Configurar os sem clientes SSL VPN (WebVPN) no ASA

Índice

Introdução

Este documento fornece uma configuração direta para o 5500 Series adaptável da ferramenta de segurança de Cisco (ASA) a fim permitir o acesso do secure sockets layer dos sem clientes (SSL) VPN aos recursos de rede interna. Os sem clientes SSL Virtual Private Network (WebVPN) permitem limitado, mas o artigo de valor, acesso seguro à rede corporativa de todo o lugar. Os usuários podem conseguir o acesso com base em navegador seguro aos recursos corporativos a qualquer hora. Nenhum cliente adicional é precisado a fim aceder aos recursos internos. O acesso é fornecido usando um protocolo de transferência de hipertexto sobre a conexão SSL.

Os sem clientes SSL VPN fornecem o acesso seguro e fácil a uma escala larga dos recursos da Web e Web-permitido e aplicativos legados de quase todo o computador que puder alcançar locais do Internet do protocolo de transferência de hipertexto (HTTP). Isso inclui:

- Web site internos
- Microsoft SharePoint 2003, 2007, e 2010
- Acesso à Web 2003, 2007, e 2013 do Microsoft outlook

- Microsoft outlook Web App 2010
- Acesso à Web do dominó (DWA) 8.5 e 8.5.1
- Server 4.x da apresentação de Citrix Metaframe
- Versão 5 à 6.5 de Citrix XenApp
- Versão 5 à 5.6 de Citrix XenDesktop, e 7.5
- Opinião 4 de VMware

Uma lista de software suportado pode ser encontrada em Plataformas apoiadas VPN, 5500 Series de Cisco ASA.

Pré-requisitos

Requisitos

Certifique-se de atender a estes requisitos antes de tentar esta configuração:

- navegador SSL-permitido
- ASA com versão 7.1 ou mais recente
- Certificado X.509 emitido ao Domain Name ASA
- Porta TCP 443, que não deve ser obstruída ao longo do trajeto do cliente ao ASA

A lista completa das exigências pode ser encontrada em Plataformas apoiadas VPN, 5500 Series de Cisco ASA.

Componentes Utilizados

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

- Versão ASA 9.4(1)
- Versão 7.4(2) adaptável do Security Device Manager (ASDM)
- ASA 5515-X

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

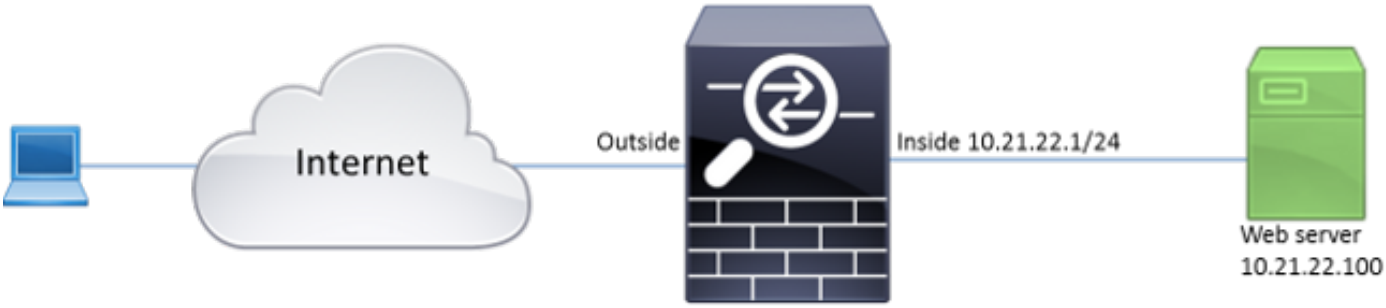
Configurar

Este artigo descreve o processo de configuração para o ASDM e o CLI. Você pode escolher seguir qualquer uma das ferramentas a fim configurar o WebVPN, mas algumas das etapas de configuração podem somente ser conseguidas com o ASDM.

> **Note**: Use a ferramenta de consulta de comandos (clientes registrados somente) para obter mais informação sobre os comandos usados nesta seção.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



Informações de Apoio

O WebVPN usa o protocolo SSL a fim fixar os dados transferidos entre o cliente e o server. Quando o navegador inicia uma conexão ao ASA, o ASA apresenta seu certificado para autenticar-se ao navegador. A fim assegurar-se de que a conexão entre o cliente e o ASA seja segura, você precisa de fornecer o ASA o certificado que é assinado pelo Certificate Authority esse as confianças do cliente já. Se não o cliente não terá os meios verificar a autenticidade do ASA que conduz à possibilidade do ataque que envolva pessoas e da experiência deficiente do usuário, porque o navegador produz um aviso que a conexão não está confiada.

> **Note**: À revelia, o ASA gerencie um certificado X.509 auto-assinado em cima da partida. Este certificado é usado a fim servir à revelia conexões de cliente. Não se recomenda usar este certificado porque sua autenticidade não pode ser verificada pelo navegador. Além disso, este certificado é regenerado em cima de cada repartição assim que muda após cada repartição.

A instalação certificada é fora do âmbito deste documento.

Configuração

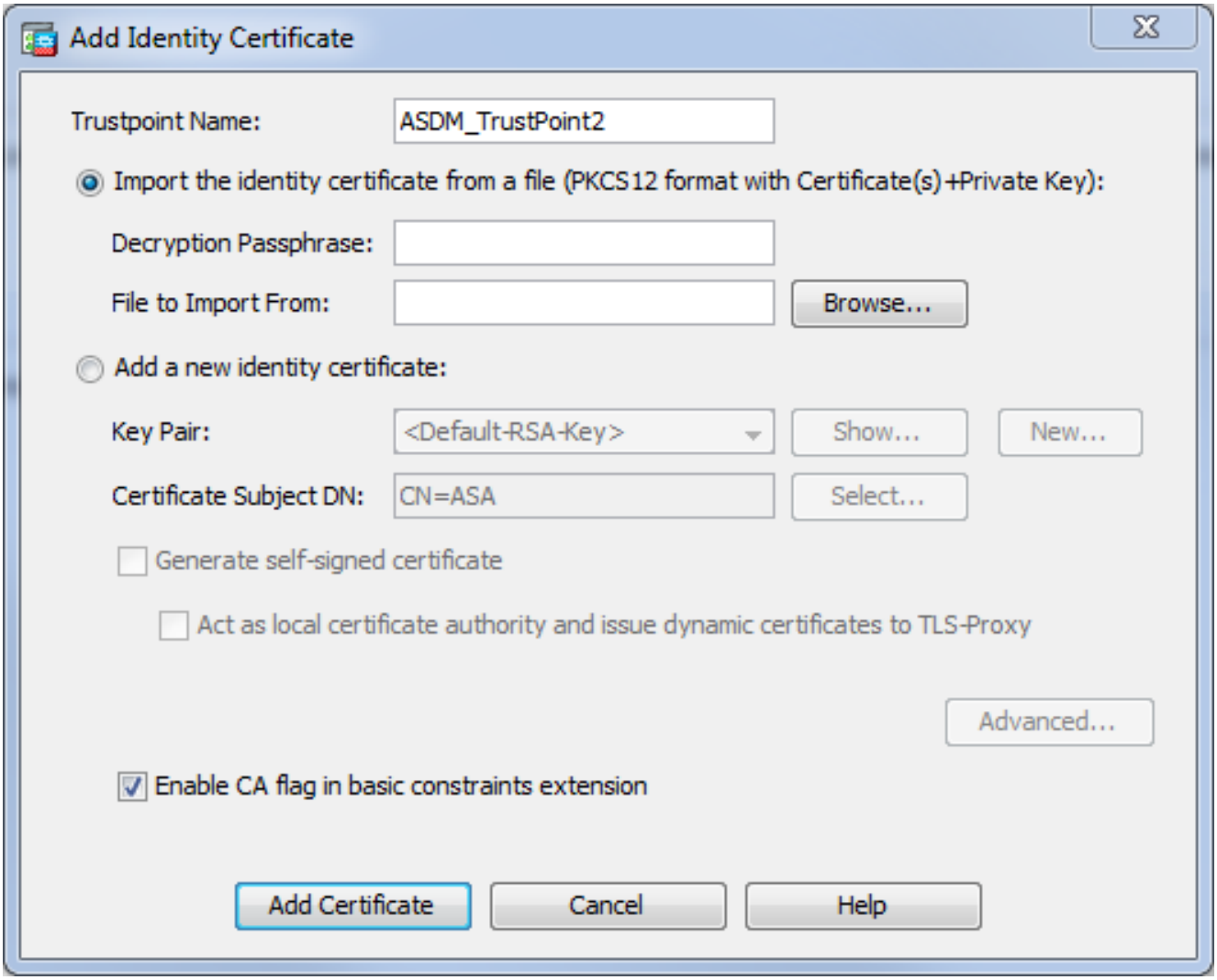
Configurar o WebVPN no ASA com cinco etapas principal:

- Configurar o certificado que será usado pelo ASA.
- Permita o WebVPN em uma relação ASA.
- Crie uma lista dos server e/ou do Uniform Resource Locator (URL) para o acesso WebVPN.
- Crie uma política do grupo para usuários WebVPN.
- Aplique a política nova do grupo a um grupo de túneis.

