Web Conferencing: Unleash the Power of Secure, Real-Time Collaboration

본 백서에서는 Cisco WebEx Meeting Center, Cisco WebEx Training Center, Cisco WebEx Support Center와 Cisco WebEx Event Center의 보안 정보를 중심으로 설명합니다.

머릿말

Cisco WebEx® 온라인 솔루션은 글로벌 직원들과 팀들이 마치 한 방에서 일하는 것 처럼 가상에서 만나 실시간으로 협업할 수 있도록 해 줍니다. 실제로, 온라인 협업은 출장 시간과 비용, 회의실 공간의 제약까지 없애 기존의 대면 협업 방식을 개선할 수 있습니다. 전 세계의 기업, 기관 및 정부가 Cisco WebEx® 솔루션을 비즈니스 프로세스를 단순화하고 세일즈, 마케팅, 교육, 프로젝트 관리를 개선하고 팀을 지원하는데 필요로 하고 있습니다.

이들 회사와 기관에 보안은 근본적인 문제입니다. 온라인 협업 솔루션은 미팅 예약부터 참가자 인증, 문서 공유에 이르기까지 여러 단계의 보안을 제공해야 합니다.

Cisco는 네트워크, 플랫폼, 애플리케이션의 설계와 구축, 유지 보수에 있어서 보안을 최우선으로 합니다. 보안 요건이 아무리 엄격한 환경이라도 걱정 없이 비즈니스 프로세스에 WebEx® 솔루션을 적용할 수 있습니다.

Cisco WebEx 온라인 애플리케이션의 보안 기능과 기본 통신 인프라인 Cisco WebEx Cloud를 이해하는 것은 투자 결정에 있어 중요한 부분입니다.

The Cisco WebEx Cloud Infrastructure

Cisco WebEx Meetings는 SaaS(Software-as-a-service) 솔루션으로서, 업계 최고 수준의 성능, 통합 기능, 유연성, 확장성, 가용성을 겸비한 매우 안전한 서비스 제공 플랫폼인 Cisco WebEx Cloud를 통해 제공됩니다. Cisco WebEx Cloud는 간편한 구축 방식과 애플리케이션 제공 방식을 제공하며, 총 소유 비용을 낮추는 동시에 최고 수준의 엔터프라이즈 보안을 실현합니다.

스위치 아키텍처

Cisco는 전 세계적으로 분산된 고속 미팅 스위치의 전용 네트워크를 구축합니다. 발표자의 컴퓨터에서 전송되어 참석자의 컴퓨터에 수신되는 미팅 세션 데이터는 Cisco WebEx Cloud를 통해 스위칭되고 절대로 영구 저장되지 않습니다.[1]

[1] 사용자가 NBR(network-based recording)을 활성화하면 미팅이 녹화되고 저장됩니다. WebEx는 NBR 외에 사용자 프로필 데이터와 사용자 파일도 저장합니다.

데이터 센터

Cisco WebEx Cloud는 실시간 웹 커뮤니케이션을 위해 특별히 제작된 커뮤니케이션 인프라입니다. WebEx 미팅 세션에는 전 세계의 여러 데이터 센터에 위치한 스위칭 장비가 사용됩니다. 이 데이터 센터는 주요 **인터넷** 액세스 포인트에 전략적으로 배치되어 있으며, 전 세계에 트래픽을 라우팅하는 데 전용 고대역폭 파이버를 사용합니다. Cisco는 Cisco WebEx Cloud 내에서 전체 인프라를 운영합니다. 따라서 미국 내의 데이터는 미국 지역을 벗어나지 않고 유럽의 데이터는 유럽 지역을 벗어나지 않습니다.

또한 Cisco는 네트워크 PoP(point-of-presence) 지점을 운영합니다. 이 지점은 엔드 유저 성능과 가용성을 높이기 위해 사용되는 백본 연결, 인터넷 피어링, 글로벌 사이트 백업 및 캐싱 기술을 지원합니다. Cisco 담당자가 매일 24 시간, 연중무휴로 물류 보안, 운영 및 변경 관리와 관련한 지원을 제공합니다.

철정한 보안을 갖춘 WebEx Meeting Experience 개요

WebEx 미팅 환경은 다음을 포괄적으로 지원합니다.

