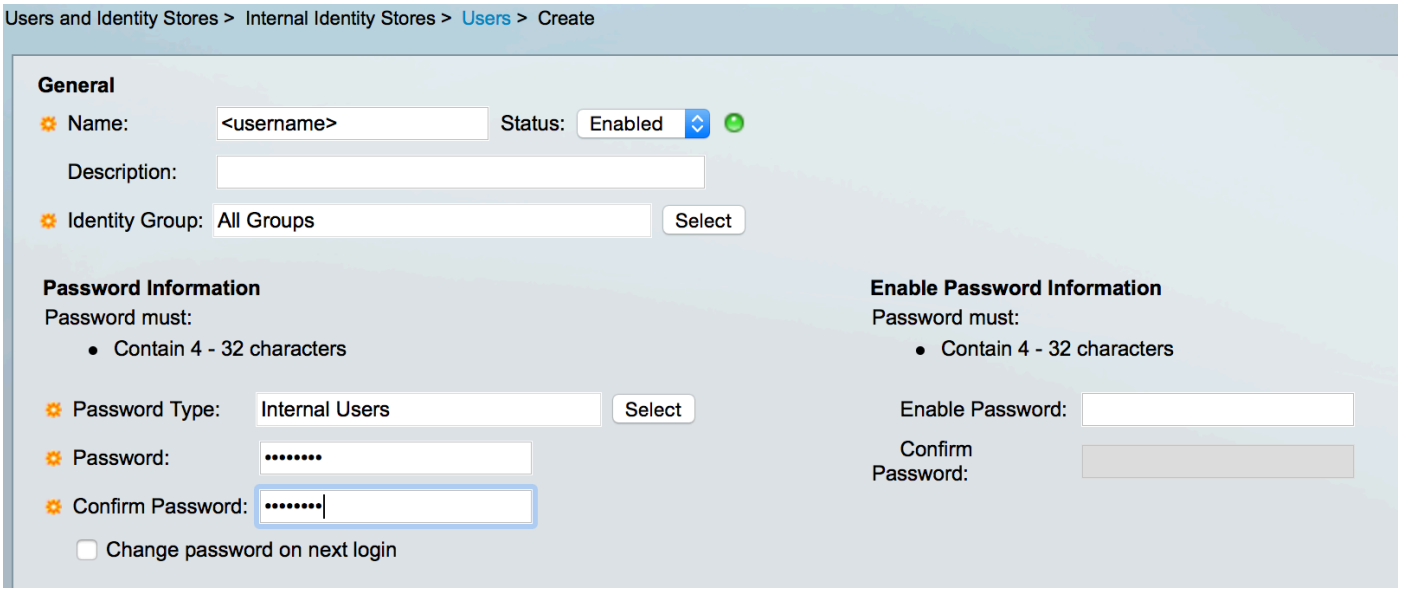
Изменения конфигурации головного узла

Примечание: См. вышеупомянутый раздел для отдыха конфигурации.