> **Note**: No ASA libera-se mais tarde do que a liberação 9.4, o algoritmo usado para escolher cifras SSL foi mudada (veja Release Note para a série de Cisco ASA, 9.4(x)).If somente que os clientes curva-capazes elípticos serão usados, a seguir é seguro usar a chave privada elíptico da curva para o certificado. Se não a série feita sob encomenda da cifra deve ser usada a fim evitar ter o presente ASA um certificado provisório auto-assinado. Você pode configurar o ASA para usar somente cifras RSA-baseadas com o comando "AES256-SHA:AES128-SHA:DHE-RSA-AES256-SHA:DHE-RSA-AES128-SHA:DES-CBC3-sha:des-

CBC-SHA:RC4-SHA:RC4-Md5" feito sob encomenda da cifra tlsv1.2 SSL.

1. **Opção 1** - Importe o certificado com o arquivo do pkcs12.Escolha a **configuração > o Firewall > avançou o > gerenciamento de certificado > o > Add dos certificados de identidade**. Você pode instalá-lo com o arquivo do pkcs12 ou para colar os índices no Privacy Enhanced Mail (PEM)
formate.

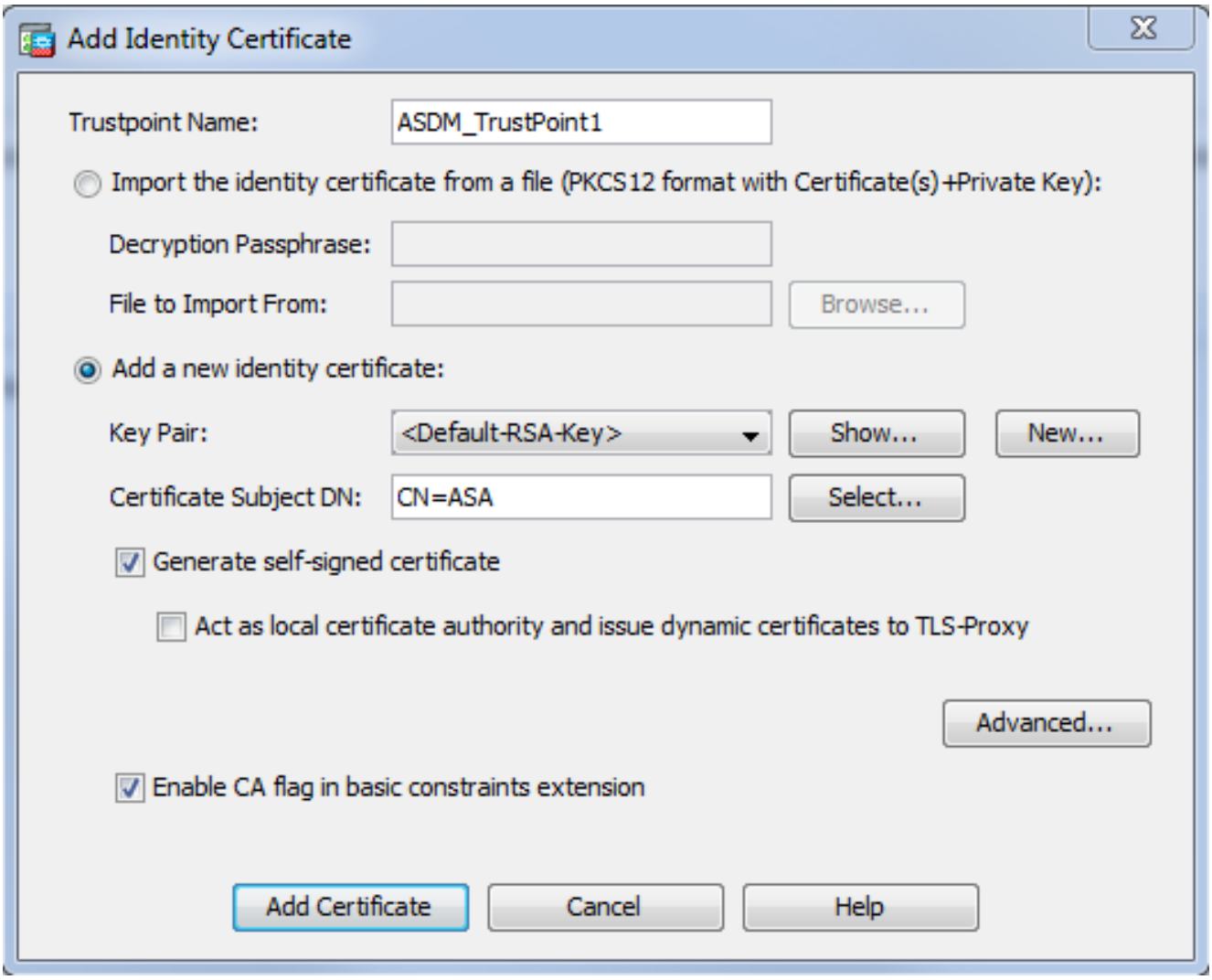


CLI:

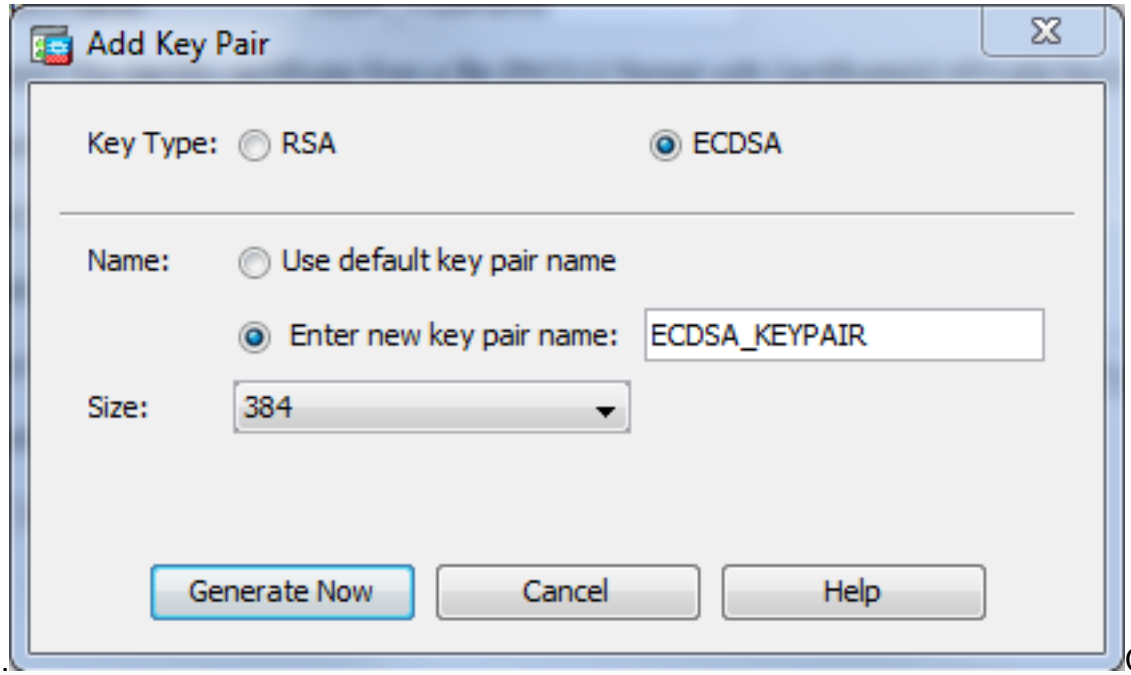
```
ASA(config)# crypto ca import TrustPoint-name pkcs12 "password"


Enter the base 64 encoded pkcs12.
End with the word "quit" on a line by itself:
MIIJUQIBAzCCCRcGCSqGSIb3DQEHAaCCCQgEggkEMIIJADCCBf8GCSqGSIb3DQEH
BqCCBfAwggXsAgEAMIIF5QYJKoZIhvcNAQcBMBwGCiqGSIb3DQEMAQYwDgQI8F3N
+vkvjUgCAggAgIIFuHFrV6enVflNv3sBByB/yZswhELY5KpeALbXhfrFDpLNncAB
z3xMfg6JkLYR6Fag1KjShg+o4qkDh8r9y9GQpaBt8x3Ozo0JJxSAafmTWqDOEOS/
7mHsaKMoao+pv2LqKTWh0O7No4Ycx75Y5sOhyuQGPhLJRdionbi1s1ioe4Dplx1b


--- output ommited ---


Enter the base 64 encoded pkcs12.
End with the word "quit" on a line by itself:
```

```
MIIJUQIBAzCCCRcGCSqGSIb3DQEHAaCCCQgEggkEMIIJADCCBf8GCSqGSIb3DQEH
BqCCBfAwggXsAgEAMIIF5QYJKoZIhvcNAQcBMBwGCiqGSIb3DQEMAQYwDgQI8F3N
+vkvjUgCAggAgIIFuHFrV6enVflNv3sBByB/yZswhELY5KpeALbXhfrFDpLNncAB
z3xMfg6JkLYR6Fag1KjShg+o4qkDh8r9y9GQpaBt8x3Ozo0JJxSAafmTWqDOEOS/
7mHsaKMoao+pv2LqKTWh0O7No4Ycx75Y5sOhyuQGPhLJRdionbi1s1ioe4Dplx1b

quit


INFO: Import PKCS12 operation completed successfully
```

