ASA: Túnel elegante usando el ejemplo de la Configuración de ASDM

Contenido

Introducción

Un túnel elegante es una conexión entre una aplicación TCP basada y un sitio privado, usando una sesión de VPN del clientless SSL (basado en buscador) con el dispositivo de seguridad como el camino y el dispositivo de seguridad como servidor proxy. Usted puede identificar las aplicaciones a las cuales usted quiere conceder el acceso elegante del túnel y especificar el trayecto local a cada aplicación. Para las aplicaciones que se ejecutan en Microsoft Windows, usted puede también requerir una coincidencia del hash SHA-1 de la suma de comprobación como condición para conceder el acceso elegante del túnel.

Lotus SameTime y *Microsoft Outlook Express* son ejemplos de las aplicaciones a las cuales usted puede ser que quiera conceder el acceso elegante del túnel.

El dependiente encendido si la aplicación es un cliente o es una aplicación red-habilitada, configuración del túnel elegante requiere uno de estos procedimientos:

- Cree una o más listas elegantes del túnel de las aplicaciones de cliente, y después asigne la

lista a las directivas del grupo o a las directivas del usuario local para las cuales usted quiere proporcionar el acceso elegante del túnel.
- Cree una o más entradas de la lista del marcador que especifiquen los URL de las aplicaciones red-habilitadas elegibles para el acceso elegante del túnel, y entonces asignan la lista a los DAP, las directivas del grupo, o las directivas del usuario local para las cuales usted quiere proporcionar el acceso elegante del túnel.Usted puede también enumerar las aplicaciones red-habilitadas para que automaticen la presentación de las credenciales del login en las conexiones del túnel elegantes sobre las sesiones de VPN del clientless SSL.

Este documento asume que la configuración de cliente VPN de Cisco AnyConnect SSL está hecha ya y trabaja correctamente para poder configurar la característica elegante del túnel en la configuración existente. Para más información sobre cómo configurar al cliente VPN de Cisco AnyConnect SSL, refiera a ASA 8.x: Permita el Túnel dividido para el cliente VPN de AnyConnect en el ejemplo de configuración ASA.

Refiera a configurar una directiva elegante del túnel del túnel para más información sobre cómo configurar el Túnel dividido junto con el túnel elegante.

Nota: Aseegurese que los pasos *4.b a 4.l* describieron en la configuración ASA usando la sección del ASDM 6.0(2) del *ASA 8.x: Permita el Túnel dividido para el cliente VPN de AnyConnect en el ejemplo de configuración ASA* no se realiza para configurar la característica elegante del túnel.

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

prerrequisitos

Requisitos

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.

- Dispositivos de seguridad adaptable Cisco ASA de la serie 5500 que funciona con la versión de software 8.0(2)
- PC que ejecuta Microsoft Vista, Windows XP SP2, o Windows 2000 Professional SP4 con la versión 3.1 del Instalador Microsoft
- Cisco Adaptive Security Device Manager (ASDM) versión 6.0(2)

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

Convenciones

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

Antecedentes

Configuración elegante del acceso del túnel

La tabla elegante del túnel visualiza las listas elegantes del túnel, que identifica una o más aplicaciones elegibles para el acceso elegante del túnel y su operating system (OS) asociado. Porque cada directiva del grupo o las admite una políticas del usuario local una lista elegante del túnel, usted debe agrupar las aplicaciones nonbrowser-basadas que se soportarán en una lista elegante del túnel. Después de la configuración de una lista, usted puede asignarla a uno o más grupo limpia o a las directivas del usuario local.

Nota: Para más información sobre la configuración del túnel elegante, refiera a configurar el acceso elegante del túnel.

La ventana elegante de los túneles (**configuración > VPN de acceso remoto > acceso > portal del clientless SSL VPN > los túneles elegantes**) permite que usted complete estos procedimientos:

- **Agregue una lista elegante del túnel y agregue las aplicaciones a la lista**Complete estos pasos para agregar una lista elegante del túnel y agregar las aplicaciones a la lista:Haga clic en Add (Agregar).El cuadro de diálogo elegante de la lista del túnel del agregar aparece.Ingrese un nombre para la lista, y haga clic en AddEl ASDM abre el cuadro elegante del cuadro de diálogo de entrada del túnel del agregar, que permite que usted asigne los atributos de un túnel elegante a la lista.Después de que usted asigne los atributos deseados para el túnel elegante, haga clic la **AUTORIZACIÓN**.El ASDM visualiza esos atributos en la lista.Relance estos pasos cuanto sea necesario para completar la lista, y después haga clic la **AUTORIZACIÓN** en el cuadro de diálogo elegante de la lista del túnel del agregar.
- **Cambie una lista elegante del túnel**Complete estos pasos para cambiar una lista elegante del túnel:Haga doble clic la lista o elija la lista en la tabla, y el tecleo **edita**.Haga clic **agregan** para insertar un nuevo conjunto de los atributos del túnel elegantes en la lista o para elegir una entrada en la lista, y el tecleo **edita** o **borra**.
- **Quite una lista**Para quitar una lista, elegir la lista en la tabla, y hacer clic la **cancelación**.
- **Agregue un marcador**Después de la configuración y de la asignación de una lista elegante del túnel, usted puede hacer un túnel elegante fácil de utilizar agregando un marcador para el servicio y haciendo clic la opción **elegante del túnel del permiso** en el agregar o editar el cuadro de diálogo del marcador.

