가상 사설 네트워크의 작동 방식

목차

소개

이 문서에서는 기본 VPN 구성 요소, 기술, 터널링, VPN 보안과 같은 VPN의 기본 사항을 다룹니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

표기 규칙

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

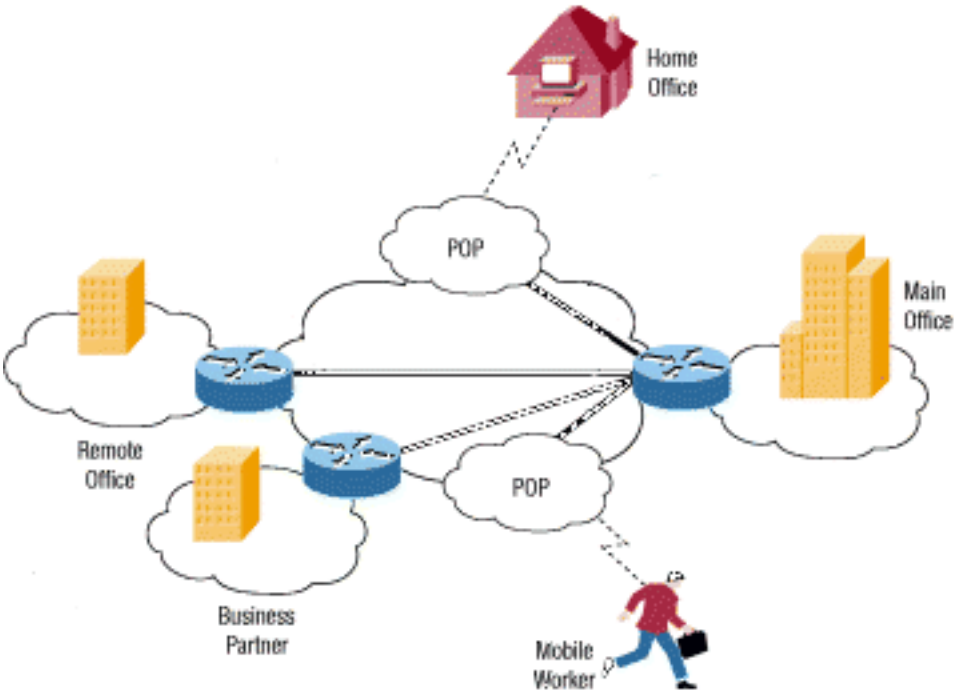
배경 정보

지난 20년 동안 세상은 많이 변했습니다.이제 많은 기업이 현지 또는 지역적 문제를 해결하는 대신 글로벌 시장과 물류 문제에 대해 생각해야 합니다.많은 회사들이 전국 또는 심지어 전 세계에 걸쳐 시설을 가지고 있습니다.그러나 모든 기업이 필요로 하는 한 가지 사항이 있습니다.사무실 위치에 관계없이 빠르고 안전하며 안정적인 통신을 유지할 수 있는 방법.

최근까지 안정적인 통신으로 임대 회선을 사용하여 WAN(Wide Area Network)을 유지할 수 있었습

니다. 144Kbps로 실행되는 ISDN(Integrated Services Digital Network)에서 155Mbps로 실행되는 OC3(Optical Carrier-3) 광선에 이르는 임대 회선은 회사가 가까운 지리적 범위를 넘어 개인 네트워크를 확장할 수 있는 방법을 제공합니다.WAN은 인터넷과 같은 공용 네트워크에 비해 신뢰성, 성능 및 보안과 관련하여 확실한 이점을 제공합니다.하지만 WAN 유지 관리, 특히 임대 회선을 사용할 경우 비용이 상당히 많이 들 수 있습니다(사무실 간 거리가 늘어나면 비용이 많이 절감되는 경우가 종종 있음). 또한 임대 회선은 인력 중 일부가 이동성이 매우 높고(마케팅 직원의 경우처럼) 기업 네트워크에 원격으로 연결하고 중요한 데이터에 자주 액세스해야 하는 조직에 적합한 솔루션이 아닙니다.

