

FlexVPN: Acesso remoto de AnyConnect IKEv2 com AnyConnect-EAP

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar](#)

[Usuários da autenticação e do Authorizing que usam o base de dados local](#)

[Autenticação, autorização e contabilidade usando um servidor AAA remoto](#)

[Diagrama de Rede](#)

[Alterações de configuração do final do cabeçalho](#)

[Configuração de servidor RADIUS](#)

[Configuração de perfil do cliente de AnyConnect](#)

[Mude o identity\(Optional\) de AnyConnect IKE do padrão](#)

[Contorneie Downloader\(Optional\)](#)

[Fluxo de comunicação](#)

[Troca IKEv2 e EAP](#)

[Verificar](#)

[Troubleshooting](#)

Introdução

Este documento fornece uma configuração de exemplo de como configurar um final do cabeçalho IOS/IOS-XE para o Acesso remoto usando o método de autenticação IKEv2 e AnyConnect-EAP de AnyConnect.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Liberação 3.15 IOS-XE (15.5(2)S) ou mais tarde
- Versão do IOS 15.5(2)T ou mais tarde
- 3.0 da versão de cliente de AnyConnect ou mais tarde

[Componentes Utilizados](#)

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco ASR1002-X que executa IO XE 3.15
- Versão de cliente 3.1.8009 de AnyConnect que é executado em Windows 7
- Servidor ACS Cisco 5.3 (opcional)

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Informações de Apoio

O AnyConnect-EAP, igualmente conhecido como a autenticação agregada, permite que um server do cabo flexível autentique o cliente de AnyConnect que usa o método AnyConnect-EAP proprietário de Cisco. Os métodos baseados padrão diferente do Extensible Authentication Protocol (EAP) tais como a placa de token EAP-genérica (EAP-GTC), o resumo de mensagem EAP 5 (EAP-MD5) e assim por diante, o server do cabo flexível não se operam no modo de passagem EAP. Toda a comunicação EAP com o cliente termina no server do cabo flexível e a chave de sessão exigida usada para construir o payload do AUTH é computada localmente pelo server do cabo flexível. **O server do cabo flexível tem que autenticar-se ao cliente que usa Certificados segundo as exigências do IKEv2 RFC.**

A autenticação de usuário local é apoiada agora no server do cabo flexível e a autenticação remota é opcional. Isto é ideal para disposições da pequena escala com menos número de usuários de acesso remotos e nos ambientes sem o acesso a uma autenticação externa, a um server da autorização, e da contabilidade (AAA). Contudo, para distribuições em larga escala e nas encenações onde os atributos por usuário são desejados ainda recomenda-se usar um AAA externo separa para a authentication e autorização. A aplicação AnyConnect-EAP permite o uso do radius or tacacs para a autenticação remota, a autorização e a contabilidade.

Configurar

Usuários da autenticação e do Authorizing que usam o base de dados local

Note: A fim autenticar usuários contra o base de dados local no roteador, o EAP precisa de ser usado. Contudo, a fim usar o EAP, o método de autenticação local tem que ser RSA-SIG, assim que o roteador precisa um certificado apropriado instalado nele, e não pode ser um certificado auto-assinado.

Configuração de exemplo que usa a autenticação de usuário local, a autorização do usuário remoto e do grupo e contabilidade remota.

Configuração AnyConnect-EAP específica mostrada em corajoso

Etapa 1. Permita o AAA, e configurar lista da autenticação, da autorização e da contabilidade (a lista de atributos aaa é opcional) e adicionar um username ao base de dados local:

```
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
```

Etapa 2. Configurar um ponto confiável para obter um certificado ID de um server de CA (o roteador pode ser configurado como CA também):

```
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  
rsaкеypair rsaкеy
```

Etapa 3. Defina um conjunto local IP para atribuir endereços aos clientes VPN de AnyConnect:

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

Etapa 4. Crie uma política da autorização local IKEv2:

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

Etapa 5. Create desejou a proposta IKEv2 e a política:

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

Etapa 6. Crie um perfil IKEv2 para o método AnyConnect-EAP de autenticação do cliente:

```
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
```

Note: Configurar o método de autenticação remota antes que o método de autenticação local estiver aceitado pelo CLI, mas não pode tomar o efeito nas versões de código afetadas por [CSCva46032](#). Se você copia/pasta a configuração deste documento, assegure-se de por favor que o método de autenticação remota de fato tome o efeito e se não tem satisfaça reenter o comando.

