귀사에 적합한 VPN 솔루션은 무엇입니까?

목차

소개

VPN(Virtual Private Networks)은 더 저렴하고 더 유연한 방식으로 광역 전체에 네트워크를 구축하는 방식으로 점점 더 인기를 끌고 있습니다.기술의 발전으로 VPN 솔루션 구현을 위한 다양한 옵션이 증가하고 있습니다.이 기술 노트에서는 이러한 옵션 중 일부를 설명하고 가장 잘 사용할 수 있는 위치를 설명합니다.

시작하기 전에

표기 규칙

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

사전 요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

참고: Cisco는 Cisco Secure PIX Firewall, Cisco VPN 3000 Concentrator 및 Cisco VPN 5000

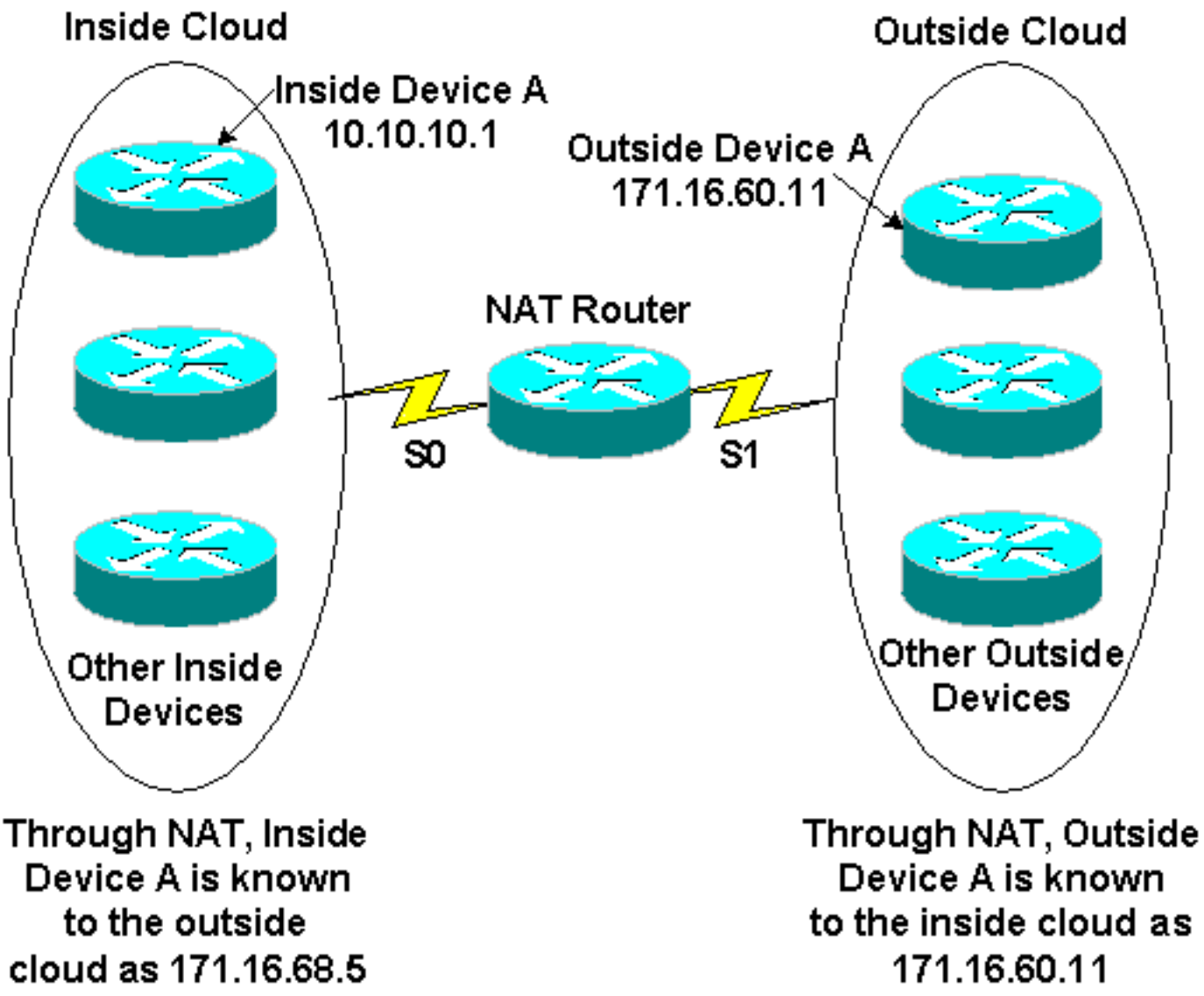
Concentrator를 비롯한 비 IOS 플랫폼에서도 암호화를 지원합니다.

