Cisco AnyConnect Secure Mobility Client

사용이 쉽고, 강력한 보안을 자랑합니다. Cisco AnyConnect® Secure Mobility Client가 전 세계에서 널리 애용되는 이유입니다. 그리고 매번 새로운 릴리즈를 내놓음으로써 다양한 종류의 PC와 모바일 디바이스를 통한 원격 액세스 기능에 대해 고객의 기대치를 꾸준히 높여왔습니다.

제품 개요

모바일 근무자는 일반적으로 다양한 장소로 이동하며 VPN을 사용합니다. 따라서 상시 작동(Always-on)하는 인텔리전트 VPN은 AnyConnect가 설치된 클라이언트 디바이스로 하여금 최적의 네트워크 액세스 포인트를 자동으로 선택하고 터널링 프로토콜을 가장 효율적인 방식으로 사용하도록 지원합니다. 지연에 민감한 트래픽, VoIP(Voice over IP) 트래픽 또는 TCP 기반 애플리케이션 액세스에 적합한 DTLS(Datagram Transport Layer Security) 프로토콜이 포함될 수 있습니다. IPsec IKEv2(IP Security Internet Key Exchange version 2)에 대해서도 터널링 지원이 제공됩니다. 릴리즈 4.x의 애플리케이션당 VPN 기능을 사용하면 선택한 애플리케이션 VPN 액세스를 Apple iOS, Google Android(5.0 이상), Samsung KNOX에서 실행할 수 있습니다.

AnyConnect 4.x는 강력한 통합 엔드포인트 규정준수를 지원합니다. Cisco ASA(Adaptive Security Appliance)는 엔드포인트의 보안 포스처에 따라 VPN 액세스를 제한함으로써 기업 네트워크의 무결성을 보호합니다. 유/무선 환경 전반에 걸친 엔드포인트 포스처 평가(posture assessment) 및 치료 기능으로 다양한 안티바이러스, 개인 방화벽 및 안티스파이웨어 제품을 인증합니다. 규정준수 위반 엔드포인트 강화 기능은 액세스가 허용되기 전에 추가적인 시스템 검사를 실행하고 문제가 조치될 수 있도록 옵션을 제공합니다.

AnyConnect Secure Mobility 솔루션은 높은 보안수준을 필요로 하는 엔터프라이즈 모빌리티 솔루션에 대한 원격 액세스 기능 이외에 내장형 웹 보안, 악성코드 위협 방어, 피싱 방지, 명령 및 제어 콜백 차단 기능을 지원합니다. 웹기반 기업 리소스 접근 및 클라우드 보호 서비스에 대해 신뢰성 및 높은 안정성을 제공하려면 프레미스 기반 Cisco Web Security Appliance 또는 클라우드 기반 Cisco Cloud Web Security를 선택하십시오. Cisco Umbrella Roaming은 VPN이 꺼져 있더라도 디바이스의 장소에 관계없이 악성코드, 피싱, 명령 및 제어 서버에 대한 콜백으로부터 보호해주는 클라우드 기반 보안 서비스입니다.

Windows 및 Mac OS X 플랫폼에서 네트워크 가시성 모듈을 사용함으로써 관리자는 엔드포인트 애플리케이션 사용을 모니터링하여 잠재적인 비정상 행동을 찾아내고 더 많은 정보를 바탕으로 네트워크 설계에 대해 의사 결정을 내릴 수 있습니다. 사용 데이터는 IPFIX(Internet Protocol Flow Information Export) 지원 네트워크 분석 툴과 공유될 수 있습니다.

Cisco AMP(Advanced Malware Protection) Enabler를 사용하여 AnyConnect에서 Cisco Advanced Malware Protection for Endpoints의 구축을 지원할 수 있습니다. 이 기능을 통해 단순 VPN을 사용하는 엔드포인트뿐만 아니라 802.1X 네트워크 액세스, 포스처 등을 이용하는 AnyConnect 서비스에 대해서도 보안을 대폭 강화시켜 줍니다. 또한 엔터프라이즈 환경에 연결된 호스트로부터의 공격 가능성을 줄입니다. Cisco AMP for Endpoints는 AnyConnect와는 별도로 라이센스를 구매해야 합니다.

