Cisco VPN 5000 Concentrator Series용 가상 사설 네트워크 및 인터넷 키 교환

목차

소개

IKE(Internet Key Exchange)는 안전한 인증된 통신을 정렬하는 데 사용되는 표준 방법입니다.Cisco VPN 5000 Concentrator는 IKE를 사용하여 IPSec 터널을 설정합니다.이 IPSec 터널은 이 제품의 백본입니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- VPN 5000 Series Concentrator

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.

표기 규칙

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

IKE 작업

IKE는 다음 작업을 처리합니다.

- 인증
- 세션 협상
- 키 교환
- IPSec 터널 협상 및 구성

인증

인증은 IKE가 수행하는 가장 중요한 작업이며 가장 복잡합니다.협상할 때마다 누구와 협상하는지 아는 것이 중요하다.IKE는 여러 방법 중 하나를 사용하여 협상 상대방을 인증할 수 있습니다.

- **공유 키** - IKE는 해싱 기술을 사용하여 동일한 키를 가진 사용자만 IKE 패킷을 전송할 수 있도록 합니다.
- **DSS(Digital Signature Standard) 또는 Rivest, Shamir, Adelman(RSA) 디지털 서명** - IKE는 공개 키 디지털 서명 암호화를 사용하여 각 당사자가 누구인지를 확인합니다.
- **RSA 암호화** - IKE는 두 가지 방법 중 하나를 사용하여 협상을 충분히 암호화하여 올바른 개인 키를 가진 당사자만 협상을 계속할 수 있도록 합니다.

세션 협상
세션 협상 중에 IKE는 당사자가 인증을 수행하는 방법과 향후 협상(즉, IPSec 터널 협상)을 보호하는 방법을 협상할 수 있도록 합니다. 이러한 항목은 협상됩니다.

- **인증 방법** - 이 문서의 인증 섹션에 나열된 방법 중 하나입니다.
- **키 교환 알고리즘** - 공용 미디어(Diffie-Hellman)를 통해 암호화 키를 안전하게 교환하기 위한 수학적 기술입니다. 키는 암호화 및 패킷 서명 알고리즘에 사용됩니다.
- **암호화 알고리즘** - DES(Data Encryption Standard) 또는 3DES(Triple Data Encryption Standard)
- **패킷 서명 알고리즘** - MD5(Message Digest 5) 및 SHA-1(Secure Hash Algorithm 1).

키 교환

IKE는 협상된 키 교환 방법(이 문서의 세션 협상 섹션 참조)을 사용하여 향후 트랜잭션을 보호하기 위해 충분한 암호화 키 자료를 생성합니다.이 방법을 사용하면 각 IKE 세션이 새로운 보안 키 세트로 보호됩니다.

인증, 세션 협상 및 키 교환은 IKE 협상 중 1단계를 구성합니다.VPN 5000 Concentrator의 경우 이러한 속성은 Protection 키워드를 통해 **IKE Policy** 섹션에 구성됩니다.이 키워드는 세 개의 항목이 있는 레이블입니다.인증 알고리즘, 암호화 알고리즘 및 키 교환 알고리즘조각들은 밑줄로 구분되어 있다.MD5_DES_G1 레이블은 IKE 패킷 인증에 MD5를 사용하고, IKE 패킷 암호화에 DES를 사용하고, 키 교환에 Diffie-Hellman 그룹 1을 사용함을 의미합니다.자세한 내용은 IPSec 터널 보안을 위한 IKE 정책 구성을 참조하십시오.

IPSec 터널 협상 및 구성

IKE가 정보 교환에 대한 보안 방법(1단계) 협상을 완료한 후 IKE를 사용하여 IPSec 터널을 협상합니다.이는 IKE 2단계를 사용하여 수행됩니다.이 교환에서 IKE는 IPSec 터널에서 사용할 새로운 키

자료를 생성합니다(IKE 1단계 키를 기반으로 사용하거나 새 키 교환을 수행하여). 이 터널에 대한 암호화 및 인증 알고리즘도 협상됩니다.

IPSec 터널은 VPN 클라이언트 터널의 VPN Group(이전의 STEP(Secure Tunnel Establish Protocol) Client) 섹션 및 LAN-to-LAN 터널의 Tunnel Partner 섹션을 사용하여 구성됩니다.VPN **Users(VPN 사용자)** 섹션에서는 각 사용자에 대한 인증 방법을 저장합니다.이러한 섹션은 IPSec 터널 보안을 위한 IKE 정책 구성에 설명되어 있습니다.

VPN 5000 Concentrator IKE Extensions

- **RADIUS** - IKE는 RADIUS 인증을 지원하지 않습니다.RADIUS 인증은 VPN 클라이언트에서 첫 번째 IKE 패킷 이후에 발생하는 특수 정보 교환에서 수행됩니다.PAP(Password Authentication Protocol)가 필요한 경우 특수 RADIUS 인증 암호가 필요합니다.자세한 내용은 Configuring the IKE Policy for IPSec Tunnel Security(IPSec 터널 보안을 위한 IKE 정책 구성에서 NoCHAP 및 PAPAuthSecret의 설명서를 참조하십시오.RADIUS 인증은 인증되고 암호화됩니다.PAP 교환은 PAPAuthSecret에 의해 보호됩니다.그러나 전체 IntraPort에 이러한 비밀번호가 하나뿐이므로 공유 비밀번호와 같이 보호가 취약합니다.
- **SecurID** - IKE는 현재 SecurID 인증을 지원하지 않습니다.SecurID 인증은 1단계와 2단계 사이에 특수 정보 교환에서 수행됩니다.이 교환은 1단계에서 협상된 IKE SA(Security Association)에 의해 완전히 보호됩니다.
- **STAMP(Secure Tunnel Access Management Protocol)** - VPN 클라이언트 연결은 IKE 프로세스 중에 IntraPort와 정보를 교환합니다.마지막 2개의 IKE 패킷 동안 비공개 페이로드에서 전송되는 비밀, 터널링할 IP 네트워크 또는 IPX(Internetwork Packet Exchange) 트래픽을 터널링할지 여부 등의 정보.이러한 페이로드는 호환되는 VPN 클라이언트에만 전송됩니다.

ISAKMP 및 오크리

ISAKMP(Internet Security Association and Key Management Protocol)는 인터넷(예: IP 프로토콜 사용)에서 협상을 수행하는 데 사용되는 언어입니다. 오클리는 암호 키 자료의 인증된 교환을 수행하는 방법입니다.IKE는 이 두 가지를 하나의 패키지로 묶어 보안 연결이 안전하지 않은 인터넷 전체에 설정되도록 합니다.

단계 및 스탬프

STEP(Secure Tunnel Establish Protocol)은 VPN 시스템의 이전 이름입니다.IKE 이전 날짜에서는 STAMP를 사용하여 IPSec 연결을 협상했습니다.3.0 이전 버전의 VPN 클라이언트 에서는 STAMP를 사용하여 IntraPort와의 연결을 설정합니다.

관련 정보

- Cisco VPN 5000 Series Concentrator 판매 중단 발표
- Router-to-VPN 5000 Series Concentrator LAN-to-LAN 터널 구성
- Cisco VPN 5000 Concentrator 제품 지원 페이지
- Cisco VPN 5000 클라이언트 제품 지원 페이지
- IPSec 협상/IKE 프로토콜 기술 지원
- 기술 지원 및 문서 – Cisco Systems