NAT

인터넷의 폭발적인 성장은 단기간에 예견할 수 있는 수준을 훨씬 넘어 이미 예견된 것이다.IP 버전 4.0에서 사용할 수 있는 주소의 수가 제한되어 있다는 것은 이러한 증가의 증거이며, 그 결과 주소 공간이 점점 더 줄어들고 있다는 것입니다.이 문제의 한 가지 해결 방법은 NAT(Network Address Translation)입니다.

NAT를 사용하면 외부(일반적으로 인터넷)에서 하나 또는 몇 개의 등록된 주소를 볼 수 있는 것과 같은 내부/외부 경계에 라우터가 구성되며, 내부 주소는 사설 주소 지정 체계를 사용하는 임의의 수의 호스트를 포함할 수 있습니다.주소 변환 체계의 무결성을 유지하려면 내부(사설) 네트워크와 외부(공용) 네트워크 사이의 모든 경계 라우터에 NAT를 구성해야 합니다.보안 관점에서 NAT의 장점 중 하나는 연결을 허용하도록 NAT 게이트웨이를 특별히 구성하지 않는 한 사설 네트워크의 시스템이 외부 네트워크에서 들어오는 IP 연결을 수신할 수 없다는 것입니다.또한 NAT는 소스 및 대상 디바이스에 완전히 투명합니다.NAT의 권장 작업에는 적절한 프라이빗 네트워크 주소 지정 체계를 개괄적으로 설명하는 RFC 1918 이 포함됩니다.NAT의 표준은 RFC1631에 설명되어 있습니다 .

다음 그림은 내부 변환 네트워크 주소 풀이 있는 NAT 라우터 경계 정의를 보여줍니다.



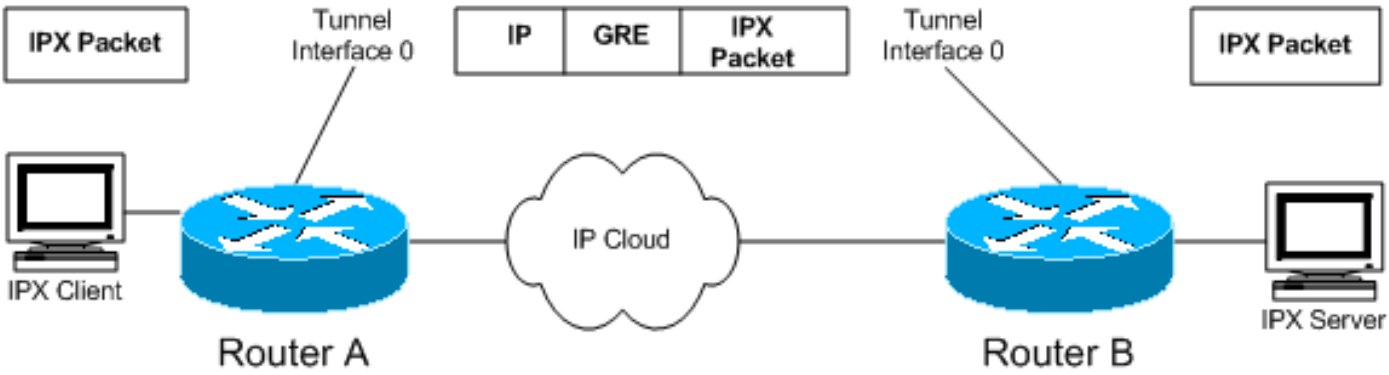
NAT는 일반적으로 인터넷에서 라우팅 가능한 IP 주소를 보존하는 데 사용되며, 비용이 많이 들고

개수가 제한됩니다.NAT는 또한 인터넷에서 내부 네트워크를 숨겨 보안을 제공합니다.

NAT 작업에 대한 자세한 내용은 NAT 작동 방식을 참조하십시오.

