FlexVPN ：与AnyConnect EAP的AnyConnect IKEv2远程访问

目录

简介

使用AnyConnect IKEv2和AnyConnect EAP认证方法，本文提供配置示例如何配置远程访问的一IOS/IOS-XE头端。

先决条件

要求

Cisco 建议您了解以下主题：

- IOS-XE版本3.15 (15.5(2)S)或以上
- IOS版本15.5(2)T或以上
- AnyConnect客户端版本3.0或以上

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 运行IOS XE 3.15的思科ASR1002-X

- 运行在Windows 7的AnyConnect客户端版本3.1.8009
- Cisco ACS服务器5.3 (可选)

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

背景信息

AnyConnect EAP，亦称聚集验证，允许弹性服务器验证使用思科所有权AnyConnect EAP方法的AnyConnect客户端。不同于根据的标准可扩展的认证协议(EAP)方法例如EAP通用的令牌卡(EAP-GTC)，消息摘要5 (EAP-MD5)等，弹性服务器在EAP直通模式不运行。与客户端的所有EAP通信在弹性服务器终止，并且修建验证有效负载弹性服务器计算用于的需要的会话密钥本地。**弹性服务器必须验证对使用证书的客户端据IKEv2 RFC要求。**

弹性服务器当前支持本地用户验证，并且远程验证可选。这对小规模部署是理想的用远程访问用户较少编号和在环境没有对外部验证，授权和核算(AAA)服务器的访问。然而，对于大规模部署和在每个用户的属性希望的方案仍然推荐使用外部AAA服务器认证和授权。AnyConnect EAP实施允许使用远程验证、授权和核算的RADIUS或TACACS。

配置

使用本地数据库的正在验证和Authorizating用户

> **注意**：为了利用在路由器的本地数据库验证用户，需要使用EAP。然而，为了使用EAP，本地认证方法必须是rsa-sig，因此路由器需要对此安装的一适当的证书，并且它不可以是自签名证书。

使用本地用户验证、远程用户和组授权和远程核算的配置示例。

在粗体显示的AnyConnect EAP特定配置

步骤1.启用AAA，并且配置验证、授权和核算列表(aaa属性列表可选)并且添加用户名到本地数据库：

```
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
```

步骤2.配置信任点从CA服务器获取ID证书(路由器可以配置作为CA)：

```
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
```

步骤3.定义Ip local pool对AnyConnect VPN客户端的分配地址：

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

步骤4.创建IKEv2本地授权策略：

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

步骤5. create希望IKEv2建议和策略：

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

步骤6.创建客户端验证AnyConnect EAP方法的一IKEv2配置文件：

```
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
```

> **注意**：配置远程验证方法，在本地认证方法将由CLI前接受，但是可能不生效对CSCva46032的影响的编码版本的。如果复制/粘贴从本文的配置，请保证远程验证方法有infact生效的，并且，如果请有不重新输入命令。

步骤7.禁用HTTP URL根据证书查找：

```
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
```

步骤8.定义用于的加密和散列算法保护数据

```
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
```

