



## Cisco Cloud/Hybrid Email Security 개요

게시: 2017년 7월 28일

수정: 2018년 1월 25일

**Cisco Systems, Inc.**

[www.cisco.com](http://www.cisco.com)

Cisco는 전 세계에 200개가 넘는 지사를 운영하고 있습니다.

주소, 전화 번호 및 팩스 번호는

다음 Cisco 웹사이트에 나와 있습니다.

[www.cisco.com/go/offices](http://www.cisco.com/go/offices)에서 확인하십시오.

이 설명서의 제품 관련 사양 및 정보는 예고 없이 변경될 수 있습니다. 이 설명서의 모든 설명, 정보 및 권장 사항이 정확하다고 판단되더라도 어떠한 형태의 명시적이거나 묵시적인 보증도 하지 않습니다. 모든 제품의 해당 애플리케이션에 대한 사용은 전적으로 사용자에게 책임이 있습니다.

동봉한 제품의 소프트웨어 라이선스 및 제한된 보증은 제품과 함께 제공된 정보 패키지에 설명되어 있으며 본 문서에 참조를 통해 포함됩니다. 소프트웨어 라이선스 또는 제한 보증을 찾을 수 없는 경우 CISCO 담당자에게 사본을 요청하십시오.

Cisco의 TCP 헤더 압축은 UNIX 운영 체제의 UCB 공개 도메인 버전의 일부로서 University of California, Berkeley(UCB)에서 개발된 프로그램을 적용하여 구현합니다. All rights reserved. Copyright © 1981, Regents of the University of California.

여기에 언급된 기타 모든 보증에도 불구하고 이러한 공급자의 모든 문서 및 소프트웨어는 모든 결함이 포함된 "있는 그대로" 제공됩니다. CISCO 및 위에 언급된 모든 공급업체는 상품성, 특정 목적에의 적합성, 타인의 권리 비침해 또는 처리, 사용, 거래 행위로 발생하는 문제에 대한 묵시적 보증을 포함하여(단, 이에 한하지 않음) 묵시적이든 명시적이든 모든 종류의 보증을 부인합니다.

Cisco 또는 해당 공급업체는 피해의 가능성에 대해 언급한 경우라도 이 설명서의 사용 또는 사용 불능으로 인해 발생하는 이익 손실, 데이터 손실 또는 손상을 포함하여(단, 이에 한하지 않음) 간접, 특별, 중대 또는 부수적 손해에 대해 어떠한 경우라도 책임을 지지 않습니다.

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, Cisco 로고, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare(디자인), Flip Ultra, Flip Video, Flip Video(디자인), Instant Broadband 및 Welcome to the Human Network는 미국 및 기타 특정 국가에서 Cisco Systems, Inc. 및/또는 그 계열사의 상표입니다. Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital(디자인), Cisco:Financed(스타일), Cisco Store, Flip Gift Card 및 One Million Acts of Green은 미국 및 기타 특정 국가에서 Cisco Systems, Inc. 및/또는 그 계열사의 서비스 마크입니다. Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, Cisco Certified Internetwork Expert 로고, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, Cisco Systems 로고, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLXN, IOS, iPhone, IronPort, IronPort 로고, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV(디자인), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx 및 WebEx 로고는 미국 및 기타 특정 국가에서 Cisco Systems, Inc. 및/또는 그 계열사의 등록 상표입니다.

본 문서 및 웹사이트에 언급된 다른 모든 상표는 각 소유자의 자산입니다. "파트너"라는 용어는 사용에 있어 Cisco와 기타 회사 간의 파트너 관계를 의미하지는 않습니다. (0910R)

이 문서에서 사용된 모든 IP(인터넷 프로토콜) 주소와 전화 번호는 실제 주소와 전화 번호가 아닙니다. 이 문서에 포함된 예제, 명령 표시 출력, 네트워크 토폴로지 다이어그램 및 다른 그림은 이해를 돕기 위한 자료일 뿐이며, 실제 IP 주소나 전화 번호가 사용되었다면 이는 의도하지 않은 우연의 일치입니다.

*Cisco Cloud/Hybrid Email Security 개요*

© 2018년 Cisco Systems, Inc. All rights reserved.



## 목 차

---

### 1장

- Cisco Email Security Service 이해 1-1**
  - Cisco Cloud Email Security Service 개요 1-1
  - Cisco Hybrid Email Security 개요 1-4
  - Cisco Email Security Service 관리 1-7
  - 서비스 및 지원 1-7

---

### 2장

- 클라우드 환경 설정 2-1**
  - 클라우드 어플라이언스 액세스 2-1
    - 웹 인터페이스 및 CLI(Command Line Interface) 액세스 2-1
  - Cloud Email Security Appliance 구성 2-1
    - 이메일 인증 구성 2-1
      - DKIM 구성 2-2
      - SPF 구성 2-2
    - 아웃바운드 이메일 라우팅 2-2
    - 로그 아카이브 2-2
  - 서버 구성 2-3
    - SMTP Call Ahead 검증 사용 2-3

---

### 3장

- Cisco End-User Spam Quarantine 사용 3-1**
  - Cisco End-User Spam Quarantine 이해 3-1
    - 허용 목록 및 차단 목록 3-1
  - 스팸 격리에서의 메시지 처리 3-2
    - 스팸 격리에서 받은 편지함으로 메시지 릴리스 3-2
    - 메시지 세부 정보 보기 3-2
    - 한 번에 여러 메시지에서 조치 수행하기 3-3
    - 허용 목록 및 차단 목록에 액세스 3-3
      - 허용 목록 또는 차단 목록에 항목 추가 3-4
    - 격리에서 메시지 검색 3-4





# Cisco Email Security Service 이해

- [Cisco Cloud Email Security Service 개요, 1-1페이지](#)
- [Cisco Hybrid Email Security 개요, 1-4페이지](#)
- [Cisco Email Security Service 관리, 1-7페이지](#)
- [서비스 및 지원, 1-7페이지](#)

## Cisco Cloud Email Security Service 개요

Cisco Cloud Email Security는 지리적으로 분산된 복원 가능한 Cisco 데이터 센터에서 유지 관리되는 인프라를 제공합니다. 이 서비스는 "클라우드에서" 또는 SaaS(Software as a Service) 모델에 기초하여 이메일 보안을 제공합니다. 조직은 클라우드 기반 인프라에 대한 액세스 및 가시성을 계속 유지할 수 있습니다.