Opção 2 - Crie um certificado auto-assinado.Escolha a **configuração > o Firewall > avançou o > gerenciamento de certificado > o > Add dos certificados de identidade**.Clique **adicionar um** botão de rádio **novo do certificado de identidade**. Verifique a **caixa de verificação do certificado auto-assinado da geração**. Escolha um Common Name (CN) esse Domain Name dos fósforos do
ASA.



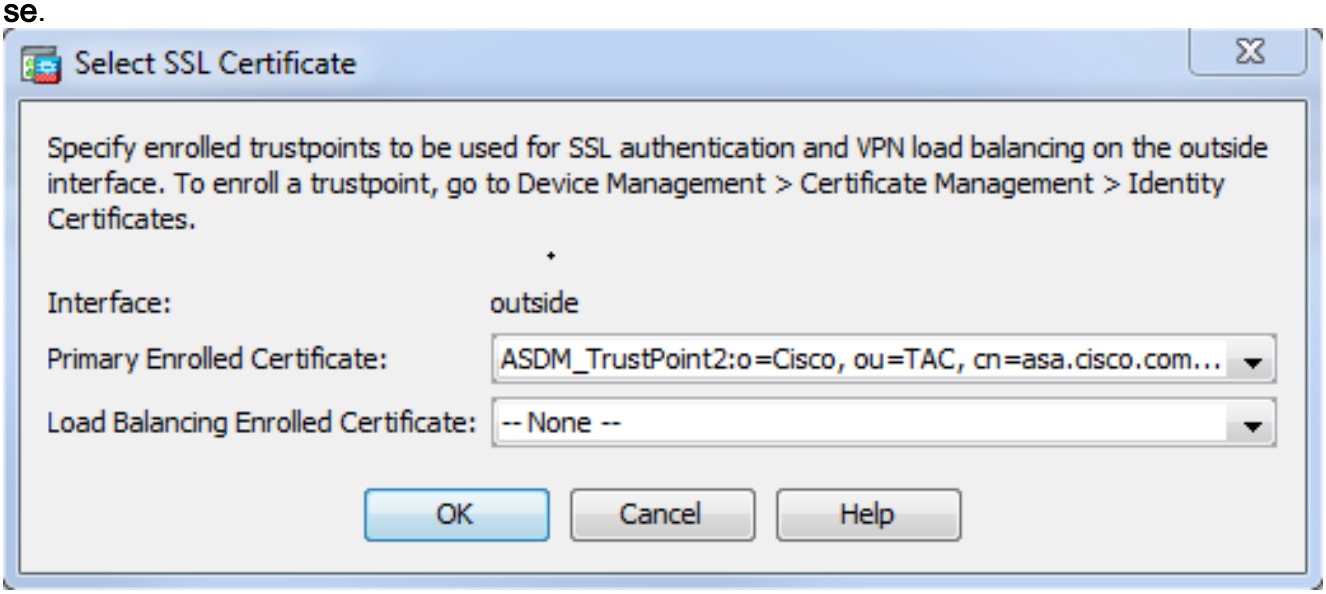
Clique **novo** a fim criar o keypair para o certificado. Escolha o tipo, o nome, e o tamanho



chaves.CLI:

```
ASA(config)# crypto key generate ecdsa label ECDSA_KEYPAIR noconfirm

ASA(config)# crypto ca trustpoint TrustPoint1
ASA(config-ca-trustpoint)# revocation-check none
ASA(config-ca-trustpoint)# id-usage ssl-ipsec
ASA(config-ca-trustpoint)# no fqdn
ASA(config-ca-trustpoint)# subject-name CN=ASA
ASA(config-ca-trustpoint)# enrollment self
ASA(config-ca-trustpoint)# keypair ECDSA_KEYPAIR
ASA(config-ca-trustpoint)# exit
ASA(config)# crypto ca enroll TrustPoint1 noconfirm
```

2. Escolha o certificado que será usado para servir conexões VPN da Web.Escolha a **configuração > o acesso remoto VPN > avançou > ajustes SSL**. Do menu dos Certificados, escolha o ponto confiável associado com o certificado desejado para a interface externa. O clique **aplica-se**.

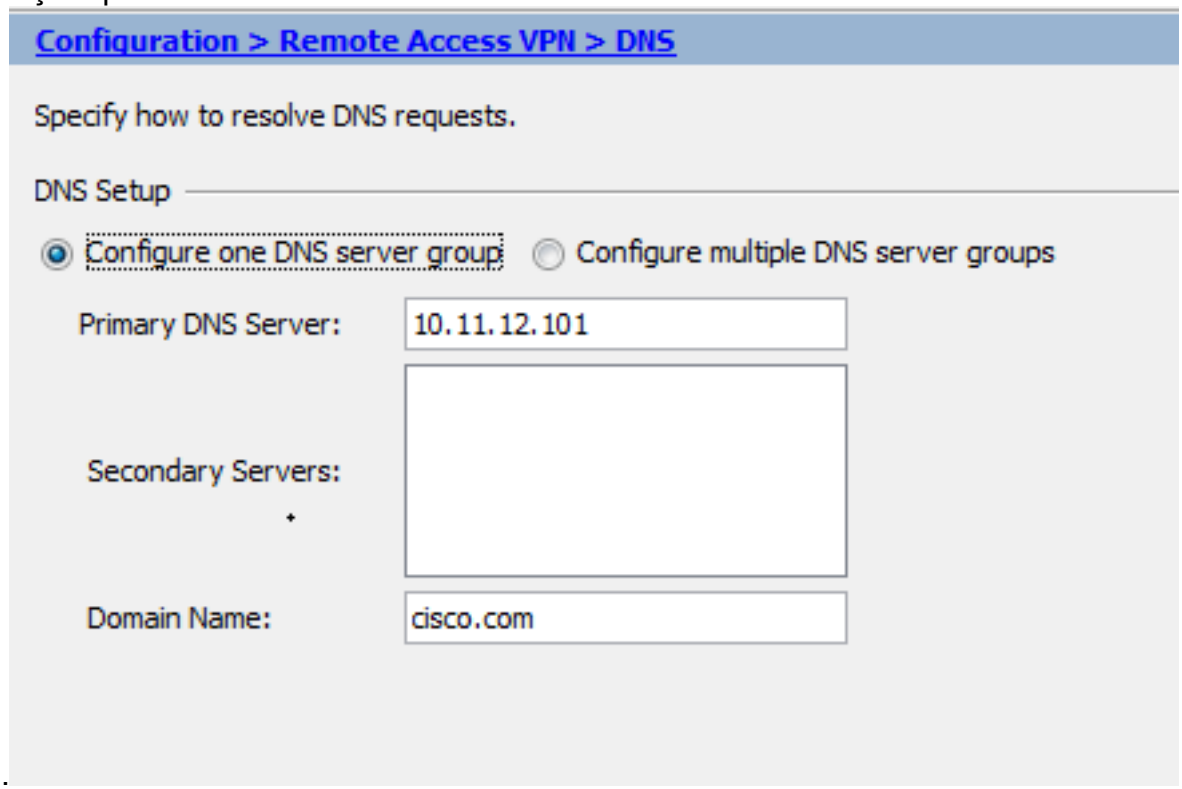


Configuração de CLI equivalente:

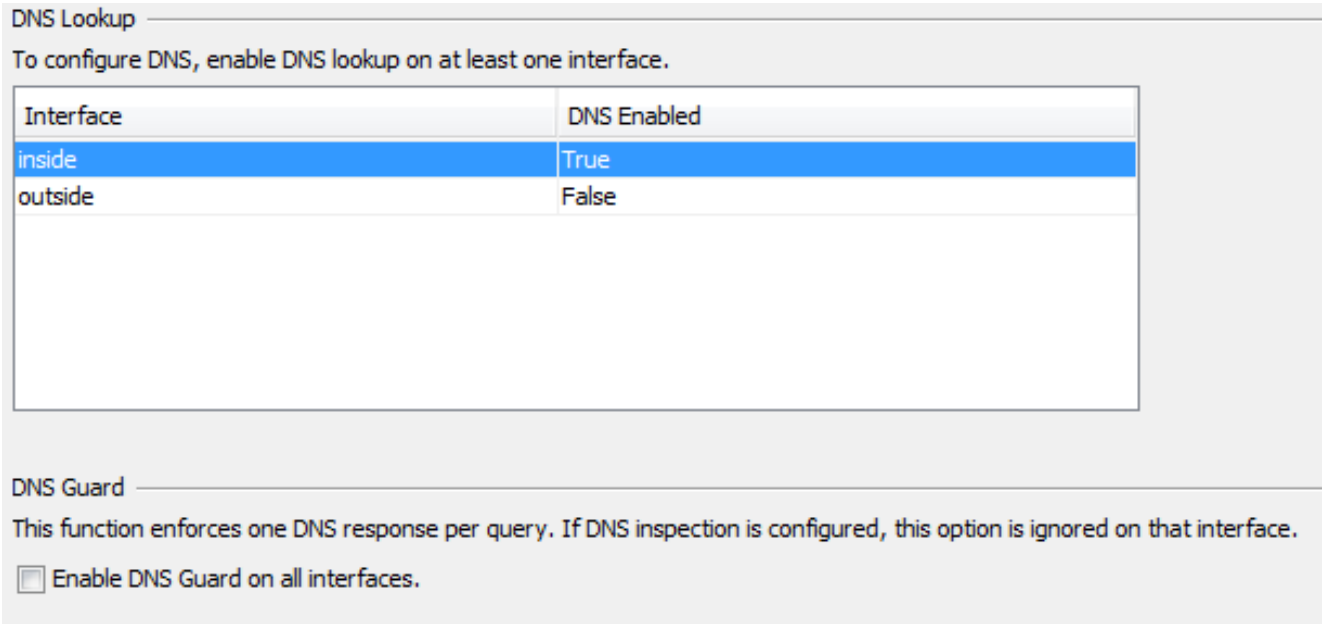
```
ASA(config)# ssl trust-point <trustpoint-name> outside
```

3. (Opcional) permita consultas do Domain Name Server (DNS).O servidor VPN da Web atua como um proxy para conexões de cliente. Significa que o ASA cria conexões aos recursos em nome do cliente. Se os clientes exigem conexões aos recursos que usam Domain Name, a seguir o ASA precisa de executar a pesquisa de DNS.Escolha a **configuração > o acesso**

remoto VPN > o DNS.Configurar pelo menos um servidor DNS e permita pesquisas de DNS na relação que enfrenta o servidor



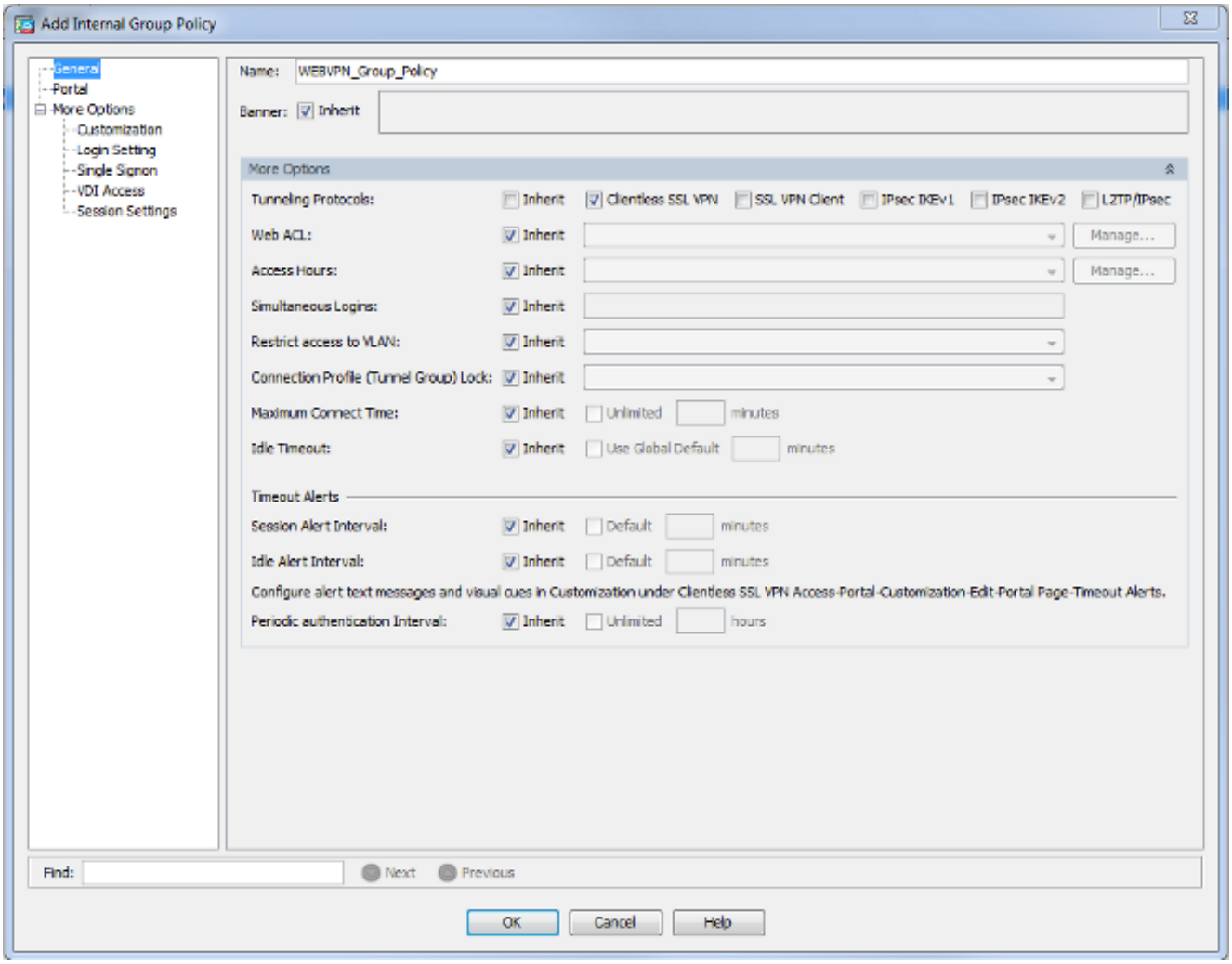
DNS.



CLI:

```
ASA(config)# dns domain-lookup inside
ASA(config)# dns server-group DefaultDNS
ASA(config-dns-server-group)# name-server 10.11.12.101
```

4. (Opcional) crie a política do grupo para conexões VPN da Web.Escolha a **configuração > o acesso do acesso remoto VPN > dos sem clientes SSL VPN > a Política interna de grupo do > Add das políticas do grupo**.Sob opções gerais mude o valor dos protocolos de Tunelling aos “sem clientes SSL
VPN”.



