Rinegoziazione delle configurazioni da LAN a LAN tra Cisco VPN concentrator, Cisco IOS e dispositivi PIX

Sommario

Introduzione

In questo documento vengono riportati i risultati dei test di laboratorio della rinegoziazione del tunnel IPSec (IP Security) da LAN a LAN tra i diversi prodotti VPN di Cisco in diversi scenari, ad esempio il riavvio dei dispositivi VPN, la reimpostazione delle chiavi e la terminazione manuale delle associazioni di sicurezza IPSec (SA).

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

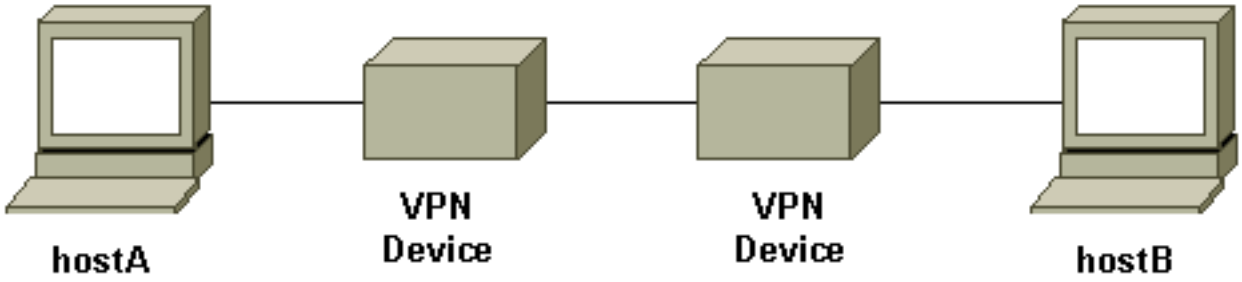
- Software Cisco IOS® versione 12.1(5)T8
- Software Cisco PIX release 6.0(1)
- Software Cisco VPN 3000 Concentrator versione 3.0(3)A
- Cisco VPN 5000 Concentrator software versione 5.2(21)

Il traffico IP utilizzato in questo test è un pacchetto ICMP (Internet Control Message Protocol) bidirezionale tra l'host A e l'host B.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Esempio di rete

Questo è un diagramma concettuale del banco di prova.



I dispositivi VPN rappresentano un router Cisco IOS, un firewall Cisco Secure PIX, un concentratore Cisco VPN 3000 o un concentratore Cisco VPN 5000.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Scenari di test

Sono stati testati tre scenari comuni. Di seguito è riportata una breve definizione degli scenari di test:

- **Terminazione manuale delle associazioni di protezione IPSec**: l'utente accede ai dispositivi VPN e cancella manualmente le associazioni di protezione IPSec tramite l'interfaccia della riga di comando (CLI) o l'interfaccia utente grafica (GUI).
- **Reimpostazione chiavi**: la normale reimpostazione delle chiavi IPSec fase I e fase II alla scadenza della durata definita. In questo test, i due dispositivi di terminazione VPN hanno la stessa durata di fase I e II configurata.
- **Riavvio del dispositivo VPN**: entrambe le estremità dei punti di terminazione del tunnel VPN sono state riavviate per simulare un'interruzione del servizio.

Nota: per i tunnel da LAN a LAN in cui viene utilizzato il concentratore VPN 5000, il concentratore viene configurato utilizzando la modalità PRINCIPALE e il risponditore del tunnel.

Risultati test

Configurazione	Interruzione manuale delle associazioni di protezione IPSec	Reimposta	Riavvio dispositivo VPN
IOS to	• Tunnel	• II	• Con IKE

PIX	ristabilito dopo la cancellazione della SA di fase I o II su entrambi i lati • Test del traffico	traffico di prova continua a funzionare dopo la fase I o la fase II della rigenerazione delle chiavi	keepalive abilitato su entrambi i dispositivi, il tunnel è stato ristabilito • Test del traffico[1] dopo il ripristino del tunnel
IOS su VPN 3000	• Tunnel ristabilito dopo la cancellazione della SA di fase I o II su entrambi i lati • Test del traffico	• Il traffico di prova continua a funzionare dopo la fase I o la fase II della rigenerazione delle chiavi	• Con IKE keepalive abilitato su entrambi i dispositivi, il tunnel è stato ristabilito • Test del traffico[1] dopo il ripristino del tunnel
IOS su VPN 5000	• Su IOS: Il traffico di prova continua a funzionare dopo la cancellazione del SA per la fase IIII tunnel VPN si disattiva quando l'associazione di sicurezza della fase I	• Il traffico di prova continua a funzionare dopo la rigenerazione della chiave	• Impossibile ripristinare il tunnel dopo il riavvio di un dispositivo VPN (con traffico di test bidirezionale) • Il traffico di

