

Configuración de Clientless SSL VPN (WebVPN) en ASA

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de la red](#)

[Antecedentes](#)

[Configuración](#)

[Verificación](#)

[Troubleshoot](#)

[Procedimientos Usados para Troubleshooting](#)

[Comandos Usados para Troubleshooting](#)

[Problemas Comunes](#)

[El usuario no puede iniciar sesión](#)

[No se puede conectar más de tres usuarios de WebVPN al ASA](#)

[Los clientes de WebVPN no pueden acceder a los marcadores y están atenuados](#)

[Conexión de Citrix a través de WebVPN](#)

[Cómo evitar la necesidad de una segunda autenticación para los usuarios](#)

[Información Relacionada](#)

Introducción

Este documento proporciona una configuración sencilla para Cisco Adaptive Security Appliance (ASA) serie 5500 para permitir el acceso VPN Secure Sockets Layer (SSL) sin cliente a los recursos de red internos. La red privada virtual (WebVPN) SSL sin cliente permite un acceso seguro limitado pero valioso a la red corporativa desde cualquier ubicación. Los usuarios pueden obtener acceso seguro basado en navegador a los recursos corporativos en cualquier momento. No se necesita ningún cliente adicional para obtener acceso a los recursos internos. El acceso se proporciona mediante un protocolo de transferencia de hipertexto sobre la conexión SSL.

Clientless SSL VPN proporciona un acceso seguro y fácil a una amplia gama de recursos web y aplicaciones tanto habilitadas para Web como antiguas desde casi cualquier ordenador que pueda alcanzar los sitios de Internet de protocolo de transferencia de hipertexto (HTTP). Esto incluye:

- Sitios web internos
- Microsoft SharePoint 2003, 2007 y 2010

- Microsoft Outlook Web Access 2003, 2007 y 2013
- Aplicación web de Microsoft Outlook 2010
- Domino Web Access (DWA) 8.5 y 8.5.1
- Servidor de presentación de Citrix Metaframe 4.x
- Citrix XenApp versiones 5 a 6.5
- Citrix XenDesktop versiones 5 a 5.6 y 7.5
- VMware View 4

Puede encontrar una lista de software soportado en [Plataformas VPN Soportadas, Cisco ASA serie 5500](#).

Prerequisites

Requirements

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- buscador habilitado para SSL
- ASA con la versión 7.1 o posterior
- Certificado X.509 emitido al nombre de dominio ASA
- Puerto TCP 443, que no se debe bloquear a lo largo de la trayectoria del cliente al ASA

La lista completa de requisitos se puede encontrar en [Plataformas VPN Soportadas, Cisco ASA serie 5500](#).

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

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

The information in this document was created from the devices in a specific lab environment. Todos los dispositivos usados en este documento comenzaron con una configuración despejada (predeterminada). If your network is live, make sure that you understand the potential impact of any command.

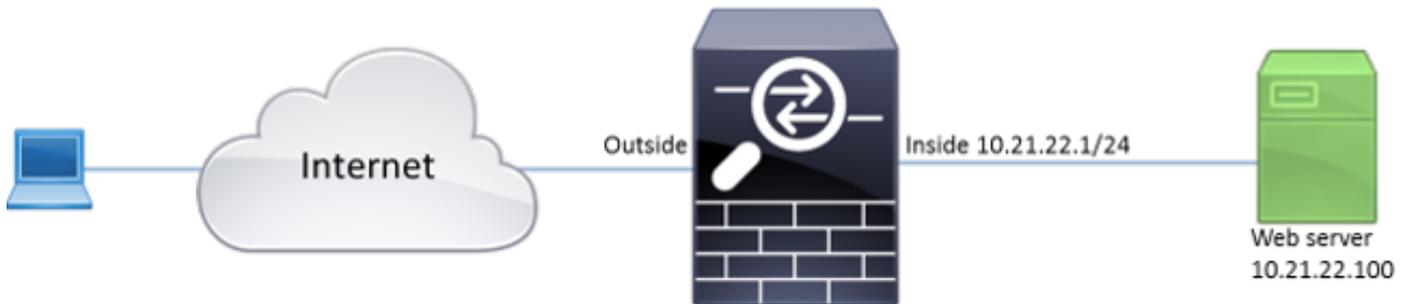
Configurar

En este artículo se describe el proceso de configuración tanto para el ASDM como para la CLI. Puede elegir seguir cualquiera de las herramientas para configurar el WebVPN, pero algunos de los pasos de configuración sólo se pueden lograr con el ASDM.

Nota: Use la [Command Lookup Tool](#) (sólo clientes registrados) para obtener más información sobre los comandos utilizados en esta sección.

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Antecedentes

WebVPN utiliza el protocolo SSL para proteger los datos transferidos entre el cliente y el servidor. Cuando el explorador inicia una conexión al ASA, el ASA presenta su certificado para autenticarse en el explorador. Para asegurarse de que la conexión entre el cliente y el ASA es segura, debe proporcionar al ASA el certificado firmado por la Autoridad de Certificación en el que el cliente ya confía. De lo contrario, el cliente no dispondrá de los medios para verificar la autenticidad del ASA, lo que da lugar a la posibilidad de que se produzca un ataque de intrusos y a una experiencia de usuario deficiente, ya que el navegador genera una advertencia de que la conexión no es de confianza.

Nota: De forma predeterminada, el ASA genera un certificado X.509 firmado automáticamente cuando se inicia. Este certificado se utiliza para servir las conexiones del cliente de forma predeterminada. No se recomienda utilizar este certificado porque el explorador no puede comprobar su autenticidad. Además, este certificado se regenera cada reinicio, por lo que cambia después de cada reinicio.

La instalación del certificado está fuera del alcance de este documento.

