Cisco Web Security Appliance

이점

- **강력한 보호:** Cisco Talos Security Intelligence and Research Group을 비롯한 고급 글로벌 위협 인텔리전스를 통해 모든 디바이스를 보호합니다.
- **완벽한 제어:** 소셜 미디어 애플리케이션과 같은 동적 웹 콘텐츠를 포함하여 모든 웹 트래픽의 첨단 제어 기능을 제공합니다.
- **투자 가치:** 유연한 구축 옵션, 기존 보안 및 네트워크 인프라와의 원활한 통합, 세계 최고 수준의 24시간 지원을 제공하여 보안 투자의 가치를 높이고 웹 보안의 TCO(총 소유 비용)를 절감합니다.

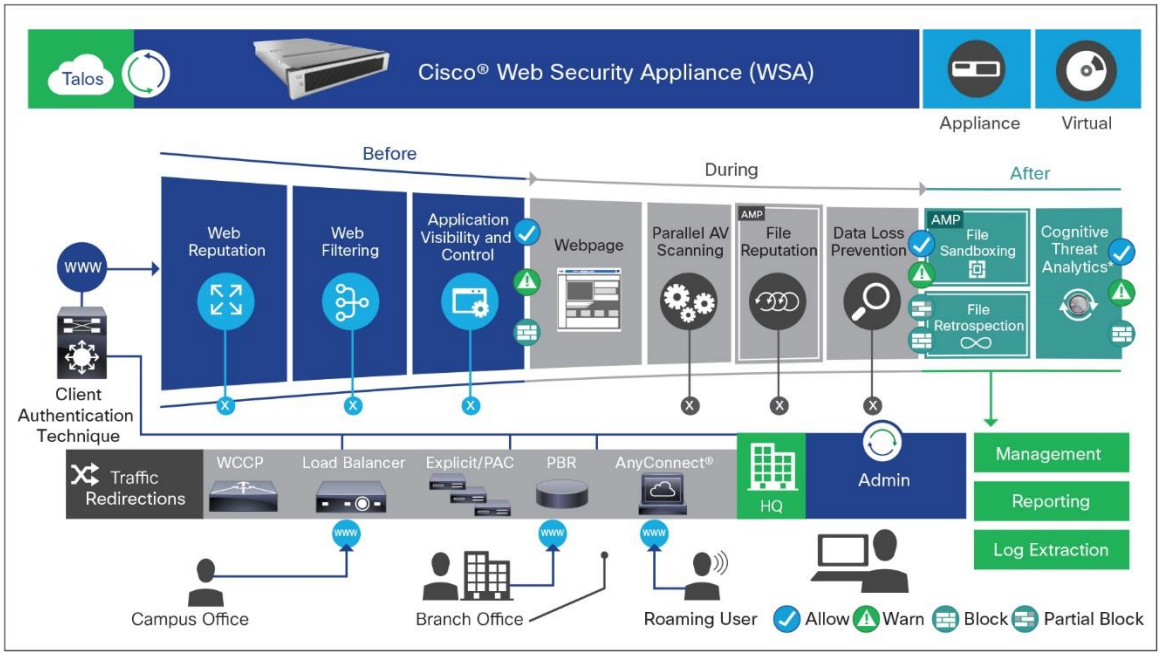
월드와이드웹(World Wide Web)은 안전하지 않습니다. 합법적인 웹사이트를 통해 바이러스에 감염되거나 악성코드를 다운로드할 가능성이 높습니다. 이 문서에서는 사무실에서뿐 아니라 이동 중에 소셜 미디어 및 Web 2.0 애플리케이션에 액세스하는 디바이스와 리소스를 보호할 수 있는 방법을 소개합니다.

오늘날의 비즈니스 환경에서 더욱 늘어나고 다양해지는 위협으로부터 보호하려면 첨단 접근 방식이 필요합니다. 즉, 수상한 사이트와 합법적인 사이트에서 사용자가 감염되기 전에 숨어 있는 악성코드를 차단할 수 있는 다양한 보호 기능이 필요합니다. 오늘날 최상의 웹 보안 솔루션이라면 최고 수준의 실시간 보안 인텔리전스를 기반으로 하여 변화하는 위협 환경을 파악하고 최신 익스플로잇이 실제로 문제를 일으키기 전에 차단할 수 있어야 합니다. 또한 첨단 웹 보안이라면 직원이 업무상 필요한 사이트에 액세스할 때는 허용하되 웹 기반 파일 공유와 같은 부적절한 사이트와 기능의 사용을 선별적으로 차단하는 정책을 지원할 만큼 치밀해야 합니다.