El acceso elegante del túnel permite que a cliente la aplicación TCP basada utilice una conexión VPN basada en buscador para conectar con un servicio. Ofrece las ventajas siguientes a los usuarios, comparados a los plug-in y a la tecnología de la herencia, expedición del puerto:

- El túnel elegante ofrece el mejor rendimiento que los enchufes.
- A diferencia de la expedición del puerto, el túnel elegante simplifica al usuario que la experiencia por no requiere la conexión del usuario de la aplicación local al puerto local.
- A diferencia de la expedición del puerto, el túnel elegante no requiere a los usuarios tener privilegios de administrador.

Requisitos, restricciones, y limitaciones elegantes del túnel

Requerimientos generales y limitaciones

El túnel elegante tiene los requerimientos generales y las limitaciones siguientes:

- El host remoto que origina el túnel elegante debe funcionar con una versión de 32 bits de Microsoft Windows Vista, de Windows XP, o del Windows 2000; o Mac OS 10.4 o 10.5.
- Auto elegante del túnel muestra-en los soportes solamente Microsoft Internet Explorer en Windows.
- El navegador debe ser habilitado con las Javas, Microsoft ActiveX, o ambos.
- El túnel elegante soporta solamente los proxys puestos entre los ordenadores que funcionan con Microsoft Windows y el dispositivo de seguridad. El túnel elegante utiliza la configuración del Internet Explorer (es decir, la que está prevista para el uso sistema-ancho en Windows). Si la computadora remota requiere un servidor proxy alcanzar el dispositivo de seguridad, el URL del extremo terminal de la conexión debe estar en la lista de URL excluidos de los servicios de representación. Si la configuración de representación especifica que el tráfico destinado para el ASA pasa con un proxy, todo el tráfico de túnel elegante pasa con el proxy.En un escenario basado en HTTP del Acceso Remoto, una subred no proporciona a veces el acceso del usuario al gateway de VPN. En este caso, un proxy colocado delante del ASA para rutear el tráfico entre la red y la ubicación del usuario final proporciona el Acceso Web. Sin embargo, solamente los usuarios de VPN pueden configurar los proxys puestos delante del ASA. Al hacer así pues, deben aseegurarse soporte de estos proxys el método de la CONEXIÓN. Para los proxys que requieren la autenticación, el túnel elegante apoya solamente el tipo del asimilar autenticación básico.
- Cuando el túnel elegante comienza, el dispositivo de seguridad hace un túnel todo el tráfico del proceso del navegador el usuario usado para iniciar la sesión del clientless. Si el usuario comienza otro caso del proceso del navegador, pasa todo el tráfico al túnel. Si el proceso del navegador es lo mismo y el dispositivo de seguridad no proporciona el acceso a un URL dado, el usuario no puede abrirlo. Como solución alternativa, el usuario puede utilizar a un diverso navegador del que está usado para establecer la sesión del clientless.
- Una falla de estado no conserva las conexiones del túnel elegantes. Los usuarios deben volver a conectar después de una Conmutación por falla.

Requisitos y limitaciones de Windows

Los requisitos y las limitaciones siguientes se aplican a Windows solamente:

- Solamente el Winsock 2, las aplicaciones TCP basadas es elegible para el acceso elegante del túnel.
- El dispositivo de seguridad no soporta el proxy del intercambio del Microsoft Outlook (MAPI). Ni vire la expedición hacia el lado de babor ni el túnel elegante soporta el MAPI. Para la comunicación del intercambio del Microsoft Outlook usando el protocolo MAPI, los usuarios remotos deben utilizar AnyConnect.
- Los usuarios de Microsoft Windows Vista que utilizan la expedición elegante del túnel o del puerto deben agregar el URL del ASA a la zona del sitio confiable. Para acceder la zona del sitio confiable, comience al Internet Explorer, y elija las **herramientas > las opciones de Internet**, y haga clic a los usuarios de cuadro Vista de la **Seguridad** puede también inhabilitar el modo protegido para facilitar el acceso elegante del túnel; sin embargo, Cisco recomienda contra este método porque aumenta la vulnerabilidad para atacar.

Requisitos y limitaciones del Mac OS

Estos requisitos y limitaciones se aplican al Mac OS solamente:

- Safari 3.1.1 o 3.0 posterior o de Firefox o más adelante
- Sun JRE 1.5 o más adelante
- Solamente las aplicaciones comenzadas de la página porta pueden establecer las conexiones del túnel elegantes. Este requisito incluye el soporte elegante del túnel para Firefox. Usando Firefox comenzar otro caso de Firefox durante el primer uso de un túnel elegante requiere el perfil del usuario nombrado csco_st. Si este perfil del usuario no está presente, la sesión indica al usuario que cree uno.
- Las aplicaciones usando el TCP que se conectan dinámicamente a la biblioteca SSL pueden trabajar sobre un túnel elegante.
- El túnel elegante no soporta estas características y aplicaciones en el Mac OS:Servicios de representaciónAuto muestra-enAplicaciones que utilizan los espacios para nombre de dos nivelesaplicaciones Consola-basadas, tales como Telnet, SSH, y rizoLas aplicaciones usando dlopen o dlsym para localizar las llamadas del libsocketAplicaciones estáticamente conectadas para localizar las llamadas del libsocket

Configurar

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

Nota: Utilice la herramienta Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos utilizados en esta sección.

Agregue o edite la lista elegante del túnel

El cuadro de diálogo elegante de la lista del túnel del agregar le deja agregar una lista de entradas elegantes del túnel a la configuración del dispositivo de seguridad. El cuadro de diálogo elegante de la lista del túnel del editar le deja modificar el contenido de la lista.