본 가이드에서 "어플라이언스"라는 용어는 가상 어플라이언스를 의미합니다.

Cisco Cloud Email Security는 모든 기능이 포함된 서비스로서, 소프트웨어, 하드웨어 및 지원 서비스가 함께 제공됩니다. 이 서비스는 다음과 같은 특성 및 기능이 포함하고 있습니다.

- **새로운 DLP(Data Loss Prevention) 솔루션.** Cisco는 이제 RSA DLP에서 생성된 기존의 모든 DLP 정책을 새로운 DLP 엔진으로 원활하게 마이그레이션해 주는 대체 DLP 솔루션을 제공합니다. 업그레이드를 수행한 후, 웹 인터페이스의 **Mail Policies(메일 정책) > DLP Policy Manager(DLP 정책 관리자)** 페이지에서 마이그레이션된 DLP 정책을 확인하거나 수정할 수 있습니다.



**참고** AsyncOS 11.0 이상 버전에서는 RSA Enterprise Manager Integration이 지원되지 않습니다. RSA Enterprise Manager에서 DLP 정책을 생성한 경우, 업그레이드 후에 어플라이언스에서 해당 정책을 다시 생성해야 합니다.

- **Anti-Spam(안티스팸).** SenderBase 평판 필터와 IronPort Anti-Spam이 통합된 고유한 멀티레이어 접근 방식을 통해 게이트웨이에서 제공됩니다.
- **Anti-Virus(안티바이러스).** Sophos 및 McAfee Anti-Virus 검사 엔진과 함께 게이트웨이에서 제공됩니다.
- **그레이메일 탐지 및 안전한 수신 거부** Cisco Email Security Appliance를 사용하여 다음 작업을 수행할 수 있습니다.
  - 통합 그레이메일 엔진을 사용하여 그레이메일을 식별하고 적절한 정책 제어를 적용합니다.
  - 최종 사용자가 클라우드 기반 Unsubscribe Service(수신 거부 서비스)를 사용하여 원하지 않는 그레이메일의 수신을 거부할 수 있도록 안전하고 손쉬운 메커니즘을 제공합니다.

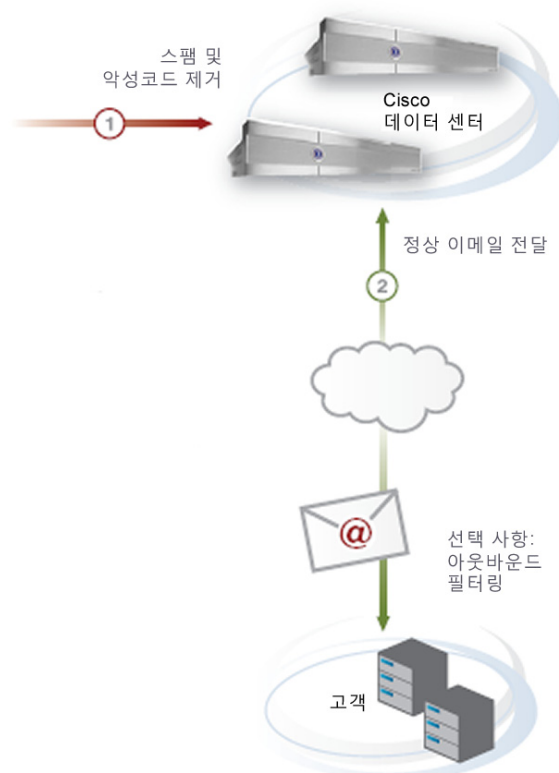
- **Outbreak Filters(보안 침해 필터)™**. 신종 바이러스, 스팸 및 피싱 보안 침해에 대처하는 Cisco의 고유한 보호 기능으로, 새 업데이트가 적용될 때까지 위험한 메시지를 격리함으로써 새 메시지 위협에 대한 취약성 기간을 단축합니다.
- **Policy(정책), Virus(바이러스) 및 Outbreak Quarantines(보안 침해 격리)**. 관리자가 평가할 수 있도록 의심스러운 메시지를 저장하기 위한 안전한 장소를 제공합니다.
- **Spam Quarantine(스팸 격리)**. 격리된 스팸 및 의심스러운 스팸에 대한 최종 사용자 액세스를 제공합니다.
- **Email Authentication(이메일 인증)**. 이 어플라이언스는 SPF(Sender Policy Framework), SIDF(Sender ID Framework) 및 DKIM(DomainKeys Identified Mail) 수신 메일 확인, 그리고 DomainKeys 및 DKIM 발신 메일 서명 등 다양한 형식의 이메일 인증을 지원합니다.
- **File Reputation Filtering and File Analysis(파일 평판 필터링 및 파일 분석)**. Advanced Malware Protection은 다음을 기준으로 수신 및 발신 메시지에서 새로운 위협과 표적 파일 기반 위협을 식별합니다.
  - File reputation(파일 평판)
  - 파일 분석(평판을 알 수 없는 특정 파일 해당)
  - 판정 업데이트
- **URL Filtering(URL 필터링)**. URL 필터링은 여러 가지 새로운 기능을 사용할 수 있도록 수신 및 발신 메시지에서 URL의 평판 및 카테고리를 획득합니다.
- **S/MIME Security Services(S/MIME 보안 서비스)**. 이제 조직은 Cisco Email Security Appliance를 사용하여 모든 최종 사용자가 고유한 인증서를 소유할 필요 없이 S/MIME를 사용하여 안전하게 통신할 수 있습니다. 조직은 개인 대신 조직을 식별하는 인증서를 사용하여 게이트웨이 수준에서 메시지 서명, 암호화, 확인 및 암호 해독을 처리할 수 있습니다.
- **Email Encryption(이메일 암호화)**. HIPAA, GLBA 및 유사한 규제 의무를 준수하도록 발신 메일을 암호화할 수 있습니다. 이렇게 하려면 Cisco Email Security Appliance에서 암호화 정책을 구성하고 호스팅된 키 서비스를 사용하여 메시지를 암호화합니다.
- **Message Tracking(메시지 추적)**. 이 어플라이언스는 Cisco Email Security Appliance가 처리하는 메시지의 상태를 손쉽게 확인할 수 있는 메시지 추적 기능을 제공합니다.
- **Mail Flow Monitoring(메일 플로우 모니터링)**. 모든 인바운드 및 아웃바운드 메시지의 메일 플로우를 모니터링하여, 해당 기업의 모든 이메일 트래픽에 대한 완벽한 가시성을 제공합니다.
- **Access Control(액세스 제어)**. 인바운드 발신자의 IP 주소, IP 주소 범위 또는 도메인을 기반으로 인바운드 발신자의 액세스를 제어합니다.
- **메시지 필터링**. 포괄적인 메시지 필터링 기능을 통해 회사 정책을 시행하고 특정 메시지가 회사 인프라를 드나들 때 작업을 수행할 수 있습니다. 필터 규칙은 메시지나 첨부 파일 내용, 네트워크에 대한 정보, 메시지 봉투, 메시지 헤더, 메시지 본문 등을 기반으로 메시지를 식별합니다. 필터 작업을 통해 메시지를 삭제, 반송, 보관, 숨은 참조 또는 변경하거나 알림을 생성할 수 있습니다.
- **TLS(Transport Layer Security)로 보안되는 SMTP를 통한 메시지 암호화**. 회사 인프라와 기타 신뢰할 수 있는 호스트 사이를 오가는 메시지를 암호화합니다.

