

Configurar VPN SSL sem cliente (WebVPN) no ASA

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de Rede](#)

[Informações de Apoio](#)

[Configuração](#)

[Verificar](#)

[Troubleshoot](#)

[Procedimentos usados para solucionar problemas](#)

[Comandos usados para solucionar problemas](#)

[Problemas comuns](#)

[O usuário não pode fazer login](#)

[Não é possível conectar mais de três usuários WebVPN ao ASA](#)

[Clientes WebVPN não podem atingir marcadores e estão em cinza](#)

[Conexão Citrix por WebVPN](#)

[Como evitar a necessidade de uma segunda autenticação para os usuários](#)

[Informações Relacionadas](#)

Introduction

Este documento fornece uma configuração direta para o Cisco Adaptive Security Appliance (ASA) 5500 Series para permitir o acesso VPN SSL (Secure Sockets Layer) sem cliente aos recursos de rede internos. A rede privada virtual SSL sem cliente (WebVPN) permite acesso limitado, mas valioso, à rede corporativa a partir de qualquer local. Os usuários podem obter acesso seguro baseado em navegador aos recursos corporativos a qualquer momento. Nenhum cliente adicional é necessário para obter acesso a recursos internos. O acesso é fornecido usando uma conexão Hypertext Transfer Protocol sobre SSL.

A VPN SSL sem cliente fornece acesso seguro e fácil a uma ampla variedade de recursos da Web e aplicativos habilitados para a Web e herdados de praticamente qualquer computador que possa acessar sites HTTP (Hypertext Transfer Protocol Internet). Isso inclui:

- Sites internos
- Microsoft SharePoint 2003, 2007 e 2010
- Microsoft Outlook Web Access 2003, 2007 e 2013

- Microsoft Outlook Web App 2010
- Domino Web Access (DWA) 8.5 e 8.5.1
- Citrix Metaframe Presentation Server 4.x
- Citrix XenApp versão 5 a 6.5
- Citrix XenDesktop versão 5 a 5.6 e 7.5
- VMware View 4

Uma lista de softwares compatíveis pode ser encontrada em [Plataformas VPN suportadas, Cisco ASA 5500 Series](#).

Prerequisites

Requirements

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

- navegador habilitado para SSL
- ASA com versão 7.1 ou superior
- Certificado X.509 emitido para o nome de domínio do ASA
- Porta TCP 443, que não deve ser bloqueada ao longo do caminho do cliente para o ASA

A lista completa de requisitos pode ser encontrada em [Plataformas VPN suportadas, Cisco ASA 5500 Series](#).

Componentes Utilizados

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

- ASA versão 9.4(1)
- Adaptive Security Device Manager (ASDM) versão 7.4(2)
- ASA 5515-X

The information in this document was created from the devices in a specific lab environment. Todos os dispositivos usados neste documento começaram com uma configuração limpa (padrão). If your network is live, make sure that you understand the potential impact of any command.

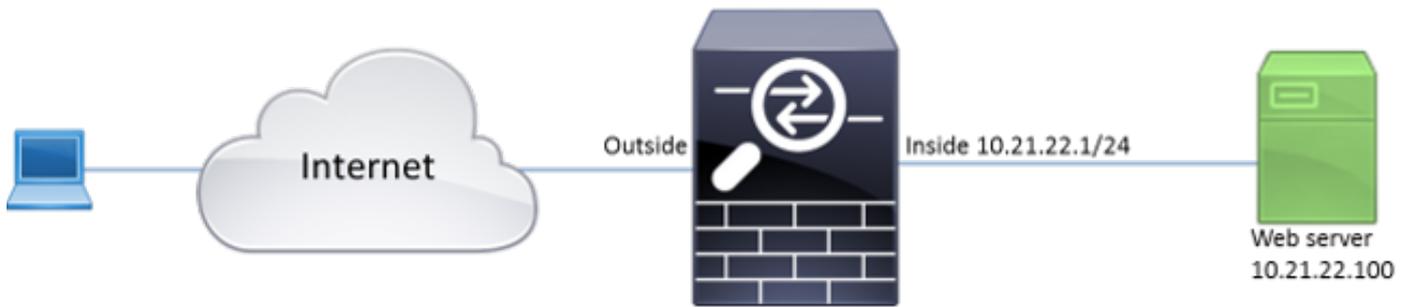
Configurar

Este artigo descreve o processo de configuração do ASDM e da CLI. Você pode optar por seguir qualquer uma das ferramentas para configurar o WebVPN, mas algumas das etapas de configuração só podem ser realizadas com o ASDM.

Nota: Use a [Command Lookup Tool](#) ([somente](#) clientes [registrados](#)) para obter mais informações sobre os comandos usados nesta seção.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



Informações de Apoio

A WebVPN usa o protocolo SSL para proteger os dados transferidos entre o cliente e o servidor. Quando o navegador inicia uma conexão com o ASA, o ASA apresenta seu certificado para se autenticar no navegador. Para garantir que a conexão entre o cliente e o ASA seja segura, você precisa fornecer ao ASA o certificado assinado pela autoridade de certificação em que o cliente já confia. Caso contrário, o cliente não terá os meios para verificar a autenticidade do ASA, o que resulta na possibilidade de um ataque intermediário e uma experiência de usuário ruim, pois o navegador produz um aviso de que a conexão não é confiável.

Note: Por padrão, o ASA gera um certificado X.509 autoassinado na inicialização. Esse certificado é usado para servir conexões de cliente por padrão. Não é recomendável usar este certificado porque sua autenticidade não pode ser verificada pelo navegador. Além disso, esse certificado é regenerado a cada reinicialização, de modo que é alterado após cada reinicialização.

A instalação do certificado está fora do escopo deste documento.

