안티스팸, 안티바이러스, 그레이메일 및 Outbreak Filter 모범 사례 가이드

목차

개요

이메일을 통해 조직이 직면한 위협, 공격 및 미묘한 문제의 대부분은 스팸, 악성코드, 복합적 공격의 형태로 나타납니다.Cisco의 ESA(Email Security Appliance)에는 이러한 위협이 조직에 침투하기 전에 게이트웨이에서 차단할 수 있는 다양한 기술과 기능이 포함되어 있습니다.이 문서에서는 인바운드 및 아웃바운드 이메일 흐름 모두에서 안티스팸, 안티바이러스, 그레이메일 및 신종 바이러스 필터를 구성하는 모범 사례에 대해 설명합니다.

안티스팸

안티스팸 보호는 스팸, 피싱, 좀비 공격을 비롯한 각종 알려진 위협과 "419" 스캠과 같이 감지하기가 어렵고 수명이 짧은 낮은 이메일 위협을 해결합니다.또한 안티스팸 보호는 다운로드 URL 또는 실행 파일을 통해 악성 콘텐츠를 배포하는 스팸 공격과 같은 새롭고 발전하는 복합적인 위협을 식별합니다.

Cisco Email Security는 다음과 같은 안티스팸 솔루션을 제공합니다.

- IronPort IPAS(안티스팸 필터링)
- Cisco IMS(Intelligent Multi-Scan Filtering)

ESA에서 두 솔루션을 모두 라이센스 및 활성화할 수 있지만 특정 메일 정책에서만 사용할 수 있습니다.이 모범 사례 문서에서는 IMS 기능을 사용합니다.

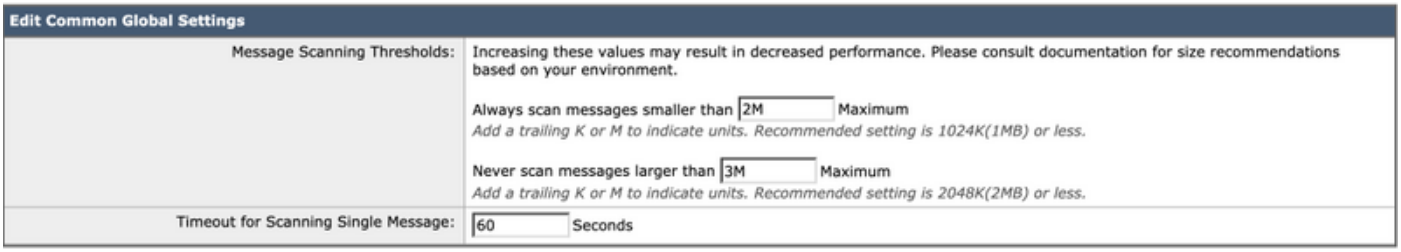
기능 키 확인

- ESA에서 System **Administration(시스템 관리)** > Feature Keys(**기능 키)로 이동합니다.**
- Intelligent Multi-Scan 라이센스를 찾고 해당 라이센스가 활성 상태인지 확인합니다.

IMS(Intelligent Multi-Scan)를 전역적으로 활성화

- 켜짐 이(가) ESA, 탐색 대상 **보안 서비스> IMS 및 그레이메일**
- 클릭 이(가) **사용**단추를 **IMS 전역 설정**:

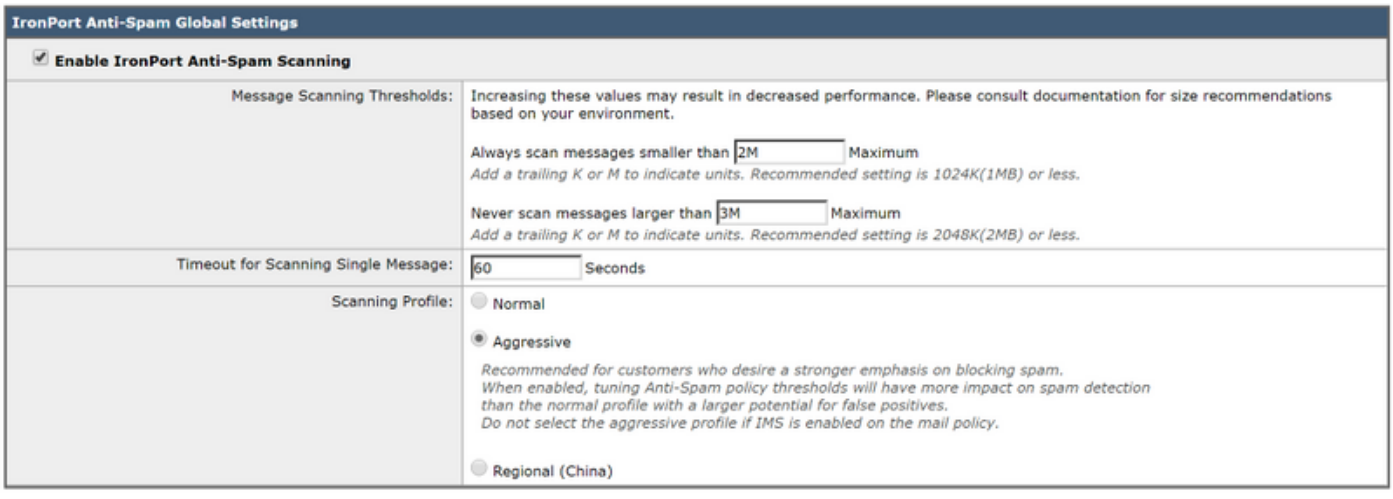
- 공통 전역 **설정** 및 Edit **Global Settings(전역 설정 편집)를 클릭합니다.**
- 여기 YouTube 이(가) 구성 다중 설정. 더 권장 설정 다음과 같습니다. 표시 인 이(가) 이미지 아래:



- Submit(제출)을 **클릭합니다.**및 **커밋 변경.**

IMS 라이센스 서브스크립션이 없는 경우:

- Security **Services(보안 서비스) > IronPort Anti-Spam으로 이동합니다.**
- 클릭 이(가) **사용**IronPort **Anti-Spam 개요 단추**
- 전역 **설정 편집을 클릭합니다.**
- 여기 YouTube 이(가) 구성 다중 설정. 더 권장 설정 다음과 같습니다. 표시 인 이(가) 이미지 아래:

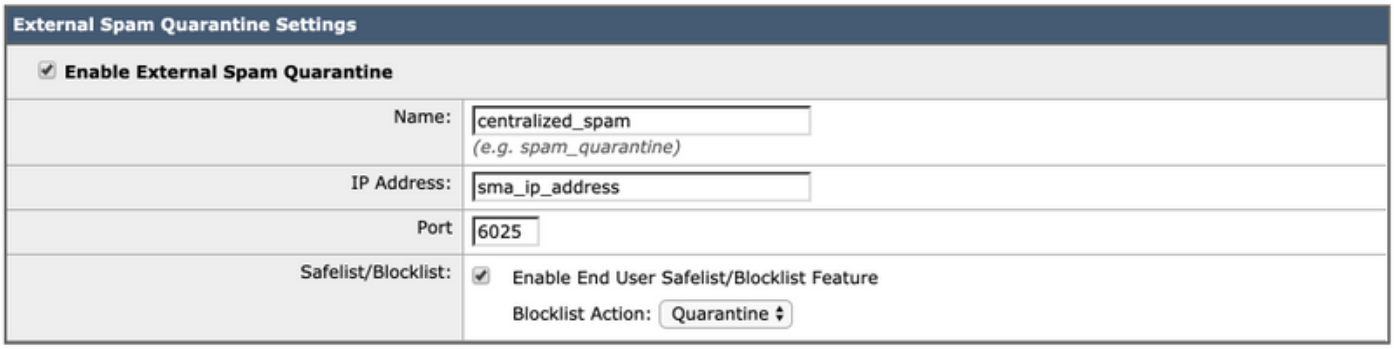


- Cisco는 스팸 차단을 강력하게 강조하려는 고객에게 **적극적인** 스캐닝 프로필을 선택하는 것을 권장합니다.
- Submit(제출)을 **클릭합니다.**및 **커밋 변경**

중앙 집중식 스팸 격리 사용

Anti-Spam에는 쿼런틴으로 보낼 수 있는 옵션이 있으므로 스팸 격리가 설정되었는지 확인해야 합니다.

- Security **Services(보안 서비스) > Spam Quarantine(스팸 격리)으로 이동합니다.**
- 클릭통화 중 이(가) **구성**단추 다음 가져오기 YouTube 대상 이(가) 폴더채무 페이지.
- 여기 YouTube 이(가) 활성화 이(가) 격리 기준 확인 이(가) **활성화**상자 및 점e-메일 격리 대상 이(가) 중앙 집중식 켜짐 보안관리 A어플라이언스(SMA) 기준채우기 인 SMA**이름**및 **IP 주소** . 더 권장 설정 다음과 같습니다. 표시 아래:



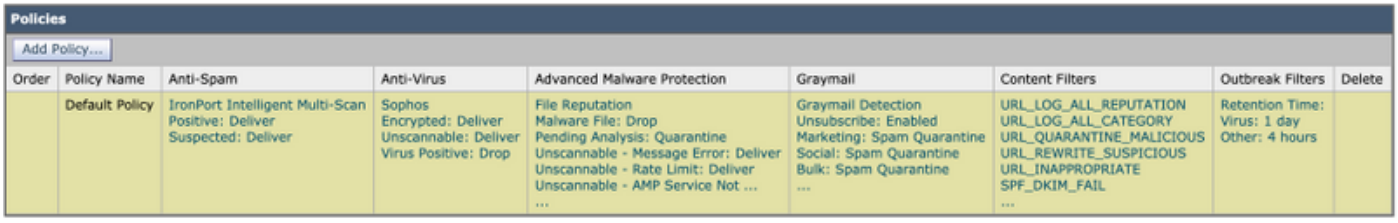
- Submit(제출)을 **클릭합니다.**및 **커밋 변경**

중앙 집중식 격리 설정 및 설정에 대한 자세한 내용은 모범 사례 문서를 참조하십시오.
[중앙 집중식 정책, 바이러스 및 Outbreak 격리 설정 및 ESA에서 SMA로의 마이그레이션을 위한 모범 사례]

정책에서 안티스팸 구성

한 번 인텔리전트 다중 - 스캔 이(가) 이(가) 구성 전 세계 , YouTube 이(가) 지금 적용 인텔리전트 다중 - 스캔 대상 메일 정책:

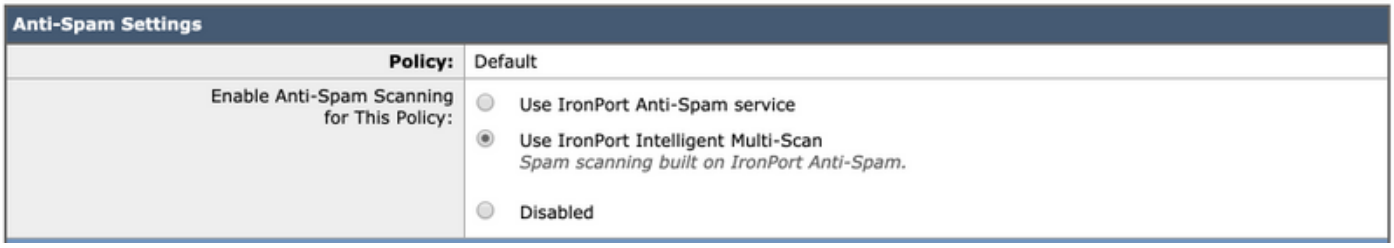
- Mail Policies(**메일 정책**) > Incoming **Mail Policies(수신 메일 정책)로 이동합니다.**
- 수신 메일 정책은 기본적으로 IronPort 안티스팸 설정을 사용합니다.
- **Anti-Spam(안티스팸)** 아래의 파란색 링크를 클릭하면 해당 정책이 맞춤형 안티스팸 설정을 사용할 수 있습니다.
- 아래에는 맞춤형 안티스팸 설정을 사용하는 기본 정책을 보여주는 예시가 나와 있습니다.



맞춤화하려는 정책에 대해 **Anti-Spam**(안티스팸)에서 파란색 링크를 클릭하여 수신 메일 정책에 대한 안티스팸 설정을 사용자 지정합니다.

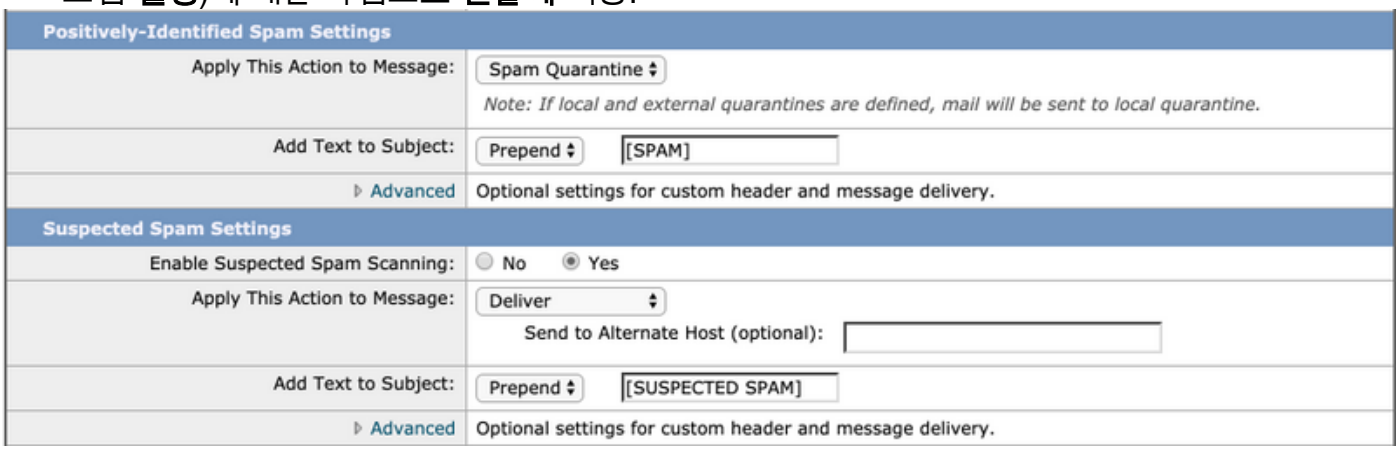
여기 YouTube 이(가) 선택 이(가) 안티-Spam 검사 중 옵션 YouTube 소원 대상 활성화 대상 이(가) 정책.

- 대상 이(가) 목적 의 이(가) 최고 제품얼음 문서, 클릭 이(가) 라디오 단추 다음 대상 사용 **IronPort Intelligent Multi-스캔:**

