Cisco Webex

The bridge to possible

Webex Calling 보안 백서

Webex Calling 보안 백서

1. 서론

Webex® Calling 은 조직 규모에 상관없이 기업에게 최적화된 클라우드 기반의 전화 시스템입니다. 데스크톱, 모바일 및 원격 근로자에게 꼭 필요한 비즈니스 통화 기능을 제공하며 글로벌 Webex 협업 플랫폼을 통해 제공됩니다. Webex Calling 은 클라우드를 기반으로 유연성, 빠른 혁신, 예측 가능한 운영 비용, 신속한 글로벌 확장을 제공하며 Webex 협업 플랫폼에 연결하여 온프레미스 투자 자산을 보호합니다.
먼저 용어에 관해 설명하자면 이 문서에서 Webex 와 Webex 협업 플랫폼은 다양한 위치로 언급되어 있지만 Webex Calling, Webex Meetings, Webex App 서비스, 이러한 서비스들이 각각 운영되는 인프라 등 Webex 전체 제품 라인을 지칭합니다. Webex Calling 은 Webex 제품 라인의 핵심 서비스로 Webex 협업 플랫폼에서 실행됩니다.

Webex 보안과 개인 정보 보호의 차이점

Webex 는 제품을 설계하고 구현할 때부터 보안과 개인 정보를 기본적으로 고려하여 접근합니다. 또한 검사 프로세스와 균형을 적절히 유지하는 보안 문화를 조성하는 데 투자를 아끼지 않습니다. Webex Calling 을 비롯한 모든 Webex 서비스는 보안 기본 설정을 자동으로 제공하므로 사용자가 구성에 신경 쓸 필요 없이 마음 편히 협업을 수행할 수 있습니다. 그와 동시에 Webex 는 보안을 저해하지 않는 훌륭한 사용자 경험을 제공합니다.

Webex 와 Webex Calling 에는 네트워크에서부터 엔드포인트, 데이터 센터, 클라우드 서비스에 이르기까지 시스코의 풍부한 보안 노하우와 전문성이 뒷받침됩니다. 모든 Webex 제품과 서비스는 CSDL(Cisco Secure Development Lifecycle)을 사용하여 보안 기준에 맞게 구축됩니다. 이러한 제품의 보안은 다양한 직무를 맡은 수백 명의 보안 전문가들로 구성된 팀이 독자적으로 검증합니다. Webex 는 조직 내부에서 협업하거나 다른 사업부와 협업할 때 보안을 기본으로 유지하고 데이터를 보호해주는 엔터프라이즈급 강화형 협업 플랫폼입니다.

프라이버시, 보안, 및 투명성: Webex 의 3 가지 보안 원칙

We Webex 는 고객의 데이터 프라이버시를 존중합니다.

- Webex 는 사용자 데이터를 타사에 대여하거나 판매하지 않습니다.
- Webex 는 항상 보안과 데이터 프라이버시를 염두에 두고 기능을 구현합니다.
- Webex 는 프라이버시 관행을 투명하게 공개합니다.

Webex 는 기본적으로 보안이 유지됩니다.

- Webex 보안은 근본적인 핵심 요소로 구축되며 기본적으로 보안이 유지됩니다. 또한 개인 정보 보호를 위해 옵트 아웃 방식으로 데이터 공유를 거부하거나 설정을 변경하더라도 고객에게 책임을 묻지 않습니다.
- Webex 는 어떤 서비스에서든 강력한 비밀번호를 기본적으로 지원합니다.
- Webex 는 보안 사이버 거버넌스를 바탕으로 보안 문제가 발생할 경우 투명하게 공개합니다.
- Cisco STO(Security and Trust Organization) 팀이 Webex 에 대한 보안 및 개인 정보 보호를 관리 감독하며, 보안 취약점이 발견되면 공개적으로 알립니다.

시스코는 보안을 그 무엇보다 중요하게 생각합니다. 지금까지 보안과 개인 정보 보호를 위해 지속적으로 투자해왔고, 앞으로도 아낌없이 투자하려는 이유도 바로 여기에 있습니다. Webex Calling 은 고객에게 처음부터 끝까지 총체적으로 유지되는 보안을 제공하도록 설계되었습니다. 또한 완성도 높은 프로세스와 거버넌스를 바탕으로 개인 정보를 보호하고 신뢰할 수 있는 보안을 제공합니다. 시스코의 목표는 보안을 저해하지 않고 사용자의 협업을 지원하는 것입니다.

Webex Calling 과 Webex 협업 플랫폼은 관리 업무에서부터 최종 사용자 상호작용에 이르기까지 다양한 작업을 지원하도록 다양한 보안 수준을 제공합니다.

이 백서에서는 고객이 Webex Calling 과 Webex Calling 을 실행하는 Webex 협업 플랫폼 인프라에 대한 투자 여부를 결정할 때 큰 영향을 미치는 주요 보안 기능에 대해 자세히 알아보겠습니다.

1.1 학습 내용

Webex Calling 과 Webex 협업 플랫폼을 안전하게 보호하는 Cisco® 도구, 프로세스, 인증 및 엔지니어링 기법에 대해 알아봅니다.

2. 시스코 보안 모델

시스코는 클라우드 보안 분야를 꾸준히 선도하기 위해 부단히 노력하고 있습니다. Cisco STO(Cisco Security & Trust Organization)는 시스코의 모든 팀과 협력하여 핵심 인프라를 설계, 개발 및 운영하는 데 활용되는 프레임워크에 보안과 신뢰 및 투명성을 확립하여 모든 부분에서 가장 엄격한 보안 수준을 충족합니다.

또한 Cisco STO 는 고객에게 사이버 보안 위험을 완화하고 관리하는 데 필요한 정보를 제공합니다.

Webex 보안 모델(그림 1)의 보안 기반은 시스코의 모든 제품과 솔루션에서 사용되는 것과 동일합니다.