Etapa 7. O URL DO HTTP do desabilitação baseou a consulta do certificado:

```
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
```

Etapa 8. Defina a criptografia e os algoritmos de hash usados para proteger dados

```
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
```

Note: Consulte [este documento](#) para confirmar se seu hardware de roteador apoia os algoritmos de criptografia NGE (por exemplo o exemplo acima tem algoritmos NGE). Se não a instalação IPsec SA no hardware falhará na última fase da negociação.

Etapa 9. Crie um perfil IPsec:

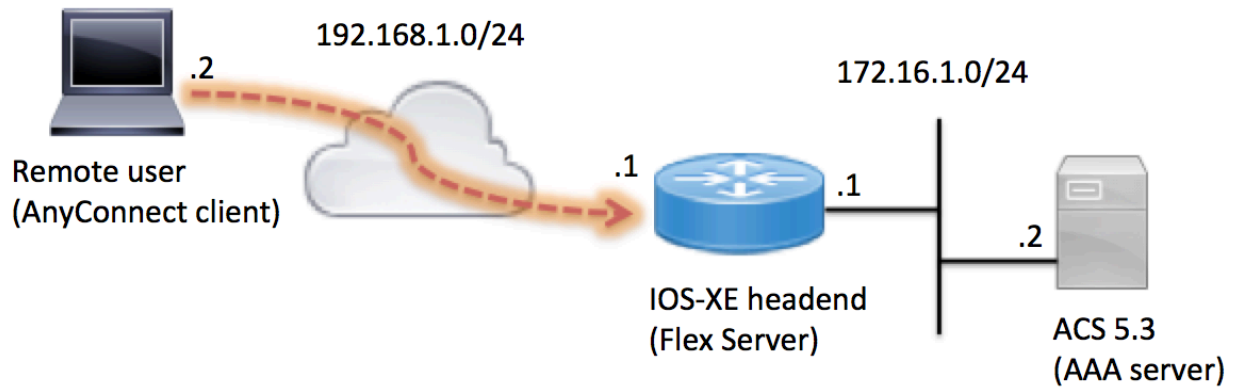
```
crypto ikev2 profile AnyConnect-EAP
match identity remote key-id *$AnyConnectClient$*
authentication remote anyconnect-eap aggregate
authentication local rsa-sig
pki trustpoint IKEv2-TP
aaa authentication anyconnect-eap a-eap-authen-local
aaa authorization group anyconnect-eap list a-eap-author-grp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

Etapa 10. Configurar um virtual-molde (associe o molde no perfil 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
```

Autenticação, autorização e contabilidade usando um servidor AAA remoto

Diagrama de Rede



Alterações de configuração do final do cabeçalho

Note: Refira a seção acima para o resto da configuração.

```

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

```

Configuração de servidor RADIUS

Etapa 1. Crie um username (para a authentication e autorização do usuário e/ou do grupo), segundo as indicações da imagem:

Users and Identity Stores > Internal Identity Stores > Users > Create

General

Name: <username> Status: Enabled

Description:

Identity Group: All Groups

Password Information

Password must:

- Contain 4 - 32 characters

Password Type: Internal Users

Password:

Confirm Password:

Change password on next login

Enable Password Information

Password must:

- Contain 4 - 32 characters

Enable Password:

Confirm Password:

Etapa 2. Configurar a política da autorização, segundo as indicações da imagem:

Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles > Edit: "AnyConnect-EAP"

General Common Tasks RADIUS Attributes

Name: AnyConnect-EAP

Description:

= Required fields

Etapa 3. Adicionar agora atributos RADIUS, segundo as indicações da imagem:

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

Etapa 4. Segundo as indicações da imagem, crie a política da autorização da política de acesso e do associado.

