Cisco Firepower Management Center

Cisco Firepower™ Management Center는 원활한 중앙 집중식의 통합 관리를 제공하여 Cisco® 네트워크 보안 솔루션의 효과를 향상합니다.

제품 개요

Cisco FirePOWER Management Center는 서로 다른 플랫폼에서 실행되는 여러 Cisco 보안 제품의 운영 중추 역할을 하고 있습니다. 방화벽, 애플리케이션 제어, 침입 방지, URL 필터링, 지능형 악성코드 차단에 대한 완전한 통합형 관리 기능을 제공합니다. Management Center는 다음 솔루션의 이벤트 및 정책을 관리하는 중심 지점입니다.

- Cisco Firepower NGFW(Next-Generation Firewall)
- Cisco ASA with FirePOWER Services
- Cisco Firepower NGIPS(Next-Generation IPS)
- Cisco FirePOWER Threat Defense for ISR
- Cisco AMP(Advanced Malware Protection)

Firepower Management Center는 네트워크에 있는 사용자, 애플리케이션, 디바이스, 위협, 취약성에 대한 광범위한 인텔리전스를 제공합니다. 또한 이러한 정보를 사용하여 네트워크의 취약성을 분석하며, 어떤 보안 정책을 적용해야 하고, 어떤 보안 이벤트를 조사해야 할지에 대해 맞춤된 권고를 제공합니다.

Management Center는 액세스를 제어하고 알려진 공격을 차단할 수 있도록 사용하기 쉬운 정책 화면을 제공합니다. 이는 지능형 악성코드 차단(AMP) 및 샌드박싱 기술을 통합하며, 네트워크 전반에 걸쳐 악성코드 감염을 추적할 수 있는 툴을 제공합니다. 또한 하나의 관리 인터페이스에 이러한 모든 기능을 통합합니다. 방화벽 관리부터 애플리케이션 제어, 악성코드 침해 조사 및 치료에 이르기까지 모든 작업을 쉽게 관리할 수 있습니다.

그림 1. 중앙 집중화된 정책, 이벤트, 디바이스 관리

엔터프라이즈급 관리

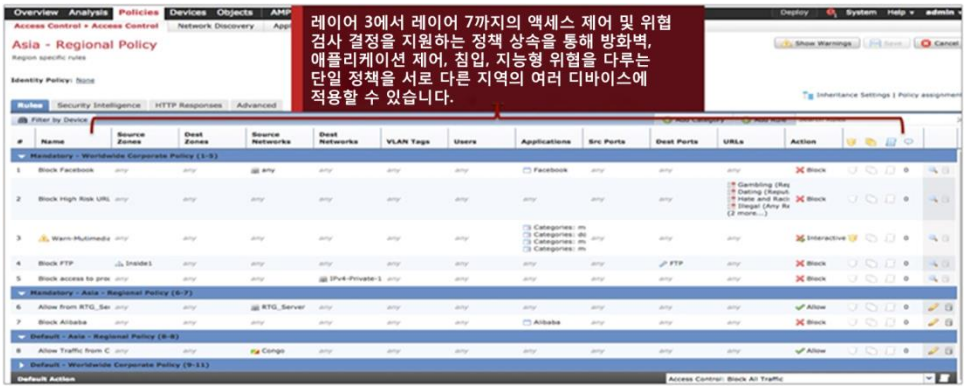
Cisco Firepower Management Center는 변화하는 네트워크 리소스와 운영에 대한 실시간 정보를 찾아내므로 완전한 상황 정보를 토대로 정보에 입각한 결정을 내릴 수 있습니다(그림 1 참조). Firepower Management Center는 광범위한 인텔리전스를 제공하는 것 외에도 다음과 같은 세부적인 기능을 제공합니다.

