ASA: Ejemplo de Configuración de Túnel Inteligente con ASDM

Contenido

Introducción

Un túnel inteligente es una conexión entre una aplicación basada en TCP y un sitio privado, que utiliza una sesión SSL VPN sin cliente (basada en navegador) con el dispositivo de seguridad como ruta y el dispositivo de seguridad como servidor proxy. Puede identificar las aplicaciones a las que desea conceder acceso de túnel inteligente y especificar la ruta de acceso local a cada aplicación. Para las aplicaciones que se ejecutan en Microsoft Windows, también puede requerir una coincidencia del hash SHA-1 de la suma de comprobación como condición para conceder acceso de túnel inteligente.

Lotus SameTime y *Microsoft Outlook Express* son ejemplos de aplicaciones a las que quizá desee otorgar acceso de túnel inteligente.

En función de si la aplicación es un cliente o una aplicación habilitada para Web, la configuración de túnel inteligente requiere uno de estos procedimientos:

- Cree una o más listas de túnel inteligentes de las aplicaciones cliente y, a continuación, asigne la lista a las políticas de grupo o a las políticas de usuario locales para las que desea proporcionar acceso de túnel inteligente.

- Cree una o más entradas de lista de marcadores que especifiquen las URL de las aplicaciones habilitadas para Web que cumplen los requisitos para el acceso de túnel inteligente y, a continuación, asigne la lista a los DAP, las políticas de grupo o las políticas de usuario local para las que desea proporcionar acceso de túnel inteligente.También puede enumerar las aplicaciones habilitadas para Web para las cuales automatizar el envío de credenciales de inicio de sesión en conexiones de túnel inteligentes a través de sesiones VPN SSL sin cliente.

Este documento asume que la configuración de Cisco AnyConnect SSL VPN Client ya está hecha y funciona correctamente para que la función de túnel inteligente se pueda configurar en la configuración existente. Para obtener más información sobre cómo configurar Cisco AnyConnect SSL VPN client, refiérase a ASA 8.x: Ejemplo de configuración para permitir la tunelización dividida del cliente VPN de AnyConnect en ASA.

Nota: Asegúrese de que los pasos *4.b a 4.l* descritos en la sección Configuración de ASA con ASDM 6.0(2) de la sección *ASA 8.x : Allow Split Tunneling for AnyConnect VPN Client en el Ejemplo de Configuración de ASA* no se realiza para configurar la función de túnel inteligente.

Este documento describe cómo configurar el túnel inteligente en Cisco ASA 5500 Series Adaptive Security Appliances.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

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

- Cisco ASA 5500 Series Adaptive Security Appliances que ejecutan la versión de software 8.0(2)
- PC que ejecuta Microsoft Vista, Windows XP SP2 o Windows 2000 Professional SP4 con Microsoft Installer versión 3.1
- Cisco Adaptive Security Device Manager (ASDM) versión 6.0(2)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Antecedentes

Configuración de Smart Tunnel Access

La tabla de túnel inteligente muestra las listas de túnel inteligentes, cada una de las cuales identifica una o más aplicaciones que cumplen los requisitos para el acceso de túnel inteligente y su sistema operativo (OS) asociado. Dado que cada política de grupo o política de usuario local admite una lista de túnel inteligente, debe agrupar las aplicaciones no basadas en explorador para que se admitan en una lista de túnel inteligente. Después de configurar una lista, puede asignarla a una o varias políticas de grupo o políticas de usuario locales.

La ventana de túneles inteligentes (**Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Túneles inteligentes**) le permite completar estos procedimientos:

- **Agregar una lista de túnel inteligente y agregar aplicaciones a la lista**Complete estos pasos para agregar una lista de túnel inteligente y agregar aplicaciones a la lista:Haga clic en Add (Agregar).Aparecerá el cuadro de diálogo Agregar lista de túnel inteligente.Ingrese un nombre para la lista, y haga clic en AddASDM abre el cuadro de diálogo Agregar entrada de túnel inteligente, que le permite asignar los atributos de un túnel inteligente a la lista.Después de asignar los atributos deseados para el túnel inteligente, haga clic en **Aceptar**.ASDM muestra esos atributos en la lista.Repita estos pasos según sea necesario para completar la lista y, a continuación, haga clic en **Aceptar** en el cuadro de diálogo Agregar lista de túnel inteligente.
- **Cambio de una Lista de Túnel Inteligente**Complete estos pasos para cambiar una lista de túnel inteligente:Haga doble clic en la lista o elija la lista en la tabla y haga clic en **Editar**.Haga clic en **Agregar** para insertar un nuevo conjunto de atributos de túnel inteligentes en la lista o elija una entrada en la lista, y haga clic en **Editar** o **Eliminar**.
- **Eliminar una lista**Para quitar una lista, elija la lista en la tabla y haga clic en **Eliminar**.
- **Agregar un marcador**Después de configurar y asignar una lista de túnel inteligente, puede hacer que un túnel inteligente sea fácil de usar agregando un marcador para el servicio y haciendo clic en la opción **Habilitar túnel inteligente** en el cuadro de diálogo Agregar o editar marcador.