AnyConnect 모빌리티 클라이언트는 업계 최고 수준의 VPN 기능을 제공할 뿐만 아니라 IEEE 802.1X 기능을 지원하여 사용자 및 디바이스 ID를 관리하는 단일 인증 프레임워크와 무선 네트워크에서 유선 네트워크로 원활하게 전환하는 데 필요한 네트워크 액세스 프로토콜을 제공합니다.

VPN 기능과 마찬가지로, 유선 네트워크에서 데이터 기밀성, 데이터 무결성, 데이터 출처 인증을 보장하는 IEEE 802.1AE(MACsec)를 지원하여 신뢰할 수 있는 네트워크 구성 요소 간 통신을 보호합니다.

그림 1에는 Microsoft Windows의 VPN 구성이 나와 있습니다.

그림 1. Microsoft Windows의 아이콘 및 샘플 VPN 구성

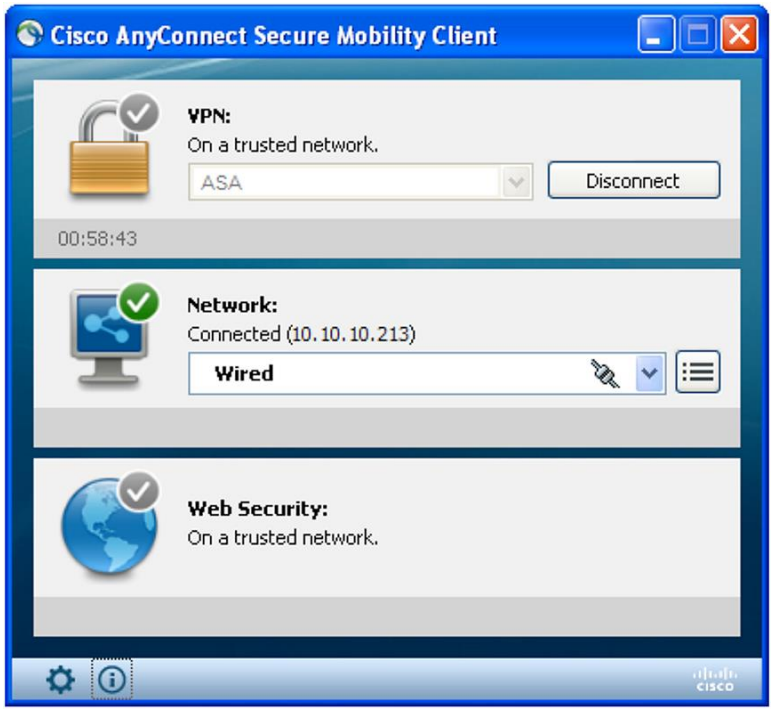
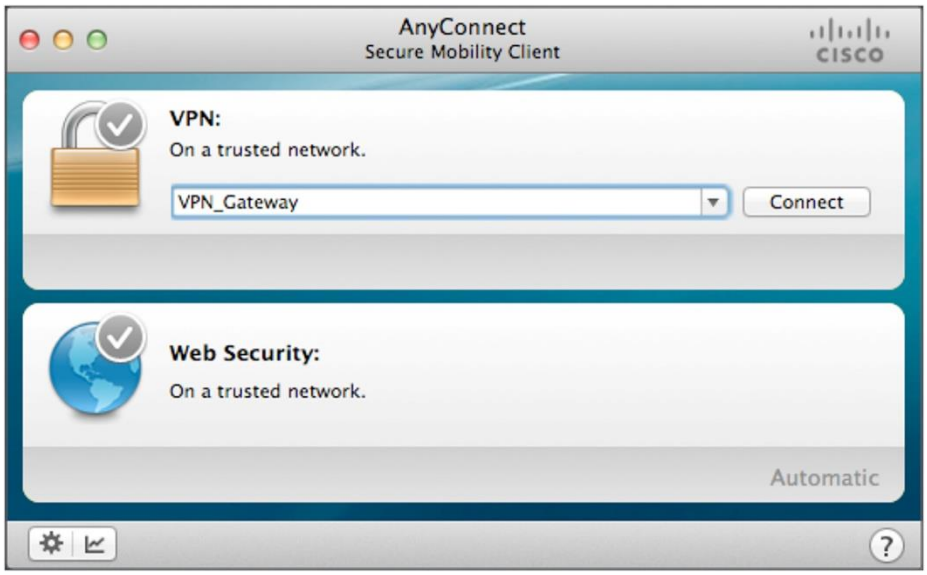


그림 2에는 Apple OS X의 VPN 구성이 나와 있습니다.