인터넷의 인기가 높아짐에 따라 기업들은 자체 네트워크를 확장하기 위한 수단으로 이 기술에 눈을 돌렸습니다.처음에는 회사 직원들에게만 사용하도록 설계된 사이트인 인트라넷이 왔다.이제 많은 기업이 원격 직원과 원격 사무실의 요구를 수용하기 위해 자체 VPN(Virtual Private Network)을 구축합니다.



일반적인 VPN은 회사의 본사에 주 LAN(Local-Area Network)을, 원격 사무실 또는 시설에 다른 LAN을, 현장 외부에서 연결하는 개별 사용자를 포함할 수 있습니다.

VPN은 공용 네트워크(일반적으로 인터넷)를 사용하여 원격 사이트 또는 사용자를 함께 연결하는 사설 네트워크입니다.VPN은 임대 회선과 같은 전용 실제 연결을 사용하는 대신 인터넷을 통해 라우팅된 "가상" 연결을 회사의 사설 네트워크에서 원격 사이트 또는 직원까지 사용합니다.

VPN을 만드는 이유

VPN에는 두 가지 일반적인 유형이 있습니다.

- **원격 액세스**—VPDN(Virtual Private Dial-up Network)이라고도 하며, 다양한 원격 위치에서 개인 네트워크에 연결해야 하는 직원이 있는 회사에서 사용하는 사용자-LAN 연결입니다.일반적으로 대규모 원격 액세스 VPN을 설정하려는 기업은 인터넷 서비스 공급자(ISP)를 사용하여 사용자에게 일종의 인터넷 전화 접속 계정을 제공합니다. 재택 근무자는 1-800 번호로 전화를 걸어 인터넷에 접속하고 VPN 클라이언트 소프트웨어를 사용하여 기업 네트워크에 액세스할 수 있습니다.원격 액세스 VPN을 필요로 하는 기업의 좋은 예로는 수백 명의 영업 인력을 보유한

대규모 기업이 있습니다.원격 액세스 VPN은 서드파티 서비스 제공자를 통해 회사의 개인 네트워크와 원격 사용자 간에 안전하고 암호화된 연결을 허용합니다.

- **Site-to-Site**—전용 장비 및 대규모 암호화를 통해 인터넷 등의 공용 네트워크를 통해 여러 고정 사이트를 연결할 수 있습니다.각 사이트에는 동일한 공용 네트워크에 대한 로컬 연결만 필요하므로 사설 임대 회선에 대한 비용이 절약됩니다.Site-to-Site VPN은 인트라넷 또는 엑스트라넷으로 더욱 분류될 수 있습니다.같은 회사의 사무실 간에 구축된 사이트 간 VPN은 인트라넷 VPN이라고 하며, 회사를 파트너 또는 고객에게 연결하기 위해 구축된 VPN은 익스트라넷 VPN이라고 합니다.

잘 설계된 VPN은 기업에 큰 도움이 될 수 있습니다.예를 들어 다음과 같은 작업을 수행할 수 있습니다.

- 지리적 연결 확장
- 기존 WAN에 비해 운영 비용 절감
- 원격 사용자의 전송 시간 및 출장 비용 절감
- 생산성 향상
- 네트워크 토폴로지 간소화
- 글로벌 네트워킹 기회 제공
- 재택 근무자 지원 제공
- 기존 WAN보다 빠른 ROI(투자 수익) 제공

잘 설계된 VPN에는 어떤 기능이 필요합니까?다음과 같은 항목을 통합해야 합니다.

- 보안
- 신뢰성
- 확장성
- 네트워크 관리
- 정책 관리

비유:각 LAN은 IsLANd입니다.

여러분이 거대한 바다에 있는 섬에 살고 있다고 상상해 보세요.여러분 주위에는 수천 개의 다른 섬들이 있고, 일부는 매우 가깝고 다른 섬들은 더 멀리 있습니다.일반적인 여행 방법은 섬에서 어느 섬에 가고자 하는 섬으로 배를 타는 것이다.페리를 타고 여행하는 것은 사생활을 거의 가지고 있지 않다는 것을 의미한다.당신이 하는 모든 것은 다른 사람이 볼 수 있습니다.

