Cisco IOS Easy VPN

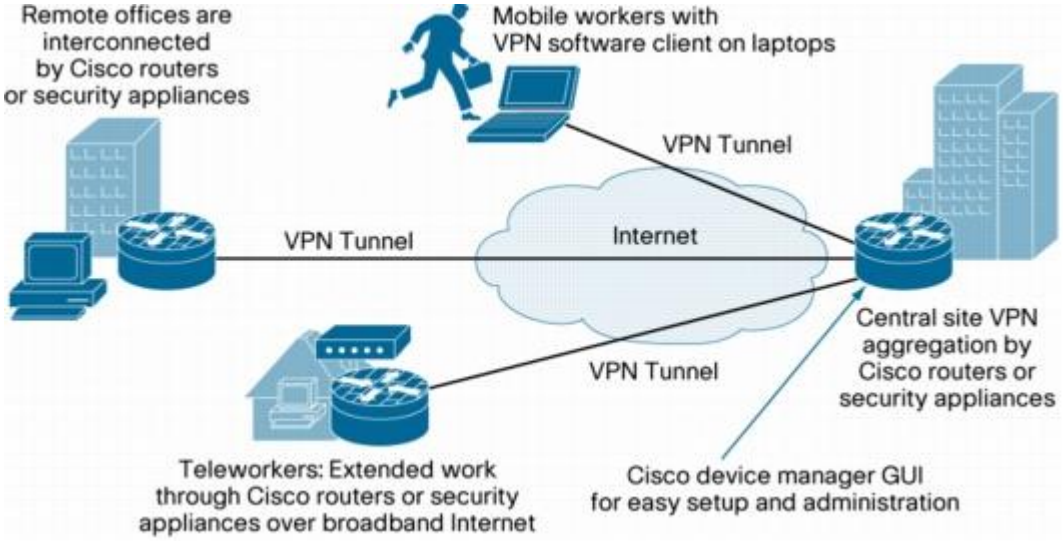
Cisco Easy VPN on Cisco IOS Software-Based Routers

Cisco Easy VPN 솔루션 개요

Cisco® Easy VPN 솔루션(그림 1)은 사이트간(site-to-site) 그리고 원격 액세스간 VPN에서 유연성과 확장성 및 사용 용이성을 제공합니다.

- 규모가 작은 지사 사무실이나 재택 작업 환경 또는 이동 근무자처럼 기술 지원 담당자를 두기가 어려운 곳에서 VPN 을 구현해야 하는 고객에게 매우 유용합니다.
- 이 솔루션은 시스코 라우터, 보안 어플라이언스 및 소프트웨어 VPN 클라이언트를 단일 구현으로 통합하여 VPN 장치의 선택권과 지원 면에서 매우 뛰어난 유연성을 제공합니다.
- 대규모 VPN 을 구현할 경우 모든 시스코 VPN 장치 간에 일관된 정책과 키 관리 방식을 중앙에서 적용함으로써 관리의 복잡성을 줄여줍니다.

그림 1. Cisco Easy VPN 솔루션 개요



애플리케이션: 소규모 구현

이동 작업자나 재택 근무자의 경우 고성능 인터넷 연결을 가지기가 쉽지 않습니다. 업무의 효율성을 높이려면 이러한 작업자들이 전자 리소스를 집에서 안전하고 완전하게 액세

