Renegociação de configurações de LAN para LAN entre Cisco VPN Concentrators, Cisco IOS e dispositivos PIX

Contents

Introduction

Este documento relata os resultados do teste de laboratório da renegociação de túnel LAN para LAN de Segurança IP (IPSec - IP Security) entre diferentes produtos Cisco VPN em vários cenários, como reinicialização de dispositivo VPN, rechaveamento e terminação manual de associações de segurança (SAs - Security Association) IPSec.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

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

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

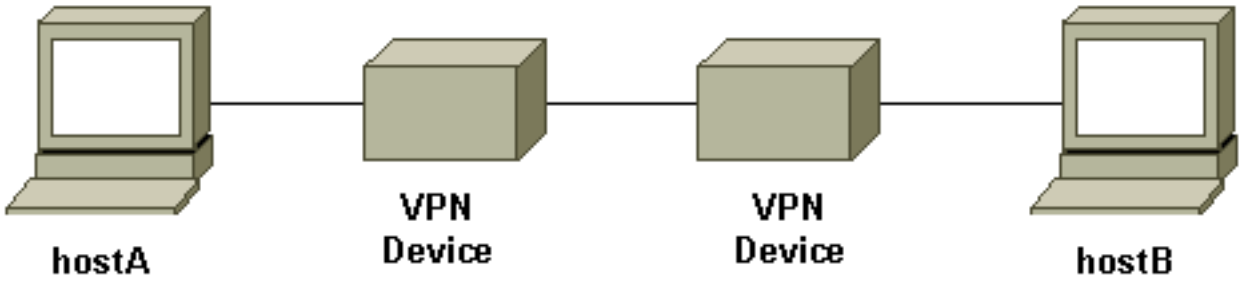
O tráfego IP usado neste teste são pacotes bidirecionais do Internet Control Message Protocol (ICMP) entre o host A e o host B.

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 Rede

Este é um diagrama de conceito do campo de teste.



Os dispositivos VPN representam um roteador Cisco IOS, um Cisco Secure PIX Firewall, um Cisco VPN 3000 Concentrator ou um Cisco VPN 5000 Concentrator.

Conventions

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

Cenários de teste

Três cenários comuns foram testados. Veja a seguir uma breve definição dos cenários de teste:

- **Terminação manual de SAs de IPSec**—O usuário faz logon nos dispositivos VPN e limpa manualmente as SAs de IPSec usando a interface de linha de comando (CLI) ou a interface gráfica do usuário (GUI).
- **Rekey** — chave de fase I e II do IPSec normal quando o tempo de vida definido expira. Neste teste, os dois dispositivos de terminação VPN têm a mesma fase I e a fase II configuradas.
- **Reinicialização do dispositivo VPN** — Qualquer extremidade dos pontos de terminação do túnel VPN foi reinicializada para simular a interrupção do serviço.

Observação: para túneis LAN a LAN em que o VPN 5000 Concentrator é usado, o concentrador é configurado usando o modo MAIN e o respondedor de túnel.

Resultados do teste

Instalação	Terminação manual de SAs IPSec	Rekey	Reinicialização do dispositivo VPN
IOS para PIX	• Túnel restabelecido após a fase I ou fase II SA ser limpo de cada lado	• O tráfego de teste ainda funci	• Com o keepalive IKE habilitado em ambos os

	• Testar trabalhos de tráfego	ona após a fase I ou a fase II	dispositivos, o túnel foi restabelecido • O tráfego de teste [1] funciona após recuperação do túnel
IOS para VPN 3000	• Túnel restabelecido após a fase I ou fase II SA ser limpo de cada lado • Testar trabalhos de tráfego	• O tráfego de teste ainda funciona após a fase I ou a fase II	• Com o keepalive IKE habilitado em ambos os dispositivos, o túnel foi restabelecido • O tráfego de teste [1] funciona após recuperação do túnel
IOS para VPN 5000	• No IOS: O tráfego de teste ainda funciona após a fase II da SA ter sido limpaO túnel VPN é desativado quando o SA da fase I é limpoO tráfego de teste para de funcionar • No VPN 5000: O túnel falha na recuperação após a limpeza manual da SADeve limpar as SAs de fase I e II no IOS para	• O tráfego de teste ainda funciona após a rechave da fase II • A fase I da rechave derrubou o túnel	• O túnel falha ao recuperar após a reinicialização de qualquer dispositivo VPN (com tráfego de teste bidirecional) • O tráfego de teste para de funcionar • Deve limpar manualmente o SA no dispositivo que não foi

	restabelecer o túnel	• O tráfego de teste para de funcionar • Deve limpar manualmente as SAs para trazer o túnel de volta	reinicializado para trazer o túnel de volta
PIX para VPN 3000	• Túnel restabelecido após a fase I ou fase II SA ser limpo de cada lado • Testar trabalhos de tráfego	• O tráfego de teste ainda funciona após a fase I ou a fase II	• O tráfego de teste [1] funciona após recuperação do túnel • Com Dead Peer Detection (DPD)[2] (ativado por padrão), o túnel foi restabelecido
PIX para VPN 5000	• No PIX: O tráfego de teste ainda funciona após a fase II da SA ter sido limpaO túnel VPN foi desativado quando o SA da fase I foi limpoO	• O tráfego de teste ainda funciona após a recha	• O túnel falha ao recuperar após a reinicialização de qualquer dispositivo VPN (com tráfego de

	tráfego de teste para de funcionar • No VPN 5000: O túnel falha ao se recuperar após o descarte manual da SADeve limpar as SA de fase I e II no PIX para restabelecer o túnel	ve da fase II • A fase I da recha ve derru bou o túnel • O tráfeg o de teste para de funci onar • Deve limpa r manu alme nte as SAs para trazer o túnel de volta	teste bidirecional) • O tráfego de teste para de funcionar • Deve limpar manualment e o SA no dispositivo que não foi reinicializad o para trazer o túnel de volta
VPN 3000 para VPN 5000	• No VPN 3000: O túnel é recuperado após a limpeza manual da sessãoO tráfego ainda funciona • No VPN 5000: O túnel não se recupera depois de limpar manualmente o túnelO tráfego de teste para de funcionarDeve	• O tráfeg o de teste ainda funci ona após a chav e de fase I ou de fase II	• O túnel falha ao recuperar após a reinicializaç ão de qualquer dispositivo VPN (com tráfego de teste bidirecional) • O tráfego de teste para de

	limpar SA no VPN 3000 para restabelecer o túnel		funcionar • Deve limpar manualmente o SA no dispositivo que não foi reinicializado para trazer o túnel de volta

[1] Conforme descrito acima, o tráfego de teste usado é de pacotes ICMP bidirecionais entre hostA e hostB. No teste de reinicialização do dispositivo VPN, o tráfego unidirecional também é testado para simular o pior cenário (onde o tráfego é somente do host por trás do dispositivo VPN que não é reinicializado para o dispositivo VPN que é reinicializado). Como pode ser visto na tabela, com o IKE keepalive ou com o protocolo DPD, o túnel VPN pode ser recuperado do pior cenário possível.

[2] DPD faz parte do protocolo Unity. Atualmente, esse recurso está disponível somente no Cisco VPN 3000 Concentrator com versão de software 3.0 e superior e no PIX Firewall com versão de software 6.0(1) e superior.

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