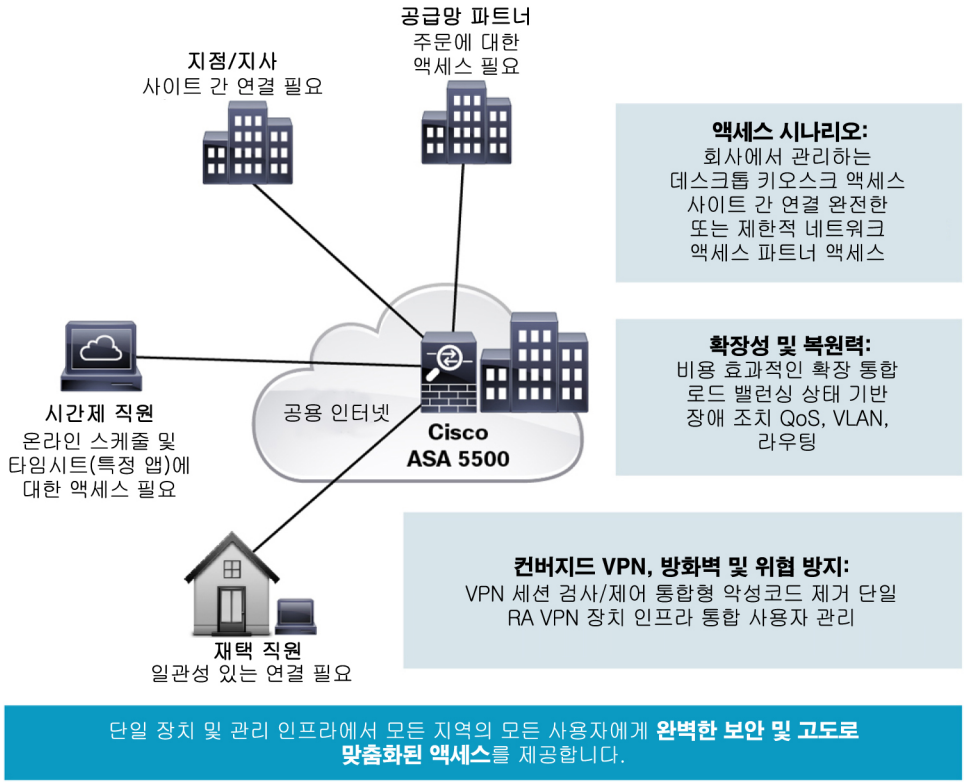
Cisco AnyConnect Secure Mobility Solution: Cisco AnyConnect Secure Mobility Client 및 Cisco ASA 5500 Series(SSL/IPsec VPN Edition)

Cisco® ASA 5500 Series ASA(Adaptive Security Appliance)는 중소기업 및 대기업 애플리케이션에 맞는 동급 최고의 보안 및 VPN 서비스를 갖춘 맞춤형 플랫폼입니다. Cisco ASA 5500 Series는 원격 액세스(SSL/IPsec VPN), 사이트 간 VPN, 방화벽, 콘텐츠 보안 및 침입 방지 기능을 갖춘 특별한 제품으로 특정 구축 환경 및 옵션에 맞게 맞춤화할 수 있습니다.

Cisco AnyConnect Secure Mobility Solution은 기업 보안 정책의 무결성(integrity)에 손상을 주지 않고 조직에 인터넷 전송의 연결과 비용 혜택을 제공합니다. SSL(Secure Sockets Layer) 및 IPsec(IP Security) VPN 서비스와 포괄적인 위협 방어 기술을 결합하여 Cisco ASA 5500 Series는 다양한 구축 환경의 필요 요건에 맞춰 편리하게 맞춤화할 수 있는 네트워크 액세스를 제공하는 동시에 고급 엔드포인트 및 네트워크 보안을 제공합니다(그림 1).

그림 1. 모든 구축 시나리오에 맞게 맞춤화 가능한 VPN 서비스



Cisco ASA 5500 Series SSL/IPsec VPN Edition

이 모델은 모든 연결 시나리오에 맞는 유연한 VPN 기술을 제공하며 디바이스당 동시 사용자를 최대 10,000명까지 확장할 수 있습니다. 또한 다음을 통해 관리하기 쉬운 풀터널(Full-tunnel) 네트워크 액세스를 제공합니다.

- SSL(DTLS 및 TLS)
- IPsec VPN 클라이언트 기술
- Cisco Web Security에 맞게 최적화된 Cisco AnyConnect Secure Mobility Solution
- 고급 클라이언트리스 SSL VPN 기능
- 네트워크 인식 사이트 간 VPN 연결

이를 통해 모바일 사용자, 원격 사이트, 계약자 및 비즈니스 파트너에게 공용 네트워크 전반에서 매우 안전한 연결을 지원합니다. VPN 확장 및 보안을 위한 보조 장비를 구매할 필요가 없으므로 VPN 구축 및 운영과 관련된 비용이 절감됩니다.

Cisco AnyConnect Secure Mobility Solution의 장점은 다음과 같습니다.

- **SSL(TLS & DTLS) 및 IPsec 기반 전체 네트워크 액세스:** 전체 네트워크 액세스 기능으로 네트워크 레이어에서 원격 사용자 연결을 거의 모든 애플리케이션 또는 네트워크 리소스에 제공합니다. 이러한 기능은 회사 소유 노트북 컴퓨터와 같은 관리되고 있는 컴퓨터의 액세스를 확장하는 데에 자주 사용됩니다. 자동으로 다운로드되는 Cisco AnyConnect Secure Mobility Client, Microsoft L2TP(레이어 2 터널링 프로토콜)/IPsec VPN 클라이언트 및 Apple iPhone/Mac OS X 10.6+ IPsec VPN 클라이언트를 통해 연결이 가능합니다.

