Heronderhandeling van LAN-to-LAN configuraties tussen Cisco VPN-connectors, Cisco IOS en PIX-apparaten

Inhoud

Inleiding

Dit document meldt de testresultaten van IP Security (IPSec) LAN-to-LAN tunnelheronderhandeling tussen verschillende Cisco VPN-producten in verschillende scenario's, zoals de herstart van VPN-apparaten, herstel en de handmatige beëindiging van IPSec security associaties (SA's).

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco IOS®-softwarerelease 12.1(5)T8
- Cisco PIX-softwarerelease 6.0(1)S
- Cisco VPN 3000 Concentrator-software versie 3.0(3)A
- Cisco VPN 5000 Concentrator-softwareversie 5.2(21)

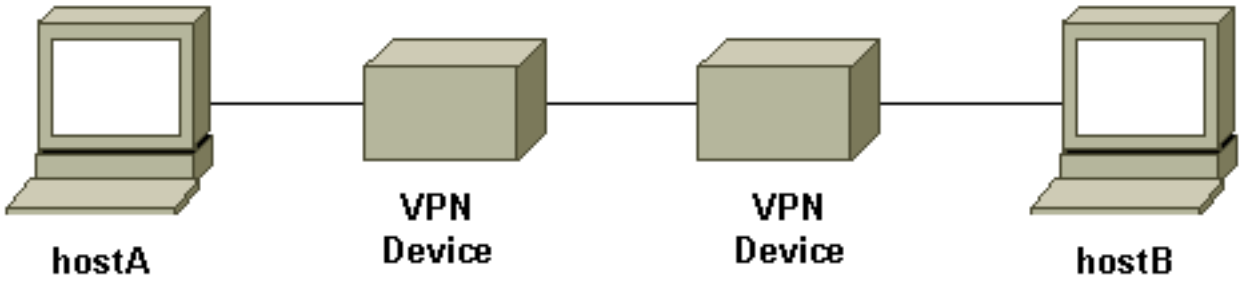
Het IP-verkeer dat in deze test wordt gebruikt, is bidirectionele pakketten van het Internet Control Message Protocol (ICMP) tussen hostA en hostB.

De informatie in dit document is gebaseerd op de apparaten in een specifieke

laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Netwerkdiagram

Dit is een ontwerpschema van het testbed.



VPN-apparaten vertegenwoordigen een Cisco IOS-router, een Cisco Secure PIX-firewall, een Cisco VPN 3000 Concentrator of een Cisco VPN 5000 Concentrator.

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

Testscenario's

Drie gemeenschappelijke scenario's werden getest. Hieronder volgt een korte omschrijving van de testscenario's:

- **Handmatige beëindiging van IPSec SAs**—Gebruiker logt in op de VPN-apparaten en reinigt handmatig de IPSec SA**'s** met behulp van de opdrachtregel interface (CLI) of de grafische gebruikersinterface (GUI).
- **Rekey**—Normale IPSec fase I en fase II gaan terug wanneer de gedefinieerde levensduur verstrijkt. In deze test hebben de twee VPN eindapparaten de zelfde fase I en fase II leven gevormd.
- **Herstart van VPN-apparaat** - of het einde van de VPN-tunneleindpunt werd herstart om serviceresources te simuleren.

Opmerking: Voor LAN-to-LAN tunnels waar de VPN 5000 Concentrator wordt gebruikt, wordt de concentrator ingesteld met behulp van de MAIN-modus en de tunnelresponder.

Testresultaten

Instellen	Beëindiging van IPSec SAs handmatig	Rekey	VPN-apparaatherstart
IOS naar PIX	• De tunnelwerking na fase I of fase	• Test nog stee	• Indien IKE op beide apparaten in