> **注意**：*参考*本文确认您的路由器硬件是否支持NGE加密算法(例如以上示例有NGE算法)。否则硬件的SA IPSec安装失效在协商最后阶段。

步骤9.创建IPSec简档：

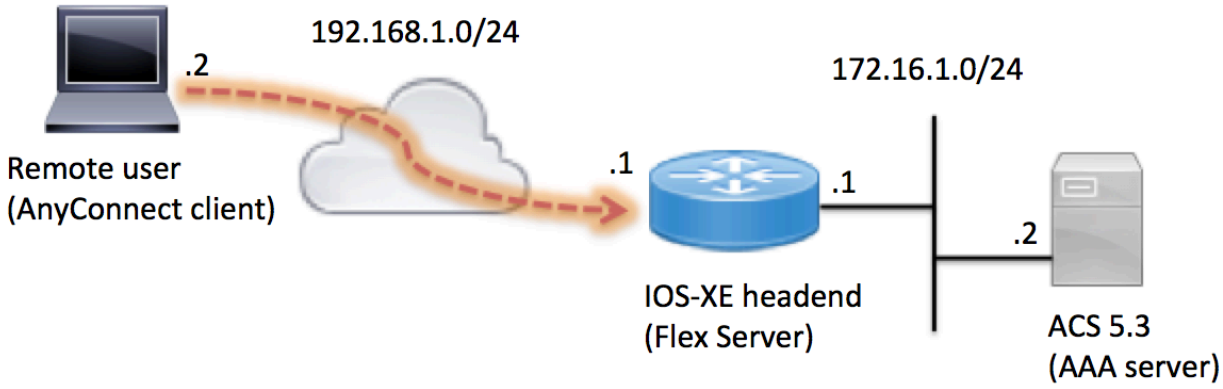
```
crypto ikev2 profile AnyConnect-EAP
match identity remote key-id *$AnyConnectClient$*
authentication remote anyconnect-eap aggregate
authentication local rsa-sig
pki trustpoint IKEv2-TP
aaa authentication anyconnect-eap a-eap-authen-local
aaa authorization group anyconnect-eap list a-eap-author-grp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

步骤10.配置虚拟模板(请关联在IKEv2配置文件的模板)

```
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
```

验证、授权和核算使用远程AAA服务器

网络图



头端配置更改

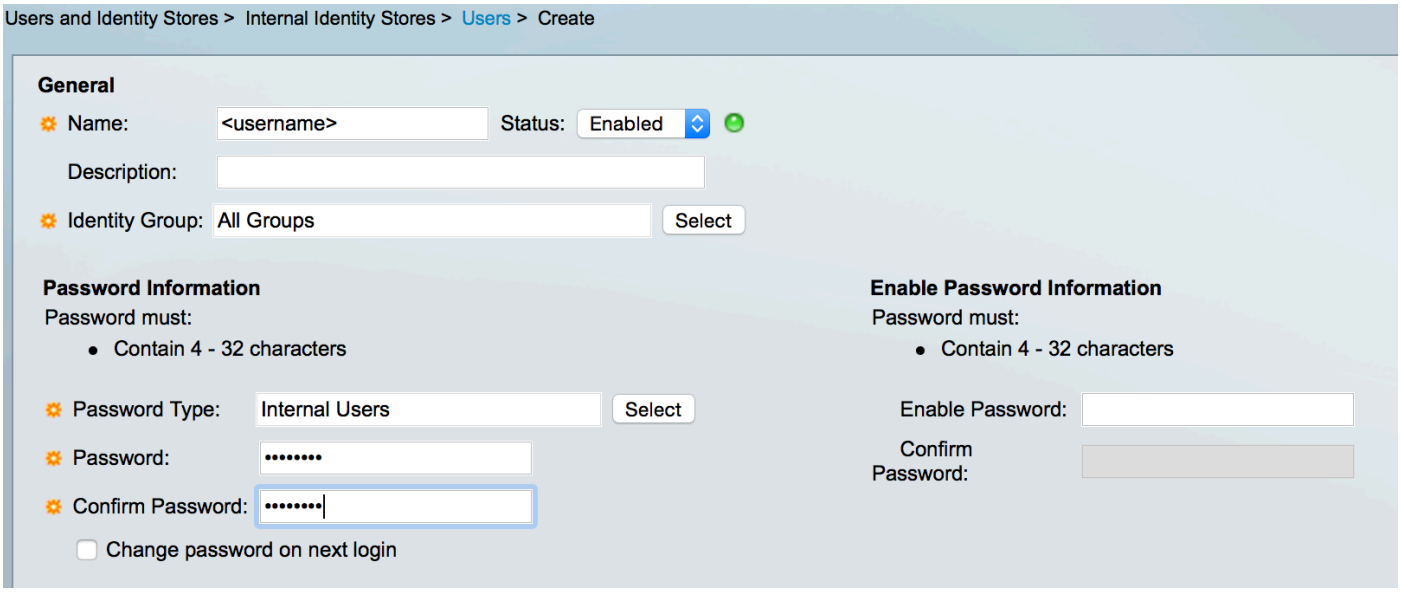
注意：参考配置的其余的上述部分。