Campo

Nombre de la lista — Ingrese un nombre único para la lista de aplicaciones o los programas. No hay restricción en el número de caracteres en el nombre. No utilice los espacios. Después de la configuración de la lista elegante del túnel, el nombre de la lista aparece al lado del List Attribute elegante del túnel en las directivas del grupo VPN del clientless SSL y las directivas del usuario local. Asigne un nombre que le ayude a distinguir su contenido o propósito de otras listas que usted es probable configurar.

Agregue o edite la entrada elegante del túnel

El agregar o edita el cuadro elegante del cuadro de diálogo de entrada del túnel le deja especificar los atributos de una aplicación en una lista elegante del túnel.

- **ID de la aplicación** — Ingrese una cadena para nombrar la entrada en la lista elegante del túnel. La cadena es única para el OS. Típicamente, nombra la aplicación para ser concedida el acceso elegante del túnel. Para soportar las versiones múltiples de una aplicación para la cual usted elija especificar diversas trayectorias o los valores de troceo, usted puede utilizar

este atributo para distinguir las entradas, especificando el OS y el nombre y la versión de la aplicación soportada por cada entrada de la lista. La cadena puede ser hasta 64 caracteres.

- **Nombre del proceso** — Ingrese el nombre del archivo o la trayectoria a la aplicación. La cadena puede estar hasta los caracteres 128Windows requiere un exacto - coincidencia de este valor al lado derecho del trayecto de aplicación en el host remoto para calificar la aplicación para el acceso elegante del túnel. Si usted especifica solamente el nombre del archivo para Windows, el SSL VPN no aplica una restricción de la ubicación en el host remoto para calificar la aplicación para el acceso elegante del túnel.Si usted especifica una trayectoria y el usuario instaló la aplicación en otra ubicación, esa aplicación no califica. La aplicación puede residir en cualquier trayectoria mientras el lado derecho de las correspondencias de cadenas el valor que usted ingresa.Para autorizar una aplicación para el acceso elegante del túnel si está presente en una de varias trayectorias en el host remoto, o especifique solamente el nombre y la extensión de la aplicación en este campo o cree una entrada elegante única del túnel para cada trayectoria.Para Windows, si usted quiere agregar el acceso elegante del túnel a una aplicación comenzado del comando prompt, usted debe especificar “cmd.exe” en el nombre del proceso de una entrada en la lista elegante del túnel y especificar la trayectoria a la aplicación sí mismo en otra entrada porque “cmd.exe” es el padre de la aplicación.El Mac OS requiere la ruta completa al proceso y es con diferenciación entre mayúsculas y minúsculas. Para evitar especificar una trayectoria para cada Nombre de usuario, inserte una tilde (~) antes de la trayectoria parcial (por ejemplo, ~/bin/vnc).
- **OS** — Haga clic Windows o el mac para especificar el host OS de la aplicación.
- **Hash** — (*opcional y aplicable solamente para Windows*) para obtener este valor, ingrese la suma de comprobación del archivo ejecutable en una utilidad que calcule un hash usando el algoritmo SHA-1. Un ejemplo de tal utilidad es el verificador de la integridad de la suma de comprobación del archivo de Microsoft (FCIV), que está disponible en http://support.microsoft.com/kb/841290/ . Después de instalar FCIV, ponga una copia temporaria de la aplicación que se desmenuzará en una trayectoria que no contenga ningún espacio (por ejemplo, c: /fciv.exe), entonces ingresan la aplicación fciv.exe -sha1 en la línea de comando (por ejemplo, fciv.exe -sha1 c:\msimn.exe) para visualizar el hash SHA-1.El hash SHA-1 es siempre 40 caracteres hexadecimales.Antes de autorizar una aplicación para el acceso elegante del túnel, el clientless SSL VPN calcula el hash de la aplicación que corresponde con el ID de la aplicación. Califica la aplicación para el acceso elegante del túnel si el resultado hace juego el valor del hash.Ingresar un hash ofrece una garantía razonable que el SSL VPN no califica un archivo ilegítimo que corresponda con la cadena que usted especificó en el ID de la aplicación. Porque la suma de comprobación varía con cada versión o corrección de una aplicación, el hash que usted ingresa puede corresponder con solamente una versión o corrección en el host remoto. Para especificar un hash para más de una versión de una aplicación, cree una entrada elegante única del túnel por cada valor de troceo.**Nota:** Usted debe poner al día la lista elegante del túnel en el futuro si usted ingresa los valores de troceo y usted quiere soportar las versiones futuras o las correcciones de una aplicación con el acceso elegante del túnel. Un problema súbito con el acceso elegante del túnel pudo ser una indicación que la aplicación que contiene los valores de troceo no es actualizada con una actualización de aplicación. Usted puede evitar este problema no ingresando un hash.
- Una vez que usted configura la lista elegante del túnel, usted debe asignarla a una directiva del grupo o a una directiva del usuario local para que haga activo como sigue:Para asignar la lista a una directiva del grupo, elegir los **Config > las directivas del acceso > del grupo del clientless SSL VPN del Acceso Remoto VPN> > Add o editarlos > portal**, y elegir el nombre

de túnel elegante de la lista desplegable al lado del List Attribute elegante del túnel.Para asignar la lista a una directiva del usuario local, elegir los **Config > el Acceso Remoto VPN> AAA puestos > usuarios locales > Add o editarlos > política del VPN > clientless SSL VPN**, y elegir el nombre de túnel elegante de la lista desplegable al lado del List Attribute elegante del túnel.