- **트렌드 및 상위 통계**: 관리자와 경영진이 특정 시점의 보안 상태뿐만 아니라 좋건 나쁘건 변화하는 상황을 이해할 수 있도록 지원
- **이벤트 세부 정보, 컴플라이언스, 포렌식**: 방어 기능을 개선하고, 보안 침해 억제 노력을 지원하며, 법적 시행 조치를 돕기 위해 보안 이벤트 중 발생한 상황에 대한 정보 제공
- **워크플로 데이터**: 다른 솔루션으로 쉽게 내보내기 하여 보안 사고 대응 관리 개선

기능 및 이점

기능	이점
여러 솔루션 전반에 걸쳐 다양한 보안 기능을 통합적으로 관리	다음과 같은 Cisco 보안 환경에 대한 중앙 집중식 관리가 용이하게 이루어질 수 있도록 합니다. • Cisco Firepower NGFW(Next-Generation Firewall) • Cisco ASA with FirePOWER Services • Cisco Firepower NGIPS • Cisco FirePOWER Threat Defense for ISR • Cisco AMP
다양한 보안 기능에 대한 통합된 정책 관리	단 하나의 정책으로 방화벽 액세스, 애플리케이션 제어, 위협 방지, URL 필터링, 지능형 악성코드 차단 설정 편리한 정책 관리, 오류 감소, 일관성 증진 여러 보안 솔루션에 단일 정책 구축 지원
우수한 위협 인텔리전스	최신 위협 차단을 위해 Cisco Talos Group의 보안, 위협, 취약성 인텔리전스 통합 IP 기반 및 URL 기반 보안 인텔리전스로 신종 공격 방법 처리 네트워크 경계 밖의 위협 가시성을 지원하는 Cisco OpenDNS를 포함
애플리케이션 가시성 및 제어	4,000개 이상의 상용 애플리케이션을 정확하게 제어하여 네트워크에 대한 위협 더욱 감소 맞춤형 애플리케이션을 자세히 식별하고 제어하는 데 오픈 소스 표준 OpenAppID를 사용
멀티테넌시 관리 및 정책 상속	역할 기반 액세스 제어를 통해 시행된 별도의 이벤트 데이터, 보고, 네트워크 매핑을 활용하여 최대 50개의 관리 도메인 생성 정책 계층 구조를 통해 일관되고 효율적인 관리를 구현하며, 각 레벨은 상위의 정책을 상속
보고 및 대시보드	맞춤형 및 템플릿 기반 보고서가 포함된 맞춤 설정 가능한 대시보드를 통해 필요한 가시성이 제공됨 일반 정보와 중점 정보 모두에 대한 포괄적인 보고 및 알림 제공 이벤트 및 상황 정보를 하이퍼링크 표, 그래프, 차트로 표시하여 사용하기 쉬운 분석 지원 네트워크 동작 및 성능을 모니터링하여 이상 징후를 식별하고 시스템 상태 유지

그림 2. 단일 정책으로 다양한 보안 기능 지원



최고의 가시성 및 인사이트

눈으로 확인 불가능한 요소를 보호할 수는 없으므로, Cisco Firepower Management Center는 환경에서 실행 중인 모든 항목에 대한 상황 정보를 자동으로 수집 및 분석하고 표시합니다. 표 1에서는 기존의 보안 기술로는 탐지하지 못하는 위협 벡터에 대한 완벽한 상황 인식 기능을 어떻게 제공하는지를 설명합니다. 네트워크에 대한 이러한 중요한 통찰력을 보호 정책에서 사용할 수 있으므로 다른 솔루션이 제공하지 못하는 보호 수준을 제공합니다.

표 1. 풀 스택 가시성

카테고리	Cisco Firepower Management Center	일반 IPS	일반 차세대 방화벽
위협	예	예	예
사용자	예	예	예
웹 애플리케이션	예	아니요	예
애플리케이션 프로토콜	예	아니요	예
파일 전송	예	아니요	예
악성코드	예	아니요	아니요
커맨드 앤 컨트롤 서버	예	아니요	아니요
클라이언트 애플리케이션	예	아니요	아니요
네트워크 서버	예	아니요	아니요
운영 체제	예	아니요	아니요
라우터 및 스위치	예	아니요	아니요
모바일 디바이스	예	아니요	아니요
프린터	예	아니요	아니요
VoIP 폰	예	아니요	아니요
가상 머신	예	아니요	아니요
취약성 정보	예	아니요	아니요

공격 전, 공격 중, 공격 후에 걸친 모든 범위 관리

Cisco Firepower Management Center는 공격 전, 중, 후의 전 범위에 걸쳐 통합된 관리를 제공합니다.