Configuración

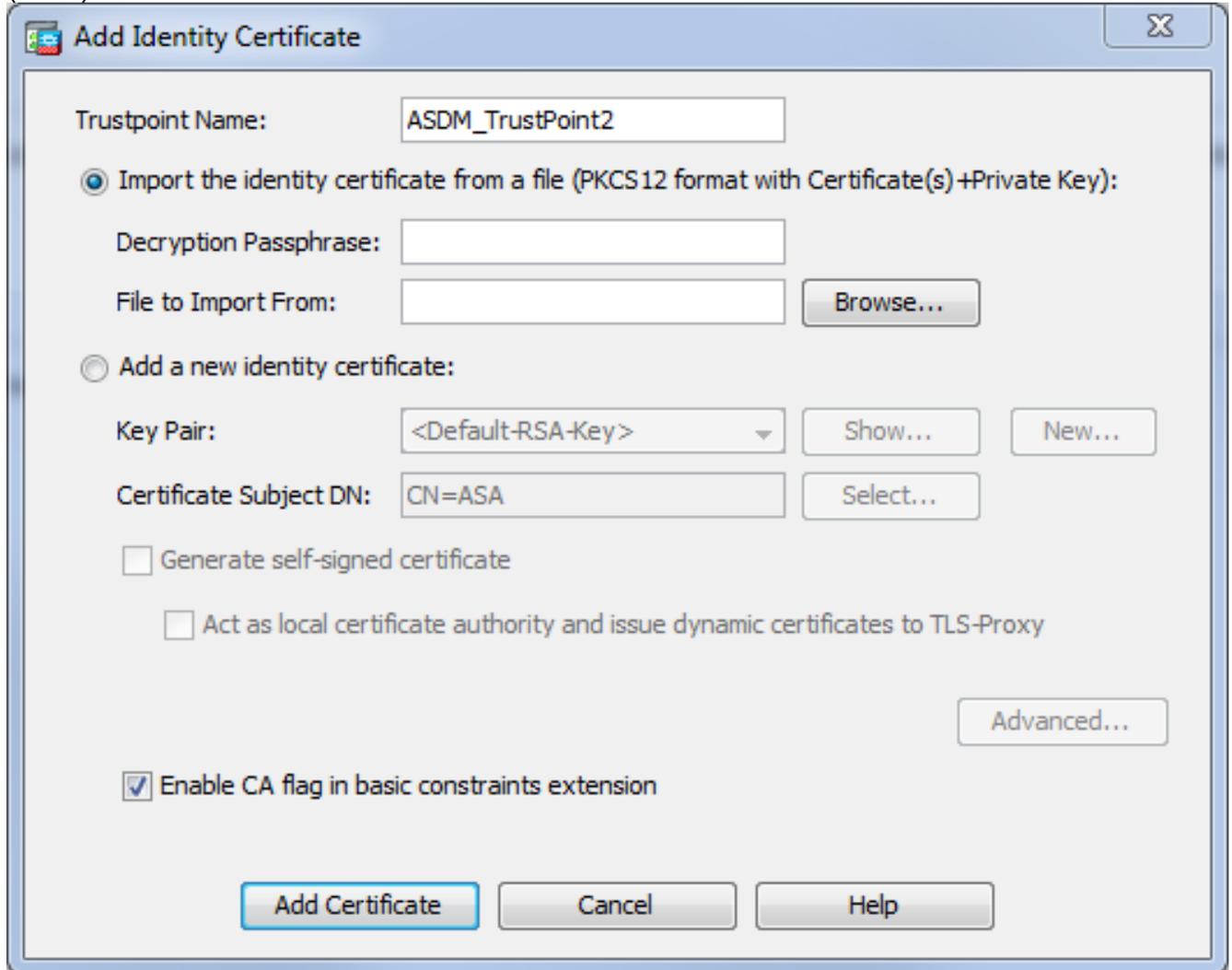
Configure el WebVPN en el ASA con cinco pasos principales:

- Configure el certificado que utilizará el ASA.
- Habilite el WebVPN en una interfaz ASA.
- Cree una lista de servidores y/o localizador uniforme de recursos (URL) para el acceso WebVPN.
- Cree una política de grupo para los usuarios de WebVPN.
- Aplique la nueva política del grupo a un grupo de túnel.

Nota: En las versiones de ASA posteriores a la versión 9.4, se ha cambiado el algoritmo utilizado para elegir los cifrados SSL (consulte [Release Notes for the Cisco ASA Series, 9.4\(x\)](#)). Si sólo se utilizarán clientes con capacidad para curva elíptica, es seguro utilizar la clave privada de curva elíptica para el certificado. De lo contrario, se debe utilizar el conjunto

de cifrado personalizado para evitar que el ASA presente un certificado temporal autofirmado. Puede configurar el ASA para que utilice solamente los cifrados basados en RSA con el cifrado `ssl tlsv1.2 personalizado "AES256-SHA:AES128-SHA:DHE-RSA-AES256-SHA:DHE-RSA-AES128-SHA:DES-CBC3-SHA:DES-CBC-SHA:RC4-SHA:RC4-MD5"`.

1. **Opción 1:** Importe el certificado con el archivo pkcs12. Elija **Configuration > Firewall > Advanced > Certificate Management > Identity Certificates > Add**. Puede instalarlo con el archivo pkcs12 o pegar el contenido en el formato de Correo mejorado de privacidad (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:

```
MIIJUQIBAzCCCRcGCSqGSIb3DQEHAaCCCQgEggkEMIIJADCCBf8GCSqGSIb3DQEH
BqCCBfAwggXsAgEAMIIF5QYJKoZIhvcNAQcBMBwGCiqGSIb3DQEMAQYwDgQI8F3N
+vkvjUgCaggAgIIFuHFrV6enVflNv3sBBYB/yZswhELY5KpeALbXhfrFDpLNncAB
z3xMfg6JkLYR6Fag1KjShg+o4qkDh8r9y9GQpaBt8x30zo0JJxSAafmTWqDOEOS/
7mHsaKMoao+pv2LqKTWh007No4Ycx75Y5s0hyuQGPhLJRdionbils1ioe4Dplx1b
```