Consolidated and robust reporting(통합 및 강력한 보고) 옵션은 지리적으로 분산된 인프라 구축의 트래픽 데이터를 분석하여 완벽하게 통합된 보안 보고 기능을 제공합니다. Cisco Email Security Appliance의 3세대 보고 기술을 사용하면 전 세계에서 가장 큰 규모의 네트워크에 대해서도 탁월한 통찰력을 확보할 수 있습니다. 상세하고 정확한 정보를 조직의 모든 레벨에 적합한 명확하고 유익한 보고서에 통합합니다.

Message tracking(메시지 추적) 기능은 메시지에 대한 근 실시간 가시성을 제공하여 조직이 메시지 처리를 추적할 수 있게 합니다. 이 기능을 사용하면 메시지의 정확한 위치를 확인하여 헬프데스크 통화를 신속하게 처리할 수 있습니다. 로그 파일을 검색할 필요 없이 유연한 추적 인터페이스를 사용하여 메시지를 찾을 수 있습니다.

그림 1-1은 Cisco Cloud Email Security 구축 모델을 보여줍니다.

그림 1-1 Cisco Cloud Email Security 구축



Cisco Cloud Email Security는 다음과 같이 동작합니다.

- Email Security Appliance는 클러스터 컨피그레이션이라고 하는 다른 Email Security Appliance 간에 컨피그레이션 정보를 동기화합니다.
- Email Security Appliance의 클라우드 기반 클러스터는 인바운드 메일을 수락하고 처리합니다.
- 클라우드 기반 Security Management Appliance는 Cloud Email Security Appliance에서 보고 및 추적 데이터를 수집합니다. 이는 Email Security Appliance 클러스터에서 스팸으로 격리되었거나 정책에 의해 격리된 메시지를 보관하는 중앙 위치 역할을 합니다.
- 정책에 의해 필터링된 메일은 중앙에서 격리됩니다.
- 시스템은 그룹웨어 서버 또는 MTA(Mail Transfer Agent)에 처리한 메일을 직접 전송하며, 그룹웨어 서버에서 온 아웃바운드 메일을 처리하고 고급 콘텐츠 필터링 및 이메일 암호화를 제공합니다.
- (선택 사항) 아웃바운드 메일은 Email Security Appliance 클러스터를 통해 인터넷으로 전송될 수 있습니다.

# Cisco Hybrid Email Security 개요

Cisco Hybrid Email Security는 클라우드 기반 이메일 보안 구축을 어플라이언스 기반 이메일 보안 구축(온프레미스)과 결합하는 특별한 서비스 솔루션으로, 조직에 최대한의 선택 사항과 제어 기능을 제공합니다. 클라우드 기반 인프라는 일반적으로 인바운드 이메일 정리에 사용되는 반면 온프레미스 어플라이언스는 DLP(Data Loss Prevention) 및 암호화 기술을 통해 민감한 정보를 보호하면서 더 정밀한 제어 기능을 제공합니다.

Cisco Cloud Email Security 서비스와 마찬가지로 하이브리드 서비스는 소프트웨어, 하드웨어 및 지원 서비스를 함께 제공하는 모든 기능이 포함된 서비스입니다. 이 서비스는 다음과 같은 특성 및 기능이 포함하고 있습니다.

- **새로운 DLP(Data Loss Prevention) 솔루션.** Cisco는 이제 RSA DLP에서 생성된 기존의 모든 DLP 정책을 새로운 DLP 엔진으로 원활하게 마이그레이션해 주는 대체 DLP 솔루션을 제공합니다. 업그레이드를 수행한 후, 웹 인터페이스의 **Mail Policies(메일 정책) > DLP Policy Manager(DLP 정책 관리자)** 페이지에서 마이그레이션된 DLP 정책을 확인하거나 수정할 수 있습니다.