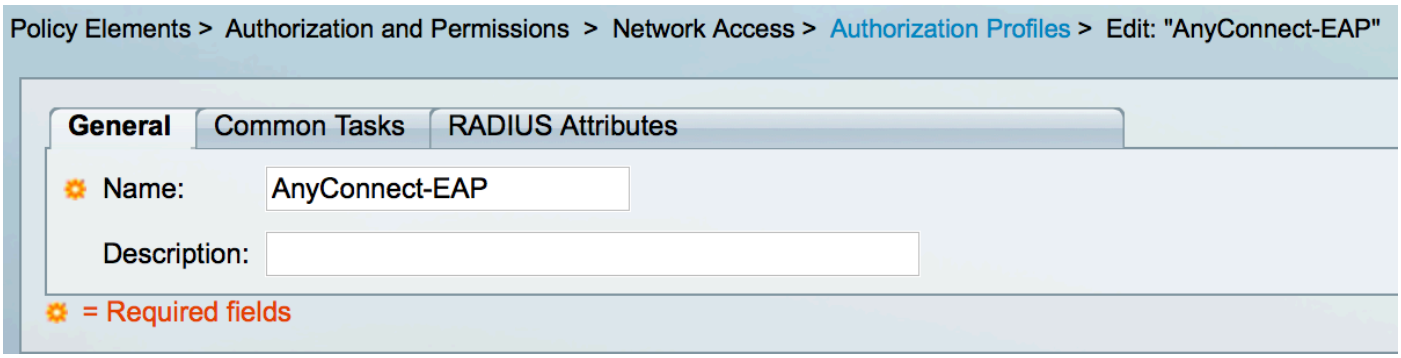
```
aaa group server radius ACS
server name ACS
!
radius server ACS
address ipv4 172.16.1.2 auth-port 1645 acct-port 1646
key Cisco123!
!
aaa authentication login a-eap-authen group ACS
aaa authorization network a-eap-author group ACS
aaa accounting network a-eap-acc start-stop group ACS
!
crypto ikev2 name-mangler NM
eap suffix delimiter @
!
crypto ikev2 profile AnyConnect-EAP
aaa authentication anyconnect-eap a-eap-authen
aaa authorization group anyconnect-eap list a-eap-author <aaa-username>
aaa authorization user anyconnect-eap list a-eap-author name-mangler NM
aaa accounting anyconnect-eap a-eap-acc
```

Конфигурация сервера RADIUS

Шаг 1. Создайте имя пользователя (для проверки подлинности пользователя и/или групповой аутентификации и авторизации), как показано в образе:



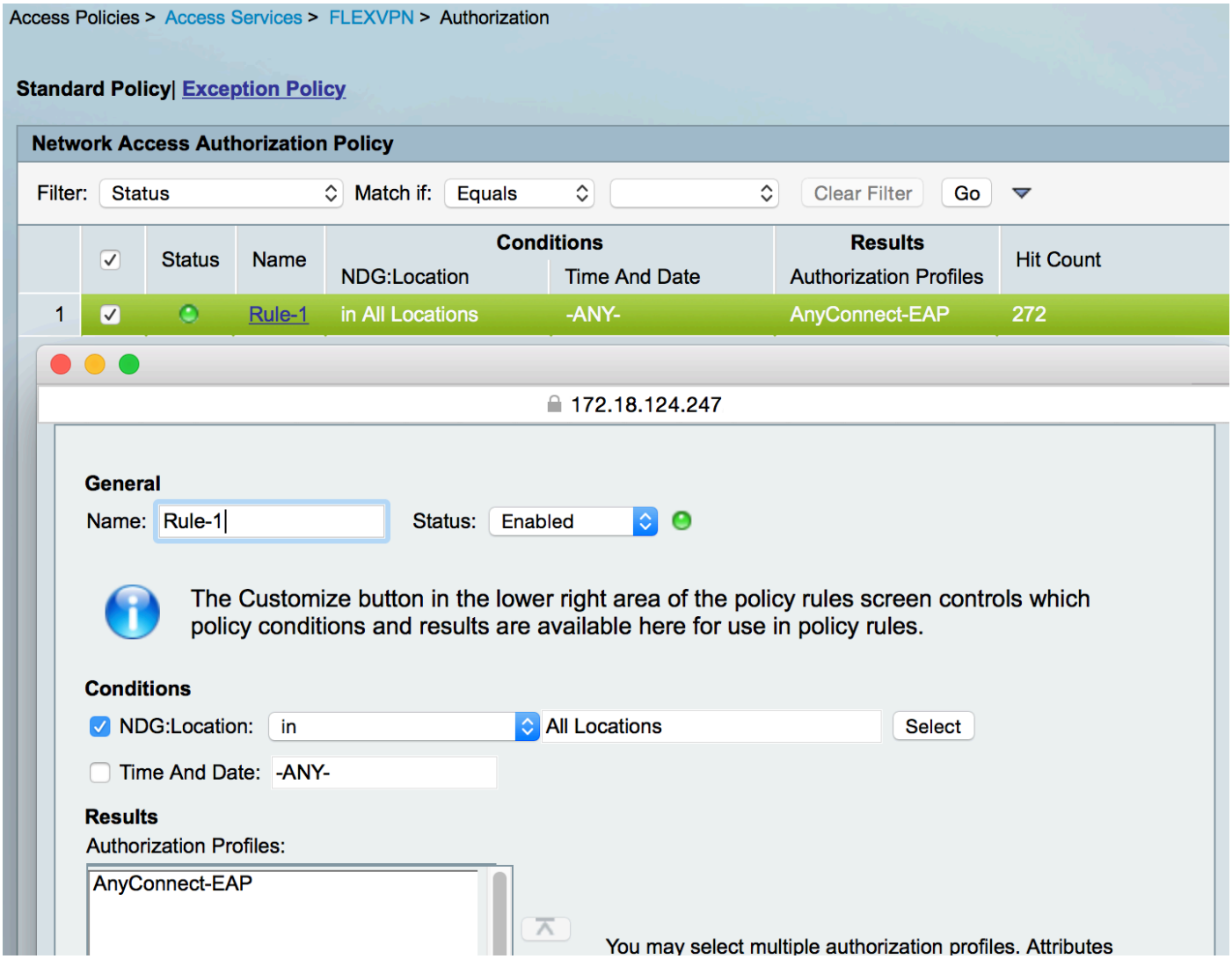
Шаг 2. Настройте Политику авторизации, как показано в образе:



Шаг 3. Теперь добавьте атрибуты RADIUS, как показано в образе:

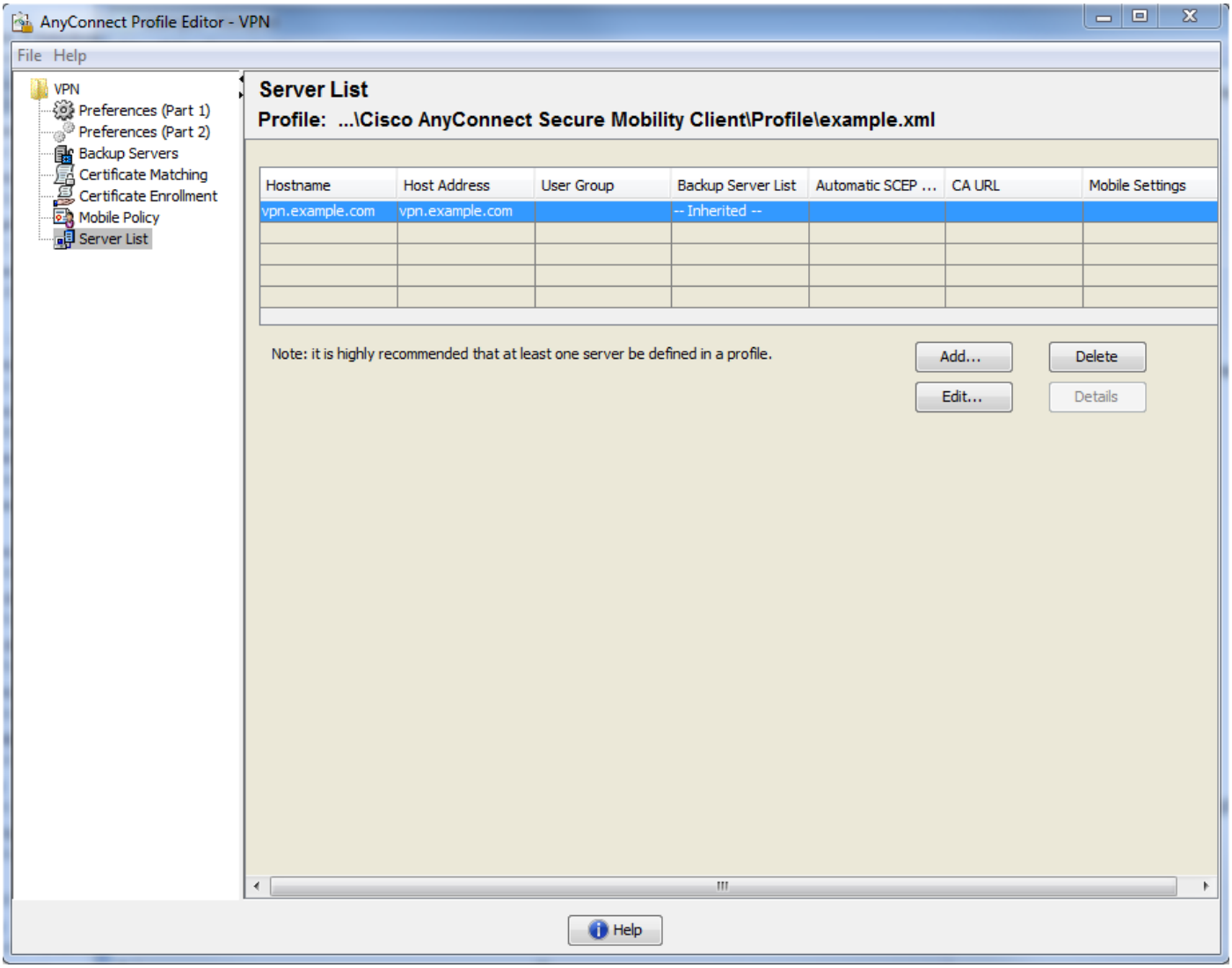
Attribute	Type	Value
cisco-av-pair	String	ipsec:default-domain=ciscotac.com
cisco-av-pair	String	ipsec:banner=AnyConnect
cisco-av-pair	String	ipsec:addr-pool=ACPOOL
cisco-av-pair	String	ipsec:route-set=prefix 172.16.1.0/24
cisco-av-pair	String	ipsec:route-set=access-list split-acl