--- output omitted ---

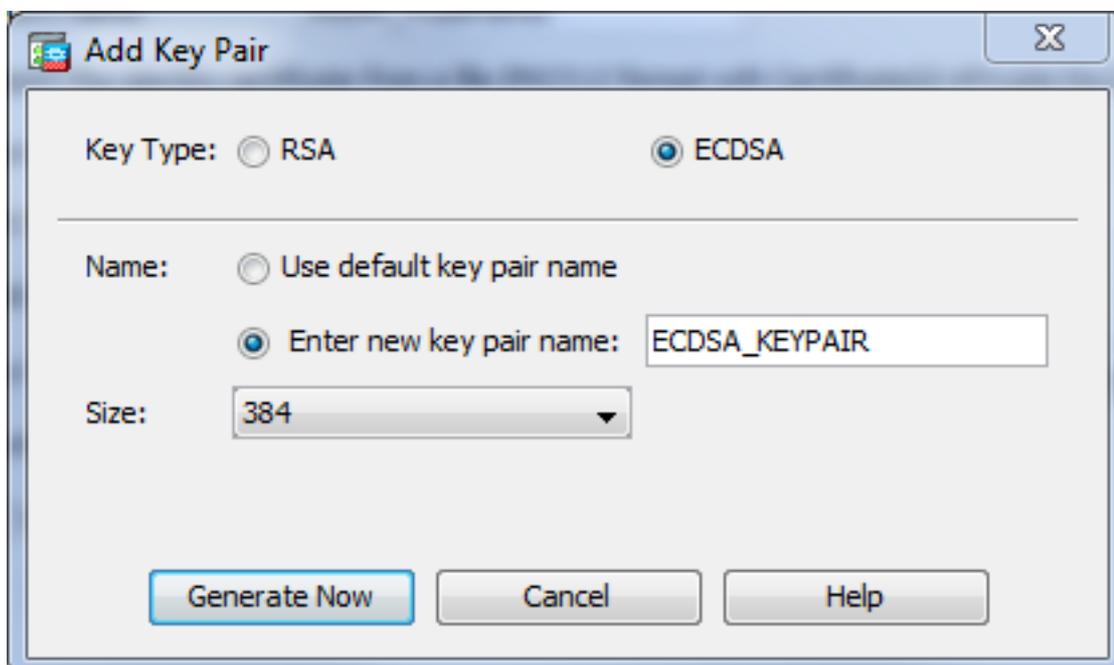
```
Enter the base 64 encoded pkcs12.  
End with the word "quit" on a line by itself:  
MIIJUQIBAzCCRCGCSqGSIb3DQEHAaCCCQgEggkEMIIJADCCBf8GCSqGSIb3DQEH  
BqCCBfAwggXsAgEAMIIF5QYJKoZIhvcNAQcBMBwGCiqGSIb3DQEMAQYwDgQI8F3N  
+vkvjUgCAggAgIIFuHFrV6enVf1Nv3sBByB/yZswhELY5KpeALbXhfrFDpLNncAB  
z3xMfg6JkLYR6Fag1KjShg+o4qkDh8r9y9GQpaBt8x3Ozo0JJxSAafmTWqDOEOS/  
7mHsaKMoao+pv2LqKTWh007No4Ycx75Y5s0hyuQGPhLJRdionbi1s1ioe4Dplx1b  
  
quit
```

INFO: Import PKCS12 operation completed successfully

Opción 2 - Cree un certificado autofirmado. Elija **Configuration > Firewall > Advanced > Certificate Management > Identity Certificates > Add**. Haga clic en el botón de opción **Agregar un nuevo certificado de identidad**. Marque la **casilla Generar certificado autofirmado**. Elija un nombre común (CN) que coincida con el nombre de dominio del ASA.

The screenshot shows the 'Add Identity Certificate' dialog box. The 'Trustpoint Name' field contains 'ASDM_TrustPoint1'. There are two radio button options: 'Import the identity certificate from a file (PKCS12 format with Certificate(s)+Private Key):' (unselected) and 'Add a new identity certificate:' (selected). Under the first option, there are fields for 'Decryption Passphrase:' and 'File to Import From:' with a 'Browse...' button. Under the second option, there is a 'Key Pair:' dropdown menu set to '<Default-RSA-Key>' with 'Show...' and 'New...' buttons. Below that is a 'Certificate Subject DN:' field containing 'CN=ASA' with a 'Select...' button. There are two checkboxes: 'Generate self-signed certificate' (checked) and 'Act as local certificate authority and issue dynamic certificates to TLS-Proxy' (unchecked). An 'Advanced...' button is located at the bottom right. At the very bottom, there are three buttons: 'Add Certificate', 'Cancel', and 'Help'.

Haga clic en **Nuevo** para crear el par de claves para el certificado. Elija el tipo de clave, el nombre y el



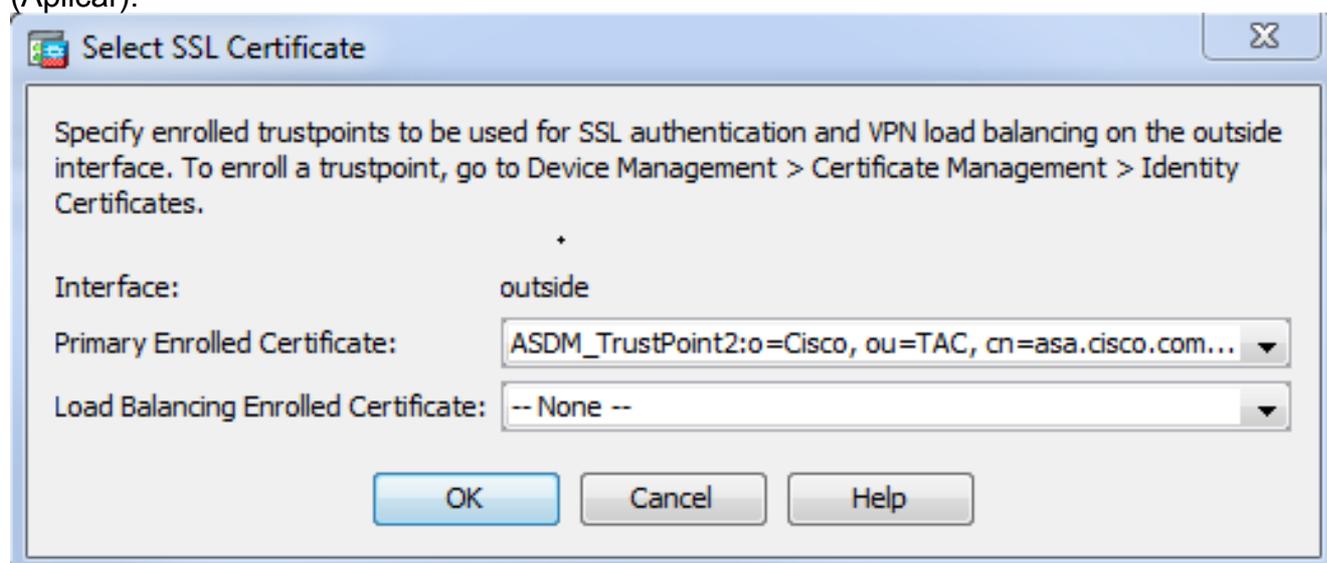
tamaño.

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. Elija el certificado que se utilizará para servir conexiones WebVPN. Elija **Configuration > Remote Access VPN > Advanced > SSL Settings**. En el menú Certificados, elija el punto de confianza asociado al certificado deseado para la interfaz externa. Haga clic en Apply (Aplicar).