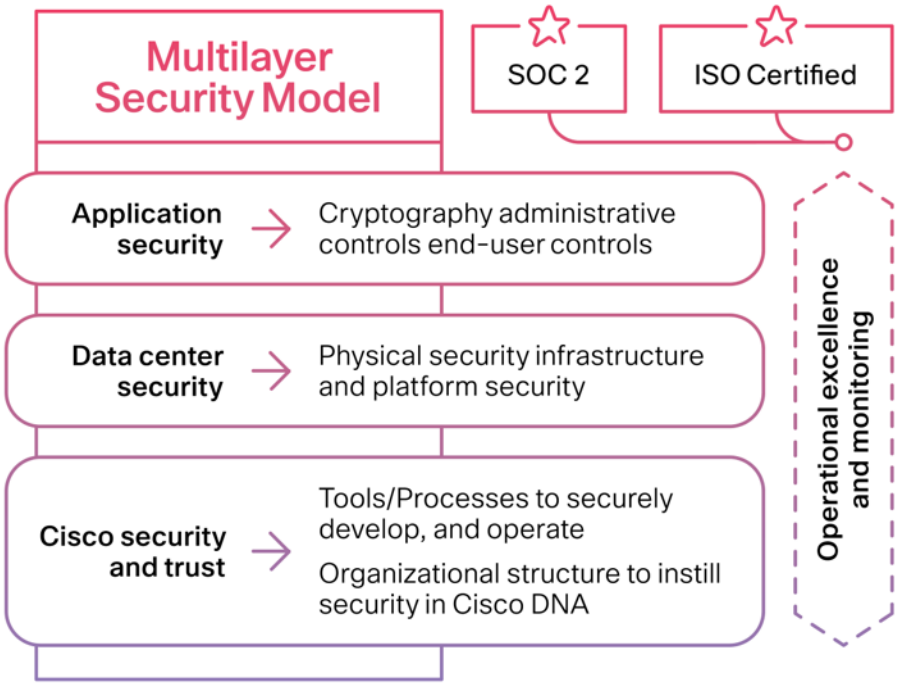

그림 1.
Webex 보안 모델

Webex 조직은 기본 원칙을 충실히 따르면서 Webex 서비스를 안전하게 개발, 운영, 모니터링합니다. 이 백서에서는 이러한 원칙도 몇 가지 살펴봅니다.

2.1 시스코의 보안 및 신뢰

시스코의 모든 제품 개발 팀은 Cisco SDL 을 따라야 합니다(그림 2). Cisco SDL 은 시스코 제품의 탄력성과 신뢰도를 높이도록 설계된, 반복과 측정이 가능한 프로세스입니다. 개발 라이프사이클의 모든 단계에 도입된 도구와 프로세스 및 의식 교육은 심층 방어 체제를 유지하고

제품의 탄력성에 대한 총체적 전략을 확립하는 데 도움이 됩니다. Webex 제품 개발 팀은 Webex Calling 제품 개발의 모든 단계에서 이 라이프사이클을 따릅니다.

보안 개발 라이프사이클(SDL)에 대해 자세히 알아보십시오.

2.2 시스코의 기본 보안 도구

Cisco STO 는 보안 조치를 취해야 하는 모든 개발자가 일관된 입장을 고수하는 데 필요한 프로세스와 도구를 제공합니다.

전담 팀이 이러한 도구를 개발하여 제공하므로 제품 개발 프로세스에서 불확실성이 해소됩니다. 이러한 도구는 대표적으로 다음과 같습니다.

- 제품이 충족해야 하는 제품 보안 기준(PSB) 요건
- 위협 모델링 과정에 사용되는 위협 시뮬레이션 도구
- 코딩 가이드라인
- 개발자가 보안 코드를 직접 작성할 필요 없이 사용할 수 있는 검증/인증된 라이브러리
- 개발 완료 후 보안 결함을 찾아내는 데 사용되는(정적 및 동적 분석용) 보안 취약점 테스트 도구
- 시스코와 타사의 라이브러리를 모니터링하고 취약점이 발견되면 제품 팀에게 알려주는 소프트웨어 추적 도구

2.3 시스코 프로세스에 보안을 구현하는 조직 구조

시스코는 보안 프로세스를 전사적으로 구현하고 관리하는 전담 부서를 두고 있습니다. 시스코는 다음과 같은 팀을 운영하여 보안 위협 및 문제를 지속적으로 파악합니다.

- Cisco 정보 보안(InfoSec) Cloud 팀
- Cisco 제품 보안사고 대응 팀(PSIRT)
- 보안 책임 분담

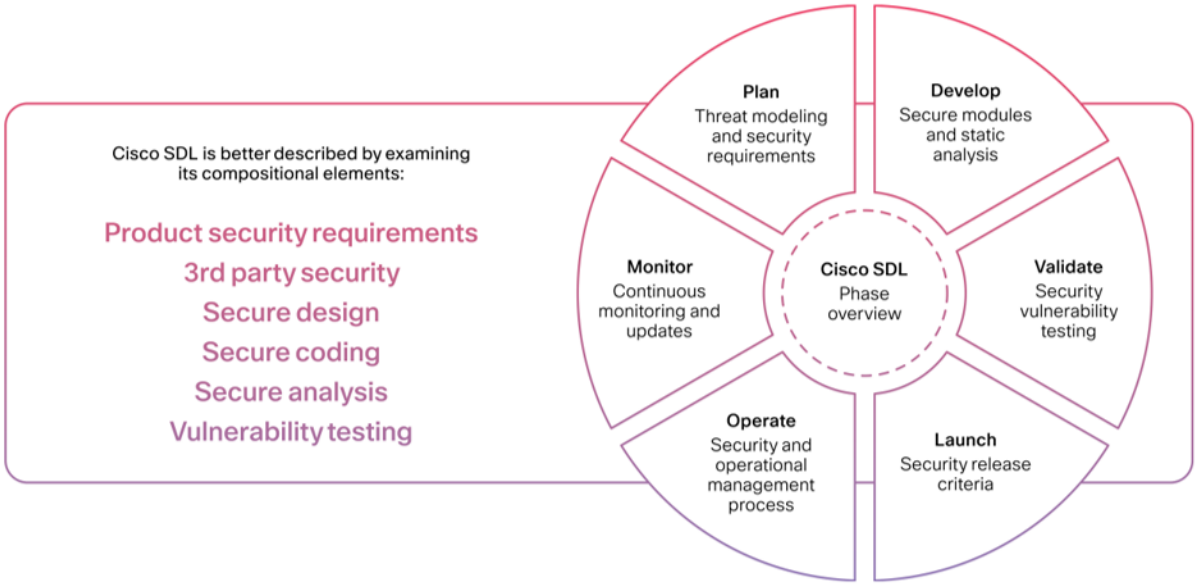

그림 2.
Cisco SDL(Secure Development Lifecycle)

2.4 Cisco 정보 보안(InfoSec) Cloud 팀

클라우드 사업부 최고 보안 책임자가 이끄는 정보 보안(InfoSec) Cloud 팀은 고객에게 안전한 Cisco Webex 환경을 제공할 책임이 있습니다. 이러한 목표를 달성하기 위해 Cisco 정보 보안(InfoSec) Cloud 팀은 Webex 를 고객에게 제공하는 과정에 관여하는 모든 부서에서 사용할 보안 프로세스와 도구를 정의하여 시행합니다.