Standard Policy | [Exception Policy](#)


Network Access Authorization Policy

Filter: Status Match if: Equals Clear Filter Go

	<input checked="" type="checkbox"/>	Status	Name	Conditions		Results	Hit Count
				NDG:Location	Time And Date	Authorization Profiles	
1	<input checked="" type="checkbox"/>	●	Rule-1	in All Locations	-ANY-	AnyConnect-EAP	272

172.18.124.247

General
 Name: Status: Enabled ●

 The Customize button in the lower right area of the policy rules screen controls which policy conditions and results are available here for use in policy rules.

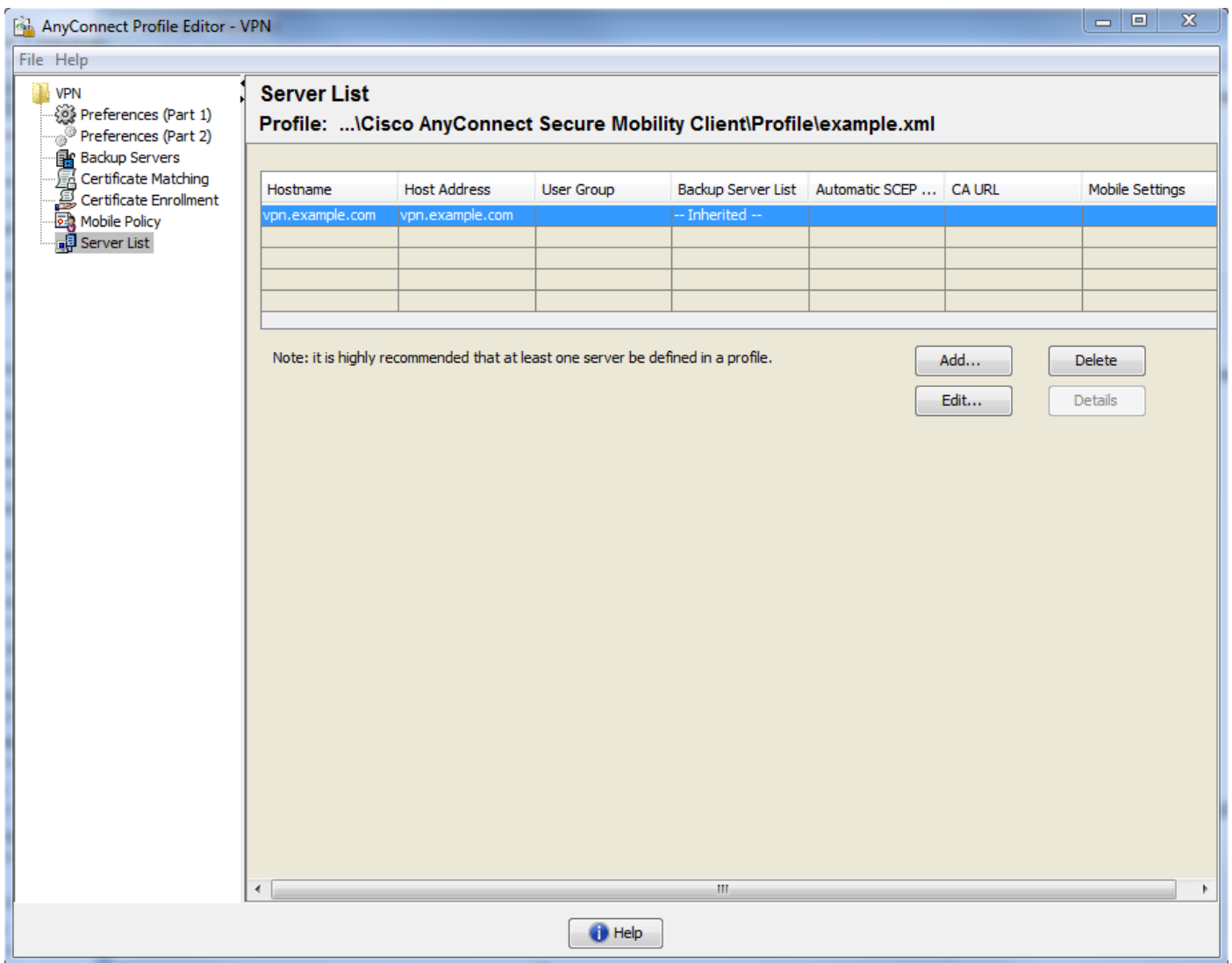
Conditions
 NDG:Location: All Locations Select
 Time And Date:

Results
 Authorization Profiles:

You may select multiple authorization profiles. Attributes

Configuração de perfil do cliente de AnyConnect

Configurar o perfil do cliente usando o editor do perfil de AnyConnect segundo as indicações da imagem:



O equivalente XML do perfil:

```
<?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>
<PPPEExclusion UserControllable="false">Automatic
<PPPEExclusionServerIP UserControllable="false"></PPPEExclusionServerIP>
</PPPEExclusion>
<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>

```

Note: AnyConnect usa “*\$AnyConnectClient\$” como sua identidade do padrão IKE do tipo chave-identificação. Contudo, esta identidade pode manualmente ser mudada no perfil de AnyConnect para combinar necessidades do desenvolvimento. **StandardAuthenticationOnly** deve ser ajustado a falso ao usar o AnyConnect-EAP segundo as indicações da imagem.

Mude o identity(Optional) de AnyConnect IKE do padrão

Se você não quer usar a identificação do ike do padrão usada pelo cliente, você pode mudar a identificação do ike no perfil do cliente, porém igualmente exigiu a identificação do ike ser mudado sob o perfil ikev2 configurado no server de Flexvpn.

Perfil do cliente:

```

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

```

Configuração de FlexServer:

```

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

```

Isto pode igualmente ser ajustado usando o editor do perfil do cliente:

Server List Entry

Host Display Name (required) Additional mobile-only settings

FQDN or IP Address /

Group URL

Backup Server List

Host Address

Load Balancing Server List

"Always On" is disabled. Load Balancing Fields have been disabled.

Host Address

Primary Protocol Standard Authentication Only (IOS gateways)

Auth Method During IKE Negotiation

IKE Identity

Automatic SCEP Host

CA URL

Prompt For Challenge Password

CA Thumbprint

Tip: Ao usar o editor do perfil do cliente, o ike ID pode somente ser mudado se a autenticação padrão é verificada. Este é um problema conhecido e o erro [CSCva64390](#) foi arquivado para endereçar esta edição. Entretanto você pode manualmente editar o arquivo do xml usando todo o editor de texto de modo que o valor para o atributo "StandardAuthenticationOnly" seja ajustado a falso.

Desvio Downloader(Optional)

Atualmente, a característica que permite que o cliente de Anyconnect transfira a versão atualizada do cliente do gateway não é apoiada no Roteadores IOS-XE. Assim se a versão de cliente que está sendo usada para conectar ao gateway é mais baixa do que a versão configurada no gateway isto conduzirá à conexão uma falha. A fim desabilitá-lo, uma mudança no arquivo da política local na máquina cliente é necessária. Para mais informação que inclui o lugar do arquivo da política local refira por favor [parâmetros da política local da mudança manualmente](#).