Configuración CLI Equivalente:

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

3. (Opcional) Habilite las búsquedas del servidor de nombres de dominio (DNS). El servidor

WebVPN actúa como proxy para las conexiones del cliente. Significa que ASA crea conexiones a los recursos en nombre del cliente. Si los clientes requieren conexiones a los recursos que utilizan nombres de dominio, el ASA debe realizar la búsqueda de DNS. Elija **Configuration > Remote Access VPN > DNS**. Configure al menos un servidor DNS y active las búsquedas de DNS en la interfaz que se encuentra frente al 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

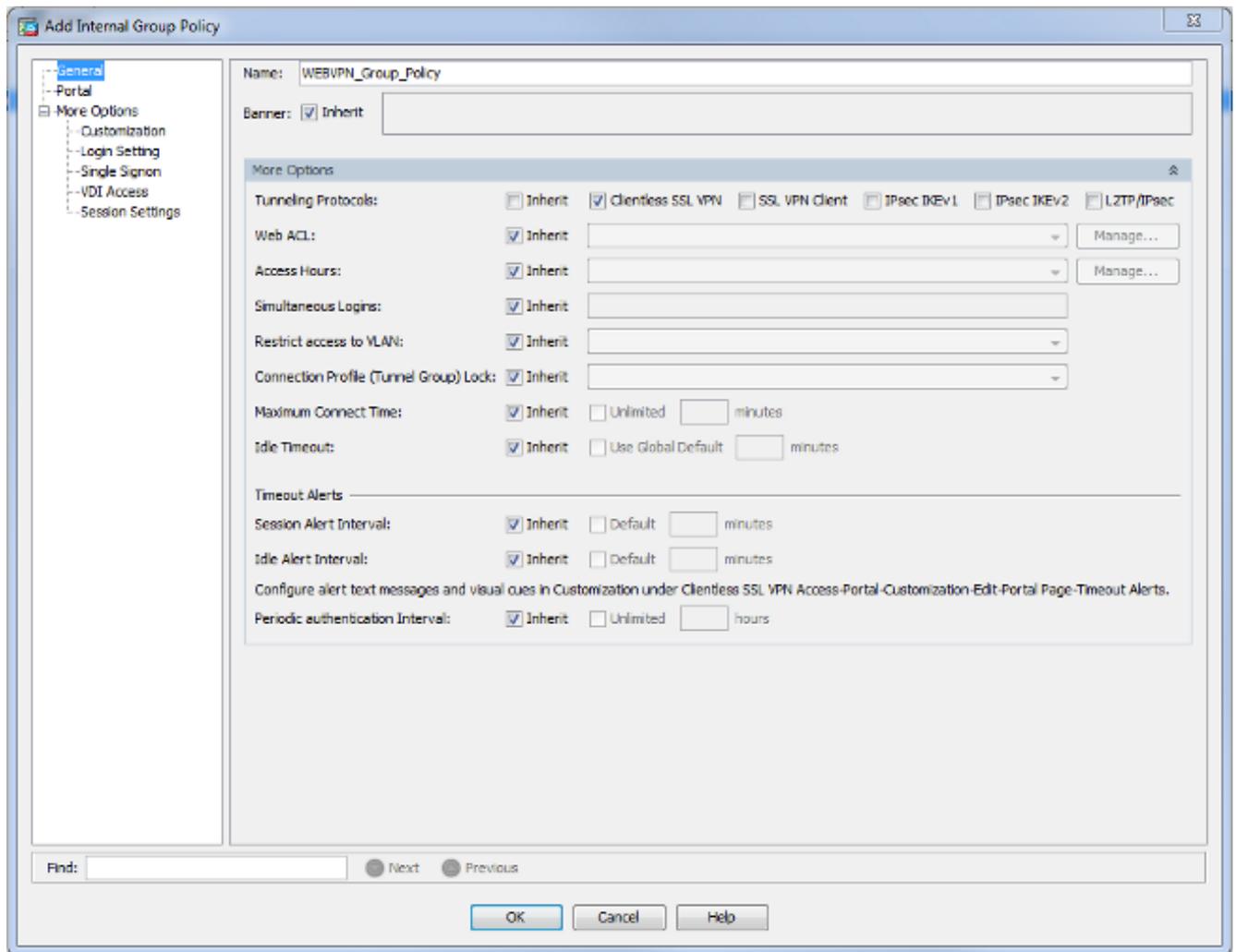
This function enforces one DNS response per query. If DNS inspection is configured, this option is ignored on that interface.

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) Cree una política de grupo para conexiones WEBVPN. Elija **Configuration > Remote Access VPN > Clientless SSL VPN Access > Group Policies > Add Internal Group Policy**. En Opciones generales, cambie el valor Tunelling Protocols a "Clientless 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. Configure el perfil de conexión. En ASDM, elija **Configuration > Remote Access VPN > Clientless SSL VPN Access > Connection Profiles**.

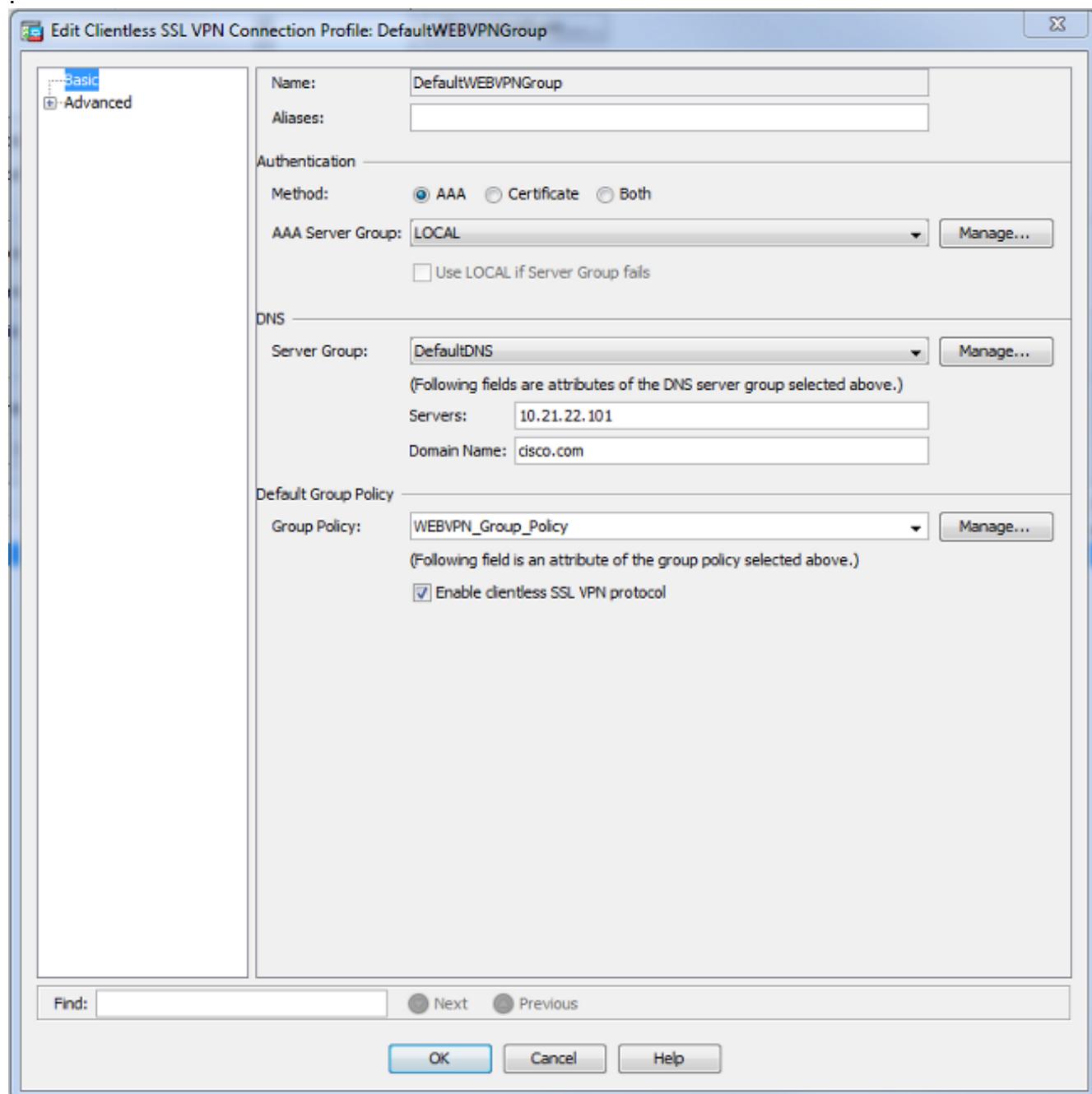
Para obtener una descripción general de los perfiles de conexión y las políticas de grupo, consulte la [Guía de Configuración de Cisco ASA Series VPN CLI, 9.4 - Perfiles de conexión, Políticas de grupo y Usuarios](#). De forma predeterminada, las conexiones WebVPN utilizan el perfil DefaultWEBVPNGroup. Puede crear perfiles adicionales. **Nota:** Hay varias maneras de asignar usuarios a otros perfiles.