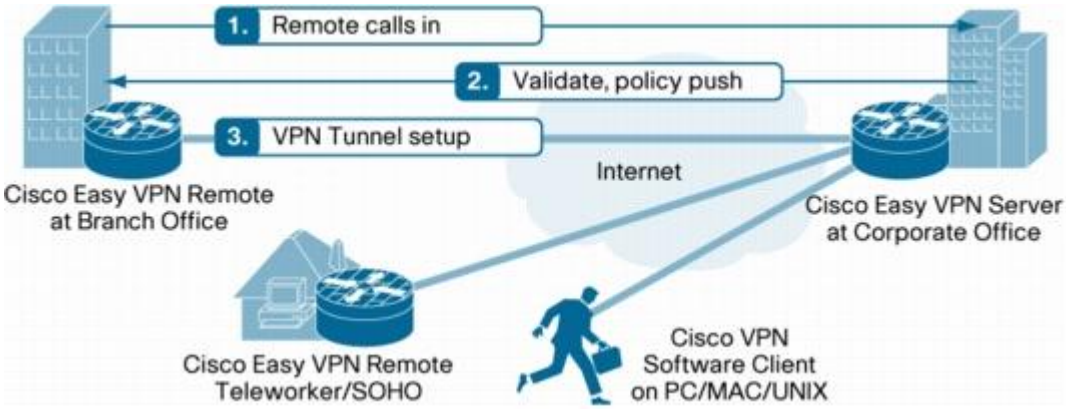
스할 수 있어야 합니다. 즉, 이러한 작업자들을 위해서는 높은 수준의 인증과 데이터 암호화 기능을 갖춘 VPN 연결을 설정하는 것이 효율적입니다. Cisco Easy VPN 솔루션은 소규모 사무실이나 기업의 지사 사무실에서 일하는 원격 작업자나 재택 작업자들이 공개 인터넷을 사용하여 VPN 연결을 설정하는 작업을 간단하게 할 수 있도록 도와줍니다. VPN 연결은 이러한 작업자들이 업무에 필요한 네트워크 리소스에 보다 빠르게 접근할 수 있게 하며, 다른 보안 방법에 비해 비용도 훨씬 작게 소요됩니다.

이전에는 원격 작업자들에게 보안 액세스를 제공할 때 주로 PPTP(Point-to-Point Tunneling Protocol)를 사용하여 홈 오피스에 연결했습니다. 하지만 이 방법은 홈 오피스 보안 연결을 사용자가 터미네이션할 수 있게 해주는 반면에, PPTP 터널이 사용자 인증을 제공하지 않기 때문에 전체적인 보안 한계를 낮추는 결과를 가져옵니다. 그 외 보안 연결을 설정하는 이 외에 다른 방법들은 네트워크에서 모든 플랫폼을 지원하지 못해서 생기는 한계를 가지고 있습니다.

솔루션 구성요소

Cisco Easy VPN 솔루션은 Cisco Easy VPN Remote와 Cisco Easy VPN Server, 이 두 가지 운영 구성요소를 기본으로 구성됩니다(그림 2).

그림 2. Cisco Easy VPN 솔루션



Cisco Easy VPN Remote는 VPN 연결을 사용하는 지사 또는 원격 사용자 측을 나타냅니다. Cisco IOS® Software 기반 라우터나 Cisco ASA 보안 어플라이언스 또는 Cisco VPN Client 소프트웨어를 실행하는 PC 등 다양한 장치가 Easy VPN Remote로 참여할 수 있습니다.

Cisco Easy VPN Server는 VPN 터널을 사용하는 헤드엔드 측을 나타냅니다. Cisco IOS Software 기반 라우터, Cisco Catalyst® 스위치 및 Cisco ASA 보안 어플라이언스는 지사 사무실이나 재택 작업 환경 또는 이동 중인 작업지에서 사용하는 장치를 포함하여 수천 개의 Easy VPN Remote 장치에 대해 Easy VPN 어그리게이션 포인트로서의 역할을 수행합니다.

Cisco Easy VPN Server는 중앙 집중식 정책 푸시 기능을 사용하여 사전에 정의된 보안

정책과 구성 매개변수를 Easy VPN Remote 장치에 자동으로 전송합니다. 예를 들어, 내부 IP 주소, 내부 서브넷 마스크, DHCP 서버 주소, WINS 서버 주소 및 분할 터널링(Split Tunneling) 플래그와 같은 구성 매개변수를 원격 장치에 푸시할 수 있으며 이를 통해 관리가 간단해집니다. 여러 원격 장치를 개별적으로 구성해야 하는 대규모 CPE(customer premises equipment) 구현이나 IT 지원에 들어가는 노력을 줄일 수 있기 때문에 원격 사무실에 매우 이상적입니다.

주요 기능 및 이점

Cisco Easy VPN 솔루션은 다음을 포함하여 이 외에도 수 많은 기능과 이점을 제공합니다.