공격 전

- 네트워크에서 어떤 항목이 실행 중인지에 대한 뛰어난 가시성을 제공하므로 어떤 요소를 보호해야 할지 확인할 수 있음
- 방화벽 규칙을 만들고, 해당 환경에서 4,000개 이상의 커머셜 및 맞춤형 애플리케이션을 사용하는 방식을 제어함

공격 중

- 적용할 침입 방지 레벨, URL 평판 규칙, Advanced Malware Protection을 정의함
- 다음과 같은 정책 적용: "이 특정 애플리케이션을 사용하는 현재 국가에서 첨부 파일이 포함된 네트워크 트래픽이 수신될 경우 이 레벨의 침입 검사을 적용하고, 파일의 악성코드 여부를 분석하며, 필요한 경우 통합 샌드박스에 파일을 전송함"

공격 후

- 공격에 의해 감염된 모든 디바이스를 그래픽으로 표시함
- 맞춤형 규칙을 쉽게 만들 수 있는 기능을 제공하여 공격이 더 이상 진행되지 못하도록 차단함
- 악성코드를 상세히 분석하여 안전하게 치료함

동적 방어를 위한 보안 자동화

Cisco Firepower Management Center에서는 네트워크가 어떻게 변하는지 지속적으로 모니터링합니다. 또한 다음을 통해 운영을 간소화하고 보안을 향상합니다.

- 새로운 공격 이벤트와 네트워크 취약성의 상관관계를 자동으로 분석하여 성공 가능성이 있는 공격에 대한 알림을 제공합니다. 보안 팀은 가장 문제가 되는 이러한 이벤트를 중점적으로 살펴볼 수 있습니다.
- 네트워크의 취약성을 분석하고, 적용할 수 있는 적합한 보안 정책을 자동으로 추천합니다. 변화하는 조건에 맞춰 방어하는 방법을 조정하고, 네트워크에 맞춤화된 보안 수단을 구현할 수 있습니다.
- 네트워크, 엔드포인트, 침입, 보안 인텔리전스 소스에서 특정 이벤트의 상관관계를 분석합니다. 개별 호스트에 알 수 없는 공격으로부터 보안 침해가 발생한 징후가 보일 경우 알림이 전송됩니다.
- 파일 정책 조건을 적용합니다. 해당 조건을 충족한 경우 파일을 자동으로 분석하여 알려진 악성코드인지 확인하거나, 해당 파일을 통합 샌드박스에 전송하여 알 수 없는 악성코드인지 확인합니다.

손쉬운 통합을 지원하는 개방형 API

Cisco Firepower Management Center는 강력하고 다양한 기능을 갖춘 네 가지 애플리케이션 프로그래밍 인터페이스를 통해 서드파티 기술과 통합할 수 있습니다. API는 다음을 위한 연결 지점을 제공합니다.

- Management Center에서 다른 플랫폼(예: SIEM(Security Information and Event Management) 솔루션)으로 이벤트 데이터 이동
- 서드파티 데이터(예: 활성 스캐너의 취약성 관리 데이터 및 운영 체제 정보)를 통해 Cisco Firepower 데이터베이스에 포함된 정보 향상
- 사용자가 정의한 상관관계 규칙(예: NAC(Network Access Control) 솔루션과 통합하여 감염된 엔드포인트 격리 또는 디지털 포렌식 프로세스 시작)에 의해 활성화된 워크플로 및 치료 단계 시작
- 이러한 솔루션을 활성화하여 Firepower Management Center 데이터베이스를 쿼리함으로써 서드파티 보고 및 분석 지원

이러한 API는 다양한 Cisco 보안 제품 및 워크플로와 통합하는 데에도 사용할 수 있습니다. 해당 제품에는 샌드박싱을 지원하는 Cisco AMP Threat Grid, 신원 데이터 및 네트워크 세그멘테이션을 지원하는 Cisco Identity Services Engine, 인터넷 전역 도메인 가시성을 지원하는 Cisco OpenDNS가 포함됩니다.

