Cisco Web Security Appliance

보안을 위해 네트워크에는 악성코드 차단, 애플리케이션 가시성 및 제어, 사용 정책 제어, 유용한 정보를 제공하는 보고 기능, 보안 모빌리티가 필요합니다. Cisco에서는 Cisco® WSA(Web Security Appliance)라는 단일 플랫폼에서 이러한 모든 보호 기능을 제공합니다.

연결성이 높고 모빌리티가 점점 더 강화되는 오늘날의 환경에서는 더 복잡하고 정교해진 위협에 대응하기 위해 여러 보안 솔루션을 사용해야 합니다. Cisco는 기업이 필요로 하는 강력한 보호 기능, 완벽한 제어력, 투자 가치를 갖춘 네트워크 인프라의 모든 레이어를 위한 보안 솔루션을 제공합니다. 또한 시장을 주도하는 글로벌 위협 인텔리전스와 함께 폭넓은 웹 보안 구축 옵션을 제공합니다. Cisco WSA는 고성능 전용 어플라이언스를 활용하여 보안을 단순화하며, Cisco WSAV(Web Security Virtual Appliance)는 기업이 필요한 경우 언제 어디서나 웹 보안을 신속하고 간편하게 구축할 수 있도록 지원합니다.

Cisco WSA는 조직에서 웹 트래픽 보안 및 제어의 증가하는 당면 과제를 해결할 수 있도록 최고의 보호 기술을 결합한 최초의 보안 웹 게이트웨이 중 하나입니다. 이 플랫폼은 더 적은 유지 보수 요건, 더 짧은 레이턴시, 더 낮은 운영 비용으로 더욱 간단하고 신속하게 구축할 수 있습니다. "한 번 설정으로 완료되는(set and forget)" 기술을 통해 초기 자동화된 정책 설정이 라이브 상태가 된 후에는 담당 인력이 더 이상 개입할 필요가 없으며 3분에서 5분 간격으로 자동 보안 업데이트가 네트워크 디바이스에 푸시됩니다. 유연한 구축 옵션 및 기존 보안 인프라와의 통합으로 빠르게 발전하는 보안 요건을 충족할 수 있습니다.

가상 어플라이언스

비디오 및 기타 리치 미디어가 증가하면서 트래픽 예측 가능성이 낮아져 초과 공급이 발생하고 성능이 저하됩니다. 이를 비롯한 여러 문제를 해결하는 과정에서 관리자는 특히 다국적 조직의 경우 하드웨어 구매 및 설치 시의 긴 리드 타임, 원격 설치 당면 과제, 관세 및 기타 물류 문제에 직면하게 됩니다.

Cisco WSAV는 관리자가 필요할 때 필요한 곳에서 보안 인스턴스를 생성할 수 있도록 함으로써 특히 매우 분산된 네트워크에서 웹 보안 구축 비용을 크게 절감합니다. Cisco WSAV는 VMware ESXi 또는 KVM 하이퍼바이저와 Cisco UCS®(Unified Computing System™) 서버를 기반으로 실행되는 Cisco WSA의 소프트웨어 버전입니다. Cisco Email 또는 Web Security 소프트웨어 번들 중 하나를 구매하면 해당 SMA 소프트웨어 라이센스와 함께 Cisco SMAV에 대한 무제한 라이센스를 받게 됩니다.

Cisco WSAV를 사용하여 관리자는 트래픽 급증에 즉시 대응하고 용량 계획의 필요성을 없앨 수 있습니다. 어플라이언스를 구매하고 배송할 필요가 없으며, 데이터 센터가 복잡해진다거나 인력을 충원하지 않아도 새로운 비즈니스 기회를 지원할 수 있습니다.

