

시스코 서비스 모듈

Catalyst 6500 시리즈 스위치 및 7600 시리즈 라우터를 위한 WebVPN Services Module

제품 개요

Cisco® WebVPN Services Module(그림 1)은 Cisco Catalyst® 6500 시리즈 스위치와 Cisco 7600 시리즈 라우터를 위한 고속의 통합 SSL(Secure Sockets Layer) VPN 서비스 모듈로서, 원격 액세스 제품으로 구성된 시스코의 기존 포트폴리오 성능을 보완한 것입니다.

그림 1. Cisco WebVPN Services Module



오늘날과 같이 날로 복잡해지고 이동성이 많아진 기업 환경에서는 다중 고정 장치와 무선 장치의 원격 액세스를 요구하고 있습니다. 그리고 지사 네트워크에서 본사로 액세스를 해야 하는 경우도 많습니다. SSL VPN의 이점은 "언제 어디서나 액세스"할 수 있다는 점입니다. SSL은 Microsoft Internet Explorer나 Netscape와 같은 표준형 브라우저에 포함되어 있기 때문에 SSL VPN은 클라이언트리스(Clientless) 솔루션의 가능성을 제공합니다. 사용자는 인터넷 접속이 가능한 곳이라면 어디서든 애플리케이션에 접속할 수 있습니다. 공항의 키오스크 화면에서도, 다른 사람의 컴퓨터에서도 또는 무선 장치를 사용하여 접속하는 경우에도 인터넷 접속만 가능하면 됩니다. SSL VPN은 광대역 네트워크를 통해 작동됩니다. 이 외에도 SSL VPN은 방화벽을 성공적으로 트래버설할 수 있으며, IP Security(IPsec) 기반 VPN을 사용할 경우 문제가 발생할 수 있는 네트워크 주소 변환(NAT) 문제점을 해결했습니다.

SSL VPN 기술에 기반한 Cisco WebVPN Services Module을 통해 영업 담당자는 현장에서 바로 고객 관계 관리 데이터를 다운로드할 수 있습니다. 제조공장 관리자의 경우, 공급 하한선이 심각한 정도에 이르기 전에 미리 재고를 추적하고 주문을 넣을 수 있습니다. 의사의 경우 환자의 병실에서 처방전 승인을 전송할 수 있습니다. 제조업체의 소매점 관리 매니저들은 현장 주문을 넣을 수도 있습니다.

Cisco WebVPN Services Module은 다양한 웹 리소스와 웹 사용 애플리케이션에 대한 간단한 액세스를 제공합니다. HTTP(HTTPS) 인터넷 사이트에 접속할 수 있는 모든 컴퓨터에서 액세스가 가능합니다. 이 모듈은 SSL 프로토콜과 TLS(Transport Layer Security)를 사용하여 원격 사용자와 중앙 사이트에서 지원하도록

구성된 특정 내부 리소스 간에 안전한 연결을 제공합니다.

Cisco WebVPN Services Module은 직원, 익스트라넷, 회사에서 관리되지 않는 장치들과 같이 최종 시스템 설치 환경에 기반한 적절한 수준의 애플리케이션 액세스를 설정하는 클라이언트리스(Clientless), 씬클라이언트(thin-client) 및 SSL 터널링(tunneling) 클라이언트 액세스 방법을 제공합니다. 시스코의 SSL VPN Client는 중앙 구성으로 지원이 간편한 라이트웨이트 SSL VPN 터널링 클라이언트를 제공하여 모든 가상 애플리케이션에 액세스할 수 있도록 지원합니다. WebVPN을 위한 SSL VPN Client는 SSL 사용 브라우저와 호환되며 사용자에게 동적으로 푸시됩니다. Cisco WebVPN Services Module에서 클라이언트리스(Clientless) 액세스를 사용하면 몇 가지 요구사항에 따라 기본 웹 브라우저에 연결하여 파일 공유와 같은 웹 서버나 기타 리소스에 액세스하고, Microsoft Outlook Web Access 2003을 통해 전자메일을 보낼 수 있습니다.

이점

확장성

Cisco WebVPN Services Module은 Cisco Catalyst 6500 및 7600 시리즈 제품에 사용할 수 있는 통합 서비스 모듈입니다. 단일 모듈은 최대 8000명의 동시 사용자와 최대 32,000개의 동시 접속을 지원합니다. 32,000명의 SSL VPN 동시 사용자와 128,000개의 동시 접속을 지원하는 단일 쉐시에 최대 4개의 모듈이 지원됩니다. Cisco WebVPN Services Module의 확장성과 고유한 가상화 기능은 관리형 서비스 제공업체에 이상적인 솔루션입니다. 이러한 솔루션은 다양한 사용자 집단이 모여 있는 대규모 엔터프라이즈에서 정책 생성과 시행 요구사항을 간소화합니다.