El acceso de túnel inteligente permite a una aplicación cliente basada en TCP utilizar una conexión VPN basada en explorador para conectarse a un servicio. Ofrece a los usuarios las siguientes ventajas, en comparación con los complementos y la tecnología antigua, el reenvío de puertos:

- El túnel inteligente ofrece un mejor rendimiento que los complementos.
- A diferencia del reenvío de puertos, el túnel inteligente simplifica la experiencia del usuario ya que no requiere la conexión del usuario de la aplicación local al puerto local.
- A diferencia del reenvío de puertos, el túnel inteligente no requiere que los usuarios tengan privilegios de administrador.

Requisitos, restricciones y limitaciones del túnel inteligente

Requisitos y limitaciones generales

El túnel inteligente tiene los siguientes requisitos y limitaciones generales:

- El host remoto que origina el túnel inteligente debe ejecutar una versión de 32 bits de Microsoft Windows Vista, Windows XP o Windows 2000; o Mac OS 10.4 o 10.5.
- El inicio de sesión automático de túnel inteligente sólo admite Microsoft Internet Explorer en Windows.

- El explorador debe estar habilitado con Java, Microsoft ActiveX o ambos.
- El túnel inteligente sólo admite proxies ubicados entre equipos que ejecutan Microsoft Windows y el dispositivo de seguridad. El túnel inteligente utiliza la configuración de Internet Explorer (es decir, la que se utiliza en todo el sistema en Windows). Si el equipo remoto requiere un servidor proxy para alcanzar el dispositivo de seguridad, la URL del extremo de terminación de la conexión debe estar en la lista de URL excluidas de los servicios proxy. Si la configuración de proxy especifica que el tráfico destinado al ASA pasa a través de un proxy, todo el tráfico de túnel inteligente pasa a través del proxy.En un escenario de acceso remoto basado en HTTP, a veces una subred no proporciona acceso de usuario al gateway VPN. En este caso, un proxy ubicado frente al ASA para rutear el tráfico entre la Web y la ubicación del usuario final proporciona acceso web. Sin embargo, sólo los usuarios de VPN pueden configurar los proxies ubicados frente al ASA. Al hacerlo, deben asegurarse de que estos proxies admiten el método CONNECT. Para los proxies que requieren autenticación, el túnel inteligente sólo admite el tipo de autenticación básica de resumen.
- Cuando se inicia el túnel inteligente, el dispositivo de seguridad tuneliza todo el tráfico desde el explorador, proceso que el usuario utilizó para iniciar la sesión sin cliente. Si el usuario inicia otra instancia del proceso del explorador, pasa todo el tráfico al túnel. Si el proceso del explorador es el mismo y el dispositivo de seguridad no proporciona acceso a una dirección URL determinada, el usuario no puede abrirla. Como solución temporal, el usuario puede utilizar un explorador diferente del utilizado para establecer la sesión sin cliente.
- Un stateful failover no conserva las conexiones de túnel inteligentes. Los usuarios deben volver a conectarse después de un failover.

Requisitos y limitaciones de Windows

Los siguientes requisitos y limitaciones se aplican únicamente a Windows:

- Solo las aplicaciones basadas en TCP de Winsock 2 pueden optar al acceso de túnel inteligente.
- El dispositivo de seguridad no admite el proxy Microsoft Outlook Exchange (MAPI). Ni el reenvío de puertos ni el túnel inteligente admiten MAPI. Para la comunicación de Microsoft Outlook Exchange mediante el protocolo MAPI, los usuarios remotos deben utilizar AnyConnect.
- Los usuarios de Microsoft Windows Vista que utilizan el túnel inteligente o el reenvío de puertos deben agregar la dirección URL del ASA a la zona Sitio de confianza. Para acceder a la zona Sitio de confianza, inicie Internet Explorer, elija **Herramientas > Opciones de Internet** y haga clic en la **ficha Seguridad**. Los usuarios de Vista también pueden inhabilitar el modo protegido para facilitar el acceso de túnel inteligente; sin embargo, Cisco recomienda no usar este método porque aumenta la vulnerabilidad al ataque.

Requisitos y limitaciones de Mac OS

Estos requisitos y limitaciones se aplican únicamente al sistema operativo Mac:

- Safari 3.1.1 o posterior o Firefox 3.0 o posterior
- Sun JRE 1.5 o posterior
- Sólo las aplicaciones iniciadas desde la página del portal pueden establecer conexiones de túnel inteligentes. Este requisito incluye la compatibilidad de túnel inteligente para Firefox. El

uso de Firefox para iniciar otra instancia de Firefox durante el primer uso de un túnel inteligente requiere el perfil de usuario denominado csco_st. Si este perfil de usuario no está presente, la sesión solicita al usuario que cree uno.
- Las aplicaciones que utilizan TCP enlazadas dinámicamente a la biblioteca SSL pueden funcionar en un túnel inteligente.
- Smart Tunnel no admite estas funciones y aplicaciones en Mac OS:Servicios de proxyInicio de sesión automáticoAplicaciones que utilizan espacios de nombres de dos nivelesAplicaciones basadas en consola, como Telnet, SSH y cURLAplicaciones que utilizan dlopen o dlsym para localizar llamadas de libsocketAplicaciones enlazadas estáticamente para localizar llamadas de libsocket

Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Agregar o editar lista de túnel inteligente

El cuadro de diálogo Agregar lista de túnel inteligente permite agregar una lista de entradas de túnel inteligentes a la configuración del dispositivo de seguridad. El cuadro de diálogo Editar lista de túnel inteligente permite modificar el contenido de la lista.