GRE 캡슐화 터널링

GRE(Generic Routing Encapsulation) 터널은 공유 WAN을 통해 특정 경로를 제공하고, 트래픽을 새 패킷 헤더로 캡슐화하여 특정 목적지로 전달하도록 합니다.트래픽은 엔드포인트에서만 터널에 들어갈 수 있으며 다른 엔드포인트에서만 남겨둘 수 있으므로 네트워크는 전용입니다.터널은 진정한 기밀성을 제공하지 않지만(암호화 방식) 암호화된 트래픽을 전달할 수 있습니다.터널은 트래픽을 전달하는 물리적 인터페이스에 구성된 논리적 엔드포인트입니다.



다이어그램에 나와 있는 것처럼 GRE 터널링을 사용하여 비 IP 트래픽을 IP로 캡슐화하고 인터넷 또는 IP 네트워크를 통해 전송할 수도 있습니다.IPX(Internet Packet Exchange) 및 AppleTalk 프로토콜은 비 IP 트래픽의 예입니다.GRE 구성에 대한 자세한 내용은 GRE 구성의 "GRE 터널 인터페이스 구성"을 참조하십시오.

IPX 또는 AppleTalk와 같은 다중 프로토콜 네트워크가 있고 인터넷 또는 IP 네트워크를 통해 트래픽을 전송해야 하는 경우 GRE가 적합한 VPN 솔루션입니다.또한 GRE 캡슐화는 일반적으로 IPSec과 같은 트래픽을 보호하는 다른 방법과 함께 사용됩니다.

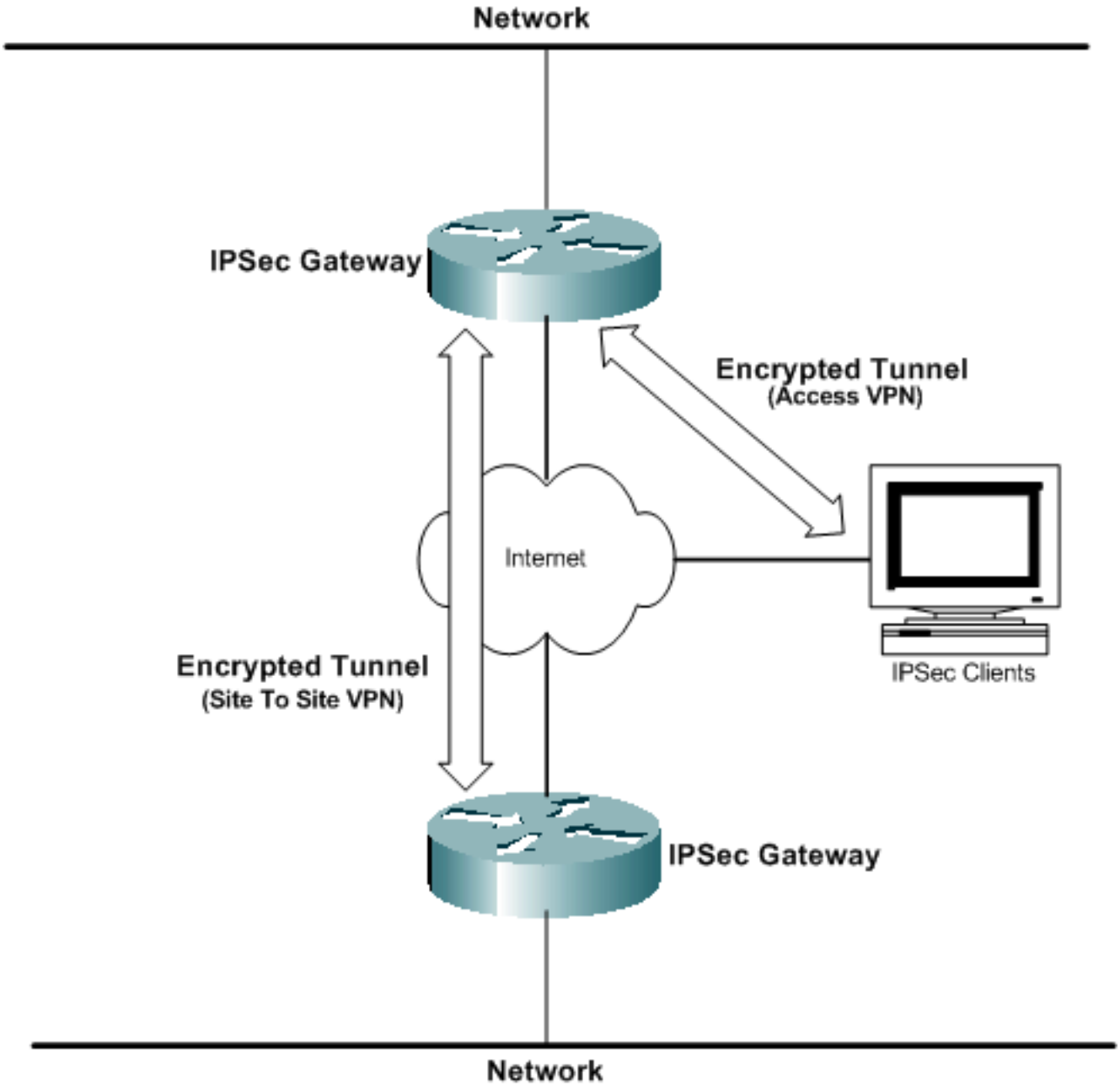
GRE에 대한 자세한 기술 정보는 RFC 1701 및 RFC 2784를 참조하십시오.