Configuración elegante del túnel ASA (ejemplo de Lotus) usando el ASDM 6.0(2)

Este documento asume que la configuración básica, tal como configuración de la interfaz, es completa y trabaja correctamente.

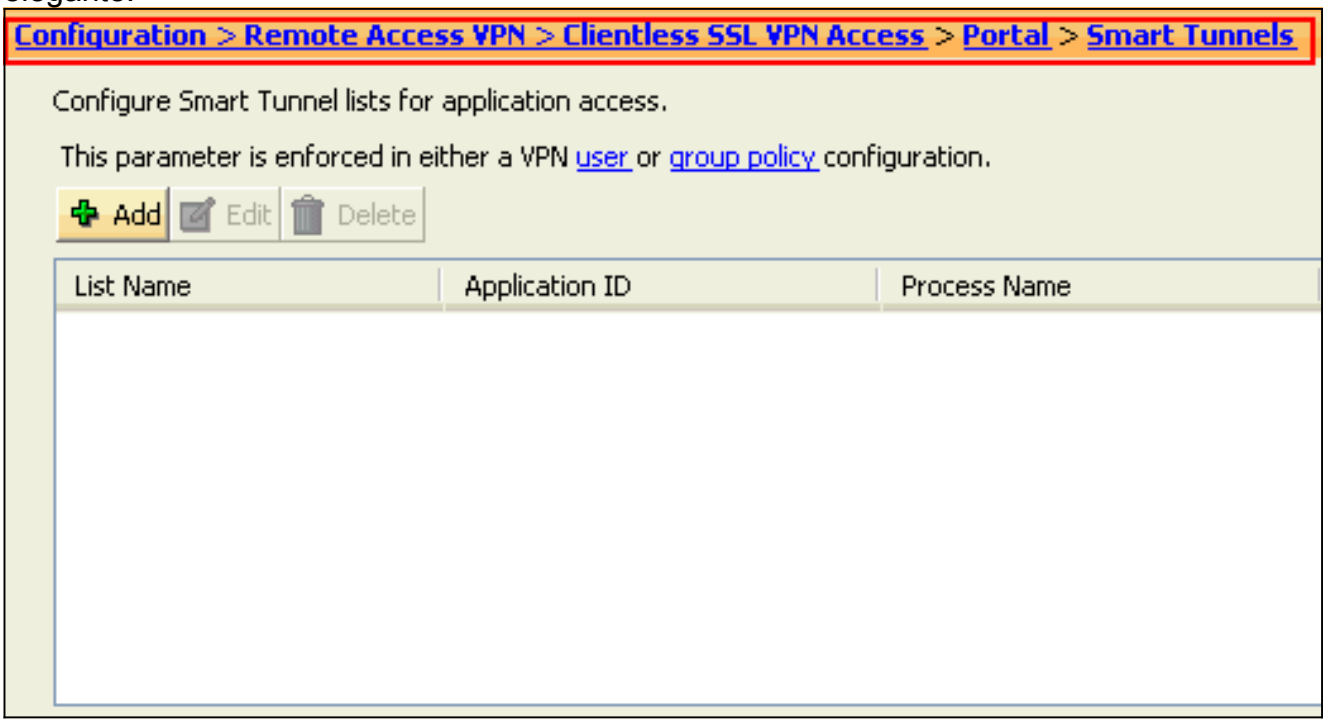
Nota: Consulte Cómo Permitir el Acceso HTTPS para el ASDM para que el ASA sea configurado por el ASDM.

Nota: El WebVPN y el ASDM no se pueden habilitar en la misma interfaz ASA a menos que cambie los números del puerto. Consulte ASDM y WebVPN Habilitados en la Misma Interfaz de ASA para obtener más información.

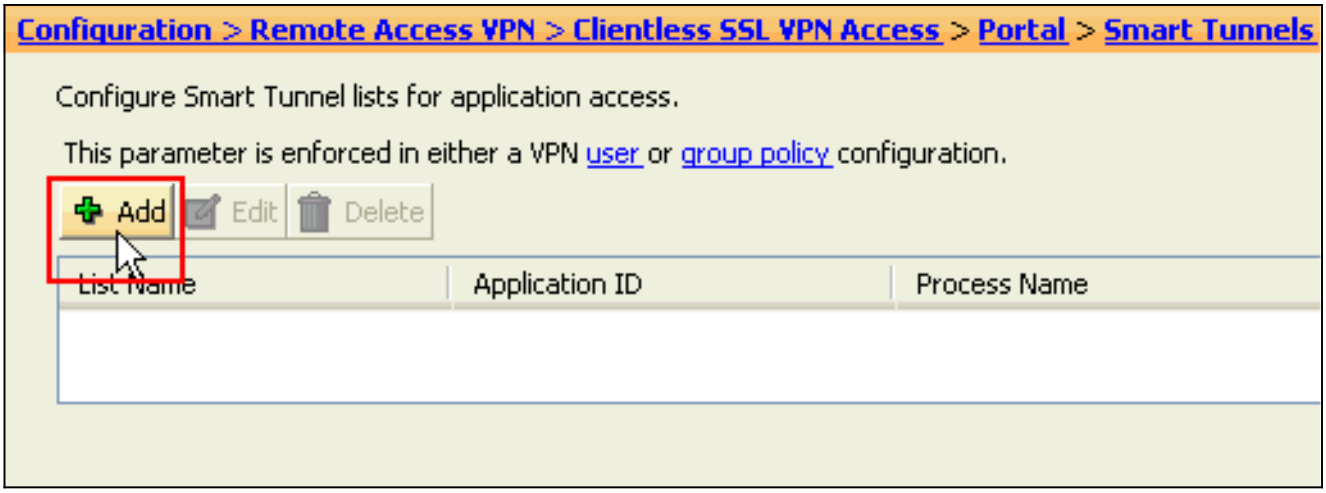
Complete estos pasos para configurar un túnel elegante:

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

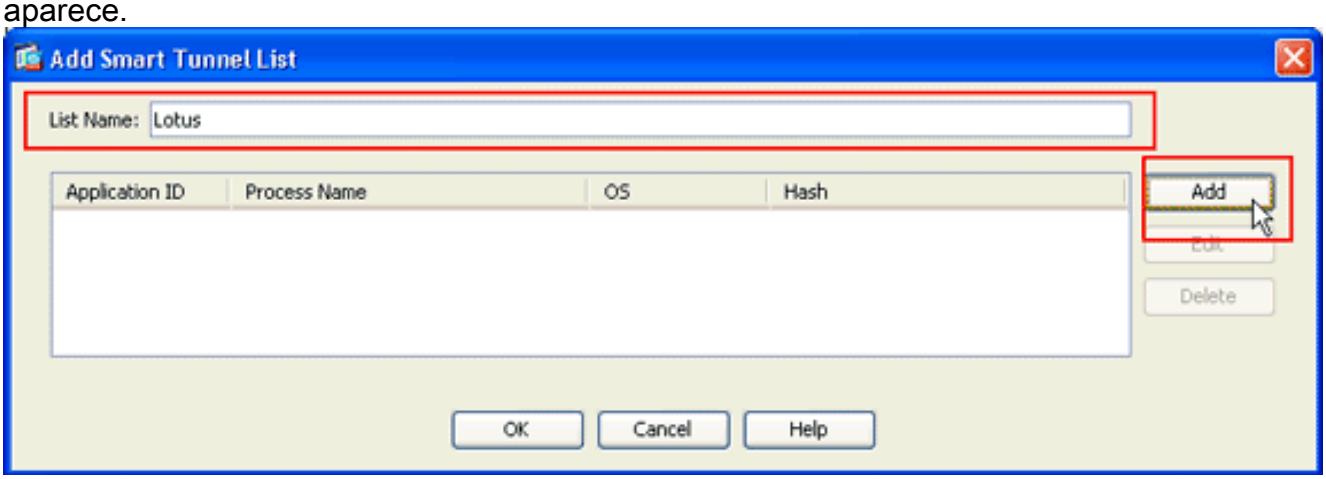
1. Elija la **configuración > el VPN de acceso remoto > el acceso > el portal del clientless SSL VPN > los túneles elegantes** para comenzar la configuración del túnel elegante.



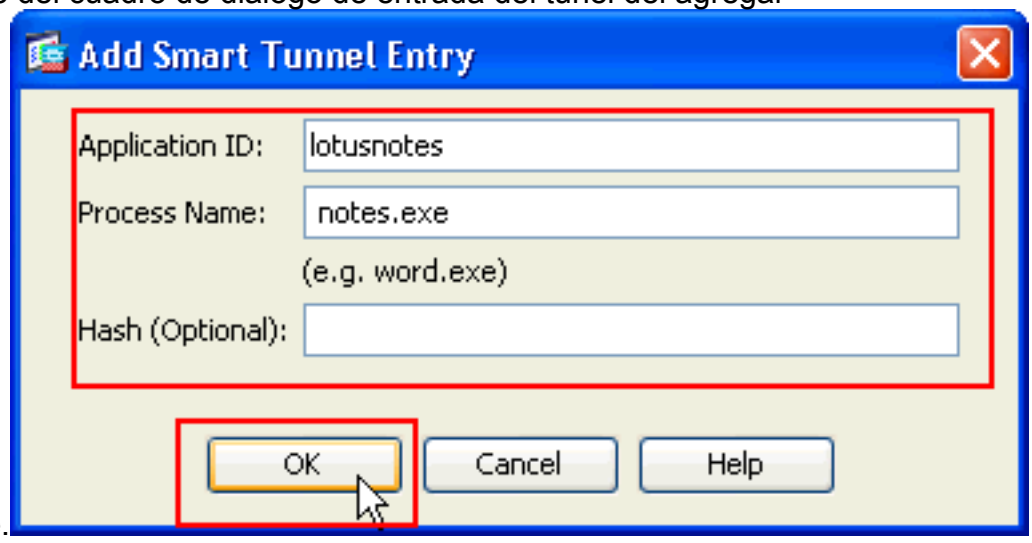
2. Haga clic en Add (Agregar).