Campo

Nombre de lista: introduzca un nombre único para la lista de aplicaciones o programas. No hay restricción en el número de caracteres del nombre. No utilice espacios. Después de la configuración de la lista de túnel inteligente, el nombre de la lista aparece junto al atributo Smart Tunnel List en las políticas de grupo SSL VPN sin cliente y las políticas de usuario local. Asigne un nombre que le ayude a distinguir su contenido o propósito de otras listas que probablemente configure.

Agregar o editar entrada de túnel inteligente

El cuadro de diálogo Agregar o editar entrada de túnel inteligente permite especificar los atributos de una aplicación en una lista de túnel inteligente.

- **Application ID**: introduzca una cadena para asignar un nombre a la entrada de la lista de túnel inteligente. La cadena es única para el SO. Normalmente, nombra la aplicación a la que se concederá acceso de túnel inteligente. Para soportar varias versiones de una aplicación para la que se elige especificar diferentes trayectos o valores hash, se puede utilizar este atributo para diferenciar entradas, especificando el SO y el nombre y la versión de la aplicación soportada por cada entrada de lista. La cadena puede tener hasta 64 caracteres.
- **Nombre de proceso**: introduzca el nombre de archivo o la ruta de acceso a la aplicación. La cadena puede tener hasta 128 caracteresWindows requiere una coincidencia exacta de este valor en el lado derecho de la ruta de la aplicación en el host remoto para calificar la aplicación para el acceso de túnel inteligente. Si especifica solamente el nombre de archivo para Windows, SSL VPN no impone una restricción de ubicación en el host remoto para calificar la aplicación para el acceso de túnel inteligente.Si especifica una ruta de acceso y el

usuario instaló la aplicación en otra ubicación, esa aplicación no cumple los requisitos. La aplicación puede residir en cualquier ruta siempre y cuando el lado derecho de la cadena coincida con el valor que introduzca.Para autorizar una aplicación para el acceso de túnel inteligente si está presente en una de las varias trayectorias en el host remoto, especifique solamente el nombre y la extensión de la aplicación en este campo o cree una entrada de túnel inteligente única para cada trayectoria.Para Windows, si desea agregar acceso de túnel inteligente a una aplicación iniciada desde el símbolo del sistema, debe especificar "cmd.exe" en el nombre de proceso de una entrada de la lista de túnel inteligente y especificar la ruta de acceso a la propia aplicación en otra entrada porque "cmd.exe" es el padre de la aplicación.Mac OS requiere la ruta completa al proceso y distingue entre mayúsculas y minúsculas. Para evitar especificar una ruta de acceso para cada nombre de usuario, inserte una tilde (~) antes de la ruta parcial (por ejemplo, ~/bin/vnc).

- **OS**: haga clic en Windows o Mac para especificar el SO host de la aplicación.
- **Hash** —(*Opcional y aplicable sólo para Windows*) Para obtener este valor, ingrese la suma de comprobación del archivo ejecutable en una utilidad que calcula un hash usando el algoritmo SHA-1. Un ejemplo de tal utilidad es el Comprobador de integridad de la suma de comprobación de archivos (FCIV) de Microsoft, que está disponible en Disponibilidad y descripción de la utilidad Verificador de integridad de la suma de comprobación de archivos. Después de instalar FCIV, coloque una copia temporal de la aplicación que se va a fragmentar en una ruta de acceso que no contiene espacios (por ejemplo, c:/fciv.exe) y, a continuación, introduzca la aplicación fciv.exe -sha1 en la línea de comandos (por ejemplo, fciv.exe -sha1 c:\msimn.exe) para mostrar el hash SHA-1.El hash SHA-1 siempre tiene 40 caracteres hexadecimales.Antes de autorizar una aplicación para el acceso de túnel inteligente, la SSL VPN sin cliente calcula el hash de la aplicación que coincide con el ID de la aplicación. Califica la aplicación para el acceso de túnel inteligente si el resultado coincide con el valor de hash.Al ingresar un hash, se garantiza razonablemente que SSL VPN no califica un archivo ilegítimo que coincida con la cadena especificada en el ID de aplicación. Debido a que la suma de comprobación varía con cada versión o parche de una aplicación, el hash que introduzca sólo puede coincidir con una versión o parche en el host remoto. Para especificar un hash para más de una versión de una aplicación, cree una entrada de túnel inteligente única para cada valor hash.**Nota:** Debe actualizar la lista de túnel inteligente en el futuro si introduce valores hash y desea admitir versiones o revisiones futuras de una aplicación con acceso de túnel inteligente. Un problema repentino con el acceso de túnel inteligente puede ser una indicación de que la aplicación que contiene valores hash no está actualizada con una actualización de la aplicación. Puede evitar este problema no introduciendo un hash.
- Una vez configurada la lista de túnel inteligente, debe asignarla a una política de grupo o a una política de usuario local para que se active de la siguiente manera:Para asignar la lista a una política de grupo, elija **Config > Remote Access VPN> Clientless SSL VPN Access > Group Policies > Add o Edit > Portal**, y elija el nombre de túnel inteligente de la lista desplegable junto al atributo Smart Tunnel List.Para asignar la lista a una política de usuario local, elija **Config > Remote Access VPN> AAA Setup > Local Users > Add o Edit > VPN Policy > Clientless SSL VPN**, y elija el nombre del túnel inteligente de la lista desplegable junto al atributo Smart Tunnel List.