또한 시스코의 다른 팀과 협력하여 Webex 를 표적으로 삼은 모든 보안 위협에 대응하며,

Webex 의 보안 상태를 지속적으로 개선합니다.

2.5 Cisco STO – 사고 지휘 팀

Cisco STO – 사고 지휘 팀은 시스코의 제품 및 서비스와 관련된 보안 문제의 수집, 조사 및 보고 업무를 전담 관리하는 글로벌 팀입니다. 사고 지휘 팀은 보안 문제의 심각성에 따라 다양한 매체를 사용하여 정보를 공개합니다. 보고 형식은 다음과 같은 조건에 따라 달라집니다.

- 취약점을 해소할 수 있는 소프트웨어 패치나 대책, 또는 심각한 취약점을 해소할 수 있는 코드 픽스를 공개할 예정인 경우
- 시스코 고객에게 더 큰 위험을 초래할 수 있는 취약점을 적극 악용한 사례를 사고 지휘 팀이 확인한 경우 이 경우 사고 지휘 팀은 해당 취약점을 설명하는 보안 공지를 가급적 빨리 게시합니다. 패치를 배포할 준비가 안 된 상태이기 때문입니다.
- 시스코 제품에 영향을 미치는 취약점에 대한 대중의 인식 부족 때문에 시스코 고객이 더 큰 위험에 빠질 수 있는 경우 이 경우에도 역시 패치를 배포할 준비가 되지 않았더라도 사고 지휘 팀이 고객에게 상황을 알립니다.

어떤 경우든 사고 지휘 팀은 최종 사용자가 취약점의 영향을 평가하고 자사의 환경을 보호하기 위한 조치를 취하는 데 필요한 최소한의 정보만 공개합니다. 사고 지휘 팀은 CVSS(Common Vulnerability Scoring System) 척도를 사용하여 공개된 문제의 심각도를 평가합니다. 그리고 정보 공개 시 취약점을 악용할 가능성을 고려해 취약점의 세부 정보는 공개하지 않습니다.

사고 지휘 팀에서 공개하는 취약점을 tools.cisco.com/security/center/publicationListing.x 에서 알아보십시오.

독보적인 가시성과 위협 차단 능력을 자랑하는 Cisco Talos 팀

300 명 이상의 연구원으로 구성된 Cisco Talos 는 세계 최대 규모의 상업적 위협 인텔리전스 팀으로, 오늘날 공격에 광범위하게 사용되는 악성 도메인과 IP, URL 및 파일을 찾아내어 차단합니다. 또한 수많은 전 세계 인터넷 활동 정보를 통계와 머신 러닝이 결합된 모델에 입력하여 인터넷에서 발생하는 새로운 공격을 탐지합니다. 그 밖에도 안티 바이러스 엔진인 Cisco Advanced Malware Protection(AMP)과 Cisco Threat Grid 의 샌드박싱으로 수백만 개에 이르는 새로운 멀웨어 샘플을 매일 분석하여 인텔리전스 정보를 이용하기 때문에 악성 파일을 가장 효과적으로 차단할 수 있습니다.

2.6 보안 책임 분담

Webex 그룹의 모든 구성원이 보안에 대한 책임이 있지만, 주요 책임자는 다음과 같습니다.

- 보안 및 애플리케이션 부문 수석 부사장/총괄 관리자
- 협업 부문 수석 부사장/총괄 관리자
- Webex 플랫폼 및 인프라 엔지니어링 부문 부사장
- 협업 부문 최고 정보 보안 책임자

3. Webex Calling 데이터 센터 보안

Webex Calling 은 Webex 클라우드를 통해 제공되는 클라우드 솔루션입니다. Webex 클라우드는 업계 최고의 성능, 통합, 유연성, 확장성, 가용성을 자랑하는 매우 안전한 서비스 제공 플랫폼입니다. 또한 오디오, 비디오 및 콘텐츠를 실시간으로 공유하는 목적에 적합한 통신 인프라이기도 합니다.

Webex Calling 은 전 세계 곳곳의 데이터 센터에 설치된 컴퓨팅 장비를 사용합니다. 주요 인터넷 액세스 포인트와 가까운 곳에 전략적으로 배치된 데이터 센터는 전용 고대역폭 광섬유 통신을 이용해 전 세계의 트래픽을 전송합니다.

데이터 센터는 SSAE-16 과 SOC-2 인증을 획득했으며, 물리적 보안 경계, 물리적 출입 통제, 사무소/사무실/시설 보호, 외부 위협 및 환경 위협 차단, 보안 구역 근무, 공공 전력/케이블 보안/배송 및 하역장 지원 등 SOC2 규정 준수 인증 여부에 대한 평가를 매년 받고 있습니다. Webex Calling 애플리케이션과 서비스는 시스코를 비롯한 타사 데이터 센터에서 다수의 서버를 통해 실행됩니다. Webex Calling 은 보안 및 가용성 기법과 절차를 고려하여 설계되어 물리적 접근 및 보호, 네트워크 연결, 원격 및 로컬 액세스, 애플리케이션 및 서버 관리, 가용성, 고객의 중요 데이터 보호 등을 지원합니다. 시스코는 대규모 데이터 센터의 설계, 구현 및 운영에 수년간의 경험을 쌓은 데이터 센터 운영 기관과 협력합니다. 이러한 기관들은 물리 및 환경적 보안과 액세스 보안을 제공하여 Webex Calling 물리 및 가상 애플리케이션 환경을 보호합니다. 예를 들면 다음과 같습니다.