Configuração

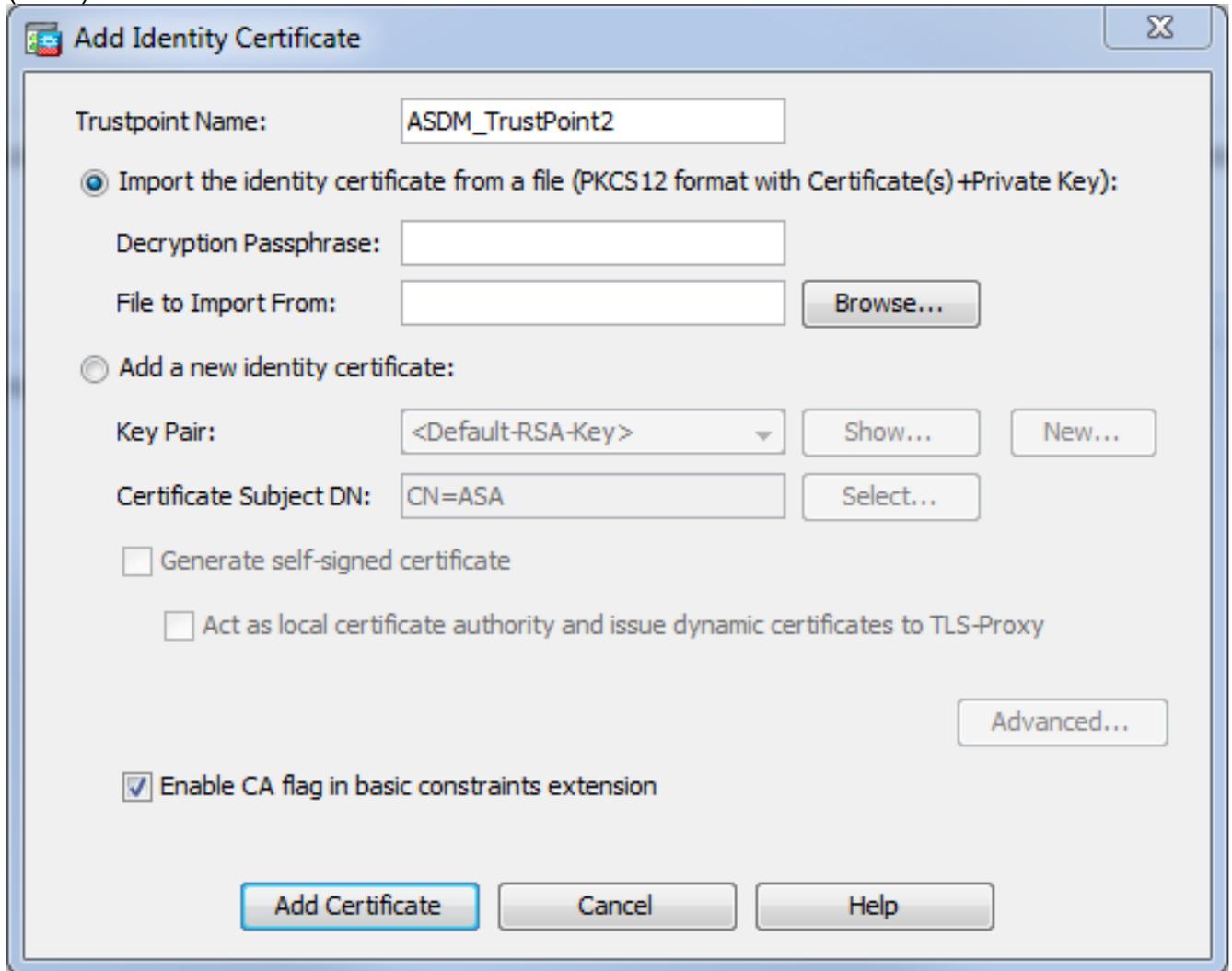
Configure o WebVPN no ASA com cinco etapas principais:

- Configure o certificado que será usado pelo ASA.
- Ative o WebVPN em uma interface ASA.
- Crie uma lista de servidores e/ou URL (Uniform Resource Locator) para acesso à WebVPN.
- Crie uma política de grupo para usuários do WebVPN.
- Aplique a nova política de grupo a um Grupo de Túneis.

Note: Nas versões do ASA posteriores à versão 9.4, o algoritmo usado para escolher cifras SSL foi alterado (consulte [Notas de versão do Cisco ASA Series, 9.4\(x\)](#)). Se somente clientes com capacidade para curva elíptica forem usados, então é seguro usar a chave privada de curva elíptica para o certificado. Caso contrário, o pacote de cifras personalizado deve ser usado para evitar que o ASA apresente um certificado temporário autoassinado. Você pode configurar o ASA para usar somente cifras baseadas em RSA com a **cifra ssl tlv1.2 personalizada "AES256-SHA:AES128-SHA:DHE-RSA-AES256-SHA:DHE-RSA-**

AES128-SHA:DES-CBC3-SHA:DHA DES-CBC-SHA:RC4-SHA:RC4-MD5" comando.

1. Opção 1 - Importe o certificado com o arquivo pkcs12. Escolha **Configuração > Firewall > Avançado > Gerenciamento de Certificados > Certificados de Identidade > Adicionar**. Você pode instalá-lo com o arquivo pkcs12 ou colar o conteúdo no formato Privacy Enhanced Mail (PEM).



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:

```
MIIJQUIBAzCCCRcGCSqGSIB3DQEHAAcCCQgEggkEMIIJADCCBf8GCSqGSIB3DQEH  
BqCCBfAwggXsAgEAMIIF5QYJKoZIhvcNAQcBMBwGCiqGSIB3DQEMAQYwDgQI8F3N  
+vkvjUgCAggAgIIFuHFrV6enVf1Nv3sBBYB/yZswHELY5KpeALbXhfrFDpLNncAB  
z3xMfg6JkLYR6Fag1KjShg+o4qkDh8r9y9GQPaBt8x30zo0JJxSAafmTWqDOEOS/  
7mHsaKMoao+pv2LqKTWh007No4Ycx75Y5s0hyuQGPhLJRdionbils1ioe4Dplx1b
```

--- output omitted ---

Enter the base 64 encoded pkcs12.

End with the word "quit" on a line by itself:

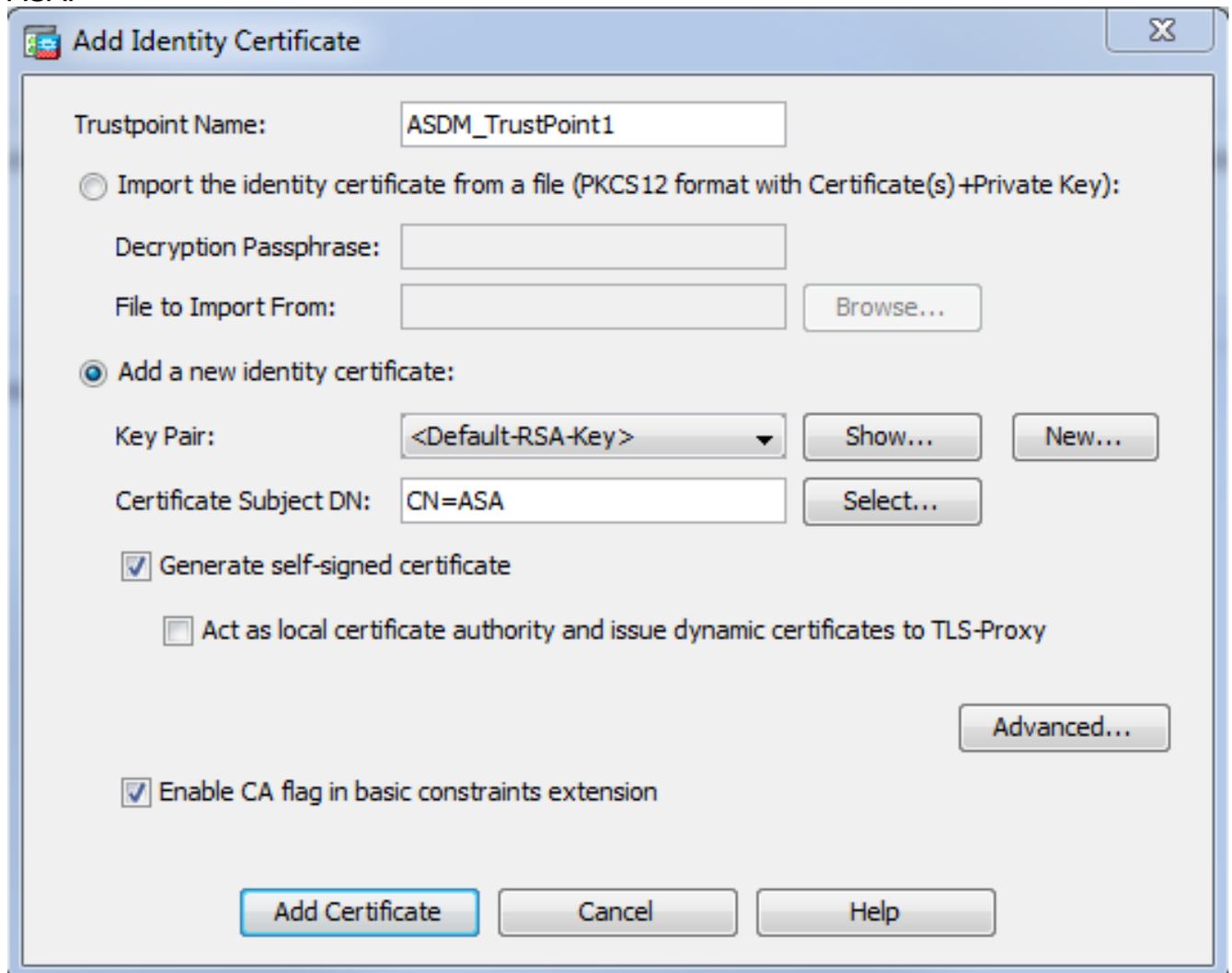
```
MIIJQUIBAzCCCRcGCSqGSIB3DQEHAAcCCQgEggkEMIIJADCCBf8GCSqGSIB3DQEH
```