CLI:

```
ASA(config)# group-policy WEBVPN_Group_Policy internal
ASA(config)# group-policy WEBVPN_Group_Policy attributes
ASA(config-group-policy)# vpn-tunnel-protocol ssl-clientless
```

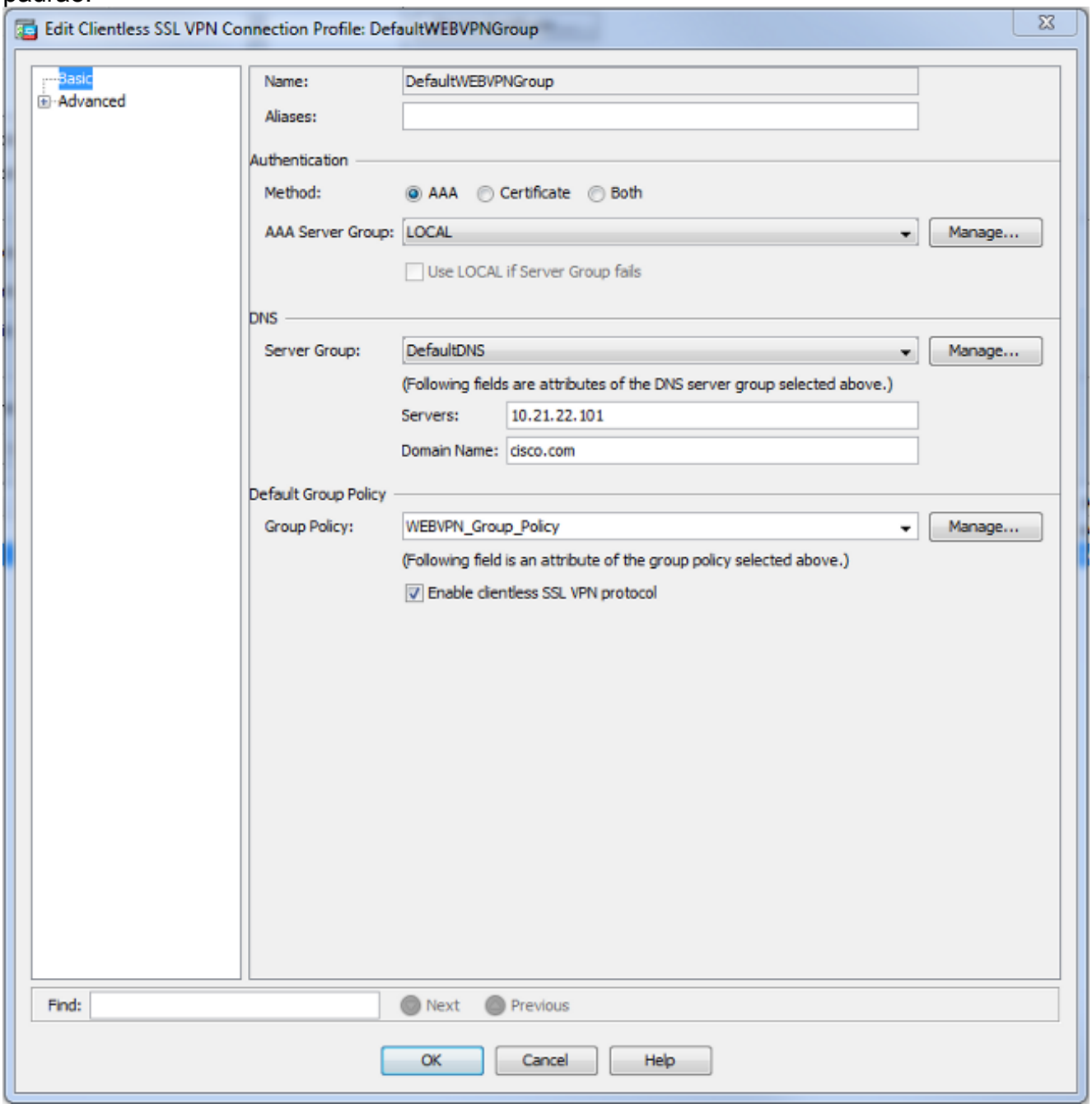
5. Configurar o perfil de conexão.No ASDM, escolha a **configuração > o acesso remoto VPN > o acesso > os perfis de conexão dos sem clientes SSL VPN**.
   Para uma vista geral dos perfis de conexão e das políticas do grupo, consulte o guia de configuração de CLI da série VPN de Cisco ASA, os 9.4 - perfis de conexão, as políticas do grupo, e os usuários.Àrevelia, as conexões VPN da Web usam o perfil de DefaultWEBVPNGroup. Você pode criar perfis adicionais.**Note**: Há umas várias maneiras de atribuir usuários a outros perfis.

   - Os usuários podem manualmente selecionar o perfil de conexão da lista de drop-down ou com uma URL específica. Veja ASA 8.x: Permita que os usuários selecionem um grupo no início de uma sessão WebVPN através do Grupo-pseudônimo e do método Grupo-URL.

   - Quando você usa um servidor ldap, você pode atribuir o perfil de usuário baseado nos atributos recebidos do servidor ldap, vê o uso ASA do exemplo de configuração dos mapas do atributo LDAP.

   - Quando você usa a autenticação certificado-baseada dos clientes, você pode traçar o usuário aos perfis baseados nos campos contidos no certificado, vê o guia de configuração de CLI da série VPN de Cisco ASA, 9.4 - configurar o grupo do certificado que combina para IKEv1.

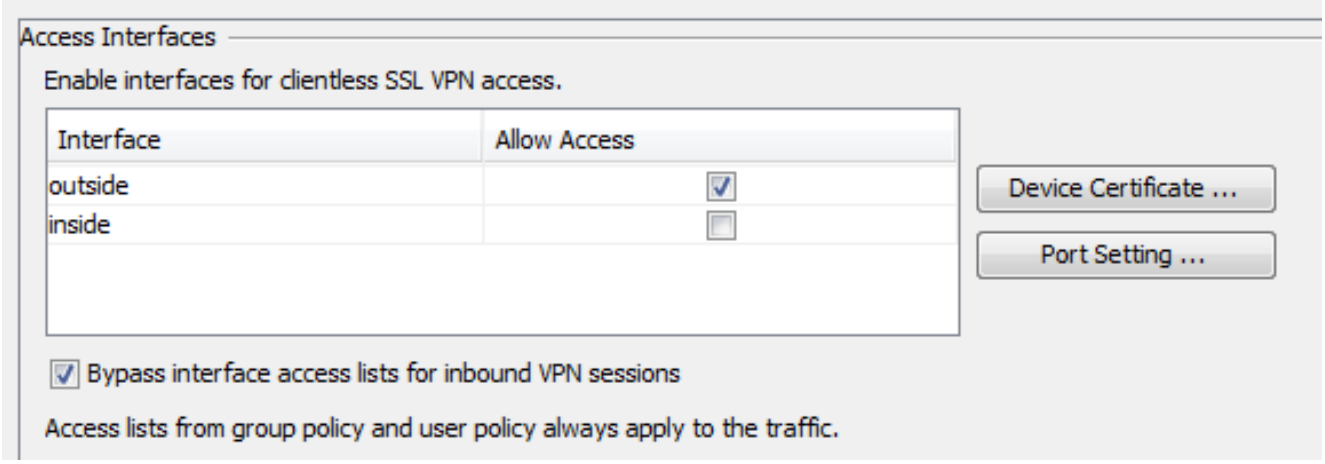
- A fim atribuir manualmente os usuários à política do grupo, veja o guia de configuração de CLI da série VPN de Cisco ASA, 9.4 - configurando atributos para usuários individuaisEdite o perfil de DefaultWEBVPNGroup e escolha o WEBVPN_Group_Policy sob a política do grupo
padrão.



CLI:

```
ASA(config)# tunnel-group DefaultWEBVPNGroup general-attributes
ASA(config-tunnel-general)# default-group-policy WEBVPN_Group_Policy
```