- 24 시간 상주하는 보안 요원
- 아무런 설명이나 표시 없이 자연스럽게 경계를 보호하는 시설
- 지역의 치안 기관에 자동으로 신고하는 무소음 경보 시스템
- 지역 정부 표준에 따른 건축 법규 준수
- 환경 보호
- 완전한 이중화 HVAC 시설
- 자동 방화 시스템, 이중 경보(열기/연기), 교차 링크를 통해 이벤트를 관리하는 이중 인터록
- 이중화 백업 발전기와 함께 전체 데이터 센터 전력량을 지원하는 N+ 1 이중화 무정전 전력원(UPS) 시스템
- 위치별 재해복구 계획(지진, 홍수 통제)
- 접근에 대한 생체인식 스캔 및/또는 이중 요소 인증
- 전원 연결 통로를 통한 출입(침입자 통제)
- 접근 시 정부에서 발급하는 유효한 사진 ID 요구, 감사 목적으로 모든 접근 이력 기록
- 액세스 이전 권한 요구, 합법적인 비즈니스 목적에 한해 액세스 권한 제공
- 코로케이션 구역에서 벽을 세워 수발신 분리
- 출입 시 현장 보안 요원이 도착하는 모든 물품을 검사

Webex Calling 컴퓨팅 자산에 액세스할 때는 관리자가 이중 요소 인증(2FA)을 사용합니다. 사용자와 관리자의 모든 활동이 기록됩니다. Webex Calling 보안 운영 센터(SOC)가 시스템 로그를 비롯한 침입 탐지 시스템(IDS)과 방화벽 경보를 24 시간 모니터링하여 공격 또는 잘못된 사용을 탐지하고 차단합니다.

4. 인프라 및 플랫폼 보안

시스코의 보안 접근 방식은 Webex 협업 플랫폼을 구성하는 네트워크, 시스템 및 전체 데이터 센터의 보안 문제를 해결합니다. 네트워크 서비스 엔지니어들이 패치를 통해 운영 체제와 인프라를 강화하여 각종 보안 취약점으로부터 시스템을 보호합니다. 서버에서 데이터를 전송할 때는 안전성과 신뢰성이 보장되어야 합니다.

운영 체제, 미들웨어 및 애플리케이션 강화 방법:

- 보안에 민감한 시스템에 대한 지속적인 강화
- 프로덕션 환경 배포 이전 보안 심사 및 인수 검증
- 취약점 검사 및 진단
- 보안 패치

- 멀웨어 차단
- 강력한 로깅 구현 및 구성
- 강력한 인증
- 신중한 액세스 제어, “최소 권한” 및 “알 필요” 구성
- 정보 백업

적합한 액세스 제어를 통해 강화된 시스템은 명시적으로 필요한 사용자나 예상되는 시스템 기능에 따라 허용되는 사용자로 시스템 기능에 대한 액세스를 제한합니다. 시스템, 소프트웨어 버전 및 업그레이드는 스테이징 환경에서 교차 검사를 비롯해 필요한 테스트를 받아야만 프로덕션 환경에 대한 배포와 사용이 허용됩니다. 또한 정보 시스템의 기술적 취약점이 모니터링 및 기록됩니다. 운영 팀은 이러한 취약점에 대한 노출 여부를 평가한 후 필요한 패치 관리 라이프사이클 조치를 통해 관련된 위험을 해소합니다. 그 밖에도 정보 처리 시설의 이용 상황을 모니터링할 수 있는 프로세스가 마련되어 있으며 운영 팀이 이러한 모니터링 활동을 주기적으로 검토합니다.

5. 네트워크 통신 보안

네트워크를 통해 서로 연결되는 정보와 시스템은 중요한 비즈니스 자산입니다. 따라서 모든 수준에서 네트워크 보안을 유지하고 보장할 수 있어야 합니다. 운영 팀은 기술적 수단과 관리 절차를 통해 이러한 네트워크 보안을 구현합니다.

네트워크 보안을 예로 들면 다음과 같습니다.

- DMZ(Demilitarized Zone)
- 방화벽
- 침입 탐지
- 시스템 인증
- 데이터 암호화

보안 관리 팀이 모든 네트워크 서비스의 보안 기능, 서비스 수준, 관리 요건을 결정합니다. 네트워크를 관리하고 제어하여 위협으로부터 보호할 뿐만 아니라 네트워크를 사용하는 시스템과 애플리케이션의 보안을 유지하며, 여기에는 전송 정보에 대한 보안도 포함됩니다. 또한 적절한 사용자 인지도 절차와 함께 탐지, 예방 및 복구 제어를 통해 악성 코드를 차단합니다. 감사 로그는 사용자 활동, 예외 및 정보 보안 이벤트를 빠짐없이 기록합니다. 운영 보안 팀은 이러한 로그를 보관하여 앞으로 있을 조사와 액세스 제어 모니터링을 지원합니다. 그 밖에도 정기적인 독립 검토를 통해 정보 보안 프로세스가 적합한지, 완전한지, 목적에 부합하는지, 적용되는지를 확인합니다.

6. Webex Calling 애플리케이션 보안

6.1 암호화

6.1.1 전송 데이터 보호

Webex Calling 은 액세스 측에서 네트워크 통신에 액세스할 수 있도록 데이터 암호화를 구현합니다. Webex Calling 은 액세스 측에서 네트워크 통신에 액세스할 수 있도록 데이터 암호화를 구현합니다. 시스템에 대한 관리자 액세스는 다음과 같은 전송 계층 보안(TLS) 버전과 강력한 암호 제품군을 사용해 암호화됩니다.

TLS 1.3 암호 제품군:

- TLS_CHACHA20_POLY1305_SHA256

- TLS_AES_256_GCM_SHA384
- TLS_AES_128_GCM_SHA256

TLS 1.2 암포 제품군:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA

SIP 엔드포인트와 서비스 사이에서 전송되는 SIP 콜 제어 신호는 다음과 같은 전송 계층 보안(TLS) 버전과 강력한 암호 제품군을 사용해 암호화됩니다.

TLS 1.2 암호 제품군:

- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_GCM_SHA384

SIP 엔드포인트와 서비스 간 미디어 스트림은 RFC 3711 에서 설명하는 보안 실시간 전송 프로토콜(SRTP)을 통해 보호됩니다.