그림 2. Apple OS X의 아이콘 및 샘플 VPN 구성

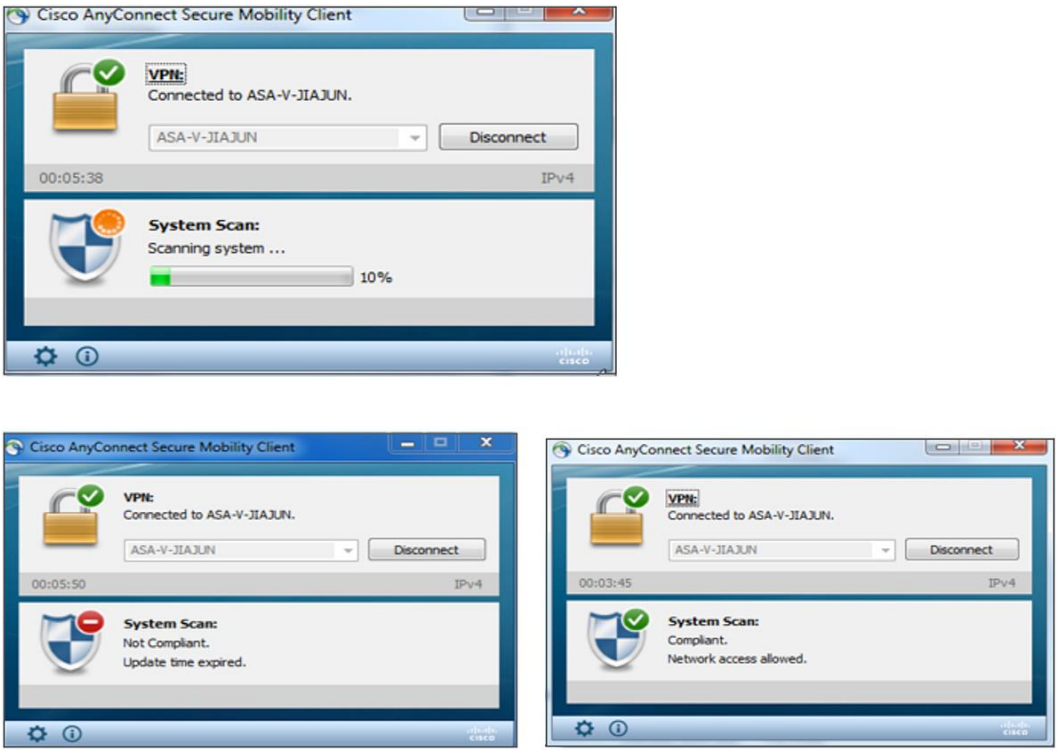


클라이언트 모듈

AnyConnect 클라이언트는 고도로 모듈화된 경량형 보안 클라이언트로, 기업의 개별 요구 사항에 따라 쉽게 맞춤형으로 구성할 수 있는 기능을 제공합니다. VPN, 802.1X, 컴플라이언스 검사, 네트워크 가시성, Cisco Umbrella Roaming, Cisco Cloud Web Security와의 통합 기능, AMP for Endpoints 설치 및 제거 기능 등이 개별 모듈 및 서비스 형태로 모두 제공되므로, 조직은 연결 요구 사항에 따라 가장 적합한 기능을 선택할 수 있습니다. 이를 통해 AnyConnect의 빠른 속도와 높은 운영 효율성을 유지하는 동시에 조직에는 유연성과 혜택을 제공할 수 있습니다.