- **네트워크 통합:** Cisco IOS Software 는 다양한 토폴로지와 사용 사례에서 작업할 수 있는 고급 VPN 솔루션을 제공하는데 이 솔루션의 핵심은 네트워크 통합입니다. 즉, 네트워크에서 사용되는 다양한 장치 간의 문제뿐 아니라, 같은 장치에서 VPN 과 IP 서비스를 어떻게 통합할 것인지가 중요합니다.
- **간단한 관리:** Cisco Easy VPN 솔루션은 중앙 집중식 정책 푸시 기능과 Easy VPN 의 향상된 아키텍처(가상 터널 인터페이스 통합)와 같은 기능을 통해 간단하고 지속적인 관리를 제공합니다.
- **인증:** Cisco Easy VPN 은 그룹 및 xauth 수준 인증을 모두 사용하는 원격 클라이언트와 사용자의 인증을 위해 두 가지 준비 프로세스를 지원합니다.
- **확장성 및 고가용성:** Cisco Easy VPN Server 는 수 천 개의 원격 장치를 어그리게이션할 수 있어 고도로 확장 가능한 구현이 가능합니다. 이러한 시나리오에서 가장 중요한 고려사항은 고가용성으로, 수많은 사이트에서 장치 고장이나 연결 실패가 발생하지 않도록 하기 위해 이를 지원하는 다양한 매커니즘이 Cisco Easy VPN 솔루션에 내장되어 있습니다.
- **소유 비용 절감**: 보안과 VPN 을 단일 장치에 결합함으로써 비즈니스 요구가 확대될 때 확장성과 모듈식 방식에 따라 투자 보호뿐 아니라 초기 비용을 절감할 수 있습니다. 특히 필수적인 지점 라우터(branch router)의 경우에는 그 효과가 더 큽니다. 또한 학습해야 할 관리 솔루션도 한 가지로 줄어들기 때문에 교육의 요구도 최소화되고 지속적인 운영도 간소화됩니다. Cisco IOS Software 기반 라우터는 업계 최고의 장치 관리 기능과 함께 다중 프로토콜 라우팅, 경계선 보안(perimeter security), 침입 방지, 고급 VPN 등을 모두 수용하는 확장 가능한 최강의 올인원 솔루션을 제공합니다.

네트워크 통합

표 1은 Cisco Easy VPN 솔루션의 주요 네트워크 통합 기능과 이점을 설명합니다.

표 1. 네트워크 통합 기능 및 이점

주요 기능	설명 및 이점
새롭게 강화된 Easy VPN Virtual Tunnel Interface(VTI) 통합	• Enhanced Easy VPN 아키텍처는 GRE(generic routing encapsulation)와 같은 IPsec 내부 프로토콜을 캡슐화하지 않아도 IP Security(IPsec)를 사용하여 직접 구성할 수 있는 새로운 가상 인터페이스를 제공하며. 네트워크 통합은 다음과 같은 이점을 제공합니다. • QoS와 같은 사용자별 속성 - VTI를 사용하면 사용자별로 쉽게 정책을 구성할 수 있습니다. VTI는 원하는 애플리케이션 성능을 제공하고 사용자의 생산성과 의욕을 유지할 수 있게 관리자의 능동적인 관리를 지원합니다. • 터널 특정 기능 - VTI를 사용하면 각 분기 VPN 터널을 자체 매개변수 세트를 사용하여 구성할 수 있으며, 사이트별 요구사항에 맞춰 구성과 보안을 직접 정의할 수 있는 유연성을 제공합니다.
VRF(가상 경로 포워딩) 통합	VTI 를 사용한 VRF 통합을 통해 여러 VRF 인스턴스를 여러 인터페이스에서 터미네이션할 수 있습니다. 이 기능은 대규모 서비스 제공업체와 엔터프라이즈 MPLS(Multiprotocol Label Switching) 구현을 용이하게 합니다.
TCP 기반 방화벽 트래버셜	IPsec TCP 패킷을 타사 방화벽 장치를 통해 터널링할 수 있습니다. 표준 ESP(Encapsulating Security Payload) 또는 UDP(User Datagram Protocol) 포트 500 을 허용 또는 비허용할 수 있습니다.
NAT(네트워크 주소 변환) 통합	NAT 통합은 UDP 포트 500(RFC 3947)에 따라 NAT 투명성을 지원함으로써 IPsec 와 NAT 사이에 알려진 비호환성 문제를 처리하고 해결합니다.
SafeNet 클라이언트	SafeNet 클라이언트는 특정 ISAKMP(Internet Security Association and Key Management Protocol) 로컬 주소를 사용하여 클라이언트 구성 그룹으로 바인딩합니다. 서로 다른 고객들이 서로 다른 로컬 터미네이션 주소를 사용하여 동일한 피어 ID 와 ISAKMP 키를 사용할 수 있습니다.