  Cisco AnyConnect Secure Mobility Client는 네트워크 제한 사항을 기반으로 터널링 프로토콜을 가장 효율적인 방법으로 조정하며, VoIP(Voice-over-IP) 트래픽 또는 TCP 기반 애플리케이션 액세스 등과 같은 레이턴시에 민감한 트래픽에 맞게 최적화된 연결을 제공하는 데 DTLS 프로토콜을 사용하는 최초의 VPN 제품입니다. SSL(TLS & DTLS) 및 IPsec 기반 원격 액세스 VPN 기술을 지원하므로 Cisco ASA 5500 Series는 다양한 구축 시나리오를 충족할 수 있는 탁월한 유연성을 제공합니다.
- **뛰어난 클라이언트리스(clientless) 네트워크 액세스:** 인터넷 브라우저에서 사용할 수 있는 SSL 암호화의 편재성을 사용하여 AnyConnect Secure Mobility Solution은 클라이언트리스 원격 액세스를 제공합니다. 따라서 데스크톱 VPN 클라이언트 소프트웨어가 없어도 위치와 상관없이 네트워크 애플리케이션 및 리소스에 액세스할 수 있습니다.

  이 솔루션은 웹 기반 애플리케이션 또는 리소스, Citrix 등의 터미널 서비스 애플리케이션, 최적화된 Microsoft Outlook Web Access 및 Lotus iNotes에 클라이언트리스 액세스를 제공합니다. 또한, 이메일, 일정, 인스턴트 메시징, FTP, 텔넷, SSH 애플리케이션 등 일반적인 씩 클라이언트(Thick Client) 애플리케이션에도 액세스를 제공합니다. Cisco ASA 5500 Series는 뛰어난 콘텐츠 리라이팅(content rewriting) 기능으로 Java, JavaScript, ActiveX, Flash 및 기타 고급 콘텐츠가 포함된 복잡한 웹 페이지를 안정적으로 표현할 수 있습니다.
- **Cisco AnyConnect Secure Mobility Solution:** 엔터프라이즈, 사내 소유 또는 SaaS 애플리케이션 모두 사용자의 위치와 상관 없이 모든 트랜잭션에 보안 정책을 시행합니다. 관리자는 Secure Mobility를 사용하여 액세스가 불가능할 경우 네트워크 연결을 허용하거나 거부하는 정책을 사용하여 상시 보안 테트워크 연결을 요구할 수 있습니다. 이러한 서비스는 Cisco Web Security와 사용하도록 최적화되어 있으며, AnyConnect Premium 라이센스 또는 Secure Mobility 라이센스가 필요합니다.
- **네트워크-인식 사이트 간 VPN:** 여러 곳의 사무실 사이에 매우 안전한 고속 통신이 가능합니다. VPN 전반에서 QoS(Quality of service) 및 라우팅이 지원되므로 음성, 비디오, 터미널 서비스 등 레이턴시에 민감한 애플리케이션을 안정적인 비즈니스 품질로 제공할 수 있습니다.
- **위협 방지 원격 액세스 VPN:** VPN은 네트워크에 악성코드가 침투하게 되는 주요 소스입니다. 악성코드에는 웜, 바이러스, 스파이웨어, 키로거, 트로이 목마, 루트킷 등이 포함됩니다. Cisco ASA 5500 Series는 침입 방지, 안티바이러스, 애플리케이션 인지 방화벽(Application-Aware Firewall) 및 VPN 엔드포인트 보안 기능의 깊이와 다양성으로 VPN 연결이 보안 위협 침투의 매개체가 될 수 있는 위험을 최소화됩니다.

- **비용 효율적인 VPN 구축 및 운영:** VPN을 확장하거나 보안을 적용하려면 대부분 추가적인 로드 밸런싱(load balancing)과 보안 장비가 필요하며, 이로 인해 장비 및 운영 비용이 증가합니다. Cisco ASA 5500 Series에는 이러한 기능이 통합되어 오늘날 사용 가능한 VPN 제품 중에서 전례 없는 수준의 네트워크 및 보안 통합을 제공합니다. 단일 플랫폼에서 유연한 터널링 옵션을 지원하는 Cisco ASA 5500 Series는 고객에게 병렬 VPN 인프라 구축을 대체할 수 있는 비용 효율적인 대안을 제공합니다.
- **확장성 및 복원력 -** Cisco ASA 5500 Series는 디바이스당 최대 10,000개의 동시 사용자 세션을 지원할 수 있으며, 통합 클러스터링 및 로드 밸런싱 기능을 통해 수만 개의 동시 사용자 세션으로 확장할 수 있습니다. 스테이트풀 페일오버(Stateful failover) 기능으로 탁월한 업타임의 고가용성 서비스를 제공합니다.
- **OpenSSL 기술 -** Cisco AnyConnect Secure Mobility Client에는 OpenSSL Toolkit에 사용하도록 OpenSSL Project에서 개발된 소프트웨어가 포함되어 있습니다(http://www.openssl.org).

맞춤화 가능한 원격 액세스 VPN 기능

전체 네트워크 액세스

Cisco ASA 5500 Series SSL/IPsec VPN Edition은 Cisco AnyConnect Secure Mobility Client(표 1 참조) 또는 Cisco IPsec VPN Client에서 사용 가능한 네트워크 터널링 기능을 통해 폭넓은 애플리케이션 및 네트워크 리소스 액세스를 제공합니다.