6.1.2 유휴 데이터 보호

Webex Calling 은 비즈니스에 중요할 수 있는 조직 데이터와 사용자 데이터를 저장합니다. Webex Calling 은 다음과 같은 보안 조치를 통해 유휴 데이터를 보호합니다.

- AES 256 에 따른 유휴 데이터 암호화
- 단방향 해싱 알고리즘과 Salt 를 사용하여 모든 사용자 비밀번호 저장
- 기타 비밀번호 암호화(SIP 인증)
- 모든 백업 파일 및 아카이브 암호화

6.2 액세스 제어

Webex 서비스에서는 적합한 액세스 제어 수준이 정의되어 운영 환경에 구현됩니다. 이러한 정책에 따라 액세스 제어가 각 시스템, 애플리케이션, 데이터베이스 또는 네트워크에 적용되어 다양한 유형의 데이터와 데이터에 액세스하는 사용자를 관리합니다. 액세스 제어는 권한을 요청하거나, 승인하거나, 부여하거나,

취소하는 표준 프로세스, 사용자 액세스를 수정하는 표준 프로세스, 사용자 역할을 정의하는 표준 프로세스로 구성됩니다. 또한 직무 분석, 최소 권한 액세스, 사용자 비밀번호, 사용자 식별 정책 및 표준, 사용자 액세스에 대한 감사 기대 효과, 네트워크 액세스 제어 목록, 네트워크 및 액세스 활동에 대한 감사가 서로 분리되어 구성됩니다.

시스템과 애플리케이션에서 구성과 정보에 액세스해야 하는 경우에는 액세스 제어 정책에 따라 사용자 계정과 액세스 제어를 구현해야 합니다. 정책 및 제어 범위는 시스코 고객 경험(시스코 서비스) 팀에서 소유하여 운영 또는 관리하는 인프라와 애플리케이션에 대한 액세스로 제한됩니다.

사용자 계정과 액세스 제어는 다음과 같은 보안 요건을 충족합니다.

- 모든 사용자에게 고유한 ID 가 할당되며, 할당된 권한 구성 요소에 액세스할 때는 인증을 받아야 합니다.
- ID 와 인증 자격 증명은 단일 사용자 외부로 배포되지 않으며, 그룹/공유 자격 증명은 공유하거나 배포되지 않습니다.
- 사용자 ID, 자격 증명 또는 기타 식별자 객체의 추가, 삭제 및 변경은 시스템에서 제어합니다.
- 액세스는 직무 책임에 필요한 최소 권한에 따라 권한 있는 사용자 ID 로 제한됩니다.
- 특정 액세스의 경우, 권한 있는 사용자가 식별되어야 합니다.
- 계약이 종료된 사용자의 액세스는 즉시 취소됩니다.
- 유효하지 않은 사용자 계정은 취소 또는 비활성화됩니다.
- 타사에서 시스템 구성 요소에 액세스하거나, 지원하거나, 유지할 때 사용되는 ID 도 관리할 수 있습니다.

이러한 제어 범위는 관리 책임자 또는 지정된 보안 책임자가 정의, 승인, 이행, 감독합니다. 또한 내부에서, 그리고 외부 감사 기관을 통해 최소 년 1 회 제어 범위에 대한 정확성과 효과를 심사합니다.

6.3 사용자 인증

구독 사용자들은 독립적인 아이덴티티 관리 또는 고객 프레미스 하이브리드 아이덴티티 통합을 제공하는 클라우드 규모의 ID 플랫폼인 Webex Identity 에 등록됩니다. 또한 Active Directory 사용자 계정 복제, 주요 공급업체(Okta, Ping Identity 등)가 포함된 SSO(Single Sign-On), 고객용 API 등이 통합됩니다. 그 밖에도 CI 가 최신 기술과 표준(SAML 2.0, OAuth2, REST 등)을 기반으로 시스코의 클라우드 협업 포트폴리오를 뒷받침할 뿐만 아니라 향후 확장과 조정, 그리고 클라우드 규모 애플리케이션에 맞게 설계되었습니다.

7. 가용성

Webex Calling 은 이동통신 사업자 수준의 가용성을 고려하여 설계되었습니다(99.99% 가용성). 이동통신 사업자 수준의 가용성을 구현하는 기법은 다음과 같습니다.

- N+1 서버 클러스터링
- 지리적 이중화(3 개 대륙에 10 개의 데이터 센터 구축, 그림 3 참조)
- 데이터 센터 내에서, 데이터 센터 간 데이터 자동 복제
- 분산 서비스 거부 공격(DDoS) 탐지 및 방지

Webex Calling 재해 복구 계획에는 Webex Calling 엔지니어링 팀과 운영 팀에서 운영하는 네트워크 및 서비스 요소의 이중화 설계 방식을 비롯해 재해 발생 시 네트워크 및 서비스 기능을 정상적인 상태로 빠르게 복구하는 방법이 정의되어 있습니다. 시스코는 지리적으로 이중화된 데이터 센터를 통해 Webex Calling 서비스를 제공합니다.