- Los usuarios pueden seleccionar manualmente el perfil de conexión de la lista desplegable o con una URL específica. Véase [ASA 8.x: Permitir que los Usuarios Seleccionen un Grupo en Login WebVPN a través de Group-Alias y Group-URL Method](#).

- Cuando utiliza un servidor LDAP, puede asignar el perfil de usuario basándose en los atributos recibidos del servidor LDAP, vea [Ejemplo de Configuración de Uso de Mapas de Atributo LDAP de ASA](#).

- Cuando utiliza la autenticación basada en certificados de los clientes, puede asignar el usuario a los perfiles basándose en los campos contenidos en el certificado, consulte [Guía de Configuración de Cisco ASA Series VPN CLI, 9.4 - Configuración de la Coincidencia de Grupos de Certificados para IKEv1](#).

- Para asignar los usuarios manualmente a la política de grupo, consulte [Guía de Configuración de Cisco ASA Series VPN CLI, 9.4 - Configuración de Atributos para Usuarios Individuales](#) Edite el perfil DefaultWEBVPNGroup y elija WEBVPN_Group_Policy en Default Group Policy

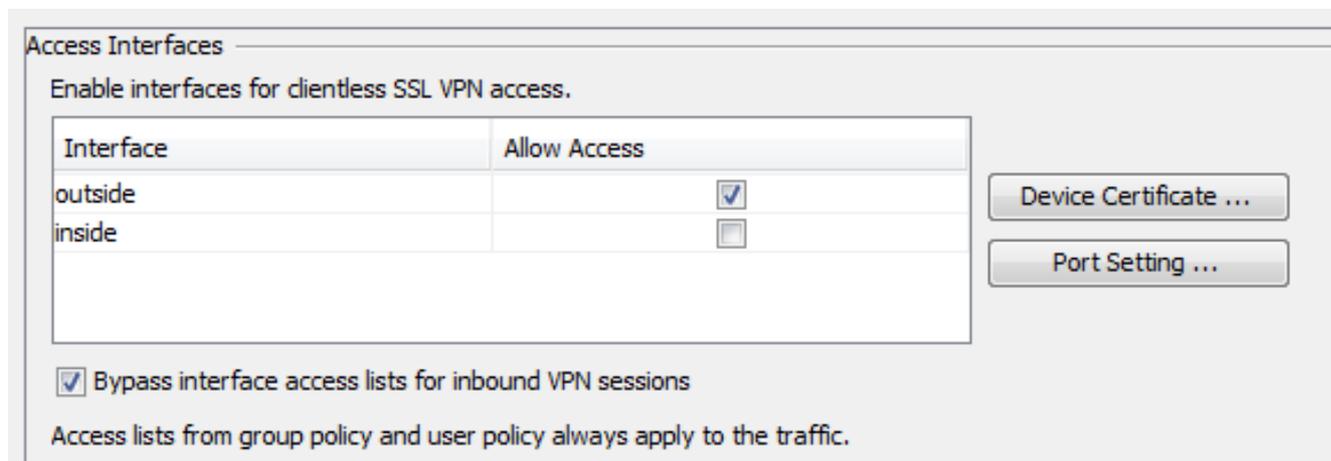


CLI:

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

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

6. Para habilitar el WebVPN en la interfaz exterior, elija **Configuration > Remote Access VPN > Clientless SSL VPN Access > Connection Profiles**. Marque la casilla de verificación **Permitir acceso** junto a la interfaz exterior.