Cisco® WSA(Web Security Appliance)는 이 모든 기능 외에도 많은 추가 기능을 제공합니다(그림 1). Cisco WSA는 광범위한 위협 인텔리전스, 여러 레이어의 악성코드 방어, 필수적인 DLP(데이터 유출 방지) 기능을 통해 공격 전 범위에서 기업을 보호합니다. 일체형(all-in-one) 웹 게이트웨이로서 광범위한 보호, 포괄적인 제어, 투자 가치라는 이점을 제공합니다. 또한 경쟁력 있는 웹 보안 구축 옵션을 다양하게 제공하며, 각 옵션에는 Cisco의 업계 최고 글로벌 위협 인텔리전스 인프라가 포함됩니다.

Figure 1. Cisco Web Security Appliance

Figure 2. Protection from Cisco Web Security



공격 전: Cisco Security Intelligence Operations

Cisco WSA는 세계 최대 규모의 위협 탐지 네트워크인 Cisco Talos를 활용하여 실시간으로 위협을 탐지하고 상관관계를 파악합니다. Cisco Talos는 위협이 숨어 있는 위치를 찾아내기 위해 방화벽, IPS, 웹, 이메일, VPN 등 여러 벡터에서 방대한 양의 정보를 수집합니다. Cisco Talos는 Cisco WSA 및 기타 네트워크 보안 디바이스에 인텔리전스를 주고받으면서 3~5분 간격으로 지속적으로 정보를 새로고침합니다. 따라서 Cisco WSA는 경쟁 제품보다 몇 시간, 심지어 며칠 먼저 업계 최고의 방어 기능을 제공할 수 있습니다. 그런 다음 Cisco Talos의 인텔리전스와 Sourcefire Vulnerability Research Team의 인텔리전스가 결합되어 다음과 같은 추가적인 이점을 제공합니다.

- 매일 180,000개 이상의 파일 샘플 처리
- AMP(Advanced Malware Protection) 커뮤니티와 연계
- Microsoft 및 업계보다 먼저 공개
- Snort® 및 ClamAV 오픈소스 커뮤니티
- 허니팟
- Sourcefire AEGIS(Awareness, Education, Guidance, and Intelligence Sharing) 프로그램
- 비공개/공개 위협 정보 피드

- 동적 분석

Web Reputation Filter

Cisco WSA는 알려지지 않은 URL을 분석하여 분류하고 지정된 보안 임계값에 미치지 못하면 차단합니다. 웹 요청이 생성되는 즉시 웹 평판 필터가 200여 종의 웹 트래픽 및 네트워크 관련 파라미터를 분석하여 해당 사이트의 위험 레벨을 판단합니다. 도메인 소유자, 사이트가 호스팅되는 서버, 사이트가 생성된 시간, 사이트 유형을 확인한 다음 사이트에 평판 점수를 부여합니다. 평판 점수와 선별된 보안 정책에 따라 사이트를 차단, 허용, 경고 메시지와 함께 제공합니다. Cisco Talos는 3~5분 간격으로 웹 평판 필터링 인텔리전스를 업데이트합니다.

Cisco 웹 사용 제어

기존의 URL 필터링과 실시간 동적 콘텐츠 분석을 결합합니다. 구체적인 URL 필터링 정책을 통해 악성코드를 호스팅한 것으로 알려진 사이트에 대한 액세스를 차단하는 데 사용될 수 있으며, 5천만 개 이상의 차단된 사이트가 수집된 Cisco 데이터베이스의 알려진 웹사이트 목록과 대조합니다. DCA(동적 콘텐츠 분석) 엔진을 사용하여 알려지지 않은 URL의 90%에서 부적절한 콘텐츠를 실시간으로 정확하게 파악할 수 있습니다. DCA 엔진은 텍스트를 스캔하고 텍스트의 연관성에 점수를 지정한 다음 모델 문서 근접성을 계산하고 가장 일치하는 카테고리를 반환합니다. Cisco Talos는 방화벽, IPS, 웹, 이메일, VPN 등 여러 벡터에서 수집한 정보로 URL 데이터베이스를 업데이트합니다. Talos는 Cisco WSA 및 기타 네트워크 보안 디바이스에 인텔리전스를 주고받으면서 3~5분 간격으로 지속적으로 정보를 새로고침합니다.

