Cisco VPN Concentrator, Cisco IOS 및 PIX 디바이스 간 LAN-to-LAN 구성 재협상

목차

소개

이 문서에서는 VPN 디바이스 재부팅, 키 재설정, IPSec SA(Security Associations)의 수동 종료 등 다양한 시나리오에서 서로 다른 Cisco VPN 제품 간의 IP Security(IPSec) LAN-to-LAN 터널 재지정의 랩 테스트 결과를 보고합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

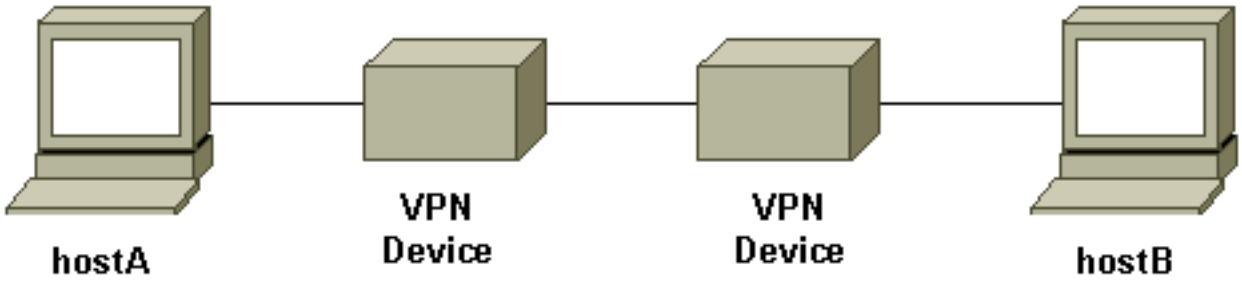
- Cisco IOS® 소프트웨어 릴리스 12.1(5)T8
- Cisco PIX Software 릴리스 6.0(1)
- Cisco VPN 3000 Concentrator 소프트웨어 버전 3.0(3)A
- Cisco VPN 5000 Concentrator 소프트웨어 버전 5.2(21)

이 테스트에 사용된 IP 트래픽은 hostA와 hostB 간의 양방향 ICMP(Internet Control Message Protocol) 패킷입니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

네트워크 다이어그램

이것은 시험대의 개념도입니다.



VPN 디바이스는 Cisco IOS 라우터, Cisco Secure PIX Firewall, Cisco VPN 3000 Concentrator 또는 Cisco VPN 5000 Concentrator를 나타냅니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참고하십시오.

테스트 시나리오

세 가지 일반적인 시나리오를 테스트했습니다. 다음은 테스트 시나리오에 대한 간단한 정의입니다.

- **IPSec SA의 수동 종료** - 사용자가 VPN 디바이스에 로그온하고 CLI(Command Line Interface) 또는 GUI(Graphical User Interface)를 사용하여 IPSec SA를 수동으로 지웁니다.
- **Rekey**(키 재설정) - 정의된 수명이 만료될 때 일반 IPSec 단계 I 및 단계 II 키 재설정 이 테스트에서는 2개의 VPN 종료 디바이스가 동일한 단계 I 및 단계 II 수명을 구성합니다.
- **VPN 디바이스 재부팅** - 서비스 중단을 시뮬레이션하기 위해 VPN 터널 종단 지점 중 하나가 재부팅되었습니다.

참고: VPN 5000 Concentrator가 사용되는 LAN-to-LAN 터널의 경우 MAIN 모드 및 터널 응답기를 사용하여 Concentrator가 구성됩니다.

테스트 결과

설정	IPSec SA 수동 종료	키 재설정	VPN 디바이스 재부팅
IOS에서 PIX로	• 1단계 또는 2단계 SA가 양쪽에서 지워진 후 터널이 재설정됨 • 트래픽 작동 테스트	• 테스트 트래픽은 I 단계 또는 I 단계 키 재설정 후에도 계속 작동합니다.	• 두 디바이스 모두에서 IKE keepalive가 활성화된 경우 터널이 재설정됨 • 터널 복구 후 트래픽 [1] 테스트