표 1. Cisco AnyConnect Secure Mobility Client 기능

기능	혜택
폭넓은 운영 체제 지원	• Windows 7 32-bit (x86) 및 64 bit (x64) • Windows Vista 32-bit (x86) 및 64-bit (x64), SP1/SP2(서비스 팩 1, 2) 포함 • XP SP2+ 32-bit (x86) 및 64-bit (x64) • Mac OS X 10.6 이상 • Linux Intel
소프트웨어 액세스	• ASA(Adaptive Security Appliance)에 유효한 SMARTnet 계약이 있는 고객은 Cisco.com에서 사용 가능
최적화된 네트워크 액세스 - VPN 프로토콜 선택 SSL(TLS 및 DTLS) 및 IPsec/IKEv2	• AnyConnect에서 VPN 프로토콜을 선택할 수 있으므로 관리자는 비즈니스 요구에 가장 적합한 프로토콜을 사용할 수 있음 • 터널링 지원에는 SSL(TLS[Transport Layer Security] 및 DTLS[Datagram Transport Layer Security])과 차세대 IPsec(IKEv2)이 포함됨 • DTLS는 VoIP 트래픽 또는 TCP 기반 애플리케이션 액세스 등 레이턴시에 민감한 트래픽에 맞게 최적화된 연결 제공 • TLS(HTTP over TLS/SSL)는 웹 프록시 서버를 사용하는 환경 등 밀폐된 환경에서 네트워크 연결의 가용성 보장 • IPsec/IKEv2는 보안 정책 상 IPsec을 사용해야 하는 경우 레이턴시에 민감한 트래픽에 맞게 최적화된 연결 제공
최적의 게이트웨이 선별	• 최적의 네트워크 액세스 포인트에 연결을 결정하여 설정하므로, 엔드 유저가 가장 가까운 위치를 결정할 필요가 없음
모빌리티 친화적	• 모바일 사용자를 위한 설계 • IP 주소 변경, 연결 손실, 절전 모드또는 대기 모드 중에도 VPN 연결이 유지되도록 구성할 수 있음 • Trusted Network Detection 기능을 통해 엔드 유저가 사무실에 있으면 자동으로 연결이 끊어지고, 원격 위치에 있으면 자동으로 연결되도록 VPN 연결 설정 가능
암호화	• AES-256 및 3DES-168을 비롯한 강력한 암호화 지원(보안 게이트웨이 디바이스에 강력한 암호화 라이센스가 설정되어 있어야 함) • NSA Suite B 알고리즘, IKEv2가 포함된 ESPv3, 4096비트 RSA 키, Diffie-Hellman Group 24 및 고급 SHA2(SHA-256 및 SHA-384)를 비롯한 차세대 암호화(IPsec IKEv2 연결에만 적용됨, Premium ASA 라이센스 필요)
광범위한 구축 및 연결 옵션	구축 옵션: • Microsoft Installer를 비롯한 사전 구축 • ActiveX(Windows 전용) 및 Java를 사용하는 자동 보안 게이트웨이 구축(초기 설치 시 관리자 권한 필요) 연결 모드: • 시스템 아이콘을 사용하는 독립형 • 브라우저에서 시작(Weblaunch) • 클라이언트리스 포털에서 시작 • CLI(Command Line Interface)에서 시작 • API(Application Programming Interface)에서 시작

기능	혜택
광범위한 인증 옵션	• RADIUS • NTLM(NT LAN Manager)에 대한 비밀번호 만료(MSCHAPv2)가 포함된 RADIUS • RADIUS OTP(1회 비밀번호) 지원(상태/응답 메시지 특성) • RSA SecurID(SoftID 통합 포함) • Active Directory/Kerberos • 내장된 CA(Certificate Authority) • 디지털 인증서/스마트카드(Machine Certificate 지원 포함), 자동 선택 또는 사용자 선택 • 비밀번호 만료 또는 기한 경과가 포함된 LDAP(Lightweight Directory Access Protocol) • 일반 LDAP 지원 • 인증서 및 사용자 이름/비밀번호 멀티팩터 인증 결합(이중 인증)
일관성 있는 사용자 환경	• 풀 터널 클라이언트 모드는 LAN과 같은 일관된 사용자 환경이 필요한 원격 액세스 사용자 지원 • 다중 전달 방법으로 Cisco AnyConnect의 폭넓은 호환성 보장 • 사용자는 AnyConnect에 대한 푸시 업데이트 지연 가능 • 고객 경험 피드백 옵션
중앙 집중식 정책 제어 및 관리	• 정책을 로컬에서 구성하거나 미리 구성할 수 있으며, VPN 보안 게이트웨이에서 자동으로 업데이트할 수 있음 • AnyConnect용 API(Application Programming Interface)를 통해 웹 페이지 또는 애플리케이션에서 손쉽게 구축 • 신뢰할 수 없는 인증서 확인 및 사용자에게 경고 • 인증서를 로컬에서 리포팅 관리할 수 있음
고급 IP 네트워크 연결	• IPv4 및 IPv6 네트워크와의 공개 연결 • SSL을 통해 내부 IPv4 및 IPv6 네트워크 리소스에 액세스(내부 v6에는 TLS/DTLS 필요) • 관리자가 제어하는 스플릿/전체 터널링 네트워크 액세스 정책 • 액세스 제어 정책 IP 주소 할당 메커니즘: • 정적 • 내부 풀 • DHCP(Dynamic Host Configuration Protocol) • RADIUS/LDAP
사전 연결 상태 평가(Premium 라이센스 필요)	• HostScan 확인 기능은 Cisco Secure Desktop과 함께 사용할 경우, 네트워크 액세스를 허용하기 전에 엔드포인트 시스템에 안티바이러스 소프트웨어, 개인 방화벽 소프트웨어 및 Windows 서비스 팩이 있는지 여부를 확인합니다. • 관리자는 실행 중인 프로세스의 존재 여부를 기반으로 맞춤화 보안 상태 확인을 정의할 수 있습니다. • Cisco Secure Desktop은 원격 시스템에서 워터마크의 존재를 탐지할 수 있으며, 회사에서 소유한 자산을 식별하고 차별화된 액세스를 제공하는 데 이를 사용할 수 있습니다. 다음과 같은 워터마크 확인 기능을 포함합니다. ◦ 시스템 레지스트리 값 ◦ 필수 CRC32 체크섬과 일치하는 파일 존재 ◦ IP 주소 범위 일치 ◦ 일치에 의해/대해 발급된 인증서 • 규정을 준수하지 않는 애플리케이션의 복구 프로세스를 자동화하는 데 고급 엔드포인트 평가 옵션을 사용할 수 있습니다.
클라이언트 방화벽 정책	• 스플릿 터널링 구성에 보호 기능 추가 • Cisco Secure Mobility와 함께 사용할 경우 로컬 액세스 예외 허용 가능(예: 인쇄, 테더링 디바이스 등) • IPv4용 포트 기반 규칙 및 IPv6용 네트워크/IP ACL(Access control lists) 지원 • Windows XP SP2, Vista, Windows 7 및 Mac OS X에서 사용 가능
현지화	영어 외에도 다음 언어가 지원됩니다. • 체코어(cs-cz) • 독일어(de-de) • 라틴 아메리카 스페인어(es-co) • 캐나다 프랑스어(fr-ca) • 일본어(ja-jp) • 한국어(ko-kr) • 폴란드어(pl-pl) • 중국어 간체(zh-cn)