IPSec 암호화

공유 네트워크를 통해 전송되는 데이터의 암호화는 VPN과 가장 자주 연결된 VPN 기술입니다.Cisco는 IPSec(IP Security) 데이터 암호화 방법을 지원합니다.IPSec은 네트워크 레이어의 참여 피어 간에 데이터 기밀성, 데이터 무결성 및 데이터 인증을 제공하는 개방형 표준의 프레임워크입니다.

IPSec 암호화는 IPSec 클라이언트 소프트웨어에서 DES(Data Encryption Standard) 56비트 및 3DES(Triple DES) 168비트 대칭 키 암호화 알고리즘을 지원하는 IETF(Internet Engineering Task Force) 표준입니다.GRE 컨피그레이션은 IPSec에서 선택 사항입니다.IPSec은 인증 기관 및 IKE(Internet Key Exchange) 협상을 지원합니다.IPSec 암호화는 클라이언트, 라우터 및 방화벽 간에 독립형 환경에서 구축하거나 액세스 VPN에서 L2TP 터널링과 함께 사용할 수 있습니다.IPSec은 다양한 운영 체제 플랫폼에서 지원됩니다.

IPSec 암호화는 네트워크에 대한 진정한 데이터 기밀성을 원하는 경우 적합한 VPN 솔루션입니다.IPSec은 개방형 표준이므로 서로 다른 장치 간의 상호 운용성을 손쉽게 구현할 수 있습니다.



PPTP 및 MPPE

PPTP(Point-to-Point Tunneling Protocol)는 Microsoft에서 개발했습니다.RFC2637에 설명되어 있습니다 .PPTP는 Windows 9x/ME, Windows NT, Windows 2000 및 Windows XP 클라이언트 소프트웨어에 널리 구축되어 자발적 VPN을 지원합니다.

Microsoft MPPE(Point-to-Point Encryption)는 RC4 기반 40비트 또는 128비트 암호화를 사용하는 Microsoft의 정보 IETF 초안입니다.MPPE는 Microsoft의 PPTP 클라이언트 소프트웨어 솔루션의 일부이며 자발적 모드 액세스 VPN 아키텍처에서 유용합니다.PPTP/MPPE는 대부분의 Cisco 플랫폼에서 지원됩니다.

Cisco 7100 및 7200 플랫폼의 Cisco IOS Software 릴리스 12.0.5.XE5에 PPTP 지원이 추가되었습니다.Cisco IOS 12.1.5.T에 더 많은 플랫폼에 대한 지원이 추가되었습니다.Cisco Secure PIX Firewall 및 Cisco VPN 3000 Concentrator에는 PPTP 클라이언트 연결에 대한 지원도 포함됩니다.

PPTP는 비 IP 네트워크를 지원하므로 원격 사용자가 기업 네트워크에 전화를 걸어 이기종 기업 네트워크에 액세스해야 하는 경우에 유용합니다.

PPTP 구성에 대한 자세한 내용은 PPTP 구성을 참조하십시오.