각 섬이 전용 LAN을 나타내고 바다가 인터넷이라고 가정합니다.페리를 타고 여행할 때 인터넷을 통해 웹 서버 또는 다른 장치에 연결할 때와 비슷합니다.여러분은 인터넷을 구성하는 와이어와 라우터를 제어할 수 없습니다. 마치 페리에 있는 다른 사람들을 제어할 수 없는 것처럼 말입니다.따라서 공용 리소스를 사용하여 두 프라이빗 네트워크 간에 연결을 시도하면 보안 문제가 발생할 수 있습니다.

당신의 섬은 사람들이 그 두 섬 사이를 더 쉽고, 더 안전하고, 직접적인 방법으로 여행할 수 있도록 다른 섬으로 다리를 건설하기로 결심합니다.연결 중인 섬이 매우 가깝지만 다리를 세우고 유지하는 것은 비용이 많이 듭니다.하지만 안정적이고 안전한 경로가 필요한 것은 너무 커서 어쨌든 가능합니다.당신의 섬은 훨씬 더 멀리 있는 두 번째 섬에 연결하기를 원하지만 당신은 그것이 너무 비싸다고 판단합니다.

이 상황은 임대 회선을 가지는 것과 매우 비슷합니다.브리지(임대 회선)는 해양(인터넷)과 분리되지만 섬(LAN)을 연결할 수 있습니다. 많은 기업이 원격 사무실 연결에 있어서 보안과 신뢰성이 필요하기 때문에 이 경로를 선택했습니다.하지만 사무실 간격이 아주 멀리 떨어져 있으면 먼 다리를 건설

하려는 것처럼 비용이 엄청나게 많이 들 수 있습니다.

그렇다면 VPN은 이러한 유사점에 어떻게 부합할까요?우리는 우리의 섬의 각 개체들에게 이러한 특성으로 그들 자신의 작은 잠수함을 제공할 수 있습니다.

- 빠릅니다.
- 어디를 가든지 너와 함께 하는 것은 쉬워.
- 그것은 다른 어떤 배나 잠수함으로부터 당신을 완전히 숨길 수 있습니다.
- 그것은 믿을 수 있다.
- 최초 도입 후 잠수함 추가도 비용이 별로 들지 않는다.

비록 그들이 다른 교통과 함께 바다에서 여행하고 있지만, 우리의 두 섬의 주민들은 사생활과 안전을 가지고 그들이 원할 때마다 앞뒤로 이동할 수 있습니다.이는 VPN이 작동하는 방식입니다.네트워크의 각 원격 구성원은 인터넷을 사설 LAN에 연결하는 매체로 사용하여 안전하고 안정적인 방식으로 통신할 수 있습니다.VPN은 임대 회선보다 훨씬 쉽게 더 많은 사용자와 다른 위치를 수용할 수 있도록 확장할 수 있습니다.사실 확장성은 VPN이 일반적인 임대 회선보다 더 큰 장점입니다.관련 거리에 따라 비용이 증가하는 임대 회선과는 달리 각 사무실의 지리적 위치는 VPN을 구축하는 데 별로 중요하지 않습니다.

VPN 기술

잘 설계된 VPN은 연결 및 데이터 보안을 유지하기 위해 여러 방법을 사용합니다.