기능	혜택
간편한 클라이언트 관리	• 관리자는 헤드엔드 보안 어플라이언스에서 소프트웨어 및 정책 업데이트를 자동으로 구축할 수 있으므로, 클라이언트 소프트웨어 업데이트와 관련된 관리 작업이 제거됩니다. • 관리자는 엔드 유저 구성을 위해 어떤 기능을 사용할지를 결정할 수 있습니다. • 도메인 로그인 스크립트를 사용할 수 없을 경우 관리자는 연결/연결 해제 시 엔드포인트 스크립트를 트리거할 수 있습니다. • 관리자는 엔드 유저에게 표시될 메시지를 완전히 맞춤화 및 현지화할 수 있습니다.
AnyConnect 프로필 편집기	• Cisco ASDM(Adaptive Security Device Manager)에서 직접 AnyConnect 정책을 맞춤화할 수 있습니다.
진단	• 온-디바이스 통계 및 로깅 정보 • 디바이스의 로그 보기 • Cisco 또는 관리자에게 로그를 분석용으로 손쉽게 이메일할 수 있음
FIPS(Federal Information Processing Standard)	• FIPS 140-2 Level 2 규격(플랫폼, 기능 및 버전 제한 적용)
간편한 클라이언트 관리	• 관리자는 Cisco AnyConnect Secure Mobility Client를 통해 보안 게이트웨이에서 소프트웨어 및 정책 업데이트를 자동으로 구축할 수 있으므로, 클라이언트 소프트웨어 업데이트와 관련된 관리 작업이 제거됩니다. • 관리자는 엔드 유저 구성을 위해 어떤 기능을 사용할지를 결정할 수 있습니다. • 도메인 로그인 스크립트를 사용할 수 없을 경우 관리자는 연결/연결 해제 시 엔드포인트 스크립트를 트리거할 수 있습니다. • 관리자는 엔드 유저에게 표시될 메시지를 완전히 맞춤화 및 현지화할 수 있습니다.
일관성 있는 사용자 환경	• 전체 터널 클라이언트 모드는 LAN과 같은 일관된 사용자 환경이 필요한 원격 액세스 사용자 지원 • 여러 제공 방법 및 작은 다운로드 크기 덕분에 Cisco AnyConnect Secure Mobility Client의 폭넓은 호환성과 빠른 다운로드가 보장됨
고급 IP 네트워크 연결	• IPv4 및 IPv6 네트워크와의 공개 연결 • SSL을 통해 내부 IPv4 및 IPv6 네트워크 리소스에 액세스(v6 내부에는 TLS/DTLS 필요) • 관리자가 제어하는 분할/전체 터널링 네트워크 액세스 정책 • 액세스 제어 정책 IP 주소 할당 메커니즘: • 정적 • 내부 풀 • DHCP(Dynamic Host Configuration Protocol) • ADIUS/LDAP(Lightweight Directory Access Protocol)
클라이언트 방화벽 정책	• 스플릿 터널링 구성을 위한 보호 기능 추가 • Cisco Mobile User Security와 함께 사용할 경우 로컬 액세스 예외 허용 가능(예: 인쇄, 테더링 디바이스 등) • IPv4용 포트 기반 규칙 및 IPv6용 네트워크/IP ACL(Access control lists) 지원 • Windows XP SP2, Vista, Windows 7 및 Mac OS X에서 사용 가능
Cisco AnyConnect 프로필 편집기	• Cisco ASDM(Adaptive Security Device Manager)에서 직접 AnyConnect 정책을 맞춤화할 수 있습니다.

표 2에는 Cisco AnyConnect 라이센싱 옵션이 요약되어 있습니다.

표 2. Cisco AnyConnect 라이센싱 옵션

라이센스 요구 사항 (아래의 각 라이센스가 필요함)	설명
Cisco ASA 플랫폼 라이센스	**Cisco AnyConnect Essentials**[1](P/N: (L-ASA-AC-E-55**=) 05, 10, 20, 40, 50,80, 85) • 매우 안전한 원격 액세스 연결 • ASA 디바이스 모델당 단일 라이센스(사용자당 라이센스 아님), 플랫폼에서 최적의 동시 사용자 지원 • 엔터프라이즈 애플리케이션에 풀-터널링 액세스
	Cisco AnyConnect Premium[2](P/N: (L-ASA-SSL-***=) 10, 25, 50, 100, 250, 500, 1000, 2500, 5000, 10,000) • Cisco Secure Desktop HostScan 및 Always-On VPN 연결을 비롯한 데스크톱 AnyConnect 플랫폼에서 사용할 수 있는 클라이언트리스 SSL VPN 및 기능 지원 제공 • 동시 사용자 수 기반 라이센스, 단일 디바이스 또는 공유 라이센스로서 사용 가능

[1] **를 ASA 모델 번호의 마지막 숫자 두 개와 교체하십시오.
[2] ***를 총 라이센스 시트 수와 교체하십시오.

Cisco AnyConnect 모바일 라이센스[5] P/N: (L-ASA-AC-M-55*=) 05, 10, 20, 40, 50,80, 85	• 모바일 OS 플랫폼 호환성 지원 • ASA 디바이스 모델당 단일 라이센스(사용자당 라이센스 아님), Essentials 또는 Premium 라이센스 외에 추가로 필요

클라이언트 네트워크 액세스

표 3과 같이 Cisco ASA 5500 Series 클라이언트리스 SSL VPN 액세스 기능을 사용하면 특정 네트워크 리소스 및 애플리케이션에 정확하게 제어된 웹 기반 방식으로 액세스할 수 있습니다. 인터넷 키오스크, 공유 컴퓨터, 엑스트라넷 파트너, 직원 소유 데스크톱, 회사 소유 직원 데스크톱 등에서 액세스할 수 있습니다.

