Configuraciones de LAN a LAN de renegociación entre los Concentradores VPN de Cisco, el Cisco IOS, y los dispositivos PIX

Contenido

Introducción

Este documento señala los resultados de la prueba del laboratorio de la renegociación del túnel de LAN a LAN de la seguridad IP (IPSec) entre diversos Productos del Cisco VPN en los diversos escenarios, tales como reinicialización del dispositivo VPN, los reintroduce, y la terminación manual de las asociaciones de seguridad IPSec (SA).

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.

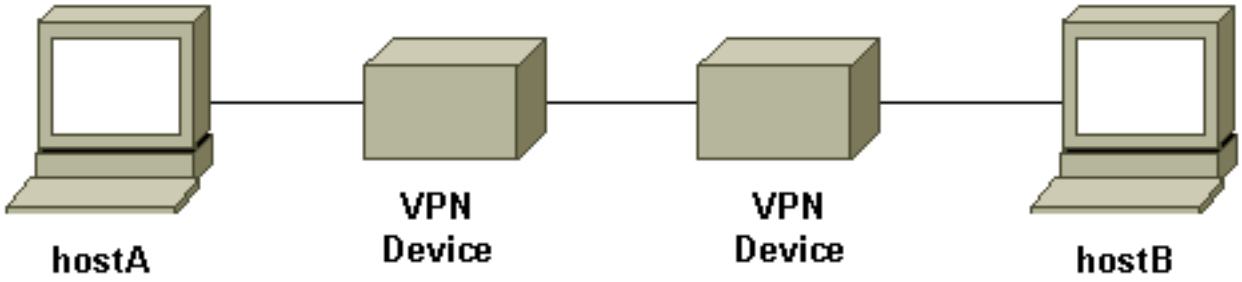
- Software Release 12.1(5)T8 de Cisco IOS®
- Software Release 6.0(1) del Cisco PIX
- Versión de software 3.0(3)A del Cisco VPN 3000 Concentrator
- Versión concentrador software del Cisco VPN 5000 5.2(21)

El tráfico IP usado en esta prueba es paquetes bidireccionales del Internet Control Message Protocol (ICMP) entre el hostA y el hostB.

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.

Diagrama de la red

Éste es un diagrama de concepto de la plataforma de ensayo.



Los dispositivos VPN representan un router del Cisco IOS, un Cisco Secure PIX Firewall, un Cisco VPN 3000 Concentrator o un concentrador del Cisco VPN 5000.

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Escenarios de prueba

Tres escenarios frecuentes fueron probados. Lo que sigue es una definición abreviada de los escenarios de prueba:

- **Terminación manual del SA de IPSec** — El usuario abre una sesión a los dispositivos VPN y borra manualmente el SA de IPSec usando el comando line interface(cli) o el Interfaz gráfica del usuario (GUI).
- **Reintroduzca** — Normal fase IPSec yo y la fase II reintroducen cuando expira la vida útil definida. En esta prueba, los dos dispositivos de la terminación VPN tienen el mismo curso de la vida de la fase I y de la fase II configurado.
- **Reinicialización del dispositivo VPN** — Cualquier extremo de los puntos de terminación del túnel VPN fue reiniciado para simular la interrupción del servicio.

Nota: Para los túneles de LAN a LAN donde se utiliza el VPN 5000 concentrator, el concentrador se configura usando el respondedor del modo principal y del túnel.

Resultados de la prueba

Configuración	Manualmente terminación del SA de IPSec	Reintroduzca	Reinicialización del dispositivo VPN
IOS al PIX	• El túnel restableció	• El tráfico	• Con el keepalive