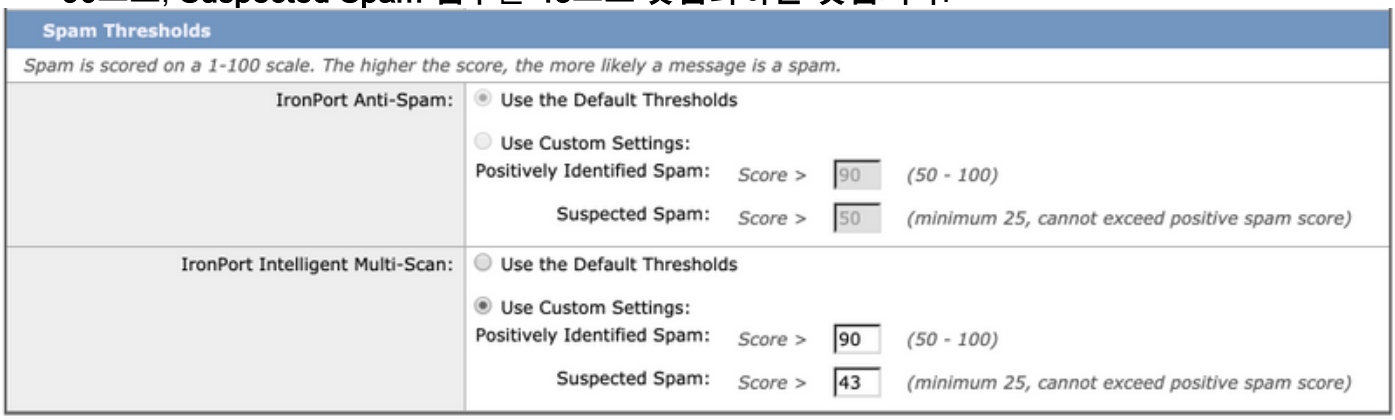


다음 두 섹션에는 **Positively-Identified Spam Settings(양성으로 식별된 스팸 설정)** 및 **Suspected Spam Settings(의심스런 스팸 설정)가** 포함됩니다.

- 권장 모범 사례는 제목 및 제목에 **추가된** 접두어 **[SPAM]** 텍스트를 사용하여 Positively-Identified **Spam** 설정에 **격리** 작업을 구성하는 것입니다.
- 제목에 **[SUSPECTED SPAM]**이 추가된 접두사가 포함된 **Suspected Spam Settings**(의심되는 스팸 **설정**)에 대한 작업으로 **전달에** 적용:



- **Spam Threshold** 설정을 변경할 수 있으며, 권장 설정은 Positively-Identified Spam 점수**를 90**으로, **Suspected Spam 점수**를 **43**으로 **맞춤화하는 것입니다**.



- Submit(제출)을 **클릭합니다.**및 **커밋 변경**

안티바이러스

Anti-Virus 보호 기능은 Sophos 및 McAfee의 두 서드파티 엔진을 통해 제공됩니다.이러한 엔진은 알려진 모든 악성 위협을 필터링하여, 삭제, 청소 또는 구성된 대로 격리합니다.

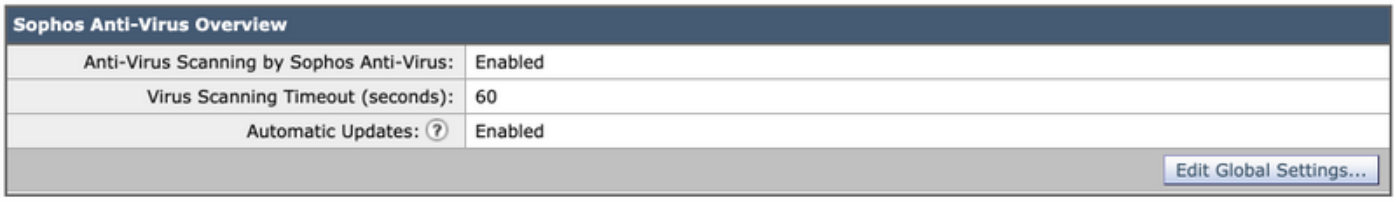
기능 키 확인

두 기능 키가 모두 활성화 및 활성화되었는지 확인하려면 다음을 수행합니다.

- System **Administration(시스템 관리)** > Feature Keys(**기능 키)로 이동합니다.**
- Sophos **Anti-Virus** 및 **McAfee** 라이센스가 모두 활성 상태인지 확인합니다.

안티바이러스 검사 사용

- 탐색 대상 **보안 서비스> 안티바이러스 - Sophos**
- 클릭 이(가) **사용**단추를 클릭합니다.
- 자동 **업데이트**가 활성화되고 Sophos Anti-Virus 파일 업데이트가 제대로 작동하는지 확인합니다.필요한 경우 **Update Now(지금 업데이트)**를 클릭하여 파일 업데이트를 즉시 시작합니다.



- Submit(제출)을 **클릭합니다.**및 **커밋 변경.**

McAfee 라이센스도 활성 상태이면 대상 **보안 서비스> 안티바이러스 - McAfee**

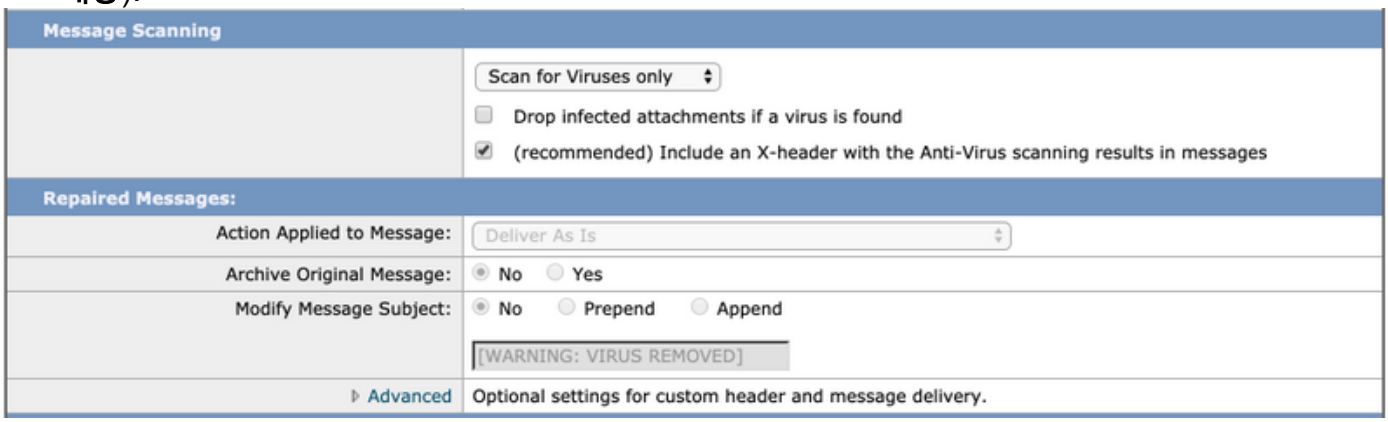
- 클릭 이(가) **사용**단추를 클릭합니다.
- Automatic **Update(자동 업데이트)**가 **Enabled(활성화됨)**이고 McAfee Anti-Virus 파일 업데이트가 제대로 작동하는지 확인합니다.필요한 경우 **Update Now(지금 업데이트)**를 클릭하여 파일 업데이트를 즉시 시작합니다.
- Submit(제출)을 **클릭합니다.**및 **커밋 변경**