- 미팅 사이트 컨피그레이션
- 예약할 때 보안 옵션
- WebEx 미팅 시작 및 참가 옵션
- 암호화 기술
- TLS(Transport Layer Security)
- 방화벽 호환성
- 미팅 데이터 프라이버시
- 미팅 중 보안
- SSO(Single Sign-On)
- 서드파티 인증(외부 감사를 통한 Cisco WebEx 보안 검증)

"WebEx 미팅"과 "Cisco WebEx 미팅 세션"이라는 용어는 모든 Cisco WebEx 온라인 제품에 사용되는 통합 오디오 회의, 인터넷 음성 회의, 싱글 및 멀티 포인트 비디오 회의를 지칭합니다. 여기에는 다음의 제품이 포함됩니다.

- Cisco WebEx Meeting Center
- Cisco WebEx Training Center
- Cisco WebEx Event Center
- Cisco WebEx Support Center(Cisco WebEx Remote Support 및 Cisco WebEx Remote Access 포함)

별도로 명시되지 않은 한, 이 문서에서 설명하는 보안 기능은 위에 언급한 모든 WebEx 애플리케이션에 동일하게 적용됩니다.

WebEx 미팅 역할

WebEx 미팅에는 호스트, 대체 호스트, 발표자, 참석자의 네 가지 역할이 있습니다. 다음 섹션에서는 각 역할의 보안 권한을 설명합니다.

호스트

호스트는 WebEx 미팅을 예약하고 시작합니다. 호스트는 미팅 중 환경을 제어합니다. 보안 상의 관점에서 호스트는 참석자에게 발표자 권한을 부여할 수 있습니다. 호스트는 미팅에 로크를 걸고 참석자를 퇴출할 수 있습니다.

대체 호스트

호스트는 본인을 대신해 예약된 WebEx 미팅을 시작할 수 있는 대체 호스트를 지명합니다. 보안 상의 관점에서 대체 호스트는 호스트와 동일한 권한을 갖습니다.

발표자

발표자는 프레젠테이션, 특정 애플리케이션 또는 전체 데스크톱을 공유합니다. 발표자는 주석 툴을 제어합니다. 보안 상의 관점에서 발표자는 개별 참석자에게 공유 애플리케이션과 데스크톱을 통해 원격 제어 권한을 부여하고 철회할 수 있습니다.

참석자

참석자는 보안과 관련한 책임이나 권한이 없습니다.

WebEx 사이트 관리 모듈

인증된 관리자는 WebEx 사이트 관리 모듈을 통해 미팅 별로 호스트와 발표자의 권한에 대한 보안 정책을 관리하고 적용할 수 있습니다. 예를 들어, 사이트 별 또는 사용자 별로 발표자가 애플리케이션을 공유하거나 파일을 전송하지 못하도록 세션 구성을 맞춤화할 수 있습니다.

WebEx 사이트 관리 모듈에서 다음의 보안 관련 기능을 관리합니다.

어카운트 관리

- 구성 가능한 시도 횟수만큼 로그인에 실패할 경우 계정 차단
- 지정한 시간 경과 후 잠긴 계정을 자동으로 잠금 해제
- 정해진 기간 동안 사용하지 않을 경우 계정 비활성화

특정 사용자 계정 작업

- 다음 로그인 시에 사용자가 암호를 변경하도록 요구
- 사용자 계정 잠금 또는 잠금 해제
- 사용자 계정 활성화 또는 비활성화

계정 생성

- 신규 계정 요청 시 보안 텍스트 입력 요구
- 신규 계정 확인 이메일 요구
- 신규 계정 셀프 등록(가입) 허용
- 신규 계정 셀프 등록에 관한 규칙 구성

계정 암호

다음과 같은 강력한 암호 요건 적용:

- 대/소문자 혼합
- 최소 길이
- 최소 숫자 개수
- 최소 알파벳 문자 개수

- 최소 특수 문자 개수
- 같은 문자를 3 회 이상 반복할 수 없음
- 이전에 사용한 암호를 지정된 횟수 이상 재사용할 수 없음
- 동적 텍스트(사이트 이름, 호스트 이름, 사용자 이름) 사용 불가
- 구성 가능한 목록의 항목을 암호로 사용하지 못하도록 제한(예: "password")
- 암호를 변경할 수 있는 최소 간격
- 구성 가능한 시간 간격으로 호스트가 계정 암호 변경
- 다음 로그인 시에 모든 사용자가 암호 변경

개인 미팅 룸

개인 미팅 룸(Personal Meeting Rooms)은 개별화된 URL과 암호를 사용하여 액세스할 수 있습니다. 이 미팅 룸에서는 호스트가 예약된 미팅과 진행 중인 미팅의 목록을 표시하고, 미팅을 시작 및 참가하고, 미팅 참석자들과 파일을 공유할 수 있습니다. 관리자는 다음과 같이 개인 미팅 룸의 보안과 관련한 기능을 설정할 수 있습니다.