그림 3은 유/무선 환경에 걸친 AnyConnect 통합 엔드포인트 컴플라이언스 기능을 보여 줍니다.

그림 3. 엔드포인트 컴플라이언스 점검



기능 및 이점

표 1에는 Cisco AnyConnect Secure Mobility Client의 기능과 장점이 나와 있습니다.

표 1. 기능 및 장점

기능	장점 및 설명
원격 액세스 VPN	
폭넓은 운영 체제 지원	• Windows 10, 8.1, 8, 7 • Mac OS X 10.8 이상 • Linux Intel(x64) • 모바일 플랫폼에 대한 내용은 AnyConnect Mobile 데이터 시트를 참조하십시오.
소프트웨어 액세스	• Cisco.com Software Center에서 다운로드가 가능합니다. • AnyConnect에 대한 기술 지원 및 소프트웨어 이용 자격은 모든 기간 기반 Plus 및 Apex 라이센스에 포함되어 있으며, Plus 영구 라이센스용으로 별도로 구매 가능합니다. • 계약 번호는 Cisco.com ID와 연결되어야 합니다. 자세한 내용은 AnyConnect 주문 가이드를 참조하십시오.
최적화된 네트워크 액세스: VPN protocol choice SSL(TLS 및 DTLS), IPsec IKEv2	• AnyConnect에서는 VPN 프로토콜을 선택할 수 있으므로 관리자는 비즈니스 요구에 가장 적합한 프로토콜을 사용할 수 있음 • 터널링 지원에는 SSL(TLS 1.2 및 DTLS) 및 차세대 IPsec IKEv2 포함 • DTLS는 VoIP 트래픽 또는 TCP 기반 애플리케이션 액세스 등 지연에 민감한 트래픽에 맞게 최적화된 연결 제공 • TLS 1.2(HTTP over TLS 또는 SSL)는 웹 프록시 서버를 사용하는 환경 등 제한된 환경에서의 네트워크 연결에 대한 가용성 보장 • IPsec IKEv2는 보안 정책에서 IPsec을 사용해야 하는 경우 지연에 민감한 트래픽에 맞게 최적화된 연결 제공

기능	장점 및 설명
최적의 게이트웨이 선택	• 네트워크 액세스 포인트에 대해 최적화된 연결을 선택하므로, 최종 사용자는 가장 가까운 위치를 결정할 필요가 없음
모빌리티 지원	• 모바일 사용자를 위한 설계 • IP 주소 변경, 연결 손실, 절전 또는 대기 모드 중에도 VPN 연결이 유지되도록 구성할 수 있음 • Trusted Network Detection 기능을 통해 최종 사용자가 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, ESPv3 with IKEv2, 4096 비트 RSA 키, Diffie-Hellman 그룹 24, 확장 SHA2(SHA-256 & SHA-384)와 같은 차세대 암호화 IPsec IKEv2 연결에만 적용됨. AnyConnect Apex 라이센스가 필요함.
폭넓은 구축 및 연결 옵션	**구축 옵션:** • Microsoft Installer를 포함한 사전 구축 • ActiveX(Windows 전용) 및 Java를 사용하는 자동 보안 게이트웨이 구축(초기 설치 시 관리자 권한 필요) **연결 모드:** • 시스템 아이콘으로 독립형으로 실행 • 브라우저에서 시작(웹 실행) • 클라이언트리스 포털에서 시작 • CLI로 시작 • API로 시작
다양한 인증 옵션	• RADIUS • NTLM(NT LAN Manager)에 대한 비밀번호 만료(MSCHAPv2)가 포함된 RADIUS • RADIUS OTP(One-Time Password) 지원(상태 및 응답 메시지 특성) • RSA SecurID(SoftID 통합 포함) • Active Directory 또는 Kerberos • 내장형 CA(Certificate Authority) • 디지털 인증서 또는 스마트카드(시스템 인증서 지원 포함), 자동 선택 또는 사용자 선택 • 곧 만료될 예정이거나 오래된 비밀번호를 사용한 LDAP(Lightweight Directory Access Protocol) • 일반 LDAP 지원 • 인증서 및 사용자 이름/비밀번호 멀티 팩터 인증 결합(이중 인증)
일관된 사용자 경험	• 풀 터널(Full-tunnel) 클라이언트 모드는 LAN환경과 같이 일관된 사용자 환경을 필요로 하는 원격 액세스 사용자 지원 • 다중 전달 방법으로 AnyConnect의 폭넓은 호환성 보장 • 사용자는 푸시 업데이트 지연 가능 • 고객 경험 피드백 옵션 제공
중앙 집중식 정책 제어 및 관리	• 정책을 로컬에서 구성하거나 미리 구성할 수 있으며, VPN 보안 게이트웨이에서 자동으로 업데이트할 수 있음 • 웹 페이지 또는 애플리케이션을 통한 손쉬운 구축을 지원하는 AnyConnect용 API • 신뢰할 수 없는 인증서를 확인하여 사용자에게 경고 • 인증서를 로컬에서 보고 관리할 수 있음
고급 IP 네트워크 연결	• IPv4 및 IPv6 네트워크와의 공개 연결 • 내부 IPv4 및 IPv6 네트워크 리소스에 액세스 • 관리자 제어 기반의 스플릿 터널링 및 전체 터널링 네트워크 액세스 정책 • 액세스 제어 정책 • Google Android(Lollipop) 및 Samsung KNOX에 대한 애플리케이션당 VPN 정책(릴리즈 4.0에서 새롭게 지원: Cisco ASA 5500-X와 OS 9.3 이상 및 AnyConnect 4.0 라이센스 필요) **IP 주소 할당 메커니즘:** • 정적 • 내부 풀 • DHCP(Dynamic Host Configuration Protocol) • RADIUS/LDAP(Lightweight Directory Access Protocol)