	II SA wordt aan beide zijden geklaard • Testwerkzaamheden	ds werkt na fase I of fase II rekking	stand is gehouden, wordt de tunnel hersteld • Test traffic [1] werkt na herstel van de tunnel
IOS naar VPN-router 3000	• De tunnelwerking na fase I of fase II SA wordt aan beide zijden geklaard • Testwerkzaamheden	• Test nog steeds werkt na fase I of fase II rekking	• Indien IKE op beide apparaten in stand is gehouden, wordt de tunnel hersteld • Test traffic [1] werkt na herstel van de tunnel
IOS naar VPN-router 5000	• Op IOS: Test nog werkt na fase II SAVPN-tunnel gaat omlaag als fase I wordt gewistTestverkeer stopt met werken • Op VPN 5000: Tunnel herstelt niet na handmatig opruimen van de SAMoet zowel fase I als fase II SA op IOS wissen om tunnel te herstellen	• Test nog steeds werkt na fase II rekking • Fase I rekey heeft de tunnel omlaag gebracht • Test verkeer stopt	• Tunnel herstelt niet nadat u een van beide VPN-apparaten opnieuw hebt opgestart (met bidirectionele testverkeer) • Testverkeer stopt met werken • Dient de SA handmatig te verwijderen op het apparaat dat niet is herstart om de tunnel terug te

		met werken • Moet de SA's handmatig verwijderen om de tunnel terug te brengen	brengen
PIX aan VPN 3000	• De tunnelwerking na fase I of fase II SA wordt aan beide zijden geklaard • Testwerkzaamheden	• Test nog steeds werkt na fase I of fase II rekking	• Test traffic [1] werkt na herstel van de tunnel • Met Dead Peer Detection (DPD)[2] (standaard ingeschakeld), tunnelherstel
PIX aan VPN 5000	• Over PIX: Test nog werkt na fase II SAVPN-tunnel ging omlaag toen fase I SA werd gewistTestverkeer stopt met werken • Op VPN 5000: Tunnel herstelt zich niet nadat SA handmatig is opgeklaardMoet zowel fase I als	• Test nog steeds werkt na fase II rekking • Fase I reke y heeft	• Tunnel herstelt niet nadat u een van beide VPN-apparaten opnieuw hebt opgestart (met bidirectionele testverkeer) • Testverkeer stopt met

	fase II SA op PIX ontruimen om de tunnel te herstellen	de tunnel omlaag gebracht • Test verkeer stopt met werken • Moet de SA's handmatig verwijderen om de tunnel terug te brengen	werken • Dient de SA handmatig te verwijderen op het apparaat dat niet is herstart om de tunnel terug te brengen
VPN 3000-router naar VPN 5000	• Op VPN 3000: Tunnel wordt hersteld nadat de sessie handmatig is gewistVerkeers werken • Op VPN 5000: Tunnel herstelt zich niet nadat u de tunnel handmatig hebt ontgrendeldTest verkeer stopt met werkenMoet SA op VPN 3000 ontruimen	• Test nog steeds werkt na fase I of fase II rekking	• Tunnel herstelt niet nadat u een van beide VPN-apparaten opnieuw hebt opgestart (met bidirectionele testverkeer) • Testverkeer stopt met werken • Dient de SA

	om tunnel te herstellen		handmatig te verwijderen op het apparaat dat niet is herstart om de tunnel terug te brengen

[1] Zoals hierboven beschreven, is het gebruikte testverkeer bidirectionele ICMP-pakketten tussen hostA en hostB. In de herstarttest van VPN-apparaat wordt het unidirectionele verkeer ook getest om het slechtste scenario te simuleren (waarbij het verkeer alleen van de host achter het VPN-apparaat komt en niet opnieuw wordt opgestart op het VPN-apparaat dat opnieuw wordt opgestart). Zoals uit de tabel is gebleken, kan met IKE in leven blijven of met het DPD-protocol de VPN-tunnel worden hersteld van het ergste casescenario.

[2] DPD maakt deel uit van het Unity Protocol. Deze optie is momenteel alleen beschikbaar in Cisco VPN 3000 Concentrator met softwareversie 3.0 en hoger en in de PIX-firewall met softwareversie 6.0(1) en hoger.

Gerelateerde informatie

- Ondersteuning van Cisco VPN 3000 Series Concentrator-pagina
- Ondersteuning van Cisco VPN 5000 Concentrator-pagina
- PIX-ondersteuningspagina
- IPsec-ondersteuningspagina
- Technische ondersteuning en documentatie – Cisco Systems