공격 중: 실시간 안티 멀웨어 스캐닝

Cisco WSA는 단일 어플라이언스에서 여러 시그니처 스캐닝 엔진을 동시에 실행하면서 악성코드 방어 범위를 강화합니다. 시중 솔루션 중 가장 강력한 안티 멀웨어 검사를 포함하여 처리 속도를 최적화하고 트래픽 병목 현상을 방지합니다. 대응형 스캐닝 기능은 URL 평판, 콘텐츠 유형, 스캐너 효율성 등을 기준으로 가장 적절한 스캐너를 동적으로 선택하고 스캔 로드가 많을 경우 고위험 개체를 먼저 스캔하여 탐지율을 높입니다. 자동화된 업데이트로 추가된 최신 범위에 대한 정보를 받을 수 있습니다.

레이어 4 트래픽 모니터

Cisco WSA는 통합된 레이어 4 트래픽 모니터 기능으로 모든 트래픽, 포트, 프로토콜을 스캔하여 스파이웨어 "폰홈" 통신을 탐지 및 차단합니다. 이 스캐닝을 바탕으로 감염된 클라이언트를 식별하여 기존의 웹 보안 솔루션을 우회하려는 악성코드를 차단할 수 있도록 지원합니다. 또한 레이어 4 트래픽 모니터는 알려진 악성코드 도메인의 IP 주소를 차단할 악성 엔티티 목록에 동적으로 추가할 수 있습니다. 이 동적 검색 기능을 통해 레이어 4 트래픽 모니터는 악성코드의 동태를 실시간으로 모니터링할 수 있습니다.

ICAP를 사용한 서드파티 DLP 통합

더 강력한 DLP 기능을 제공하기 위해 Cisco WSA는 ICAP(nternet Control Adaptation Protocol)를 사용하여 주요 벤더의 DLP 솔루션과 통합됩니다. 모든 아웃바운드 트래픽을 서드파티 DLP 어플라이언스로 전송하면 서드파티 규칙과 정책에 따라 콘텐츠가 허용 또는 차단됩니다. 규정 준수 및 지적 재산 보호를 위해 콘텐츠 심층 검사도 제공됩니다. 강력한 엔진이 아웃바운드 트래픽을 검사하고 비공개 파일, 신용카드 번호, 고객 데이터 등의 콘텐츠 마커가 있는지 분석하여 이 데이터가 웹에 업로드되지 않도록 방지합니다.

Cloud Access Security

Cisco는 클라우드 애플리케이션에 숨어 있는 위협으로부터 보호할 수 있습니다. 주요 CASB(Cloud Access Security Broker) 제공자와 파트너 관계를 맺고 실시간으로 클라우드 애플리케이션 사용 현황을 모니터링하여 새로운 가시성을 제공합니다. 클라우드 우선, 모바일 우선 환경에서 제어 범위를 확장하고, 데이터 과학을 기반으로 한

인텔리전트 보호를 통해 진화하는 위협의 차단을 지원합니다. Elastica 등의 에코시스템 파트너는 기존 보안 아키텍처와 원활하게 통합되어 온프레미스 보호를 클라우드까지 확장합니다.

Cloud Access Security 솔루션은 클라우드 애플리케이션 환경에 대한 완전한 가시성을 제공하므로 게이트웨이를 통과하는 모든 클라우드 트래픽을 분류하여 침입 및 데이터 유출을 탐지하고, 허가받았거나 허가받지 않은 모든 애플리케이션을 대상으로 새로운 글로벌 보안 정책을 자동으로 적용할 수 있습니다.