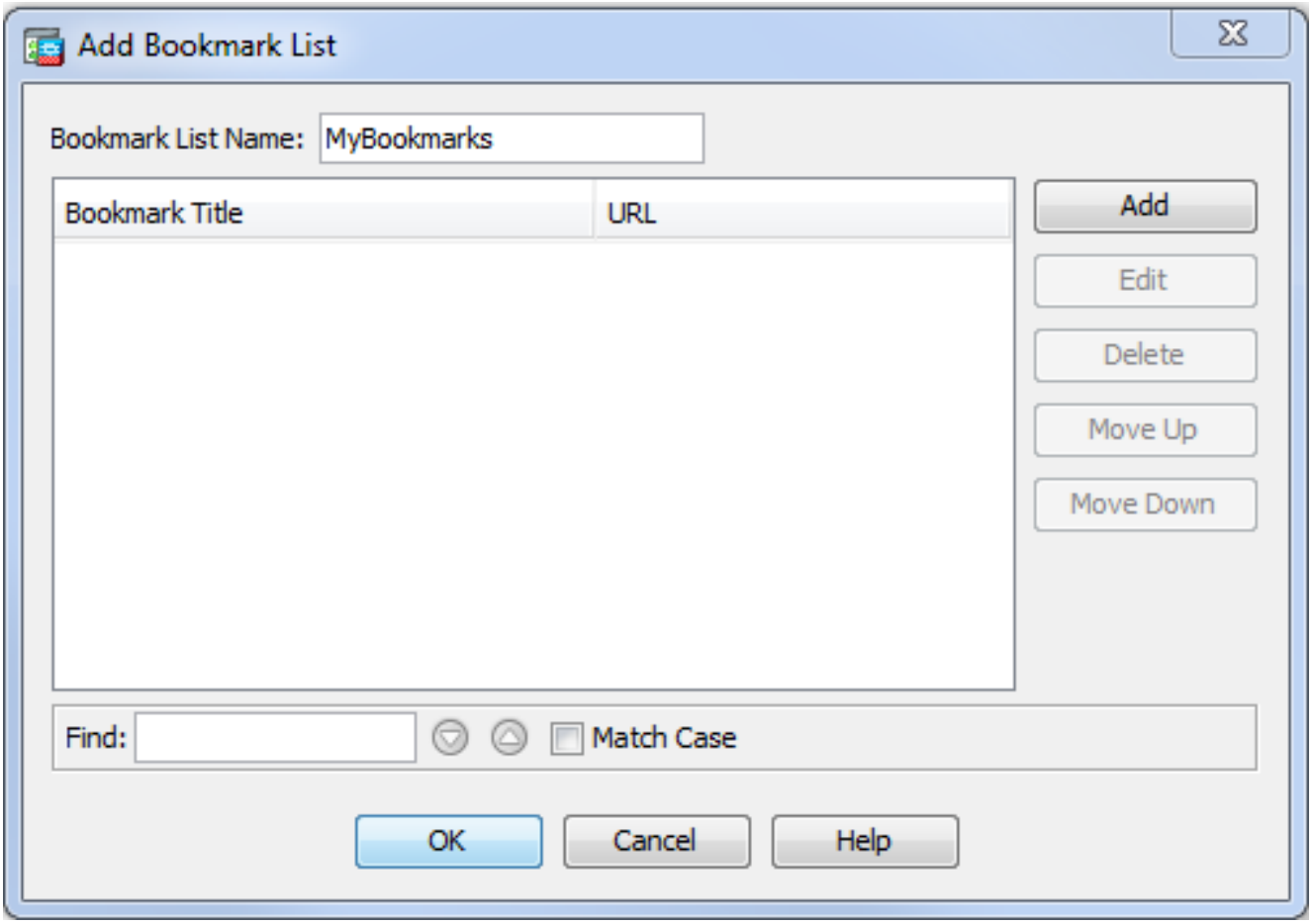
6. A fim permitir o WebVPN na interface externa, escolha a **configuração > o acesso remoto VPN > o acesso > os perfis de conexão dos sem clientes SSL VPN**.Verifique a caixa de seleção do **acesso reservar** ao lado da interface
externa.



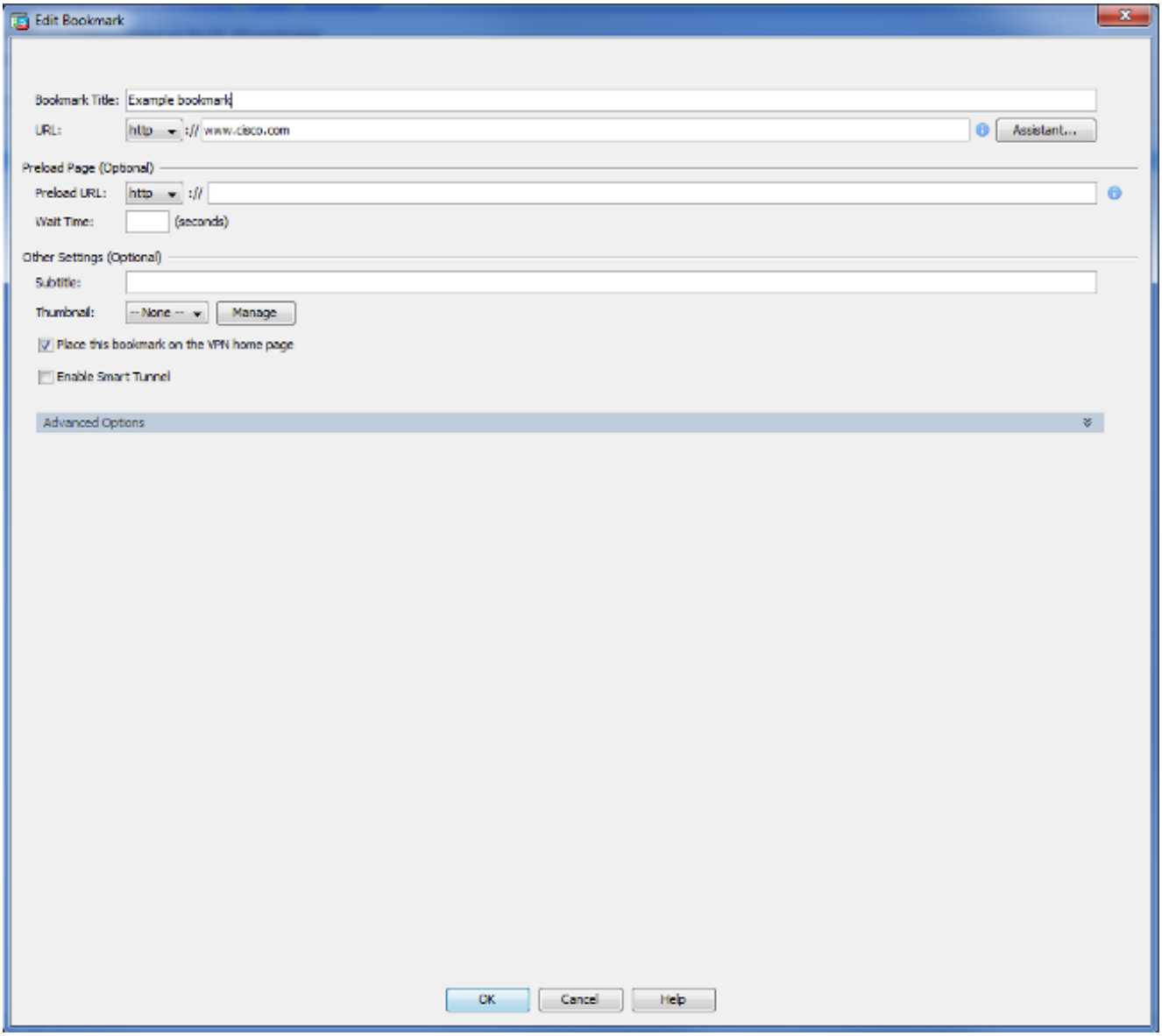
CLI:

```
ASA(config)# webvpn
ASA(config-webvpn)# enable outside
```

7. (Opcional) crie endereços da Internet para o índice.Os endereços da Internet permitem que o usuário consulte facilmente os recursos internos sem ter que recordar as URL.A fim criar um endereço da Internet, escolha a **configuração > o acesso remoto VPN > do acesso > do Portal > dos endereços da Internet dos sem clientes SSL VPN > Add**.