```
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
```

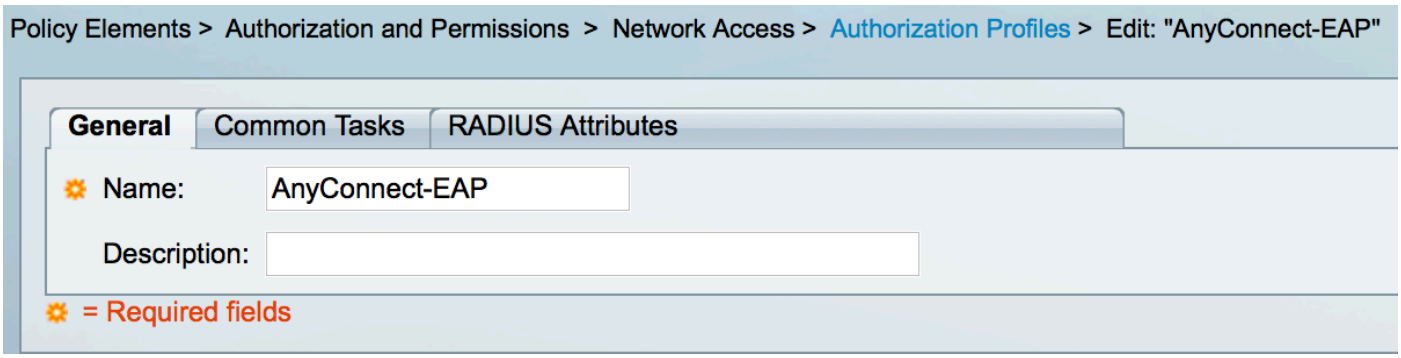
```
!
crypto ikev2 name-mangler NM
eap suffix delimiter @
!
crypto ikev2 profile AnyConnect-EAP
aaa authentication anyconnect-eap a-eap-authen
aaa authorization group anyconnect-eap list a-eap-author <aaa-username>