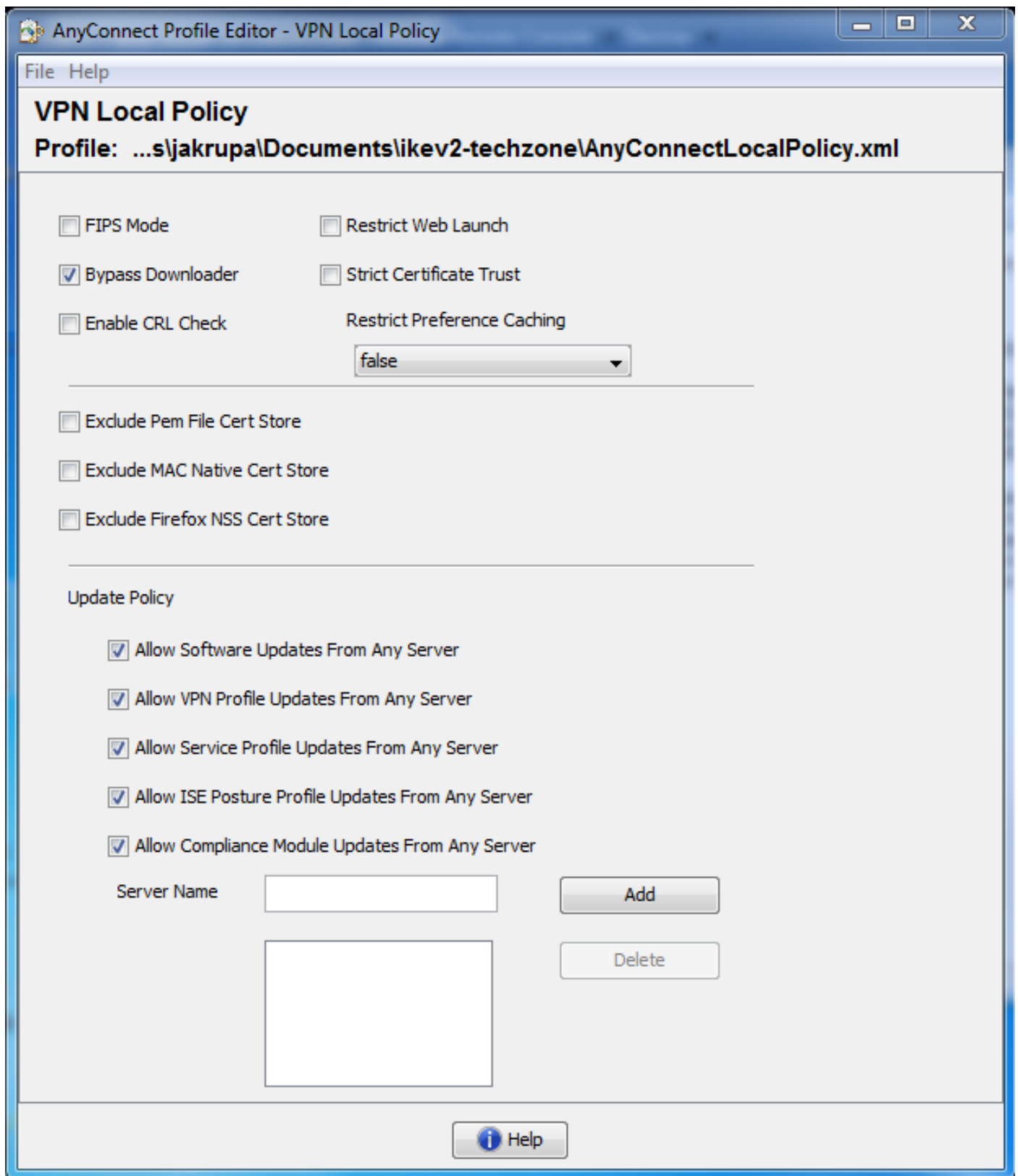
Mude o valor de **BypassDownloader** para retificar.

```
<?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>
```

Pode ser feito com manualmente da edição do arquivo ou usando a ferramenta do editor do perfil de AnyConnect:



Fluxo de comunicação

Troca IKEv2 e EAP

