인프라 보안 개요

Cisco IronPort® Cloud Email Security에서는 최고의 기술을 결합하여 현재 가장 확장성이 뛰어나고 정교한 이메일 보호 기능을 제공합니다. Fortune 1000대 기업의 40%를 인바운드 및 아웃바운드 이메일 위협으로부터 보호하는 업계 최고의 기술을 기반으로 하는 Cisco IronPort Cloud Email Security를 사용하는 고객은 온사이트 데이터 센터 설치 공간을 절약하고 이메일 보안 관리 작업을 신뢰할 수 있는 보안 전문가에게 위임할 수 있습니다. 이 솔루션은 최고 레벨의 서비스 가용성과 데이터 보호 기능을 유지할 수 있도록 복원력이 뛰어난 여러 데이터 센터의 전용 이메일 보안 인스턴스를 제공합니다. Cisco IronPort Email Security 솔루션은 물리적 액세스와 논리적 액세스 측면 둘 다에서 최고 레벨의 클라우드 인프라 보안과 가용성을 제공합니다. 이 디자인에는 데이터 센터 건물에 대한 액세스 제어, 고객 데이터 액세스를 보호하는 프로세스, 하드웨어 인프라 가용성 등의 측면이 포함됩니다. 그림 1에는 이러한 측면이 중점적으로 나와 있습니다.

물리적 보안

보안 인프라를 항상 안전하게 유지하기 위한 기반이 되는 요소는 데이터 센터의 물리적 보안입니다. 최고 레벨의 물리적 인프라 보안을 제공하는 보안 담당자가 관리하는 최신 감시 시스템을 통해 데이터 센터 보안이 지원됩니다. 여기에는 다음 항목이 포함됩니다.

1. **감시 시스템**

   Cisco는 온사이트 관리 담당자를 배치할 뿐 아니라 디지털 비디오 시스템을 통한 자동화된 감시 인터페이스도 제공합니다. 모든 고정 카메라는 0.01lux까지 확인이 가능한 자동 저조도 스위칭 기능이 포함된 고해상도 컬러 카메라입니다. 외부 및 민감한 구역에서는 PTZ(Pan-tilt-zoom) 카메라가 사용됩니다. 모든 PTZ는 현재 고정 카메라 위치로 즉시 재배치할 수 있도록 "UTC(up-the-coax)" 프로토콜을 사용합니다.

   비디오는 동작 시 15IPS/운영자 명령 시 30IPS로 720x240픽셀에서 녹화됩니다. 대부분의 비디오 채널에서는 오디오도 동시에 녹음합니다. 비디오는 약 100일 동안 보관됩니다. 데이터 센터에서는 IOU(식별, 관찰 및 인지) 방법을 사용해 카메라 시스템을 작동하는 상주 관리자와 함께 활성 감시 시스템을 구축합니다. 이처럼 IOU가 사용되므로 모니터를 보다 자세히 확인할 수 있으며, 조사를 위한 뛰어난 품질의 비디오 녹화물이 제공됩니다. 중역 팀원은 PDA 및 VPN 노트북 컴퓨터 액세스를 통해 비디오에 원격으로 액세스할 수 있습니다. 모든 비디오는 최소 90일 동안 M-JPEG 형식으로 보관됩니다.

2. **액세스 제어/침입 탐지**

   모든 입구를 연중 무휴로 중앙에서 모니터링합니다. 외부 출입문의 경우 추가로 보호할 수 있도록 설계 및 설치됩니다. 즉, 추가 보호 기능인 탐지 디바이스 및 액세스 제어 기능이 외부 출입문에 적용되며 고정 카메라를 통해 외부 출입문을 독립적으로 확인할 수 있습니다. 외부 액세스 포인트는 최소한으로 유지되며 대부분의 경우에는 각 시설에서 문 하나만 출입용으로 사용할 수 있습니다. 이러한 문에는 12게이지 스테인리스 스틸로 제작되며 ¼인치 알루미늄으로 코팅된 특수 제작 맨트랩 장치가 부착됩니다. 맨트랩 장치가 없는 모든 액세스 포인트의 경우 카드 소유자가 추가로 생체 인증을 해야 하며 맨트랩 릴레이 논리를 입력해야 합니다. 또한 맨트랩에는 하나 이상의 고정 카메라와 공간 오디오 감시 장치가 장착됩니다.