aaa authorization user anyconnect-eap list a-eap-author name-mangler NM
aaa accounting anyconnect-eap a-eap-acc
```

RADIUS服务器配置

步骤1.创建用户名(为用户和组验证和授权)如镜像所显示， ：



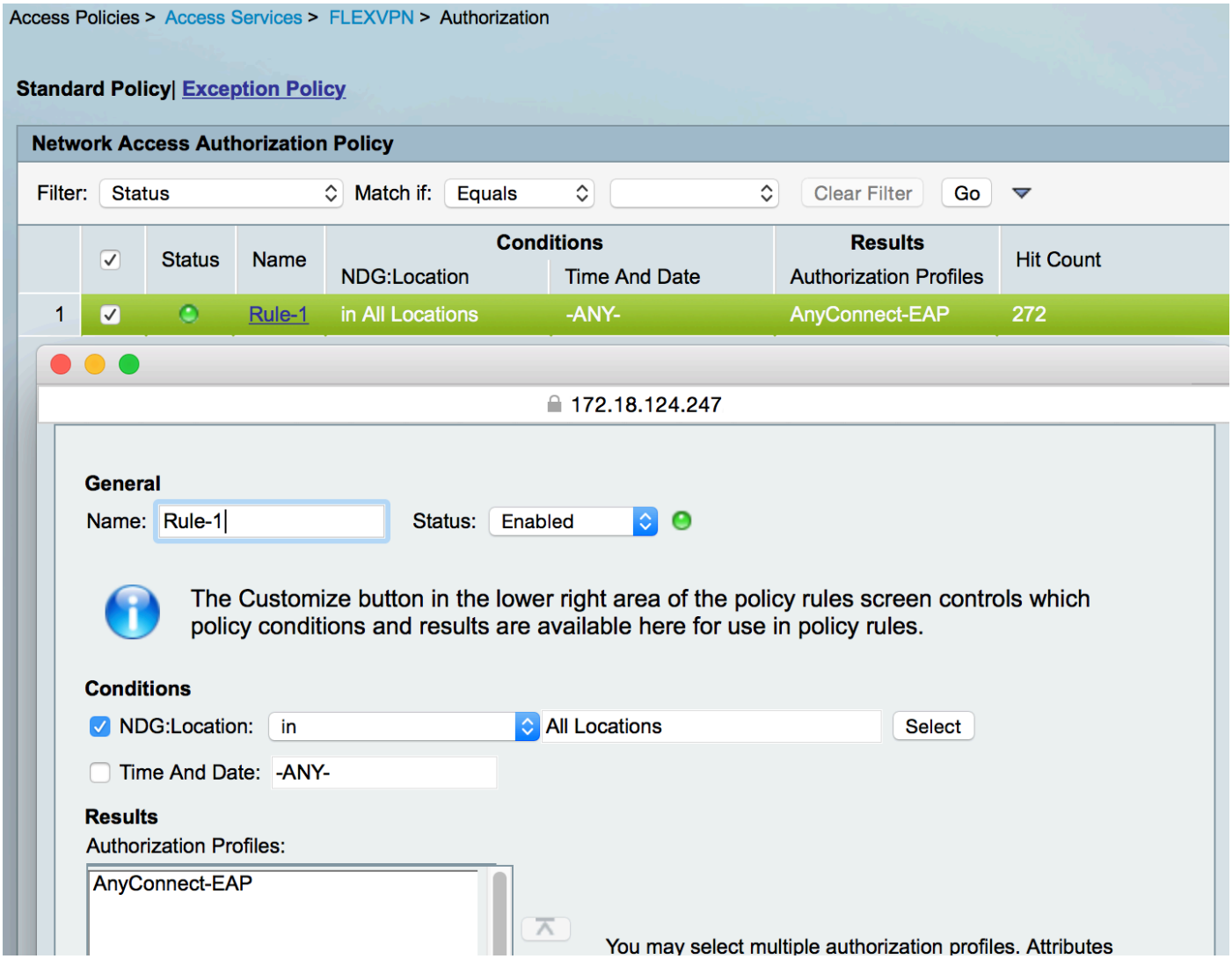
步骤2.如镜像所显示，配置授权策略， ：



第三步：如镜像所显示，现在请添加RADIUS属性， ：

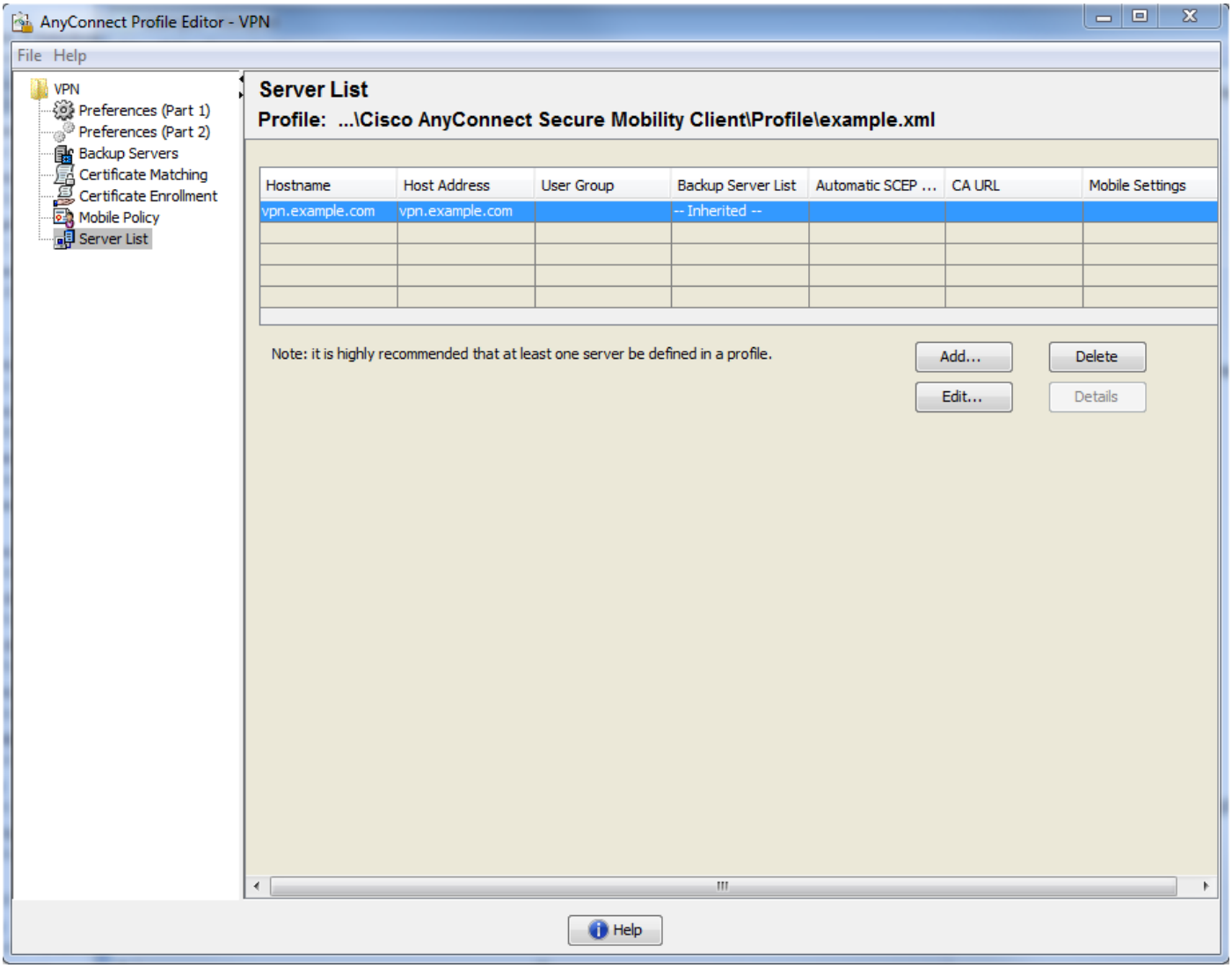
Attribute	Type	Value
cisco-av-pair	String	ipsec:default-domain=ciscotac.com
cisco-av-pair	String	ipsec:banner=AnyConnect
cisco-av-pair	String	ipsec:addr-pool=ACPOOL
cisco-av-pair	String	ipsec:route-set=prefix 172.16.1.0/24
cisco-av-pair	String	ipsec:route-set=access-list split-acl

步骤4.如镜像所显示，请创建访问策略和关联授权策略。



AnyConnect客户端配置文件配置

如镜像所显示，配置客户端配置文件使用AnyConnect配置文件编辑器：



配置文件的XML等同：

