

PIX/ASA: Ejemplo de configuración de la característica del automóvil Update Button del cliente del IPSec VPN

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Cómo configurar la actualización de clientes para Windows con el CLI](#)

[Cómo configurar la actualización de clientes para Windows con el ASDM](#)

[Verificación](#)

[Información Relacionada](#)

Introducción

Este documento describe cómo configurar la característica del automóvil Update Button del Cliente Cisco VPN en el dispositivo de seguridad y el Dispositivos de seguridad Cisco PIX de la serie 500 adaptantes de las 5500 Series de Cisco ASA.

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.

- El dispositivo de seguridad adaptante de las 5500 Series de Cisco ASA funciona con la versión 7.x y posterior
- Versión 7.x y posterior de los funcionamientos del Dispositivos de seguridad Cisco PIX de la serie 500
- Versión 5.x y posterior del Cisco Adaptive Security Device Manager (ASDM)
- Cliente Cisco VPN 4.x y posterior

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.

[Cómo configurar la actualización de clientes para Windows con el CLI](#)

La característica de la actualización de clientes deja a los administradores en una ubicación central automáticamente notificar a los usuarios de cliente VPN cuando es hora de poner al día el software cliente VPN y la imagen del VPN 3002 Hardware Client.

Publique el comando de la **actualización de clientes** en el modo de configuración de los IPsec-
atributos del grupo de túnel para configurar la actualización de clientes. Si el cliente está funcionando con ya una versión de software en la lista de números de revisión, no necesita poner al día su software. Si el cliente no funciona con una versión de software en la lista, debe ponerse al día. Usted puede especificar hasta cuatro entradas de la actualización de clientes.

La sintaxis del comando es la siguiente:

```
client-update type type {url url-string} {rev-nums rev-nums} no client-update [type]
```

- **REV-nums** *REV-nums* — Especifica el software o las imágenes de firmware para este cliente. Ingrese hasta cuatro, separado por las comas.
- *tipo* — Especifica los sistemas operativos para notificar de una actualización de clientes. La lista de sistemas operativos comprende de éstos:Microsoft Windows: todas las Plataformas basadas en WindowsWIN9X: Windows 95, Windows 98, y Windows YO PlataformasWinNT: Plataformas del Windows NT 4.0, del Windows 2000, y de Windows XPvpn3002: VPN 3002 Hardware Client
- *cadena URL* **URL** — Especifica el URL para el software/la imagen de firmware. Este URL debe señalar a un archivo apropiado para el cliente.

Este ejemplo configura los parámetros de la actualización de clientes para el grupo de túnel del acceso remoto llamado remotegrp. Señala el número de revisión 4.6.1 y el URL para la extracción de la actualización, que es `https://support/updates`.

```
ASA
hostname(config)#tunnel-group remotegrp type ipsec_ra
hostname(config)#tunnel-group remotegrp ipsec-attributes
hostname(config-ipsec)#client-update type windows url
https://support/updates/rev-nums 4.6.1
```

[Cómo configurar la actualización de clientes para Windows con el ASDM](#)

Este documento supone que la configuración básica, tal como la configuración de la interfaz, ya fue realizada y funciona correctamente.

Refiera a [permitir el acceso HTTPS para el ASDM](#) para permitir que el ASA sea configurado por el ASDM