기능 및 이점

Talos Security Intelligence	다음과 같은 가장 광범위한 가시성과 가장 큰 설치 범위를 통해 세계 최대 위협 탐지 네트워크에서 지원하는 신속하고 포괄적인 웹 보호 정보를 제공받습니다. • 하루100 TB의 보안 인텔리전스 • 방화벽, IPS, 웹, 이메일 어플라이언스를 포함하는160 만 대의 보안 장치 구축 • 1억5000 만 개의 엔드포인트 • 매일130 억 건의 웹 요청 • 전 세계 기업 이메일 트래픽의%35 매일24 시간 글로벌 트래픽 활동을 감시하여 이상 징후를 분석하고, 새로운 위협을 탐지하고, 트래픽 추세를 모니터링할 수 있도록 해줍니다. Talos는3 분에서5 분마다 WSA에 업데이트를 제공하는 새 규칙을 지속적으로 생성하여 제로 아워(zero-hour) 공격을 차단함으로써 경쟁업체보다 몇 시간 또는 며칠 앞서 업계 최고의 위협 방어 조치를 취합니다.
Cisco Web Usage Controls	전통적인 URL 필터링을 동적 콘텐츠 분석과 결합하여 규정준수, 책임 및 생산성 위험을 완화합니다. 5천만 개 이상의 차단된 사이트를 포함하여 지속적으로 업데이트되는 Cisco의 URL 필터링 데이터베이스가 알려진 웹 사이트에 대해 탁월한 정보를 제공하고, DCA(Dynamic Content Analysis) 엔진이 알 수 없는 URL의%90 를 실시간으로 정확하게 식별합니다. 즉, 텍스트를 검사하고, 텍스트의 관련성 점수를 매기며, 모델 문서 근접성을 계산하여 일치하는 가장 가까운 범주를 반환합니다. 관리자는 특정 범주를 선택하여 지능적인 HTTPS 검사를 실시할 수도 있습니다.
Advanced Malware Protection	AMP(Advanced Malware Protection)는 모든 Cisco WSA 고객이 사용할 수 있는 라이센스가 부여된 추가 기능입니다. AMP는 악성코드 탐지 및 차단, 지속적인 분석, 회귀적 알림 등의 기능을 제공하는 포괄적인 악성코드 방어 솔루션입니다. AMP는 Cisco와 Sourcefire® 기술의 방대한 클라우드 보안 인텔리전스 네트워크를 모두 사용합니다. AMP는 향상된 파일 평판 기능, 세부적인 파일 동작 보고, 지속적인 파일 분석, 회귀적 판단 알림 등의 기능을 통해 Cisco WSA에서 이미 제공하고 있는 악성코드 탐지 및 차단 기능을 더욱 강화합니다. Cisco AMP Threat Grid는 클라우드에 악성코드 샘플을 제출할 때 규정준수 또는 정책 제한사항을 적용해야 하는 조직에 온프레미스 어플라이언스를 통한 악성코드 차단 기능을 제공합니다. 레이어4 트래픽 모니터는 활동을 지속적으로 스캔하여 스파이웨어 “폰홈(phone-home)” 커뮤니케이션을 탐지 및 차단합니다. 레이어4 트래픽 모니터는 모든 네트워크 애플리케이션을 추적하므로 전형적인 웹 보안 솔루션을 우회하려는 악성코드를 효과적으로 차단합니다. 또한 알려진 악성코드 도메인의 IP 주소를 차단할 악성 엔티티 목록에 동적으로 추가합니다.
Cognitive Threat Analytics	Cisco Cognitive Threat Analytics는 네트워크 내에서 작동하는 위협의 검색 시간을 단축하는 클라우드 기반 솔루션입니다. 동작 분석 및 이상 징후 탐지를 통해 악성코드 감염이나 데이터 보안 침해의 증상을 파악하여 경계 기반 방어의 허점을 보완합니다. Web Security 솔루션에 간단한 애드온 라이센스를 적용하여 Cisco Cognitive Threat Analytics를 활용할 수 있습니다. 복잡성을 낮추면서도 계속 변화하는 위협 환경과 함께 진화하는 탁월한 보호 기능을 제공합니다.
AVC(Application Visibility and Control)	수백 개의 Web 2.0 애플리케이션과15 만 개 이상의 마이크로애플리케이션 사용을 간편하게 제어합니다. 관리자는 세분화된 정책 제어를 통해 Dropbox, Facebook과 같은 애플리케이션의 사용을 허용하면서 문서 업로드, "좋아요" 버튼 클릭과 같은 사용자 활동을 차단할 수 있습니다. WSA는 네트워크 전체에서 일어나는 각종 활동에 대한 가시성을 제공합니다. 새로운 기능: 고객은 사용자, 그룹 및 정책당 맞춤형 대역폭 및 시간 할당량을 구축할 수 있습니다.
데이터 유출 방지(DLP)	기본 DLP를 위한 상황 기반 규칙을 생성하여 기밀 데이터가 네트워크에서 유출되는 것을 방지합니다. 또한 Cisco WSA는 심층적인 콘텐츠 검사 및 DLP 정책 실행을 위해 서드파티 DLP 솔루션과 통합하는 데 ICAP(Internet Content Adaptation Protocol)를 사용합니다. Cisco WSA는 Secure ICAP를 지원하여 WSA와 서드파티 DLP 솔루션 간에 교환되는 트래픽을 암호화할 수도 있습니다.