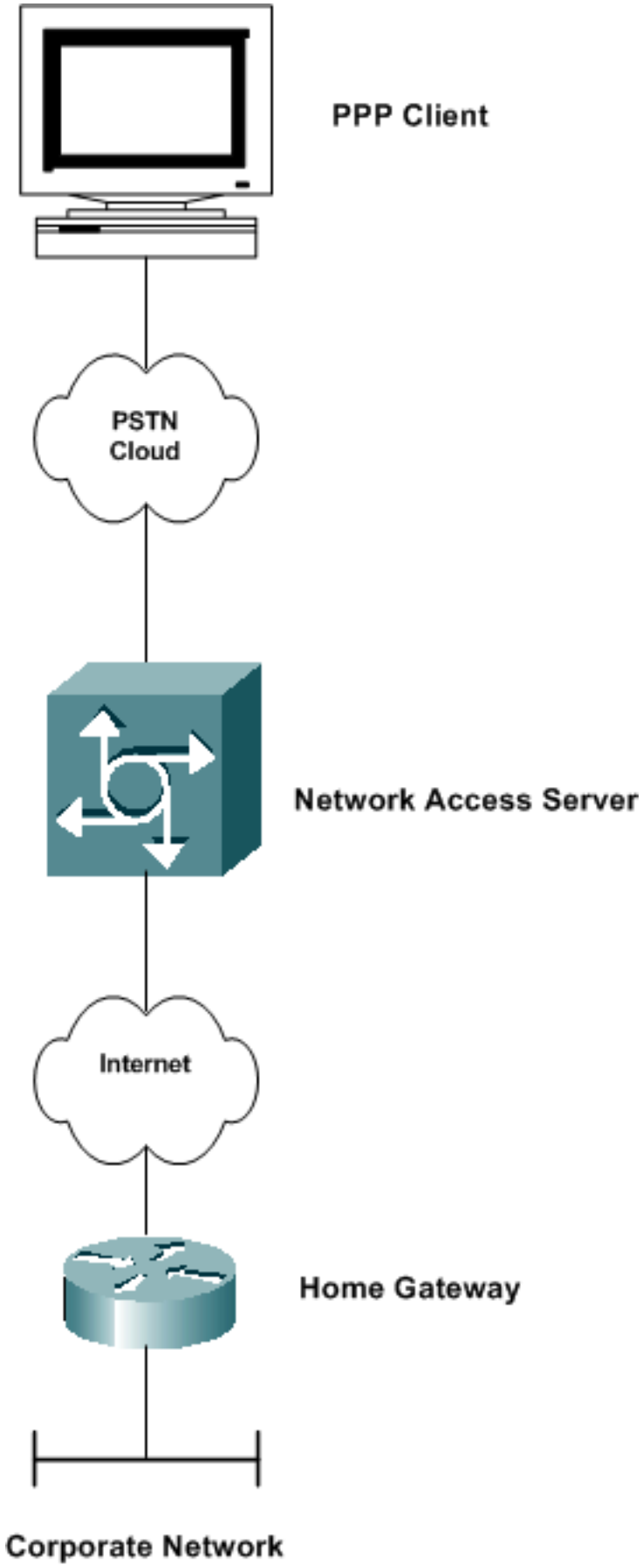
VPDN 및 L2TP

VPDN

VPDN(Virtual Private Dialup Network)은 전용 네트워크 다이얼인 서비스가 원격 액세스 서버에 걸쳐 분산되도록 허용하는 Cisco 표준입니다.VPDN의 맥락에서 전화를 거는 액세스 서버(예: AS5300)는 일반적으로 NAS(Network Access Server)라고 합니다. 전화 접속 사용자의 대상을 HGW(홈 게이트웨이)라고 합니다.

기본 시나리오는 PPP(Point-to-Point Protocol) 클라이언트가 로컬 NAS에 전화를 거는 것입니다 .NAS는 PPP 세션을 해당 클라이언트의 홈 게이트웨이 라우터로 전달해야 한다고 결정합니다.그런 다음 HGW가 사용자를 인증하고 PPP 협상을 시작합니다.PPP 설정이 완료되면 모든 프레임이 NAS를 통해 클라이언트 및 홈 게이트웨이로 전송됩니다.이 방법은 여러 프로토콜과 개념을 통합합니다.

VPDN 구성에 대한 자세한 내용은 *보안 기능* 구성*에서 가상 사설 전화 접속 네트워크 구성*을 참조하십시오.