구축 모드 선택

Cisco Firepower Management Center는 물리적 또는 가상 어플라이언스로 구축 가능하므로 해당 환경에 가장 적합한 옵션을 선택할 수 있습니다. 물리적 어플라이언스는 대개 가상 어플라이언스보다 많은 수의 센서를 관리하고 더 강력한 이벤트 스토리지 기능을 제공합니다. 가상 어플라이언스는 편리하게 기존 VM 인프라를 사용할 수 있습니다. VMware vSphere 프로비저닝을 사용하여 편리하게 구축할 수 있으며 물리적 네트워크의 자산을 관리하는 데 활용할 수 있습니다. 버전 5.x 및 버전 6.x 가상 어플라이언스는 VMware ESX 및 ESXi 하이퍼바이저에서 호스팅할 수 있으며 최대 25개의 물리적 또는 가상 센서를 관리합니다.

플랫폼 사양

Cisco Firepower Management Center는 다양한 모델이 있습니다. 모니터링할 센서 어플라이언스 수(물리적 및 가상 모두), 해당 환경의 호스트 수, 예상 보안 이벤트 발생률을 기준으로 귀사에 적합한 모델을 선택하십시오(표 2 참조). 모든 모델이 다음과 같은 관리 기능을 공통으로 제공합니다.

- 중앙 집중식 디바이스, 라이센스, 이벤트 및 정책 관리
- 역할 기반 관리(관리자 역할 또는 그룹을 기반으로 세분화되고 격리된 보기 및 임무)
- 맞춤 보고서 및 템플릿 기반 보고서가 제공되는 맞춤형 대시보드
- 일반 정보와 집중식 정보 모두에 대한 포괄적인 보고 및 경고
- 하이퍼링크 테이블, 그래프 및 차트로 볼 수 있는 이벤트 및 상황별 정보
- 네트워크 활동 및 성능 모니터링
- 단일 장애 지점을 허용하지 않는 강력한 고가용성 옵션
- 실시간으로 위협을 대응할 수 있는 상관관계 및 복원 기능

- 방화벽, 네트워크 인프라, 로그 관리, 트러블 티켓팅(trouble ticketing), 패치 관리 등의 서드파티 솔루션 및 고객 워크 스트림과 통합하는 개방형 API

표 2에서는 사용 가능한 물리적 및 가상 Cisco Firepower Management Center 어플라이언스의 용량과 처리량을 비교하여 보여줍니다.

표 2. Cisco Firepower Management Center 모델

기능	FS 750	FS 2000	FS 4000	FS -VMW-SW
관리되는 센서의 최대 개수	10	70	300	25 10 2
IPS 이벤트 최대 개수	2,000만	6,000만	3억	1,000만
이벤트 스토리지	100GB	1.8TB	3.2TB	250GB
최대 네트워크 맵(호스트/사용자)	2,000/2,000	150,000/150,000	600,000/600,000	50,000/50,000
최대 플로우 속도(초당 플로우 수)	2,000fps	12,000fps	20,000fps	각기 다름*
네트워크 인터페이스	2 x 1Gbps	2 x 1Gbps 2 x 10Gbps(Cisco Commerce에서 제공되는 선택적 SFP)	2 x 1Gbps 2 x 10Gbps(Cisco Commerce에서 제공되는 선택적 SFP)	1 x 1Gbps
고가용성	LOM(Lights-out management)	RAID 5, LOM, 고가용성 페어링	RAID 5, LOM, 고가용성 페어링	아니요

* 가상 Cisco Firepower Management Center 성능은 선택한 가상 환경(CPU, 메모리, 스토리지 등)에 따라 크게 달라집니다. 또한 디바이스 2개 및 10개를 관리하는 "FS-VMW-SW" 열에 나열된 가상 Firepower Management Centers는 ASA에서 FirePOWER Services를 관리하기 위한 프로모션 솔루션의 일부입니다. 이는 개별 FirePOWER 센서를 관리하는 데 사용할 수 없습니다.

참고: 센서를 작동하려면 Cisco Firepower Management Center 어플라이언스가 있어야 합니다. 모든 센서 라이센싱 및 관리는 Management Center에서 처리됩니다. 또한 Cisco ASA를 FirePOWER Services 제품과 함께 다룰 경우, 모든 Cisco Firepower Management Centers는 구축 과정에서 FirePOWER 부분만 관리합니다.