파일 평판 및 Cisco AMP를 사용한 분석

Cisco WSA는 3~5분 간격으로 업데이트되는 Cisco Talos의 최신 위협 인텔리전스를 사용하여 파일을 평가합니다. Cisco WSA는 게이트웨이를 통과하는 각 파일의 핑거프린트를 수집하고 이를 Cisco 클라우드 기반 위협 인텔리전스 네트워크로 전송하여 제로 데이 익스플로잇과 대조한 평판 판정을 받습니다. 시스템에 영향을 주는 악성코드와 보안 침해를 식별할 수도 있습니다. 악성코드가 탐지되면 AMP는 파일 동작에 대한 정확한 세부사항을 수집하고 해당 데이터를 자세한 사람 및 시스템 분석과 결합하여 샌드박스에서 파일의 위협 레벨을 파악합니다.

공격 후: 파일 회귀 분석

Cisco WSA는 지속적으로 네트워크를 검사하여 탐지되지 않은 악성코드와 보안 침해가 있는지 확인합니다. Cisco WSA는 최초 탐지 후에도 상당 기간 최신 탐지 기능과 종합적 위협 인텔리전스로 파일을 검사하므로 업데이트된 디스포지션 렌더링과 추가 분석이 가능합니다.

Cognitive Threat Analytics

Cisco WSA에서는 행동 기반의 위협 탐지 기능을 통해 검색 시간을 단축하여 공격의 확산을 방지할 수 있습니다. Cisco WSA는 행동 이상 징후 탐지 알고리즘과 신뢰 모델링을 사용하여 감염 징후를 찾아냅니다. 애드온 라이선스인 Cisco CTA(Cognitive Threat Analytics)는 기계 학습을 통해 시간 경과에 따라 적응합니다. 규칙이 필요하지 않습니다. CTA가 스스로 위협을 찾아냅니다.

활용 사례: 제한적 사용

Cisco WSA를 사용하여 AVC(Application Visibility and Control), 제한적 사용 정책 제어, 통찰력 있는 보고, 보안 모빌리티를 하나의 어플라이언스에서 결합합니다. 단일 인터페이스에서 온프레미스 및 모바일 환경 전반에 걸쳐 글로벌 보안 인프라를 일관성 있게 제어할 수 있습니다. Cisco WSA에서는 정책을 시행하고 상황 인식 검사를 통해 애플리케이션 및 사용 행동을 정밀하게 제어할 수도 있습니다. 내장된 Cisco WSA 기능 또는 주요 벤더와의 통합에 의한 고급 DLP 기능으로 데이터를 보호합니다.

정책 관리

중앙 집중식 관리 및 보고

Cisco WSA 어플라이언스에 구현된 사용하기 간편한 중앙 집중식 툴에서 보안 및 네트워크 운영을 제어할 수 있습니다. 통찰력 있고 실행 가능한 보고 기능으로 간편하게 분석하고 신속하게 트러블슈팅을 처리하며 보안 정책의 개선할 점을 파악합니다. 또는 M-Series Content Cisco SMA(Security Management Appliance)의 중앙 관리 및 보고 기능으로 가상 인스턴스를 비롯한 여러 위치와 어플라이언스를 관리합니다.

Cisco AVC

Cisco AVC는 진화하는 애플리케이션 콘텐츠의 심층 가시성을 위해 가장 연관성 있고 널리 사용되는 수백 개의 Web 2.0 및 모바일 애플리케이션(예: Facebook), 150,000여 개의 마이크로애플리케이션(예: Facebook 게임)을 식별하고 분류하여 애플리케이션 및 사용 행동에 대한 가장 정밀한 제어 기능을 제공합니다. Facebook, Dropbox 등의 애플리케이션은 허용하되 좋아요 버튼 클릭, 문서 업로드 등의 사용자 활동은 차단합니다. 개인용 웹 메일 사용에 대해서는 모든 사용을 차단하거나, 사용자의 읽기 및 전송은 허용하되 문서 업로드를 차단하거나, 트랜잭션의 암호를 해독하여 서드파티 DLP 솔루션으로 전송합니다.