로밍 사용자 보호	Cisco WSA는 Cisco AnyConnect® Secure Mobility Client와 통합하여 로밍 사용자를 보호합니다. 이 클라이언트는 트래픽을 온프레미스 솔루션에 다시 리디렉션하는 VPN 터널을 가동하여 원격 클라이언트에 웹 보안을 제공합니다. Cisco AnyConnect 기술은 액세스를 허용하기 전에 실시간으로 트래픽을 분석합니다. Cisco WSA는 Cisco ISE(Identity Services Engine)와도 통합됩니다. 이와 같은 기능 향상으로 이제 고객은 요청 시 Cisco WSA에 Cisco ISE의 강력한 기능을 활용할 수 있습니다. Cisco ISE 통합으로 관리자는 단일 로그인 프로세스를 통해 Cisco ISE에서 수집한 프로파일 또는 멤버십 정보를 토대로 Cisco WSA에 대한 정책을 생성할 수 있습니다.
중앙 집중식 관리 및 보고	위협, 데이터 및 애플리케이션에 대해 실행 가능한 정보를 제공받습니다. Cisco WSA에서는 운영 제어, 정책 관리, 보고서 보기를 지원하는 사용하기 편리한 중앙 집중식 관리 툴을 제공합니다. Cisco M-Series Content Security Management Appliance는 가상 인스턴스를 비롯한 여러 어플라이언스와 여러 위치 전반에 대한 중앙 집중식 관리 및 보고 기능을 제공합니다. Cisco® Web Security Reporting Application은 Cisco WSA(Web Security Appliances) 및 Cisco CWS(Cloud Web Security)에서 생성되는 로그를 신속하게 색인화하고 분석하는 보고 솔루션입니다. 이 툴은 트래픽 및 스토리지 요구 사항이 많은 고객에게 알맞은 확장식 보고 기능을 제공합니다. 또한 관리자가 웹 사용 및 멀웨어 위협에 대한 세부적인 통찰력을 수집할 수 있는 보고 기능도 제공합니다.
융통성 있는 구축	Cisco WSAV는 Cisco WSA와 동일한 기능을 모두 제공할 뿐만 아니라 즉각적인 셀프 서비스 프로비저닝을 비롯하여 가상 구축 모델의 더 큰 편리성과 비용 절감 효과를 구현합니다. Cisco WSAV 라이센스를 통해 기업은 로컬에 저장된 새로운 Cisco WSAV 가상 이미지 파일에 라이센스를 적용하여 인터넷에 연결하지 않고도 웹 보안 가상 게이트웨이를 구축할 수 있습니다. 필요한 경우 초기 상태 가상 이미지 파일을 복제하여 여러 웹 보안 게이트웨이를 즉시 구축할 수 있습니다. 동일한 구축에서 하드웨어 및 가상 머신을 실행합니다. 소규모 지사 또는 원격 위치에서 하드웨어를 설치 및 지원할 필요 없이 Cisco WSA에서 제공하는 동일한 보호 기능을 해당 위치에 구현할 수 있습니다. Cisco M-Series Content Security Management Appliance를 통해 맞춤형 구축을 간편하게 관리할 수 있습니다.

제품 사양

표 1, 2에는 Cisco WSA 성능 및 하드웨어 사양이 각각 나와 있습니다.