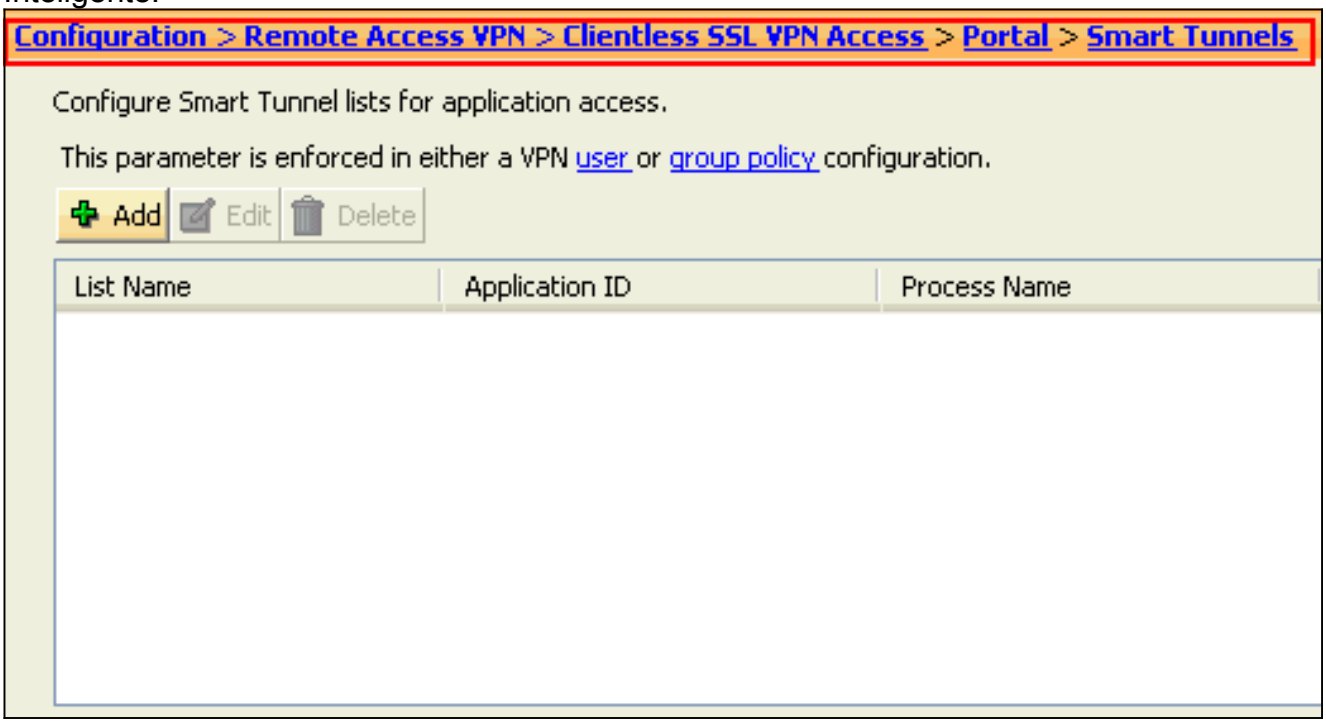
Configuración del túnel inteligente de ASA (ejemplo de Lotus) mediante ASDM 6.0(2)

Este documento asume que la configuración básica, como la configuración de la interfaz, está completa y funciona correctamente.

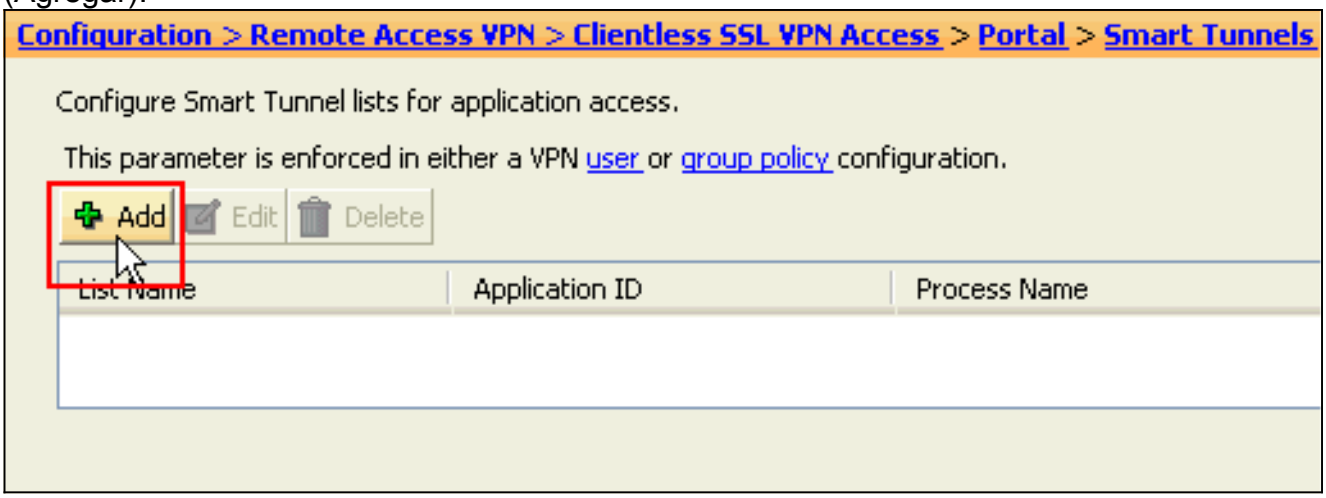
Complete estos pasos para configurar un túnel inteligente:

Nota: En este ejemplo de configuración, el túnel inteligente se configura para la aplicación Lotus.