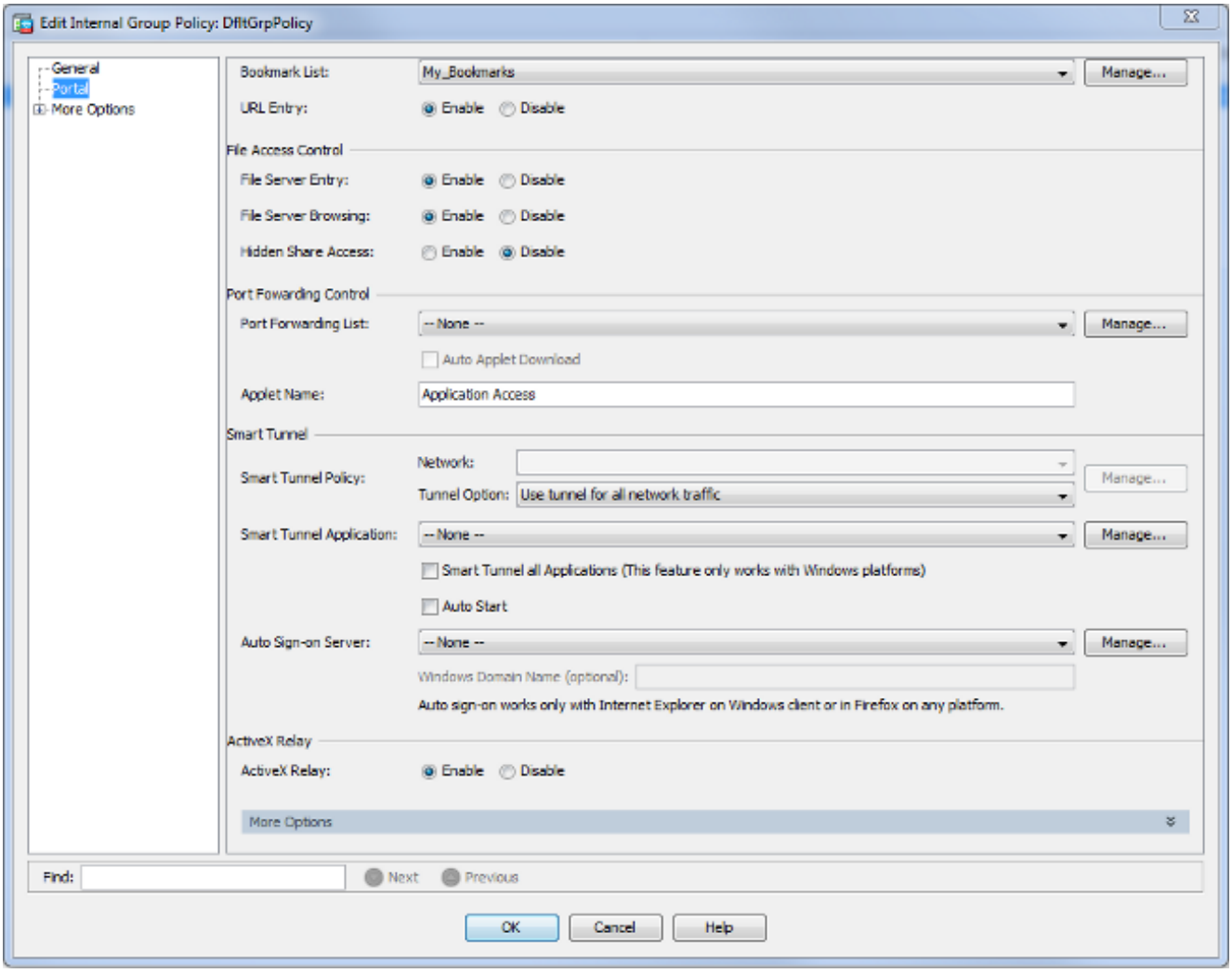


Escolha **adicionam** a fim adicionar um endereço da Internet específico.



CLI:Éimpossível criar endereços da Internet através do CLI porque são criados como arquivos XML.

8. (Opcional) atribua endereços da Internet a uma política específica do grupo.Escolha a **configuração > o acesso remoto VPN > do acesso > do grupo dos sem clientes SSL VPN políticas > editam > lista do portal > do endereço da Internet**.

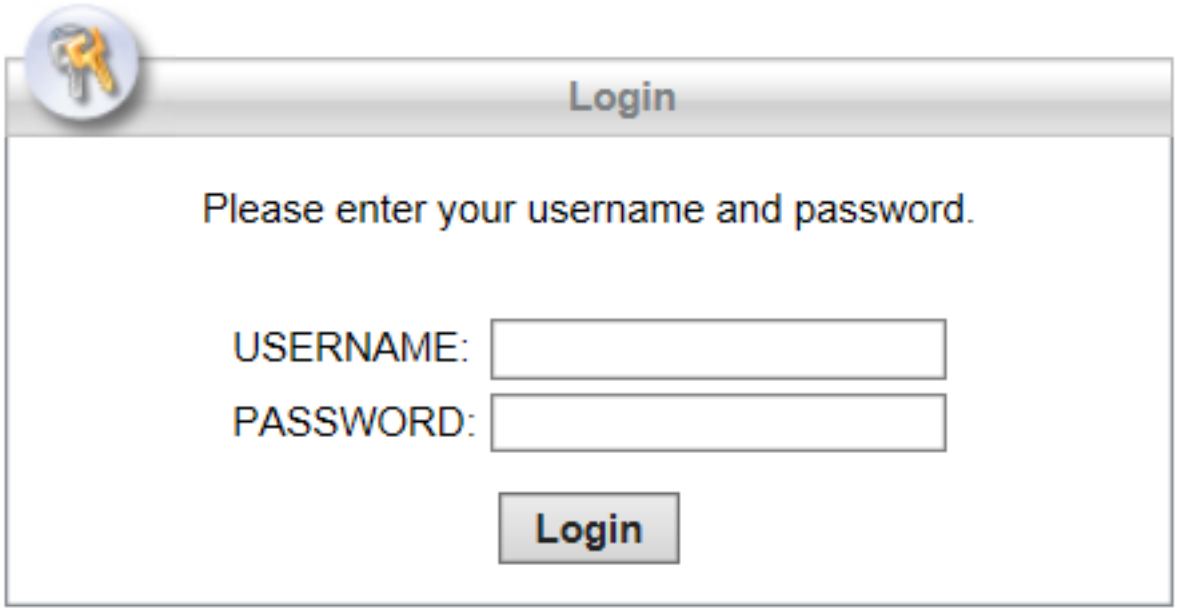


CLI:

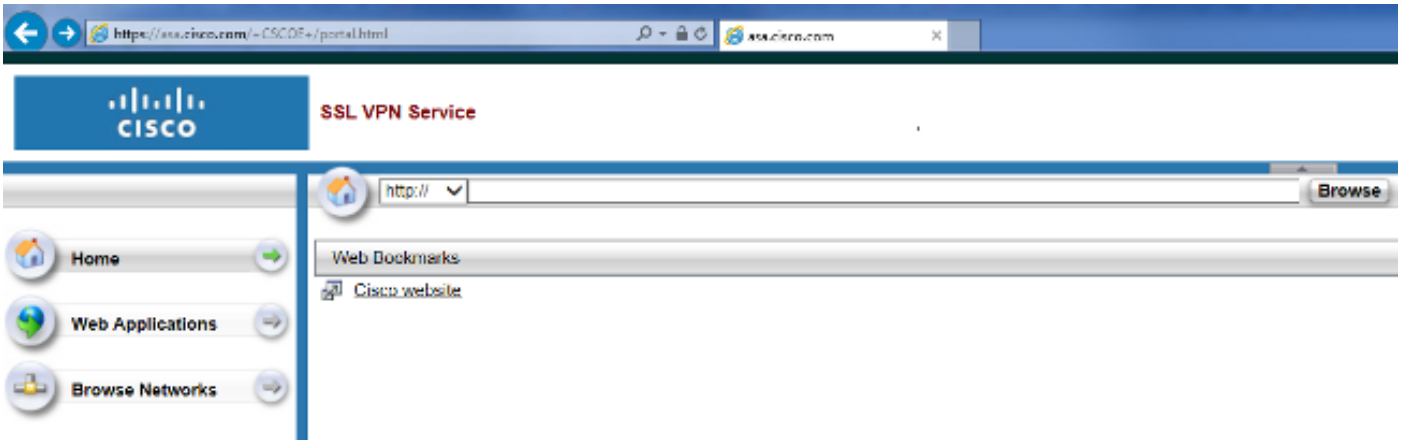
```
ASA(config)# group-policy DfltGrpPolicy attributes
ASA(config-group-policy)# webvpn
ASA(config-group-webvpn)# url-list value My_Bookmarks
```

Verificar

Uma vez que o WebVPN foi configurado, use o endereço https:// <FQDN do *ASA*> *no* navegador.



Após a abertura você deve poder ver a barra de endereços usada para navegar aos Web site e aos endereços da Internet.



Troubleshooting

Procedimentos usados para pesquisar defeitos

Siga estas instruções a fim pesquisar defeitos sua configuração.