- **데이터 기밀성**—VPN 구현에서 제공하는 가장 중요한 서비스입니다.개인 데이터가 공용 네트워크를 통해 전송되므로 데이터 기밀성은 매우 중요하며 데이터를 암호화하여 얻을 수 있습니다.이것은 한 컴퓨터가 다른 컴퓨터로 보내는 모든 데이터를 가져와 다른 컴퓨터만 디코딩할 수 있는 형식으로 인코딩하는 프로세스입니다.대부분의 VPN은 이러한 프로토콜 중 하나를 사용하여 암호화를 제공합니다.**IPsec**—IPsec(Internet Protocol Security Protocol)은 강력한 암호화 알고리즘 및 더욱 포괄적인 인증과 같은 향상된 보안 기능을 제공합니다.IPsec에는 두 가지 암호화 모드가 있습니다.터널 및 전송.터널 모드는 각 패킷의 헤더와 페이로드를 암호화하는 반면 전송 모드는 페이로드만 암호화합니다.IPsec 호환 시스템만 이 프로토콜을 활용할 수 있습니다.또한 모든 디바이스는 공통 키 또는 인증서를 사용해야 하며 매우 유사한 보안 정책을 설정해야 합니다.원격 액세스 VPN 사용자의 경우 일부 형태의 타사 소프트웨어 패키지를 통해 사용자 PC에 대한 연결 및 암호화를 제공합니다.IPsec은 56비트(단일 DES) 또는 168비트(3중 DES) 암호화를 지원합니다.**PPTP/MPPE** - PPTP는 US Robotics, Microsoft, 3COM, Ascend 및 ECI Telematics를 포함하는 컨소시엄인 PPTP Forum에 의해 생성되었습니다.PPTP는 Microsoft MPPE(Point-to-Point Encryption)라는 프로토콜을 사용하여 40비트 및 128비트 암호화를 사용하여 다중 프로토콜 VPN을 지원합니다. PPTP 자체는 데이터 암호화를 제공하지 않습니다.**L2TP/IPsec** - 일반적으로 L2TP over IPsec이라고 하는 이 기능은 L2TP(Layer 2 Tunneling Protocol) 터널링을 통해 IPsec 프로토콜의 보안을 제공합니다.L2TP는 PPTP 포럼, Cisco 및 IETF(Internet Engineering Task Force)의 구성원 간의 파트너십 결과입니다. Windows 2000은 네이티브 IPsec 및 L2TP 클라이언트를 제공하므로 Windows 2000 운영 체제를 사용하는 원격 액세스 VPN에 주로 사용됩니다.인터넷 서비스 제공자는 다이얼인 사용자를 위한 L2TP 연결을 제공하고, 액세스 포인트와 원격 사무실 네트워크 서버 간에 IPsec을 사용하여 해당 트래픽을 암호화할 수도 있습니다.
- **데이터 무결성**—데이터가 공용 네트워크를 통해 암호화되는 것이 중요하지만 전송 중에 변경되지 않았음을 확인하는 것도 중요합니다.예를 들어 IPsec에는 패킷의 암호화된 부분 또는 패킷의 전체 헤더 및 데이터 부분이 변조되지 않도록 하는 메커니즘이 있습니다.변조가 탐지되면 패킷이 삭제됩니다.데이터 무결성은 원격 피어 인증도 포함할 수 있습니다.