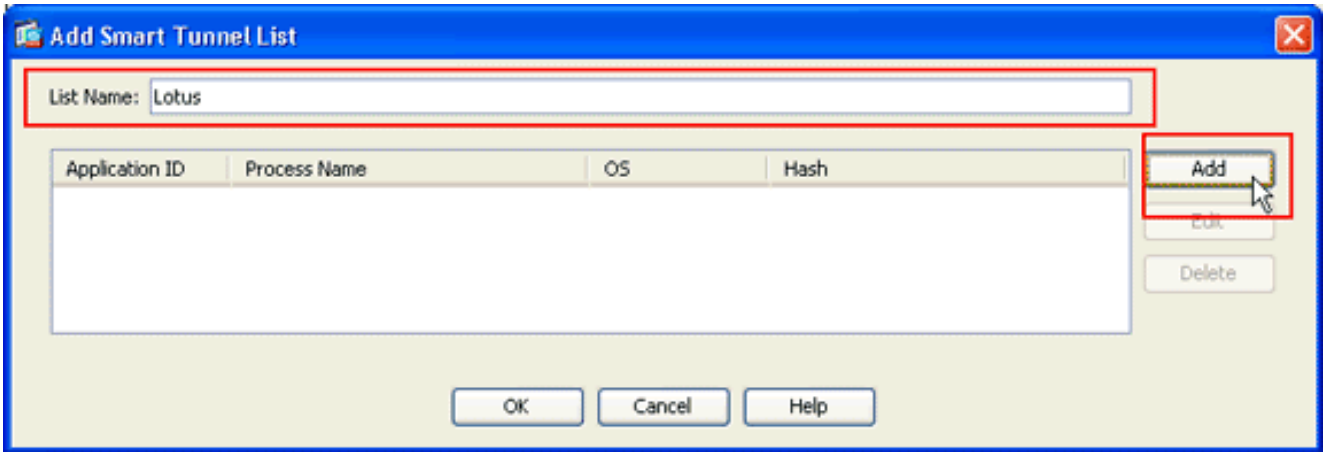
1. Elija **Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Túneles Inteligentes** para iniciar la configuración del Túnel Inteligente.



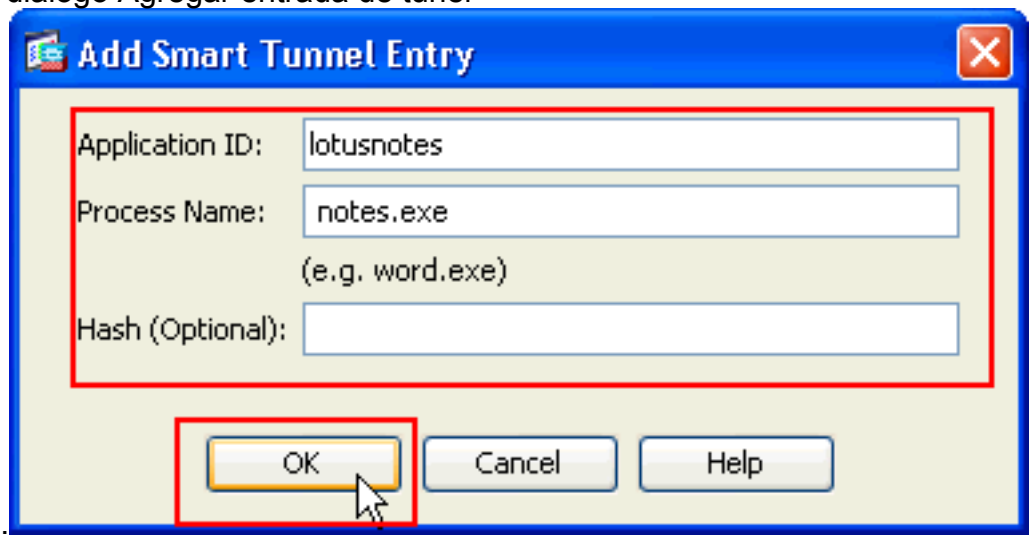
2. Haga clic en Add (Agregar).



Aparecerá el cuadro de diálogo Agregar lista de túnel inteligente.