기능	장점 및 설명
강력한 통합 엔드포인트 컴플라이언스(Apex 라이센스 필요)	• 유/무선 환경의 엔드포인트 보안 상태 평가 및 치료(Cisco Identity Services Engine NAC Agent 대체). Identity Services Engine 1.3 이상과 Identity Services Engine Apex 라이센스가 필요함. • ISE Posture(ISE와 함께 연동) 및 Hostscan(VPN 전용)은 네트워크 액세스를 허용하기 전에 엔드포인트 시스템에 악성코드 차단 소프트웨어, Windows 서비스 팩/패치 상태, 다양한 기타 소프트웨어 서비스가 있는지 여부를 확인함 • 관리자는 실행 중인 프로세스를 기반으로 사용자 지정 포스처 확인을 정의할 수 있음 • ISE Posture 및 Hostscan은 원격 시스템에서 워터마크 존재 유무를 탐지할 수 있음. 워터마크는 기업 소유의 자산을 식별하는 데 사용할 수 있으며 그에 따라 차별화된 액세스를 제공함. 워터마크 확인 기능에는 시스템 레지스트리 값, 필요한 CRC32 체크섬과 일치하는 파일 존재 유무, 다양한 기타 기능이 포함됨. 컴플라이언스 위반 애플리케이션에 대한 추가 기능이 지원됨. • 기능은 운영 체제에 따라 다름. 자세한 내용은 Host Scan 지원 차트를 참조.
클라이언트 방화벽 정책	• 스플릿 터널링 컨피그레이션을 위한 추가적인 보호 기능 제공 • AnyConnect 클라이언트와 함께 사용할 경우 로컬 액세스 예외 허용 가능(예: 인쇄, 테더링 디바이스 지원 등) • IPv4용 포트 기반 룰 및 IPv6용 네트워크/IP ACL(Access Control List) 지원 • Windows 및 Mac OS X 플랫폼에 사용 가능
현지화	**영어 외에도 다음 언어가 지원됩니다.** • 체코어(cs-cz) • 독일어(de-de) • 스페인어(es-es) • 프랑스어(fr-fr) • 일본어(ja-jp) • 한국어(ko-kr) • 폴란드어(pl-pl) • 중국어 간체(zh-cn) • 중국어(대만)(zh-tw) • 네덜란드어(nl-nl) • 헝가리어(hu-hu) • 이탈리아어(it-it) • 포르투갈어(브라질)(pt-br) • 러시아어(ru-ru)
간편한 클라이언트 관리	• 관리자는 헤드엔드(Head-end) 보안 어플라이언스에서 소프트웨어 및 정책 업데이트를 자동으로 구축할 수 있으므로, 클라이언트 소프트웨어 업데이트와 관련된 관리 작업이 제거됨 • 관리자는 최종 사용자 구성에 어떤 기능을 사용할지 결정할 수 있음 • 도메인 로그인 스크립트를 사용할 수 없을 경우 관리자는 연결 및 연결 해제 시 엔드포인트 스크립트를 트리거할 수 있음 • 관리자는 최종 사용자에게 표시될 메시지에 대해 사용자 지정 및 현지 언어화를 할 수 있음
프로파일 편집기	• Cisco ASDM(Adaptive Security Device Manager)에서 직접 AnyConnect 정책을 사용자 지정할 수 있음
진단	• 온-디바이스 통계 및 로깅 정보 사용 가능 • 디바이스에서 로그를 볼 수 있음 • Cisco 또는 관리자에게 로그를 분석용으로 손쉽게 이메일 전송할 수 있음
FIPS(Federal Information Processing Standard)	• FIPS 140-2 Level 2 규격(플랫폼, 기능 및 버전 제한 적용)
보안 모빌리티 및 네트워크 가시성	
웹 보안 통합(Cloud Web Security 라이센스 필요)	• 세계 최대의 SaaS(software-as-a-service) 웹 보안 제공자인 Cloud Web Security를 사용하여 기업 네트워크에서 악성코드를 차단하고 직원의 웹 사용 제어 및 보호 • 클라우드에서 호스팅되는 컨피그레이션 및 동적 로딩 지원 • 프레미스 기반 서비스 외에도 클라우드 기반 서비스까지 지원하여 조직에 다양한 선택 옵션 제공 • Web Security Appliance와 통합 • 신뢰할 수 있는 네트워크 탐지 지원 • 사용자 위치와 관계없이 모든 트랜잭션에 보안 정책 적용 • 보안 수준이 높은 상시 작동 네트워크 연결과 액세스가 불가능할 경우 네트워크 연결을 허용 또는 거부하는 정책 필요 • 핫스팟 및 종속 포털 탐지