메일 정책에서 안티바이러스 구성

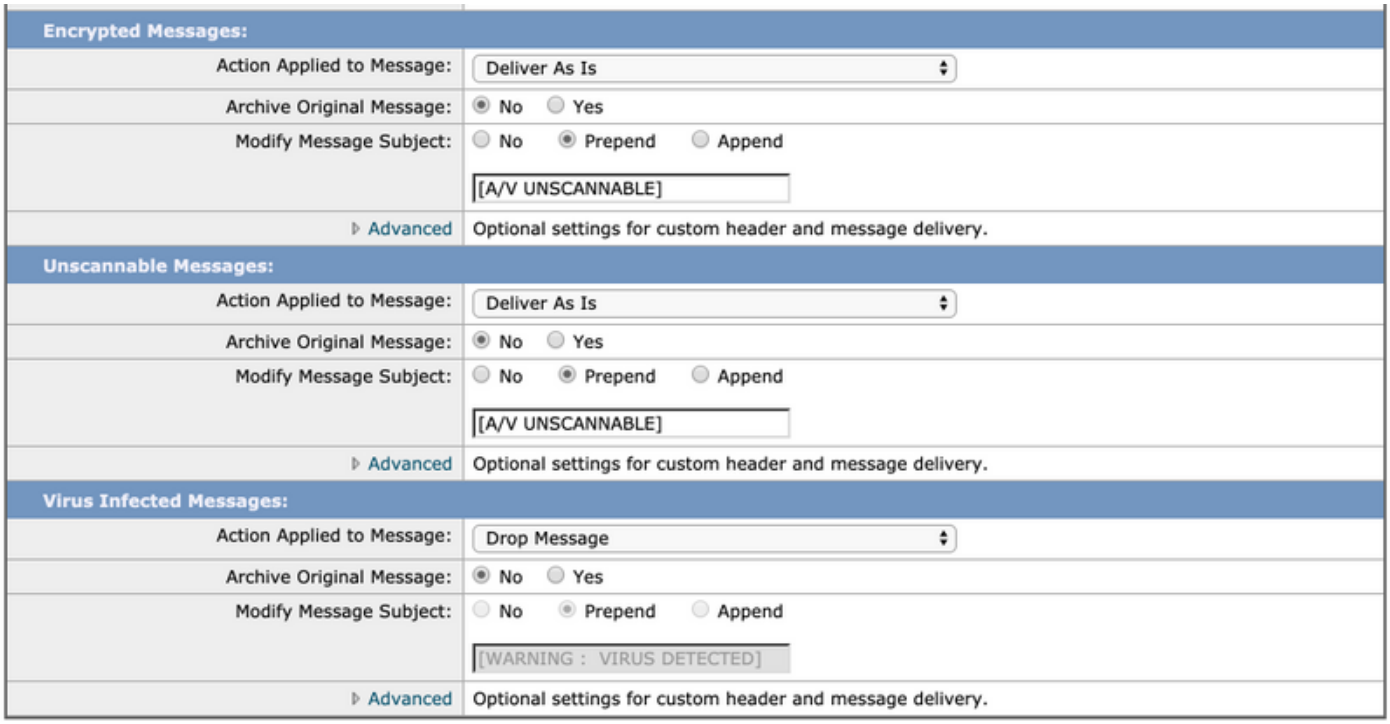
수신 메일 정책에서 다음을 권장합니다.

- Mail Policies(**메일 정책**) > Incoming **Mail Policies(수신 메일 정책)로 이동합니다.**
- 사용자 **지정할** 정책에 대해 안티바이러스 아래의 파란색 링크를 클릭하여 수신 메일 정책에 대한 안티바이러스 설정을 사용자 지정합니다.
- 여기 YouTube 이(가) 선택 이(가) 안티-바이러스 검사 중 옵션 YouTube 소원 대상 활성화 대상 이(가) 정책.
- 대상 이(가) 목적 의 이 bpract얼음 문서에서 **McAfee** 및 Sophos **Anti-Virus**를 모두 선택합니다.

- 파일을 복구하려고 시도하지 않으므로 메시지 검사는 **Scan for Viruses only(바이러스 검사만 해당)**:



- Encrypted **및 Unscannable Messages**에 대해 권장되는 작업은 수정된 제목 줄**을** 사용하여 Deliver As-Is를 수행하는 것입니다.
- 아래 이미지에 표시된 대로 모든 **바이러스 감염 메시지 삭제**는 안티바이러스에 권장되는 정책입니다.