다음 기능들은 Cisco Easy VPN에서 가장 사용하기 편리한 기능들입니다.

• **동적 정책 업데이트:** 네트워크 작업자나 서비스 제공업체가 최종 사용자의 장치를 건드리지 않고도 필요에 따라 장비와 네트워크 구성을 변경할 수 있습니다. Easy VPN Server 는 필요시 최신 보안 정책을 푸시하여 수동 구성 및 이로 인한 작업자의 오류를 최소화할 수 있으며, 이에 따라 추가 서비스 콜도 줄어드는 효과가 있습니다.

• **향상된 Easy VPN 아키텍처(VTI 통합):** 원격 지사 측뿐만 아니라 헤드엔드 측에서도 구성 요구사항이 대폭 간소화됩니다. 가상 템플릿 인터페이스를 사용하여 IP 서비스를 구성할 수 있으며,(또는 AAA 서버(authentication, authorization, 및 accounting)에서 다운로드할 수 있습니다.) 연결시 VTI 인스턴스가 이러한 템플릿에서 동적으로 복제됩니다. 따라서 각 원격 사이트에 대한 비슷한 구성 명령 세트를 수동으로 만들 필요가 없습니다. Enhanced Easy VPN 은 라우팅 프로토콜을 지원하지 않지만 여러 서브넷에 대한 연결 가능 정보를 분산하는 RRI(Reverse Route Injection)를 사용하면 정상적으로 작동됩니다.
• **하드웨어 VPN 클라이언트:** VPN 라우터 또는 보안 어플라이언스가 VPN 클라이언트 역할을 수행하여 LAN 상의 PC 사용자 대신 암호화를 처리합니다. 따라서 최종 사용자가 외부 VPN 장치를 구매하고 구성할 필요가 없습니다.
• **Cisco Easy VPN 및 Cisco Unity® 프레임워크:** PC 기반의 소프트웨어 VPN 클라이언트와 외부 하드웨어 기반의 VPN 솔루션, 그리고 기타 VPN 애플리케이션처럼 서로 다른 기반 간에 일어날 수 있는 상호운용성 문제를 줄여줍니다.

Cisco Easy VPN의 정책 푸시 기능의 동적 특성(예: 온디맨드 및 자동화)은 소규모 사무실, 재택 작업자, 원격 사무실, 지사 사무실 환경에 대한 VPN 롤아웃을 대폭 간소화하는 핵심 기능입니다. 표 2는 정책 푸시 기능의 주요 특징과 이점을 보여줍니다.

표 2. 중앙 집중식 정책 푸시 기능 및 이점

주요 기능	설명 및 이점
브라우저 프록시 구성	이 기능을 사용하면 수동으로 조작하지 않아도 Easy VPN Server 에서 프록시 서버를 원격 장치로 자동으로 푸시할 수 있습니다. 연결이 해제되면 원격 서버의 원래 프록시 설정이 자동으로 변환됩니다.
Include-Local-LAN	LAN 연결은 비분할터널(non-split-tunnel) 연결로 유지할 수 있습니다. 이렇게 하면 소스 연결이 다시 설정되었을 때 프린터나 서버와 같은 로컬 리소스의 연결을 유지할 수 있습니다.
로그인 배너(하드웨어 클라이언트에 해당)	Easy VPN Server 는 Extended Authentication(Xauth) 및 웹 기반 인증을 수행하는 동안 배너가 사용되는 원격 장치로 배너를 푸시하며, Easy VPN 터널이 처음 중단될 때 원격 장치에 개인화된 메시지를 표시할 수 있습니다.
자동 업그레이드(소프트웨어 클라이언트)	Easy VPN Server 가 Easy VPN Client 의 소프트웨어 업그레이드를 자동화하는 매커니즘을 제공하도록 구성할 수 있습니다.