- 개인 미팅 룸에서 파일을 공유할 때의 옵션
- 개인 미팅 룸에서 공유하는 파일의 암호 요건

WebEx 사이트 관리를 통해 지원되는 기타 보안 관련 기능

- 호스트 또는 참석자는 새 미팅을 손쉽게 구성하거나 참가할 수 있도록 이름과 이메일 주소를 저장할 수 있습니다.
- 호스트는 녹화 기능을 다른 호스트에게 재지정할 수 있습니다.
- 모든 호스트 및 참석자 액세스에 대해 인증을 요구하여 사이트 액세스를 제한할 수 있습니다. 목록에 있는 미팅 등의 사이트 정보에 액세스하거나 사이트의 미팅에 액세스하려면 인증이 필요할 수 있습니다.
- WebEx Access Anywhere에 강력한 암호 규칙이 적용될 수 있습니다.
- 모든 미팅은 목록에서 제외할 수 있습니다.
- "Forgot Password?(암호 찾기)" 요청에 승인이 필요할 수 있습니다.
- 계정 암호를 사용자 대신 재입력하는 것이 아니라 재설정해야 할 수 있습니다.

WebEx 미팅 예약의 보안 옵션

- 개별 호스트에게 미팅 액세스 보안을 지정할 권한을 부여할 수 있습니다(사이트 관리 레벨에 구성된 재지정할 수 없는 한계 내에서).
- 달력에 표시되지 않도록 미팅을 목록에서 제외할 수 있습니다.
- 호스트가 참가하기 전에 참석자가 먼저 미팅에 참석하도록 허용할 수 있습니다.
- 호스트가 참가하기 전에 참석자가 먼저 오디오에 액세스할 수 있습니다.
- WebEx 사이트의 계정이 있는 참석자만 참가할 수 있습니다.
- 다자간 전화회의 정보를 미팅에서 표시할 수 있습니다.
- 참석자가 한 명밖에 남지 않은 경우 일정 시간 후에 미팅을 자동으로 끝내도록 구성할 수 있습니다.
- 참석자가 미팅에 참가할 때 이메일 주소를 입력하도록 요구할 수 있습니다.

목록에 있는 미팅 또는 목록에 없는 미팅

호스트는 사용자 정의된 WebEx 사이트의 공개 미팅 달력에 미팅을 표시하도록 선택할 수 있습니다. 또는 목록에 없는 미팅으로 예약하여 미팅 달력에 표시되지 않게 할 수도 있습니다. 목록에 없는 미팅의 경우 이메일 초대 프로세스를 통해 참석자에게 링크를 보내거나 참석자가 Join Meeting(미팅 참가) 페이지에서 미팅 번호를 입력하도록 요구하여 참석자에게 미팅이 있다는 사실을 명시적으로 알려야 합니다.

내부 또는 외부 미팅

호스트는 참석자가 미팅 참가 시에 로그인하도록 함으로써 사용자 정의된 WebEx 사이트의 계정이 있는 사람만 미팅에 참가할 수 있게 제한할 수 있습니다.

미팅 암호

호스트는 미팅 암호를 설정한 후 미팅 초대 이메일에 암호를 포함하거나 제외하도록 선택할 수 있습니다.

등록

- 호스트는 등록 기능을 사용하여 미팅 액세스를 제한할 수 있습니다. 호스트는 본인이 등록하고 명시적으로 승인하여 초대한 사람만 허용하는 "ACL(Access Control List)"을 생성할 수 있습니다.
- WebEx Training Center와 WebEx Event Center에서 등록 ID의 재사용을 차단하여 미팅의 보안을 강화할 수 있습니다. 이미 사용 중인 등록 ID를 재사용하려 하는 참석자는 미팅 참가가 차단됩니다. 이것은 여러 참석자 간에 ID 공유를 방지하기 위한 것입니다.
- 또한 호스트는 액세스를 제어하고 참가자를 퇴출하여 미팅 보안을 유지할 수 있습니다.