**참고** AsyncOS 11.0 이상 버전에서는 RSA Enterprise Manager Integration이 지원되지 않습니다. RSA Enterprise Manager에서 DLP 정책을 생성한 경우, 업그레이드 후에 어플라이언스에서 해당 정책을 다시 생성해야 합니다.

- **Anti-Spam(안티스팸).** SenderBase 평판 필터와 IronPort Anti-Spam이 통합된 고유한 멀티레이어 접근 방식을 통해 게이트웨이에서 제공됩니다.
- **Anti-Virus(안티바이러스).** Sophos 및 McAfee Anti-Virus 검사 엔진과 함께 게이트웨이에서 제공됩니다.
- **그레이메일 탐지 및 안전한 수신 거부** Cisco Email Security Appliance를 사용하여 다음 작업을 수행할 수 있습니다.
  - 통합 그레이메일 엔진을 사용하여 그레이메일을 식별하고 적절한 정책 제어를 적용합니다.
  - 최종 사용자가 클라우드 기반 Unsubscribe Service(수신 거부 서비스)를 사용하여 원하지 않는 그레이메일의 수신을 거부할 수 있도록 안전하고 손쉬운 메커니즘을 제공합니다.
- **Outbreak Filters(보안 침해 필터)™.** 신종 바이러스, 스팸 및 피싱 보안 침해에 대처하는 Cisco의 고유한 보호 기능으로, 새 업데이트가 적용될 때까지 위험한 메시지를 격리함으로써 새 메시지 위협에 대한 취약성 기간을 단축합니다.
- **Policy(정책), Virus(바이러스) 및 Outbreak Quarantines(보안 침해 격리).** 관리자가 평가할 수 있도록 의심스러운 메시지를 저장하기 위한 안전한 장소를 제공합니다.
- **Spam Quarantine(스팸 격리).** 격리된 스팸 및 의심스러운 스팸에 대한 최종 사용자 액세스를 제공합니다.
- **Email Authentication(이메일 인증).** 이 어플라이언스는 SPF(Sender Policy Framework), SIDF(Sender ID Framework) 및 DKIM(DomainKeys Identified Mail) 수신 메일 확인, 그리고 DomainKeys 및 DKIM 발신 메일 서명 등 다양한 형식의 이메일 인증을 지원합니다.
- **File Reputation Filtering and File Analysis(파일 평판 필터링 및 파일 분석).** Advanced Malware Protection은 다음을 기준으로 수신 및 발신 메시지에서 새로운 위협과 표적 파일 기반 위협을 식별합니다.
  - File reputation(파일 평판)
  - 파일 분석(평판을 알 수 없는 특정 파일 해당)
  - 판정 업데이트



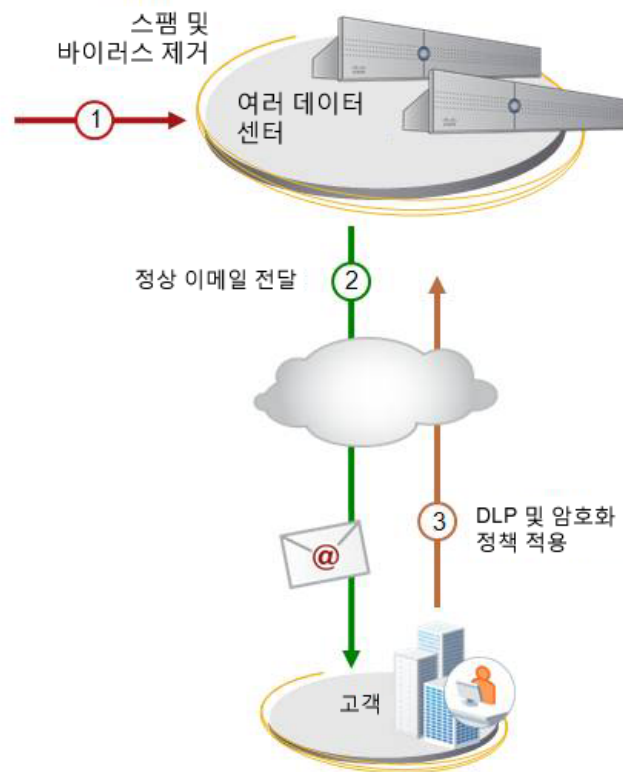
- **URL Filtering(URL 필터링)**. URL 필터링은 여러 가지 새로운 기능을 사용할 수 있도록 수신 및 발신 메시지에서 URL의 평판 및 카테고리를 획득합니다.
- **S/MIME Security Services(S/MIME 보안 서비스)**. 이제 조직은 Cisco Email Security Appliance를 사용하여 모든 최종 사용자가 고유한 인증서를 소유할 필요 없이 S/MIME를 사용하여 안전하게 통신할 수 있습니다. 조직은 개인 대신 조직을 식별하는 인증서를 사용하여 게이트웨이 수준에서 메시지 서명, 암호화, 확인 및 암호 해독을 처리할 수 있습니다.
- **Email Encryption(이메일 암호화)**. HIPAA, GLBA 및 유사한 규제 의무를 준수하도록 발신 메일을 암호화할 수 있습니다. 이렇게 하려면 Cisco Email Security Appliance에서 암호화 정책을 구성하고, 로컬 키 서버 또는 호스팅된 키 서비스를 사용하여 메시지를 암호화합니다.
- **Email Security Manager(이메일 보안 관리자)**. 어플라이언스에서 모든 이메일 보안 서비스 및 애플리케이션을 관리하기 위한 포괄적인 단일 대시보드입니다. 이메일 보안 관리자는 사용자 그룹을 기반으로 이메일 보안을 시행할 수 있습니다. 따라서 별도의 인바운드 및 아웃바운드 정책을 통해 IronPort 평판 필터, 보안 침해 필터, 안티스팸, 안티바이러스 및 이메일 콘텐츠 정책을 관리할 수 있습니다.
- **Message Tracking(메시지 추적)**. 이 어플라이언스는 Cisco Email Security Appliance가 처리하는 메시지의 상태를 손쉽게 확인할 수 있는 메시지 추적 기능을 제공합니다.
- **Mail Flow Monitoring(메일 플로우 모니터링)**. 모든 인바운드 및 아웃바운드 메시지의 메일 플로우를 모니터링하여, 해당 기업의 모든 이메일 트래픽에 대한 완벽한 가시성을 제공합니다.
- **Access Control(액세스 제어)**. 인바운드 발신자의 IP 주소, IP 주소 범위 또는 도메인을 기반으로 인바운드 발신자의 액세스를 제어합니다.
- **메시지 필터링**. 포괄적인 메시지 필터링 기능을 통해 회사 정책을 시행하고 특정 메시지가 회사 인프라를 드나들 때 작업을 수행할 수 있습니다. 필터 규칙은 메시지나 첨부 파일 내용, 네트워크에 대한 정보, 메시지 봉투, 메시지 헤더, 메시지 본문 등을 기반으로 메시지를 식별합니다. 필터 작업을 통해 메시지를 삭제, 반송, 보관, 숨은 참조 또는 변경하거나 알림을 생성할 수 있습니다.
- **TLS(Transport Layer Security)로 보안되는 SMTP를 통한 메시지 암호화**. 회사 인프라와 기타 신뢰할 수 있는 호스트 사이를 오가는 메시지를 암호화합니다.

