Neuaushandeln von LAN-zu-LAN-Konfigurationen zwischen Cisco VPN Concentrators, Cisco IOS und PIX-Geräten

Inhalt

Einführung

In diesem Dokument werden die Labortestergebnisse der Neuaushandlung von IP Security (IPSec)-LAN-zu-LAN-Tunneln zwischen verschiedenen Cisco VPN-Produkten in verschiedenen Szenarien beschrieben, z. B. Neustarts von VPN-Geräten, erneutes Auftreten und manuelle Beendigung von IPSec-Sicherheitszuordnungen (SAs).

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

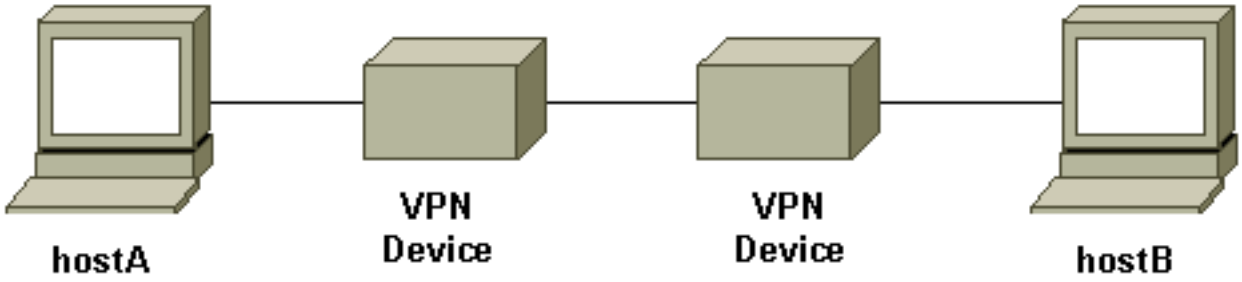
- Cisco IOS® Softwareversion 12.1(5)T8
- Cisco PIX Softwareversion 6.0(1)
- Cisco VPN 3000 Concentrator Software Version 3.0(3)A
- Cisco VPN 5000 Concentrator-Software, Version 5.2(21)

Bei dem in diesem Test verwendeten IP-Datenverkehr handelt es sich um bidirektionale ICMP-Pakete (Internet Control Message Protocol) zwischen HostA und HostB.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Netzwerkdiagramm

Dies ist ein Konzeptdiagramm der Testumgebung.



VPN-Geräte stellen einen Cisco IOS-Router, eine Cisco Secure PIX Firewall, einen Cisco VPN 3000 Concentrator oder einen Cisco VPN 5000 Concentrator dar.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Testszenarien

Es wurden drei gängige Szenarien getestet. Im Folgenden finden Sie eine kurze Definition der Testszenarien:

- **Manuelle Terminierung von IPSec SAs** - Der Benutzer meldet sich bei den VPN-Geräten an und löscht die IPSec SAs manuell über die Befehlszeilenschnittstelle (CLI) oder die grafische Benutzeroberfläche (GUI).
- **Rekey** - Normale IPSec-Phasen I und II rekey, wenn die definierte Lebensdauer abläuft. In diesem Test ist für die beiden VPN-Terminierungsgeräte dieselbe Lebensdauer für Phase I und Phase II konfiguriert.
- **Neustart des VPN-Geräts** - Beide Endpunkte des VPN-Tunnels wurden neu gestartet, um einen Service-Ausfall zu simulieren.

Hinweis: Bei LAN-to-LAN-Tunneln, in denen der VPN 500-Konzentrator verwendet wird, wird der Konzentrator mithilfe des MAIN-Modus und des Tunnel-Responders konfiguriert.

Testergebnisse

Einrichtung	Manuelle Beendigung von IPSec SAs	Umschalten	Neustarten von VPN-Geräten
IOS zu	• Tunnel, der nach Phase I oder	• Der Testd	• Bei aktivierter

PIX	Phase II SA wiederhergestellt wird, wird auf beiden Seiten gelöscht • Testdatenverkehr funktioniert	atenverkehr funktioniert nach Phase I oder Phase II-Neustart weiterhin	IKE-Keepalive-Funktion auf beiden Geräten wurde Tunnel wiederhergestellt. • Testen des Datenverkehrs[1] nach der Tunnelwiederherstellung
IOS zu VPN 300	• Tunnel, der nach Phase I oder Phase II SA wiederhergestellt wird, wird auf beiden Seiten gelöscht • Testdatenverkehr funktioniert	• Der Testdatenverkehr funktioniert nach Phase I oder Phase II-Neustart weiterhin	• Bei aktivierter IKE-Keepalive-Funktion auf beiden Geräten wurde Tunnel wiederhergestellt. • Testen des Datenverkehrs[1] nach der Tunnelwiederherstellung
IOS zu VPN 500	• IOS: Testdatenverkehr funktioniert nach der Freigabe der Phase II SA nochDer VPN-Tunnel fällt aus, wenn Phase I SA gelöscht wird.Test-Datenverkehr stoppt	• Testdatenverkehr funktioniert nach Phase II-Neustart weiterhin	• Tunnel kann nach dem Neustart eines VPN-Geräts (mit bidirektionalem Testdatenverkehr) nicht wiederhergestellt