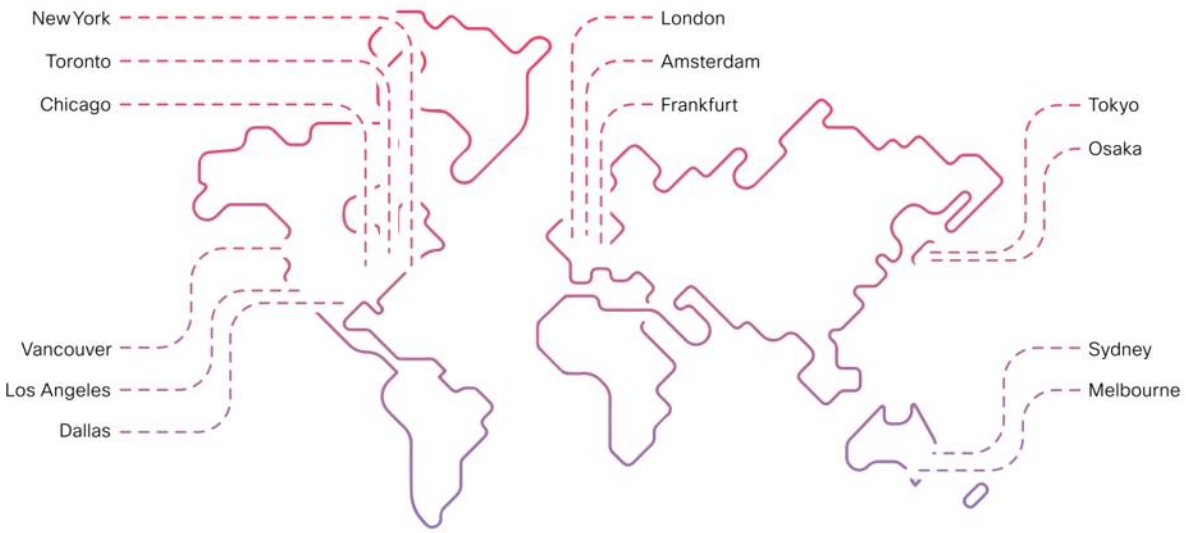

그림 3.
데이터 센터 위치

이들 데이터 센터에는 고객에게 서비스를 제공하는 데 필요한 데이터 네트워크와 서버 장비가 모두 포함되어 있습니다. 시스코 직원들이 상주하는 사무소는 이러한 데이터 센터와 물리적으로 분리되어 있습니다. 따라서 이벤트가 발생하여 시스코 직원의 사무소 중 한 곳을 사용할 수 없게 되더라도 데이터 센터를 통해 제공되는 고객 서비스는 아무런 영향도 받지 않습니다. 또한 이벤트가 발생하여 시스코 사무소 한 곳에 영향을 미칠 경우에는 Webex Calling 운영 팀이 전 세계 어디에서나 보안 VPN 액세스를 통해 원격으로 네트워크 및 서비스 요소를 운영할 수 있습니다.

나아가 Webex Calling 솔루션은 데이터 센터 한 곳에서 이벤트가 발생하여 사용할 수 없게 되어도 트래픽을 다른 데이터 센터로 리디렉션하여 처리할 수 있도록 설계되었습니다. 시스코는 세계적인 수준의 데이터 센터 공급업체를 통해 네트워크와 서비스 기능에 필요한 공간과 전력을 제공합니다. 이러한 공급업체들은 모두 99.99%가 넘는 가동 시간과 24 시간 데이터 센터 모니터링으로 SSAE 16 Type 2 를 준수합니다. 모든 음성 통화 제어 요소와 음성 서비스 요소는 데이터 센터 한 곳을 사용할 수 없게 되었을 때 데이터 센터 사이에서 자동으로 마이그레이션하도록(장애 조치) 설계되었습니다. 전체 장애 조치 프로세스는 실시간에 가깝게 자동으로 실행됩니다. 프로비저닝, 구성 웹 인터페이스 같은 운영 서비스 요소는 모두 활성/대기 아키텍처로 설계되어 데이터 센터 한 곳을 사용할 수 없게 될 경우 다른 데이터 센터로 직접 마이그레이션할 수 있습니다.

8. Webex Calling 운영 보안

8.1 보안 정책

Webex Calling 비즈니스 프로세스에서는 정보와 정보 시스템 및 관련된 모든 자산이 반드시 필요하며, 무엇보다 중요합니다. Webex Calling 은 민감도, 가치, 중요도에 따라 정보 자산을 보호합니다. 보안 조치는 정보가 저장되는 미디어, 정보를 처리하는 시스템 또는 정보를 전송하는 기법에 상관없이 적용됩니다.

시스코는 보안 라이프사이클 관리 프로세스에 따라 정보 보안 정책을 관리합니다. 여기에는 다음과 같은 정책 중심 구성 요소가 포함됩니다:

- 인가, 승인, 구현
- 연간 검토, 업데이트(필요 시) 및 재인증
- 연간 통신 및 인식 교육
- 예외 관리

8.2 사기 탐지

시스코는 사기 탐지의 중요성을 인지하고 있습니다. 복합적이고 광범위한 애플리케이션을 개발하는 이유도 바로 여기에 있습니다. 이러한 애플리케이션들은 통화 세부 기록(CDR)을 이용해 사기 활동을 나타내는 통화 패턴을 분석하여 시스코 운영을 뒷받침하는 동시에 플랫폼에서 통화 트래픽을 모니터링하여 운영 팀을 지원합니다.

8.3 정보 분류

정보 분류는 적절한 보안 수준으로 자산을 적용하는 데 유용합니다.

관리 팀과 리소스 팀이 미디어 유형에 상관없이 내부 또는 외부 배포를 엄격하게 제어합니다.

대표적으로 다음과 같은 제어조치가 있습니다:

- 데이터 민감도를 판단할 수 있는 미디어 분류
- 비즈니스 또는 법률상의 이유로 더 이상 필요가 없는 미디어 파기
- 데이터를 재구성할 수 없도록 필사물의 파쇄, 소각 또는 재생지 사용 여부 결정
- 파기할 자료를 안전하게 보관할 수 있는 컨테이너

8.4 자산 관리

인프라 자산 관리는 필요한 서비스 수준을 가장 비용 효율적인 방법으로 제공한다는 목적 하에 관리, 재무, 경제, 엔지니어링, 기타 물리적 자산에 적용되는 방침을 통칭하는 용어입니다.

Webex Calling 은 인프라 자산 관리 인벤토리를 시스템과 구성 요소로 구현하며, 시스템과 구성 요소는 소유자, 연락처 정보, 자산 목적을 언제든지 정확하게 알아낼 수 있는 방법으로 구성됩니다. 그 밖에도 물리적 호스트와 가상 머신 인벤토리가 자산 관리에 포함될 수 있습니다.

운영 관리 팀은 서비스 플랫폼 환경에 배포되는 자산을 모두 책임집니다. 환경 내에서 관리가 되지 않거나 사용하기 부적절한 자산은 허용되지 않습니다. 만약 환경 내에서 관리가 되지 않는 자산이 발견되면 운영 관리 팀의 책임으로 귀속되거나, 환경에서 제거 및/또는 차단되어야 합니다.

시스코는 고객들에게 모든 미디어에 대한 인벤토리 로그를 유지하면서 최소 년 1 회, 그리고 자산을 이동, 추가, 변경, 폐기할 때마다 미디어 인벤토리를 구성하도록 권장하고 있습니다.