- Submit(제출)을 **클릭합니다.**및 **커밋 변경**

발신 메일 정책에도 유사한 정책이 권장되지만 아웃바운드 이메일의 제목 줄은 수정하지 않는 것이 좋습니다.

그레이메일

Email Security Appliance의 그레이메일 관리 솔루션은 두 가지 구성 요소로 구성됩니다.통합된 그레이메일 스캐닝 엔진 및 클라우드 기반 Unsubscribe Service.그레이메일 관리 솔루션을 사용하면 통합 그레이메일 엔진을 사용하여 그레이메일을 식별하고 적절한 정책 제어를 적용하며, 최종 사용자가 수신 거부 서비스를 사용하여 원치 않는 메시지를 수신 거부할 수 있는 손쉬운 메커니즘을 제공할 수 있습니다.

그레이메일 범주에는 마케팅 이메일, 소셜 네트워크 이메일 및 대량 이메일이 포함됩니다.고급 옵션에는 사용자 지정 헤더 추가, 대체 호스트로 전송, 메시지 아카이빙이 포함됩니다.이 모범 사례를

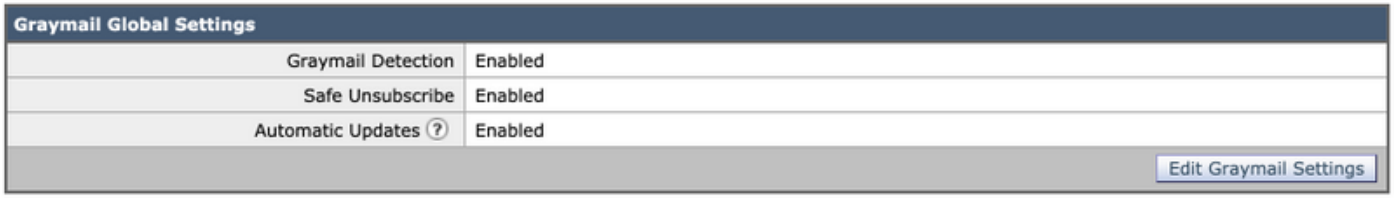
위해 기본 메일 정책에 대해 그레이메일의 안전 수신 거부 기능을 활성화합니다.

기능 키 확인

- ESA에서 System **Administration(시스템 관리)** > Feature Keys(**기능 키)로 이동합니다.**
- 그레이메일 **안전 구독 취소**를 찾아 활성 상태인지 확인합니다.

그레이메일 및 안전한 수신 거부 서비스 사용

- 켜짐 이(가) ESA, 탐색 대상 **보안 서비스> IMS 및 그레이메일**
- 클릭 이(가) **그레이메일 설정 편집**Graymail Global **Settings(그레이메일 전역 설정)의 버튼**
- Enable Graymail Detection(그레이메일 **탐지 활성화), Enable Safe Unsubscribe(안전 수신 거부 활성화)** 및 Enable Automatic Updates(**자동 업데이트 활성화)** 모든 옵션**을 선택합니다.**