Шаг 4. . Как показано в образе, создайте Политику доступа и привяжите Политику авторизации.



Настройка профиля клиента AnyConnect

Настройте клиентский профиль с помощью Редактора Профиля AnyConnect как показано в образе:



XML, эквивалентный из профиля:

```
<?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>
<AllowLocalProxyConnections>false</AllowLocalProxyConnections>
<AuthenticationTimeout>12</AuthenticationTimeout>
<AutoConnectOnStart UserControllable="true">false</AutoConnectOnStart>
<MinimizeOnConnect UserControllable="true">true</MinimizeOnConnect>
<LocalLanAccess UserControllable="true">false</LocalLanAccess>
<ClearSmartcardPin UserControllable="true">true</ClearSmartcardPin>
<IPProtocolSupport>IPv4,IPv6</IPProtocolSupport>
<AutoReconnect UserControllable="false">true
<AutoReconnectBehavior UserControllable="false">ReconnectAfterResume</AutoReconnectBehavior>
</AutoReconnect>
<AutoUpdate UserControllable="false">false</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>
<EnableAutomaticServerSelection UserControllable="true">false
<AutoServerSelectionImprovement>20</AutoServerSelectionImprovement>
<AutoServerSelectionSuspendTime>4</AutoServerSelectionSuspendTime>
</EnableAutomaticServerSelection>
<RetainVpnOnLogoff>false
</RetainVpnOnLogoff>
<AllowManualHostInput>true</AllowManualHostInput>
</ClientInitialization>
<ServerList>
<HostEntry>
<HostName>vpn.example.com</HostName>
<HostAddress>vpn.example.com</HostAddress>
 <PrimaryProtocol>IPsec</PrimaryProtocol>
</HostEntry>
</ServerList>
</AnyConnectProfile>
```

> **Примечание:** AnyConnect использует '* $AnyConnectClient$*' в качестве его идентичности IKE по умолчанию ключевого идентификатора типа. Однако эта идентичность может быть вручную изменена в профиле AnyConnect для соответствия с потребностями развертываний. **StandardAuthenticationOnly** должен быть установлен в False при использовании EAP AnyConnect как показано в образе.