8.5 직무 분리

직무 분리는 우발적이거나 고의적인 시스템 오용 위험을 줄이기 위한 방법으로 적용됩니다. 정책, 프로세스 및 절차에 대한 실사를 통해 누구든지 한 사람이 승인 없이, 혹은 은밀하게 자산에 액세스하거나, 자산을 변경하거나, 자산을 사용하지 못하도록 방지합니다.

이벤트 시작은 승인과 서로 분리되어 있습니다. 이러한 제어 설계 덕분에 결탁 가능성에 대한 관리 감독과 거버넌스가 가능합니다.

IT 인프라 및 애플리케이션을 위한 개발 환경, 테스트 환경, 프로덕션 환경이 서로 분리되어 운영 시스템에 대한 무단 액세스 또는 변경 위험이 줄어듭니다. 운영 팀은 액세스에 필요한 비즈니스 및 보안 요건에 따라 액세스 제어 절차를 구성, 기록, 검토합니다. 구성 정보와 애플리케이션 코드는 안전하게 암호화된 데이터베이스에 저장됩니다.

8.6 로깅 및 모니터링

운영 팀은 폭넓은 운영 프로세스를 바탕으로 고가용성을 지원합니다. 이러한 프로세스로는 주요 인적 자원 선정, 지원 및 연락 프로세스, 시스템 로깅, 모니터링, 시스템 테스트 프로세스, 네트워크 성능 등이 있습니다. 이때 비정상적인 문제로 인해 경고가 발생하면 심각도를 기준으로 해결됩니다.

운영 팀은 모든 서버와 인터넷 연결, 지연 시간, 가용성, 대역폭, 심각도를 지속적으로 모니터링하여 서버 네트워크 성능을 유지관리합니다. 모든 운영 및 보안 로그는 가용성 유지를 위해 장기간 보관됩니다. 네트워크 운영 팀은 용량 계획의 일환으로 이러한 기록을 주기적으로 검토합니다.

8.7 공급업체 관리와 공급업체 관계

시스코는 공급업체 보안 평가 프로그램을 관리하여 Webex Calling 에 제공되는 모든 타사 서비스가 보안 위험 및 규정 준수 요건에 상응하는 보안 상태를 유지하도록 관리하고 있습니다. 주요 공급업체들은 이 프로그램에 따라 보안 상태에 변화가 없는지 주기적으로 재평가를 받습니다.

8.8 변경 관리

변경 관리는 서비스 관리에서 빼놓을 수 없는 요소인 동시에 서비스 전송 네트워크에 변경 사항을 도입하는 표준 프로세스이기도 합니다. 어떤 변경 사항이든지 성공적으로 구현하려면 변경 관리가 반드시 필요합니다. 변경은 엔지니어링, 시스템 엔지니어링, 서비스 관리, 지원, 전문 서비스, 심지어 고객까지 다양한 그룹에서 비롯됩니다.

변경 사항을 구현하는 프로세스를 설계 및 검토한 후 모든 조직에게 알려야 하며, 이러한 과정은 공식 발표된 기간 내에 이루어집니다. 이를 통해 모든 이해관계자가 변경 사항에 대해 알고 있고, 어떤 관점에서든지 발생할 수 있는 문제를 예상하고, 변경 적용을 인지하고, 변경 사항 도입에 따라 실제로 문제가 발생했을 때 비정상적인 동작의 원인을 찾아낼 수 있습니다. 시스코는 공개 웹 페이지를 통해 예정된 Webex Calling 유지보수 정보를 실시간으로 제공하고 있습니다.

8.9 인적 자원

8.9.1 관리자 및 개발자 신원 조회

시스코는 지정된 개인 및 법인에 대한 신원 조회와 관련된 프로세스 및 절차를 명시하는 신원 조회 정책을 마련했습니다.

8.9.2 고용 약관: 허용되는 사용 사례

시스코 자산을 사용하거나, 시스코 자산에 액세스하는 직원 및 외부 당사자는 시스코 정책 및 IT 핸드북에서 규정하는 허용 사용 사례에 대한 정책을 인지해야 합니다. 모든 직원과 계약자는 시스코 정책 및 IT 핸드북을 읽고 이해하였음을 동의해야 합니다. 시스코 정책을 위반한 것으로 드러난 직원은 징계 처분을 받을 수 있으며, 심할 경우 고용 해지 조치를 당할 수 있습니다.

8.10 교육

모든 직원은 오리엔테이션 프로세스에서 폭넓은 보안 교육을 받으며, 이후로도 매년 계속해서 보안 교육을 받습니다. 또한 직무에 따라 보안 관련 교육을 추가로 받아야 할 수도 있습니다.

8.11 고객 지원

고객 지원 엔지니어는 다양한 도구를 이용해 모든 시스템 구성 요소의 상태를 지속적으로 모니터링하여 모든 시스템과 클라이언트 애플리케이션이 정상적으로 가동되도록 관리해야 합니다. 이러한 도구들은 문제 발생 징후가 처음 발견되면 담당자에게 경고하여 실제로 네트워크 운영에 영향을 미치기 전에 잠재적 문제를 해결하는 데 효과적입니다. 그 밖에 문제 해결 절차(진단 실행 등)를 자동으로 시작하는 기능도 있습니다.

지원 엔지니어들은 네트워크 운영을 모니터링하면서 네트워크 긴급 상황에 대응할 뿐만 아니라 고객 지원 팀과 고객을 연결하는 주요 통신 링크 역할을 합니다. 또한 고객이 보고한 문제를 자동 문제 추적 시스템에 기록하고, 빠르게 문제를 해결하는 데 필요한 작업을 지속적으로 조정하여 고객 만족도를 높입니다.

지원 구조의 계층화와 더불어 이러한 정책을 시행하면 개인 정보가 권한이 없는 자에게 노출되지 않도록 지원 인시던트가 보호하는 데 유용합니다.

8.12 정보 보안 사고 관리

시스코의 사고 대응 계획 관리 매뉴얼은 미국 국립표준기술연구소(NIST) 800-61 컴퓨터 보안 사고 처리 가이드를 준수합니다. 사고 관리 정책은 비즈니스 크리티컬 서비스를 제공하거나, 비즈니스 크리티컬 서비스를 지원하는 애플리케이션, 소프트웨어 또는 하드웨어를 유지 보수하는 서비스 담당자에게 적용됩니다.