이러한 예약 옵션은 보안 정책에 맞게 어떤 조합으로든 세부 설정할 수 있습니다.

WebEx 미팅 시작 및 참가

WebEx 미팅은 WebEx 사이트에서 호스트의 사용자 ID 및 암호가 인증된 후에 시작됩니다. 호스트는 최초 발표자로서 처음에 미팅을 제어하게 됩니다. 호스트는 어떤 참석자에게든 호스트 또는 발표자 권한을 부여/철회하거나 선택한 참석자를 퇴출하거나 언제든지 세션을 종료할 수 있습니다.

호스트는 본인이 참석할 수 없거나 미팅 연결이 끊긴 경우에 미팅을 시작하고 제어할 대체 호스트를 지명할 수 있습니다. 이 기능은 호스트 역할이 예기치 않게 인증되지 않은 참석자에게 할당될 가능성을 없애 미팅의 보안을 유지해 줍니다.

사용자 정의된 WebEx 사이트를 구성하여 참석자가 호스트보다 먼저 오디오 부분을 포함한 미팅에 참가하도록 허용하고 조기 참가자들이 채팅과 오디오만 사용할 수 있도록 기능을 제한할 수 있습니다.

참석자가 처음으로 WebEx 미팅에 참가하면 WebEx 클라이언트 소프트웨어가 자동으로 다운로드되어 참석자의 컴퓨터에 설치됩니다. WebEx 클라이언트 소프트웨어는 VeriSign에서 발급한 인증서를 사용하여 디지털 서명됩니다. 이후 미팅에서 WebEx 애플리케이션은 변경 사항 또는 업데이트가 포함된 파일만 다운로드하여 설치합니다. 참석자는 컴퓨터의 운영 체제에서 제공되는 설치 제거 기능으로 WebEx 파일을 손쉽게 제거할 수 있습니다.

암호화 기술

WebEx 미팅은 WebEx 미팅 세션 내에서 각 참석자에게 실시간 리치 미디어 콘텐츠를 안전하게 제공하도록 설계되었습니다. 발표자가 공유하는 문서나 프레젠테이션은 데이터를 공유하는 데 최적화하는 Cisco® 독점 기술인 UCF(범용 통신 형식)로 인코딩됩니다. iPad, iPhone, BlackBerry 등의 모바일 디바이스에 설치된 WebEx 미팅 애플리케이션은 PC 클라이언트와 유사한 암호화 메커니즘을 사용합니다.

WebEx 미팅은 다음과 같은 암호화 메커니즘을 제공합니다.

- PC와 모바일 디바이스의 WebEx 미팅에서는 128 비트 SSL(Secure Sockets Layer)을 사용하여 클라이언트에서 Cisco WebEx Cloud로 데이터가 전송됩니다.
- 엔드 투 엔드 암호화는 Cisco WebEx Meeting Center에 제공되는 옵션입니다. 이 방식은 호스트의 컴퓨터에서 무작위로 생성되어 공용 키 기반 메커니즘을 통해 참석자들에게 배포되는 256 비트 키를 사용한 AES(Advanced Encryption Standard)를 기반으로 미팅 참가자들 간에 모든 미팅 콘텐츠를 엔드 투 엔드로 암호화합니다. Cisco WebEx Cloud 측에서 종료되는 SSL 암호화 방식과 달리, E2E 암호화는 Cisco WebEx Cloud 인프라 내에서 모든 미팅 콘텐츠를 암호화합니다. 일반 텍스트 미팅 콘텐츠 데이터는 미팅 참가자의 컴퓨터 메모리에서만 표시됩니다.[2]
- 사용자가 관련 "Remember me(내 정보 저장)" 옵션을 선택한 경우 PC와 모바일 디바이스에 저장되는 해당 사용자의 WebEx 미팅 로그인 ID와 암호가 128 비트 AES를 사용하여 암호화됩니다.

사이트 관리자와 호스트는 "Meeting type(미팅 종류)" 옵션을 사용하여 E2E 암호화를 선택할 수 있습니다. E2E 솔루션을 사용하면 키가 미팅 호스트와 참석자에게만 공개되므로 AES를 사용할 때보다 보안이 강화됩니다(단, E2E 암호화에서도 페이로드 암호화에 AES 사용).