통합 모듈

Cisco WebVPN Services Module은 Cisco Catalyst 6500 시리즈 또는 Cisco 7600 시리즈 장치의 포트가 SSL VPN 포트로 작동되도록 해줍니다. 이러한 기능은 랙 공간이 부족할 경우 매우 유용합니다. 이 모듈을 함께 사용할 경우 Cisco Catalyst 6500 시리즈는 멀티레이어 LAN, WAN 및 MAN 스위칭 기능뿐만 아니라 방화벽 서비스, 침입 감지 및 VPN과 같은 인텔리전트한 서비스를 요구하는 고객에게 적합한 IP 서비스 스위칭 플랫폼으로 부상하고 있습니다.

가상화 및 VRF 인식

가상화 기술은 물리적 특성과 리소스 사용자로부터 리소스의 한계를 마스킹하는 반면, 리소스를 풀링하는 방법이기도 합니다. 모듈당 최대 128개의 가상 VRF(Virtual Routing & Forwarding) 인식 가상 컨텍스트가 지원됩니다.

사용자를 VRF 컨텍스트로 매핑할 때 다음 두 가지 기본 모델이 사용됩니다.

- **단일 IP 모델** - 서로 다른 엔터프라이즈의 사용자가 단일 HTTPS 프록시에 대한 VPN 세션을 설정합니다. 브라우저에 사용된 URL 이름 또는 로그인 프로세스에서 사용된 로그인 이름을 통해 실제 사용자와 VRF 간 매핑이 완료됩니다.
- **다중 IP 모델** - 서로 다른 엔터프라이즈의 사용자가 다중 HTTPS 프록시에 대한 VPN 세션을 설정합니다(HTTP 프록시당 1 개의 엔터프라이즈). HTTPS 프록시 인스턴스에 따라 사용자와 VRF 간의 매핑이 포함됩니다.

각 VRF 컨텍스트는 다음과 같은 네트워크 리소스를 지원합니다.

- **VRF 인증, 권한 부여 및 계정(AAA) 단위 서버** - 사용자 인증용
- **VRF DNS(Domain Name System) 단위 서버** - 엔터프라이즈 수준의 이름 변환
- **VRF 기본 단위 게이트웨이** - VRF 도메인 내 라우팅 IP 패킷
- **VRF 단위 허용된 최대 사용자 수** - 엔터프라이즈 수준의 출입 제한

어드밴스드 엔드포인트 보안

Cisco Secure Desktop은 Cisco WebVPN Services Module의 기본 구성 요소로서, 사전 연결 보안 상태 평가를 수행하며 SSL VPN 세션이 종료된 이후에 남아 있는 쿠키, 브라우저 기록, 임시 파일, 다운로드된 콘텐츠 등과 같은 데이터를 최소화합니다.

SSL VPN 에 대한 광범위한 애플리케이션 지원

Cisco WebVPN Services Module은 동적으로 다운로드된 SSL VPN 클라이언트를 통해 포괄적인 애플리케이션 지원을 제공하여 모든 가상 애플리케이션에 네트워크 레이어 연결을 지원합니다. 이 모듈은 웹 기반 애플리케이션을 위한 클라이언트리스(Clientless) 지원을 완벽하게 제공하므로 VPN 사용자는 표준 웹 브라우저를 통해 네트워크 리소스를 투명하고 저렴하게 확장할 수 있습니다. 엑스트라넷과 같은 제한된 애플리케이션 액세스 요구사항을 지닌 환경에서 클라이언트리스(Clientless), 씬클라이언트 포트 포워딩 옵션을 배포할 수 있습니다.

유연성

SSL 및 IPsec는 고유한 사용자 액세스 요구사항을 해결하는 동시에 다양한 기업 사용자 기반의 요건을 충족하는 데 필수적인 보안 기술입니다. IPsec와 SSL VPN을 모두 지원하므로 기업에서 다른 시나리오를 통해 네트워크에 액세스하는 사용자에게 가장 적합한 기술을 선택할 수 있도록 해줍니다. 이 소프트웨어는 단일 플랫폼에서 최대의 유연성과 애플리케이션 액세스를 모두 제공하므로 인프라를 개별적으로 배포하여 관리할 필요가 없습니다.