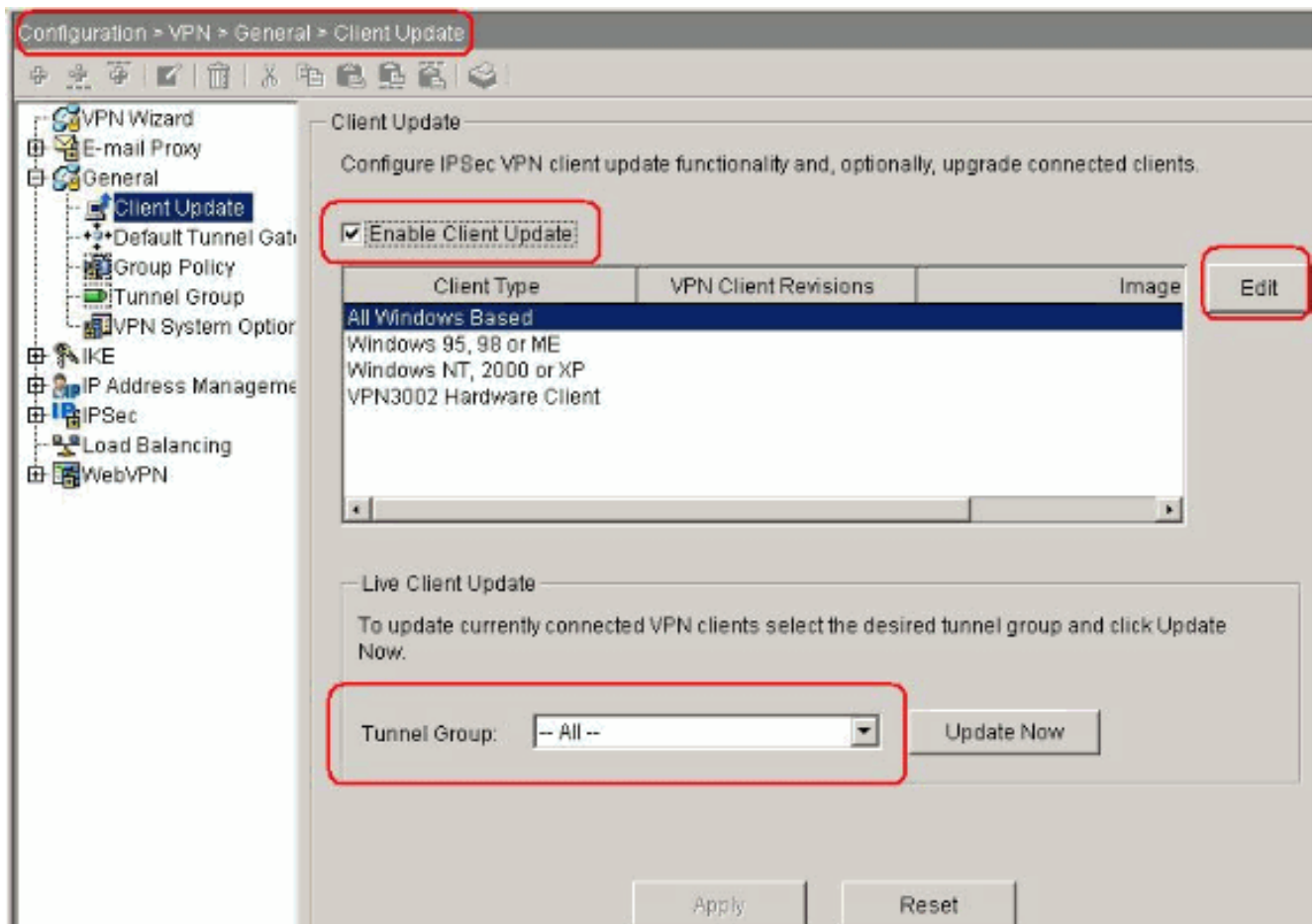
El ASDM abarca dos clases de actualización de clientes: uno que soporta los clientes de Windows y el VPN 3002 Hardware Clients a través de un grupo de túnel, y el otro que soporta los dispositivos ASA que actúan como Auto Update Server.

Los usuarios remotos pueden utilizar las versiones anticuadas del software VPN o del hardware cliente. Usted puede realizar una actualización de clientes en cualquier momento para hacer estas funciones:

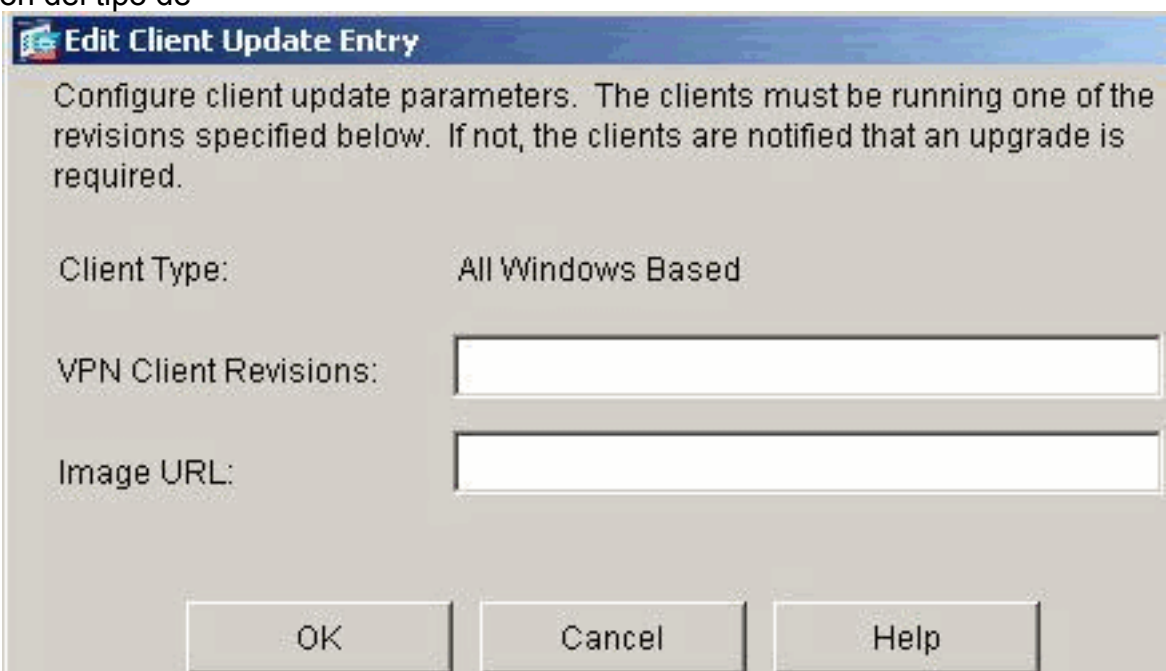
- Permiso que pone al día las revisiones del cliente.
- Especifique los tipos y a los números de revisión de clientes a quienes la actualización se aplique.
- Proporcione un URL o una dirección IP de los cuales conseguir la actualización.
- Notifique opcionalmente a los usuarios de cliente de Windows que deben poner al día su versión del cliente VPN.
- Para los clientes de Windows, usted puede proporcionar un mecanismo para que los usuarios logren la actualización.
- Para los usuarios del VPN 3002 Hardware Client, la actualización ocurre automáticamente, sin la notificación.

Complete estos pasos para configurar una actualización de clientes:

1. Elija la **configuración > el VPN > el general > la actualización de clientes** para ir a la ventana de la actualización de clientes. La ventana de la actualización de clientes se abre. Marque la casilla de verificación de la **actualización de clientes del permiso** para habilitar la actualización de clientes. Elija el tipo de cliente a quien usted quiere aplicar la actualización de clientes. Los tipos de cliente disponibles son **todos basados en Windows, Windows 95, 98 o YO, el Windows NT 4.0, 2000 o XP, y el VPN 3002 Hardware Client**. Si el cliente está funcionando con ya una versión de software en la lista de números de revisión, no necesita poner al día su software. Si el cliente no está funcionando con una versión de software en la lista, debe ponerse al día. Usted puede especificar hasta tres de estas entradas de la actualización de clientes. Toda la selección basada en Windows cubre todas las plataformas de Windows permisibles. Si usted selecciona esto, no especifique los tipos individuales del cliente de Windows. El tecleo **edita** para especificar las revisiones aceptables del cliente y la fuente para el software o la imagen de firmware actualizado para la actualización de clientes.