Cisco Identity Services Engine

Cisco WSA와 Cisco ISE(Identity Services Engine)가 통합되면서 WSA는 ID 및 네트워크 상황 정보로 웹 보안 정책 특성을 보완하여 특정 웹사이트에 대한 사용자 액세스의 보다 세분화된 제어 및 향상된 가시성을 통해 더 나은 사용자 경험을 제공할 수 있습니다. 두 솔루션을 모두 구축하는 고객은 Cisco ISE 디바이스 유형 및 네트워크 액세스 상황 정보를 바탕으로 사용자가 웹 리소스에 액세스하는 방법, 시점, 해당 디바이스를 파악함으로써 엔드 유저에게 더 우수한 콘텐츠 배달 경험을 제공할 수 있습니다. 사용자 역할 또는 사용자 디바이스에 따라 웹 액세스 정책을 개선하고, 승인된 콘텐츠나 민감한 콘텐츠에 대한 사용자 액세스 권한 부여를 더 효과적으로 제어할 수 있습니다. 엔드포인트가 IT 사용 정책을 준수하는지 여부를 파악하여 웹 기반 콘텐츠에 대한 액세스를 허용 또는 거부하는 디바이스별 웹 액세스 정책을 생성합니다.

> "[Cisco] WSA는 첫 3개월 만에 전체 웹 트랜잭션의 1%, 즉 3천만 건을 차단했습니다. 여기에는 봇넷과 주고받은 명령, 사용자 비밀번호나 기타 개인 정보의 검색 또는 유출, 악성코드 다운로드 등이 포함되었을 수 있습니다."
>
> **- Jeff Bollinger, Cisco IT 수석 정보 보안 조사관**

컴플라이언스

Cisco 웹 사용 제어

Cisco WSA에서는 기존의 URL 필터링과 실시간 DCA를 활용하여 컴플라이언스, 법적 책임, 생산성 관련 위험을 완화할 수 있습니다. 5천만 개 이상의 차단된 사이트 정보가 포함된 Cisco URL 필터링 데이터베이스를 바탕으로 알려진 웹사이트를 가장 광범위하게 관리합니다. 알려지지 않은 URL의 90%를 실시간으로 식별합니다. DCA 엔진은 텍스트를 스캔하고 텍스트의 연관성에 점수를 지정한 다음 모델 문서 근접성을 계산하고 가장 일치하는 카테고리를 반환합니다. Cisco Talos는 방화벽, IPS, 웹, 이메일, VPN 등 여러 벡터에서 수집한 정보로 URL 데이터베이스를 업데이트합니다. Cisco Talos는 WSA 및 기타 네트워크 보안 디바이스에 인텔리전스를 주고받으면서 3~5분 간격으로 지속적으로 정보를 새로고침합니다. 관리자는 특정 카테고리를 선택하여 인텔리전트 HTTPS 검사를 실시할 수도 있습니다.

데이터 유출 방지

Cisco WSA에서는 규정 준수 및 지적 재산 보호에 대한 비즈니스 요건에 따라 콘텐츠를 허용하거나 차단할 수 있습니다. 기본적인 DLP를 위한 상황 기반 규칙을 생성하거나, ICAP를 통해 서드파티 DLP 솔루션과 손쉽게 통합하여 콘텐츠 심층 검사 및 DLP 정책 적용을 수행함으로써 기밀 데이터가 네트워크에서 전송되는 것을 방지합니다. 업로드된 콘텐츠를 제목, 메타데이터, 크기를 기준으로 스캔하고 웹 메일과 클라우드 기반 파일 공유 서비스(예: Dropbox)에 업로드하지 않도록 방지하여 기본 DLP 기능으로 데이터를 보호합니다. 원하는 제한 수준에 따라 맞춤형 정책을 생성합니다. 예를 들어 개인용 웹 메일 사용을 모두 차단하거나, 사용자의 개인 웹 메일 읽기 및 전송은 허용하되 문서 업로드는 차단하거나, 트랜잭션의 암호를 해독하여 분석을 위해 서드파티 DLP 솔루션으로 전송하도록 선택합니다.

원격 디바이스 관리

Cisco AnyConnect Secure Mobility Client

Cisco AnyConnect Secure Mobility Client로 상시 웹 보안 보호 기능을 모바일 사용자까지 확장합니다. 사용자가 회사 네트워크에서 나가면 Cisco AnyConnect가 자동으로 사용자가 로밍 중임을 탐지하고 회사 네트워크의 Cisco WSA로 트래픽을 리디렉션합니다. Cisco AnyConnect Client는 VPN 터널을 통해 온프레미스 라우터나 방화벽으로 트래픽을 리디렉션하고, 분석을 위해 다시 Cisco WSA로 리디렉션해야 합니다. 그런 다음 Cisco WSA에서 모든 웹 보안 기능을 적용합니다.