Consolidated and robust reporting(통합 및 강력한 보고) 옵션은 지리적으로 분산된 인프라 구축의 트래픽 데이터를 분석하여 완벽하게 통합된 보안 보고 기능을 제공합니다. Cisco Email Security Appliance의 3세대 보고 기술을 사용하면 전 세계에서 가장 큰 규모의 네트워크에 대해서도 탁월한 통찰력을 확보할 수 있습니다. 상세하고 정확한 정보를 조직의 모든 레벨에 적합한 명확하고 유익한 보고서에 통합합니다.

Message tracking(메시지 추적) 기능은 메시지에 대한 근 실시간 가시성을 제공하여 조직이 메시지 처리를 추적할 수 있게 합니다. 이 기능을 사용하면 메시지의 정확한 위치를 확인하여 헬프데스크 통화를 신속하게 처리할 수 있습니다. 로그 파일을 검색할 필요 없이 유연한 추적 인터페이스를 사용하여 메시지를 찾을 수 있습니다. 클라우드 기반 어플라이언스 및 온프레미스 어플라이언스를 모두 추적합니다.

그림 1-2는 Cisco Hybrid Email Security 구축 모델을 보여줍니다.

그림 1-2 Cisco Hybrid Email Security 구축



Cisco Hybrid Email Security는 다음과 같이 동작합니다.

- Email Security Appliance는 클러스터 컨피그레이션이라고 하는 다른 Email Security Appliance 간에 컨피그레이션 정보를 동기화합니다.
- Cloud Email Security Appliance는 인바운드 메일을 수락하고 처리합니다. 시스템은 처리한 메일을 온프레미스 Email Security Appliance로 전송하며, 이 어플라이언스는 추가 콘텐츠 필터링을 통해 메시지를 정책별로 필터링합니다.
- 클라우드 기반 Security Management Appliance는 Cloud Email Security Appliance뿐만 아니라 온프레미스 Email Security Appliance에서도 보고 및 추적 데이터를 수집합니다.
- 클라우드 기반 Security Management Appliance는 클라우드 기반 Email Security Appliance에서 격리된 스팸을 보관하는 중앙 격리 역할을 합니다.
- 정책에 의해 필터링된 메일은 메시지를 필터링한 Cisco Security Management Appliance에서 격리됩니다.
- 온프레미스 Email Security Appliance는 그룹웨어 서버에 메일을 전달하고 그룹웨어 서버에서 온 아웃바운드 메일을 처리하며 고급 콘텐츠 필터링 및 이메일 암호화를 제공합니다.
- 온프레미스 Email Security Appliance는 아웃바운드 메일을 인터넷에 전송합니다.

클라우드 기반 어플라이언스가 대량 마케팅 메일러 같은 대량 아웃바운드 메시지를 릴레이하도록 허용하지 않는 것이 좋습니다. 대신, 트랜잭션 이메일로 릴레이하는 트래픽을 제한할 수 있습니다. 용량 보장은 마케팅 커뮤니케이션 또는 이메일 생성 프로그램이나 엔티티를 포함하지 않습니다.

# Cisco Email Security Service 관리

이 어플라이언스를 사용하여 클라우드 기반 이메일 보안 서비스를 직접 관리하고 변경할 수 있습니다.

이 어플라이언스를 사용하여 다음 작업을 수행할 수 있습니다.

- 클라우드 기반 이메일 보안 서비스에 대한 정보를 확인하고 추적합니다.
- 보고서에 액세스합니다.
- 클라우드 기반 어플라이언스의 컨피그레이션에 액세스하고 수정합니다.

## 서비스 및 지원



### 참고

Cisco CES(Cloud Email Security)에 대한 지원을 받으려면 Cisco TAC에 전화 문의를 할 때 계약 번호를 준비하십시오.

Cisco TAC: [http://www.cisco.com/en/US/support/tsd\\_cisco\\_worldwide\\_contacts.html](http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html)

레거시 IronPort에 대한 지원 사이트: <http://www.cisco.com/web/services/acquisitions/ironport.html>

심각하지 않은 문제의 경우, 어플라이언스에서 고객 지원에 액세스할 수도 있습니다. 관련 지침은 사용 설명서 또는 온라인 도움말을 참조하십시오.





## 클라우드 환경 설정

- 클라우드 어플라이언스 액세스, 2-1페이지
- Cloud Email Security Appliance 구성, 2-1페이지
- 서버 구성, 2-3페이지

### 클라우드 어플라이언스 액세스

- 웹 인터페이스 및 CLI(Command Line Interface) 액세스, 2-1페이지

### 웹 인터페이스 및 CLI(Command Line Interface) 액세스

어플라이언스를 통해 직접, 또는 환영문에 나와 있는 URL을 사용하여 모든 클라우드 어플라이언스의 웹 인터페이스에 액세스할 수 있습니다.