BqCCBfAwggXsAgEAMIIF5QYJKoZIhvcNAQcBMBwGCiqGSIb3DQEEMAQYwDgQI8F3N
+vkvjUgCAggAgIIFuHFrV6enVf1Nv3sBBYB/yZswHELY5KpeALbXhfrFDpLNncAB
z3xMfg6JkLYR6Fag1KjShg+o4qkDh8r9y9GQpaBt8x3Ozo0JJxSAafmTWqDOEOS/
7mHsaKMoao+pv2LqKTWh007No4Ycx75Y5sOhyuQGPhLJRdionbilslieo4Dplx1b

quit

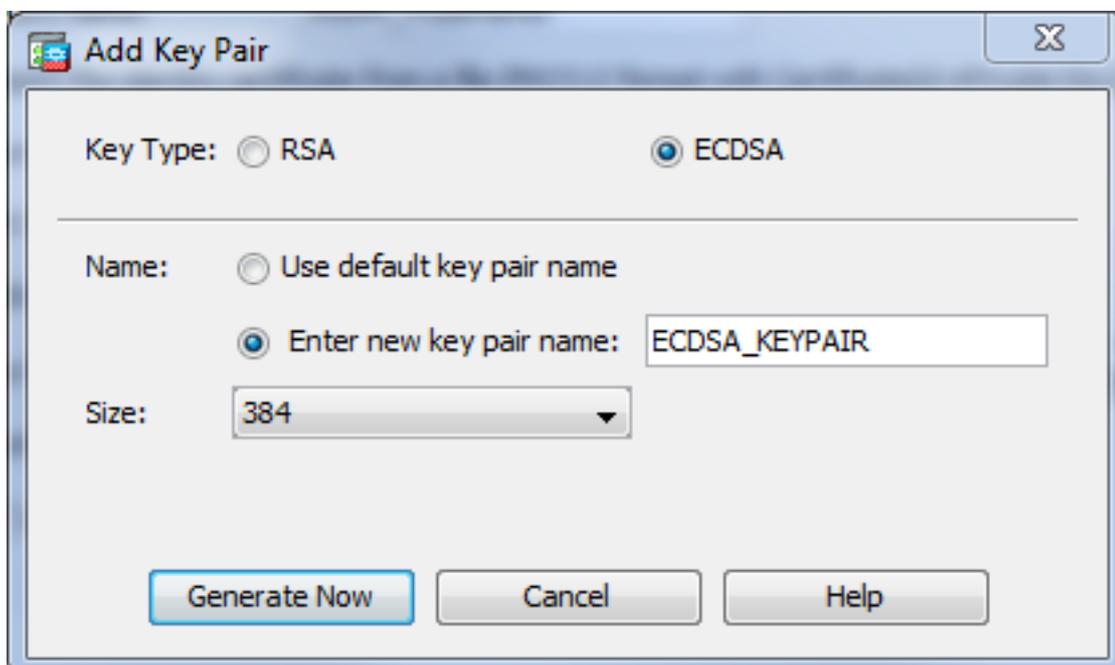
INFO: Import PKCS12 operation completed successfully

Opção 2 - Crie um certificado autoassinado. Escolha **Configuração > Firewall > Avançado > Gerenciamento de Certificados > Certificados de Identidade > Adicionar**. Clique no botão de rádio **Add a new identity certificate** (Adicionar um novo certificado de identidade). Marque a caixa de seleção **Gerar certificado autoassinado**. Escolha um nome comum (CN) que corresponda ao nome de domínio do ASA.



The screenshot shows the 'Add Identity Certificate' dialog box. The 'Trustpoint Name' field is set to 'ASDM_TrustPoint1'. The 'Import the identity certificate from a file (PKCS12 format with Certificate(s) + Private Key)' option is unselected. The 'Add a new identity certificate' option is selected. The 'Key Pair' dropdown is set to '<Default-RSA-Key>'. The 'Certificate Subject DN' field is set to 'CN=ASA'. The 'Generate self-signed certificate' checkbox is checked. The 'Act as local certificate authority and issue dynamic certificates to TLS-Proxy' checkbox is unchecked. The 'Enable CA flag in basic constraints extension' checkbox is checked. The 'Advanced...' button is visible. At the bottom, there are 'Add Certificate', 'Cancel', and 'Help' buttons.

Clique em **New** para criar o par de chaves para o certificado. Escolha o tipo, o nome e o tamanho da



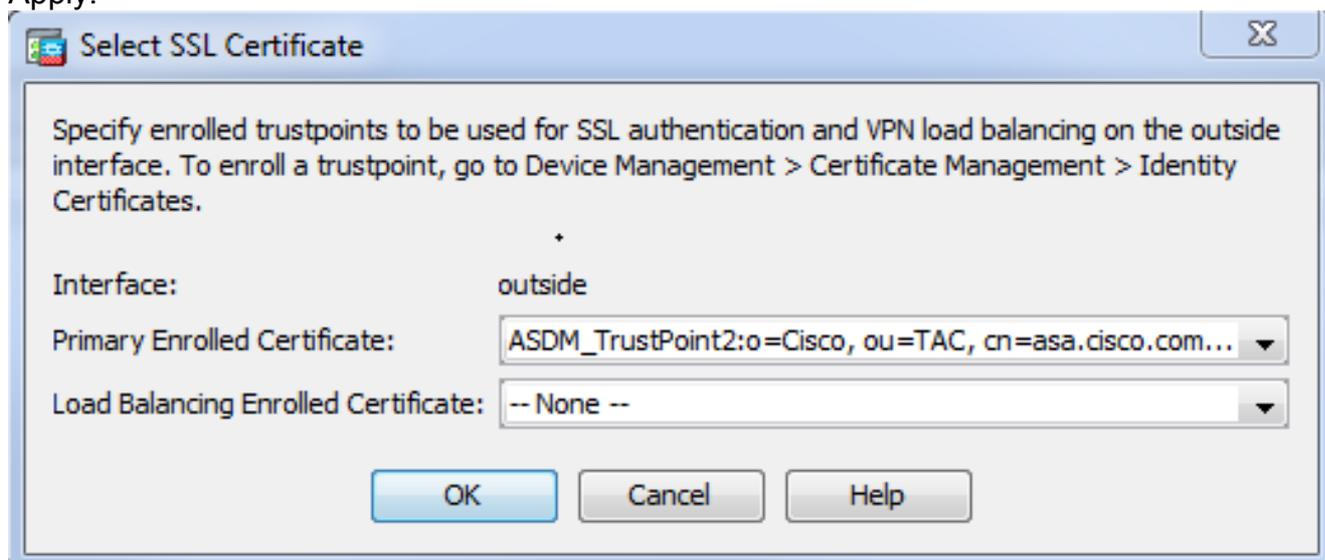
chave.