```
<?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>
```

> **注意**：AnyConnect使用'*$AnyConnectClient$*'作为类型key-id其默认IKE标识。然而，此标识在AnyConnect配置文件可以手工更改匹配部署需要。当曾经AnyConnect EAP如镜像所显示时，应该设置**StandardAuthenticationOnly**到错误。

更改默认AnyConnect IKE identity(Optional)

如果不要使用客户端使用的默认ike id，您能更改在客户端配置文件的ike id，然而也要求将更改的ike id在Flexvpn服务器配置的ikev2配置文件下。

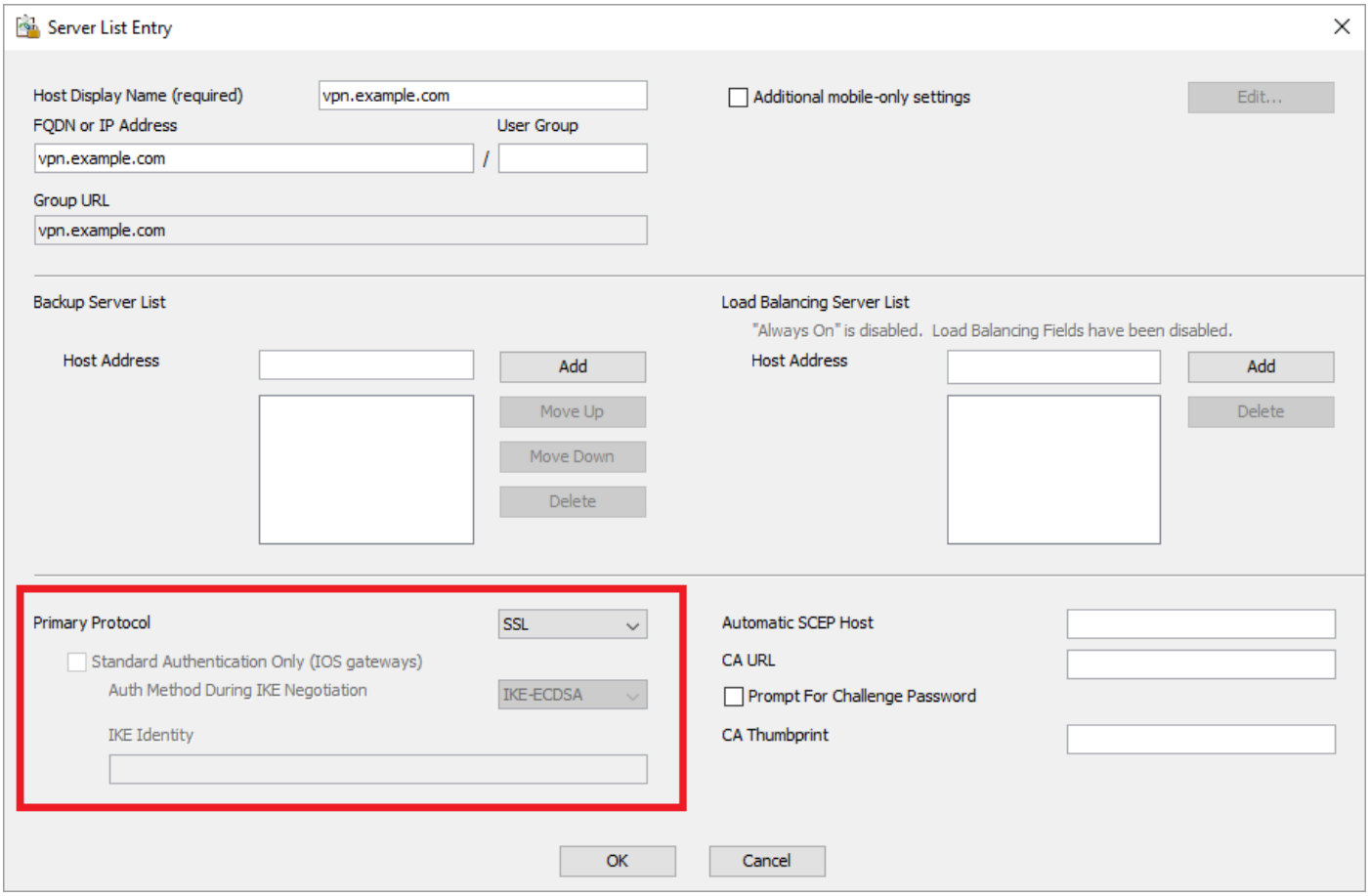
客户端配置文件：

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

FlexServer配置：

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