자동 구성 업데이트	Easy VPN Server 가 Easy VPN 원격 클라이언트에 대한 소프트웨어 및 펌웨어 업그레이드를 자동화하는 매커니즘을 제공하도록 구성할 수 있습니다. 또한 모든 클라이언트를 직접 터치할 필요 없이 간단하게 구성 변경을 푸시할 수 있습니다.
통합 클라이언트 방화벽을 위한 중앙 정책 푸시	이 기능을 사용하면 Cisco IOS Software 기반 Easy VPN Server 에서 분할 터널링에 대해 향상된 보안을 허용하도록 클라이언트 시스템에 대한 개인 방화벽을 구성할 수 있습니다. EasyVPN Server 는 최신 방화벽 구성 정책이 없는 클라이언트가 VPN 에 참가하는 것을 허용하지 않도록 지정할 수도 있습니다.
DHCP 클라이언트 프록시 및 분산 DNS	Easy VPN Server 는 프록시 DHCP 클라이언트 역할을 수행하며, DHCP 서버로부터 IP 주소를 가져오고 클라이언트로 이 IP 주소를 푸시합니다. Cisco Easy VPN Server 에서 이 기능을 사용하여 회사 DHCP 서버로부터 클라이언트로 IP 주소를 지정하여 IP 주소 지정 관리를 중앙화할 수 있습니다.
분할 터널링	분할 터널링(Split tunneling)을 사용하면 인트라넷 대상 트래픽(Internet-destined traffic)을 암호화하지 않은 상태로 인터넷으로 직접 보낼 수 있습니다. 이 기능을 사용하지 않으면 모든 트래픽은 헤드엔드측 장치로 전송된 후 대상 리소스로 다시 라우팅됩니다. (웹 액세스 경로에서 회사 네트워크를 제거합니다) 분할 터널링은 원격 위치에서 중요한 업무 데이터와 애플리케이션에 액세스하는 사람의 대역폭을 늘림으로써, 회사의 IT 리소스를 보다 효율적으로 사용할 수 있게 합니다.
분할 DNS 지원	Easy VPN 클라이언트는 분할 DNS(Split-DNS)를 통해 DNS 프록시 역할을 수행하여,인터넷 질의를 ISP 의 DNS 서버로 보내고, 회사의 DNS 요청을 회사 DNS 서버로 보냅니다.

인증

표 3은 Cisco Easy VPN 솔루션의 주요 인증 기능과 이점을 설명합니다.

표 3. 인증 기능 및 이점

주요 기능	설명 및 이점
AAA 서비스	RADIUS 클라이언트 역할을 수행하여 RADIUS 를 통해 사용자 인증을 수행합니다. 즉, 로컬 인증 및 권한 부여를 수행하고 어카운팅 세션 정보를 지원합니다.
디지털 인증서	터널 엔드포인트 인증을 위한 디지털 인증서를 지원합니다.
암호화된 암호	Cisco IOS Software 의 비밀번호를 쉽게 알아낼 수 없도록 암호화 스키마를 강화하여 강력한 암호를 사용합니다.
관심 트래픽에 대한 터널 활성화(ACL 트리거)	ACL(액세스 제어 목록)에 정의된 관심 트래픽에 기반하여 보안 터널을 구축할 수 있습니다. 어떤 트래픽을 암호화할 것인지 세분화된 단계에서 제어하는 기능을 사용하면 잠재적인 대역폭 사용량을 줄일 수 있습니다.
Xauth 을 위한 웹 인터셉터	Cisco IOS Software 기반 하드웨어 클라이언트에 대한 Xauth 자격 증명을 입력할 수 있는 HTTP 인터페이스를 제공하므로 로그인하기 위해 CLI 를 사용할 필요가 없어졌습니다. 이에 따라 사용자가 단일 포트가 아닌 전체 장치를 인증할 수 있게 되었습니다.
Xauth 우회	터널을 우회하는 옵션을 제공하여 재택 근무자의 암호화되지 않은 인터넷 액세스가 허용됩니다.
AAA 를 사용하여 암호 만료	이전 암호가 만료되면 VPN 클라이언트 사용자가 새 암호를 입력할 수 있습니다.

확장성 및 고가용성

표 4는 Cisco Easy VPN 솔루션의 주요 고가용성 및 확장성 기능과 이점을 설명합니다.