Cisco 서비스

Cisco Branded Services

- **Cisco SMARTnet™ Service for Web Security Appliance** : 고객은 언제든지 직접 Cisco 전문가에게 문의하거나 셀프 헬프 지원 툴과 신속한 하드웨어 교체에 액세스하여 네트워크 문제를 빠르게 해결할 수 있습니다.
- **Cisco Security Planning and Design**: 고객의 요구사항에 적합한 Cisco WSA 모델을 평가할 수 있도록 지원합니다. 이 서비스를 활용하여 빠르고 쉽게, 비용 효과적으로 강력한 보안 솔루션을 구축하십시오.
- **Cisco Web Security Configuration and Installation**: 보안 솔루션의 설치, 구성, 올바른 테스트를 통해 웹 보안 위험을 완화할 수 있도록 지원합니다.
- **Cisco Optimization Service for Security**: 이미 웹 어플라이언스를 구축했고 AMP와 같은 기능으로 이를 최적화하거나 확장하려는 고객을 위한 서비스입니다 사전 대응 차원에서 네트워크를 평가하고 강화하여 진화하는 보안 위협 및 예기치 않은 사고에도 효과적으로 대응할 수 있도록 지원합니다.

Cisco Financing

Cisco Capital®에서는 고객의 비즈니스 요구사항에 부합하는 맞춤형 파이낸싱 솔루션을 제공합니다. 따라서 고객이 더 빨리 Cisco 기술을 활용하면서 비즈니스 성과를 거둘 수 있습니다.

마켓 리더십

- Gartner는 2015년 보안 웹 게이트웨이 Magic Quadrant에서 Cisco Web Security를 Challenger 그룹에 선정했습니다.
- IDC의 조사에서 Cisco는 전체 보안 어플라이언스 시장의 점유율 1위를 차지했습니다(2015년 6월).
- 또한 Gartner는 2015년 네트워크 액세스 제어 및 이메일 보안 Magic Quadrant에서도 Cisco를 Leader 그룹에 선정했습니다.

왜 Cisco를 선택해야 할까요?

Cisco를 선택한 고객은 Talos, 제로 데이, 지능형 위협 차단, 여러 안티 멀웨어 엔진을 하나의 디바이스에서 모두 사용하여 광범위한 위협으로부터 보호받을 수 있습니다. 중앙 집중식 관리 및 보고 기능을 통해 심층 가시성이 제공됩니다. 유연한 구축 옵션으로 물리적 리소스 또는 가상 리소스를 십분 활용할 수 있습니다. 세계 각처에서 24시간 제공되는 업계 최고 수준의 지원 서비스는 언제라도 Cisco 전문가의 도움을 받아 신속하게 궁금증이나 문제점을 해결할 수 있도록 보장합니다. 또한 Cisco WSA는 ISE 및 AMP와 같은 다른 Cisco 제품과의 통합을 통해 네트워크 성능 저하 없이 투자 가치를 확대하고 보안을 실현합니다. 마지막으로, "한 번만 설정하면 되는 Cisco 기술" 덕분에 컨피그레이션을 설정하고 최초 정책 설정을 적용한 후에는 관리 시간이 크게 단축됩니다.

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 Financing을 통해 하드웨어, 소프트웨어, 서비스, 보완적인 서드파티 장비를 유연성 있게 도입할 수 있습니다. 또한, 예측 가능한 비용 결제를 한 번만 하면 됩니다. Cisco Capital은 100여 개 국가에서 이용할 수 있습니다. 자세히 보기.

다음 단계

http://www.cisco.com/go/wsa 에서 Cisco WSA에 대해 자세히 알아보십시오.

Cisco Sales Representative, 채널 파트너 또는 시스템 엔지니어와 함께 Cisco WSA with AMP 및 기타 Cisco 보안 제품이 여러분 회사의 시급한 보안 요구사항과 필요조건을 어떻게 효과적으로 충족하는지를 평가해보십시오.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C22-732948-02 01/16