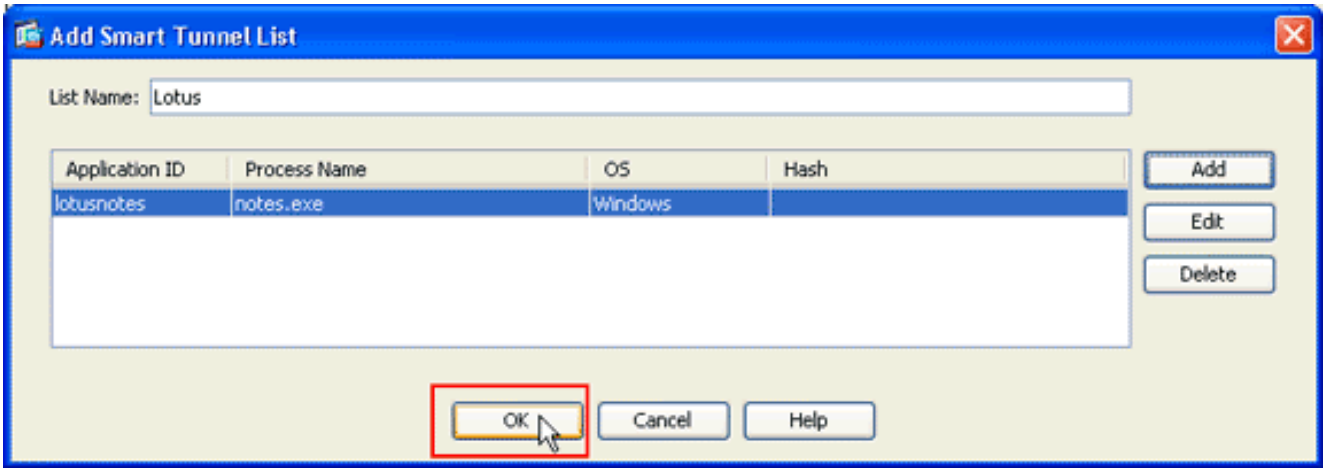
El cuadro de diálogo elegante de la lista del túnel del agregar aparece.



3. En el cuadro de diálogo elegante de la lista del túnel del agregar, haga click en AddEl cuadro elegante del cuadro de diálogo de entrada del túnel del agregar aparece.

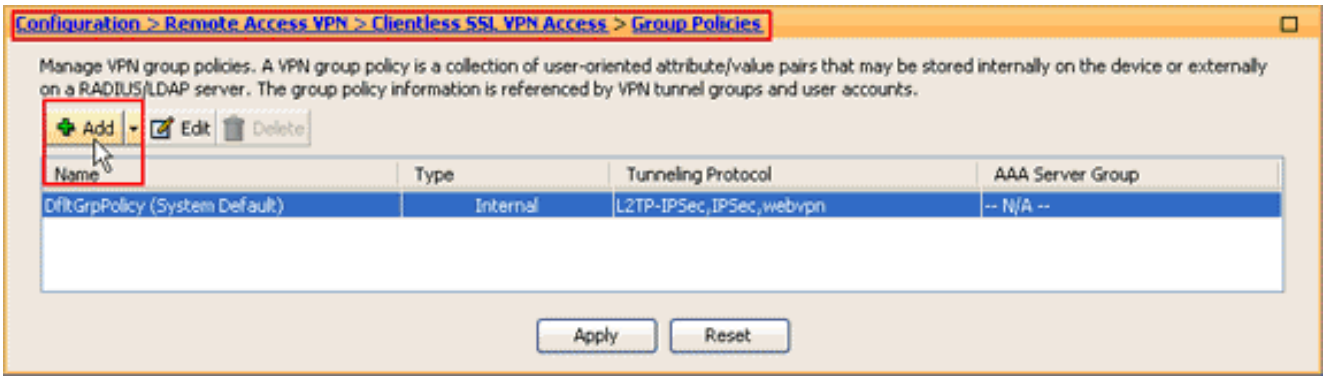


4. En el campo del ID de la aplicación, ingrese una cadena para identificar la entrada dentro de la lista elegante del túnel.
5. Ingrese un nombre del archivo y una extensión para la aplicación, y haga clic la AUTORIZACIÓN.
6. En el cuadro de diálogo elegante de la lista del túnel del agregar, haga clic la AUTORIZACIÓN.