표 4. 고가용성 및 확장성 기능과 이점

주요 기능	설명 및 이점
RRI(Reverse Route Injection)	고가용성 또는 로드 밸런싱 중 하나를 필요로 하는 VPN 을 위해 RRI 가 네트워크 설계를 간소화했습니다. RRI 는 헤드앤드 장치 측의 각 원격 네트워크나 호스트에서 동적 경로 전달(propagation)을 허용하도록 경로를 만듭니다.
DPD(Dead Peer Detection) 및 Keepalives	DPD 는 서로 다른 서브넷 상의 집선기(concentrator)들 간의 장애복구를 원하는 환경에서 이상적입니다. 라우터는 정기적인 간격으로 IKE 피어에게 질의하여 데드 피어를 조기 감지할 수

	있습니다.
HSRP(Hot Standby Router Protocol)	HSRP 는 단일 라우터의 가용성에 의존하지 않고 이더넷 네트워크 상의 호스트로부터 IP 트래픽을 라우팅하여 높은 네트워크 가용성을 제공합니다. RRI 와 HSRP 를 함께 사용하면 VPN 에 보다 안정된 네트워크 설계를 제공하고 원격 피어 구성에서 복잡성을 줄일 수 있습니다.
IPsec 상태저장 장애복구	상태저장 장애복구(Stateful failover)는 계획되었거나 계획되지 않은 전원 중단이 발생해도 라우터에서 IPsec 를 계속 처리하고 포워딩하도록 합니다.
잘못된 SPI(Security Parameter Index) 복구	잘못된 SPI 메시지가 수신되면 자동으로 수신자를 트리거하여 새 키 교환을 초기화합니다. Keepalive 또는 DPD 를 지원하지 않는 IKE 피어는 잘못된 SPI 복구 기능을 사용하여 장애복구 후에 피어를 재동기화할 수 있습니다.
다중 백업 피어	이 기능을 사용하면 라우터에서 로컬 다중 피어 구성을 지원할 수 있습니다.
기본 피어 재활성화(Primary Peer Reactivation)	기본 VPN 터널 연결이 해제되면 Easy VPN 클라이언트는 장애 복구가 발생한 후 기본 피어와의 연결을 계속 재시도하게 됩니다. 기본 피어를 사용할 수 있게 되면 연결이 다시 설정되고 백업 연결은 삭제됩니다.
원격 이중 터널(Remote Dual Tunnels)	이 기능을 사용하면 인터페이스 내부 및 외부에서 공통 인터페이스를 공유하는 여러 Easy VPN 터널이 서로 다른 VPN 서버로 두 피어를 동시에 연결하도록 구성할 수 있습니다.
IPsec Single Security Association	이 기능은 지원되는 다중 서브넷 수와 split-include 목록의 크기에 상관없이 단일 IPsec 터널을 설정합니다. VPN 라우터에 대한 리소스 사용이 감소되고 확장 기능이 강화됩니다.
서버 로드 밸런싱:	Cisco IOS Software 는 구성된 로드 밸런싱 알고리즘을 기반으로 서버를 선택합니다. 선택한 서버 중 하나가 실패할 경우 모든 수신 요청이 나머지 서버로 동적으로 라우팅됩니다.

총 소유 비용 절감

Cisco Easy VPN 솔루션은 기업의 총 소유 비용을 다음과 같이 다양한 방식으로 절감합니다.

- **자본 지출 절감:** 통합된 Cisco IOS Software 기반 솔루션은 별도로 어플라이언스를 설치하는 것과 비교하면 초기 구매 비용을 줄여줍니다. 이 솔루션은 VPN 클라이언트 소프트웨어를 함께 제공하므로, 추가 기능 라이센스가 없어도 원격 액세스 사용자에 대한 지원을 제공할 수 있습니다.
- **교육 비용 절감:** Cisco Easy VPN 기능은 표준 IOS CLI 를 사용하여 구성할 수 있습니다. 새로운 교육을 확장하지 않아도 네트워크 작업자가 솔루션을 쉽고 직관적으로 설치하고 문제 해결을 처리할 수 있으며, 새로운 하드웨어와 소프트웨어를 학습할 필요가 없습니다.
- **운영비 절감:** 원격 하드웨어와 소프트웨어에 대한 변경사항이 계속 진행 중인 경우에도 사용자 개입을 최소화하는 중앙 집중식 정책 푸시 기능의 대규모 구현 이점을 누려보십시오. 소규모 구현에서는 제공되는 장치 관리 애플리케이션, Cisco 라우터 및 Security Device Manager(SDM)를 사용하여 Cisco Easy VPN 을 구성할 수 있습니다. 간단한 Cisco SDM 마법사를 통해 라우팅, QoS, VPN 및 보안 기능(예: Cisco TAC-승인 기본 방화벽 정책)뿐 아니라 방화벽 로그의 실시간 모니터링을 구성할 수 있습니다.
- **지원 및 유지보수 비용 절감:** 단일 통합 장치는 단일 지원 계약을 의미합니다. 단일 지원 계약은 다중 장치에 지속적으로 발생하는 비용을 절감해주며, 단일 공급업체를 관리하므로 여러 관계를 관리하는 것보다 훨씬 간단합니다.