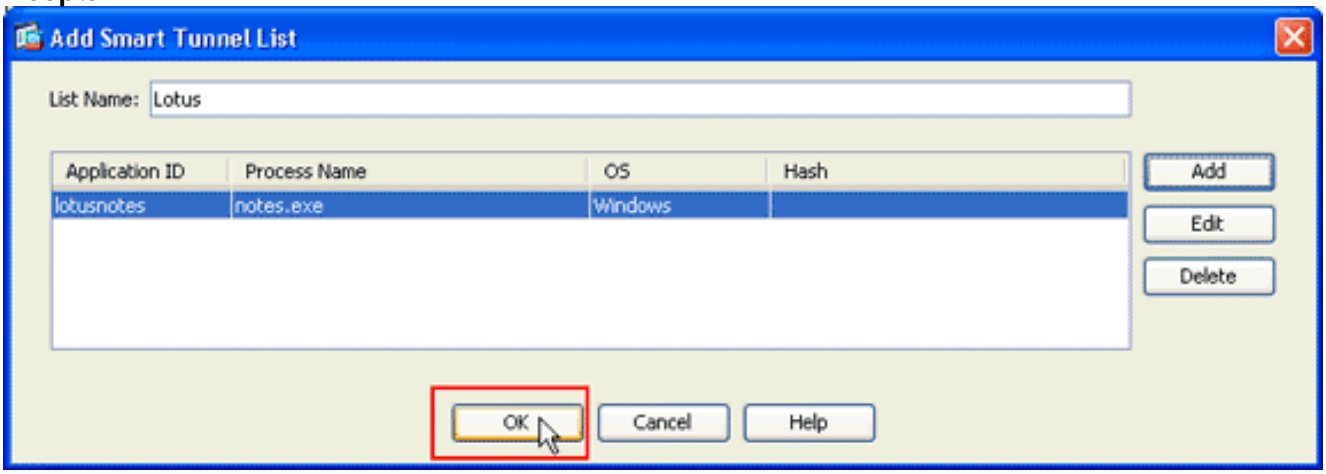


3. En el cuadro de diálogo Agregar lista de túnel inteligente, haga clic en **Agregar**.Aparecerá el cuadro de diálogo Agregar entrada de túnel



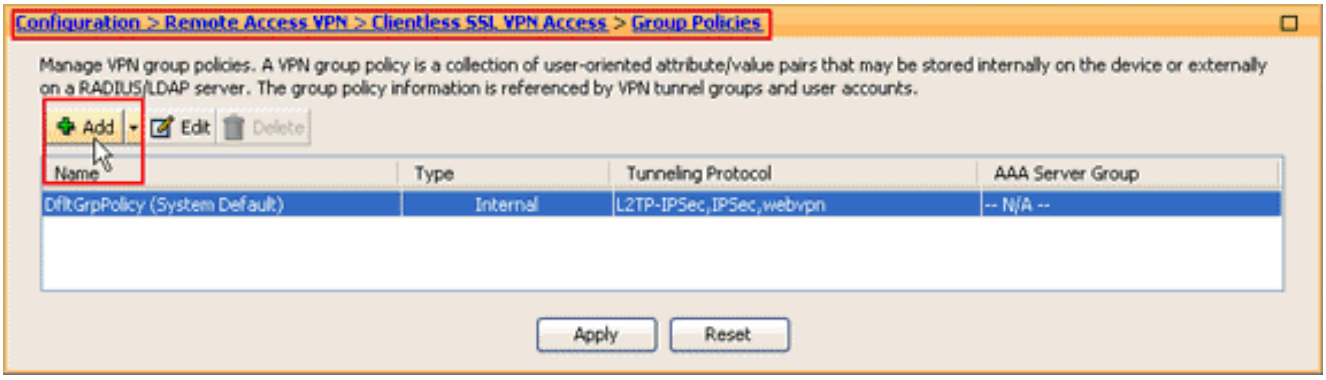
inteligente.

4. En el campo Application ID (ID de aplicación), introduzca una cadena para identificar la entrada dentro de la lista de túnel inteligente.
5. Introduzca un nombre de archivo y una extensión para la aplicación y haga clic en **Aceptar**.
6. En el cuadro de diálogo Agregar lista de túnel inteligente, haga clic en **Aceptar**.

