Renegociación de las Configuraciones de LAN a LAN entre Concentradores VPN de Cisco, Cisco IOS y Dispositivos PIX

Contenido

Introducción

Este documento informa de los resultados de las pruebas de laboratorio de la renegociación del túnel de LAN a LAN de IP Security (IPSec) entre diferentes productos de Cisco VPN en diversos escenarios, como reinicio del dispositivo VPN, reclave y terminación manual de asociaciones de seguridad IPSec (SA).

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.

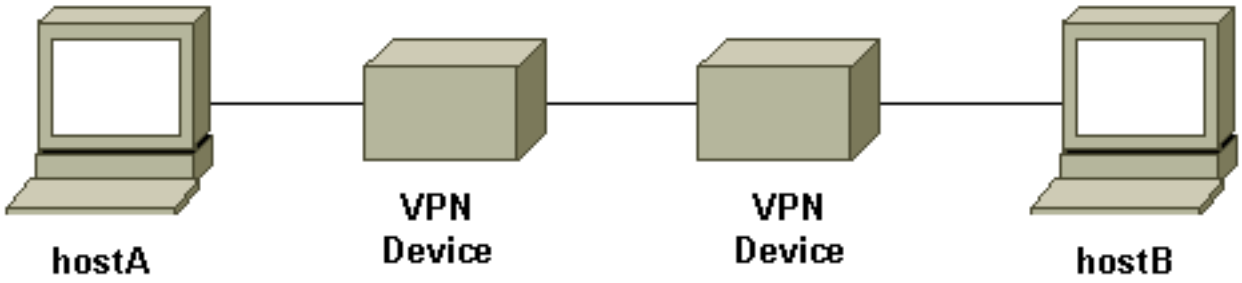
- Versión 12.1(5)T8 del software del IOS® de Cisco
- Versión 6.0(1) del software Cisco PIX
- Software Cisco VPN 3000 Concentrator versión 3.0(3)A
- Software Cisco VPN 5000 Concentrator versión 5.2(21)

El tráfico IP utilizado en esta prueba son paquetes de protocolo de mensajes de control de Internet (ICMP) bidireccionales entre el hostA y el hostB.

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.

Diagrama de la red

Este es un diagrama conceptual del banco de pruebas.



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

Convenciones

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

Escenarios de prueba

Se probaron tres escenarios comunes. A continuación se ofrece una breve definición de los escenarios de prueba:

- **Terminación manual de las SAs IPSec**: el usuario inicia sesión en los dispositivos VPN y borra manualmente las SAs IPSec mediante la interfaz de línea de comandos (CLI) o la interfaz gráfica de usuario (GUI).
- **Rekey**: la fase I normal de IPSec y la fase II vuelven a ser clave cuando caduca la vida útil definida. En esta prueba, los dos dispositivos de terminación VPN tienen configuradas la misma vida útil de fase I y fase II.
- **Reinicio del dispositivo VPN**: cualquiera de los extremos de los puntos de terminación del túnel VPN se reinició para simular la interrupción del servicio.

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

Resultados de la prueba

Configuración	Terminación manual de SAs IPSec	Rekey	Reinicio del dispositivo VPN
IOS a PIX	• El túnel restablecido después de la	• El tráfico de	• Con la señal de mantenimi

	fase I o la fase II SA se elimina en cualquiera de los lados • El tráfico de prueba funciona	prueba sigue funcionando después de la fase I o de la fase II de la nueva clave	ento IKE activada en ambos dispositivos, el túnel se restablece • El tráfico de prueba [1] funciona después de que se recupere el túnel
IOS a VPN 3000	• El túnel restablecido después de la fase I o la fase II SA se elimina en cualquiera de los lados • El tráfico de prueba funciona	• El tráfico de prueba sigue funcionando después de la fase I o de la fase II de la nueva clave	• Con la señal de mantenimiento IKE activada en ambos dispositivos, el túnel se restablece • El tráfico de prueba [1] funciona después de que se recupere el túnel
IOS a VPN 5000	• En IOS: El tráfico de prueba todavía funciona después de que se borra la SA de fase IIEl túnel VPN se desactiva cuando se borra la SA de fase IEl tráfico de prueba deja de funcionar	• El tráfico de prueba todavía funciona después de la reclave de la fase II • La nueva clave de la	• El túnel no puede recuperarse después de reiniciar cualquier dispositivo VPN (con tráfico de prueba bidireccional) • El tráfico de prueba deja de funcionar

	• En VPN 5000: El túnel no puede recuperarse después de limpiar manualmente la SADebe borrar tanto la fase I como la fase II SA en el IOS para restablecer el túnel	fase I ha derribado el túnel • El tráfico de prueba deja de funcionar • Debe borrar manualmente las SA para volver a traer el túnel	• Debe borrar manualmente la SA en el dispositivo que no se reinició para devolver el túnel
PIX a VPN 3000	• El túnel restablecido después de la fase I o la fase II SA se elimina en cualquiera de los lados • El tráfico de prueba funciona	• El tráfico de prueba sigue funcionando después de la fase I o de la fase II de la nueva clave	• El tráfico de prueba [1] funciona después de que se recupere el túnel • Con la detección de par muerto (DPD)[2] (activada de forma predeterminada), se restablece el túnel
PIX a VPN 5000	• En PIX: El tráfico de prueba todavía funciona después de que se borra la SA de fase	• El tráfico de prueba todavía funciona después	• El túnel no puede recuperarse después de reiniciar cualquier dispositivo VPN (con

	IIEl túnel VPN se desactivó cuando se borró la fase I SAEl tráfico de prueba deja de funcionar • En VPN 5000: El túnel no se recupera después de limpiar manualmente SADebe borrar tanto la fase I como la fase II SA en el PIX para restablecer el túnel	s de la reclave de la fase II • La nueva clave de la fase I ha derriba do el túnel • El tráfico de prueba deja de funcion ar • Debe borrar manual mente las SA para volver a traer el túnel	tráfico de prueba bidireccion al) • El tráfico de prueba deja de funcionar • Debe borrar manualme nte la SA en el dispositivo que no se reinició para devolver el túnel
VPN 3000 a VPN 5000	• En VPN 3000: El túnel se recupera después de borrar manualmente la sesiónEl tráfico todavía funciona • En VPN 5000: El túnel no puede recuperarse después de borrar manualmente el túnelEl tráfico de prueba deja	• El tráfico de prueba todavía funcion a despué s de la reclave de fase I o fase II	• El túnel no puede recuperars e después del reinicio de cualquier dispositivo VPN (con tráfico de prueba bidireccion al) • El tráfico de prueba deja de funcionar • Debe borrar

	de funcionarDebe borrar SA en VPN 3000 para restablecer el túnel		manualmente la SA en el dispositivo que no se reinició para devolver el túnel

[1] Como se describe anteriormente, el tráfico de prueba utilizado son paquetes ICMP bidireccionales entre el hostA y el hostB. En la prueba de reinicio del dispositivo VPN, el tráfico unidireccional también se prueba para simular el peor de los escenarios (donde el tráfico es solamente del host detrás del dispositivo VPN que no se reinicia al dispositivo VPN que se reinicia). Como se puede ver en la tabla, con keepalive IKE o con el protocolo DPD, el túnel VPN se puede recuperar del peor de los casos.

[2] DPD es parte del protocolo Unity. Actualmente, esta función sólo está disponible en el Cisco VPN 3000 Concentrator con la versión de software 3.0 y superiores y en el PIX Firewall con la versión de software 6.0(1) y superiores.

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