2. La ventana de entrada de la actualización de clientes del editar aparece y muestra la selección del tipo de

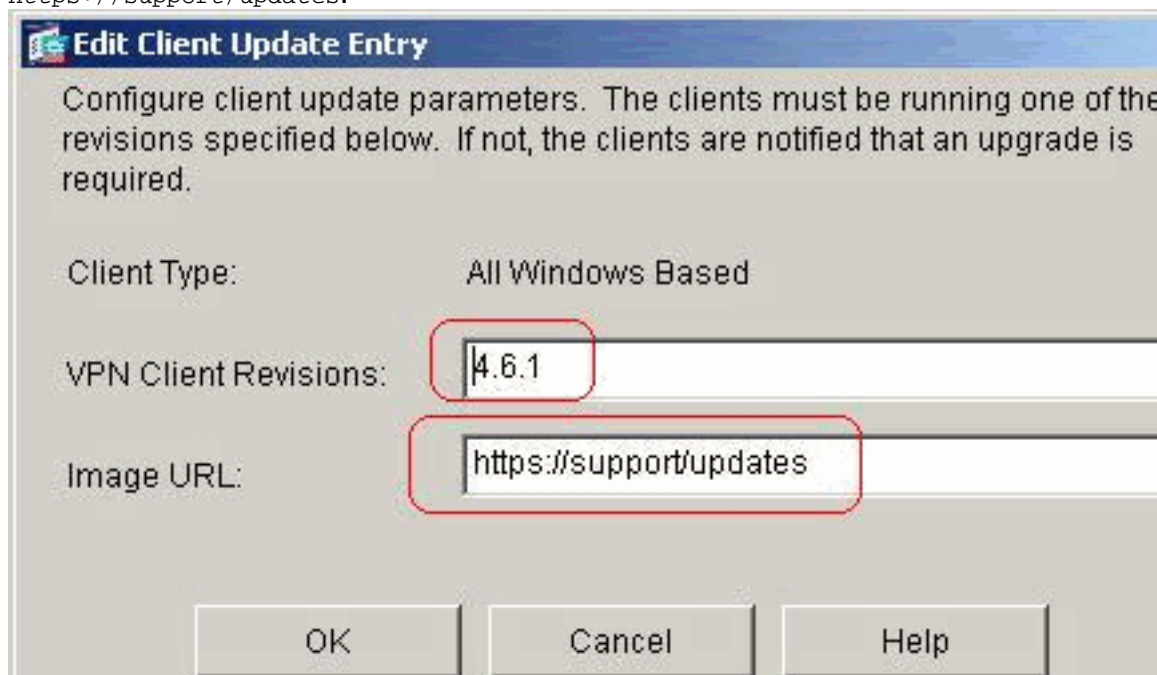


cliente.

3. Especifique la actualización de clientes que usted quiere aplicar a todos los clientes del tipo seleccionado a través del dispositivo de seguridad entero. Es decir, especifique el tipo de cliente, el URL o la dirección IP de quienes conseguir la imagen actualizada, y el número de revisión o los números aceptables para ese cliente. Usted puede especificar hasta cuatro números de revisión, separados por las comas. Sus entradas aparecen en las columnas apropiadas la tabla en la ventana de la actualización del cliente después de que usted haga clic la **AUTORIZACIÓN**. Si el número de revisión del cliente hace juego uno de los números de revisión especificados, no hay necesidad de poner al día al cliente. **Nota:** Para todos los

clientes de Windows, usted debe utilizar el protocolo `http://` o `https://` como el prefijo para el URL. Para el VPN 3002 Hardware Client, usted debe especificar el protocolo `fttp://` en lugar de otro. Inicia una actualización de clientes para todos los clientes de Windows para las revisiones corrientes de un grupo de túnel del acceso remoto más viejas de 4.6.1 y especifica el URL para la extracción de la actualización como

`https://support/updates:`



Alternativa

mente, usted puede configurar la actualización de clientes apenas para los tipos de cliente individuales, bastante que para todos los clientes de Windows, que usted puede ver si el paso 1-c. La actualización de los clientes del VPN 3002 sin la intervención del usuario y los usuarios no reciben ningún mensaje de notificación. Usted puede tener el navegador automáticamente comenzar una aplicación si usted incluye el nombre de la aplicación en el final del URL; por ejemplo: `https://support/updates/vpnclient.exe`.

4. Opcionalmente, usted puede enviar un aviso a los usuarios activos con los clientes de Windows anticuados que necesitan poner al día a su cliente. Utilice el área viva de la actualización de clientes de la ventana de la actualización de clientes para enviar este aviso. Elija el grupo de túnel (o todo) y **ahora** haga clic la **actualización**. Un cuadro de diálogo aparece en la figura y pide que usted confirme que usted quiera notificar a los clientes conectados sobre la actualización.



Los

usuarios señalados ven una ventana emergente, que les ofrece la oportunidad de poner en marcha a un navegador y de descargar el software actualizado del sitio que usted especificó

en el URL. La única parte de este mensaje que usted pueda configurar es el URL. (Véase los pasos 1-b o 1-c.) Los usuarios que no son activos consiguen un mensaje de notificación la próxima vez que abren una sesión. Usted puede enviar este aviso a todos los clientes activos en todos los grupos de túnel, o usted puede enviarlo a los clientes en un grupo del túnel particular. Si el número de revisión del cliente hace juego uno de los números de revisión especificados, no hay necesidad de poner al día al cliente, y no se envía ningún mensaje de notificación al usuario. La actualización de los clientes del VPN 3002 sin la intervención del usuario y los usuarios no reciben ningún mensaje de notificación.

Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Información Relacionada

- [Soporte Técnico y Documentación - Cisco Systems](#)