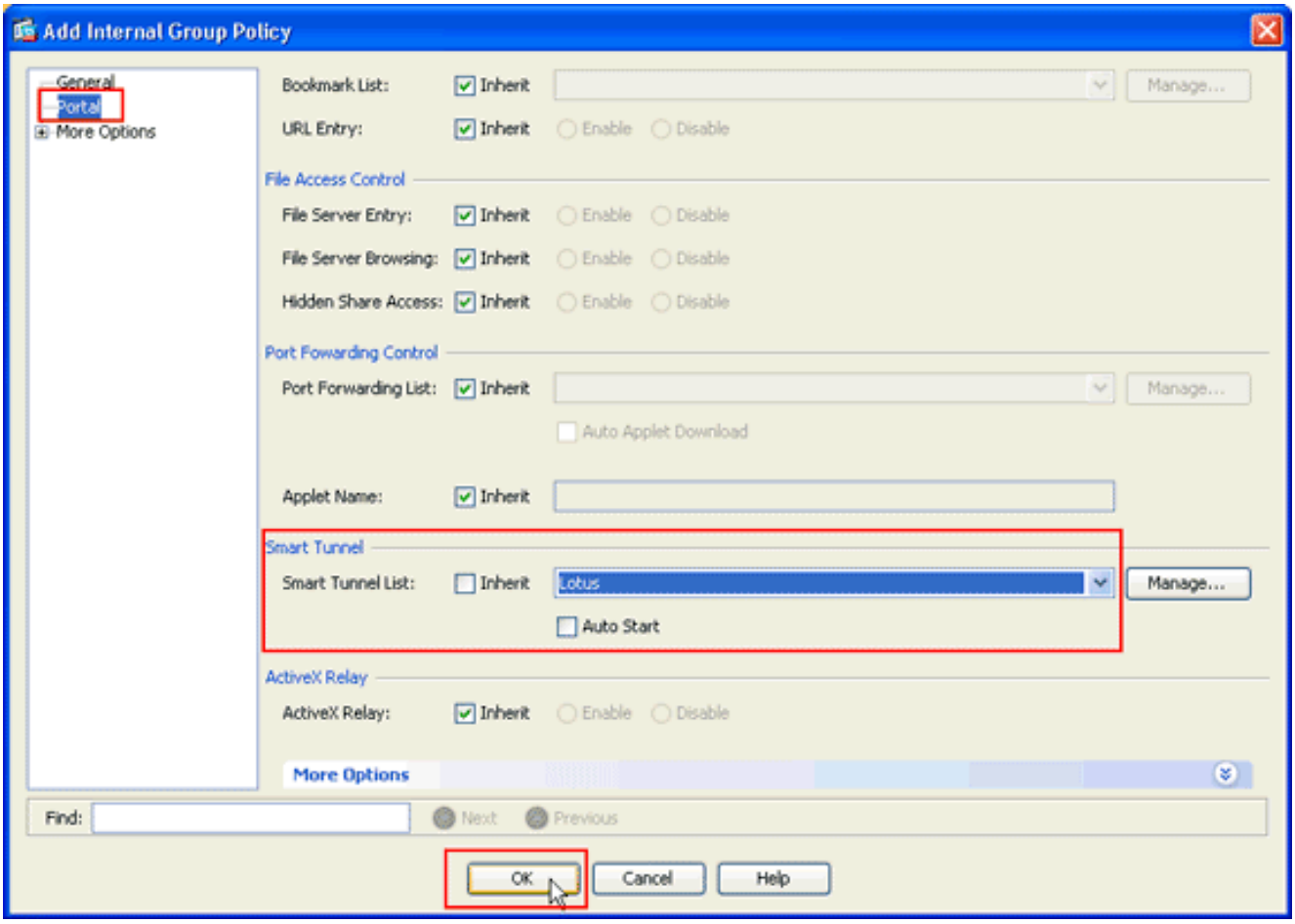


Nota: Aquí está el comando de configuración CLI equivalente:

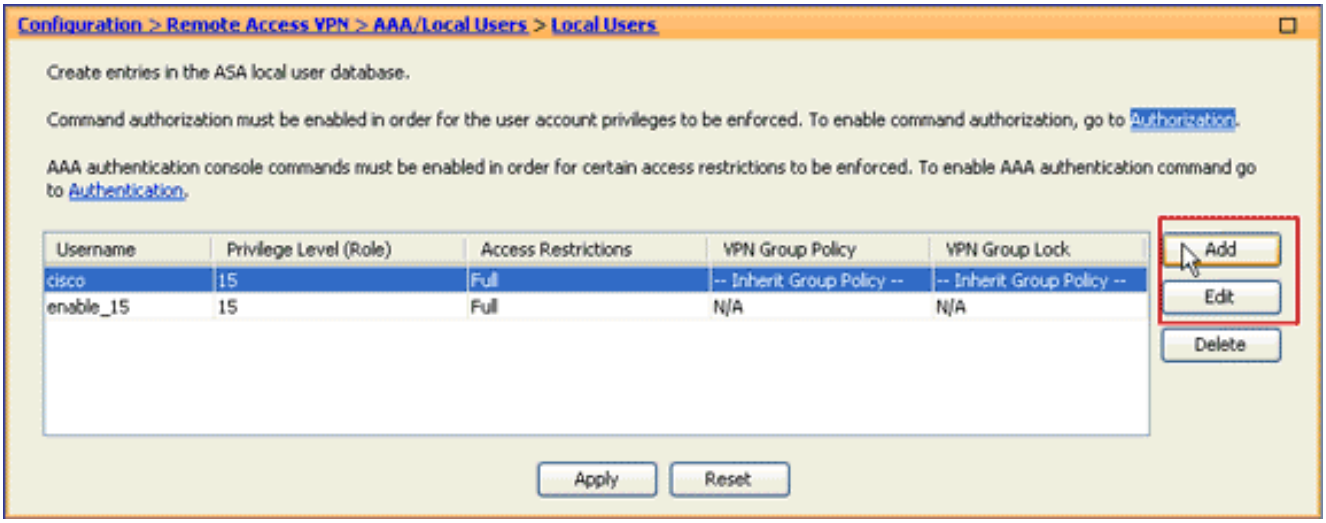
7. Asigne la lista a las directivas del grupo y a las directivas del usuario local a las cuales usted quiere proporcionar el acceso elegante del túnel a las aplicaciones asociadas como sigue:Para asignar la lista a una directiva del grupo, elegir las **directivas del acceso > del grupo del clientless SSL VPN de la configuración > del Acceso Remoto VPN>**, y el tecleo **agregue** o **edite.**