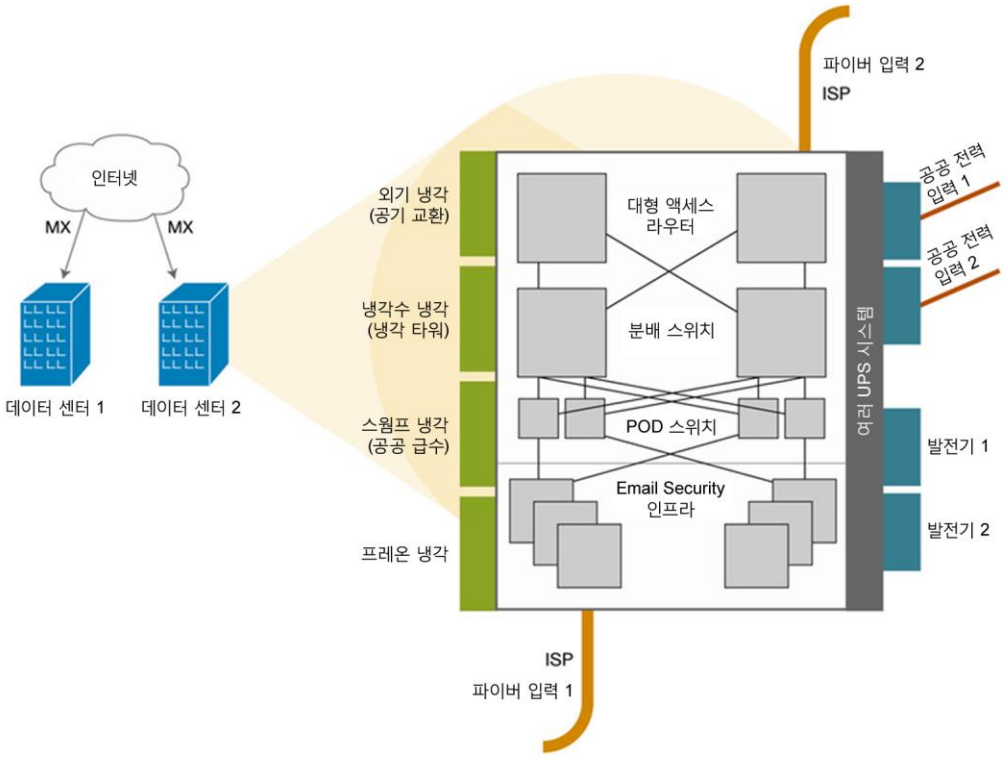
데이터 센터 업타임

그림 2에서는 Cisco IronPort Cloud Email Security 솔루션의 아키텍처를 설명합니다. 이 솔루션의 주요 특징은 다음과 같습니다.

1. 재해 복구를 위해 여러 위치에 분산된 데이터 센터
2. SAS 70 유형 II 인증 데이터 센터
3. 각 데이터 센터 내의 네트워크 연결, 전원, 냉각 및 대역폭 이중화
4. 최대 20Gbps의 네트워크 트래픽을 처리할 수 있는 대역폭

Cisco IronPort Cloud Email Security에는 여러 SAS 70 유형 II 데이터 센터가 액티브-액티브 구축 아키텍처로 포함되어 있습니다. 이 솔루션은 여러 MX 레코드가 이러한 데이터 센터를 가리키도록 지정하여 데이터 센터 중 하나에서 예상치 않은 재해가 발생하더라도 이메일을 계속 사용할 수 있도록 합니다. 이처럼 여러 데이터 센터가 포함된 아키텍처를 통해 Cisco IronPort Cloud Email Security 서비스의 가용성을 최고 레벨로 유지할 수 있습니다.