Измените идентичность IKE AnyConnect по умолчанию (Необязательно)

Если вы не хотите использовать идентификатор ike по умолчанию, используемый клиентом, можно изменить идентификатор ike в клиентском профиле, однако это также потребовало, чтобы идентификатор ike был изменен под профилем ikev2, настроенным на сервере Flexvpn.

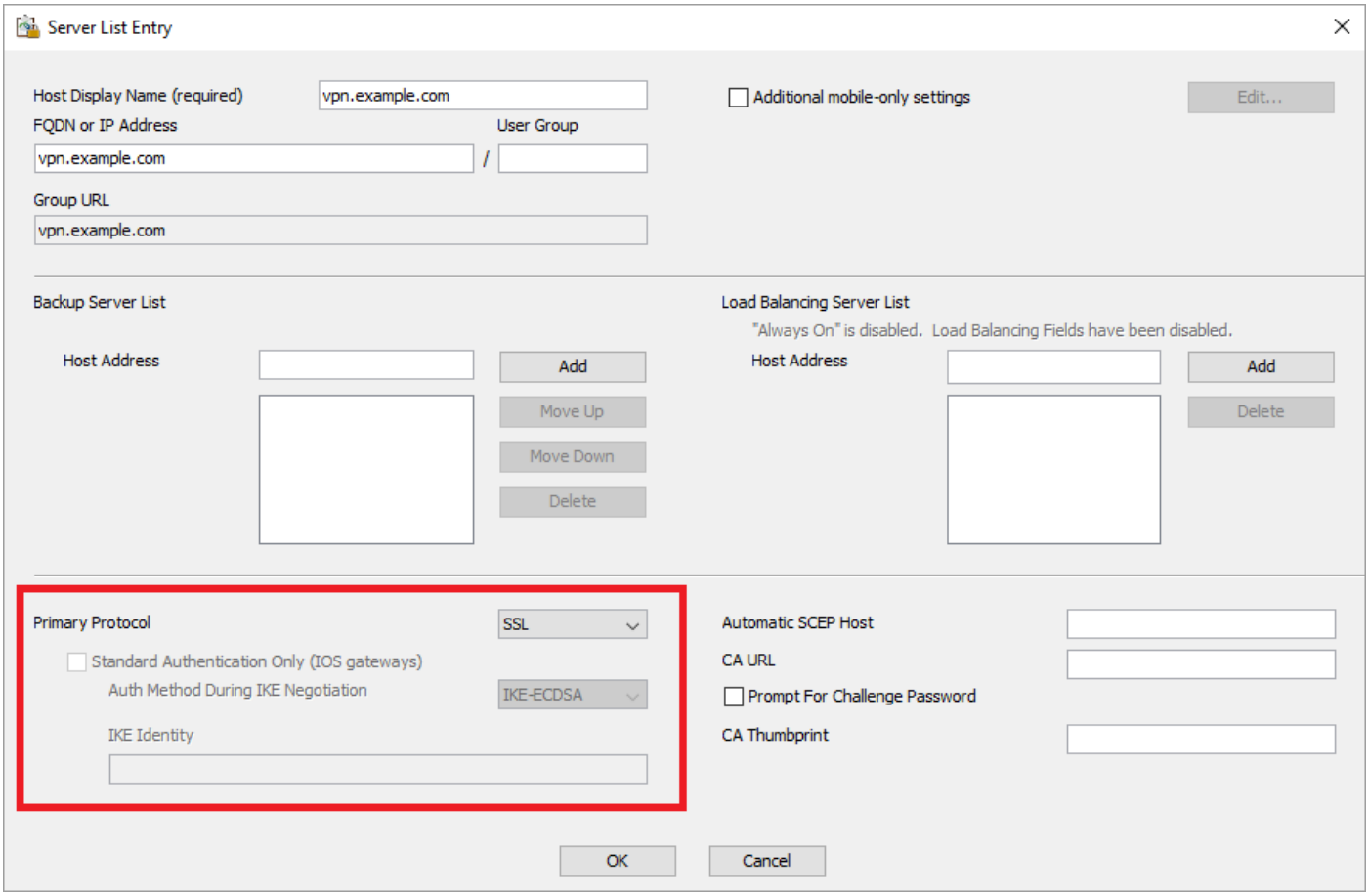
Клиентский профиль:

```
 <ServerList>
<HostEntry>
<HostName>vpn.example.com</HostName>
<HostAddress>vpn.example.com</HostAddress>
<PrimaryProtocol>IPsec
<StandardAuthenticationOnly>false
     <IKEIdentity>ANYCONNECT-IKEID</IKEIdentity>
</StandardAuthenticationOnly>
</PrimaryProtocol>
</HostEntry>
</ServerList>
```