기능	장점 및 설명
Cisco Umbrella Roaming(Cisco Umbrella Roaming 라이센스 필요)	• VPN이 꺼져 있는 경우 로밍 디바이스에 대해 보안 적용 • 로밍 디바이스에서 자동으로 악성코드, 피싱 및 C2 콜백 차단 • 디바이스 위치와 관계없이 간단한 보호 방법 제공 • VPN이 꺼져 있거나 스플릿 터널(터널 외 통신에 적용)을 사용하는 경우 DNS 기반 보안을 적용하기 위해 엔드포인트 리디렉션 활용
네트워크 가시성 모듈(Apex 라이센스 필요)	• 사용자, 엔드포인트, 애플리케이션, 위치 및 대상에 대한 풍부한 상황 정보로 엔드포인트 플로우 포착 • 온프레미스 및 오프프레미스에서 유연한 수집 설정 • 애플리케이션 사용을 모니터링하여 잠재적인 동작 이상 징후 식별 • 보다 많은 정보에 입각한 네트워크 설계 결정 지원 • 사용 데이터를 IPFIX(Internet Protocol Flow Information Export) 지원 네트워크 분석 툴과 공유할 수 있음
AMP(Advanced Malware Protection) for Endpoints Enabler(AMP for Endpoints 라이센스 별도)	• Cisco AMP for Endpoints를 배포 및 사용 설정하여 AnyConnect 엔드포인트에 대한 위협 차단 서비스 지원 간소화 • 원격 엔드포인트까지 엔드포인트 위협 서비스를 확장하여 엔드포인트 위협 보호 범위 확대 • 보다 사전 대응적인 보호 기능을 제공하여 원격 엔드포인트에 대한 공격이 신속하게 완화되도록 함
폭넓은 운영 체제 지원	• Windows 10, 8.1, 8, 7 • Mac OS X 10.8 이상
네트워크 액세스 관리자 및 802.1X	
미디어 지원	• 이더넷(IEEE 802.3) • Wi-Fi(IEEE 802.11a/b/g/n)
네트워크 인증	• IEEE 802.1X-2001, 802.1X-2004 및 802.1X-2010 • 기업이 단일 802.1X 인증 프레임워크를 구축하여 유선 네트워크 및 무선 네트워크 모두에 액세스할 수 있도록 지원 • 보다 높은 수준의 보안 액세스가 요구되는 사용자 및 디바이스 ID와 네트워크 액세스 프로토콜을 관리 • Cisco의 통합 유/무선 네트워크에 연결하는 사용자의 경험 최적화
EAP(Extensible Authentication Protocol) 방식	• EAP-TLS(Transport Layer Security) • 다음 inner method를 사용하는 EAP-PEAP(Protected Extensible Authentication Protocol): ◦ EAP-TLS ◦ EAP-MSCHAPv2 ◦ EAP-GTC(Generic Token Card) • 다음 inner method를 사용하는 EAP-FAST(Flexible Authentication via Secure Tunneling): ◦ EAP-TLS ◦ EAP-MSCHAPv2 ◦ EAP-GTC • 다음 inner method를 사용하는 EAP-TTLS(Tunneled TLS): ◦ PAP(Password Authentication Protocol) ◦ CHAP(Challenge Handshake Authentication Protocol) ◦ Microsoft CHAP(MSCHAP) ◦ MSCHAPv2 ◦ EAP-MD5 ◦ EAP-MSCHAPv2 • LEAP(Lightweight EAP), Wi-Fi 전용 • EAP-MD5(Message Digest 5), 관리자가 구성, 이더넷 전용 • EAP-MSCHAPv2, 관리자가 구성, 이더넷 전용 • EAP-GTC, 관리자가 구성, 이더넷 전용
무선 암호화 방식(해당 802.11 NIC 지원 필요)	• 개방성 • WEP(Wired Equivalent Privacy) • Dynamic WEP • WPA(Wi-Fi Protected Access) Enterprise • WPA2 Enterprise • WPA Personal(WPA-PSK) • WPA2 Personal(WPA2-PSK) • CCKM(Cisco CB21AG Wireless NIC 필요)