표1 . Cisco WSA 성능 사양

	모델	디스크 공간	RAID 미러링	메모리	CPU
대기업	S690	4.8TB (8 x 600GB SAS)	예(RAID 10)	64GB, DDR4	2 x 2.5Ghz, 24C
대기업	S690X	9.6TB (16x600GB SAS)	예(RAID 10)	64GB, DDR4	2 x 2.5Ghz, 24C
대기업	S680	2.4TB (8x300GB SAS)	예(RAID 10)	32GB DDR3	2 x 2.7Ghz, 16C
중견기업	S390	2.4TB (4 x 600GB SAS)	예(RAID 10)	32 GB, DDR4	1 x 2.4Ghz, 8C
중견기업	S380	2.4TB (4 x 600GB SAS)	예(RAID 10)	16GB DDR3	1 x 2.0Ghz, 6C
중소기업(SMB) 및 지사	S190	1.2TB (2x600GB SAS)	예(RAID 1)	8 GB, DDR4	1 x 1.9Ghz, 6C
중소기업(SMB) 및 지사	S170	500GB (2x500GB SATA)	예(RAID 1)	4GB DDR3	1 x 2.8Ghz, 2C

* 현재 및 향후 요구 사항을 충족하는 솔루션을 구축할 수 있도록 Cisco 콘텐츠 보안 전문가에게 규모 결정에 대한 안내를 받으시기 바랍니다.

표2 . Cisco WSA 하드웨어 사양

	Cisco S690	Cisco S690X	Cisco S680	Cisco S390	Cisco S380	Cisco S190	Cisco S170
하드웨어 플랫폼							
폼 팩터	2RU	2RU	2RU	1RU	2RU	1RU	1RU
규격	3.4" x 19" x 29"	3.4" x 19" x 29”	3.5” x 19” x 29”	1.7" x 19" x 31"	3.5” x 19” x 29”	1.7" x 19" x 31"	1.64” x 19” x 15.25”
예비 전원 공급 장치	예	예	예	예	예	예(액세서리 옵션)	아니요
원격 전원 주기	예	예	예	예	예	아니요	아니요
DC 전원 옵션	예	예	예	아니요	예	아니요	아니요
운영중 교체 가능한 H/D	예	예	예	예	예	예	예
Ethernet 인터페이스	6포트1 G Base-T UTP 네트워크 인터페이스(NIC), RJ - 45	6포트1 G Base-T UTP 네트워크 인터페이스(NIC), RJ - 45	6포트1 G Base-T UTP 네트워크 인터페이스(NIC), RJ - 45	6포트1 G Base-T UTP 네트워크 인터페이스(NIC), RJ - 45	6포트1 G Base-T UTP 네트워크 인터페이스(NIC), RJ - 45	2포트1 G Base-T UTP 네트워크 인터페이스(NIC), RJ - 45	2포트1 G Base-T UTP 네트워크 인터페이스(NIC), RJ - 45
속도(Mbps)	10/100/1000, autonegotiate	10/100/1000, autonegotiate	10/100/1000, autonegotiate	10/100/1000, autonegotiate	10/100/1000, autonegotiate	10/100/1000, autonegotiate	10/100/1000, autonegotiate
파이버 옵션	예(개별 SKU) 6포트1 G Base-SX 파이버: WSA- S690-1G 6포트10 G Base-SR 파이버 WSA- S690-10G	예(개별 SKU) 6포트1 G Base-SX 파이버: WSA- S690-1G 6포트10 G Base-SR 파이버 WSA- S690-10G	예(개별 SKU) 6포트1 G Base-SX 파이버: WSA- S680-1G 6포트10 G Base-SR 파이버 WSA- S680-10G	아니요	아니요	아니요	아니요

표 3에는 Cisco WSAV의 사양이 나와 있으며, 표 4에는 Cisco M-Series Content Security Management Appliance의 사양이 나와 있습니다.

표3 . Cisco WSAV

웹 사용자				
웹 사용자	**모델**	**디스크**	**메모리**	**코어**
<1000	S000v	250 GB	4GB	1
1000-2999	S100v	250 GB	6GB	2
3000-6000	S300v	1024 GB	8GB	4
서버		**하이퍼바이저**		
Cisco UCS **Red Hat Enterprise Linux 7.0** **Ubuntu 14.04.1 LTS**		**ESXi 5.0, 5.1, 5.5** **KVM: QEMU 1.5.3** **KVM: QEMU 2.0.0**	vmware KVM	

표4 . Cisco M-Series Content Security Management Appliance

모델	**Cisco M680**	**Cisco M380**	**Cisco M170**
사용자 수(근사치)	10,000명 이상	최대10,000 명	최대1,000 명