			작동
IOS-VPN 3000	• 1단계 또는 2단계 SA가 양쪽에서 지워진 후 터널이 재설정됨 • 트래픽 작동 테스트	• 테스트 트래픽은 I 단계 또는 I 단계 키 재설정 후에도 계속 작동합니다.	• 두 디바이스 모두에서 IKE keepalive가 활성화된 경우 터널이 재설정됨 • 터널 복구 후 트래픽[1] 테스트 작동
IOS-VPN 5000	• IOS에서: 테스트 트래픽은 II SA 단계가 지워진 후에도 계속 작동합니다.I SA 단계가 지워지면 VPN 터널이 다운됨테스트 트래픽의 작동이 중지됩니다. • VPN 5000에서: SA를 수동으로 지운 후 터널이 복구되지 않습니다.터널을 재설정하려면 IOS에서 I단계 및 I단계 SA를 모두 지워야 합니다.	• 테스트 트래픽은 II 단계 키 재설정 후에도 계속 작동합니다. • 1단계 키 재설정이 터널을 다운했습니다. • 테스트 트래픽의 작동이 중지됩니다. • 터널을 다시 가져오려면 수동으로 SA를 지워야 합니다.	• VPN 디바이스 중 하나를 재부팅한 후 터널이 복구되지 않음(양방향 테스트 트래픽 사용) • 테스트 트래픽의 작동이 중지됩니다. • 터널을 다시 가져오기 위해 재부팅되지 않은 디바이스에서 SA를 수동으로 지워야 합니다.
PIX-	• 1단계 또는 2단계	• 테스트	• 터널 복구

VPN 3000	SA가 양쪽에서 지워진 후 터널이 재설정됨 • 트래픽 작동 테스트	트래픽은 I 단계 또는 I 단계 키 재설정 후에도 계속 작동합니다.	후 트래픽[1] 테스트 작동 • DPD(Dead Peer Detection)[2](기본적으로 활성화됨), 터널이 재설정됨
PIX-VPN 5000	• PIX에서: 테스트 트래픽은 II SA 단계가 지워진 후에도 계속 작동합니다.I SA 단계가 지워지면 VPN 터널이 다운됨테스트 트래픽의 작동이 중지됩니다. • VPN 5000에서: SA를 수동으로 지운 후 터널이 복구되지 않습니다.터널을 다시 설정하려면 PIX에서 I단계 및 I단계 SA를 모두 지워야 합니다.	• 테스트 트래픽은 II 단계 키 재설정 후에도 계속 작동합니다. • 1단계 키 재설정이 터널을 다운했습니다. • 테스트 트래픽의 작동이 중지됩니다. • 터널을 다시 가져오려면 수동으로 SA를 지워야 합니다.	• VPN 디바이스 중 하나를 재부팅한 후 터널이 복구되지 않음(양방향 테스트 트래픽 사용) • 테스트 트래픽의 작동이 중지됩니다. • 터널을 다시 가져오기 위해 재부팅되지 않은 디바이스에서 SA를 수동으로 지워야 합니다.
VPN 3000에서	• VPN 3000에서: 수동으로 세션을 지운 후 터널이 복구	• 테스트 트래픽은 1단	• VPN 디바이스 중 하나를 재부

VPN 5000으로	됨트래픽이 여전히 작동 • VPN 5000에서: 터널을 수동으로 지운 후 터널이 복구되지 않습니다.테스트 트래픽의 작동이 중지됩니다.터널을 다시 설정하려면 VPN 3000에서 SA를 지워야 합니다.	계 또는 2단계 키 재설정 후에도 계속 작동합니다.	팅한 후 터널이 복구되지 않습니다(양방향 테스트 트래픽 사용). • 테스트 트래픽의 작동이 중지됩니다. • 터널을 다시 가져오기 위해 재부팅되지 않은 디바이스에서 SA를 수동으로 지워야 합니다.

[1] 위에서 설명한 대로 사용된 테스트 트래픽은 hostA와 hostB 간의 양방향 ICMP 패킷입니다. VPN 디바이스 재부팅 테스트에서는 단방향 트래픽도 테스트되어 최악의 경우(여기서 트래픽은 리부팅되지 않은 VPN 디바이스로 리부팅되지 않은 VPN 디바이스 뒤에 있는 호스트에서만) 시나리오를 시뮬레이션합니다. 표에서 볼 수 있듯이, IKE keepalive 또는 DPD 프로토콜을 사용하여 VPN 터널을 최악의 시나리오에서 복구할 수 있습니다.

[2] DPD는 Unity 프로토콜의 일부입니다. 현재 이 기능은 소프트웨어 버전 3.0 이상이 설치된 Cisco VPN 3000 Concentrator 및 소프트웨어 버전 6.0(1) 이상이 설치된 PIX 방화벽에서만 사용할 수 있습니다.

관련 정보

- Cisco VPN 3000 Series Concentrator 지원 페이지
- Cisco VPN 5000 Concentrator 지원 페이지
- PIX 지원 페이지
- IPSec 지원 페이지
- 기술 지원 및 문서 – Cisco Systems