표 3. Cisco ASA 5500 Series 웹 기반 클라이언트리스 액세스

기능	설명
신뢰할 수 있는 폭넓은 호환성	고급 전환 기능은 HTML, Java, ActiveX, JavaScript 및 Flash를 비롯한 복잡한 콘텐츠가 포함된 웹 페이지의 호환성을 보장합니다.
통합 클라이언트리스 애플리케이션 최적화	Microsoft Outlook Web Access와 Lotus iNotes 등 리소스 집약적 애플리케이션에 대한 통합 성능 최적화를 통해 뛰어난 응답 시간 및 낮은 레이턴시가 지원되므로 고품질 SSL VPN 엔드 유저 환경이 제공됩니다.
맞춤화 가능한 사용자 환경	고급 클라이언트리스 포털의 특징은 세부적인 액세스를 위한 그룹 기반 맞춤화, 사용 편의성 및 맞춤화 가능한 사용자 환경입니다. • 다중 언어, 클라이언트리스 사용자 포털 지원 • 맞춤화 가능한 리소스 책갈피 • 중요한 실시간 콘텐츠의 자동 업데이트를 위한 RSS(Really Simple Syndication) 기반 정보 리소스 게시
완전한 클라이언트리스 Citrix 액세스	클라이언트리스 SSL VPN을 통한 Citrix 액세스에 별도의 도우미 애플리케이션이 필요하지 않으므로 애플리케이션을 빠른 속도로 초기화할 수 있으며 데스크톱 소프트웨어 충돌 위험이 줄어듭니다.
통합 클라이언트-서버 애플리케이션 지원	원격 클라이언트를 미리 구축하지 않고도 일반적인 클라이언트-서버 애플리케이션에 액세스할 수 있으므로 텔넷, SSH, RDP(Remote Desktop Protocol), VNC(Virtual Network Computing) 리소스에 빠르게 액세스할 수 있습니다.
일반적인 씩 클라이언트 (thick-client) 애플리케이션 지원	포트 전달 기능 덕분에 다음과 같은 작은 Java 애플릿을 통해 대중적인 씩 클라이언트(thick-client) 애플리케이션에 클라이언트 없이 액세스할 수 있습니다. • POP(Post Office Protocol) • SMTP(Simple Mail Transfer Protocol) • IMAP(Internet Message Access Protocol) • 이메일 • 온라인 일정 • 인스턴트 메시징 • Telnet • SSH • 기타 클라이언트에서 시작되는 TCP 애플리케이션 스마트 터널링을 통해 Microsoft Windows 사용자는 관리자 권한이라는 전제 조건 없이도 TCP 애플리케이션에 액세스할 수 있고, VPN 관리자는 승인된 애플리케이션만 내부 리소스에 액세스하도록 허용할 수 있습니다.
다양한 브라우저 지원	Microsoft Internet Explorer, Firefox, Opera, Safari, PIE(Pocket Internet Explorer)를 비롯한 여러 브라우저가 지원되므로 어디에서든 폭넓은 연결 호환성이 보장됩니다.
고급 IP 네트워크 연결	내부 IPv4 및 IPv6 네트워크 리소스에 액세스합니다.

포괄적인 인증 및 권한 부여 선택 사항

Cisco ASA 5500 Series는 표 4에서 볼 수 있듯이 사용자 인증 및 권한 부여를 위한 포괄적인 옵션 집합을 제공합니다.

표 4. Cisco ASA 5500 Series 인증 및 권한 부여 옵션

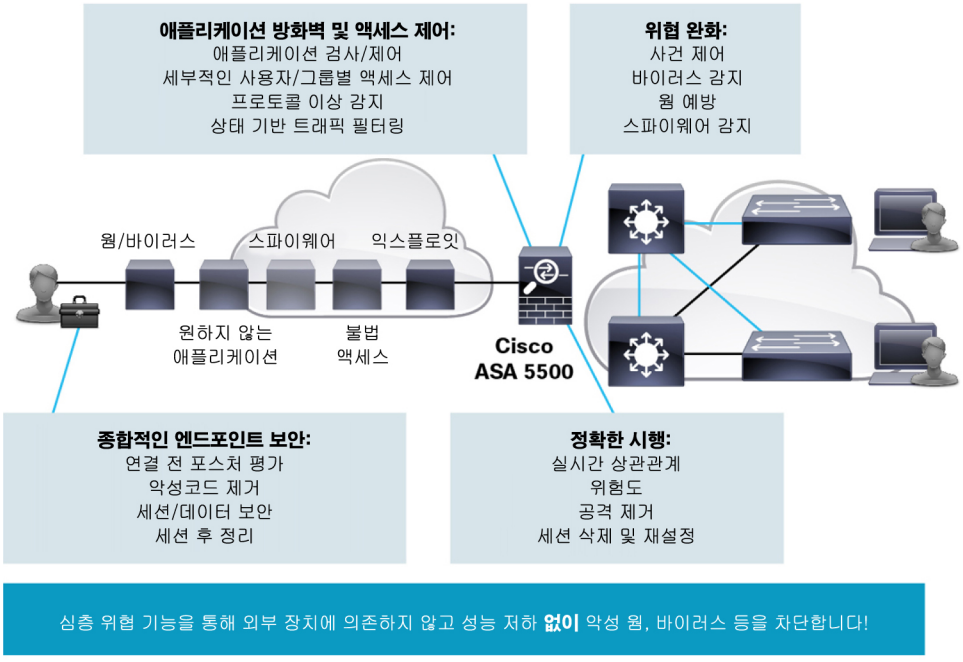
기능	설명
인증 옵션	• RADIUS • NTLM(NT LAN Manager)의 비밀번호 만료(MSCHAPv2)가 포함된 RADIUS • RADIUS 1회 비밀번호(OTP) 지원(상태/응답 메시지 특성) • RSA SecurID • 이중 인증 • Active Directory/Kerberos

	• 내장된 CA(Certificate Authority) • 디지털 인증서/스마트카드(Cisco AnyConnect용 머신 인증서 포함) • 비밀번호 만료 또는 기한 경과가 포함된 LDAP • 일반 LDAP 지원 • 인증서 및 사용자 이름/비밀번호 멀티팩터 인증 결합(이중 인증) • 간소화된 SSO(Single Sign-On)의 입력을 요구하는 내부 도메인 비밀번호 • 키스트록 로거에 대한 추가 보호를 위한 SSL VPN 가상 키보드 인증
고급 권한 부여	• RADIUS 및 LDAP에서의 정책 매핑 • 사용자 정책 작성을 위한 도메인 구성원 자격과 보안 상태를 직접 사용하는 동적 액세스 정책
클라이언트리스 SSL VPN 사용자용 단일 로그인	• 컴퓨터와 Siteminder 연결 • RSA Access Manager(ClearTrust) • SAML(Security Assertion Markup Language) • 기본/NTLM 인증 패스쓰루 • 양식 기반 인증 패스쓰루

위협 방지 VPN 기능

Cisco ASA 5500 Series SSL/IPsec VPN Edition은 통합 네트워크 및 엔드포인트 보안 기술을 통해 VPN 구축에 맞는 고급 보안을 제공합니다. 웜, 바이러스, 스파이웨어, 키로거, 트로이 목마, 루트킷, 해킹 등의 네트워크 공격을 막으려면 VPN 보안이 필요합니다. 세부적인 애플리케이션 및 액세스 제어 정책을 사용하면, 개인 및 사용자 그룹이 자격이 부여된 애플리케이션과 네트워크 서비스에만 액세스하도록 할 수 있습니다(그림 2).