Конфигурация FlexServer:

```
crypto ikev2 profile AnyConnect-EAP
match identity remote key-id ANYCONNECT-IKEID
```

Это может также быть установлено с помощью клиентского редактора профиля:



Совет: Если Стандартная аутентификация проверена, при использовании клиентского редактора профиля может только быть изменен ID ike. Это - известная неполадка и дефект, CSCva64390 был подан для решения этой проблемы. В это время можно вручную отредактировать файл xml с помощью любого текстового редактора так, чтобы значение для атрибута "StandardAuthenticationOnly" было установлено в False.

Обходной загрузчик (Необязательно)

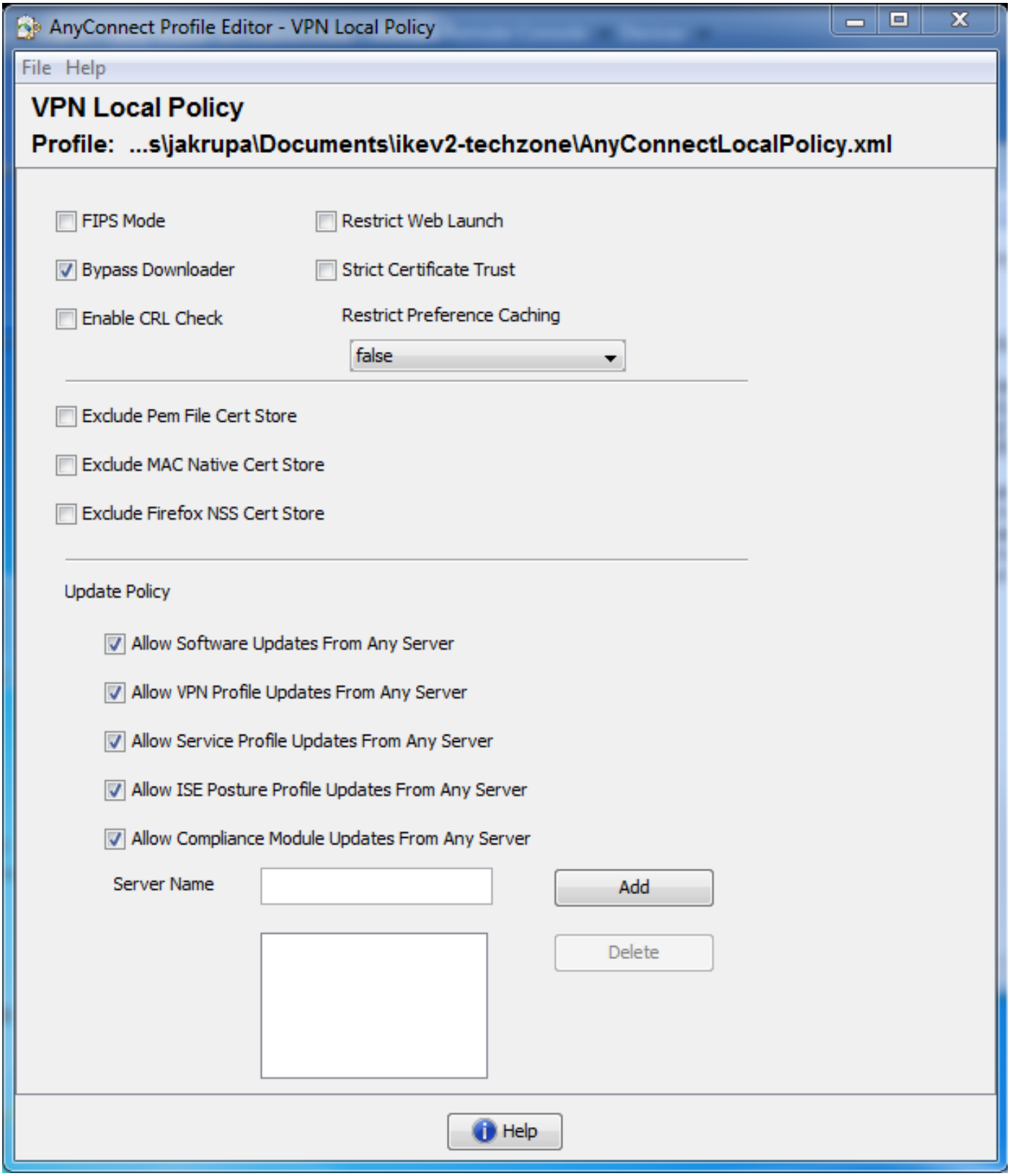
В настоящее время функция, которая позволяет клиенту Anyconnect загружать обновленную версию клиента от шлюза, не поддерживается на маршрутизаторах XE IOS. Таким образом, если версия клиентской части, используемая для соединения со шлюзом, будет ниже, чем версия, настроенная на шлюзе, то это приведет к соединению сбой. Для отключения его изменение в файле локальной политики на клиентском компьютере необходимо. Для получения дополнительной информации включая местоположение файла локальной политики см. Параметры Локальной политики Изменения Вручную.

