Clientless SSL VPN (WebVPN) de la configuración en el ASA

Contenido

Introducción

Este documento proporciona una configuración directa para las 5500 Series adaptantes del dispositivo de seguridad de Cisco (ASA) para permitir el acceso de Secure Sockets Layer (SSL) VPN del clientless a los recursos de red interna. El clientless SSL Virtual Private Network (WebVPN) permite limitado, pero el objeto de valor, acceso seguro a la red corporativa de cualquier ubicación. Los usuarios pueden alcanzar el acceso basado en buscador seguro a los recursos corporativos en cualquier momento. No hay cliente adicional necesario para acceder a los recursos internos. El acceso se proporciona usando un Protocolo de transporte de hipertexto sobre la conexión SSL.

El clientless SSL VPN proporciona seguro y de fácil acceso a una amplia gama de recursos Web y red-habilitado y las aplicaciones de legado de casi cualquier ordenador que pueda alcanzar los sitios de Internet del Protocolo de transporte de hipertexto (HTTP). Esto incluye:

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

- Acceso Web 2003, 2007, y 2013 del Microsoft Outlook
- Microsoft Outlook Web App 2010
- Acceso Web del dominó (DWA) 8.5 y 8.5.1
- Servidor 4.x de la presentación de Metaframe del Citrix
- Versión 5 a 6.5 de XenApp del Citrix
- Versión 5 a 5.6 de XenDesktop del Citrix, y 7.5
- Opinión 4 de VMware

Una lista de software admitido se puede encontrar en las Plataformas soportadas VPN, las 5500 Series de Cisco ASA.

Prerequisites

Requisitos

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- navegador SSL-habilitado
- ASA con la versión 7.1 o posterior
- Certificado X.509 publicado al Domain Name 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 las Plataformas soportadas VPN, las 5500 Series de Cisco ASA.

Componentes Utilizados

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

- Versión de ASA 9.4(1)
- Versión 7.4(2) adaptante del Administrador de dispositivos de seguridad (ASDM)
- ASA 5515-X

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos usados en este documento comenzaron con una configuración despejada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

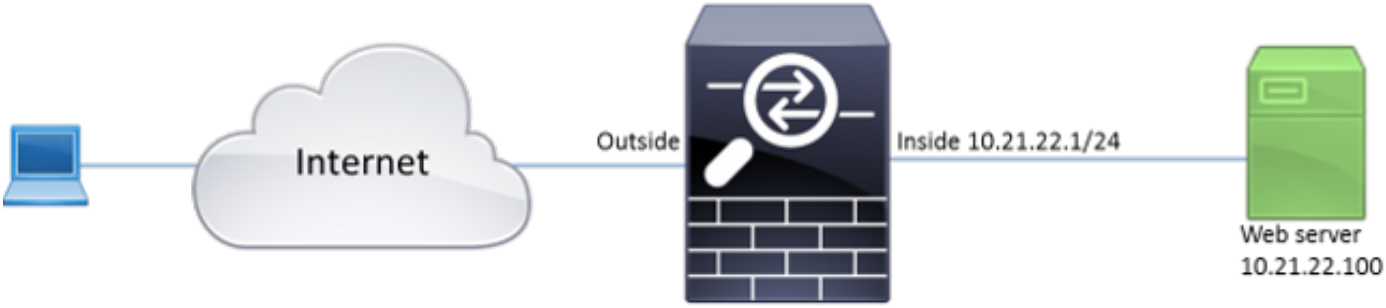
Configurar

Este artículo describe el proceso de configuración para el ASDM y el CLI. Usted puede elegir seguir cualquiera de las herramientas para configurar el WebVPN, pero algunos de los pasos para la configuración se pueden alcanzar solamente con el ASDM.

> **Note**: Use la Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos usados en esta sección.

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Antecedentes

El WebVPN utiliza el Protocolo SSL para asegurar los datos transferidos entre el cliente y el servidor. Cuando el navegador inicia una conexión al ASA, el ASA presenta su certificado para autenticarse al navegador. Para asegurarse de que la conexión entre el cliente y el ASA sea segura, usted necesita proporcionar el ASA con el certificado que es firmado por el Certificate Authority ese las confianzas del cliente ya. Si no el cliente no tendrá los medios de verificar la autenticidad del ASA que los resultados en la posibilidad del ataque del intermediario y de la experiencia pobre del usuario, porque el navegador produce una advertencia que la conexión no está confiada en.

> **Note**: Por abandono, el ASA genera un certificado uno mismo-firmado X.509 sobre el lanzamiento. Este certificado se utiliza para servir las conexiones cliente por abandono. No se recomienda para utilizar este certificado porque su autenticidad no se puede verificar por el navegador. Además, este certificado se regenera sobre cada reinicialización así que cambia después de cada reinicialización.

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

Configuración

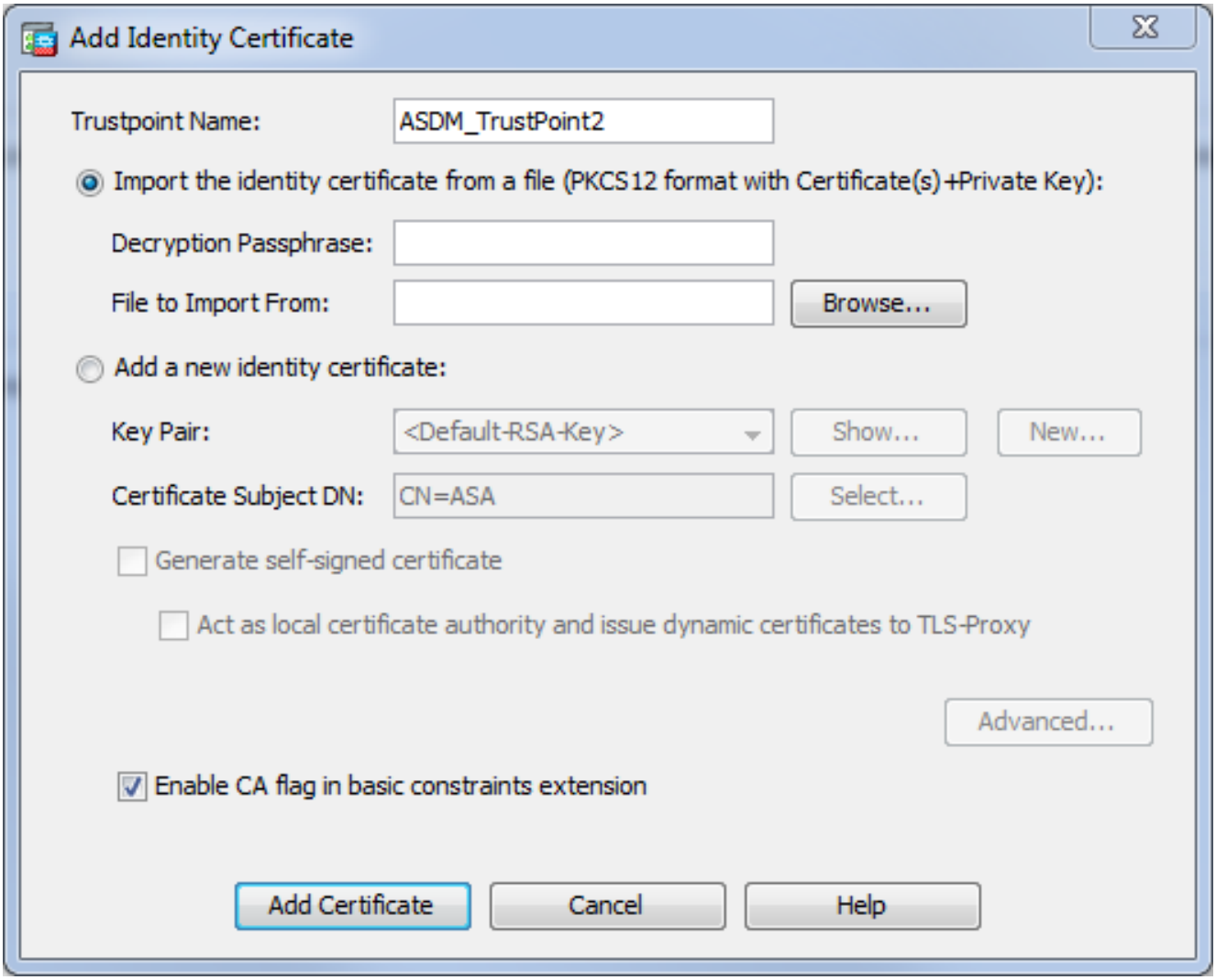
Configure el WebVPN en el ASA con cinco pasos principales:

- Configure el certificado que será utilizado por el ASA.
- Habilite el WebVPN en una interfaz ASA.
- Cree una lista de los servidores y/o del Uniform Resource Locator (URL) para el acceso del WebVPN.
- Cree una política de grupo para los usuarios de WebVPN.
- Aplique la nueva política del grupo a un grupo de túnel.

> **Note**: En las versiones ASA más adelante que la versión 9.4, el algoritmo usado para elegir las cifras SSL se ha cambiado (véase los Release Note para la serie de Cisco ASA, 9.4(x)).If solamente que utilizarán a los clientes curva-capaces elípticos, después es seguro utilizar la clave privada elíptica de la curva para el certificado. Si no la habitación de encargo

de la cifra se debe utilizar para evitar tener el presente ASA un certificado temporal uno mismo-firmado. Usted puede configurar el ASA para utilizar solamente las cifras RSA-basadas con el comando **de encargo "AES256-SHA:AES128-SHA:DHE-RSA-AES256-SHA:DHE-RSA-AES128-SHA:DES-CBC3-sha:des-CBC-SHA:RC4-SHA:RC4-Md5" de la cifra tlsv1.2 SSL**.

1. **Opción 1** - Importe el certificado con el archivo del pkcs12.Elija la **configuración > el Firewall > avanzó el Certificate Management (Administración de certificados) > los certificados de identidad > Add**. Usted puede instalarlo con el archivo del pkcs12 o pegar el contenido en Privacy Enhanced Mail (PEM)
formate.

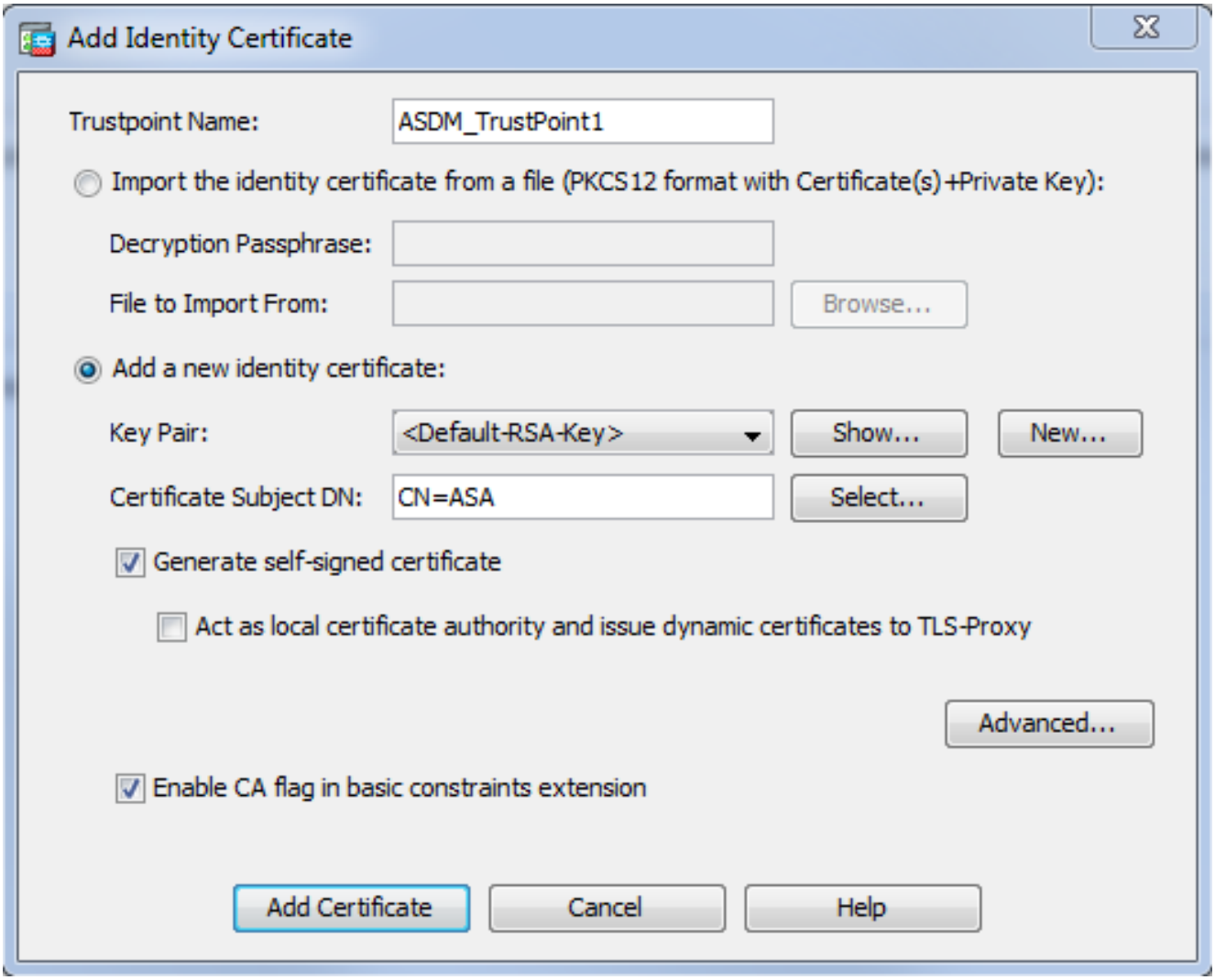


CLI:

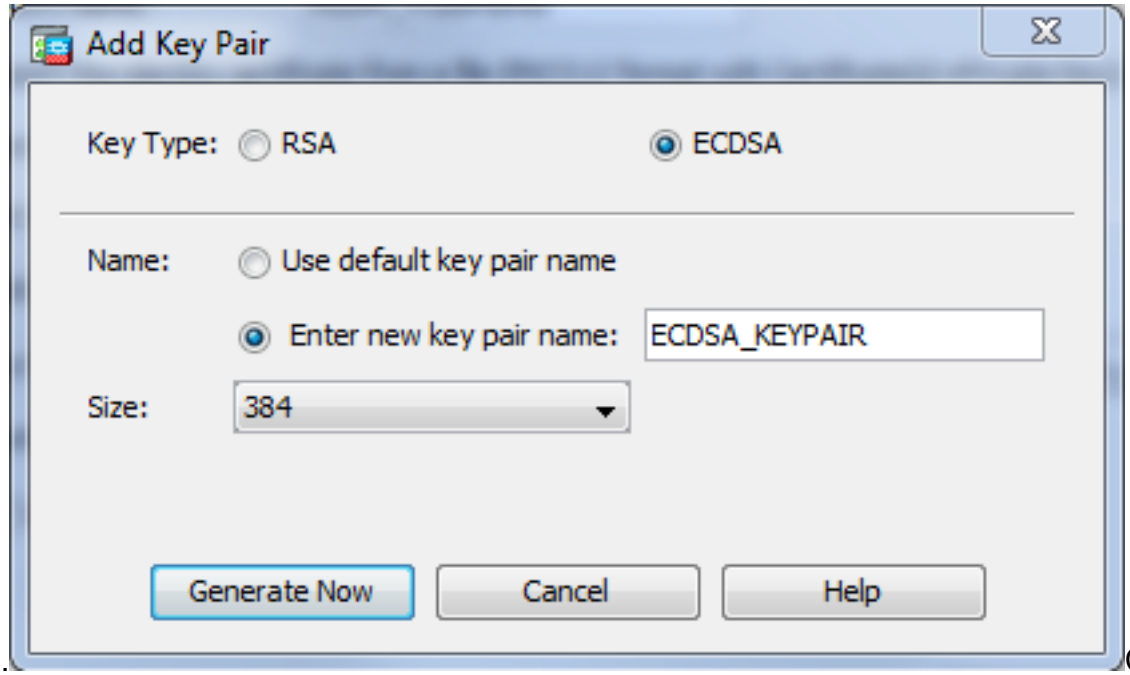
```
ASA(config)# crypto ca import TrustPoint-name pkcs12 "password"


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
```

Opción 2 - Cree un certificado autofirmado.Elija la **configuración > el Firewall > avanzó el Certificate Management (Administración de certificados) > los certificados de identidad > Add**.Haga clic el **agregar un nuevo** botón de radio del **certificado de identidad**. Marque la **casilla de verificación del certificado autofirmado de la generación**. Elija un Common Name (CN) que hace juego el Domain Name del
ASA.



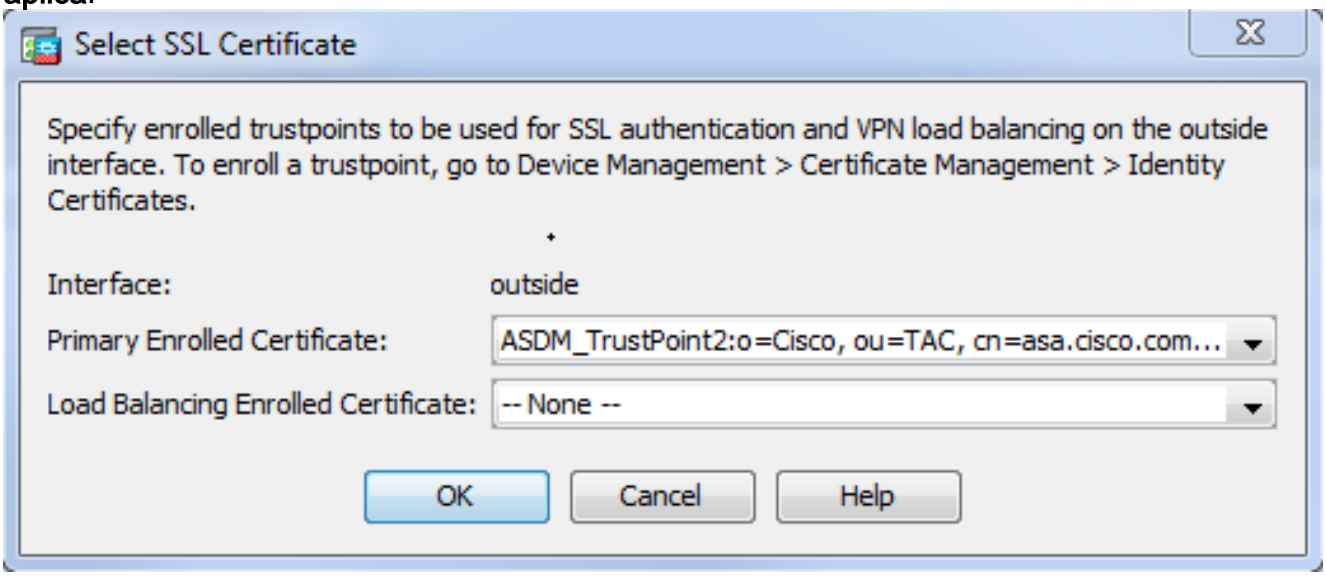
Haga clic **nuevo** para crear el keypair para el certificado. Elija el tipo, el nombre, y el tamaño