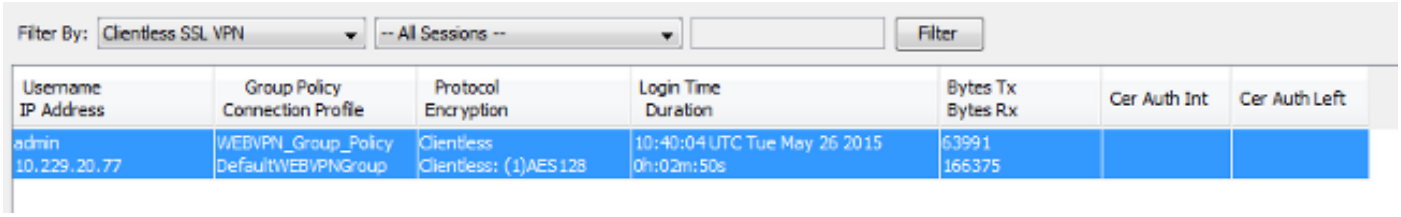
No ASDM, escolha a **monitoração > registrando > Log Viewer > opinião do tempo real**. Quando um cliente conecta ao ASA, note o estabelecimento da sessão TLS, a seleção da política do grupo, e a autenticação bem sucedida do usuário.

```
Device completed SSL handshake with client outside:10.229.20.77/61307 to 10.48.66.179/443 for TLSv1.2 session
Device completed SSL handshake with client outside:10.229.20.77/61306 to 10.48.66.179/443 for TLSv1.2 session
SSL client outside:10.229.20.77/61307 to 10.48.66.179/443 request to resume previous session
Starting SSL handshake with client outside:10.229.20.77/61307 to 10.48.66.179/443 for TLS session
SSL client outside:10.229.20.77/61306 to 10.48.66.179/443 request to resume previous session
Starting SSL handshake with client outside:10.229.20.77/61306 to 10.48.66.179/443 for TLS session
Built inbound TCP connection 107 for outside:10.229.20.77/61307 (10.229.20.77/61307) to identity:10.48.66.179/443 (10.48.66.179/443)
Built inbound TCP connection 106 for outside:10.229.20.77/61306 (10.229.20.77/61306) to identity:10.48.66.179/443 (10.48.66.179/443)
Group <WEBVPN_Group_Policy> User <admin> IP <10.229.20.77> Authentication: successful, Session Type: WebVPN.
Device selects trust-point ASA-self-signed for client outside:10.229.20.77/53047 to 10.48.66.179/443
Group <WEBVPN_Group_Policy> User <admin> IP <10.229.20.77> WebVPN session started.
DAP: User admin, Addr 10.229.20.77, Connection Clientless: The following DAP records were selected for this connection: DfltAccessPolicy
AAA transaction status ACCEPT : user = admin
AAA retrieved default group policy (WEBVPN_Group_Policy) for user = admin
AAA user authentication Successful : local database : user = admin
Device completed SSL handshake with client outside:10.229.20.77/61304 to 10.48.66.179/443 for TLSv1.2 session
Device completed SSL handshake with client outside:10.229.20.77/61303 to 10.48.66.179/443 for TLSv1.2 session
```

CLI:

```
ASA(config)# logging buffered debugging
ASA(config)# show logging
```

No ASDM, escolha a **monitoração** > o **VPN** > as **estatísticas de VPN** > as **sessões** > **o filtro por: Sem clientes SSL VPN.** Procure a sessão de VPN da Web nova. Seja certo escolher o filtro WebVPN e clicar o **filtro**. Se um problema ocorre, contorneie temporariamente o dispositivo ASA para assegurar-se de que os clientes possam alcançar os recursos de rede desejados. Reveja as etapas de configuração alistadas neste documento.



CLI:

```
ASA(config)# show vpn-sessiondb webvpn

Session Type: WebVPN

Username : admin Index : 3
Public IP : 10.229.20.77
Protocol : Clientless
License : AnyConnect Premium
Encryption : Clientless: (1)AES128 Hashing : Clientless: (1)SHA256
Bytes Tx : 72214 Bytes Rx : 270241
Group Policy : WEBVPN_Group_Policy Tunnel Group : DefaultWEBVPNGroup
Login Time : 10:40:04 UTC Tue May 26 2015
Duration : 0h:05m:21s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : 0a1516010000300055644d84
Security Grp : none
```

Comandos usados para pesquisar defeitos

A Output Interpreter Tool (apenas para clientes registrados) (OIT) suporta determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

> **Note**: Consulte Informações Importantes sobre Comandos de Depuração antes de usar comandos **debug**.

- **webvpn da mostra** - Há muitos **comandos show** associados com o WebVPN. A fim ver em detalhe o uso dos **comandos show**, veja a seção de referência de comandos do dispositivo do Cisco Security.
- **debugar o webvpn -** O uso dos **comandos debug** pode adversamente impactar o ASA. A fim ver com maiores detalhes o uso dos **comandos debug**, veja a seção de referência de comandos do dispositivo do Cisco Security.

Problemas comuns

O usuário não pode entrar

Problema

A mensagem dos “o acesso sem clientes (navegador) SSL VPN não é permitida.” aparece no navegador após uma tentativa de login mal sucedida. A licença superior de AnyConnect não é instalada no ASA ou não é uso “pela licença superior de AnyConnect não é permitido dentro como mostrado no ASA.”

Solução

Permita a licença superior de AnyConnect com estes comandos:

```
ASA(config)# webvpn
ASA(config-webvpn)# no anyconnect-essentials
```

Problema

A mensagem “início de uma sessão falhado” aparece no navegador após uma tentativa de login mal sucedida. O limite da licença de AnyConnect foi excedido.

Solução

Procure esta mensagem nos logs:

```
ASA(config)# webvpn
ASA(config-webvpn)# no anyconnect-essentials
```

Também, verifique seu limite da licença:

```
ASA(config)# show version | include Premium
AnyConnect Premium Peers : 2 perpetual
```

Problema

A mensagem “AnyConnect não é permitida no servidor de VPN” aparece no navegador após uma tentativa de login mal sucedida. O protocolo de VPN dos sem clientes não é permitido na grupo-política.

Solução

Procure esta mensagem nos logs:

```
ASA(config)# show version | include Premium
AnyConnect Premium Peers : 2 perpetual
```

Certifique-se de que o protocolo de VPN dos sem clientes está permitido para a grupo-política desejada:

```
ASA(config)# show version | include Premium
AnyConnect Premium Peers : 2 perpetual
```

Incapaz de conectar mais de três usuários WebVPN ao ASA

Problema

Somente três clientes WebVPN podem conectar ao ASA. A conexão para o quarto cliente falha.

Solução

Na maioria dos casos, esta edição é relacionada a um ajuste simultâneo do início de uma sessão dentro da política do grupo. Use esta ilustração a fim configurar o número desejado de inícios de uma sessão simultâneos. Neste exemplo, o valor desejado é 20.

```
ASA(config)# group-policy Cisco attributes
ASA(config-group-policy)# vpn-simultaneous-logins 20
```

Os clientes WebVPN não podem bater endereços da Internet e são esmaecidas para fora

Problema

Se estes endereços da Internet estiveram configurados para que os usuários assinem dentro aos sem clientes VPN, mas na tela home sob “aplicativos de web” aparecem como esmaecida para fora, como posso eu permitir estes links HTTP de modo que os usuários possam os clicar e entrar na URL particular?

Solução

Você deve primeiramente certificar-se de que o ASA pode resolver os Web site com o DNS. Tente sibilar por nome os Web site. Se o ASA não pode resolver o nome, o link é esmaecida para fora. Se os servidores DNS são internos a sua rede, configurar a interface confidencial da consulta de domínio DNS.

Conexão de Citrix com o WebVPN

Problema

O Mensagem de Erro “o **cliente AIC recebeu um arquivo corrompido AIC.**” ocorre para Citrix sobre o WebVPN.

Solução

Se você usa o modo *seguro do gateway* para a conexão de Citrix com o WebVPN, o arquivo ICA pode corromper. Porque o ASA não é compatível com este modo de operação, crie um arquivo novo ICA no modo direto (modo NON-seguro).

Como evitar a necessidade para uma segunda autenticação para os usuários

Problema

Quando você alcança os links CIFS no portal dos sem clientes WebVPN, você está alertado para credenciais depois que você clica o endereço da Internet. O Lightweight Directory Access Protocol (LDAP) é usado a fim autenticar os recursos e os usuários têm incorporado já credenciais LDAP para entrar à sessão de VPN.

Solução

Você pode usar a característica do auto-signon neste caso. Sob a grupo-política específica que está sendo usada e sob seus atributos WebVPN, configurar isto:

```
ASA(config)# group-policy WEBVPN_Group_Policy attributes
ASA(config-group-policy)# webvpn
ASA(config-group-webvpn)# auto-signon allow uri cifs://X.X.X.X/* auth-type all
```

onde `X.X.X.X=IP do` server e do `*=restof` CIFS o `trajeto para alcançar o` arquivo/dobrador da parte na pergunta.

Um snippet do exemplo de configuração é mostrado aqui:

```
ASA(config)# group-policy ExamplePolicy attributes
ASA(config-group-policy)# webvpn
ASA(config-group-webvpn)# auto-signon allow uri
https://*.example.com/* auth-type all
```

Para obter mais informações sobre disto, veja configurar o SSO com o HTTP básico ou a autenticação de NTLM.

Informações Relacionadas

- ASA: Túnel esperto usando o exemplo da configuração ASDM
- Suporte Técnico e Documentação - Cisco Systems