그림 1. Cisco IronPort Cloud Email Security 데이터 센터 아키텍처



Cisco의 각 데이터 센터 인프라에서는 여러 레벨의 이중화가 기본적으로 제공됩니다. 첫째로, 네트워크 인프라에는 여러 캐리어급 액세스 라우터, 분산 스위치, PoD 스위치(포트 100~1,000개 사이의 대규모 이더넷 스위치)가 포함되어 있으므로 단일 장애 포인트가 없습니다. 이 솔루션은 이처럼 고도로 이중화된 네트워킹 인프라에서 여러 개의 전용 Cisco IronPort 이메일 보안 인스턴스를 메일 처리, 보고, 추적 등에 사용합니다. 장애를 방지하고 입력 중 하나에 영향을 주는 예기치 않은 사고 발생 시에도 연결을 유지하기 위해 데이터 센터에서는 물리적으로 분리된 두 파이버 입력을 사용합니다. 또한 이들 데이터 센터는 최대 20Gbps의 네트워크 트래픽을 처리할 수 있는 대역폭 용량을 보유하고 있습니다.

오늘날의 대다수 데이터 센터는 장비의 발열을 부적절하게 관리하고 제어하는 경우에 발생하는 심각한 문제를 해결할 수 있어야 합니다. Cisco IronPort 데이터 센터는 업계의 최고급 공간 및 전원 디자인을 사용하여 구축되었습니다. 따라서 1차 전원 회로 및 장애 조치 전원 연결을 포함하는 정교한 그리드 아키텍처를 통해 전원 가용성 100%를 제공합니다. 1차 전원 회로와 장애 조치 연결은 모두 완전히 분리된 N+2 전원 시스템에서 제공됩니다. 이러한 각 시스템에는 별도의 UPS 배터리, 발전기, PDU 및 RPP가 포함되어 있습니다. 색이 구분된 콘센트를 꽂는 방식으로 각 랙에 전원이 공급됩니다. 따라서 시스템에 연결되는 이메일 보안 인스턴스의 일정한 업타임이 유지됩니다.

서버의 집적도가 높아짐에 따라 냉각 시스템 수요도 크게 증가했습니다. 각 Cisco IronPort 데이터 센터 시설에는 이메일 보안 인스턴스에서 생성되는 열을 적절하게 없앨 수 있는 충분한 1차 및 백업 냉각 기능이 포함되어 있으며, 냉각 시스템 중 하나에 장애가 발생하더라도 충분한 백업 냉각을 사용할 수 있습니다. 냉각 인프라는 프레온, 스웜프, 냉각수 및 외기 메커니즘을 통해 제공됩니다.

표 1과 2에는 데이터 센터 전원 공급을 위한 인프라 작동 사양이 나와 있습니다.

표 1. 전원 사양

랙당 전력 및 냉각 17kW	UPS 백업 전원
End-of-Sale 날짜	120/208VAC 및 –48 VDC 사용 가능
100% 발전기 백업	48VDC 배터리 플랜트
1~2MW 발전기 여러 개에 해당하는 발전기 용량	1,200A->10,000A로 확장 가능
연료 탱크 크기: 1,000~2,000갤런	배터리 비축량 2시간(비이중화)/4시간(이중화)
발전기 자동 시작/자동 전송 자동 전송 스위치의 격리 우회 기능	실제 A/B 급전
실행 시간 최소 24시간에 해당하는 연료 용량	NFPA 70에 따른 접지
2시간 이내에 연료 배달	