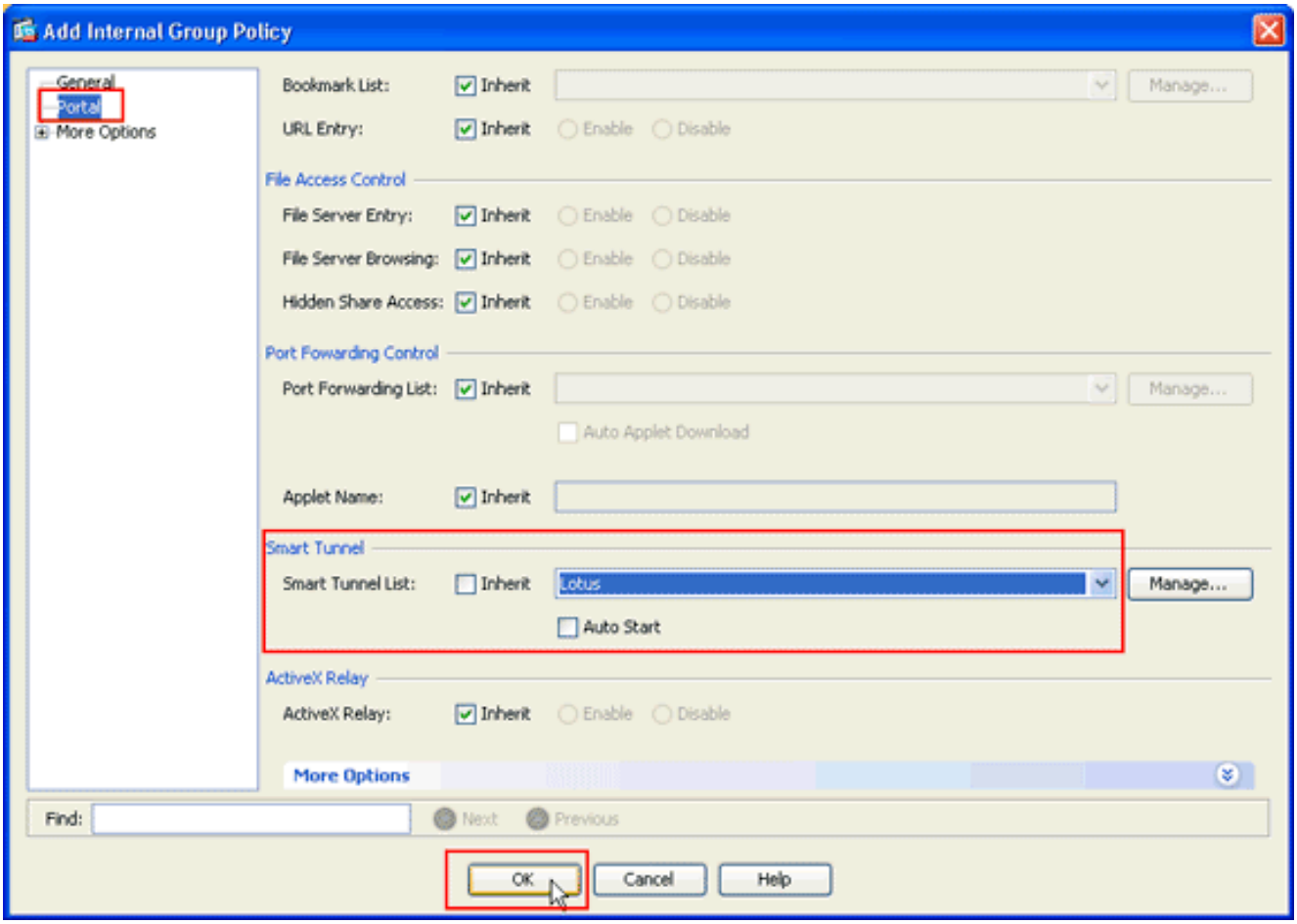


Nota: Este es el comando de configuración CLI equivalente:

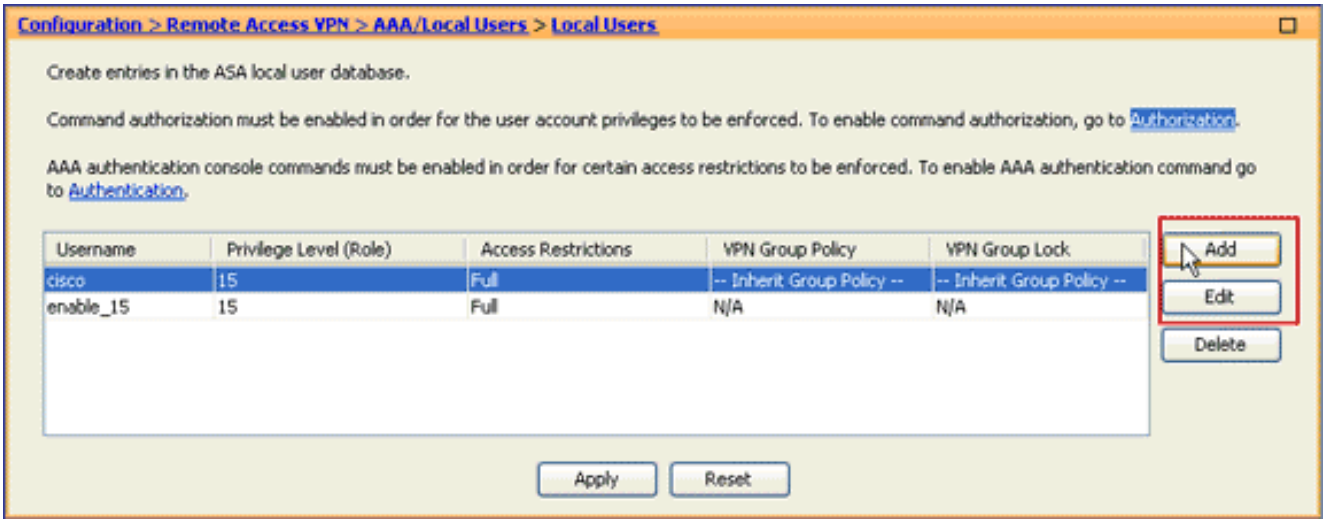
7. Asigne la lista a las políticas de grupo y a las políticas de usuario locales a las que desea proporcionar acceso de túnel inteligente a las aplicaciones asociadas de la siguiente manera:Para asignar la lista a una política de grupo, elija **Configuration > Remote Access VPN> Clientless SSL VPN Access > Group Policies**, y haga clic en **Add** o **Edit.**