구축

Cisco WSA는 Explicit 모드(PAC[Proxy Automatic Configuration] 파일, WPAD[Web Proxy Auto-Discovery], 브라우저 설정) 또는 Transparent 모드(WCCP[Web Cache Communication Protocol], PBR[Policy-Based Routing], 로드 밸런서)로 구축할 수 있는 전달 프록시입니다. Cisco Catalyst® 6000 시리즈 스위치, Cisco ASR 1000 Series Aggregation Services Routers, Cisco Integrated Services Routers, Cisco ASA 5500-X 시리즈 차세대 방화벽 등의 WCCP 호환 디바이스는 웹 트래픽을 Cisco WSA에 다시 라우팅합니다.

Cisco WSA는 HTTP, HTTPS, SOCKS, 네이티브 FTP 및 FTP over HTTP 트래픽을 프록시하여 데이터 유출 방지, 모바일 사용자 보안, 고급 가시성 및 제어 등의 추가 기능을 제공할 수 있습니다.

라이센싱

Cisco WSAV 라이센스는 모든 Cisco Web Security 소프트웨어 번들(Cisco Web Security Essentials, Cisco Web Security Antimalware, Cisco Web Security Premium)에 포함됩니다. 이 라이센스는 번들에 포함된 나머지 소프트웨어 서비스와 기간이 동일하며 필요한 수의 가상 머신에 대해 사용할 수 있습니다.

기간 기반 서브스크립션 라이센스

1년, 3년 또는 5년의 기간 기반 서브스크립션 라이센스입니다.

수량 기반 서브스크립션 라이센스

Cisco Web Security 포트폴리오에는 디바이스가 아니라 사용자 범위에 기반한 계층형 가격이 적용됩니다. 영업 및 파트너 담당자가 각 고객 구축에 대해 올바른 크기를 결정할 수 있도록 도와드립니다.

Web Security 소프트웨어 라이센스

Cisco Web Security Essentials, Cisco Anti-Malware, Cisco Web Security Premium, McAfee Anti-Malware의 4가지 Web Security 소프트웨어 라이센스를 사용할 수 있습니다. 각 소프트웨어 제품의 주요 구성 요소는 다음과 같습니다.

Cisco Web Security Essentials

- Cisco Talos를 통한 위협 인텔리전스
- 레이어 4 트래픽 모니터링
- AVC(Application Visibility and Control)
- 정책 관리
- 실행 가능한 보고
- URL 필터링
- ICAP를 통한 서드파티 DLP 통합

Cisco Anti-Malware

- 실시간 악성코드 스캔

Cisco Web Security Premium

- Web Security Essentials
- 실시간 악성코드 검사

AMP(Advanced Malware Protection)

- AMP는 파일 평판 점수 및 차단, 정적 및 동적 파일 분석(샌드박싱) 및 파일 회귀 분석으로 위협을 지속적으로 분석하여 악성코드 탐지 및 차단 기능을 보강합니다.

Cognitive Threat Analytics

- CTA는 고급 통계 모델링 및 기계 학습을 사용하여 독립적으로 새로운 위협을 식별하고 파악한 내용을 학습하며 시간을 두고 조정합니다.

Cloud Access Security

- Cisco with Elastica는 조직이 SaaS 가시성, 세분화된 제어 기능의 확장, 지능형 보호 기능을 통해 보안 정책을 유지하면서 클라우드 애플리케이션의 이점을 실현할 수 있도록 지원합니다.

McAfee Anti-Malware

- McAfee 실시간 악성코드 검사는 별개의 단일 라이센스로 이용할 수 있습니다.

소프트웨어 라이센스 계약

Cisco EULA(End-User License Agreement) 및 Cisco Web Security SEULA(Supplemental End-User License Agreement)가 각 소프트웨어 라이센스 구매 시 제공됩니다.

소프트웨어 서브스크립션 지원

모든 Cisco Web Security 라이센스에는 비즈니스 크리티컬 애플리케이션을 사용 가능하고, 안전하며, 최고 성능으로 운영되는 상태로 유지하는 데 필수적인 소프트웨어 서브스크립션 지원이 포함됩니다. 이러한 지원에는 구매한 소프트웨어 서브스크립션 기간 동안 고객이 아래와 같은 서비스를 이용할 수 있는 권한이 포함됩니다.