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
```

- Escolha o certificado que será usado para atender às conexões WebVPN. Escolha **Configuration > Remote Access VPN > Advanced > SSL Settings**. No menu Certificados, escolha o ponto de confiança associado ao certificado desejado para a interface externa. Clique em **Apply**.



Configuração via CLI Equivalente:

```
ASA(config)# ssl trust-point
```

3. (Opcional) Habilite as pesquisas do Servidor de Nomes de Domínio (DNS).O servidor WebVPN atua como um proxy para conexões de clientes. Isso significa que o ASA cria conexões com os recursos em nome do cliente. Se os clientes precisarem de conexões com os recursos que usam nomes de domínio, o ASA precisará executar a pesquisa de DNS.Escolha **Configuration > Remote Access VPN > DNS**.Configure pelo menos um servidor DNS e ative as pesquisas DNS na interface que enfrenta o servidor

Configuration > Remote Access VPN > DNS

Specify how to resolve DNS requests.

DNS Setup

Configure one DNS server group Configure multiple DNS server groups

Primary DNS Server:

Secondary Servers:

Domain Name:

DNS.

DNS Lookup

To configure DNS, enable DNS lookup on at least one interface.

Interface	DNS Enabled
inside	True
outside	False

DNS Guard

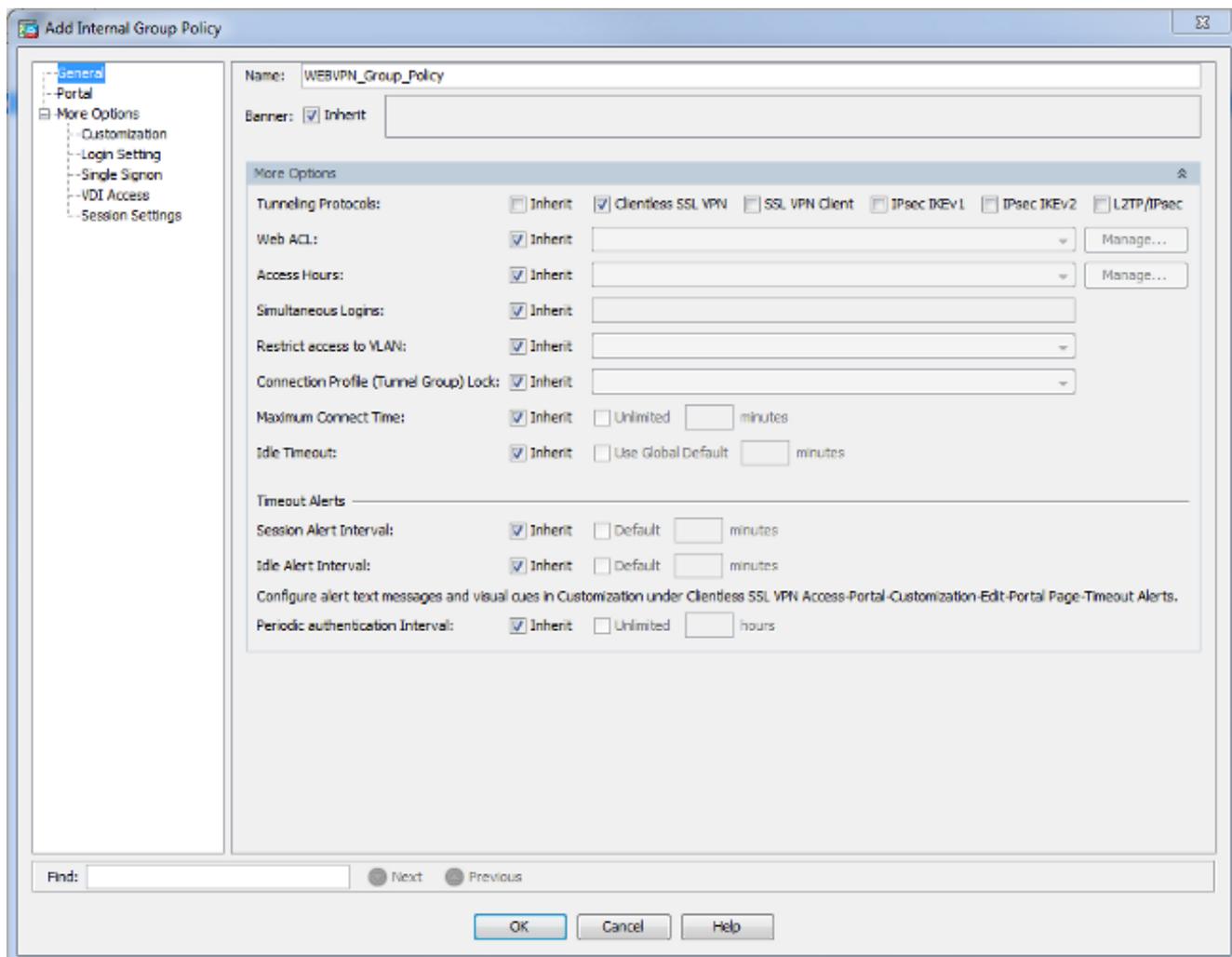
This function enforces one DNS response per query. If DNS inspection is configured, this option is ignored on that interface.

Enable DNS Guard on all interfaces.

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) Criar Política de Grupo para conexões WEBVPN.Escolha **Configuration > Remote Access VPN > Clientless SSL VPN Access > Group Policies > Add Internal Group Policy**.Em Opções gerais, altere o valor de Protocolos de tunelamento para "VPN SSL sem cliente".