표 5는 Cisco 플랫폼에 따라 지원되는 Cisco Easy VPN 터널의 수를 나타냅니다.

Table 5. 플랫폼별로 지원되는 터널 수

플랫폼	Easy VPN 터널의 최대 수
Cisco 870 시리즈 통합 서비스 라우터	10
Cisco 1801, 1802, 1803, 1811, 1812 통합 서비스 라우터	50
SSL VPN 고급 통합 모듈 1 을 사용하는 Cisco 1841 통합 서비스 라우터(AIM-VPN/SSL-1)	800
AIM-VPN/SSL-2 를 사용하는 Cisco 2800 시리즈 통합 서비스 라우터	1500
AIM-SSL-3 을 사용하는 Cisco 3825 통합 서비스 라우터	2000
AIM-SSL-3 을 사용하는 Cisco 3845 통합 서비스 라우터	2500
VPN Acceleration Module 2+(VAM2+)를 사용하는 Cisco 7200 시리즈 라우터	5000
NPE-G2 Network Processing Engine 및 VPN Services Adapter 를	5000

사용하는 Cisco 7200VXR Routers	
VAM2+를 사용하는 Cisco 7301 라우터	5000
IPSec VPN 공유 포트 어댑터를 사용하는 Cisco 7600 시리즈 라우터	16,000
IPsec VPN SPA 를 사용하는 Cisco Catalyst 6500 시리즈 스위치	16,000

시스템 요구사항

표 6은 Cisco IOS Software를 실행하는 Cisco 라우터 및 스위치에서 Cisco Easy VPN 소프트웨어를 실행할 수 있는 시스템 요구사항을 나타냅니다.

표 6. 시스템 사양

주요 기능	설명
하드웨어	• Easy VPN Remote: • Cisco 800, 1800, 2800 시리즈 통합 서비스 라우터 • Cisco ASA 5500 시리즈 적응형 보안 어플라이언스 • Easy VPN Server: • Cisco 1800, 2800, 3800 시리즈 통합 서비스 라우터 • Cisco ASA 5500 시리즈 적응형 보안 어플라이언스 • Cisco 7200 시리즈 라우터, Cisco 7301 라우터 및 Cisco Catalyst 6500 시리즈 스위치
소프트웨어 호환성	• Cisco IOS Software Release 12.4XW • Cisco IOS Software Release 12.4XJ • Cisco IOS Software Release 12.4T

주문 정보

모든 Cisco 라우터 보안 번들에는 Cisco Easy VPN에 대한 지원이 포함됩니다. 라우터 보안 번들 목록은 http://www.cisco.com/go/securitybundles를 참조하십시오.
주문을 하려면 시스코 주문 홈 페이지를 방문해주십시오. 소프트웨어를 다운로드하려면 다음 시스코 소프트웨어 센터(Cisco Software Center)를 방문하십시오. http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml.

시스코 서비스

시스코 서비스는 네트워크와 애플리케이션 그리고 그것을 사용하는 사람들의 협업을 효율

적으로 개선합니다.
오늘날, 네트워크는 사용자, 정보 그리고 아이디어 간의 효율적인 통합을 요구하는 전략적 플랫폼이며, 고객의 비즈니스 요구와 기회를 고려하여 적합한 서비스 및 제품으로 솔루션을 구성할 때 보다 효과적으로 작동합니다.
시스코만의 서비스 라이프사이클 접근법은 네트워크 라이프사이클의 각 단계에 맞는 활동을 정의하여 서비스 우수성을 보장합니다. 시스코와 시스코 파트너 간의 숙련된 네트워크, 그리고 고객들의 힘이 결합된 협업 방식을 통해 최선의 결과를 얻을 수 있습니다.

추가 정보

Cisco Easy VPN에 대한 자세한 내용은 http://www.cisco.com/go/easyvpn을 참조하거나 시스코 영업 담당자에게 문의하십시오.

<업데이트: 2008년 11월 20일>