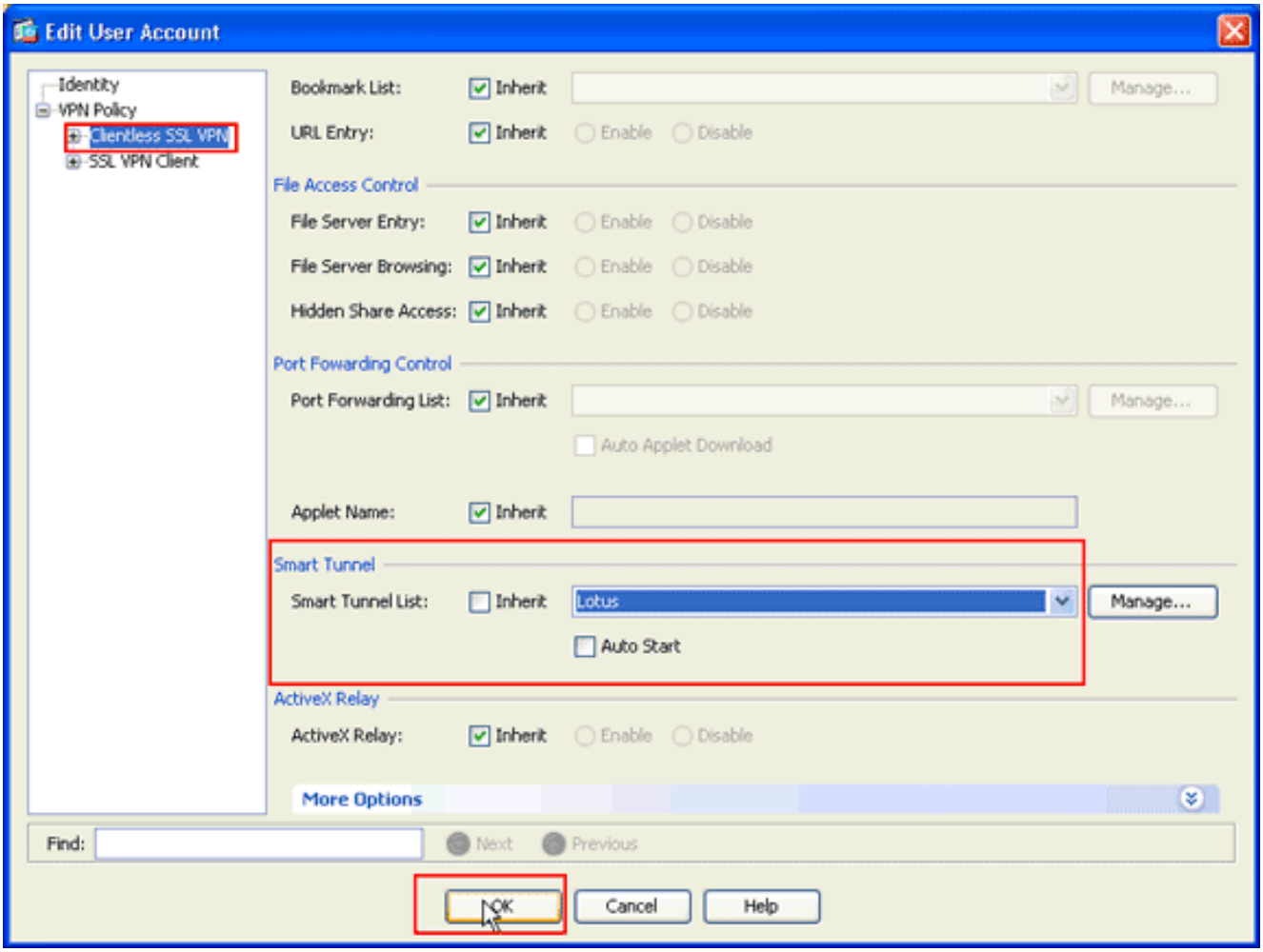
Aparecerá el cuadro de diálogo Agregar directiva de grupo interna.



8. En el cuadro de diálogo Agregar política de grupo interna, haga clic en **Portal**, elija el nombre de túnel inteligente en la lista desplegable Lista de túnel inteligente y haga clic en **Aceptar**.**Nota:** En este ejemplo se utiliza *Lotus* como nombre de lista de túnel inteligente.
9. Para asignar la lista a una política de usuario local, elija **Configuration > Remote Access VPN> AAA Setup > Local Users**, y haga clic en **Add** para configurar un usuario nuevo o haga clic en **Edit** para editar un usuario existente.



Aparecerá el cuadro de diálogo Editar cuenta de usuario.



10. En el cuadro de diálogo Edit User Account (Editar cuenta de usuario), haga clic en **Clientless SSL VPN**, elija el nombre del túnel inteligente de la lista desplegable Smart Tunnel List y haga clic en **OK**.**Nota:** En este ejemplo se utiliza *Lotus* como nombre de lista de túnel inteligente.

La configuración del túnel inteligente ha finalizado.

Troubleshoot

No puedo conectarme mediante una URL de túnel inteligente guardada como

favoritos en el portal sin cliente. ¿Por qué ocurre este problema y cómo puedo resolverlo?

Este problema ocurre debido al problema descrito en Cisco Bug ID CSCsx05766 (sólo clientes registrados) . Para resolver este problema, vuelva a actualizar el complemento Java Runtime a una versión anterior.

¿Puedo ajustar la URL de un enlace de túnel inteligente configurado en WebVPN?

Cuando se utiliza un túnel inteligente en el ASA, no puede ajustar la dirección URL ni ocultar la barra de direcciones del explorador. Los usuarios pueden ver las URL de los enlaces configurados en WebVPN que utilizan túnel inteligente. Como resultado, pueden cambiar el puerto y acceder al servidor para algún otro servicio.

Para resolver este problema, utilice las ACL de WebType. Consulte Listas de Control de Acceso WebType para obtener más información.

Información Relacionada

- Cisco ASA 5500 Series Adaptive Security Appliances
- Ejemplo de Configuración de SSL VPN Client (SVC) en ASA con ASDM
- Soporte Técnico y Documentación - Cisco Systems