WebEx 미팅 클라이언트에서 WebEx Cloud로의 모든 연결은 암호화 토큰을 사용하여 인증되므로 허용된 사용자만 해당 미팅에 참가할 수 있습니다.

TLS(Transport Layer Security)

애플리케이션 레이어 보안에 더해, 모든 미팅 데이터는 128 비트 SSL을 사용하여 전송됩니다. SSL은 표준 HTTP 인터넷 트래픽에 사용되는 방화벽 포트 80 대신 HTTPS 트래픽에 사용되는 방화벽 포트 443 을 통해 방화벽을 통과합니다.

WebEx 미팅 참석자는 애플리케이션/프레젠테이션/세션 레이어에서 논리적 연결을 사용하여 Cisco WebEx Cloud에 연결됩니다. 참석자의 컴퓨터 간에 P2P 연결은 없습니다.

방화벽 호환성

WebEx 미팅 애플리케이션은 Cisco WebEx Cloud와 통신하면서 HTTPS(포트 443)를 사용하여 신뢰성이 높고 고도의 보안이 적용되는 연결을 설정합니다. 따라서 방화벽을 별도로 구성하지 않아도 WebEx 미팅이 가능합니다.

미팅 데이터 프라이버시

모든 WebEx 미팅 콘텐츠(채팅, 오디오, 비디오, 데스크톱 또는 문서 공유)는 일시적입니다(미팅이 진행되는 동안에만 존재). 미팅 콘텐츠는 Cisco 클라우드 또는 참석자의 컴퓨터에 기본적으로 저장되지 않습니다. Cisco는 두 가지 미팅 정보만 보존합니다. 보존되는 정보는 다음과 같습니다.

[2] E2E 암호화를 사용하는 경우 NBR을 사용할 수 없습니다. 이 옵션은 WebEx Meeting Center에서만 사용할 수 있습니다.

- **EDR(Event detail records):** Cisco는 요금 청구와 보고에 EDR을 사용합니다. 사용자 정의된 WebEx에 호스트 ID를 사용하여 로그인하면 이벤트 세부 정보를 확인할 수 있습니다. 인증되면 이 데이터를 WebEx 사이트에서 다운로드하거나 WebEx API를 통해 액세스할 수도 있습니다. EDR에는 미팅(미팅 ID)에 누가(사용자 이름 및 이메일) 언제(참가 및 퇴장 시간) 참가하는지를 비롯한 기본 미팅 참석 정보가 포함되어 있습니다.
- **NBR(Network-based recording) 파일:** 호스트가 WebEx 미팅 세션을 녹화하도록 선택한 경우 녹화 파일이 Cisco WebEx Cloud에 저장되어 사용자 정의된 WebEx 사이트의 MyRecordings 영역에서 액세스할 수 있습니다. 이 파일은 호스트가 미팅 중에 NBR을 활성화하거나 모든 미팅을 녹화하는 사이트 전체 옵션을 선택한 경우에만 생성됩니다. NBR은 URL 링크를 통해 액세스할 수 있습니다. 각 링크에는 예측 불가능한 토큰이 포함되어 있습니다. 호스트는 파일을 삭제하거나 공유하거나 암호를 추가하여 보호하는 등 NBR 파일에 대한 액세스를 완벽하게 제어할 수 있습니다. NBR 기능은 선택 사항이며 관리자가 해제할 수 있습니다.

SSO(Single Sign-On)

Cisco는 SAML(Security Assertion Markup Language) 1.1 및 2.0 프로토콜과 WS-Federation 1.0 프로토콜을 사용하여 사용자 SSO(Single Sign-On)를 위한 통합 인증을 지원합니다. SAML 1.1 에 대한 지원은 단계적으로 중단됩니다. 통합 인증을 사용하려면 공용 키 X.509 인증서를 사용자 정의된 WebEx 사이트에 업로드해야 합니다. 그러면 사용자 특성이 포함된 SAML Assertion을 생성하고 일치하는 개인 키로 Assertion을 디지털 서명할 수 있습니다. WebEx는 사용자를 인증하기 전에 사전 로드된 공용 키 인증서와 대조해 SAML Assertion 시그니처를 확인합니다.

서드파티 보고

WebEx Office of Security는 자체적으로 철저한 내부 절차를 거치는 것은 물론, 독립된 여러 서드파티를 통해 Cisco 내부 정책, 절차 및 애플리케이션에 대해 엄격한 감사를 실시합니다. 이러한 감사는 상용 애플리케이션과 정부용 애플리케이션의 미션 클리티컬 보안 요구 사항을 검증하도록 만들어졌습니다.