표 3에는 Cisco Firepower Management Center가 관리할 수 있는 지원되는 Firepower 제품 버전 및 관련 하드웨어 플랫폼이 함께 나와 있습니다.

표 3. 지원되는 Firepower 버전 및 관련 플랫폼

관리 제품	관리되는 플랫폼	하드웨어 플랫폼
Cisco Firepower Management Center	Firepower v6.x	Firepower 4100 Series Firepower 9300 FirePOWER 7000 Series FirePOWER 8000 Series ISR 4000 Series(위협 방어 전용) ISR G2 Series(위협 방어 전용)
Cisco Firepower Management Center	Firepower v5.4	ASA 5500-X(FirePOWER Services 전용) FirePOWER 7000 Series FirePOWER 8000 Series

하이퍼바이저 호환성

Cisco FirePOWER Management Center 가상 어플라이언스는 표 4에 정리된 하이퍼바이저 버전을 지원합니다.

표 4. 가상 어플라이언스 하이퍼바이저 지원

하이퍼바이저	버전 및 세부사항	가상 Cisco Firepower Management Center 버전
VMware vSphere	5.1, 5.5: • ESXi Server • vCenter Server(선택 사항) • vSphere Web Client, vSphere Client 또는 OVF Tool for Windows/Linux	5.4, 6.0

라이센싱

Cisco 라이센싱 메커니즘은 기능을 쉽게 활성화하고 솔루션을 확장할 수 있도록 지원합니다. 소프트웨어 기능은 일반적으로 라이센스 키로 활성화되며 업데이트 서브스크립션은 다년 약정(1년, 3년, 5년)으로 제공됩니다. 대기업의 경우 ELA(Enterprise License Agreement)가 Cisco ONE에 포함되어 제공됩니다. ELA는 다양한 제품 또는 솔루션 부문의 기본 및 고급 보안 기능을 고정된 가격으로 구매할 수 있도록 지원하여 신속한 구축 및 종합적인 솔루션 채택을 장려합니다. 마지막으로, Cisco Smart Licensing은 라이센스 키의 부담을 완화하고 가상 라이센스를 재사용할 수 있도록 하여 동적 클라우드 및 가상 구현에 대한 지원을 향상합니다.

주문 정보

Cisco Smart Licensing

Cisco Firepower Management Center는 Cisco Smart Licensing을 사용하여 판매됩니다. Cisco에서는 소프트웨어 라이센스 구매, 구축, 관리, 추적이 매우 복잡하다는 점을 잘 알고 있습니다. Cisco Smart Software Licensing은 고객이 Cisco 소프트웨어가 네트워크 전반에서 사용되는 방식을 이해하는 데 도움을 주는 표준화된 라이센싱 플랫폼입니다. 이는 관리 오버헤드를 줄이고 운영 비용을 절감할 수 있도록 고안되었습니다.

Smart Licensing을 사용하면 하나의 포털에서 소프트웨어, 라이센스 및 디바이스를 전체적으로 파악할 수 있습니다. 라이센스를 쉽게 등록하고 활성화할 수 있으며 유사한 하드웨어 플랫폼 간에 이동할 수 있습니다. 추가 정보는 http://www.cisco.com/web/ordering/smart-software-licensing/index.html에서 확인할 수 있습니다. Smart Accounts에 대한 관련 정보는 http://www.cisco.com/web/ordering/smart-software-manager/smart-accounts.html에서 확인할 수 있습니다.

Cisco Smart Net Total Care 지원

Cisco Smart Net Total Care™는 수상 경력을 자랑하는 기술 지원 서비스로서, IT 담당자가 Cisco TAC(Technical Assistance Center) 엔지니어와 Cisco.com 리소스에 언제든지 직접 액세스할 수 있도록 지원합니다. 중요한 네트워크 문제를 해결하는 데 필요한 전문가 응답과 책임 있는 지원을 제공합니다.

Smart Net Total Care에서는 다음과 같은 디바이스 레벨 지원을 제공합니다.