使用客户端配置文件编辑器，这可能也设置：



提示：当使用客户端配置文件编辑器时， ike ID可能只更改，如果标准的验证被检查。这是已知问题，并且归档bug CSCva64390解决此问题。同时您能手工编辑xml文件使用所有文本编辑，以便属性的“StandardAuthenticationOnly”值设置对错误。

旁路Downloader(Optional)

目前，允许Anyconnect客户端下载客户端升级版本从网关的IOS-XE路由器不支持的功能。因此，如果使用的客户端版本连接到网关比在网关配置的版本更低这将导致连接失败。为了禁用它，在本地策略文件上的一个变化在客户端机器是必要的。欲知更多信息包括本地策略文件的位置请参考崔凡吉莱手工本地策略参数。

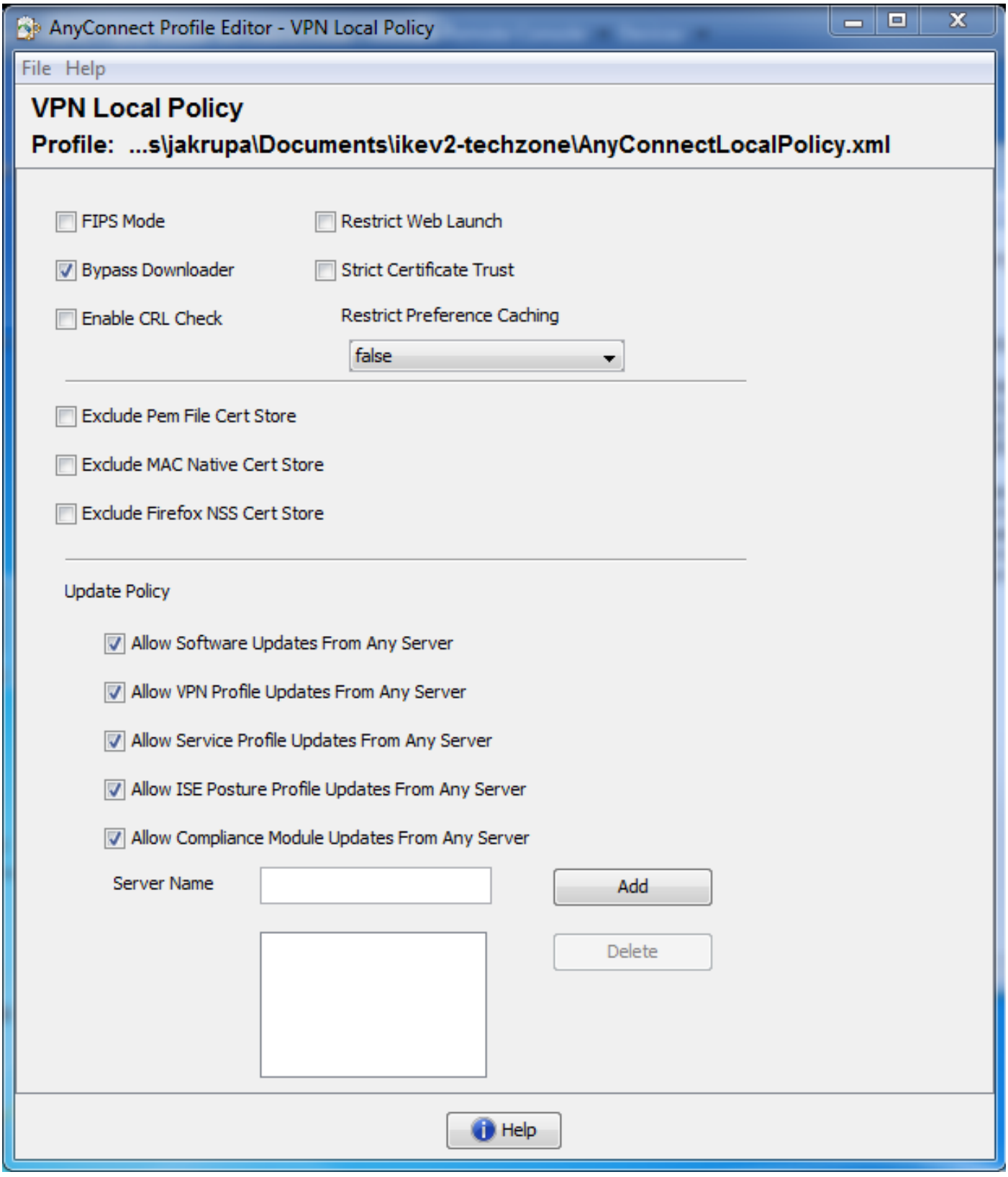
对真的崔凡吉莱**BypassDownloader**值。

```
<?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>
```

通过使用AnyConnect配置文件编辑器工具，它可以执行通过手工编辑文件或：



通信流

IKEv2和EAP交换