기능	장점 및 설명
무선 암호화 프로토콜	• AES(Advanced Encryption Standard) 알고리즘을 사용한 CCMP(Counter mode with Cipher Block Chaining Message Authentication Code Protocol) • RC4(Rivest Cipher 4) 스트림 암호를 사용한 TKIP(Temporal Key Integrity Protocol)
세션 재개	• EAP TLS, EAP-FAST, EAP-PEAP, EAP-TTLS를 사용한 RFC2716(EAP-TLS) 세션 재개 • EAP-FAST 스테이트리스 세션 재개 • PMK-ID 캐싱(Proactive Key Caching 또는 Opportunistic Key Caching), Windows XP 전용
이더넷 암호화	• 미디어 액세스 제어: IEEE 802.1AE(MACsec) • 키 관리: MKA(MACsec Key Agreement) • 유선 이더넷 네트워크의 보안 인프라를 정의하여 데이터 기밀성, 데이터 무결성 및 데이터 출처 인증 제공 • 신뢰할 수 있는 네트워크 구성 요소 간 통신 보호
한 번에 하나의 연결	• 네트워크에 대해 하나의 연결만 허용하고 나머지는 연결 해제 • 어댑터 간 브리징 없음 • 우선순위에 따라 자동으로 이더넷 연결
복잡한 서버 검증	• "ends with" 및 "exact match" 규칙 지원 • 이름 공통성이 없는 서버에 대해 30여 개 규칙 지원
EAP-Chaining(EAP-FASTv2)	• 기업 자산인지 아닌지에 따라 액세스 차별화 • 단일 EAP 트랜잭션에서 사용자 및 디바이스 검증
ECE(Enterprise Connection Enforcement)	• 사용자가 올바른 기업 네트워크에만 연결하도록 보장 • 사용자가 사무실에서 서드파티 액세스 포인트에 연결하여 인터넷을 검색하지 못하도록 방지 • 사용자가 게스트 네트워크에 대한 액세스를 설정하지 못하도록 방지 • 번거로운 블랙리스트 등록을 없앰
차세대 암호화 (Suite B)	• 최신 암호화 표준 지원 • Elliptic Curve Diffie-Hellman 키 교환 • ECDSA(Elliptic Curve Digital Signature Algorithm) 인증서
크리덴셜 유형	• 인터랙티브 사용자 비밀번호 또는 Windows 비밀번호 • RSA SecurID 토큰 • OTP(One-time password) 토큰 • 스마트 카드(Axalto, Gemplus, SafeNet iKey, Alladin) • X.509 인증서 • ECDSA(Elliptic Curve Digital Signature Algorithm) 인증서
원격 데스크톱 지원	• RDP(Remote Desktop Protocol) 사용 시 로컬 네트워크에 대해 원격 사용자 크리덴셜 인증
지원되는 운영 체제	• Windows 10, 8.1, 8, 7