또한 환영문에 나와 있는 세부 정보를 사용하여 CLI(Command Line Interface)를 통해 모든 클라우드 어플라이언스에 액세스할 수 있습니다.

### Cloud Email Security Appliance 구성

- 이메일 인증 구성, 2-1페이지
- 아웃바운드 이메일 라우팅, 2-2페이지
- 로그 아카이브, 2-2페이지

### 이메일 인증 구성

SPF(Sender Policy Framework) 또는 DKIM(DomainKeys Identified Mail)을 사용하여 이메일을 인증할 수 있습니다.

DKIM은 발신자가 사용하는 서명 키에 따라 이메일의 신뢰성을 확인합니다. SPF는 DNS TXT 레코드에 따라 이메일의 신뢰성을 확인합니다. SPF를 통해 인터넷 도메인 소유자는 특수 형식의 DNS 레코드를 사용하여, 해당 도메인에 대한 이메일을 전송할 수 있는 시스템을 지정할 수 있습니다.

## DKIM 구성

DKIM 구성 및 콘텐츠 필터 및 메시지 필터 규칙 정의에 대한 지침은 *AsyncOS for Cisco Email Security Appliances 사용 설명서*에서 다음 장을 참조하십시오.

- 이메일 인증
- 메시지 필터를 사용하여 이메일 정책 적용

## SPF 구성

Cisco는 DNS TXT 레코드에 대해 권장하는 SPF 항목을 제공하지만, Email Security Appliance의 RAT(Recipient Access Table) 같은 고객 소유 도메인의 DNS는 관리하지 않습니다. 레코드의 형식은 다음과 같습니다.

```
v=spf1 -exists:%{i}.spf.<unique_name>.iphmx.com -all
```

서비스 및 지원, 1-7페이지을 참조하십시오.

DNS에 SPF 레코드를 추가한 이후에 SPF 확인을 설정하고 콘텐츠 필터 및 메시지 필터 규칙을 정의할 수 있습니다. *AsyncOS for Cisco Email Security Appliances 사용 설명서*에서 다음 장을 참조하십시오.

- 이메일 인증
- 메시지 필터를 사용하여 이메일 정책 적용

## 아웃바운드 이메일 라우팅

Cloud Email Security Appliance를 통해 전송되는 아웃바운드 메일의 경우, 클라우드 기반 서버가 사용자 대신 메일을 릴레이하도록 어플라이언스를 구성해야 합니다. *AsyncOS for Cisco Email Security Appliances 사용 설명서*에서 라우팅 및 전송 기능 구성 장을 참조하십시오.

## 로그 아카이브

Cisco는 클라우드 어플라이언스에서 발생한 로그를 보관하지 않습니다. 이력 로그는 아카이브되지 않으며 로그 로테이션으로 덮어쓸 수 있습니다. 로그를 보존하려는 경우, 클라우드 기반 어플라이언스에 로그 서브스크립션을 구성하여 SCP 푸시(또는 원격 서버의 SCP)를 로그 검색 방법으로 사용합니다. 이 방법은 원격 컴퓨터의 SCP 서버로 로그 파일을 주기적으로 푸시합니다.

이 방법을 사용하려면 SSH1 또는 SSH2 프로토콜을 사용하는 원격 컴퓨터에 SSH SCP 서버가 있어야 합니다. 이 서브스크립션에는 원격 컴퓨터의 사용자 이름, SSH 키 및 대상 디렉토리가 필요하며 로그 파일은 설정된 롤오버 일정에 따라 전송됩니다.

방화벽이 네트워크에 대한 SSH 액세스를 차단하는 경우, Cisco Cloud Email Security 데이터 센터에서 온 인바운드 SSH 연결을 명시적으로 허용하는 것이 좋습니다.

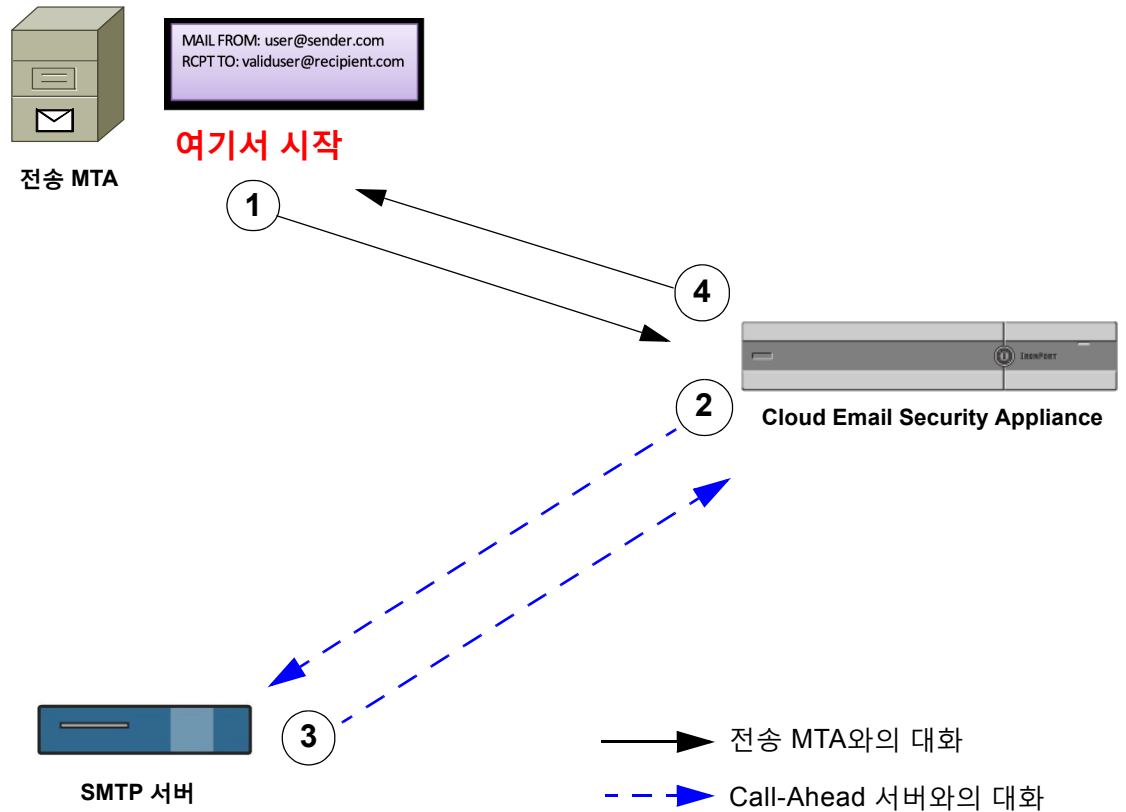
*AsyncOS for Cisco Email Security Appliances 사용 설명서*를 참조하십시오.