- **Data Origin Authentication**(데이터 원본 인증) - 전송되는 데이터의 소스 ID를 확인하는 것이 매우 중요합니다.이는 발신자의 ID를 스푸핑하는 데 의존하는 여러 공격을 방지하기 위해 필요합니다.
- **Anti Replay** - 재생된 패킷을 탐지 및 거부하고 스푸핑을 방지하는 기능입니다.
- **Data Tunneling/Traffic Flow Confidentiality**(데이터 터널링/트래픽 흐름 기밀성) - 터널링은 다른 패킷 내에서 전체 패킷을 캡슐화하여 네트워크를 통해 전송하는 프로세스입니다.데이터 터널링은 트래픽을 시작하는 디바이스의 ID를 숨기는 것이 바람직할 경우 유용합니다.예를 들어, IPsec을 사용하는 단일 디바이스는 뒤에 있는 여러 호스트에 속하는 트래픽을 캡슐화하고 기존 패킷 위에 자체 헤더를 추가합니다.원래 패킷 및 헤더를 암호화하고(그리고 위에 추가된 추가 레이어 3 헤더를 기반으로 패킷을 라우팅함) 터널링 디바이스는 패킷의 실제 소스를 효과적으로 숨깁니다.신뢰할 수 있는 피어만 추가 헤더를 제거하고 원래 헤더를 해독한 후 실제 소스를 확인할 수 있습니다.RFC 2401 , "...의사소통의 외부적 특성 공개도 일부 상황에서 문제가 될 수 있다.트래픽 흐름 기밀성은 소스 및 목적지 주소, 메시지 길이 또는 통신 빈도를 숨겨 이러한 문제를 해결하는 서비스입니다.IPsec 컨텍스트에서는 터널 모드, 특히 보안 게이트웨이에서 ESP를 사용하여 어느 정도의 트래픽 흐름 기밀성을 제공할 수 있습니다."여기에 나열된 모든 암호화 프로토콜은 터널링을 사용하여 공용 네트워크를 통해 암호화된 데이터를 전송합니다.터널링 자체는 데이터 보안을 제공하지 않는다는 점을 인식하는 것이 중요합니다.원래 패킷은 다른 프로토콜 내에서 캡슐화되며, 암호화되지 않은 경우 패킷 캡처 디바이스와 함께 표시될 수 있습니다.그러나 VPN의 기능 중 핵심적인 부분이기 때문에 여기에 언급되어 있습니다.터널링에는 세 가지 프로토콜이 필요합니다.**승객 프로토콜** - 전달되는 원래 데이터(IPX, NetBeui, IP)입니다.**캡슐화 프로토콜** - 원래 데이터를 둘러싸는 프로토콜(GRE, IPsec, L2F, PPTP, L2TP)입니다.**캐리어 프로토콜** - 정보가 이동하는 네트워크에서 사용하는 프로토콜입니다.원래 패킷(승객 프로토콜)은 캡슐화 프로토콜 내에 캡슐화되어 공용 네트워크를 통해 전송하기 위해 캐리어 프로토콜의 헤더(일반적으로 IP)에 저장됩니다.캡슐화 프로토콜은 데이터 암호화를 수행하는 경우가 많습니다.일반적으로 인터넷을 통해 전송되지 않는 IPX 및 NetBeui와 같은 프로토콜은 안전하고 안전하게 전송할 수 있습니다.사이트 간 VPN의 경우 캡슐화 프로토콜은 일반적으로 IPsec 또는 GRE(Generic Routing Encapsulation)입니다.GRE에는 캡슐화하는 패킷 유형에 대한 정보와 클라이언트와 서버 간의 연결에 대한 정보가 포함됩니다.원격 액세스 VPN의 경우 일반적으로 PPP(Point-to-Point Protocol)를 사용하여 터널링이 수행됩니다. TCP/IP 스택의 일부인 PPP는 호스트 컴퓨터와 원격 시스템 간에 네트워크를 통해 통신할 때 다른 IP 프로토콜의 통신기입니다.PPP 터널링은 PPTP, L2TP 또는 Cisco의 L2F(Layer 2 Forwarding) 중 하나를 사용합니다.
- **AAA**—원격 액세스 VPN 환경에서 더욱 안전한 액세스를 위해 인증, 권한 부여 및 계정 관리가 사용됩니다.사용자 인증 없이 사전 구성된 VPN 클라이언트 소프트웨어를 사용하여 랩톱/PC에 있는 모든 사용자가 원격 네트워크에 보안 연결을 설정할 수 있습니다.그러나 사용자 인증에서는 연결을 완료하기 전에 유효한 사용자 이름과 암호를 입력해야 합니다.사용자 이름 및 비밀번호는 VPN 종료 장치 자체에 저장되거나 Windows NT, Novell, LDAP 등과 같은 다른 여러 데이터베이스에 인증을 제공할 수 있는 외부 AAA 서버에 저장할 수 있습니다.터널 설정 요청이 전화 접속 클라이언트에서 수신되면 VPN 디바이스에서 사용자 이름과 비밀번호를 입력하라는 메시지를 표시합니다.이를 로컬에서 인증하거나 외부 AAA 서버로 전송할 수 있습니다. 그러면 다음을 확인할 수 있습니다.사용자(인증)수행할 수 있는 작업(권한 부여)실제 작업(회계)회계 정보는 보안 감사, 청구 또는 보고 목적으로 클라이언트 사용을 추적하는 데 특히 유용합니다.
- **비부인**—특정 데이터 전송, 특히 금융 거래와 관련된 데이터 전송에서, 거부는 매우 바람직한 기능입니다.이는 한 쪽 끝이 트랜잭션에 참가하지 않은 상황을 방지하는 데 유용합니다.은행이 수표를 표시하기 전에 서명을 요구하는 것과 마찬가지로, 보낸 메시지에 디지털 서명을 첨부하는 방식으로 거부되지 않습니다. 따라서 발신자가 거래 참여를 거부할 수 없습니다.