	• Auf VPN 5000: Tunnel kann nach dem manuellen Löschen des SA nicht wiederhergestellt werdenLöschen sowohl Phase I als auch Phase II SA auf IOS, um Tunnel wiederherzustellen	• Phase I rekey führte den Tunnel herunter • Test-Datenverkehr stoppt • SAs müssen manuell gelöscht werden, um den Tunnel wieder zurückzusetzen.	werden • Test-Datenverkehr stoppt • Die SA auf dem Gerät, das nicht neu gestartet wurde, muss manuell gelöscht werden, um den Tunnel zurückzusetzen.
PIX zu VPN 300	• Tunnel, der nach Phase I oder Phase II SA wiederhergestellt wird, wird auf beiden Seiten gelöscht • Testdatenverkehr funktioniert	• Der Testdatenverkehr funktioniert nach Phase I oder Phase II-Neustart weiter	• Testen des Datenverkehrs[1] nach der Tunnelwiederherstellung • Dead Peer Detection (DPD)[2] (standardmäßig aktiviert), Tunnel wieder hergestellt

		hin	
PIX zu VPN 5000	• Auf PIX: Testdatenverkehr funktioniert nach der Freigabe der Phase II SA nochDer VPN-Tunnel ist ausgefallen, wenn Phase I SA gelöscht wird.Test-Datenverkehr stoppt • Auf VPN 5000: Tunnel kann nach manueller Freigabe von SA nicht wiederhergestellt werdenLöschen sowohl Phase I als auch Phase II SA auf PIX, um Tunnel wiederherzustellen	• Testdatenverkehr funktioniert nach Phase II-Neustart weiterhin • Phase I rekey führte den Tunnel herunter • Test-Datenverkehr stoppt • SAs müssen manuell gelöscht werden, um den Tunnel wieder zurückzusetzen.	• Tunnel kann nach dem Neustart eines VPN-Geräts (mit bidirektionalem Testdatenverkehr) nicht wiederhergestellt werden • Test-Datenverkehr stoppt • Die SA auf dem Gerät, das nicht neu gestartet wurde, muss manuell gelöscht werden, um den Tunnel zurückzusetzen.
VPN 3000 zu	• Auf VPN 3000: Tunnel wird	• Testdatenv	• Tunnel kann nach

VPN 5000	wiederhergestellt, nachdem die Sitzung manuell gelöscht wurdeDatenverkehr funktioniert noch • Auf VPN 5000: Tunnel kann nach manuellem Löschen des Tunnels nicht wiederhergestellt werdenTest-Datenverkehr stopptSA auf VPN 300 muss gelöscht werden, um Tunnel wiederherzustellen	erkehr funktioniert nach Phase I oder Phase II-Recey noch	Neustart eines der VPN-Geräte (mit bidirektionalem Testdatenverkehr) nicht wiederhergestellt werden • Test-Datenverkehr stoppt • Die SA auf dem Gerät, das nicht neu gestartet wurde, muss manuell gelöscht werden, um den Tunnel zurückzusetzen.

[1] Wie oben beschrieben, wird für den Testdatenverkehr bidirektionale ICMP-Pakete zwischen HostA und HostB verwendet. Beim Neustart des VPN-Geräts wird auch unidirektionaler Datenverkehr getestet, um das Worst-Case-Szenario zu simulieren (bei dem der Datenverkehr nur vom Host hinter dem VPN-Gerät stammt, das nicht zum neu startenden VPN-Gerät neu gestartet wird). Wie aus der Tabelle ersichtlich, kann der VPN-Tunnel mit IKE-Keepalive oder mit dem DPD-Protokoll aus dem schlimmsten Fall wiederhergestellt werden.

[2] DPD ist Teil des Unity-Protokolls. Diese Funktion ist derzeit nur auf dem Cisco VPN 300 Concentrator mit Softwareversion 3.0 und höher und auf der PIX-Firewall mit Softwareversion 6.0(1) und höher verfügbar.

Zugehörige Informationen

- Support-Seite für Cisco VPN Concentrator der Serie 3000
- Support-Seite für Cisco VPN 500 Concentrator
- PIX-Support-Seite
- IPSec-Support-Seite
- Technischer Support und Dokumentation - Cisco Systems