# 서버 구성

## SMTP Call Ahead 검증 사용

Cisco Cloud Email Security는 수신자 검증을 위해 SMTP Call Ahead 검증을 사용합니다. 이 검증 방법은 관리자의 오버헤드를 최소화하면서 수신자를 검증하는 원활하고 효율적인 검증 방법입니다. 이 검증 방법은 기존 솔루션에 이미 설정되어 있는 방화벽 설정에 최소한만의 영향을 주거나 전혀 영향을 주지 않습니다.

그림 2-1 SMTP Call Ahead 서버 대화 워크플로



SMTP Call Ahead는 다음과 같이 동작합니다.

- 1단계** 이메일 전송 시스템(MTA)은 클라우드 기반 Email Security Appliance와의 연결을 엽니다. 초기 SMTP 프로토콜 대화를 위해 발신자 이메일 시스템은 RCPT TO 정보를 함께 전달합니다.
- 2단계** 클라우드 기반 이메일 보안 인프라는 수신 연결을 열어 둔 상태에서 SMTP 서버에 대한 호출을 시작합니다. 이러한 통신을 위해 클라우드 기반 Email Security Appliance는 SMTP 서버(예: Microsoft Exchange)에 RCPT TO 정보를 전달합니다.

**3단계** RCPT TO:의 사용자가 유효한지 또는 유효하지 않은지에 따라 SMTP 서버는 200 시리즈 상태 또는 500 시리즈 상태를 각각 전송합니다.

MTA 또는 그룹웨어 서버에서 SMTP Call Ahead가 제대로 동작하려면, 클라우드 기반 서버에서의 연결을 차단할 수 있는 발신자 확인 기능(예: SPF 확인, TLS 확인 및 DHAP 체계)을 지정된 IP 주소에 대해 비활성화해야 합니다.

**4단계** Cloud Email Security Appliance는 SMTP 대화를 다시 시작하고 전송 MTA에 응답을 전송하여, SMTP 서버 응답(그리고 SMTP Call-Ahead 프로필에 구성된 설정)을 기반으로 대화를 계속 진행하도록 허용하거나 연결을 삭제합니다.

이메일 파이프라인의 프로세스 순서 때문에, 특정 수신자에 대한 메시지가 RAT에 의해 거부되면 SMTP call-ahead 수신자 검증이 발생하지 않습니다. 예를 들어 *example.com*에 대한 메일만 수락하도록 RAT에 지정한 경우, *recipient@domain2.com*에 대한 메일은 SMTP call-ahead 수신자 검증이 발생하기 전에 거부됩니다.

SMTP Call Ahead 검증이 이루어지는 방식에 대한 자세한 내용은 *AsyncOS for Cisco Email Security Appliances 사용 설명서*를 참조하십시오.

---





## Cisco End-User Spam Quarantine 사용



참고

이 장은 End-User Spam Quarantine을 활성화한 경우에만 참조하십시오.

- [Cisco End-User Spam Quarantine 이해, 3-1페이지](#)
- [스팸 격리에서의 메시지 처리, 3-2페이지](#)

## Cisco End-User Spam Quarantine 이해

스팸은 다음을 포함하나 이에 국한되지 않습니다.

- 광고 메일, 다단계, 행운의 편지 및 선전
- 원치 않는 의심스러운 주제 또는 모욕적인 내용이나 협박하는 메일
- 틀리거나 잘못된 헤더, 제목 줄, 발신자, 반환 주소, 라우팅 또는 전송 경로를 포함하는 메일
- 허가 없이 서드파티 도메인 이름을 사용하는 메일

스팸 격리는 적절한 정책 및 기술을 구현하여 스팸 메일의 영향을 최소화합니다. 스팸으로 식별된 메일 메시지는 격리됩니다. 메시지가 스팸이 아닌 경우에는 격리에서 메시지를 제거하고 발신자를 허용 목록에 추가할 수 있습니다. 또는 메시지가 진짜 스팸이면 아무런 조치도 취하지 마십시오. 격리된 메일은 사서함 용량 제한으로 계산되지 않고 특정 기간(일) 이후에 자동으로 삭제됩니다.



참고

메일이 삭제되기 전에 격리에서 메일을 며칠 동안 보관할 수 있는지는 관리자에게 문의하십시오.

스팸 격리에 액세스하는 데는 특별한 하드웨어, 소프트웨어 또는 보안 권한이 필요하지 않습니다. 사용자는 스팸으로 식별된 메시지를 나열하는 스팸 격리 알림을 정기적으로 받습니다.

## 허용 목록 및 차단 목록

허용 목록과 차단 목록을 만들어 어떤 메일 메시지를 스팸으로 처리할지 더 잘 제어할 수 있습니다. 허용 목록을 사용하면 특정 사용자 또는 도메인이 스팸으로 처리되지 않으며, 차단 목록을 사용하면 특정 사용자 또는 도메인이 항상 스팸으로 처리됩니다.