L2TP

L2TP(Layer 2 Tunneling Protocol)는 PPTP 및 L2F의 최상의 특성을 통합하는 IETF 표준입니다 .L2TP 터널은 주로 IP 및 비 IP 트래픽 모두에 대한 필수 모드(즉, NAS에서 HGW로 전화 접속) 액세스 VPN에서 사용됩니다.Windows 2000 및 Windows XP는 VPN 클라이언트 연결 수단으로서 이 프

로토콜에 대한 기본 지원을 추가했습니다.

L2TP는 인터넷과 같은 공용 네트워크에서 IP를 사용하여 PPP를 터널링하는 데 사용됩니다.터널이 레이어 2에서 발생하므로 상위 레이어 프로토콜은 터널을 인식하지 못합니다.GRE와 마찬가지로 L2TP는 모든 레이어 3 프로토콜을 캡슐화할 수 있습니다.UDP 포트 1701은 터널의 개시자가 L2TP 트래픽을 전송하는 데 사용됩니다.

참고: 1996년에 Cisco는 VPDN 연결이 발생할 수 있도록 L2F(Layer 2 Forwarding) 프로토콜을 생성했습니다.L2F는 다른 기능에서도 계속 지원되지만 L2TP로 대체되었습니다.PPTP(Point-to-Point Tunneling Protocol)도 1996년에 생성되었으며 IETF에서 인터넷 초안을 작성했습니다.PPTP는 PPP 연결을 위해 GRE와 유사한 기능을 제공했습니다.

L2TP에 대한 자세한 내용은 레이어 2 터널 프로토콜을 참조하십시오.

PPPoE

PPPoE(PPPoE)는 주로 DSL(Digital Subscriber Line) 환경에 구축되는 정보 RFC입니다.PPPoE는 기존 이더넷 인프라를 활용하여 사용자가 동일한 LAN 내에서 여러 PPP 세션을 시작할 수 있도록 합니다.이 기술을 통해 사용자는 단일 원격 액세스 연결을 통해 여러 대상에 동시에 연결할 수 있는 새로운 애플리케이션인 레이어 3 서비스를 선택할 수 있습니다.PAP(Password Authentication Protocol) 또는 CHAP(Challenge Handshake Authentication Protocol)를 사용하는 PPPoE는 원격 라우터가 연결된 중앙 사이트에 알리는 데 자주 사용됩니다.

PPPoE는 주로 통신 사업자 DSL 구축 및 브리징 이더넷 토폴로지에서 사용됩니다.

PPPoE 구성에 대한 자세한 내용은 이더넷을 통한 PPPoE 및 IEEE 802.1Q VLAN 구성을 참조하십시오.

MPLS VPN

MPLS(Multiprotocol Label Switching)는 Cisco Tag Switching을 기반으로 하는 새로운 IETF 표준으로, 공급자가 액세스, 인트라넷 및 엑스트라넷 VPN 서비스를 비용 효율적으로 제공하는 데 필요한 자동화된 프로비저닝, 신속한 배포 및 확장성 기능을 지원합니다.Cisco는 MPLS 지원 VPN 서비스로 원활하게 전환하기 위해 서비스 제공업체와 긴밀히 협력하고 있습니다.MPLS는 레이블 기반 패러다임에서 작동하며, 패킷이 사업자 네트워크에 들어올 때 패킷을 태깅하여 연결 없는 IP 코어를 통해 신속하게 전달하도록 합니다.MPLS는 경로 구별자를 사용하여 VPN 멤버십을 식별하고 VPN 커뮤니티 내에서 트래픽을 포함합니다.

또한 MPLS는 트래픽 흐름이 아닌 토폴로지 정보를 기반으로 생성되는 레이블 전환 경로를 설정하여 IP 라우팅 패러다임에 연결 지향 접근 방식의 이점을 추가합니다.MPLS VPN은 통신 사업자 환경에 광범위하게 구축됩니다.

MPLS VPN 구성에 대한 자세한 내용은 기본 MPLS VPN 구성을 참조하십시오.

관련 정보

- IPSec 지원 페이지
- 가상 사설 네트워크의 작동 방식
- NAT 지원 페이지

- GRE 지원 페이지
- VPDN 지원 페이지
- PPTP 지원 페이지
- PPPoE 지원 페이지
- Technical Support - Cisco Systems