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. Configure o perfil de conexão.No ASDM, escolha **Configuration > Remote Access VPN > Clientless SSL VPN Access > Connection Profiles**.

Para obter uma visão geral dos perfis de conexão e das políticas de grupo, consulte [Cisco ASA Series VPN CLI Configuration Guide, 9.4 - Connection Profiles, Group Policies e Users](#).Por padrão, as conexões WebVPN usam o perfil DefaultWEBVPNGroup. Você pode criar perfis adicionais.**Note:** Há várias maneiras de atribuir usuários a outros perfis.

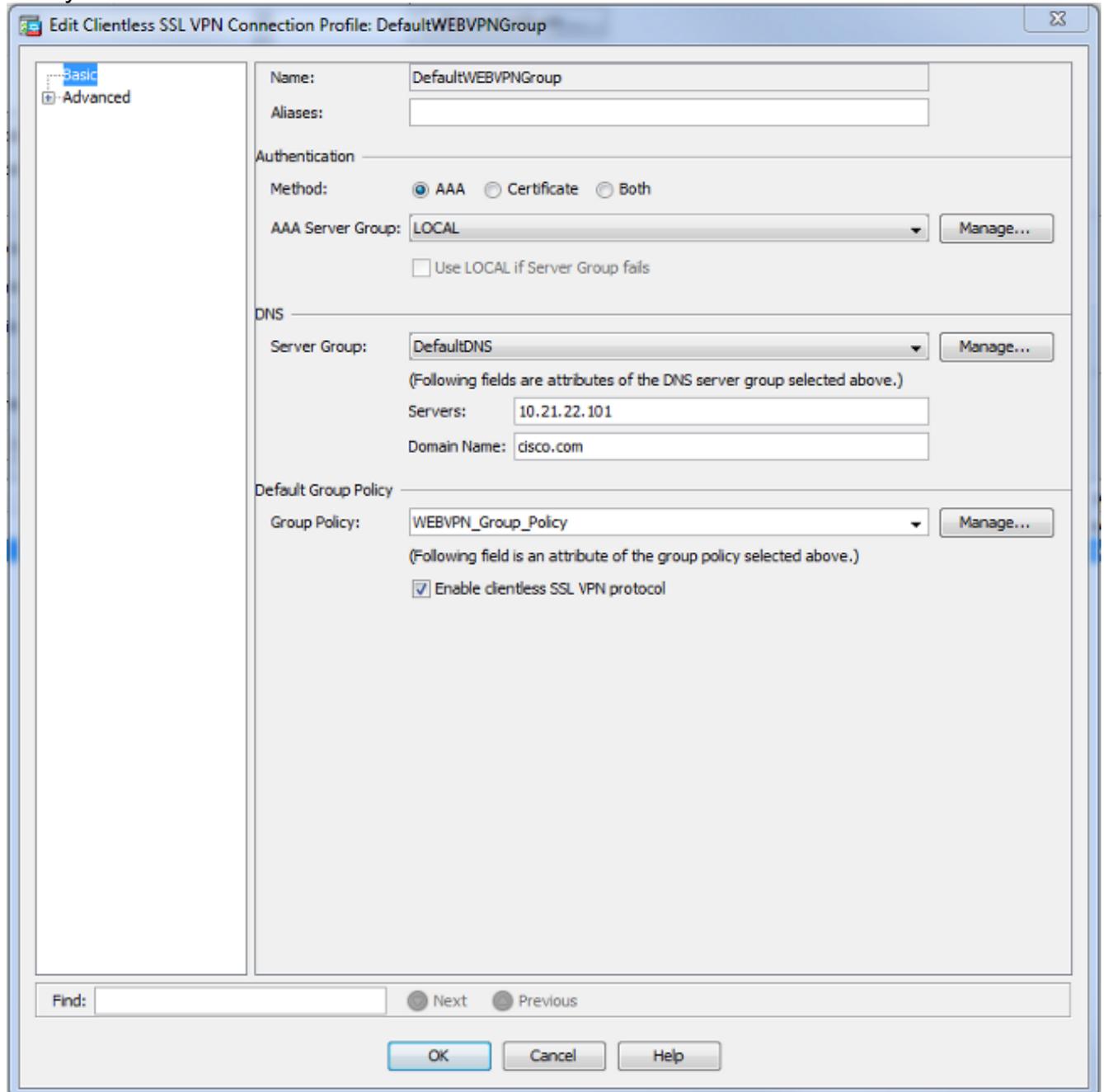
- Os usuários podem selecionar manualmente o perfil de conexão na lista suspensa ou com um URL específico. Consulte [ASA 8.x: Permitir que os usuários selecionem um grupo no login do WebVPN via Group-Alias e Group-URL Method](#).

- Ao usar um servidor LDAP, você pode atribuir o perfil de usuário com base nos atributos recebidos do servidor LDAP. Consulte [Exemplo de Configuração de Uso de Mapas de Atributos LDAP do ASA](#).

- Ao usar a autenticação baseada em certificado dos clientes, você pode mapear o usuário para os perfis com base nos campos contidos no certificado, consulte [Cisco ASA Series VPN CLI Configuration Guide, 9.4 - Configure Certificate Group Matching for IKEv1](#).

- Para atribuir os usuários manualmente à política de grupo, consulte [Cisco ASA Series VPN](#)

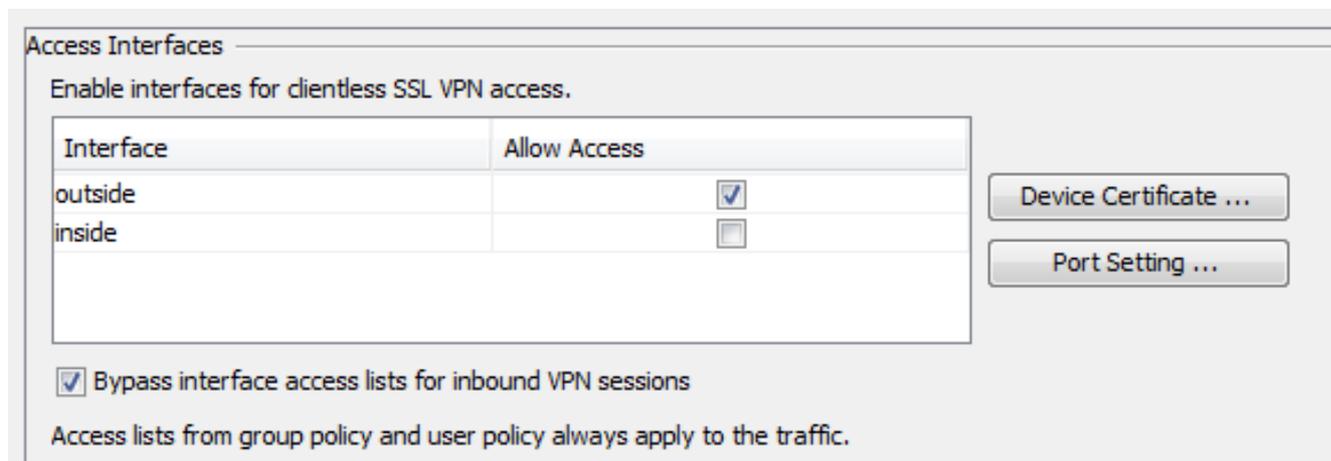
[CLI Configuration Guide, 9.4 - Configuring Attributes for Individual Users](#) Edite o perfil DefaultWEBVPNGroup e escolha WEBVPN_Group_Policy em Default Group Policy.



CLI:

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

6. Para habilitar o WebVPN na interface externa, escolha **Configuration > Remote Access VPN > Clientless SSL VPN Access > Connection Profiles**. Marque a caixa de seleção **Permitir acesso** ao lado da interface externa.

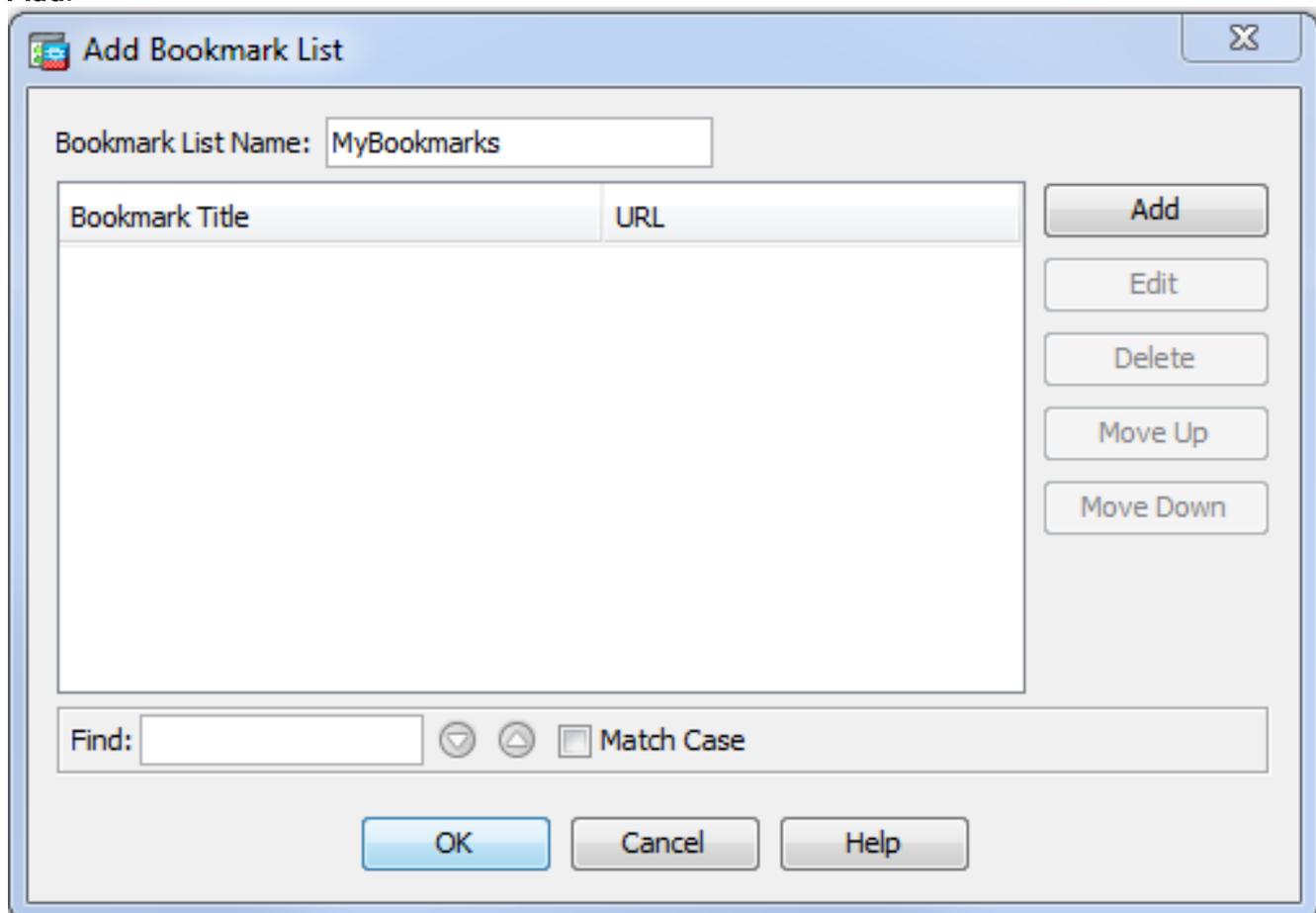


CLI:

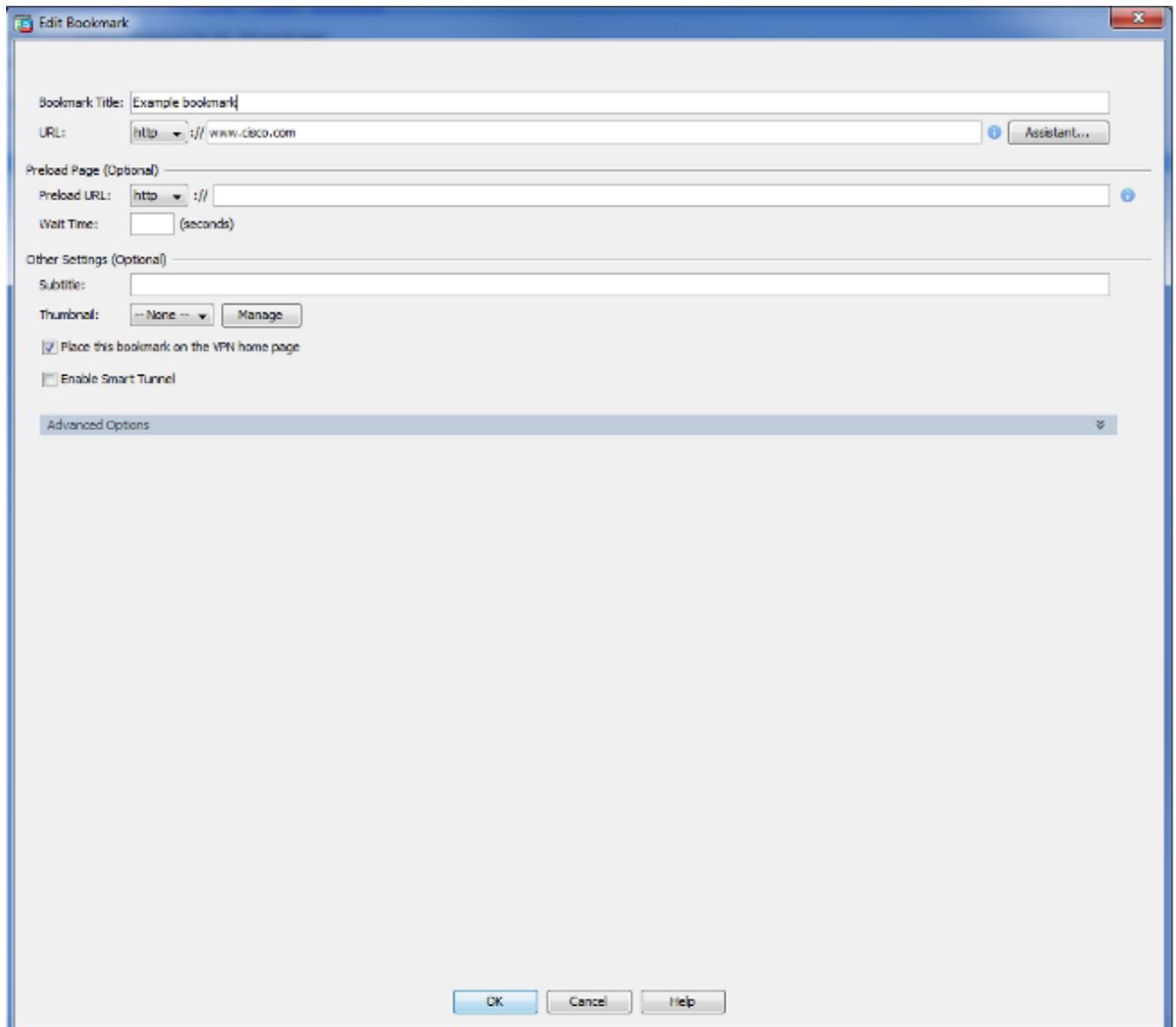