참고

허용 목록 및 차단 목록에 추가할 수 있는 최대 항목 수는 관리자에게 문의하십시오.

[허용 목록 및 차단 목록에 액세스, 3-3페이지](#)를 참조하십시오.

## 스팸 격리에서의 메시지 처리

스팸 격리 알림은 메시지가 진짜 스팸 메시지인지 확인할 수 있도록 메시지에 대한 세부 정보를 제공합니다. 스팸 격리 알림에서 직접 메시지를 처리하거나 알림의 본문에서 찾은 링크를 클릭하여 스팸 격리에 액세스할 수 있습니다.

메시지가 스팸이면 아무런 조치도 취하지 마십시오. 메시지는 격리에 특정 기간(일)(관리자에게 확인) 동안 보관된 다음 삭제됩니다.

- 스팸 격리에서 받은 편지함으로 메시지 릴리스, 3-2페이지
- 메시지 세부 정보 보기, 3-2페이지
- 메시지 세부 정보 보기, 3-2페이지
- 한 번에 여러 메시지에서 조치 수행하기, 3-3페이지
- 허용 목록 및 차단 목록에 액세스, 3-3페이지
- 격리에서 메시지 검색, 3-4페이지

## 스팸 격리에서 받은 편지함으로 메시지 릴리스

메시지가 스팸이 아닌 경우에는 메시지를 격리에서 받은 편지함으로 릴리스하십시오. 해당 발신자의 향후 메시지가 격리되는 것을 방지하기 위해 발신자를 허용 목록에 추가할 수도 있습니다.


### 절차

- 
- 1단계** 스팸 격리 알림에서 릴리스하려는 메시지 옆에 있는 **Not Spam(스팸 아님)**을 클릭합니다.
- 2단계** 표시되는 확인 메시지에서 **Add Sender to Safelist(허용 목록에 발신자 추가)**를 클릭합니다. 메시지를 릴리스하고 발신자를 허용 목록에 추가하지 않은 경우, 해당 발신자의 향후 메시지가 격리될 수도 있습니다.
- 

## 메시지 세부 정보 보기

메시지가 스팸인지 확인하기 위해 메시지 발신자 및 주제 이외에 세부 정보가 필요한 경우, 메시지에 대해 조치를 취하기 전에 전체 메시지를 확인할 수 있습니다.

### 절차

- 
- 1단계** 스팸 격리 알림에서 메시지의 제목 링크를 클릭하여 Message Details(메시지 세부 정보) 페이지를 표시합니다.
-  **참고** 메시지에 대해 이미 조치를 취한 경우, Message Not Found(메시지를 찾을 수 없음) 페이지가 나타납니다.
-

- 2단계** 드롭다운 목록에서 취할 조치를 선택합니다. 옵션에는 "Release"(릴리스), "Release and Add to Safelist"(릴리스 및 허용 목록에 추가) 및 "Delete"(삭제)가 있습니다.  
아무런 조치를 수행하지 않은 경우, 메시지는 특정 기간(일)(관리자에게 확인) 이내에 격리에서 삭제됩니다.
- 3단계** **Submit(제출)**을 클릭합니다.
- 4단계** 확인 메시지에서 의도한 작업을 확인합니다.

## 한 번에 여러 메시지에서 조치 수행하기

### 절차

- 1단계** 스팸 격리 알림에서 링크 중 하나를 클릭하여 스팸 격리에 액세스합니다.
- 2단계** 조치를 취할 각 메시지 옆에 있는 확인란을 선택합니다.
- 3단계** 드롭다운 목록에서 취할 조치를 선택하고 **Submit(제출)**을 클릭합니다.  
아무런 조치를 수행하지 않은 경우, 메시지는 특정 기간(일)(관리자에게 확인) 이내에 격리에서 삭제됩니다.
- 4단계** 확인 메시지에서 의도한 작업을 확인합니다.

## 허용 목록 및 차단 목록에 액세스

다음 형식을 사용하여 허용 목록 및 차단 목록에 항목을 추가할 수 있습니다.

- user@domain.com
- server.domain.com
- domain.com

발신자나 도메인을 동시에 허용 목록과 차단 목록에 추가할 수는 없습니다. 하지만 어떤 도메인을 허용 목록에 추가하고 그 도메인에 속한 사용자의 이메일 주소를 차단 목록에 추가할 경우(또는 그 반대의 경우), 어플라이언스는 두 규칙을 모두 적용합니다. 예를 들어, example.com을 허용 목록에 추가하고 george@example.com을 차단 목록에 추가할 경우, 어플라이언스는 example.com에서 보낸 모든 메일을 스팸 검사 없이 전달합니다. 단, george@example.com에서 보낸 메일은 스팸으로 처리합니다.

.domain.com 구문을 사용하여 하위 도메인의 범위를 허용하거나 차단할 수는 없습니다. 그러나 server.domain.com 구문을 사용하여 특정 도메인을 명시적으로 차단할 수 있습니다.

## 허용 목록 또는 차단 목록에 항목 추가

### 절차

- 
- 1단계 스팸 격리 알림에서 링크 중 하나를 클릭하여 스팸 격리에 액세스합니다.
  - 2단계 **Options(옵션)** 드롭다운 목록에서 **Safelist(허용 목록)** 또는 **Blocklist(차단 목록)**를 선택합니다.
  - 3단계 이메일 주소 또는 도메인을 입력하고 **Add to List(목록에 추가)**를 클릭합니다.
- 



**참고** 허용 목록의 항목과 달리 End-User Spam Quarantine의 Options(옵션) 메뉴에서만 차단 목록 항목을 추가할 수 있습니다.

---

## 격리에서 메시지 검색

### 절차

- 
- 1단계 스팸 격리 알림에서 링크 중 하나를 클릭하여 스팸 격리에 액세스합니다.
  - 2단계 **Search Messages(메시지 검색)** 필드에서 검색 조건을 입력하고 **Search(검색)**를 클릭합니다.
-