VPN 솔루션을 구축하는 데 사용할 수 있는 여러 프로토콜이 있습니다.이러한 모든 프로토콜은 이 문서에 나열된 서비스의 일부를 제공합니다.프로토콜 선택은 원하는 서비스 집합에 따라 달라집니

다.예를 들어, 조직은 일반 텍스트로 전송되는 데이터에 익숙하지만 무결성을 유지하는 데 매우 관심이 있는 반면, 다른 조직은 데이터 기밀성을 유지하는 것이 절대적으로 필요할 수 있습니다.따라서 프로토콜 선택이 다를 수 있습니다.사용 가능한 프로토콜과 그 상대적 강점에 대한 자세한 내용은 Which VPN Solution is Right for You?(적합한 VPN 솔루션은 무엇입니까?)를 참조하십시오.

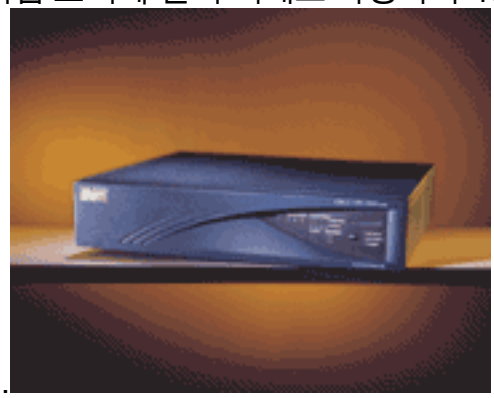
VPN 제품

VPN 유형(원격 액세스 또는 사이트 대 사이트)에 따라 VPN을 구축하려면 특정 구성 요소를 배치해야 합니다.여기에는 다음이 포함될 수 있습니다.

- 각 원격 사용자용 데스크톱 소프트웨어 클라이언트
- Cisco VPN Concentrator 또는 Cisco Secure PIX Firewall과 같은 전용 하드웨어
- 전화 접속 서비스를 위한 전용 VPN 서버
- 통신 사업자가 원격 사용자 VPN 액세스를 위해 사용하는 NAS(Network Access Server)
- 프라이빗 네트워크 및 정책 관리 센터

VPN 구현에 널리 사용되는 표준이 없기 때문에 많은 기업이 스스로 턴키 솔루션을 개발했습니다.예를 들어 Cisco는 다음과 같은 몇 가지 VPN 솔루션을 제공합니다.

- **VPN Concentrator**—가장 고급 암호화 및 인증 기술을 적용하여 원격 액세스 또는 사이트 간 VPN을 만들기 위해 특별히 제작되었으며, 단일 디바이스에서 매우 많은 수의 VPN 터널을 처리하는 데 필요한 경우 구축하는 것이 좋습니다.VPN Concentrator는 특별히 구축된 원격 액세스 VPN 디바이스의 요구 사항을 해결하기 위해 특별히 개발되었습니다.Concentrator는 고가용성, 고성능 및 확장성을 제공하며 SEP(Scalable Encryption Processing) 모듈이라는 구성 요소를 포함하고 있어 사용자가 용량과 처리량을 쉽게 늘릴 수 있습니다.Concentrator는 최대 10,000명의 동시 원격 사용자가 있는 대기업 조직에 원격 액세스 사용자가 100명 이하인 소규모 비즈니스에 적합한 모델로 제공됩니다.



- **VPN-Enabled Router/VPN-Optimized Router**—Cisco IOS® 소프트웨어를 실행하는 모든 Cisco 라우터는 IPsec VPN을 지원합니다.유일한 요구 사항은 라우터가 적절한 기능 세트와 함께 Cisco IOS 이미지를 실행해야 한다는 것입니다.Cisco IOS VPN 솔루션은 원격 액세스, 인트라넷 및 엑스트라넷 VPN 요구 사항을 완벽하게 지원합니다.즉, Cisco 라우터는 VPN 클라이언트 소프트웨어를 실행하는 원격 호스트에 연결되거나 라우터, PIX 방화벽 또는 VPN Concentrator와 같은 다른 VPN 디바이스에 연결될 때 동일하게 작동할 수 있습니다.VPN 지원 라우터는 적절한 암호화 및 터널링 요구 사항을 가진 VPN에 적합하며 Cisco IOS 소프트웨어 기능을 통해 VPN 서비스를 전적으로 제공합니다.VPN 지원 라우터의 예로는 Cisco 1000, Cisco 1600, Cisco 2500, Cisco 4000, Cisco 4500 및 Cisco 4700 시리즈가 있습니다.Cisco의 VPN 최적화 라우터는 확장성, 라우팅, 보안 및 QoS(Quality of Service)를 제공합니다. 이 라우터는 Cisco IOS 소프트웨어를 기반으로 하며, SOHO(Small-Office/Home-Office) 액세스부터 중앙 사이트 VPN 어그리게이션, 대규모 엔터프라이즈 요구 사항에 이르기까지 모든 상황에 적합한 장치가 있습니다.VPN 최적화 라우터는 높은 암호화 및 터널링 요구 사항을 충족하도록 설계되었으며 높은 성능을 얻기 위해 암호화 카드와 같은 추가 하드웨어를 사용하는 경우가 많습니

