

그레이메일 탐지 및 안전한 수신 거부 기능

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[그레이메일 탐지 및 안전한 수신 거부 기능](#)

소개

이 문서에서는 Cisco ESA(Email Security Appliance)에서 그레이메일 탐지 및 안전 수신 거부 기능이 작동하는 방식에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

그레이메일 탐지 및 안전한 수신 거부 기능

그레이메일 안전 수신 거부 프로세스 중에 최종 사용자가 로컬 웹 브라우저에 알림을 표시하는 경우가 있습니다.나중에 요청의 상태를 확인하려면 이 링크를 사용합니다.나중에 참조할 수 있도록 다음 링크와 유사한 링크를 즐겨찾기에 추가할 수 있습니다.



Safe Unsubscribe



Unsubscribing from *newsletters@cnet.online.com* is in progress.



If you want to check the status of your request at a later point, use this [link](#). For future reference, you can bookmark this link.

If you have any questions, please contact Joe Y. Phisherman, 515-555-5555, joe@bandt.com

위 예에 표시된 링크입니다.

```
http://184.94.241.137/us/status/1FOzUokNiIjWGPWfd56V8fUtDNzv_yVD9tB8h7bfo9rHKd9Z1mdbTEwEPwx2YmDBn1mYXQIh39_wEhpD9hcS3yzaAwogfuxcPzn8wvscfWrSd-NjGddCnCiCwBg8xD1HGRVQF5wXU8_8515PBsTAN1EmEOUE7YQGRvMoXA9mEQzR5n1jPBLfabt469Fzu2U1__TpLv1HxP1E7ZgK_wyxH92IbRNU9wur957bXQ5-Wi8c2-8Ht1sHLY2n9Z1zSB4mPznD-yAUVJrQ1D8V-ya0iZKHfk1tAdSBbk70xh7dMMHFpCMw9SzwDkKBhwX2o4JxKEyhT_Sj3GUPu7iePXglUHHfWoplE-yHYHfDWjQwffb0vfyKaVnbZw--S005mmacTLiBiKDkL5VdcCkxHywLVtrla36_qaxaKAR4xaduM390oCY8ABEfs_-21tw7L7I4cmzKHr9gWdVKuX-BhQ5QR2R5YTznH4gI0D1sF3ueve7jnt50YC6uL6R6tOmMaCe8N3FGexiVkBKntd5LNG5pVpQa0281U_ejq73YXHYH_urfup-X3eZoF0LSnzKhoThMxrv23jaLp5MWxAw-_NRGHA/188%3Amailto%3Aunsub-33334600008-echo3-64973c97bd6cc3e865982081e38e8d4d%40listunsub.bluehornet.come
```

수신 거부 서비스가 실시간으로 수신 거부 요청을 완료할 수 없는 경우, 이 링크는 최종 사용자가 수신 거부 요청의 상태를 나중에 확인할 수 있도록 상태 링크로 제공됩니다.

이 링크는 safe-unsubscribe.cisco.com(184.94.241.137)으로 이동하며, 이는 Akami 호스팅 IP 주소에 대한 포인터입니다.

```
$ dig safe-unsubscribe.cisco.com +short
safe-unsubscribe.ncs-cisco.com.akadns.net.
184.94.241.137
```

안전 수신 거부 서비스는 현재 다음 IP 중 하나에 매핑되어 있습니다.

- 184.94.241.137
- 208.90.58.189

또한 최종 사용자가 보안 프록시를 통해 URL 재작성(바이러스 전파 확산)에 의해 링크를 다시 쓸 수 있으며, URL은 먼저 도메인 secure-web.cisco.com(184.94.240.100)으로 리디렉션된 다음 safe-unsubscribe.cisco.com으로 리디렉션됩니다. 또한 Akami 호스팅 IP 주소에 대한 포인터입니다.

```
$ dig secure-web.cisco.com +short
secure-web.harpe-cisco.com.akadns.net.
184.94.240.100
```

원래 그레이메일 수신 거부 요청은 처음에 처리된 데이터 센터에 연결됩니다. 따라서 상태 요청을 초기 요청과 동일한 데이터 센터로 보내야 합니다.

두 서비스 모두, 그레이메일 안전 수신 거부 및 보안 프록시는 두 개의 개별 데이터 센터에서 호스팅됩니다. DNS(Domain Name System)를 통해 이중화와 고가용성을 통해 로드 밸런싱됩니다.

고객이 도메인 이름으로 IP 주소를 변경하도록 요청하는 경우 이를 달성할 수 없습니다. IP 주소 대신 도메인 이름을 갖는 클레임을 이행할 수 없습니다.

URL의 호스트 이름이 아닌 IP 주소를 통해 서비스 기능을 수행하는 경우 그레이메일 또는 안전 서브스크립션 취소에 아무런 기능적 영향이 없습니다.