간편한 배포

Cisco WebVPN Services Module과 함께 통합 장치 관리자 지원이 제공됩니다. 이 지원을 통해 배포 준비

(ready-to-deploy) 솔루션을 제공하는 외부 요소 관리 시스템을 갖추지 않고도 모듈을 구성하고 프로비전할 수 있도록 지원합니다.

작동 모드

클라이언트리스 모드(Clientless Mode)

클라이언트리스 모드(Clientless Mode)에서는 다음과 같은 애플리케이션이 지원됩니다. 이 애플리케이션들은 웹 브라우저를 클라이언트로 사용합니다.

- 웹 브라우징(HTTP/HTTPS)
- 파일 공유(CIFS: Common Internet File System)
- WebDAV 확장을 사용한 Microsoft Outlook Web Access(HTTP/HTTPS)와 같은 웹 전자메일

씬클라이언트 모드(Thin-Client Mode)

씬클라이언트 모드(Thin-Client Mode)에서 지원되는 애플리케이션(예; TCP 포트 포워딩)은 메일 기반 애플리케이션(예: SMTP, POP3 및 IMAP4), 터미널 서비스, 인스턴트 메시징 및 텔넷과 같은 TCP/IP 클라이언트 서버 애플리케이션을 지원합니다.

터널 모드(Tunnel Mode)

터널 모드(Tunnel Mode)는 대부분의 IP 기반 애플리케이션을 지원하는 SSL 터널을 통해 네트워크 레이어에서 사용자의 VPN 트래픽을 리디렉션합니다. 다른 SSL VPN 작동 모드에서 제한된 수의 애플리케이션이 지원되는 것과 달리, 터널 모드는 Meeting-Maker, Microsoft Outlook, Microsoft Exchange, Lotus Notes E-Mail 및 Telnet을 비롯하여 일반적으로 사용되고 있는 기업용 애플리케이션의 대부분이 지원됩니다. 3270 터미널 에뮬레이션과 같은 일부 레거시 애플리케이션도 지원됩니다.

표 1은 Cisco WebVPN Services Module의 주요 기능을 나타내고, 표 2는 시스템 요구사항을 나타냅니다.

표 1. 기능 가용성

주요 기능	설명
확장성	<ul style="list-style-type: none"> • 최대 8000명의 사용자 • 최대 300Mbps • 최대 64개의 SSL VPN 가상 컨텍스트 및 64개의 게이트웨이 • 새시당 최대 4개의 모듈
가상화	여러 컨텍스트를 분할하는 기능(각 컨텍스트를 개별 정책과 구성을 갖춘 WebVPN Services Module 로 완벽하고 논리적으로

	표현)
VRF 인식	<ul style="list-style-type: none"> • VRF 매핑 • 단일 IP 모델(URL 기반 또는 로그인 이름 기반) • 다중 IP 모델 • VRF AAA 단위 서버 • VRF DNS 단위 서버 • VRF 단위 게이트웨이 • VRF 단위 사용자 수
사용자 인증	<ul style="list-style-type: none"> • RADIUS • Windows NT, Active Directory, UNIX NIS • Cisco Secure Access Control Server(ACS)를 사용하여 그룹 기반 액세스 제어
엔드 시스템 무결성(Cisco Secure Desktop 통합)	<ul style="list-style-type: none"> • 바이러스 백신 검사 • 개인 방화벽 검사 • 임시 파일/쿠키 및 다운로드한 파일/쿠키가 시스템에 남아 있는 위험을 최소화하려고 합니다.
리던던시 및 로드 공유	<ul style="list-style-type: none"> • 상태비저장 장애복구 • Cisco IOS® Software Sserver-Load Balancing(SLB) 및 새시 내 Content Switching Module 통합 • 활성/활성 장애복구
애플리케이션 지원	웹 액세스, 파일 서비스, 전자메일, 텔넷, 파일 전송, 레거시 애플리케이션, 특수 애플리케이션
브라우저 지원	Netscape, Internet Explorer, Firefox
프로토콜	SSL 3.0, 3.1 및 TLS 1.0
구성 및 관리	Console CLI, HTTP, HTTPS, Telnet, SSH(Secure Shell)
Syslog 지원	콘솔 디스플레이, 외부 서버 및 내부 버퍼
암호화 제품군	<ul style="list-style-type: none"> • SSL_RSA_WITH_RC4_128_MD5 • SSL_RSA_WITH_RC4_128_SHA • SSL_RSA_WITH_RC4_128_MD5 • SSL_RSA_WITH_3DES_EDE_CBC_SHA
네트워크 액세스 제어	IP 주소, DSCP/ToS(Differentiated Services Code Point/Type of Service), TCP/UDP(User Datagram Protocol) 포트, 사용자 단위, 그룹 단위