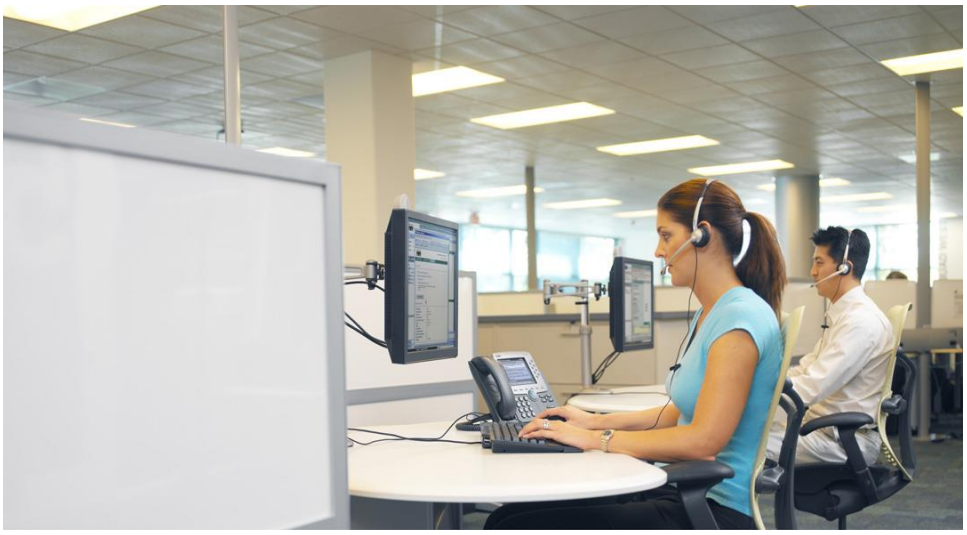
표 2. 환경 제어

컴퓨터실급 장비에서 제공하는 언더플로어 냉각 기능	평방 피트당 시간별 냉각 200Btu 이상(N+1 이중화)
ASHRAE 1%에서 온도 22.2℃(72°F) 유지(건구)	전원 공급 중단 시 HVAC 시스템과 전체 시설이 디젤 발전기를 사용하여 작동함
습도 30%~60%(비응축). 적외선 가습기를 통해 ATS Liebert 단위로 습도 조절	

Security Operations Center

Cisco SOC(Security Operations Center)는 Cisco ROS(Remote Operations Services)에 의해 운영됩니다. Cisco ROS는 세계 최고 레벨의 보안 감시를 유지하기 위해 직원, 프로세스 및 툴의 지속적인 관리 및 내부 감사를 구현합니다. 따라서 Cisco 고객은 안심하고 네트워크를 사용할 수 있으며 보안 서비스 제공 표준이 최고 레벨로 유지됩니다.

그림 2. Cisco Security Operations Center Help Desk



1. 네트워크 보안

Cisco SOC는 단일 심층 방어 설계 내에서 추가적인 보안 디바이스 및 애플리케이션 조합을 사용합니다. 추가 레이어에는 Cisco ROS에 대한 인바운드 액세스를 제어하는 여러 방화벽이 포함됩니다. 이러한 전략으로 인해 사용자는 목적에 합당한 정보에만 액세스할 수 있습니다(최소 권한).

센서로 작동하는 침입 방지 시스템이 네트워크 전반에 걸쳐 전략적으로 배치되어 트래픽을 모니터링하고 보안 이벤트를 탐지합니다. 탐지된 이벤트는 Cisco Security Management Service를 통해 관리됩니다. 네트워크 내의 여러 포인트에서 사용되는 침입 탐지 기능은 서비스 제공 네트워크와 고객 네트워크 간의 트래픽에서 의심스럽거나 악의적인 패턴을 모니터링합니다.

보안 이벤트 관리자는 서비스 제공 네트워크 전반에서 사용되는 보안 디바이스의 이벤트 및 위협 상관관계를 제공합니다. 또한 디지털 인증서를 사용하여 내부와 외부에서 모두 액세스해야 하는 고객 웹 포털 및 시스템에 대한 액세스를 보호합니다.

2. 시스템 보안

Cisco ROS는 여러 가지 제어 기능을 사용하여 관리되는 시스템의 보안을 유지합니다. 여기에는 물리적 제어 기능과 취약성 탐지 스캔이 모두 포함됩니다.

- 물리적 제어

  Cisco는 건물 내에서 눈에 잘 띄도록 착용해야 하는 사진 부착 신분증을 모든 직원과 하청업체에 제공합니다. 모든 방문자는 방문자 배지를 받아야 하며 건물 내에서 직원의 안내를 받아야 합니다.

  기업 내부 공간에서만 제어되는 데이터 센터 및 배선실 입구에 액세스할 수 있습니다. 업무상의 요구에 따라 액세스 권한이 부여됩니다. 기업 공간 역시 제어되므로 적절한 배지가 있어야 진입이 가능합니다.