서드파티 보안 평가

Cisco는 서드파티 공급업체를 통해 지속적이고 심층적인 코드 기반 침입 테스트와 서비스 평가를 실시합니다. 그 과정의 일환으로 서드파티는 다음과 같은 보안 평가를 수행합니다.

- 중요 애플리케이션 및/또는 서비스 취약성 파악과 솔루션 제안
- 아키텍처 개선을 위한 일반적인 영역의 권장 사항 제시
- 코딩 오류 파악 및 코딩 방식 개선을 위한 지침 제공
- WebEx 엔지니어링 담당자와 직접 협력하면서 평가 결과를 설명하고 해결 작업을 위한 지침 제공

Safe Harbor 인증

2012 년 3 월에 Cisco는 고객 및 파트너 데이터에 대한 Safe Harbor 인증을 획득했습니다(직원 데이터에 대한 Safe Harbor 인증은 2011 년에 획득). 이 인증은 Cisco의 포괄적인 프라이버시 규정준수 프로그램의 추가적인 요소로서, 정부나 표준 위원회의 요건은 아니지만 Cisco는 고객이 이 인증을 얼마나 중요하게 여기는지를 잘 알고 있습니다.

EU 데이터 보호법에서는 유럽 각국 국민의 개인 데이터를 EU의 프라이버시 보호 "적합성" 표준을 충족하지 않는 EU 이외의 국가로 전송하는 것을 금지하고 있습니다. 미 상무부는 EC(European Commission, 유럽연합)와 보조를 맞춰 미국의 조직이 Safe Harbor 프라이버시 원칙을 따름으로써 이 법률을 준수할 수 있도록 Safe Harbor 프레임워크를 개발했습니다. 회사에서는 미 상무부 웹 사이트에서 이 원칙의 준수 여부를 인증 받습니다. 이 프레임워크는 2000 년에 EU의 승인을 받아, 회사들이 이 원칙을 준수할 경우 EU에서 EU 국민의 프라이버시를 보호할 "적합성"을 갖춘 것으로 간주되도록 보장하고 있습니다.

SSAE16

PricewaterhouseCoopers는 매년 American Institute of Certified Public Accountants에서 정한 표준에 따라 SSAE16(Statement on Standards for Attestation Engagements No. 16) 감사를 실시합니다. SSAE16 에 대한 자세한 내용은 http://www.ssae16.com을 참조하십시오.

ISO 27001 및 27002

Cisco는 2012 년 10 월에 WebEx 서비스에 대해 ISO 27001 인증을 받았습니다. 인증은 3 년마다 갱신되며 매년 중간 외부 감사를 받습니다. ISO 27001 은 ISO(International Organization for Standardization, 국제표준화기구)에서 제정한 정보 보안 표준으로, ISMS(Information-Security Management System, 정보보안관리시스템) 구축과 관련한 모범 사례 권장 사항을 제공합니다. ISMS는 조직의 정보 위험 관리 프로세스와 관련한 법률과 관리상의 모든 물리적/기술적 통제를 아우르는 정책과 절차의 프레임워크입니다. 설명서에 따르면 ISO 27001 은 "정보 보안 관리 시스템을 구축, 구현, 운영, 모니터링, 검토, 유지 관리 및 개선하기 위한 모델을 제공"하기 위해 개발되었습니다. ISO 27001 및 27002 에 대한 자세한 내용은 http://www.27000.org/를 참조하십시오.

추가 정보

Cisco WebEx 솔루션에 대한 자세한 내용은 www.cisco.com/web/KR/products/pc/webex/index.html을 참조하거나 세일즈 담당자에게 문의하십시오.

미주 본부
Cisco Systems, Inc.
캘리포니아, 새너제이

아시아 태평양 본부
Cisco Systems (USA) Pte. Ltd.
싱가포르

유럽 본부
Cisco Systems International BV Amsterdam.
네덜란드

Cisco는 전 세계에 200개가 넘는 지역 사무소를 보유하고 있습니다. 각 사무소의 주소, 전화번호, 팩스 번호는 Cisco 웹사이트 www.cisco.com/go/offices에서 검색할 수 있습니다.

Printed in USA C11-709579-01 04/14