플랫폼 호환성

AnyConnect는 Cisco ASA 소프트웨어 릴리즈 8.0(4) 이상에서 실행 중인 모든 Cisco ASA 5500-X Series Next Generation Firewalls 및 5500 Series Enterprise Firewall Edition 모델과 호환 가능합니다. 가장 최근에 릴리즈된 소프트웨어를 이용하여 구축하는 것이 좋습니다.

특정 기능을 사용하려면 최신의 Cisco ASA 소프트웨어 릴리즈 또는 ASA 5500-X 모델이 필요합니다.

Cisco는 Cisco IOS® 15.1(2)T 릴리즈 이상에서 AnyConnect VPN 액세스에 대한 보안 게이트웨이 기능을 지원합니다(일부 기능은 제한). 자세한 내용은 Cisco IOS SSL VPN에서 지원되지 않는 기능을 참조하십시오.

자세한 Cisco IOS 기능 지원 정보는 http://www.cisco.com/go/fn을 참조하십시오.

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

라이센싱 옵션

- AnyConnect 4.x 이상에는 AnyConnect Plus 또는 Apex 라이센스가 필요합니다.
- 라이센싱 옵션과 주문에 대한 자세한 내용은 http://www.cisco.com/c/dam/en/us/products/security/anyconnect-og.pdf의 주문 가이드에서 확인할 수 있습니다.

Cisco Capital

여러분의 목표 달성을 돕는 금융 지원 솔루션

Cisco Capital이 목표 달성과 경쟁력 유지에 필요한 기술 도입을 도와드리겠습니다. 고객의 설비 투자 부담을 줄여드립니다. 성장을 가속화하십시오. 투자 및 ROI를 최적화하십시오. Cisco Capital 파이낸싱은 하드웨어, 소프트웨어, 서비스, 보완적인 서드파티 장비 도입에 유연성을 제공합니다. 또한, 예측 가능한 비용 결제를 한 번만 하면 됩니다. Cisco Capital은 100여 개 국가에서 이용 가능합니다. 자세히 보기

추가 정보

- Cisco AnyConnect Secure Mobility Client 홈페이지: http://www.cisco.com/go/anyconnect
- Cisco AnyConnect 설명서: http://www.cisco.com/c/en/us/support/security/anyconnect-secure-mobility-client/tsd-products-support-series-home.html
- Cisco AnyConnect for Mobile Platforms 데이터 시트: http://www.cisco.com/c/en/us/products/collateral/security/anyconnect-secure-mobility-client/data_sheet_c78-527494.html
- Cisco ASA 5500-X Series Adaptive Security Appliances: http://www.cisco.com/go/asa
- Cisco Cloud Web Security http://www.cisco.com/go/cws
- Cisco AMP for Endpoints http://www.cisco.com/c/en/us/products/security/fireamp-endpoints/index.html
- Cisco AnyConnect 라이센스 계약 및 개인정보 보호정책: http://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/anyconnect40/license/end_user/AnyConnect-SEULA-v4-x.html

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.

인쇄지: 미국

C78-733184-05 06/16