- 최신 기능 집합으로 애플리케이션의 최적 성능을 유지하기 위한 소프트웨어 업데이트 및 주요 업그레이드
- 신속한 전문 지원을 위해 Cisco TAC(Technical Assistance Center)에 액세스
- 사내(in-house) 전문 지식을 구축 및 확대하고 비즈니스 민첩성을 증대할 수 있는 온라인 툴
- 추가 지식 및 교육 기회를 제공하는 협업적 학습

서비스

표 5에는 Cisco Web Security 서비스가 나와 있습니다.

표5 . Cisco Web Security Services

Cisco Branded Services	Cisco Security Planning and Design: 강력한 보안 솔루션을 신속하고 비용 효율적으로 구축할 수 있도록 지원합니다. Cisco Web Security Configuration and Installation: 다음을 구현하기 위한 어플라이언스를 설치, 구성 및 테스트하여 웹 보안 위험을 완화합니다. • 제한적 사용 정책 제어 • 평판 및 악성코드 필터링 • 데이터 보안 • 애플리케이션 가시성 및 제어 Cisco Security Optimization Service: 진화하는 보안 시스템을 지원하여 보안 위협, 설계 업데이트, 성능 조정, 시스템 변경을 해결할 수 있도록 합니다.
협업/파트너 서비스	Network Device Security Assessment: 네트워크 인프라 보안상의 허점을 찾아내 더 강력한 네트워크 환경을 유지할 수 있도록 지원합니다. Smart Care: 네트워크의 성능에 대한 보안 가시성을 통해 얻은 실행 가능한 정보를 제공합니다. 추가 서비스: Cisco 파트너는 계획, 설계, 구현 및 최적화 라이프사이클 전체에서 다양한 가치 있는 서비스를 제공합니다.
Cisco 파이낸싱	Cisco Capital® 에서 비즈니스 요구사항에 부합하는 맞춤형 금융 지원 솔루션을 제공합니다. 조속히 Cisco 기술을 활용하여 더욱 신속하게 비즈니스 혜택을 누리십시오.

SMARTnet Support Services

고객은 Cisco SMARTnet® 지원 서비스를 구매하여 Cisco WSA와 함께 사용할 수 있습니다. Cisco SMARTnet 지원 서비스는 고객이 언제든 직접 Cisco 전문가에게 문의하거나 셀프 헬프 지원 툴, 빠른 하드웨어 교체를 이용하여 네트워크 문제를 신속하게 해결할 수 있도록 돕습니다. 자세한 내용은 http://www.cisco.com/go/smartnet을 참조하십시오.

Cisco WSAV 주문

Cisco WSAV를 주문하려면 다음을 수행합니다.

1. http://www.cisco.com/go/wsa로 이동합니다. 오른쪽에 있는 “Support(지원)” 아래에서 “Software Downloads, Release, and General Information(소프트웨어 다운로드, 릴리스 및 일반 정보)”을 클릭합니다. "Download Software(소프트웨어 다운로드)"를 클릭한 다음 모델을 클릭하면 제공되는 다운로드 가능한 가상 머신 이미지가 표시됩니다. 또한 다운로드 가능한 XML 평가 라이센스도 확인할 수 있습니다. 이미지 및 XML 평가 라이센스 중 하나를 다운로드해야 합니다.
2. Cisco.com에서 다음 설명서를 다운로드합니다.
   a. Cisco Security Virtual Appliance Installation Guide
   b. AsyncOS® 9.0용 설명서
3. Cisco Security Virtual Appliance Installation Guide의 지침에 따라 사용을 시작합니다. Content Security Virtual Appliance 평가는 SMARTnet 지원에 포함되지 않으므로 지원되지 않습니다.

워런티 정보

워런티 정보는 Cisco.com의 제품 워런티 페이지에서 확인하십시오.

추가 정보

자세한 정보는 http://www.cisco.com/go/wsa를 참조하십시오. Cisco WSA가 귀사에 얼마나 효과적으로 적용될 수 있을지 Cisco 영업 담당자, 채널 파트너 또는 시스템 엔지니어와 함께 평가해 보십시오.

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 C78-729630-09 12/15