```
ASA(config)# webvpn
```

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

7. (Opcional) Crie marcadores para o conteúdo. Os marcadores permitem que o usuário navegue facilmente pelos recursos internos sem ter que se lembrar dos URLs. Para criar um indicador, escolha **Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Bookmarks > Add**.

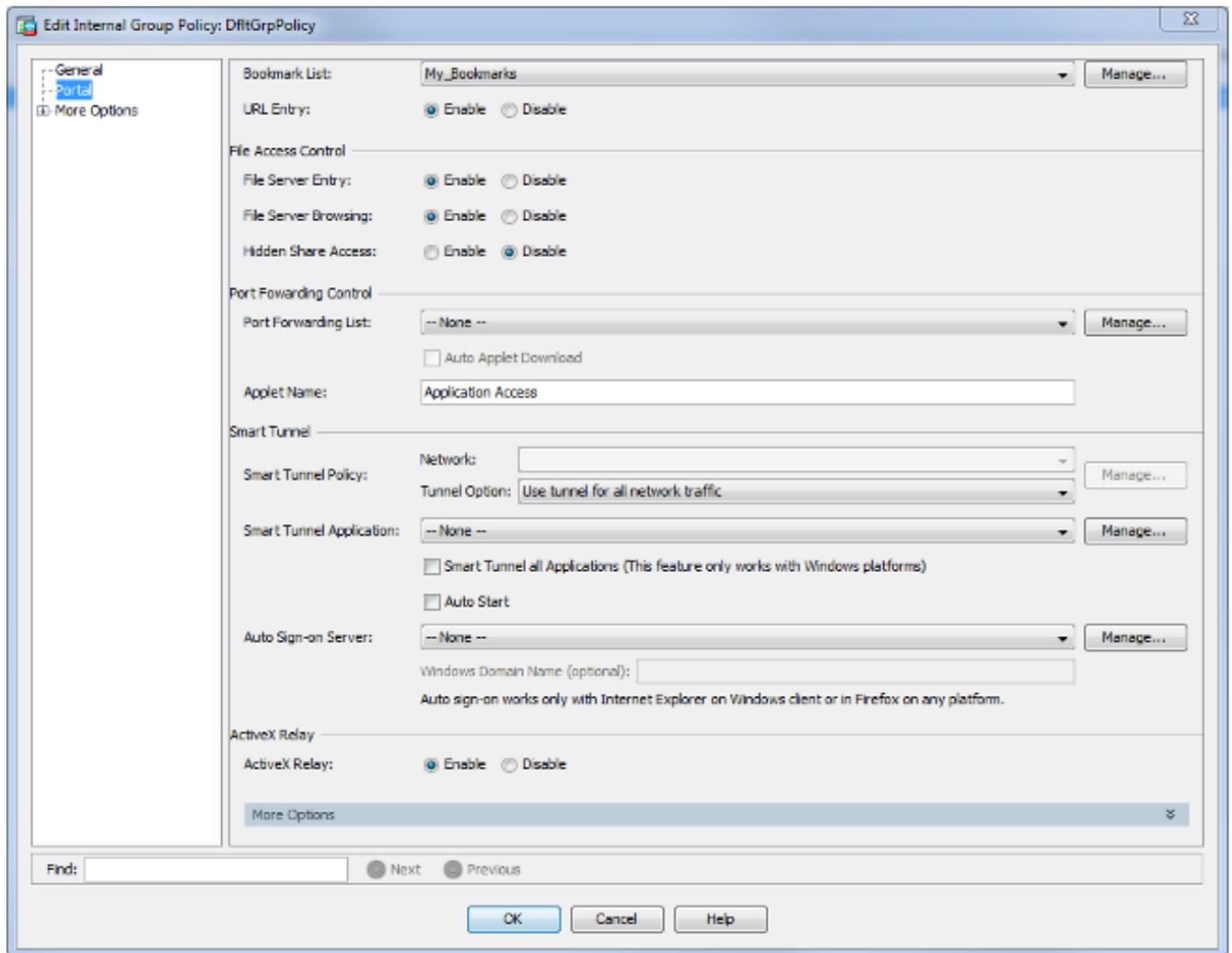


Escolha **Adicionar** para adicionar um favorito específico.



CLI:Éimpossível criar marcadores via CLI porque eles são criados como arquivos XML.

8. (Opcional) Atribuir marcadores a uma política de grupo específica. Escolha **Configuration > Remote Access VPN > Clientless SSL VPN Access > Group Policies > Edit > Portal > Bookmark List**.

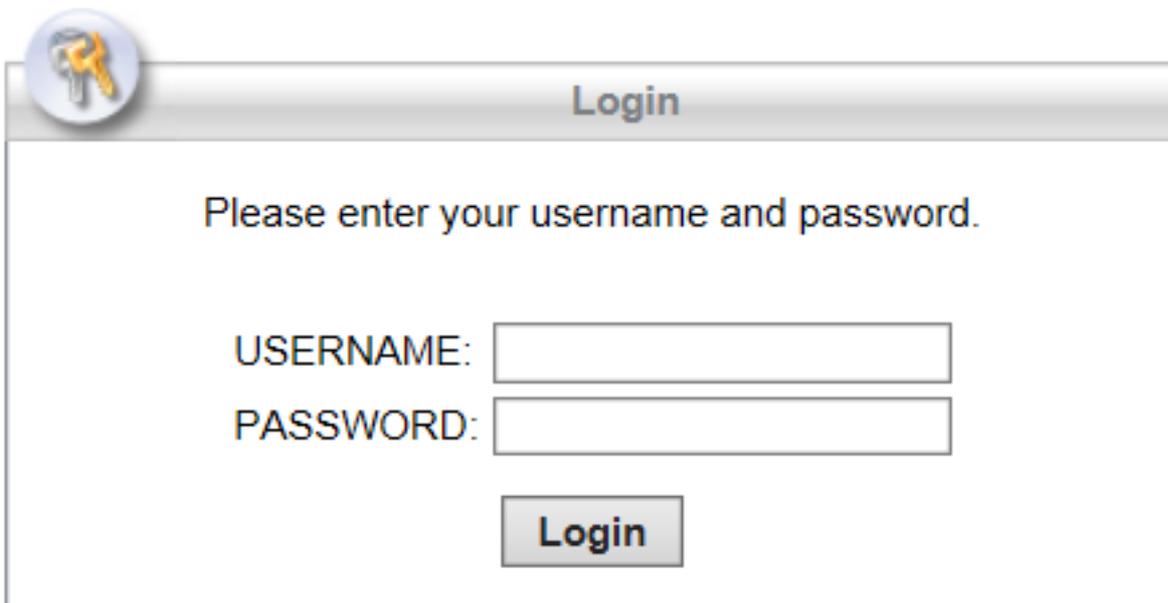


CLI:

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

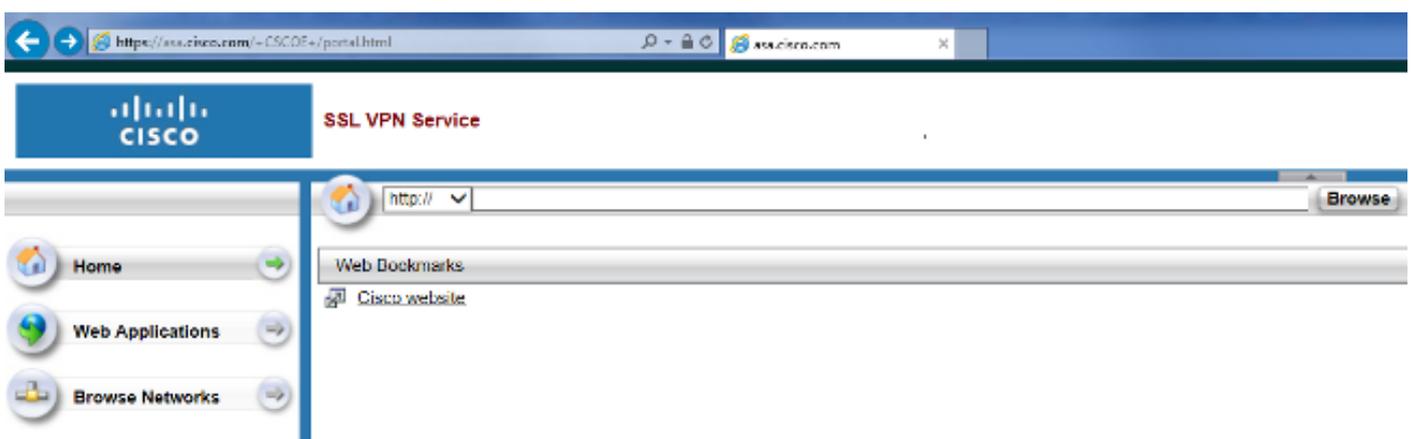
Verificar

Depois que a WebVPN tiver sido configurada, use o endereço `https://<FQDN do ASA>` no navegador.



The image shows a login window titled "Login" with a key icon in the top-left corner. The text "Please enter your username and password." is centered. Below this, there are two input fields: "USERNAME:" followed by a text box, and "PASSWORD:" followed by a text box. At the bottom center is a "Login" button.

Após fazer login, você poderá ver a barra de endereços usada para navegar para sites e marcadores.



Troubleshoot

Procedimentos usados para solucionar problemas

Siga estas instruções para solucionar problemas de sua configuração.

No ASDM, escolha **Monitoring > Logging > Real-time Log Viewer > View**. Quando um cliente se conecta ao ASA, observe o estabelecimento da sessão TLS, a seleção da política de 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 **Monitoring > VPN > VPN Statistics > Sessions > Filter by: VPN SSL sem cliente**. Procure a nova sessão WebVPN. Escolha o filtro WebVPN e clique em **Filtro**. Se ocorrer um problema, ignore temporariamente o dispositivo ASA para garantir que os clientes possam acessar os recursos de rede desejados. Reveja as etapas de configuração listadas neste documento.