dominantes.C LI:

```
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 será utilizado para servir las conexiones WebVPN.Elija la **configuración > el VPN de acceso remoto > avanzó > las configuraciones SSL**. Del menú de los Certificados, elija el trustpoint asociado al certificado deseado para la interfaz exterior. El tecleo **se aplica**.

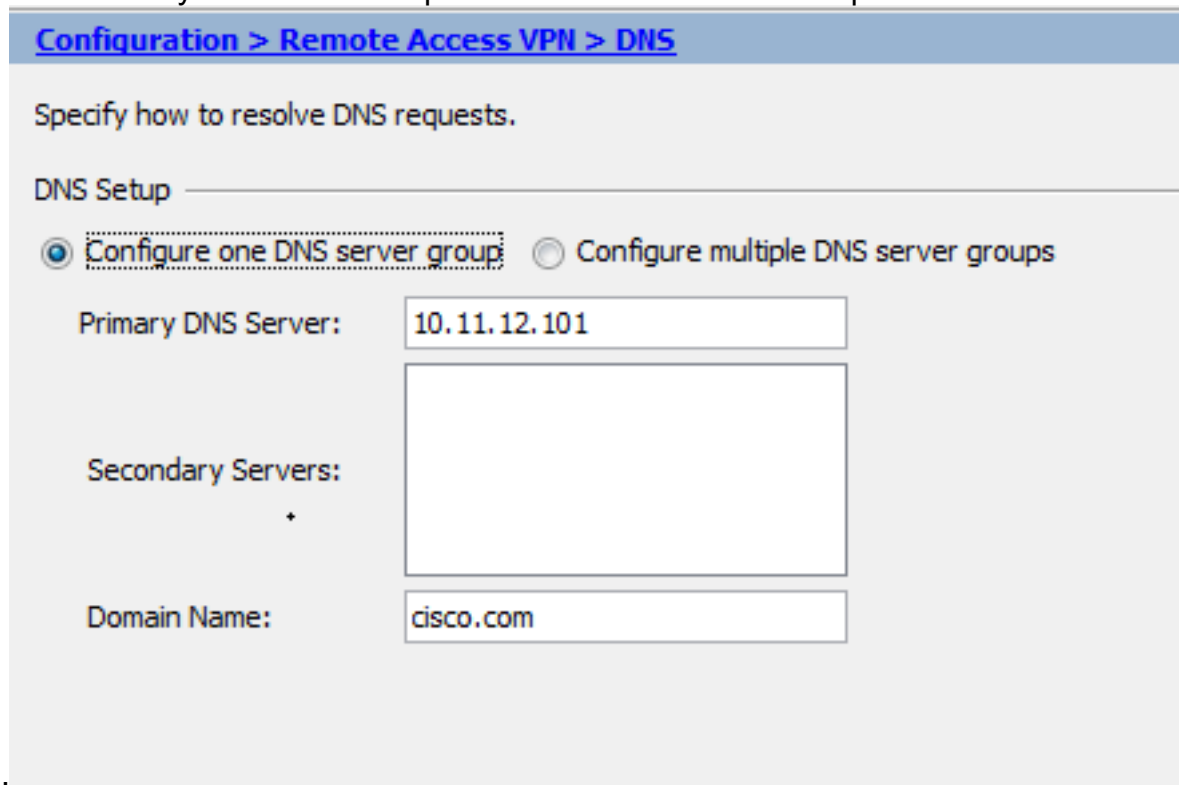


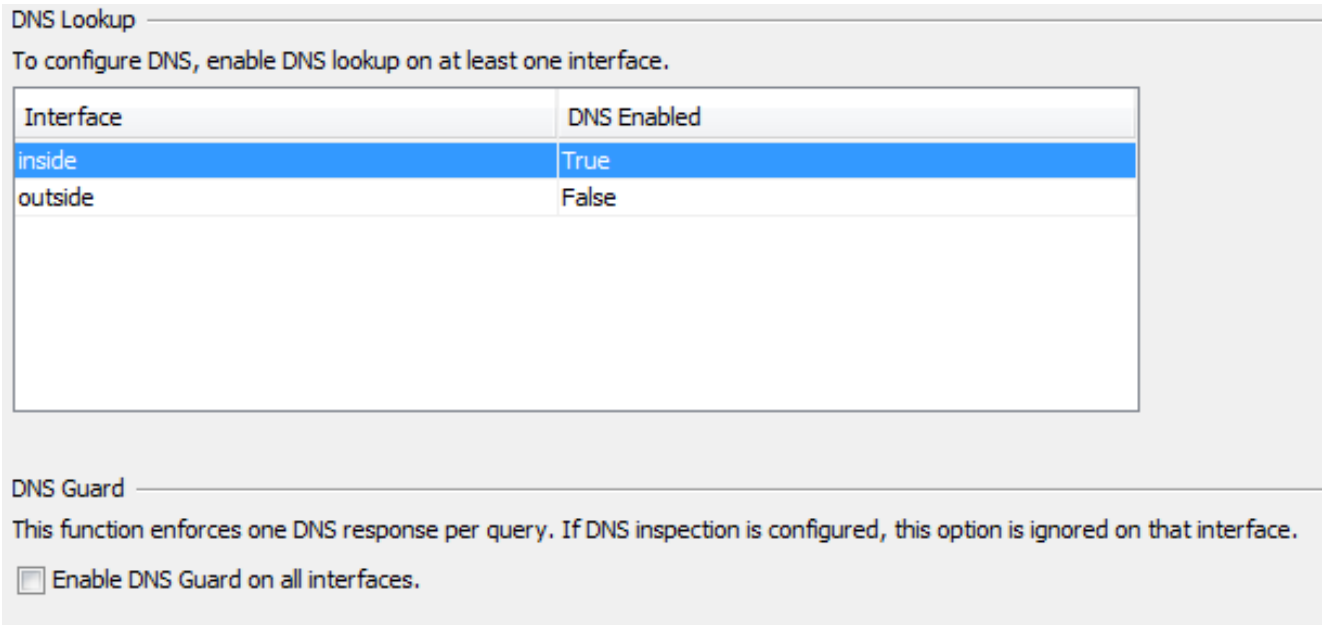
Configuración CLI equivalente:

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

3. Operaciones de búsqueda (opcionales) del Domain Name Server del permiso (DNS).El servidor WebVPN actúa como proxy para las conexiones cliente. Significa que el ASA crea las conexiones a los recursos en nombre del cliente. Si los clientes requieren las conexiones

a los recursos que utilizan los Domain Name, después el ASA necesita realizar la búsqueda de DNS.Elija la **configuración > el VPN de acceso remoto > el DNS**.Configure por lo menos a un servidor DNS y habilite las búsquedas de DNS en la interfaz que hace frente al servidor DNS.

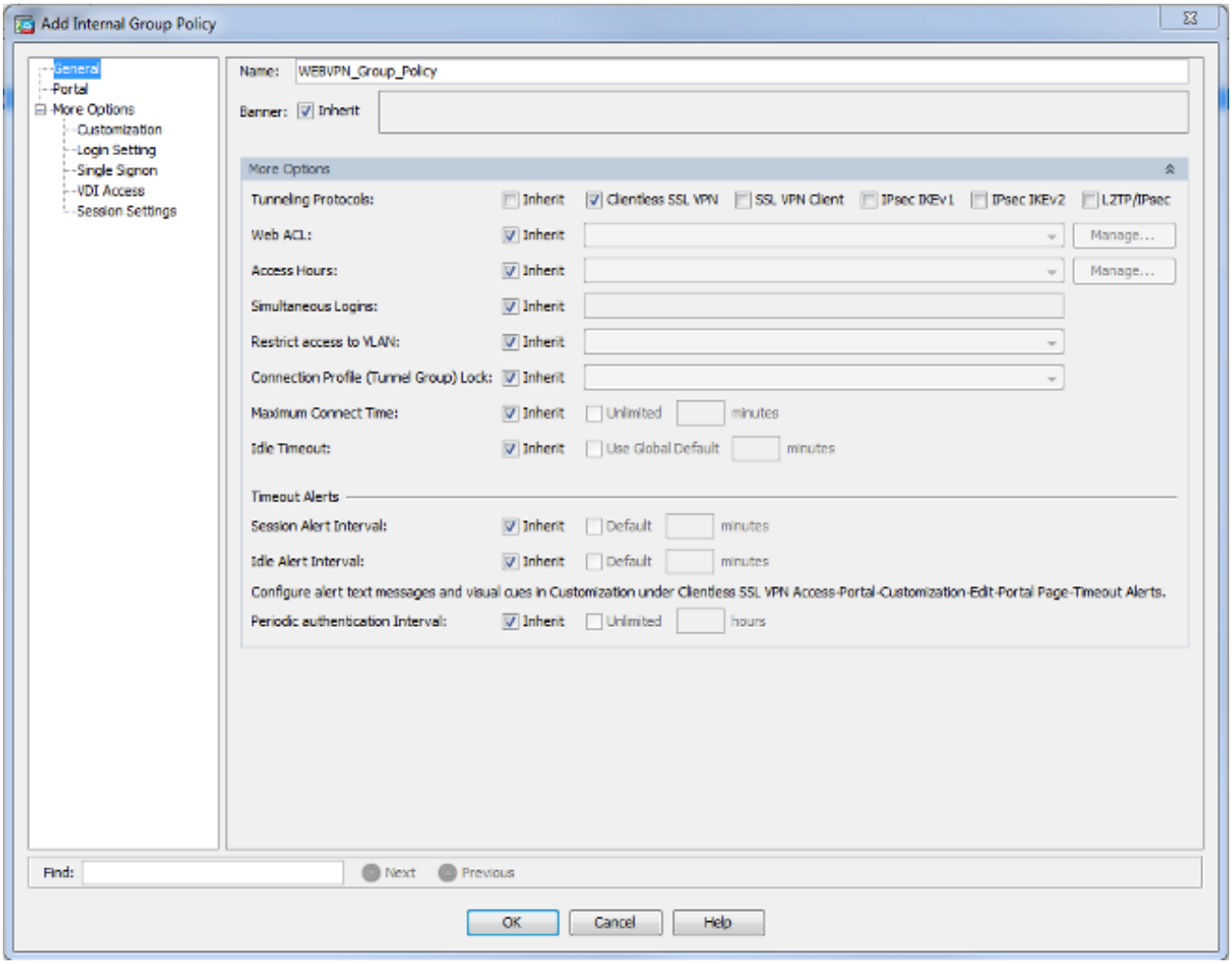




CLI:

```
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) cree la directiva del grupo para las conexiones WebVPN.Elija la **configuración > el acceso del VPN de acceso remoto > del clientless SSL VPN > el Internal group policy (política grupal interna) de las directivas del grupo > Add**.Bajo opciones generales cambie el valor de los protocolos de Tunelling al “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
```

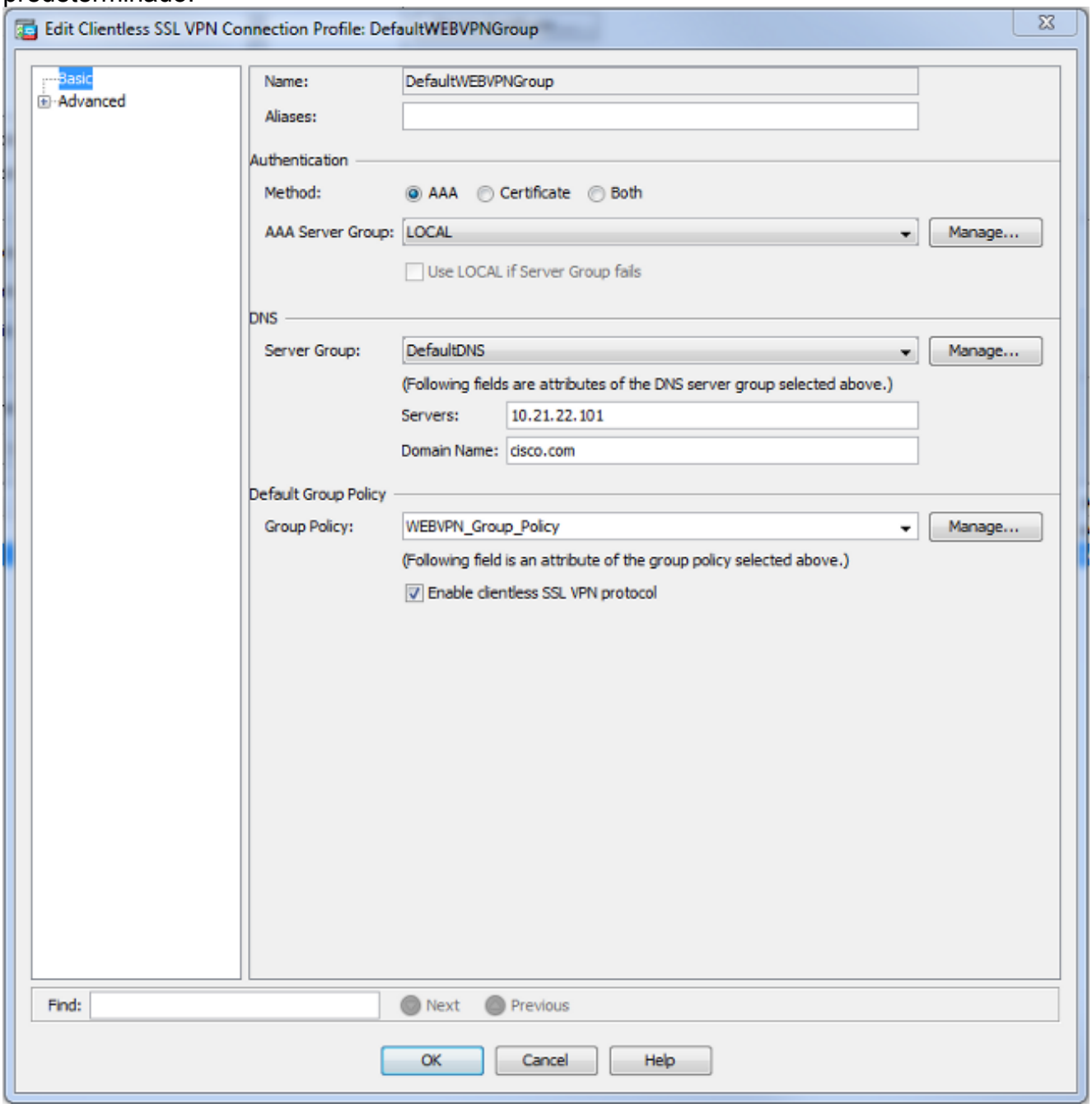
5. Configure el perfil de la conexión.En el ASDM, elija la **configuración > el VPN de acceso remoto > el acceso > los perfiles de la conexión del clientless SSL VPN**.
   Para una descripción de los perfiles de la conexión y de las directivas del grupo, consulte la guía de configuración CLI de la serie VPN de Cisco ASA, 9.4 - los perfiles de la conexión, las directivas del grupo, y a los usuarios.Por abandono, las conexiones WebVPN utilizan el perfil de DefaultWEBVPNGroup. Usted puede crear los perfiles adicionales.**Note**: Hay distintas maneras de asignar a los usuarios a otros perfiles.

   - Los usuarios pueden seleccionar manualmente el perfil de la conexión de la lista desplegable o con un URL específico. Vea ASA 8.x: Permita que los usuarios seleccionen a un grupo en el login del WebVPN vía el Grupo-alias y el método Grupo-URL.

   - Cuando usted utiliza a un servidor LDAP, usted puede asignar el perfil del usuario basado en los atributos recibidos del servidor LDAP, ve el uso ASA del ejemplo de configuración de las correspondencias del atributo LDAP.