	viene cancellataIl traffico di prova smette di funzionare • Su VPN 5000: Impossibile ripristinare il tunnel dopo la cancellazione manuale dell'associazione di protezioneÈ necessario cancellare sia la fase I che la fase II SA su IOS per ristabilire il tunnel	nella fase II • La fase I della reimpostazione delle chiavi ha abbattuto il tunnel • Il traffico di prova smette di funzionare • È necessario cancellare manualmente le associazioni di protezione per ripristinare il tunnel	prova smette di funzionare • Per ripristinare il tunnel, è necessario cancellare manualmente l'associazione di sicurezza sul dispositivo che non è stata riavviata
da PIX a VPN 3000	• Tunnel ristabilito dopo la cancellazione della SA di fase I o II su entrambi i lati • Test del traffico	• Il traffico di prova continua a funzionare dopo	• Test del traffico[1] dopo il ripristino del tunnel • Con Dead Peer Detection (DPD)[2]

		la fase I o la fase II della rigenerazione delle chiavi	(abilitato per impostazione predefinita), il tunnel viene ristabilito
da PIX a VPN 5000	• Su PIX: Il traffico di prova continua a funzionare dopo la cancellazione del SA per la fase IITunnel VPN non attivo quando l'associazione di sicurezza della fase I viene cancellataIl traffico di prova smette di funzionare • Su VPN 5000: Il ripristino del tunnel non riesce dopo la cancellazione manuale dell'associazione di sicurezzaÈ necessario cancellare sia la fase I che la fase II SA sul PIX per ristabilire il tunnel	• Il traffico di prova continua a funzionare dopo la rigenerazione della chiave nella fase II • La fase I della reimpostazione delle chiavi ha abbattuto il tunnel • Il traffico di prova smette di funzionare • È necessario	• Impossibile ripristinare il tunnel dopo il riavvio di un dispositivo VPN (con traffico di test bidirezionale) • Il traffico di prova smette di funzionare • Per ripristinare il tunnel, è necessario cancellare manualmente l'associazione di sicurezza sul dispositivo che non è stata riavviata

		cancellare manualmente le associazioni di protezione per ripristinare il tunnel	
Da VPN 3000 a VPN 5000	• Su VPN 3000: Il tunnel viene ripristinato dopo la cancellazione manuale della sessioneIl traffico funziona ancora • Su VPN 5000: Impossibile ripristinare il tunnel dopo la cancellazione manuale del tunnelIl traffico di prova smette di funzionareÈ necessario cancellare l'associazione di sicurezza sulla VPN 3000 per ristabilire il tunnel	• Il traffico di prova continua a funzionare dopo la reimpostazione della fase I o II	• Impossibile ripristinare il tunnel dopo il riavvio di uno dei dispositivi VPN (con traffico di test bidirezionale) • Il traffico di prova smette di funzionare • Per ripristinare il tunnel, è necessario cancellare manualmente l'associazione di sicurezza sul dispositivo che non è stata riavviata

[1] Come descritto sopra, il traffico di test utilizzato è un pacchetto ICMP bidirezionale tra l'host A e l'host B. Nel test di riavvio del dispositivo VPN, viene anche testato il traffico unidirezionale per simulare lo scenario peggiore (dove il traffico proviene solo dall'host dietro il dispositivo VPN che non viene riavviato sul dispositivo VPN che viene riavviato). Come mostrato dalla tabella, con IKE keepalive o con il protocollo DPD, il tunnel VPN può essere ripristinato nello scenario peggiore.

[2] DPD fa parte del protocollo Unity. Attualmente questa funzione è disponibile solo sul Cisco VPN 3000 Concentrator con software versione 3.0 e successive e sul PIX Firewall con software versione 6.0(1) e successive.

Informazioni correlate

- Cisco VPN serie 3000 Concentrator Support Page
- Pagina di supporto per Cisco VPN 5000 Concentrator
- Pagina di supporto PIX
- Pagina di supporto per IPSec
- Documentazione e supporto tecnico – Cisco Systems