Configurações de LAN para LAN renegociando entre Cisco VPN concentratores, Cisco IOS, e dispositivos de PIX

Índice

Introdução

Este documento relata os resultados de teste do laboratório da negociação nova do túnel de LAN para LAN da Segurança IP (IPsec) entre produtos Cisco VPN diferentes em várias encenações, tais como a repartição do dispositivo VPN, rekey, e a terminação manual das associações de segurança IPSec (SA).

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

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

O tráfego IP usado neste teste é pacotes bidirecionais do Internet Control Message Protocol (ICMP) entre o hostA e o hostB.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de

laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Diagrama de Rede

Este é um diagrama de conceito do aparelho de teste.

Os dispositivos VPN representam um roteador do Cisco IOS, um firewall PIX segura Cisco, um Cisco VPN 3000 Concentrator ou um concentrador do Cisco VPN 5000.

Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Cenários de teste

Três cenários comuns foram testados. O seguinte é uma breve definição dos cenários de teste:

- **Terminação manual do sas de IPSec** — O usuário entra aos dispositivos VPN e cancela manualmente o sas de IPSec usando o comando line interface(cli) ou a interface gráfica de usuário (GUI).
- **Rekey** — Fase de IPSec normal eu e a fase II rekey quando o tempo de vida definido expira. Neste teste, os dois dispositivos da terminação VPN têm a mesma fase mim e vida da fase II configurada.
- **Repartição do dispositivo VPN** — Uma ou outra extremidade dos pontos de terminação de túnel VPN foi recarregada para simular a interrupção de serviço.

Nota: Para os túneis de LAN para LAN onde o VPN 5000 concentrator é usado, o concentrador é configurado usando o que responde do modo principal e do túnel.

Resultados do teste

Instalação	Manualmente terminação do sas de IPSec	Rekey	Repartição do dispositivo VPN
IO ao PIX	• O túnel restabeleceu-me após a fase ou a fase II SA é cancelada de cada lado • Trabalhos do tráfego de teste	• O tráfego de teste ainda trabalha-me após a fase	• Com o keepalive de IKE permitido em ambos os dispositivos, túnel restabelecido • O tráfego

		ou a fase II rekey	de teste[1] trabalha após o túnel recuperado
IO ao VPN 3000	• O túnel restabeleceu-me após a fase ou a fase II SA é cancelada de cada lado • Trabalhos do tráfego de teste	• O tráfego de teste ainda trabalha-me após a fase ou a fase II rekey	• Com o keepalive de IKE permitido em ambos os dispositivos, túnel restabelecido • O tráfego de teste[1] trabalha após o túnel recuperado
IO ao VPN 5000	• Em IO: O tráfego de teste ainda trabalha após a fase II SA é canceladoO túnel VPN vai abaixo de quando fase eu SA sou canceladoO tráfego de teste para de trabalhar • No VPN5000: O túnel não recupera após manualmente ter cancelado o SADevo cancelar a fase eu e a fase II SA em IO para restabelecer o túnel	• O tráfego de teste ainda trabalha após a fase II rekey • Fase onde eu rekey derrubado o túnel • O tráfego de teste para de	• O túnel não recupera após a repartição um ou outro dispositivo VPN (com tráfego de teste bidirecional) • O tráfego de teste para de trabalhar • Obrigação manualmente clara o SA no dispositivo que não foi recarregado para trazer para trás o túnel

		trabalhar • Obrigação manualmente SA claros para trazer para trás o túnel	
PIX ao VPN 3000	• O túnel restabeleceu-me após a fase ou a fase II SA é cancelada de cada lado • Trabalhos do tráfego de teste	• O tráfego de teste ainda trabalha-me após a fase ou a fase II rekey	• O tráfego de teste[1] trabalha após o túnel recuperado • Com Dead Peer Detection (DPD) [2] (permitido à revelia), túnel restabelecido
PIX ao VPN 5000	• No PIX: O tráfego de teste ainda trabalha após a fase II SA é canceladoO túnel VPN foi abaixo de quando fase eu SA sou canceladoO tráfego de teste para de trabalhar • No VPN5000: O túnel não recupera depois que manualmente espaços livres SADevo cancelar	• O tráfego de teste ainda trabalha após a fase II rekey • Fase onde eu rekey derrubado	• O túnel não recupera após a repartição um ou outro dispositivo VPN (com tráfego de teste bidirecional) • O tráfego de teste para de trabalhar • Obrigação manualmen

	a fase eu e a fase II SA no PIX para restabelecer o túnel	o túnel • O tráfego de teste para de trabalhar • Obrigação manualmente SA claros para trazer para trás o túnel	te clara o SA no dispositivo que não foi recarregado para trazer para trás o túnel
VPN 3000 ao VPN 5000	• No VPN3000: O túnel é recuperado após manualmente claro a sessãoDo tráfego trabalhos ainda • No VPN5000: O túnel não recupera após manualmente claro o túnelO tráfego de teste para de trabalharDeve cancelar o SA no VPN3000 para restabelecer o túnel	• O tráfego de teste ainda trabalha depois que fase eu ou fase II rekey	• O túnel não recupera após a repartição de um ou outro dispositivo VPN (com tráfego de teste bidirecional) • O tráfego de teste para de trabalhar • Obrigação manualmente clara o SA no dispositivo que não foi recarregado para trazer para

			trás o túnel

[1] como descrito acima, o tráfego de teste usado é pacotes ICMP bidirecionais entre o hostA e o hostB. No teste da repartição do dispositivo VPN, o tráfego unidirecional é testado igualmente para simular o cenário do pior caso (onde o tráfego é somente do host atrás do dispositivo VPN que não é recarregado ao dispositivo VPN que é recarregado). Como pode visto da tabela, com keepalive de IKE ou com protocolo DPD, o túnel VPN pode ser recuperado do cenário do pior caso.

[2] DPD são parte do protocolo de Unity. Atualmente esta característica está somente disponível no Cisco VPN 3000 Concentrator com 3.0 da versão de software e acima e no PIX Firewall com versão de software 6.0(1) e acima.

Informações Relacionadas

- Página de suporte do Cisco VPN 3000 Series Concentrator
- Página de suporte do Cisco VPN 5000 Concentrator
- Página de suporte do PIX
- Página de suporte do IPSec
- Suporte Técnico e Documentação - Cisco Systems