   - Cuando usted utiliza la autenticación basada en el certificado de los clientes, usted puede asociar al usuario a los perfiles basados en los campos contenidos en el certificado, ve la guía de configuración CLI de la serie VPN de Cisco ASA, 9.4 - configure el grupo del certificado que corresponde con para IKEv1.

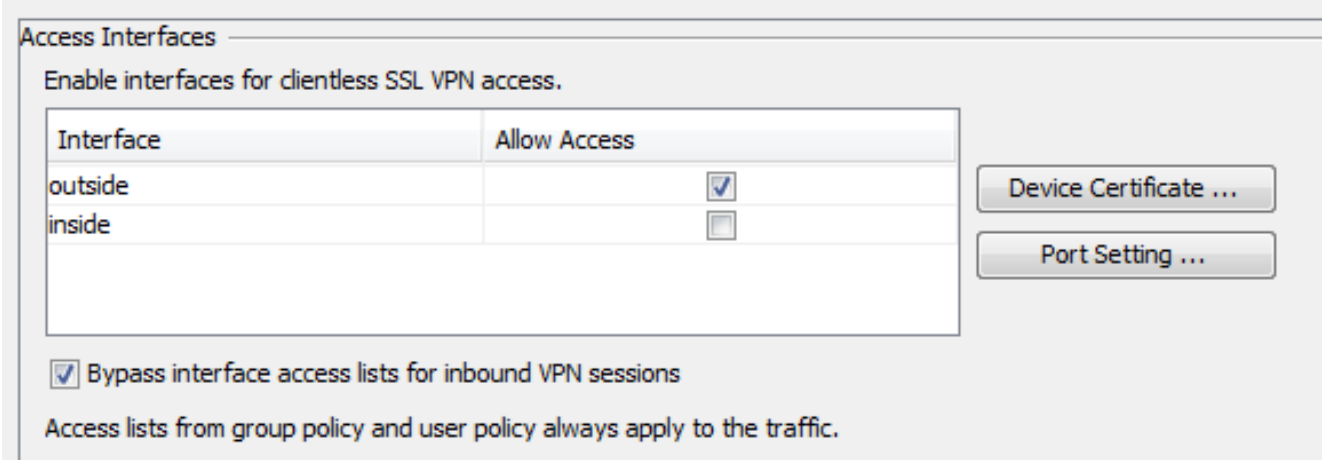
- Para asignar a los usuarios manualmente a la directiva del grupo, vea la guía de configuración CLI de la serie VPN de Cisco ASA, 9.4 - configurar los atributos para los usuarios individualesEdite el perfil de DefaultWEBVPNGroup y elija el WEBVPN_Group_Policy bajo directiva del grupo predeterminado.



CLI:

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

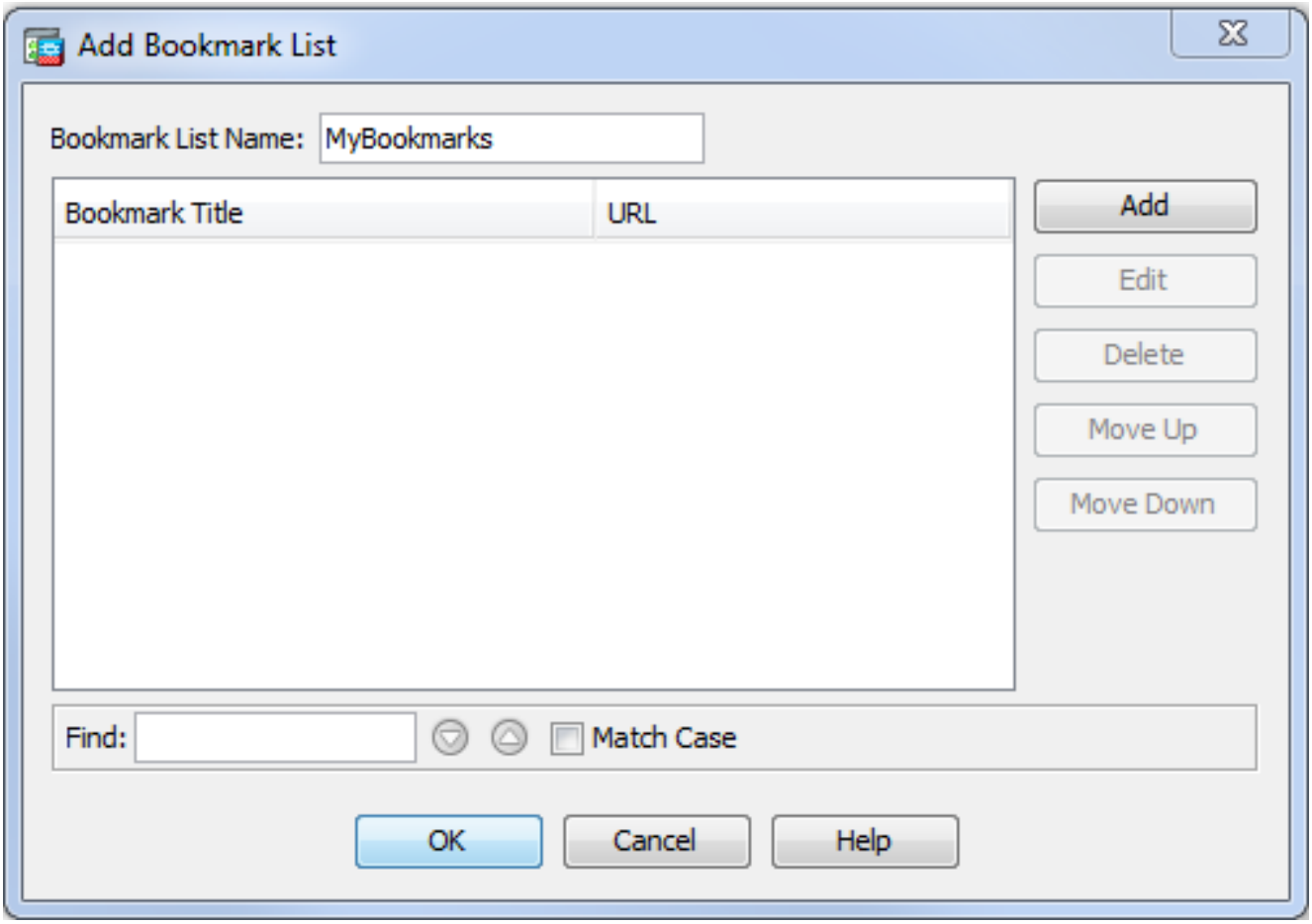
6. Para habilitar el WebVPN en la interfaz exterior, elija la **configuración > el VPN de acceso remoto > el acceso > los perfiles de la conexión del clientless SSL VPN**.Marque el checkbox del **acceso de la permit** al lado de la interfaz exterior.



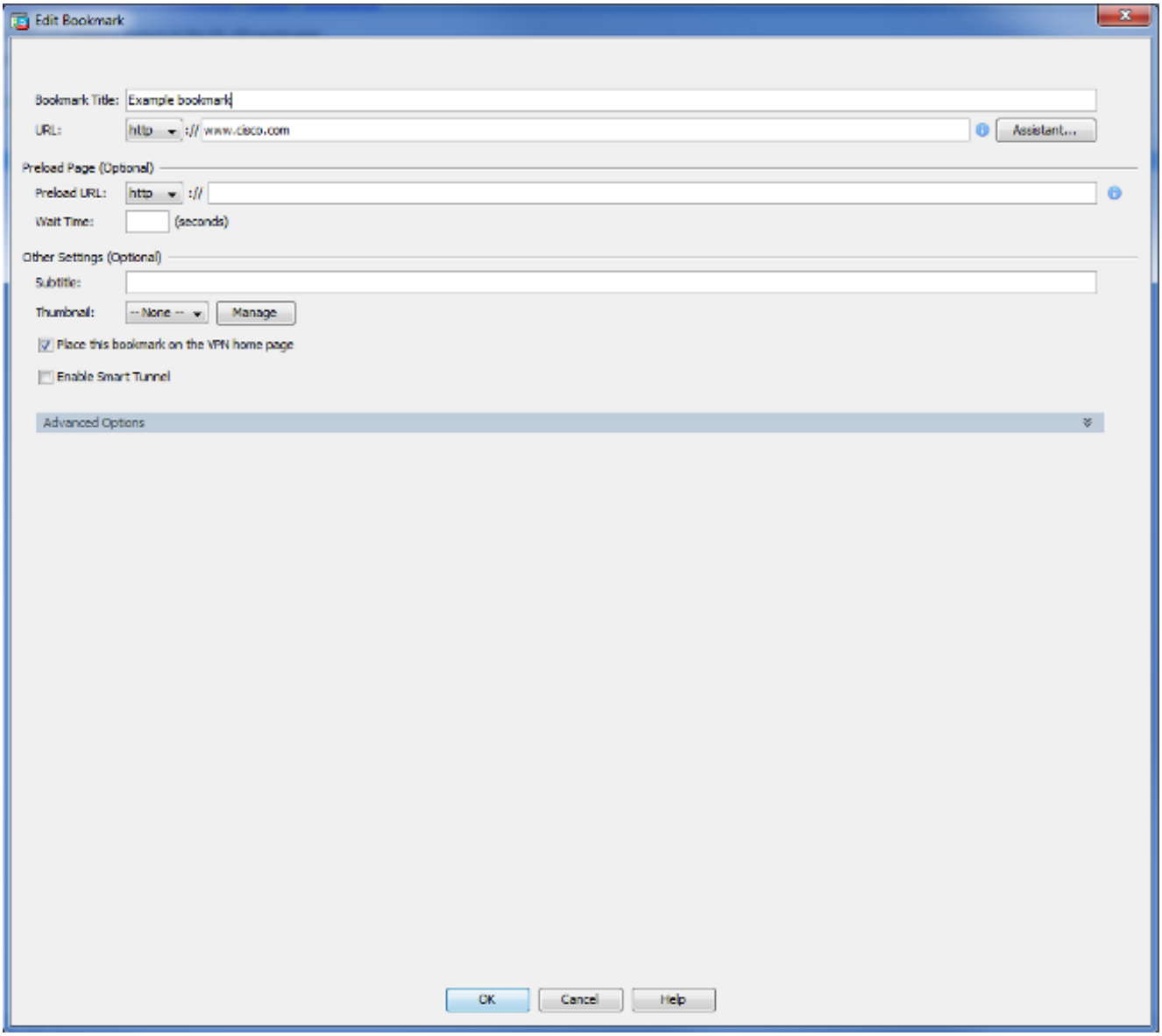
CLI:

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

7. (Opcional) cree los marcadores por contenido.Los marcadores permiten que el usuario hojee fácilmente a los recursos internos sin tener que recordar los URL.Para crear un marcador, elija la **configuración > el VPN de acceso remoto > el acceso > el portal > los marcadores del clientless SSL VPN >**