사고 관리의 목적은 정상적인 서비스 운영을 최대한 빠르게 복구하여 비즈니스 운영에 미치는 영향을 최소화하는 데 있습니다. 여기서 정상적인 서비스 운영이란 서로 합의한 서비스 수준 계약(SLA) 제한 범위 내에서 운영하는 것을 말합니다.

시스코는 보안 사고 대응 및 평가를 수행하기 위한 정책과 절차를 문서화합니다. 보안 사고에 대한 대응은 탐지, 기록, 전달, 격리, 평가, 복구, 제거의 7 단계로 이루어집니다.

8.13 비즈니스 연속성과 재해 복구

Webex Calling 조직은 운영 단위마다 비즈니스 연속성 계획 스크립트가 있습니다. 또한 다수의 데이터 센터에 필요한 예비 용량을 포함해 운영 계획을 유지하여 지속적인 가용성을 보장합니다. 그 밖에도 효과적인 비즈니스 연속성 관리 시스템을 구축 및 유지하도록 명시한 ISO 22301 의 지침을 준수합니다.

비즈니스 연속성 계획은 매년 정해진 일정에 따라 테스트를 진행합니다. 실제로 사고가 발생한 경우에는 향후 운영 평가 및 개선을 목적으로 후속 조치와 사후 분석을 실시합니다. 비즈니스 영향 분석에서는 조직 구조를 고려하여 다양한 운영 장애 시나리오에 대한 위험도 평가 결과에 따라 비즈니스 연속성 및 재해 복구 시스템을 평가하여 운영 계획을 일관되게 충족하고 있는지 점검합니다.

Webex Calling 조직은 백업 절차를 구현합니다. 매일 증분 백업을 실시하여 최소 3 주 동안 오프사이트에 저장하고, 주 1 회 전체 백업을 실시하여 최소 3 주 동안 오프사이트에 저장하며, 일부 백업은 수년간 보관합니다. 백업 데이터는 데이터 센터 두 곳으로 이중화하여 스토리지 노드에, 그리고 암호화된 타사 클라우드 스토리지에 저장됩니다. 백업 무결성을 월 1 회 이상 테스트하며, 백업 테스트와 함께 비상 계획에 대한 테스트도 년 1 회 필요합니다.

9. 산업 표준 및 규정 준수

Webex Calling 은 ISO 27001:2013 인증을 획득하였으며, 그 밖에 ISO 27017:2015 및 ISO 27018:2019 보안 제어에 대한 평가까지 추가로 받았습니다. ISO 표준은 매년 재인증 여부를 두고 심사를 받습니다. 또한 Webex Calling 은 근거가 되는 신뢰 서비스 기준을 비롯한 관련 보안 제어, 가용성, 기밀 유지, 개인 정보 보호에 대해서도 SOC 2 Type 2 인증을 획득했습니다. SOC 2 인증 역시 매년 갱신됩니다.

Webex Calling 의 표준 인증:

- ISO 27001: 2013
- ISO/IEC 27017: 2015
- ISO/IEC 27018: 2019
- 근거가 되는 신뢰 서비스 기준에 따라 보안, 가용성, 기밀 유지를 증명하는 SOC 2 Type II
- SOC 2 Type II 개인 정보 보호
- SOC 3

이러한 표준 준수는 강력한 운영 보안을 유지하고, 취약점 평가와 침투 테스트를 실시하며, 외부 감사 기관을 통해 년 1 회 감사를 받고, SLA 에 따라 사고 대응 시간을 준수하고 있다는 것을 의미합니다.

그 밖에도 Webex Calling 조직은 미국 보건복지부(HHS)의 보안 위험 평가 도구를 기반으로 한 HIPAA 자체 평가와 결제 카드 산업 데이터 보안 표준(PCI DSS) v3.2.1 자체 규정 준수 증명을 실시했습니다.

.

10. 투명성

시스코는 전 세계 치안 기관 및 국가 안보 기관의 고객 데이터 요청 또는 요구와 관련된 데이터를 공개하기 위해 최선을 다하고 있습니다. 이러한 데이터는 년 2 회(1~6 월 또는 7~12 월 신고) 공개됩니다. 다른 테크놀로지 기업과 마찬가지로 시스코 역시 임의 신고 기간 이후 6 개월이 지날 때마다 신고 시점의 제한 규정에 따라 이러한 데이터를 공개합니다.

자세한 내용은 cisco.com/web/about/doing_business/trust-center/transparency-report.html 에서 확인하십시오.
시스코는 개인 정보 보호 데이터 시트에 Webex Calling 서비스에서 수집되는 데이터를 비롯해 이러한 데이터의 보호 방법과 보관 기간을 명시하고 있습니다.

결론

전 세계 기업, 기관 및 정부 부처들은 중요한 비즈니스 커뮤니케이션이 있을 때마다 Webex Calling 을 이용합니다. 보안은 모든 기업과 기관에게 가장 중요한 관심사입니다. 따라서 클라우드 기반 텔리포니는 통화 연결부터 Webex App 과 Webex Meetings 서비스를 사용하는 모바일 협업 참여자에 대한 인증에 이르기까지 다양한 작업에서 보안을 계층화할 수 있어야 합니다.

Webex Calling 은 엄격한 내부 및 산업 표준을 준수하기 위해 지속적으로 관련 기관의 검증과 인증을 받는 확장식 아키텍처, 이동통신 사업자 수준의 가용성, 다계층 보안을 제공합니다. 시스코는 모든 것을 더 안전하게 연결하여 모든 일을 가능하게 만듭니다.

시스코 영업 담당자에게 연락하여 지금 Webex Calling 90 일 무료 평가판을 시작하십시오.
Webex 협업 플랫폼의 보안에 대해 자세히 알아보십시오.
Webex Meetings 보안에 대해 자세히 알아보십시오.
Webex 단일 플랫폼의 이점에 대해 자세히 알아보십시오.

추가 정보

webex.com 을 방문하십시오.

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 **https://www.cisco.com/go/offices**.

Printed in USA C11-743446-02 08/21