Username IP Address	Group Policy Connection Profile	Protocol Encryption	Login Time Duration	Bytes Tx Bytes Rx	Cer Auth Int	Cer Auth Left
admin 10.229.20.77	WEBVPN_Group_Policy DefaultWEBVPNGroup	Clientless Clientless: (1)AES128	10:40:04 UTC Tue May 26 2015 0h:02m:50s	63991 166375		

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 solucionar problemas

A [Output Interpreter Tool \(somente clientes registrados\) \(OIT\)](#) oferece suporte a 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](#).

- **show webvpn** - Há muitos comandos **show** associados ao WebVPN. Para ver o uso dos comandos **show** em detalhes, consulte a seção [referência de comando](#) do Cisco Security Appliance.
- **debug webvpn** - O uso de comandos **debug** pode afetar adversamente o ASA. Para ver o uso de comandos **debug** em mais detalhes, consulte a seção [referência de comando](#) do Cisco Security Appliance.

Problemas comuns

O usuário não pode fazer login

Problema

A mensagem "Acesso VPN SSL sem cliente (navegador) não é permitida." aparece no navegador após uma tentativa de login malsucedida. A licença do AnyConnect Premium não está instalada no ASA ou não está sendo usada como mostrado pela "licença do Premium AnyConnect não está habilitada no ASA".

Solução

Ative a licença Premium do AnyConnect com estes comandos:

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

Problema

A mensagem "Falha de login" aparece no navegador após uma tentativa de login malsucedida. O limite de licença do AnyConnect foi excedido.

Solução

Procure esta mensagem nos registros:

```
%ASA-4-716023: Group <DfltGrpPolicy> User <cisco> IP <192.168.1.100>  
Session could not be established: session limit of 2 reached.
```

Além disso, verifique seu limite de licença:

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

Problema

A mensagem "AnyConnect is not enabled on the VPN server" (O AnyConnect não está habilitado no servidor VPN) é exibida no navegador após uma tentativa de login malsucedida. O protocolo VPN sem cliente não está ativado na política de grupo.

Solução

Procure esta mensagem nos registros:

```
%ASA-6-716002: Group <DfltGrpPolicy> User <cisco> IP <192.168.1.100>  
WebVPN session terminated: Client type not supported.
```

Verifique se o protocolo VPN sem cliente está ativado para a política de grupo desejada:

```
ASA(config)# show run all group-policy | include vpn-tunnel-protocol  
vpn-tunnel-protocol ikev1 ikev2 l2tp-ipsec ssl-clientless
```

Não é possível conectar mais de três usuários WebVPN ao ASA

Problema

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

Solução

Na maioria dos casos, esse problema está relacionado a uma configuração de login simultâneo na política de grupo. Use esta ilustração para configurar o número desejado de logins simultâneos. Neste exemplo, o valor desejado é 20.

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

Clientes WebVPN não podem atingir marcadores e estão em cinza

Problema

Se esses marcadores foram configurados para que os usuários acessem a VPN sem cliente, mas na tela inicial em "Aplicações da Web" eles aparecerão como acinzentados, como posso ativar esses links HTTP para que os usuários possam clicar neles e ir para a URL específica?

Solução

Primeiro, você deve certificar-se de que o ASA possa resolver os sites por meio do DNS. Tente fazer ping nos sites por nome. Se o ASA não puder resolver o nome, o link ficará acinzentado. Se os servidores DNS forem internos à sua rede, configure a interface privada de pesquisa de domínio DNS.

Conexão Citrix por WebVPN

Problema

A mensagem de erro "o cliente ica recebeu um arquivo ica corrompido." ocorre para Citrix sobre WebVPN.

Solução

Se você usar o modo de *gateway seguro* para conexão Citrix por meio de WebVPN, o arquivo ICA poderá corromper. Como o ASA não é compatível com esse modo de operação, crie um novo arquivo ICA no modo direto (modo não seguro).

Como evitar a necessidade de uma segunda autenticação para os usuários

Problema

Ao acessar links CIFS no portal WebVPN sem cliente, você será solicitado a fornecer credenciais após clicar no indicador. O LDAP (Lightweight Directory Access Protocol) é usado para autenticar os recursos e os usuários já inseriram credenciais LDAP para fazer login na sessão VPN.

Solução

Você pode usar o recurso de assinatura automática neste caso. Sob a política de grupo específica sendo usada e sob seus atributos WebVPN, configure 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 servidor CIFS e *=restante do caminho para acessar o arquivo/pasta de compartilhamento em questão.

Um exemplo de trecho 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 isso, consulte [Configurando SSO com autenticação HTTP Basic ou NTLM](#).

Informações Relacionadas

- [ASA: Túnel inteligente usando o exemplo de configuração de ASDM](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)