- Submit(제출)을 **클릭합니다.**및 **커밋 변경**

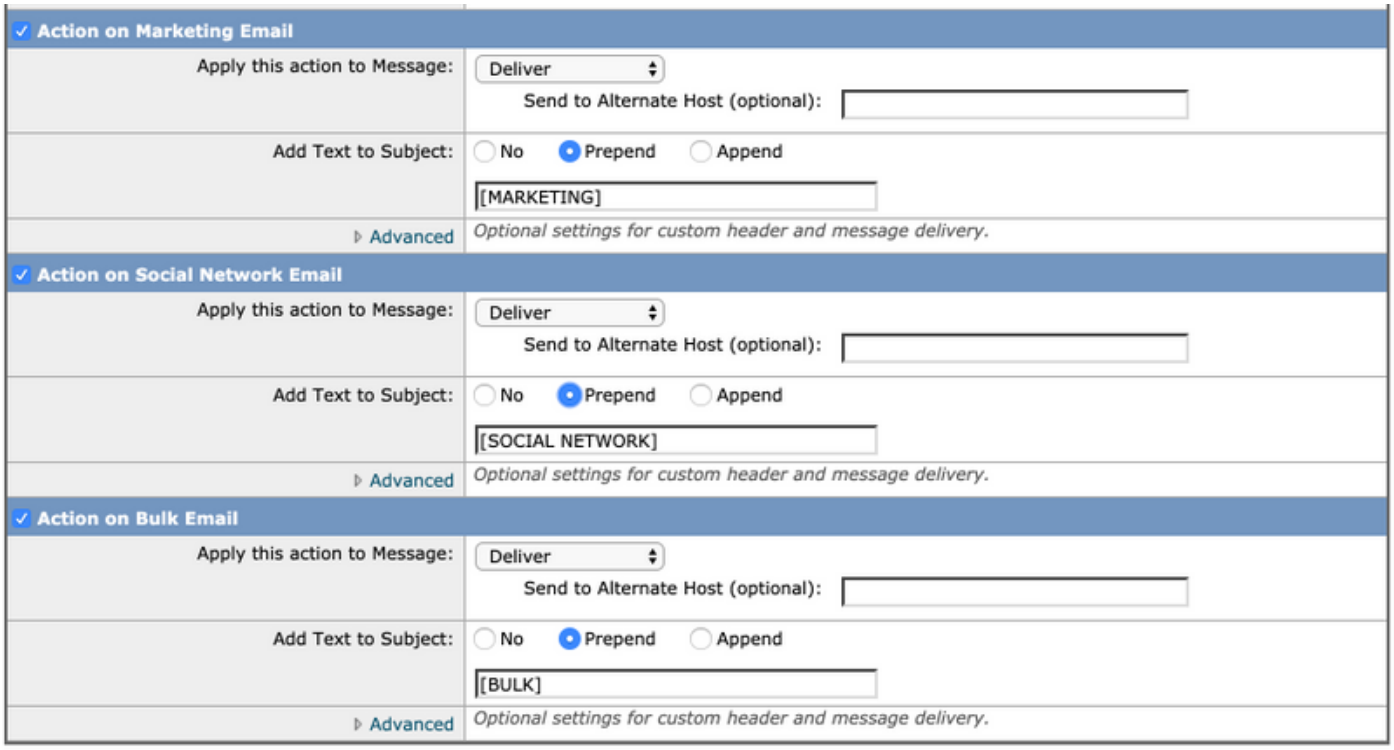
정책에서 그레이메일 및 안전 수신 거부 구성

Once 그레이메일 및 안전 수신 거부 이(가) 이(가) 구성 전 세계 , YouTube 이(가) 지금 이 서비스 적용 대상 메일 정책.

- Mail Policies(**메일 정책**) > Incoming **Mail Policies(수신 메일 정책)로 이동합니다.**
- 그레이메일 아래의 파란색 링크를 클릭하면 **해당** 특정 정책이 사용자 지정된 그레이메일 설정을 사용할 수 있습니다.
- 여기 YouTube 이(가) 선택 그레이메일옵션 YouTube 소원 대상 활성화 대상 이(가) 정책.
- 대상 이(가) 목적 의 이(가) 최상ract얼음 문서, 클릭 이(가) 라디오 단추 다음 이 **정책에 대해 그레이메일 탐지**를 활성화하고 **이 정책에 대한 그레이메일 구독 취소를 활성화하려면**:

다음 세 섹션에는 **마케팅 이메일 설정에 대한 작업**, **소셜 네트워크 이메일 설정에 대한 작업** 및 **대량 이메일 설정에 대한 작업이** 포함됩니다.

- 권장 모범 사례는 모든 항목을 사용하도록 설정하고 아래와 같이 카테고리와 관련하여 제목에 추가된 텍스트를 포함하여 **전달**으로 작업을 유지하는 것입니다.



- Submit(제출)을 **클릭합니다.**및 **커밋 변경**

발송 메일 정책에는 그레이메일**이** 비활성 **상태**로 유지되어야 합니다.

신종 바이러스 필터

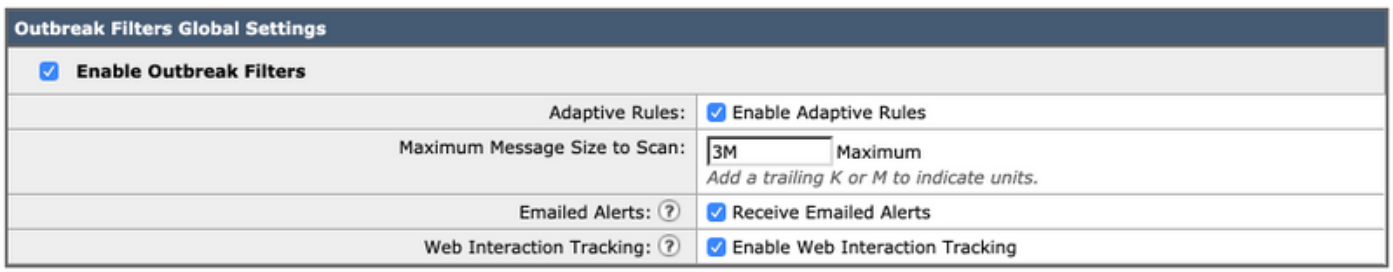
Outbreak Filter는 안티스팸 엔진, URL 스캐닝 및 탐지 기술 등을 결합하여 진정한 스팸 카테고리(예: 피싱 이메일 및 스캠 이메일)를 벗어난 항목에 올바르게 태그를 지정하고 사용자 알림 또는 격리와 함께 적절하게 처리합니다.

기능 키 확인

- ESA에서 System **Administration(시스템 관리)** > Feature Keys(**기능 키)로 이동합니다.**
- Outbreak **Filters**를 찾아 활성 상태인지 확인합니다.

Outbreak Filter 서비스 사용

- 켜짐 이(가) ESA, 탐색 대상 **보안 서비스> 신종 바이러스 필터**
- 클릭 이(가) **사용**버튼 Outbreak **Filter 개요**
- 여기 YouTube 이(가) 구성 다중 설정. 더 권장 설정 다음과 같습니다. 표시 인 이(가) 이미지 아래:

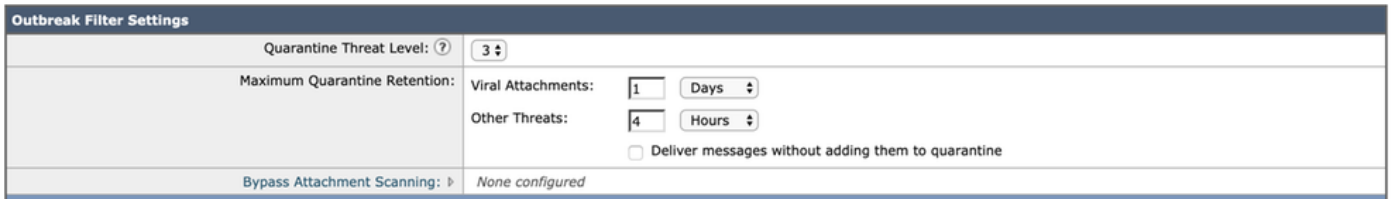


- Submit(제출)을 **클릭합니다.**및 **커밋 변경.**

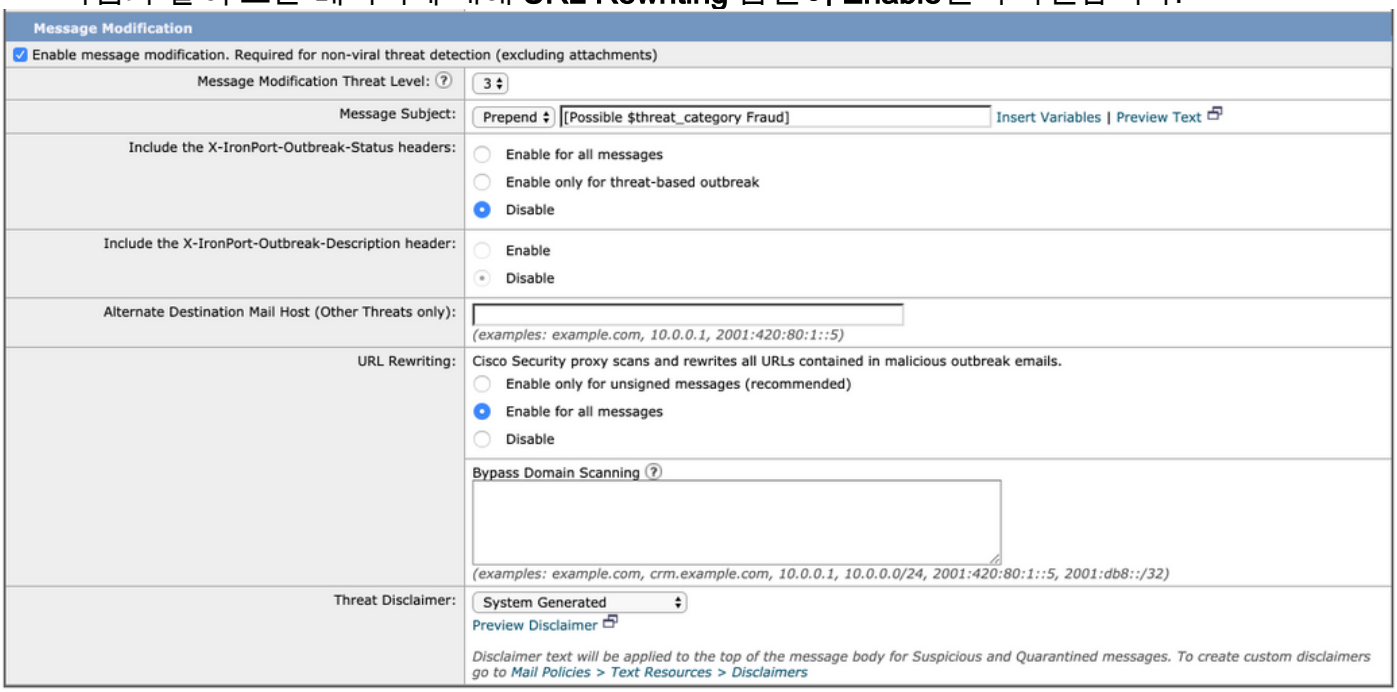
정책에서 Outbreak Filter 구성

Once Outbreak Filter 이(가) 이(가) 구성 전 세계 , YouTube 이(가) 지금 이 기능 적용 메일 정책.

- Mail Policies(**메일 정책**) > Incoming **Mail Policies(수신 메일 정책)로 이동합니다.**
- Outbreak **Filters** 아래의 파란색 링크를 클릭하면 해당 정책이 사용자 지정된 Outbreak Filter 설정을 사용할 수 있습니다.
- 대상 이(가) 목적 의 이(가) 최고 제품얼음 에서는 Outbreak Filter 설정을 기본값으로 유지합니다.



- Outbreak Filter는 URL이 악성, 의심 또는 피싱으로 간주될 경우 재작성할 수 있습니다.URL 기반 위협**을** 탐지하고 재작성하려면 Enable **message modification(메시지 수정** 활성화)을 선택합니다.
- 다음과 같이 모든 메시지에 대해 **URL Rewriting** 옵션**이 Enable**인지 확인합니다.



- Submit(제출)을 **클릭합니다.**및 **커밋 변경**

발신 메일 정책에는 Outbreak **Filter가 Disabled(비활성화됨**) 조건으로 **남아** 있어야 합니다.

결론

이 문서에서는 ESA(Email Security Appliance)의 안티스팸, 안티바이러스, 그레이메일 및 보안 침해 필터에 대한 기본 또는 모범 사례 컨피그레이션에 대해 설명합니다. 이러한 모든 필터는 인바운드 및 아웃바운드 이메일 정책 모두에서 사용할 수 있으며, 구성 및 필터링이 둘 다에서 권장됩니다. 보호 대부분은 인바운드, 아웃바운드 플로우 필터링으로 릴레이된 이메일 또는 내부 악의적인 공격에 대한 보호를 제공합니다.