- 24시간, 365일 연중무휴로 Cisco TAC의 전문 엔지니어에 글로벌 액세스
- 광범위한 Cisco.com 온라인 지식 기반, 리소스 및 툴에 언제든지 액세스 가능
- 2시간, 4시간, 익영업일(NBD) 선 교체, RFR(return for repair)을 포함한 하드웨어 교체 옵션

- 라이센스가 부여된 기능 세트 내의 주 릴리스와 부 릴리스를 모두 포함하는 지속적인 운영 체제 소프트웨어 업데이트
- Cisco Smart Call Home을 사용하는 선별된 디바이스에서 사전 대응적 진단 및 실시간 알림 제공

또한 Cisco Smart Net Total Care Onsite Service는 고객의 위치에서 교체 부품을 설치하는 현장 엔지니어 지원을 제공하고 네트워크가 최상의 레벨로 작동하도록 지원합니다. Smart Net Total Care에 대한 자세한 내용은 http://www.cisco.com/c/en/us/services/portfolio/product-technical-support/smart-net-total-care.html을 참조하십시오.

주문 방법

가상 및 물리적 Cisco Firepower Management Center 어플라이언스와 예비 하드웨어에 대한 주문 정보는 표 5를 참조하십시오. 추가 컨피그레이션 옵션 및 액세서리는 주문 가이드를 참조하십시오.

표 5. 주문 정보

Cisco Firepower Management Center(하드웨어) 어플라이언스	
부품 번호	**제품 설명**
FS750-K9	Cisco Firepower Management Center 750 섀시, 1RU
FS2000-K9	Cisco Firepower Management Center 2000 섀시, 1RU
FS4000-K9	Cisco Firepower Management Center 4000 섀시, 1RU
Cisco Firepower Management Center(하드웨어) 예비용	
FS-PWR-AC-650W=	Cisco Firepower 650W AC 전원 공급 장치
Cisco Firepower Management Center(소프트웨어) 가상 어플라이언스	
FS-VMW-SW-K9	Cisco Firepower Management Center, Virtual(VMware) Firepower License
FS-VMW-10-SW-K9	Cisco Firepower Management Center, Virtual(VMware) Firepower License, 디바이스 10개 지원
FS-VMW-2-SW-K9	Cisco Firepower Management Center, Virtual(VMware) Firepower License, 디바이스 2개 지원

제품을 주문하려면 Cisco 주문 홈 페이지를 방문하십시오.

워런티 정보

워런티 정보는 Cisco.com의 제품 워런티 페이지에서 확인하십시오.

Cisco 서비스

Cisco는 고객이 보다 빠른 시일 내에 성공을 거둘 수 있도록 다양한 서비스 프로그램을 제공합니다. Cisco의 혁신적인 서비스 프로그램은 인력과 프로세스, 툴, 파트너의 독특하고 독창적인 조합을 통해 제공되며 이를 통해 높은 수준의 고객 만족을 실현합니다. Cisco 서비스는 고객의 네트워크 투자를 보호하고 네트워크 운영을 최적화하며 새로운 애플리케이션에 맞는 네트워크의 준비를 통해 네트워크 인텔리전스와 고객의 비즈니스 능력 강화에 기여합니다. Cisco 보안 서비스에 관한 자세한 내용은 http://www.cisco.com/go/services/security를 참조하십시오.

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 이용할 수 있습니다. 자세히 알아보십시오.

추가 정보

자세한 내용은 다음 링크를 참조하십시오.

- Cisco Firepower Management Center
- Cisco Firepower Next-Generation Firewalls
- Cisco Firepower NGIPS(Next-Generation IPS)
- Cisco AMP(Advanced Malware Protection)
- Cisco FirePOWER Threat Defense for ISR
- Cisco Security Services

통신 사업자 환경을 위한 Cisco Firepower에 대한 자세한 내용은 다음을 참조하십시오.
http://www.cisco.com/c/en/us/solutions/enterprise-networks/service-provider-security-solutions/

미주 지역 본부
Cisco Systems, Inc.
캘리포니아 주 산호세

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. 주소, 전화번호 및 팩스 번호는 Cisco 웹사이트 **www.cisco.com/go/offices**에서 확인하십시오.

Printed in USA C78-736775-00 02/16