Add.

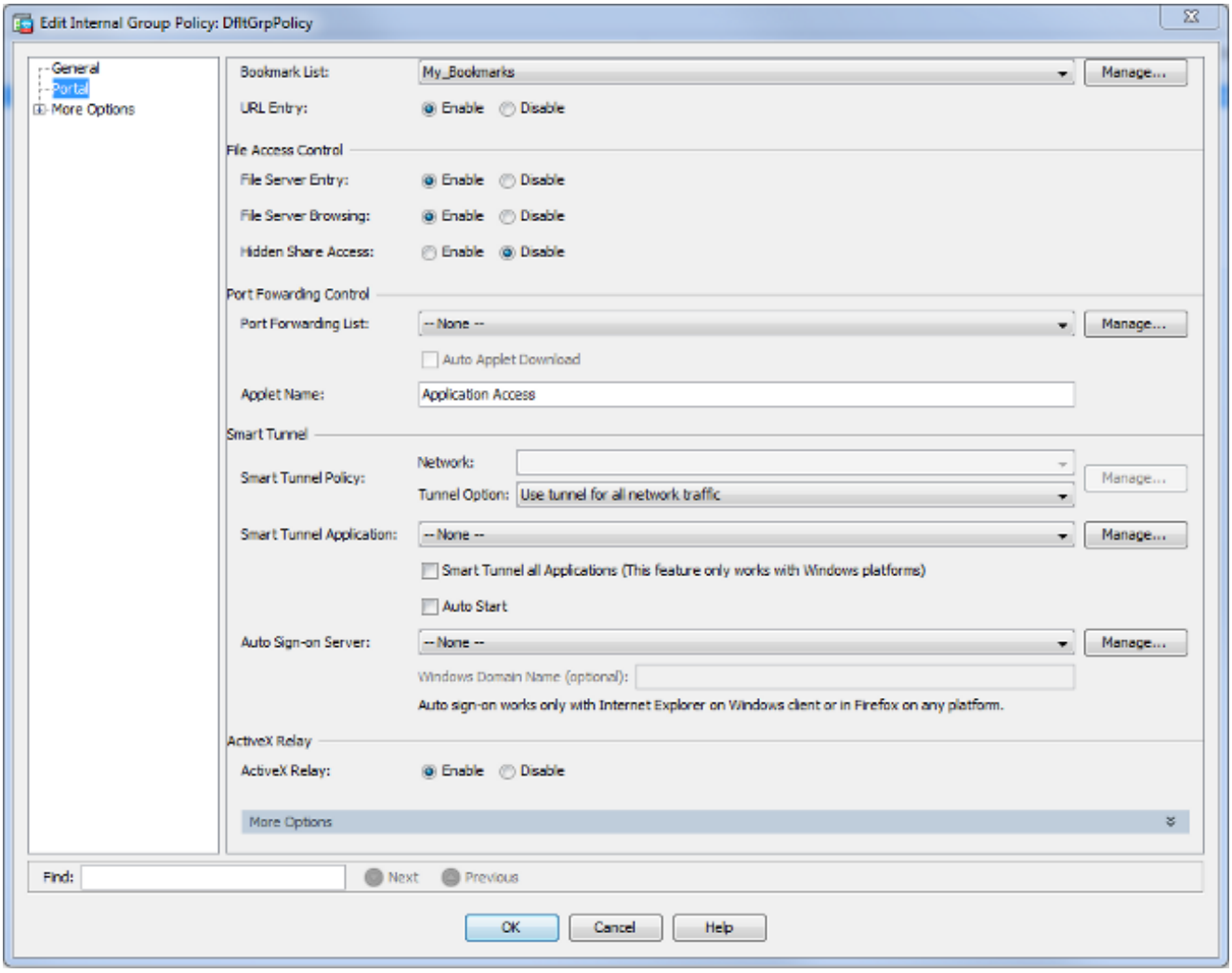


Elija **agregan** para agregar un marcador específico.



CLI:Es imposible crear los marcadores vía el CLI porque se crean como archivos XML.

8. (Opcional) asigne los marcadores a una directiva específica del grupo.Elija la **configuración > el VPN de acceso remoto > las directivas del acceso > al grupo del clientless SSL VPN > editan > lista del portal > del marcador**.

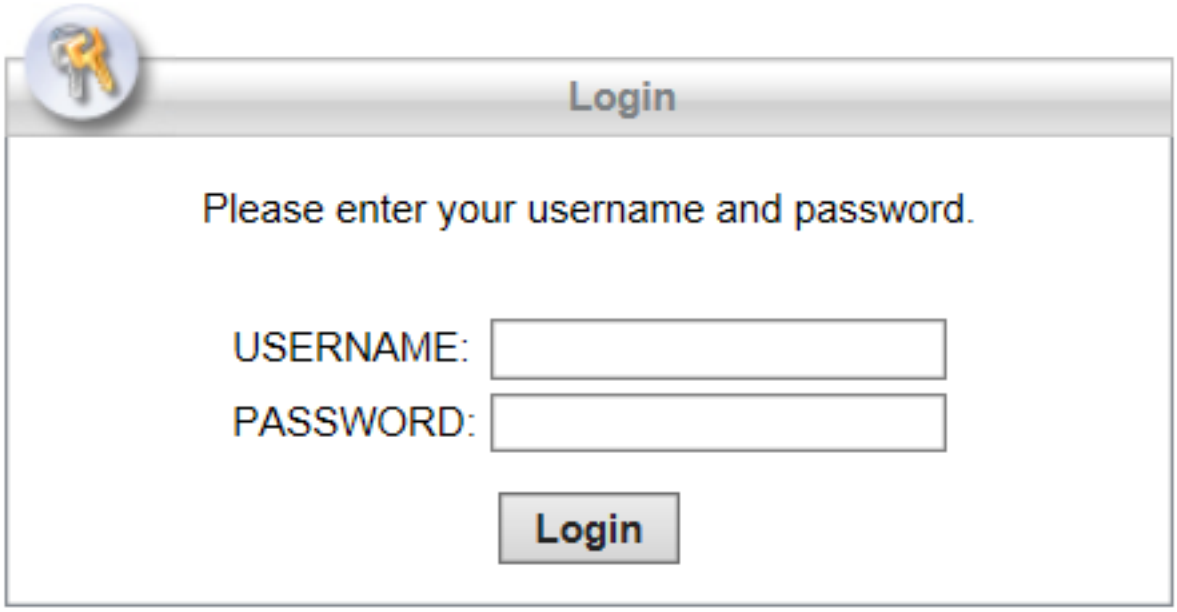


CLI:

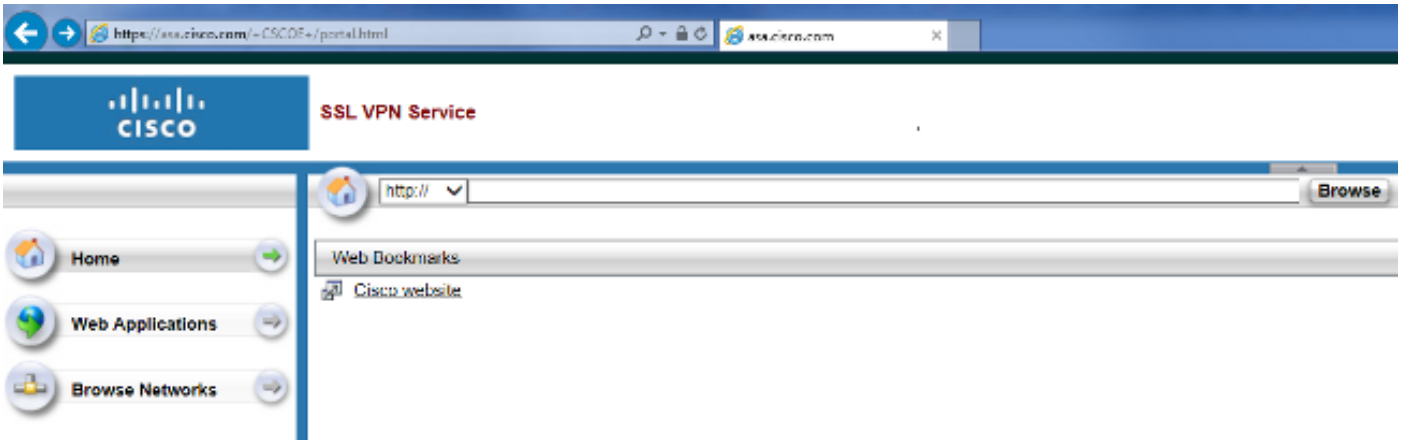
```
ASA(config)# group-policy DfltGrpPolicy attributes
ASA(config-group-policy)# webvpn
ASA(config-group-webvpn)# url-list value My_Bookmarks
```

Verificación

Una vez que se ha configurado el WebVPN, utilice el direccionamiento https:// <FQDN del *ASA*> en el navegador.



Después de abrir una sesión usted debe poder ver la barra de dirección usada para navegar a los sitios web y a los marcadores.



Troubleshooting

Procedimientos Usados para Troubleshooting

Siga estas instrucciones para resolver problemas su configuración.

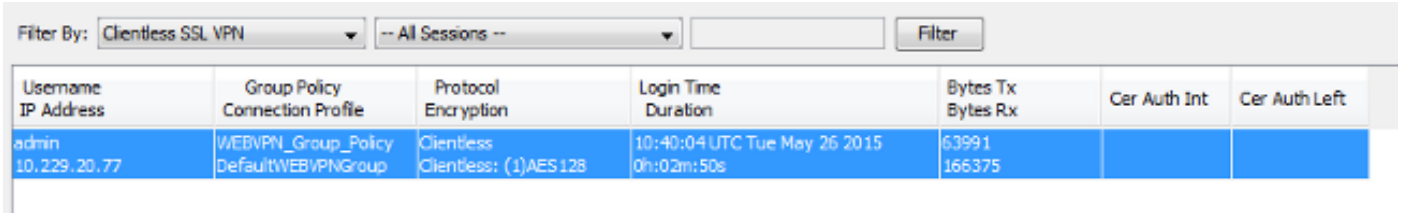
En ASDM, elija **Monitoring > Logging > Real-time Log Viewer > View**. Cuando un cliente conecta con el ASA, observe el establecimiento de sesión de TLS, la selección de directiva del grupo, y la autenticación satisfactoria del usuario.