Измените значение **BypassDownloader** на Истинный.

```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectLocalPolicy xmlns="http://schemas.xmlsoap.org/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/ AnyConnectLocalPolicy.xsd"
acversion="3.0.0592">
   <FipsMode>false</FipsMode>
   <BypassDownloader>true</BypassDownloader>
   <RestrictWebLaunch>false</RestrictWebLaunch>
   <StrictCertificateTrust>false</StrictCertificateTrust>
   <EnableCRLCheck>false</EnableCRLCheck>
   <RestrictPreferenceCaching>false</RestrictPreferenceCaching>
```

```
   <ExcludePemFileCertStore>false</ExcludePemFileCertStore>
   <ExcludeMacNativeCertStore>false</ExcludeMacNativeCertStore>
   <ExcludeFirefoxNSSCertStore>false</ExcludeFirefoxNSSCertStore>
   <UpdatePolicy>
      <AllowSoftwareUpdatesFromAnyServer>true</AllowSoftwareUpdatesFromAnyServer>
      <AllowVPNProfileUpdatesFromAnyServer>true</AllowVPNProfileUpdatesFromAnyServer>
      <AllowServiceProfileUpdatesFromAnyServer>true</AllowServiceProfileUpdatesFromAnyServer>
      <AllowISEProfileUpdatesFromAnyServer>true</AllowISEProfileUpdatesFromAnyServer>
      <AllowComplianceModuleUpdatesFromAnyServer>true</AllowComplianceModuleUpdatesFromAnyServer
>
   </UpdatePolicy>
</AnyConnectLocalPolicy>
```

Это может быть сделано или посредством ручного редактирования файла или при помощи Редактора Профиля AnyConnect программное средство:



Поток подключения

IKEv2 и обмен EAP