표 2. 시스템 사양

주요 기능	설명
샐시	Cisco Catalyst 6500 시리즈 또는 Cisco 7600 시리즈
수퍼바이저 엔진	Supervisor Engine 720 또는 Supervisor Engine 2/MSFC2
샐시 소프트웨어 호환성	<ul style="list-style-type: none"> • WebVPN Software Version 1.1 • Native Cisco IOS Software Release • 12.2(17d)SXB7 • 12.2(18)SXE2
샐시 내 모듈 최대 수	4 개
카드/포트/슬롯	모듈당 1 개 슬롯
Cisco WebVPN Software 버전	1.1
Maintenance Partition(MP) Version	3.1(1)

주문 정보

주문하려면 [시스코 주문 홈 페이지](#)를 방문하거나 표 3를 참조하십시오.

표 3. 주문 정보

부품 번호	설명
WS-SVC-WEBVPN-K9	Cisco Catalyst 6500 시리즈 및 Cisco 7600 시리즈를 위한 WebVPN Services Module
WS-SVC-WEBVPN-K9=	WebVPN Services Module(예비용)
SC-SVC-WVPN-11-K9	WebVPN Services 모듈 소프트웨어 1.1
SC-SVC-WVPN-11-K9=	WebVPN Services Module Software 1.1(예비용)

사용자 라이선스

Cisco WebVPN Services Module은 기본 시스템을 사용하여 2500명의 사용자 구성이 가능합니다. 2500명의 사용자에 대한 추가 라이선스는 필요 없습니다. 추가 사용자는 다음 부품 번호를 사용하십시오.

표 4. 사용자 라이선스

부품 번호	설명
FR-SVC-WVPN-5000	Cisco 6500 및 Cisco 7600 WebVPN 5000 사용자 라이선스
FR-SVC-WVPN-8000	Cisco 6500 및 Cisco 7600 WebVPN 8000 사용자 라이선스

소프트웨어를 다운로드하려면 [Cisco Software Center](#)(로그인 필요)를 이용하십시오.

서비스 및 지원

시스코는 고객의 성공을 촉진하는 다양한 서비스 프로그램을 제공합니다. 이러한 혁신적인 서비스 프로그램은 수준 높은 인력, 프로세스, 톨 및 파트너의 기술력이 어우러진 것으로서 그 결과는 높은 고객 만족도로 나타납니다. 시스코 서비스는 여러분의 네트워크 투자를 보호하고 네트워크 운영을 최적화하며, 새로운 애플리케이션에 대비해 네트워크 인텔리전스와 비즈니스 역량을 높일 수 있도록 도와줍니다. 시스코 서비스에 대한 자세한 내용은 [시스코 기술 지원 서비스](#)나 [시스코 어드벤스드 서비스](#)를 참조하십시오.

규정 준수

안전성

- UL 1950
- CSA C22.2 No. 950-95
- EN60950
- EN60825-1
- TS001
- CE 준수 정보
- IEC 60950
- AS/NZS3260

EMI

- FCC Part 15 Class A
- ICES-003 Class A
- VCCI Class B
- EN55022 Class B
- CISPR22 Class B
- CE 준수 정보

- AS/NZS3548 Class B

NEBS

- SR-3580-NEBS: Criteria 수준(Level 3 준수)
- GR-63-CORE-NEBS: 물리적 보호
- GR-1089-CORE-NEBS: EMC 및 안전성

ETSI

- ETS-300386-2 스위칭 장비

통신

- ITU-T G.610
- ITU-T G0.703
- ITU-T G0.707
- ITU-T G.783 섹션 9-10
- ITU-T G0.784
- ITU-T G0.803
- ITU-T G0.813
- ITU-T G0.825
- ITU-T G0.826
- ITU-T G0.841
- ITU-T G.957 테이블 3
- ITU-T G0.958
- ITU-T I.361
- ITU-T I.363
- ITU I.432
- ITU-T Q.2110
- ITU-T Q.2130
- ITU-T Q.2140
- ITU-T Q.2931
- ITU-T O.151
- ITU-T O.171
- ETSI ETS 300 417-1-1
- TAS SC BISDN(1998)
- ACA TS 026(1997)

- BABT/TC/139(Draft 1e)

<업데이트: 2008년 9월 22일>