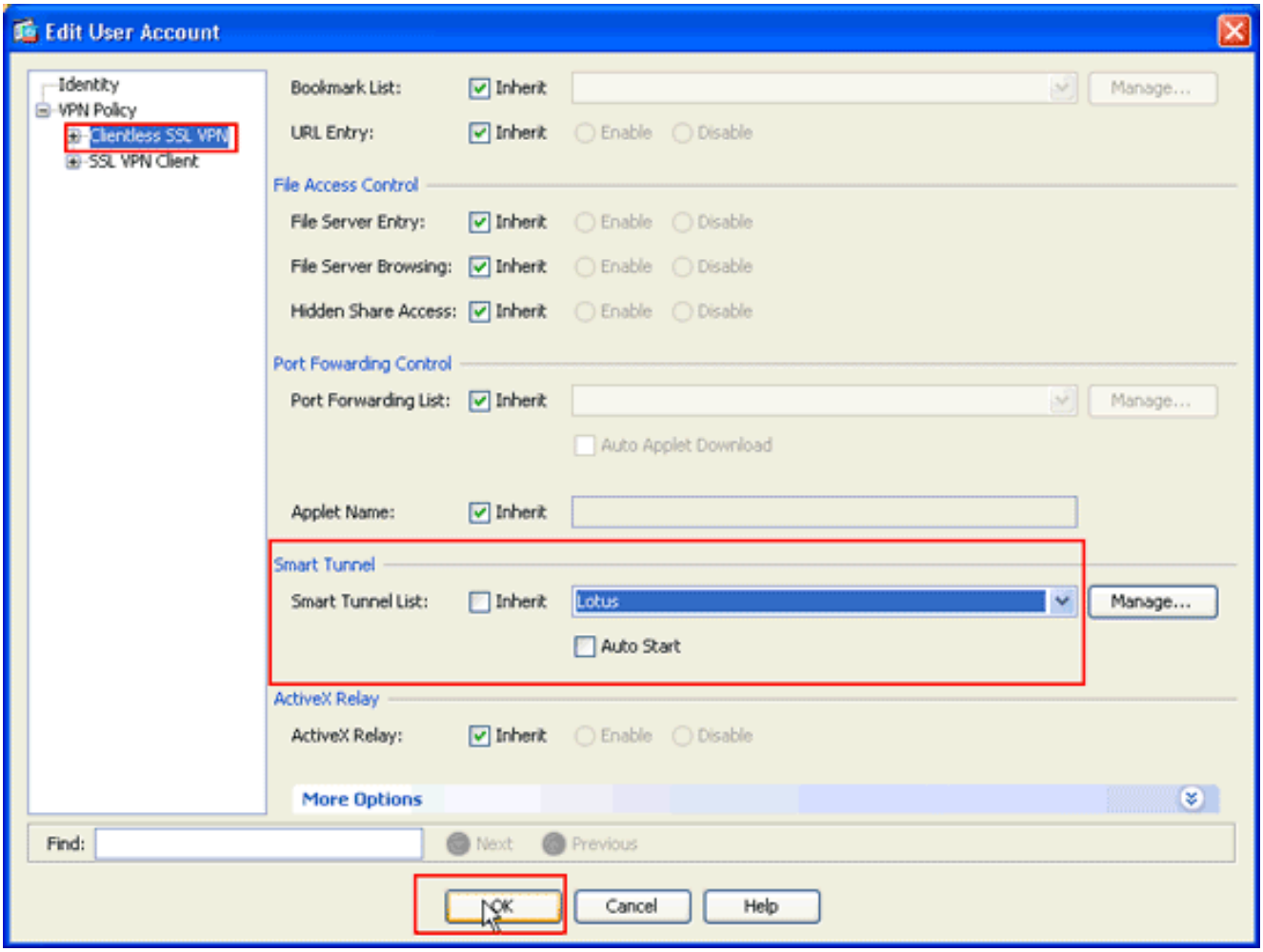
El cuadro de diálogo del Internal group policy (política grupal interna) del agregar aparece.



8. En el cuadro de diálogo del Internal group policy (política grupal interna) del agregar, haga clic el **portal**, elija el nombre de túnel elegante de la lista desplegable elegante de la lista del túnel, y haga clic la **AUTORIZACIÓN.Nota:** Este ejemplo utiliza *Lotus* como el nombre de la lista elegante del túnel.
9. Para asignar la lista a una directiva del usuario local, elegir la **configuración > el Acceso Remoto VPN> AAA ponga > los usuarios locales**, y el tecleo **agrega** para configurar la configuración un usuario nuevo o el tecleo **edita** para editar a un usuario existente.



El cuadro de diálogo de la cuenta de usuario del editar aparece.



10. En el cuadro de diálogo de la cuenta de usuario del editar, haga clic el **clientless SSL VPN**, elija el nombre de túnel elegante de la lista desplegable elegante de la lista del túnel, y haga clic la **AUTORIZACIÓN**.**Nota:** Este ejemplo utiliza *Lotus* como el nombre de la lista elegante del túnel.

La configuración del túnel elegante es completa.

Troubleshooting

No puedo conectar usando un túnel elegante marcado una dirección de la Internet URL en el portal del clientless. ¿Por qué este problema ocurre, y cómo puedo resolverlo?

Este problema ocurre debido al problema descrito en el Id. de bug Cisco CSCsx05766 (clientes registrados solamente). Para resolver este problema, retroceda el motor de ejecución Java plug-in a una versión anterior.

¿Puedo mutilar el URL de un link elegante del túnel configurado en el WebVPN?

Cuando el túnel elegante se utiliza en el ASA, usted no puede mutilar el URL u ocultar a la barra de dirección del navegador. Los usuarios pueden ver los URL de los links configurados en el WebVPN ese túnel elegante del uso. Como consecuencia, pueden cambiar el puerto y acceder el servidor para un cierto otro servicio.

Para resolver este problema, utilice WebType ACL. Refiera a crear WebType ACL para más

información.

Información Relacionada

- Cisco ASA 5500 Series Adaptive Security Appliances
- Release Note para el cliente VPN de AnyConnect, versión 2.3
- Ejemplo de Configuración de SSL VPN Client (SVC) en ASA con ASDM
- Soporte Técnico y Documentación - Cisco Systems