그림 2. VPN 위협을 막기 위해 온보드 보안을 사용하는 위협 방지 VPN 서비스



VPN 게이트웨이에서의 네트워크 보안

웜, 바이러스, 애플리케이션 내장 공격 및 애플리케이션 오용은 오늘날 네트워크에 존재하는 가장 큰 보안 문제입니다. VPN 디바이스의 제한적인 보안 기능 때문에 원격 액세스 및 원격 지사 VPN 연결이 이러한 위협의 일반적인 진입점이 됩니다. 본사 위치에서 터널 종단 지점에 대해 적절한 검사와 위협 완화 조치를 적용하지 않은 채 VPN을 구축하는 경우가 많습니다. 따라서 원격 지사 또는 사용자로부터 악성코드가 네트워크에 침투하여 확산될 수 있습니다.

Cisco ASA 5500 Series의 통합 위협 완화 기능을 사용하면 고객은 악성코드를 탐지하고, 네트워크 내부에 침투하기 전에 차단할 수 있습니다. 피어 투 피어 네트워크에서 파일 공유를 통해 확산되는 스파이웨어나 애드웨어 등의 애플리케이션 내장 공격을 막기 위해 Cisco ASA 5500 Series는 애플리케이션 트래픽을 심층적으로 검사합니다. 이 솔루션은 위험한 페이로드를 식별하고, 대상에 도달하여 손상을 일으키기 전에 해당 콘텐츠를 삭제합니다.

표 5에는 Cisco ASA 5500 Series에서 제공하는 몇 가지 VPN 게이트웨이 보안 기능이 나와 있습니다.

표 5. Cisco ASA 5500 Series VPN 게이트웨이에서의 네트워크 보안

기능	설명
확장 악성코드 완화	웜, 바이러스, 스파이웨어, 키로거, 트로이 목마 및 루트킷은 Cisco ASA 5500 Series VPN 게이트웨이에서 차단되므로 네트워크에 확산되기 전에 위협이 제거됩니다.
애플리케이션 인지 방화벽 (Application-Aware Firewall) 및 액세스 제어	애플리케이션 인식 트래픽 검사는 철저한 사용자 액세스 제어를 지원하고, VPN 연결 전체에서의 피어 투 피어 파일 공유 등 원하지 않는 애플리케이션의 오용을 방지합니다.
침입 방지	Cisco ASA 5500 Series는 수많은 악용 요소로부터 네트워크를 보호합니다.
액세스 제한	기밀 리소스에 대한 액세스의 허용 또는 거부는 유연한 구성 정책 및 현재의 상태를 기반으로 합니다.
VLAN(Virtual LAN) 매핑	사용자 기반 및 그룹 기반 트래픽 액세스 제한의 시행은 구성된 VLAN을 기반으로 합니다.

SSL VPN에 대한 포괄적인 엔드포인트 보안

SSL VPN을 구축하면 매우 안전한 엔드포인트 및 기업에서 관리하지 않는 엔드포인트 모두에서 보편적인 액세스가 가능하며, 네트워크 리소스를 다양한 사용자 커뮤니티로 확장할 수 있습니다. 사용자는 기업에서 관리하는 PC, 네트워크에 액세스할 수 있는 개인 디바이스, 공용 터미널 또는 기타 디바이스에서 네트워크에 액세스할 수 있습니다. 네트워크가 이렇게 확장되면 잠재적인 네트워크 보안 공격 지점도 증가합니다.

Cisco Secure Desktop은 쿠키, 브라우저 기록, 임시 파일, 다운로드한 콘텐츠 등 SSL VPN 세션이 종료된 후 남겨지는 데이터를 최소화합니다. Cisco NAC Appliance 및 Cisco NAC Framework의 통합을 통해 전체 네트워크 액세스 사용자에 대한 엔드포인트 상태 확인을 이용할 수도 있습니다. 표 6에서는 Cisco Secure Desktop 기능을 설명합니다 (Premium License 필요).

표 6. 네트워크에서 엔드포인트까지 포괄적인 보안 정보를 제공하는 Cisco Secure Desktop

기능	설명
사전 연결 상태 평가	호스트 무결성 확인 기능은 네트워크 액세스를 허용하기 전에 엔드포인트 시스템에 안티바이러스 소프트웨어, 개인 방화벽 소프트웨어 및 Windows 서비스 팩이 있는지를 확인합니다. 이러한 메커니즘을 통해 이제 상당히 많은 애플리케이션과 버전이 지원되며, 빈번한 업데이트를 통해 새로운 제품 릴리스를 지원할 수 있습니다. 관리자는 실행 중인 프로세스의 존재 여부를 기반으로 맞춤화 보안 상태 확인을 정의할 수 있습니다.
사전 연결 자산 평가	Cisco Secure Desktop은 원격 시스템에서 워터마크의 존재를 감지할 수 있으며, 그 결과 회사에서 소유한 자산을 식별하고 차별화된 액세스를 제공하는 데 이를 사용할 수 있습니다. 워터마크 확인 기능에는 다음이 포함됩니다. • 시스템 레지스트리 값 • 필수 CRC32 체크섬(checksum)과 일치하는 파일 존재 • IP 주소 범위 일치 • 일치에 의해/대해 발급된 인증서
포괄적인 세션 보호	비밀번호, 파일 다운로드, 기록, 쿠키, 캐시 파일 등 세션과 관련된 모든 데이터에 대해 추가 보호가 제공되며, 세션 데이터는 Cisco Secure Desktop의 매우 안전한 저장소에 암호화되어 저장됩니다.
End-of-Session 데이터 정리	세션이 끝날 때, 매우 안전한 저장소에 저장된 데이터를 덮어씁니다.
Keystroke Logger Detection	Cisco Secure Desktop은 세션이 시작될 때 특정 소프트웨어 기반 키스트로크 로깅에 대해 초기 검사를 수행합니다. 안전한 저장소 내에서 변칙적인 프로그램의 실행이 시작되면, 사용자에게 의심스러운 활동을 중지하도록 알리는 메시지가 표시됩니다.
게스트 권한으로 사용 가능	원격 시스템에서 네트워크에 액세스하는 사용자는 일부 시스템에 대해 관리자 권한을 갖지 못할 수 있는데, 이 경우 게스트 권한만으로 Cisco Secure Desktop을 설치할 수 있습니다. 이 기능을 통해 모든 시스템에서 전달과 설치가 보장됩니다.
Advanced Endpoint Assessment License	규정을 준수하지 않는 애플리케이션의 복구 프로세스를 자동화하는 데 고급 엔드포인트 평가 옵션을 사용할 수 있습니다.