  각 건물의 입구에는 비디오 카메라가 있으며, Security Facilities Operation Center에서 입구를 24시간 내내 모니터링하고 관리합니다.

  시설의 1차 전원은 해당 지역의 공공 전력 사업자가 제공합니다. 그리고 대기 UPS 시스템 및 발전기를 통해 중요 영역에 백업 전원을 제공합니다. 백업 전원 시스템에 대한 정기 점검 및 테스트가 진행됩니다. 사고 예방을 위한 유지 보수는 분기별로 수행되고 전체 테스트는 매년 진행됩니다.

- 취약성 스캔

  Cisco ROS 서비스 제공 네트워크를 정기적으로 스캔하여 위험 및 취약성을 평가합니다. 이러한 평가의 결과는 필요한 치료를 수행하기 위한 IT 사고 케이스를 생성하는 데 사용됩니다.

3. 인적 제어

정보 보안과 정보 자산/지적 재산 보호는 사용자의 인식 및 교육에서 시작됩니다. 보안을 중요시하는 분위기를 적절하게 조성하고 유지하는 조직은 모든 직원에게 보안 유지 책임이 있음을 인지하고 있습니다.

Cisco에서는 중역 팀이 회사 이니셔티브 및 업무상의 행동 강령에 보안 항목을 포함했으며, 직원들도 일상적인 업무 활동에서 보안 유지를 생활화하고 있습니다. 조직 전체의 직원들이 보안 인식의 중요성에 대한 교육을 받고 있으며, 모든 직원은 회사와 파트너 및 고객의 보안을 유지한다는 공통의 목표를 달성하기 위해 함께 노력하고 있습니다.

인적 제어는 데이터 센터 보안의 중요한 측면으로 자리잡고 있습니다. 인적 제어를 통해 통신 사업자 기업 내에서 발생할 수 있는 보안 위협으로부터 고객 데이터를 보호하는 것이 목표입니다. Cisco ROS에는 고객 데이터 보안을 유지하는 데 사용할 수 있는 다양한 제어 기능이 있습니다. Cisco는 정규직/계약직 직원 채용 과정의 일환으로 신원 조사를 진행합니다. 업무 내용 설명에는 Cisco ROS 내의 역할과 책임이 요약되어 있으며, 고객 네트워크 및 정보에 적절한 방식으로 액세스할 수 있도록 최소 권한 규칙이 적용됩니다.

Cisco ROS에서 사용하는 추가적인 인적 제어는 다음과 같습니다.

- 감사 및 테스트

  Cisco ROS는 5단계 프로세스를 통해 네트워크 기반 위협에 대한 노출을 완화합니다. 이 프로세스에서는 정의된 보안 정책을 설정하고, 규정 준수를 평가하고, 정책 위반을 모니터링하고, 노출 범위를 최소화하기 위해 정기적으로 정책을 테스트합니다. 그리고 마지막 단계에서는 식별된 모든 위협과 노출 영역을 정기적으로 확인하여 네트워크의 전반적인 보안을 개선합니다.

- 변경 제어

  변경 제어는 모든 IT 환경 및 서비스 제공 팀을 운영하는 데 있어서 중요한 요소입니다. Cisco ROS가 수행하는 변경 제어에서는 고객과 협력하여 고객 환경 내의 모든 변경을 요청/예약/구현/검증하기 위한 적절한 권한 부여 과정을 설정합니다.

결론

Cisco IronPort Cloud Email Security는 현재 사용 가능한 최고의 물리적, 유틸리티 및 데이터 이중화를 동시에 유지하는 최신 데이터 센터를 통해 지원됩니다. 또한 Cisco Security Operations Center의 지원을 통해 추가적인 보안 레이어를 제공함으로써 안전한 서비스 제공을 보장할 수 있습니다. Cisco는 이러한 방식으로 최고 레벨의 서비스 가용성 및 데이터 보호 기능을 제공할 수 있습니다.

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

Printed in USA C11-701314-00 02/12