```
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 el ASDM, elija la **supervisión** > el **VPN** > los **VPN statistics (Estadísticas de la VPN)** > las **sesiones > el filtro por: Clientless SSL VPN.** 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.



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.

> **Note**: Consulte Información Importante sobre Comandos de Debug antes de usar un **comando debug**.

- **webvpn de la demostración** - Hay muchos **comandos show** asociados al WebVPN. Para ver el uso de los **comandos show** detalladamente, vea la sección de referencia de comandos del dispositivo del Cisco Security.
- **webvpn del debug -** El uso de los **comandos debug** puede afectar al contrario el ASA. Para ver el uso de los **comandos debug** más detalladamente, vea la sección de referencia de comandos del dispositivo del Cisco Security.

Problemas Comunes

El usuario no puede iniciar sesión

Problema

El mensaje acceso el “del clientless (navegador) SSL VPN no se permite.” aparece en el navegador después de un intento de inicio de sesión fracasado. La licencia superior de AnyConnect no está instalada en el ASA o es parada como se muestra por la “licencia superior de AnyConnect no se habilita en el ASA.”

Solución

Habilite la licencia superior de AnyConnect con estos comandos:

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

Problema

El mensaje “login fallado” aparece en el navegador después de un intento de inicio de sesión fracasado. Se ha excedido el límite de la licencia de AnyConnect.

Solución

Busque este mensaje en los registros:

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

También, verifique su límite de la licencia:

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

Problema

El mensaje “AnyConnect no se habilita en el servidor VPN” aparece en el navegador después de un intento de inicio de sesión fracasado. El protocolo VPN del clientless no se habilita en la grupo-directiva.

Solución

Busque este mensaje en los registros:

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

Aseegurese que el protocolo VPN del clientless está habilitado para la grupo-directiva deseada:

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

Incapaz de conectar a más de tres usuarios de WebVPN con el ASA

Problema

Solamente tres clientes del WebVPN pueden conectar con el 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 este ejemplo para configurar el número deseado de logines 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 del WebVPN no pueden golpear los marcadores y son Grayed hacia fuera

Problema

¿Si estos marcadores fueron configurados para que a los usuarios ingresen al clientless VPN, pero en la pantalla de inicio bajo “aplicaciones de Web” aparecen como grayed hacia fuera, cómo puedo habilitar estos links HTTP de modo que los usuarios puedan hacerlos clic y entrar el URL determinado?

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 del Citrix con el WebVPN

Problema

Aparece el mensaje de error “ **the ica client received a corrupt icafile.**” ocurre para el Citrix sobre el 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 usted accede los links CIFS en el portal del WebVPN del clientless, le indican para las credenciales después de que usted haga clic el marcador. El Lightweight Directory Access Protocol (LDAP) se utiliza para autenticar los recursos y los usuarios han ingresado ya las credenciales del LDAP para iniciar sesión a la sesión de VPN.

Solución

Usted puede utilizar la característica del auto-anuncio del comienzo de las emisiones en este caso. Bajo grupo-directiva específica que es utilizada y bajo sus atributos del WebVPN, configure esto:

```
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 y del `*=restof` CIFS la `trayectoria para alcanzar el` archivo/la carpeta de la parte en la pregunta.

Un snippet del ejemplo de configuración se muestra aquí:

```
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 más información sobre esto, vea configurar el SSO con el HTTP básico o la autenticación NTLM.

Información Relacionada

- ASA: Túnel elegante usando el ejemplo de la Configuración de ASDM
- Soporte Técnico y Documentación - Cisco Systems