Network-Aware Site-to-Site VPN 기능

Cisco ASA 5500 Series SSL/IPsec VPN Edition은 Network 인식 사이트간 VPN 기능을 사용합니다. 이 기능을 이용하여 기업은 저렴한 인터넷 연결을 통해 전 세계 원격 및 위성 지사로 네트워크를 안전하게 확장할 수 있습니다(표 7).

표 7. Cisco ASA 5500 Series SSL/IPsec VPN Edition 사이트 간 VPN 연결

기능	설명
QoS 사용	음성, 비디오, 터미널 서비스 등 레이턴시에 민감한 애플리케이션을 지원합니다.
네트워크 인식 라우팅	터널링 네이버를 통해 OSPF(Open Shortest Path First) 및 BGP(Border Gateway Protocol)가 지원되므로 손쉬운 네트워크 통합을 위한 네트워크 토폴로지 인식이 지원됩니다.

플랫폼 통합을 통한 VPN 비용 효율성

Cisco ASA 5500 Series에는 보안과 로드 밸런싱 등 다양한 기능이 통합되어 있어서 VPN의 확장과 보안에 필요한 디바이스 수를 줄일 수 있으므로 장비 비용, 아키텍처의 복잡성 및 운영 비용이 줄어듭니다(표 8).

표 8. VPN 구축 보완하는 통합 기능

기능	설명
네트워크 및 엔드포인트 보안	온보드 악성코드 완화, IPS 및 방화벽 기능을 통해 VPN 보안은 향상되며, 구축해야 할 장비의 수는 줄어듭니다.
로드 밸런싱	통합 로드 밸런싱 기능은 값비싼 외부 로드 밸런싱 장비 없이도 다중 섀시 클러스터를 지원합니다.

Cisco ASA 5500 Series 플랫폼 개요

Cisco ASA 5500 Series는 소규모 사무실에서 대기업 본사까지, 사이트별 확장성을 제공합니다. 이러한 확장성은 5505, 5512-X, 5515-X, 5525-X, 5545-X, 5555-X, 5585-10, 5585-20, 5585-40 및 5585-60의 10개 모델을 통해 제공됩니다(그림 3). 5512에서 5555까지의 모델은 공통된 섀시를 공유하며, 동시 서비스 확장성, 투자 보호 및 미래 기술 확장성을 기반으로 구축됩니다.

그림 3. Cisco ASA 5500 Series 포트폴리오

표 9에는 Cisco ASA 5500 Series 모델 사양이 정리되어 있습니다.

표 9. Cisco ASA 5500 Series Adaptive Security Appliance 모델 사양

플랫폼	ASA 5505	ASA 5512-X	ASA 5515-X	ASA 5525-X	ASA 5545-X	ASA 5555-X	ASA 5585-S10	ASA 5585-S20	ASA 5585-S40	ASA 5585-S60
최대 3DES/AES VPN 처리량[1]	100Mbps	200Mbps	250Mbps	300Mbps	400Mbps	700Mbps	1Gbps	2Gbps	3Gbps	5Gbps
최대 사이트 간 및 IPsec IKEv1 클라이언트 VPN 사용자 세션[1]	25	250	250	750	2500	5000	5000	10,000	10,000	10,000
최대 Cisco AnyConnect 또는 클라이언트리스 VPN 사용자 세션	25	250	250	750	2500	5000	5000	10,000	10,000	10,000
번들된 Premium 사용자 세션	2									
스테이트풀 장애 초치(Stateful Failover)	아니오	예								

플랫폼	ASA 5505	ASA 5512-X	ASA 5515-X	ASA 5525-X	ASA 5545-X	ASA 5555-X	ASA 5585-S10	ASA 5585-S20	ASA 5585-S40	ASA 5585-S60
VPN 로드 밸런싱(VPN Load Balancing)	아니오	예								
공유 VPN 라이센스 옵션	아니오	예								