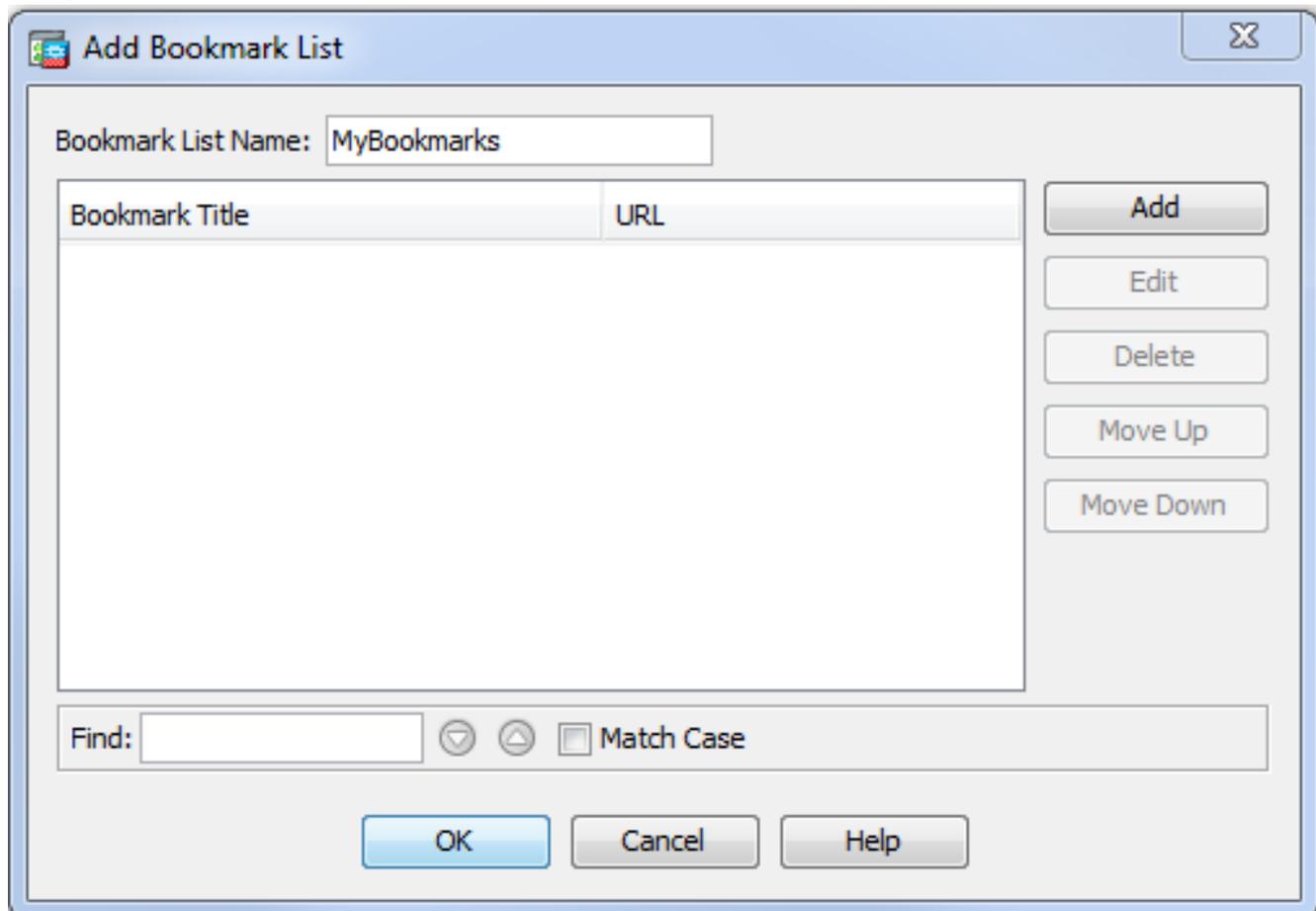
CLI:

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

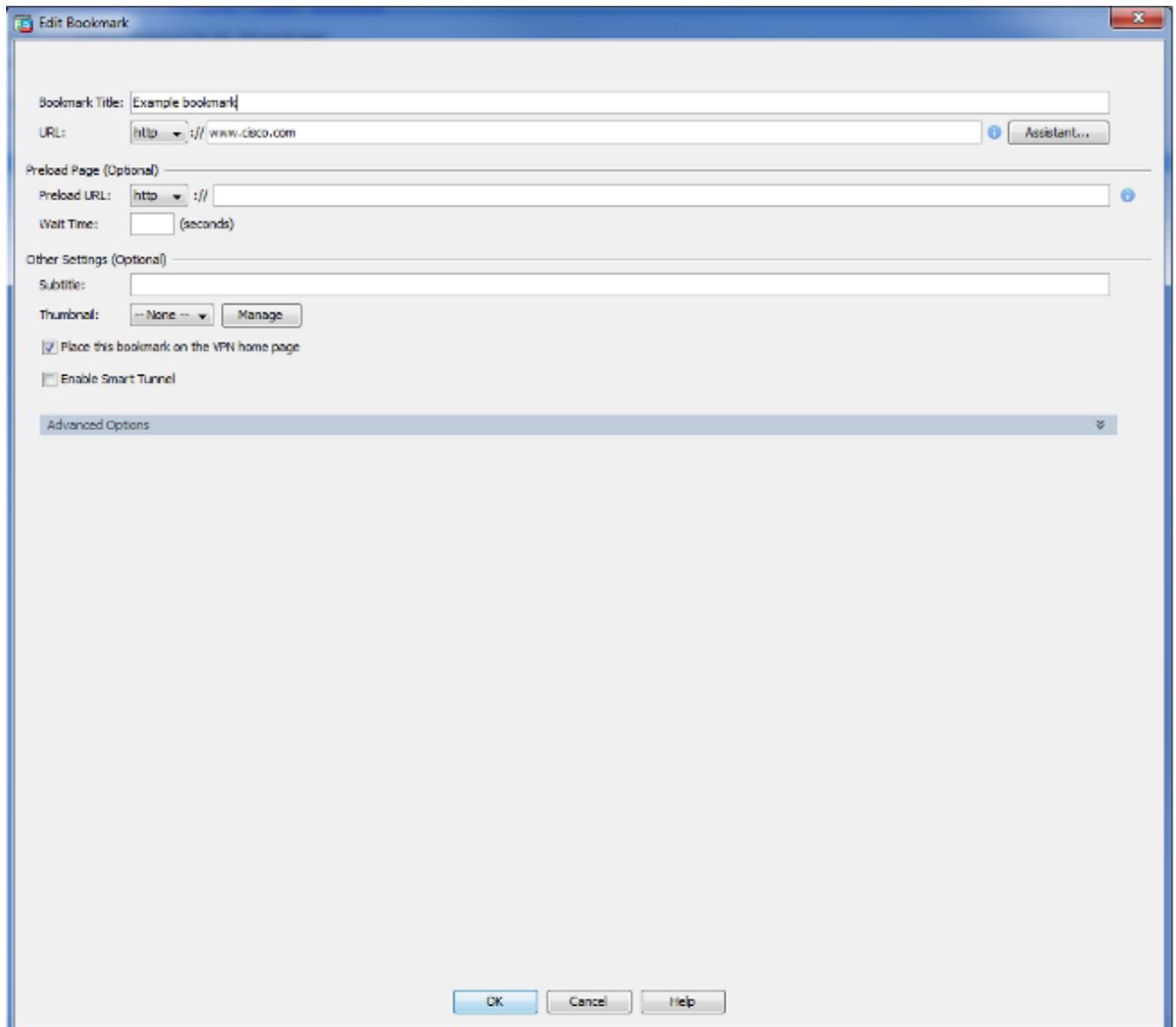
```
ASA(config-webvpn)# enable outside
```

7. (Opcional) Cree marcadores para el contenido. Los marcadores permiten al usuario navegar fácilmente por los recursos internos sin tener que recordar las URL. Para crear un marcador, elija **Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Marcadores >**

Add.