다.VPN 최적화 라우터의 예로는 Cisco 800, Cisco 1700, Cisco 2600, Cisco 3600, Cisco7200,

Cisco7500 시리즈가 있습니다.

- **Cisco Secure PIX Firewall**—PIX(Private Internet eXchange) 방화벽은 단일 하드웨어에서 동적 네트워크 주소 변환, 프록시 서버, 패킷 필터링, 방화벽 및 VPN 기능을 결합합니다.이 장치는 Cisco IOS 소프트웨어를 사용하는 대신 IP에 집중하여 매우 견고하고 성능이 뛰어난 다양한 프로토콜을 처리하는 기능을 트레이드하는 매우 간소화된 운영 체제를 갖추고 있습니다.Cisco 라우터와 마찬가지로 모든 PIX 방화벽 모델은 IPsec VPN을 지원합니다.VPN 기능을 활성화하기

위한 라이센싱 요구 사항이 충족되어야 합니다.

- **Cisco VPN Clients**—Cisco는 하드웨어 및 소프트웨어 VPN 클라이언트를 모두 제공합니다 .Cisco VPN Client(소프트웨어)는 추가 비용 없이 Cisco VPN 3000 Series Concentrator와 함께 번들로 제공됩니다.이 소프트웨어 클라이언트는 호스트 시스템에 설치할 수 있으며 중앙 사이트 집중 장치(또는 라우터 또는 방화벽과 같은 다른 VPN 장치)에 안전하게 연결하는 데 사용할 수 있습니다. VPN 3002 Hardware Client는 모든 시스템에 VPN 클라이언트 소프트웨어를 구축하는 대신 여러 디바이스에 VPN 연결을 제공합니다.

VPN 솔루션을 구축하는 데 사용할 디바이스 선택은 궁극적으로 원하는 처리량 및 사용자 수를 비롯한 여러 요소에 따라 달라집니다.예를 들어, PIX 501 뒤에 소수의 사용자가 있는 원격 사이트에서 기존 PIX를 IPsec VPN 엔드포인트로 구성할 수 있습니다. 단, 501의 3DES 처리량과 최대 5개의 VPN 피어 제한을 약 3Mbps로 수락하는 경우 가능합니다.반면, 중앙 사이트에서 많은 수의 VPN 터널에 대한 VPN 엔드포인트 역할을 하는 경우, VPN 최적화 라우터 또는 VPN Concentrator를 사용하는 것이 좋습니다.이제 설정 중인 VPN 터널의 유형(LAN-to-LAN 또는 원격 액세스)과 수에 따라 선택 사항이 달라집니다.VPN을 지원하는 광범위한 Cisco 장치는 네트워크 설계자에게 높은 수준의 유연성과 모든 설계 요구 사항을 충족하는 강력한 솔루션을 제공합니다.

관련 정보

- VPDN 이해
- 가상 사설망(VPN)
- Cisco VPN 3000 Series Concentrator 지원 페이지
- Cisco VPN 3000 클라이언트 지원 페이지
- IPsec 협상/IKE 프로토콜 지원 페이지
- PIX 500 Series 방화벽 지원 페이지
- RFC 1661:PPP(Point-to-Point Protocol)
- RFC 2661:레이어 2 터널링 프로토콜 "L2TP"

- 작동 방식:가상 사설 네트워크의 작동 방식
- VPN 개요
- Tom Dunigan의 VPN 페이지
- 가상 사설망 컨소시엄
- RFC(Request for Comments)
- Technical Support - Cisco Systems