	ASA 5505	ASA 5512-X	ASA 5515-X	ASA 5525-X	ASA 5545-X	ASA 5555-X	ASA 5585 SSP-10/20	ASA 5585 SSP-40/60
하드웨어								
CPU	싱글 코어	멀티코어 엔터프라이즈급						
메모리(RAM)	512MB	4GB	8GB		12GB	16GB	6/12GB	12/24GB
플래시(Flash)	128MB	4GB	8GB				2 GB	
통합 네트워크 (GE) 포트	8x 10/100 switch ports with 2 PoE ports	6		8			8x 10/100/1000 2x 10 GE3 SFP+ (SSP-10/20) 16x 10/100/1000 4x 10GE3 SFP+ (SSP-10/20 또는 IPS SSP-10/20)	6x 10/100/1000 4x 10 GE SFP+ (SSP-40/60) 12x 10/100/1000 8x 10GE SFP+ (SSP-40/6 또는 IPS SSP-40/60)
인터페이스 카드 슬롯	1x SSC	1x SSM						
인터페이스 카드 옵션	N/A	6-port 10/100/1000, 6-port GE SFP SX, LH, LX						
이중화 전원	아니오				예			
전력 공급 장치	외부, 96W	400W			450W		370W	
제품 외장 사양								
폼 팩터	데스크톱	1RU, 19in. 랙 마운트					2RU, 19in. 랙 마운트	
랙 마운트 옵션	예(랙 마운트 또는 벽면 마운트 키트 포함)	브래킷 포함(슬라이드 레일은 옵션)			슬라이드 레일 포함		랙 마운트 포함	
크기 (H x W x D)	1.75 x 7.89 x 6.87in. (4.45 x 20.04 x 17.45cm)	1.67 x 16.7 x 15.6in. (4.24 x 42.9 x 39.5cm)			1.67 x 16.7 x 19.1in. (4.24 x 42.9 x 48.4cm)		3.47 x 19 x 26.5in. (8.8 x 48.3 x 67.3cm)	
무게	4.0 lb (1.8 kg)	13.39 lb (6.07 kg)	13.39 lb (6.07 kg)	14.92 lb (6.77 kg)	16.82 lb (7.63 kg) 단일 전원 공급 장치 18.86 lb (8.55 kg) 이중 전원 공급 장치		50 lb (22.7 kg) 단일 전원 공급 장치 62 lb (28.2 kg) 이중 전원 공급 장치	

[1] 디바이스에는 평가 및 원격 관리 목적으로 SSL VPN 사용자 2명이 사용할 수 있는 라이센스가 포함되어 있습니다. 총 동시 IPsec 및 SSL(클라이언트리스 및 터널 기반) VPN 세션 수는 이 차트에 표시된 최대 동시 IPsec 세션 수를 초과할 수 없습니다. SSL VPN 세션 수도 디바이스에서 라이센싱된 세션 수를 초과할 수 없습니다. Cisco ASA 5580은 전체 SSL VPN 처리량과 ASA 5550을 비교했을 때에 ASA 5550보다 많은 동시 사용자를 지원합니다. 용량 계획 단계에서 이러한 요소를 고려해야 합니다.

[2] Cisco ASA 5512 Security Plus 라이센스로 업그레이드할 수 있습니다.

공유 VPN 라이센스 옵션	아니오	예	예	예	예	예	예	

플랫폼 호환성

Cisco AnyConnect Secure Mobility Client는 모든 Cisco ASA 5500과 5500-X Series Adaptive Security Appliance 모델(Cisco ASA Software Release 8.0.3 이상 실행) 및 다양한 Cisco IOS® Software 기반 라우터와 호환됩니다.

추가 호환성 정보는 http://www.cisco.com/en/US/docs/security/asa/compatibility/asa-vpn-compatibility.html에서 찾아볼 수 있습니다.

전자 라이센스 제공

대부분의 라이센스는 온라인 제공 방식으로 사용 가능하며, 이를 통해 라이센스 처리 시간이 매우 단축됩니다. 온라인 제공 방식으로 라이센스를 주문하려는 경우, 라이센스와 관련하여 질문이 있거나 평가 라이센스가 필요한 경우 "L"로 시작되는 부품 번호를 주문해야 합니다.

이미 Essentials 또는 Premium ASA 라이센스가 있는 경우 https://tools.cisco.com/SWIFT/Licensing/PrivateRegistrationServlet?FormId=717에서 자동 라이센스 요청 툴을 사용할 수 있습니다.

워런티 정보

Cisco 제품 워런티 페이지에서 워런티 정보를 찾아보십시오.

주문 정보

보안 게이트웨이 라이센스를 주문하려면 Cisco Ordering 홈 페이지를 방문하시기 바랍니다. 호환 플랫폼 및 소프트웨어 액세스 정보는 표 1을 참조하시기 바랍니다.

연결을 시작하려면 보안 게이트웨이 라이센스가 필요합니다. 사용 가능한 옵션에 대한 추가 정보는 Cisco AnyConnect 라이센싱 옵션 섹션을 참조하시기 바랍니다. Cisco AnyConnect와 연결하기 위해 사용할 수 있는 라이센싱 옵션 목록은 Cisco AnyConnect Secure Mobility Client 기능, 라이센스 및 OS 웹 페이지를 참조하시기 바랍니다.

감사의 말

본 제품에는 OpenSSL 툴킷에 사용할 수 있도록 OpenSSL Project(http://www.openssl.org)에서 개발한 소프트웨어가 포함되어 있습니다.

본 제품에는 Eric Young(eay@cryptsoft.com)이 작성한 암호화 소프트웨어가 포함되어 있습니다.

본 제품에는 Tim Hudson(tjh@cryptsoft.com)이 작성한 소프트웨어가 포함되어 있습니다.

본 제품에는 libcurl HTTP 라이브러리가 통합되어 있습니다. Copyright © 1996-2006, Daniel Stenberg, (Daniel@haax.se).

추가 정보

Cisco AnyConnect Secure Mobility Client 홈페이지: http://www.cisco.com/go/anyconnect

Cisco AnyConnect 설명서: http://www.cisco.com/en/US/products/ps8411/tsd_products_support_series_home.html

Cisco ASA 5500 Series Adaptive Security Appliances: http://www.cisco.com/go/asa

Cisco Adaptive Security Device Manager: http://www.cisco.com/go/asdm

Cisco ASA 5500 Series Adaptive Security Appliance 라이센싱 정보:
http://www.cisco.com/en/US/products/ps6120/products_licensing_information_listing.html

AnyConnect 엔드 유저 라이센스 계약 및 개인정보 보호정책:
http://www.cisco.com/en/US/docs/security/vpn_client/anyconnect/eula-seula-privacy/AnyConnect_Supplemental_End_User_License_Agreement.htm

Cisco 제품 인증: http://www.cisco.com/go/securitycert

미주 지역 본부
Cisco Systems, Inc.
San Jose CA

아시아 태평양 지역 본부
Cisco Systems (USA) Pte. Ltd.
싱가포르

유럽 지역 본부
Cisco Systems International BV Amsterdam,
네덜란드

Cisco는 전 세계에 200여 개 이상의 지사가 있습니다. 각 지사의 주소, 전화 번호 및 팩스 번호는 Cisco 웹 사이트 **www.cisco.com/go/offices**에서 확인하십시오.

Printed in USA C78-529285-02 09/12