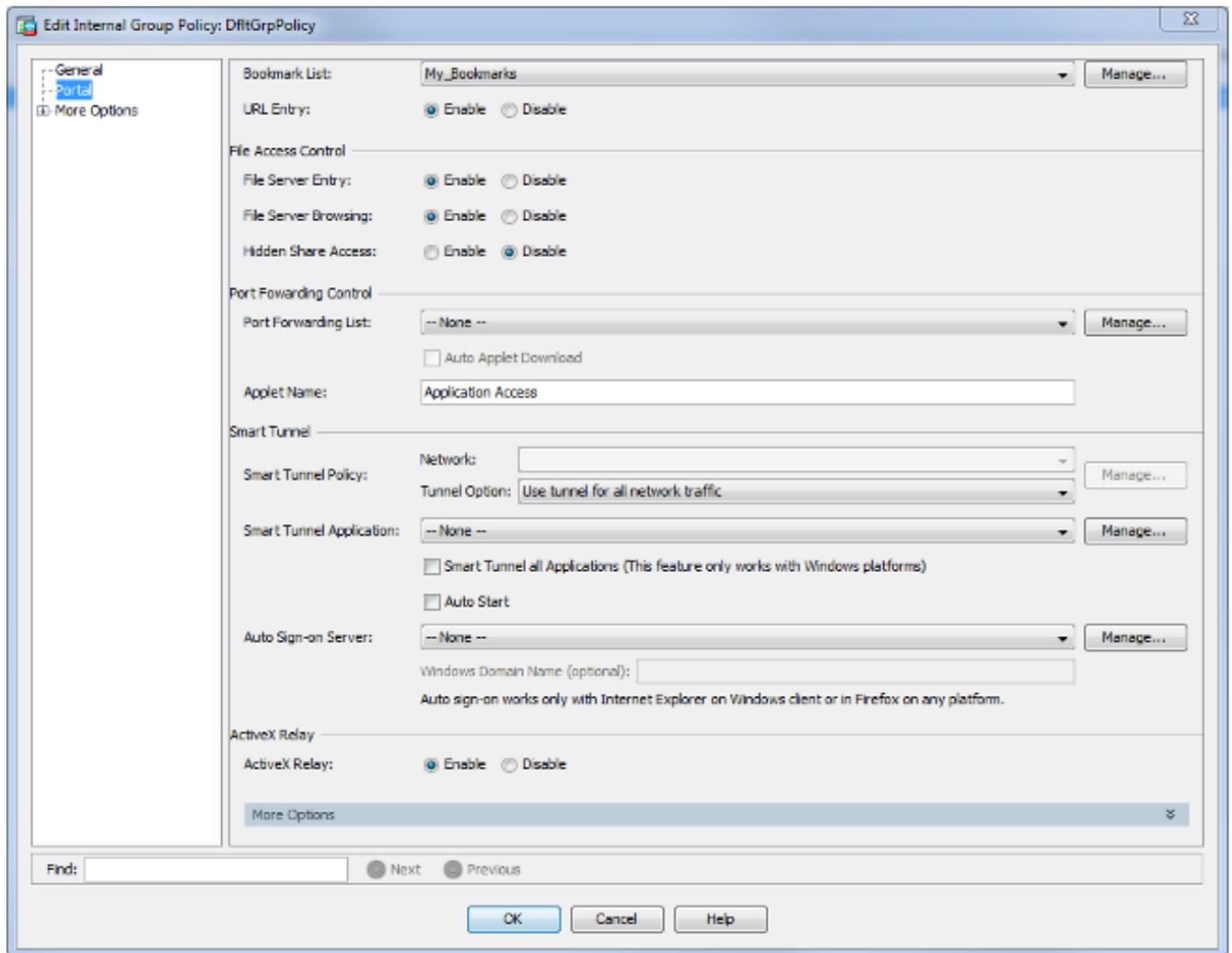


Elija **Add** para agregar un marcador específico.



CLI:Es imposible crear marcadores a través de la CLI porque se crean como archivos XML.

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

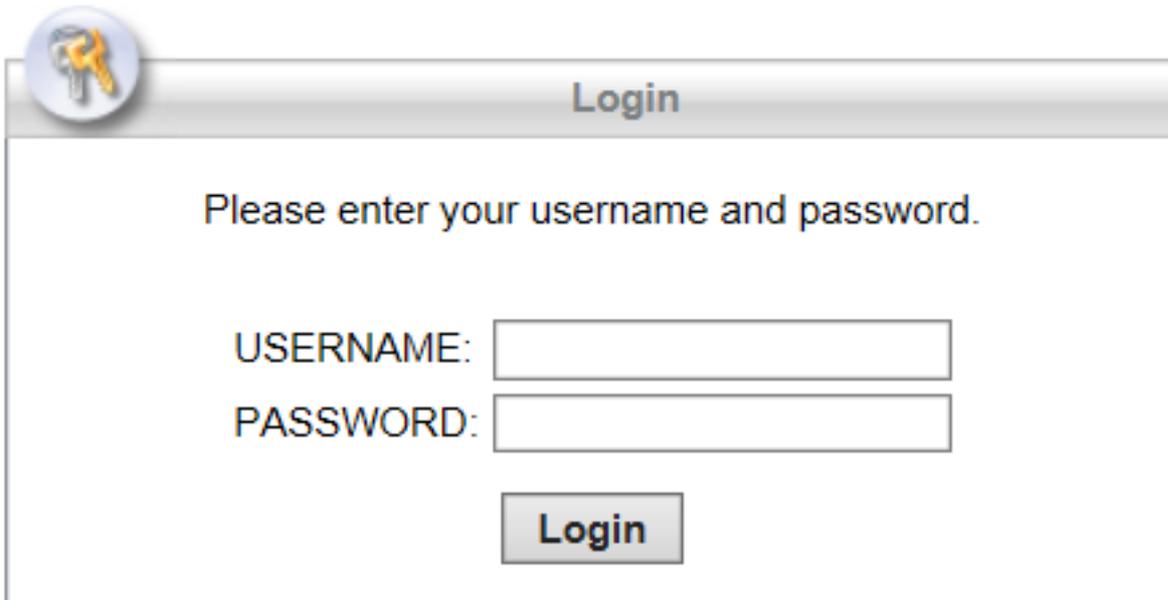


CLI:

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

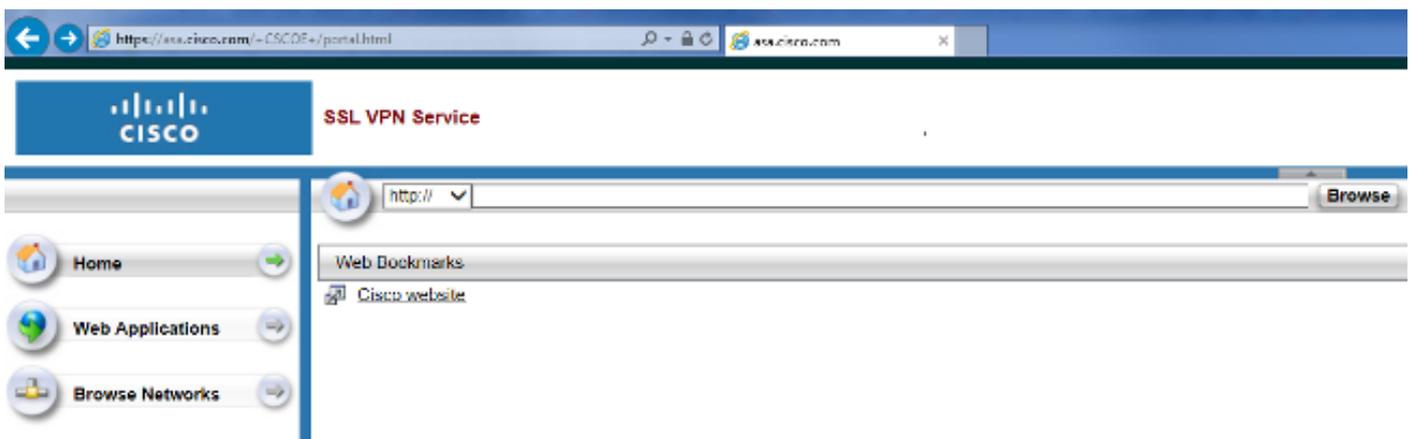
Verificación

Una vez que se ha configurado el WebVPN, utilice la dirección `https://<FQDN del ASA>` en el explorador.



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

Después de iniciar sesión, debería poder ver la barra de direcciones utilizada para navegar a los sitios web y a los marcadores.



Troubleshoot

Procedimientos Usados para Troubleshooting

Siga estas instrucciones para resolver problemas de configuración.

En ASDM, elija **Monitoring > Logging > Real-time Log Viewer > View**. Cuando un cliente se conecta al ASA, observe el establecimiento de la sesión TLS, la selección de la política de grupo y la autenticación exitosa del usuario.

```

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

```

En ASDM, elija **Monitoring > VPN > VPN Statistics > Sessions > Filter by: VPN SSL sin cliente**. Busque la nueva sesión WebVPN. Asegúrese de elegir el filtro de WebVPN y haga clic en **Filtro**. Si ocurre un problema, desvíe temporalmente el dispositivo ASA para asegurarse de que los clientes pueden acceder a los recursos de red deseados. Revisa los pasos para la configuración enumerados en este 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 Troubleshooting

[La herramienta Output Interpreter Tool \(clientes registrados solamente\) \(OIT\) soporta ciertos comandos show.](#) Utilice la OIT para ver un análisis del resultado del comando show.

Nota: Consulte Información Importante sobre Comandos de Debug antes de usar un comando debug.

- **show webvpn** - Hay muchos **comandos show** asociados con WebVPN. Para ver el uso de los comandos **show** en detalle, vea la sección [referencia de comandos](#) del Cisco Security Appliance.
- **debug webvpn** - El uso de los comandos **debug** puede afectar negativamente al ASA. Para ver el uso de los comandos **debug** con más detalle, vea la sección [referencia de comandos](#) del Cisco Security Appliance.

Problemas Comunes

El usuario no puede iniciar sesión

Problema

El mensaje "Acceso VPN SSL sin cliente (navegador) no está permitido". aparece en el navegador después de un intento de inicio de sesión fallido. La licencia AnyConnect Premium no está instalada en el ASA o no está en uso, como se muestra en "La licencia Premium AnyConnect no está habilitada en el ASA".

Solución

Habilite la licencia Premium AnyConnect con estos comandos:

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

Problema

El mensaje "Login failed" (Error de inicio de sesión) aparece en el explorador después de un intento de inicio de sesión fallido. Se ha superado el límite de licencia de AnyConnect.

Solución

Busque este mensaje en los registros:

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

Además, verifique su límite de licencia:

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

Problema

El mensaje "AnyConnect no está habilitado en el servidor VPN" aparece en el explorador después de un intento de inicio de sesión fallido. El protocolo VPN sin cliente no está habilitado en la política de grupo.

Solución

Busque este mensaje en los registros:

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

Asegúrese de que el protocolo VPN sin cliente esté habilitado para la política de grupo deseada:

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

No se puede conectar más de tres usuarios de WebVPN al ASA

Problema

Sólo tres clientes WebVPN pueden conectarse al ASA. La conexión para el cuarto cliente falla.

Solución

En la mayoría de los casos, este problema se relaciona con una configuración simultánea del login dentro de la política del grupo. Utilice esta ilustración para configurar el número deseado de inicios de sesión simultáneos. En este ejemplo, el valor deseado es 20.

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

Los clientes de WebVPN no pueden acceder a los marcadores y están atenuados

Problema

Si estos marcadores se configuraron para que los usuarios inicien sesión en la VPN sin cliente, pero en la pantalla de inicio en "Aplicaciones web" aparecen atenuados, ¿cómo puedo habilitar estos enlaces HTTP para que los usuarios puedan hacer clic en ellos e ir a la URL en particular?

Solución

Primero debe asegurarse de que el ASA pueda resolver los sitios Web con DNS. Intente hacer ping en los sitios web por nombre. Si el ASA no puede resolver el nombre, la conexión se atenuará. Si los servidores DNS son internos a su red, configure la interfaz privada de dominio de búsqueda DNS.

Conexión de Citrix a través de WebVPN

Problema

Aparece el mensaje de error “ **the ica client received a corrupt icafile.**” para el Citrix en WEBVPN.

Solución

Si utiliza el modo *seguro de gateway para la conexión del Citrix con WebVPN*, el archivo ICA puede dañarse. Como el ASA no es compatible con este modo de operación, cree un nuevo archivo ICA en el modo directo (modo NON-seguro).

Cómo evitar la necesidad de una segunda autenticación para los usuarios

Problema

Cuando accede a los enlaces CIFS en el portal WebVPN sin cliente, se le solicitarán las credenciales después de hacer clic en el marcador. El protocolo ligero de acceso a directorios (LDAP) se utiliza para autenticar tanto los recursos como los usuarios que ya han ingresado credenciales LDAP para iniciar sesión en la sesión VPN.

Solución

En este caso, puede utilizar la función de inicio de sesión automático. En la política de grupo específica que se utiliza y en sus atributos WebVPN, configure lo siguiente:

```
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
```

donde X.X.X.X=IP del servidor CIFS y *=resto de la trayectoria para alcanzar el archivo/carpeta de recursos compartidos en cuestión.

Aquí se muestra un fragmento de configuración de ejemplo:

```
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 obtener más información sobre esto, vea [Configuración de SSO con HTTP Basic o NTLM Authentication](#).

Información Relacionada

- [ASA: Ejemplo de Configuración de Túnel Inteligente con ASDM](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)