	después de la fase I o la fase II SA se borra por ambas partes • Trabajos del tráfico de prueba	de prueba todavía trabaja después de la fase I o la fase II reintroduce	IKE habilitado en ambos dispositivos, túnel restablecidos • El tráfico de prueba[1] trabaja después del túnel recuperado
IOS a VPN 3000	• El túnel restableció después de la fase I o la fase II SA se borra por ambas partes • Trabajos del tráfico de prueba	• El tráfico de prueba todavía trabaja después de la fase I o la fase II reintroduce	• Con el keepalive IKE habilitado en ambos dispositivos, túnel restablecidos • El tráfico de prueba[1] trabaja después del túnel recuperado
IOS al VPN5 000	• En el IOS: Se borra el tráfico de prueba todavía trabaja después de la fase II SAEl túnel VPN va abajo de cuando se borra la fase I SAEl tráfico de prueba para el trabajar • En el	• El tráfico de prueba todavía trabaja después de la fase II reintroduce • La fase I	• El túnel no puede recuperar después de la reinicialización cualquier dispositivo VPN (con el tráfico de prueba bidireccional) • El tráfico de prueba para el trabajar • Necesidad

	VPN5000: El túnel no puede recuperarse después manualmente de borrar el SADebe borrar la fase I y la fase II SA en el IOS para restablecer el túnel	reintroduce derribado el túnel • El tráfico de prueba para el trabajar • Necesidad manualmente SA claros para traer el túnel detrás	manualmente clara el SA en el dispositivo que no fue reiniciado para traer el túnel detrás
PIX a VPN 3000	• El túnel restableció después de la fase I o la fase II SA se borra por ambas partes • Trabajos del tráfico de prueba	• El tráfico de prueba todavía trabaja después de la fase I o la fase II reintroduce	• El tráfico de prueba[1] trabaja después del túnel recuperado • Con el Dead Peer Detection (DPD) [2] (habilitado por abandono), túnel restablecido
PIX al VPN5000	• En el PIX: Se borra el tráfico de prueba todavía trabaja después de la	• El tráfico de prueba todavía	• El túnel no puede recuperar después de la reinicialización cualquier

	fase II SAEl túnel VPN fue abajo de cuando se borra la fase I SAEl tráfico de prueba para el trabajar • En el VPN5000: El túnel no puede recuperarse después de que manualmente claros SADebe borrar la fase I y la fase II SA en el PIX para restablecer el túnel	trabaja después de la fase II reintroduce • La fase I reintroduce derribado el túnel • El tráfico de prueba para el trabajar • Necesidad manualmente SA claros para traer el túnel detrás	dispositivo VPN (con el tráfico de prueba bidireccional) • El tráfico de prueba para el trabajar • Necesidad manualmente clara el SA en el dispositivo que no fue reiniciado para traer el túnel detrás
VPN 3000 al VPN5000	• En VPN 3000: El túnel se recupera después manualmente de claro la sesiónTodavía del tráfico trabajos • En el VPN5000: El túnel no puede recuperar	• El tráfico de prueba todavía trabaja después de que la fase I o la	• El túnel no puede recuperarse después de la reinicialización de cualquier dispositivo VPN (con el tráfico de prueba bidireccional)

	después manualmente de claro el túnelEl tráfico de prueba para el trabajarDebe borrar el SA en VPN 3000 para restablecer el túnel	fase II reintroduzca	• El tráfico de prueba para el trabajar • Necesidad manualmente clara el SA en el dispositivo que no fue reiniciado para traer el túnel detrás

[1] como se describe anteriormente, el tráfico de prueba usado es paquetes icmp bidireccionales entre el hostA y el hostB. En la prueba de la reinicialización del dispositivo VPN, el tráfico unidireccional también se prueba para simular el peor de los casos (donde está el tráfico solamente del host detrás del dispositivo VPN que no se reinicia al dispositivo VPN se reinicia que). Al igual que visto de la tabla, con el keepalive IKE o con el protocolo DPD, el túnel VPN se puede recuperar del peor de los casos.

[2] DPD es parte del Unity Protocol. Esta característica está actualmente solamente disponible en el Cisco VPN 3000 Concentrator con el 3.0 de la versión de software y sobre y en el firewall PIX con la versión de software 6.0(1) y arriba.

Información Relacionada

- Página de soporte del concentrador de la serie Cisco VPN 3000
- Página de soporte del concentrador VPN 5000 de Cisco
- Página de Soporte de PIX
- Página de soporte de IPSec
- Soporte Técnico y Documentación - Cisco Systems