신뢰할 수 있는 발신자가 안티스팸을 우회하도록 허용

목차

소개

이 문서에서는 신뢰할 수 있는 발신자가 안티스팸 검사를 우회하도록 허용하는 세부 사항과 보안 이메일 게이트웨이(이전의 Email Security Appliance)에서 동일한 옵션을 선택할 수 있는 다양한 방법에 대해 설명합니다.

ALLOWED_LIST 발신자 그룹에 발신자 호스트 이름/IP 주소 추가

이 발신자 그룹은 $TRUSTED 메일 플로우 정책을 사용하므로 신뢰하는 발신자를 ALLOWED_LIST 발신자 그룹에 추가합니다.ALLOWED_LIST 발신자 그룹의 구성원은 속도 제한의 대상이 되지 않으며, 이러한 발신자의 콘텐츠는 안티스팸 엔진에서 검사되지 않지만 안티바이러스에 의해 검사됩니다.

> **참고:**기본 컨피그레이션에서는 안티바이러스 검사가 활성화되지만 안티스팸이 꺼져 있습니다.

발신자가 안티스팸 검사를 우회하도록 허용하려면 HAT(Host Access Table)의 ALLOWED_LIST 발신자 그룹에 발신자를 추가합니다. GUI 또는 CLI를 통해 HAT를 구성할 수 있습니다.

GUI에서

1. **메일 정책** 탭을 선택합니다.
2. **Host Access Table** 섹션에서 **HAT Overview**를 선택합니다.
3. 오른쪽의 InboundMail **Listener가** 현재 선택되어 있는지 확인합니다.
4. Sender **Group** 열에서 ALLOWED_**LIST를 선택합니다**.
5. 페이지의 하단에서 Add Sender(발신자 추가) 버튼을 선택합니다.
6. 첫 번째 필드에 우회를 허용할 IP 또는 호스트 이름을 입력합니다.

항목 추가를 완료하면 **제출** 버튼을 선택합니다.변경 사항을 저장하려면 **Commit Changes(변경 사항** 커밋) 버튼을 선택해야 합니다.

CLI에서

```
example.com> listenerconfig
Currently configured listeners:
1. InboundMail (on PublicNet, 172.19.1.80) SMTP TCP Port 25 Public
2. OutboundMail (on PrivateNet, 172.19.2.80) SMTP TCP Port 25 Private
Choose the operation you want to perform:
- NEW - Create a new listener.
- EDIT - Modify a listener.
- DELETE - Remove a listener.
- SETUP - Change global settings.
[]> edit
Enter the name or number of the listener you wish to edit.
[]> 1
Name: InboundMail
Type: Public
Interface: PublicNet (172.19.1.80/24) TCP Port 25
Protocol: SMTP
Default Domain:
Max Concurrency: 1000 (TCP Queue: 50)
Domain Map: Disabled
TLS: No
SMTP Authentication: Disabled
Bounce Profile: Default
Use SenderBase For Reputation Filters and IP Profiling: Yes
Footer: None
LDAP: Off

Choose the operation you want to perform:
- NAME - Change the name of the listener.
- INTERFACE - Change the interface.
- LIMITS - Change the injection limits.
- SETUP - Configure general options.
- HOSTACCESS - Modify the Host Access Table.
- RCPTACCESS - Modify the Recipient Access Table.
- BOUNCECONFIG - Choose the bounce profile to use for messages injected on this
listener.
- MASQUERADE - Configure the Domain Masquerading Table.
- DOMAINMAP - Configure domain mappings.
[]> hostaccess
Default Policy Parameters
=========================
Allow TLS Connections: No
Allow SMTP Authentication: No
Require TLS To Offer SMTP authentication: No
Maximum Concurrency Per IP: 1,000
Maximum Message Size: 100M
Maximum Messages Per Connection: 1,000
Maximum Recipients Per Message: 1,000
Maximum Recipients Per Hour: Disabled
Use SenderBase For Flow Control: Yes
Spam Detection Enabled: Yes
Virus Detection Enabled: Yes
There are currently 4 policies defined.
There are currently 5 sender groups.
Choose the operation you want to perform:
- NEW - Create a new entry.
- EDIT - Modify an entry.
- DELETE - Remove an entry.
- MOVE - Move an entry.
- DEFAULT - Set the defaults.
- PRINT - Display the table.
```

```
- IMPORT - Import a table from a file.
- EXPORT - Export the table to a file.
- CLEAR - Remove all entries.
[]> edit
1. Edit Sender Group
2. Edit Policy
[1]> 1
Currently configured HAT sender groups:
1. ALLOWED_LIST (My trusted senders have no anti-spam scanning or rate limiting)
2. BLOCKED_LIST (Spammers are rejected)
3. SUSPECTLIST (Suspicious senders are throttled)
4. UNKNOWNLIST (Reviewed but undecided, continue normal acceptance)
5. (no name, first host = ALL) (Everyone else)
Enter the sender group number or name you wish to edit.
[]> 1

Choose the operation you want to perform:
- NEW - Add a new host.
- DELETE - Remove a host.
- MOVE - Reorder the hosts.
- POLICY - Change the policy settings and options.
- PRINT - Display the current definition.
- RENAME - Rename this sender group.
[]> new
Enter the hosts to add. CIDR addresses such as 10.1.1.0/24 are allowed. IP
address ranges such as 10.1.1.10-20 are allowed. IP subnets such as 10.2.3. are
allowed. Hostnames such as crm.example.com are allowed. Partial hostnames such
as .example.com are allowed.
Ranges of SenderBase Reputation scores such as SBRS[7.5:10.0] are allowed.
SenderBase Network Owner IDs such as SBO:12345 are allowed.
Remote blocklist queries such as dnslist[query.blocklist.example] are allowed.
Separate multiple hosts with commas
[]>
```

변경 사항을 저장하려면 **commit** 명령을 실행해야 합니다.

신뢰할 수 있는 메일 플로우 정책에서 안티스팸 및 안티바이러스 검사 검토

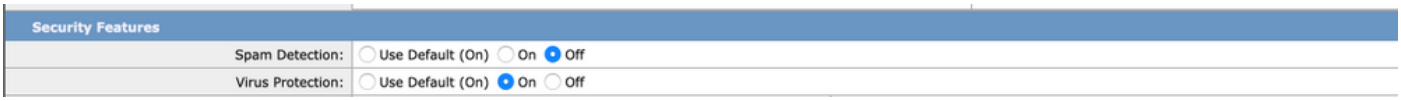
Trusted Sender의 경우 기본적으로 Trusted Present로 명명된 메일 플로우 정책이 있습니다 .Trusted Mail Flow Policy(신뢰할 수 있는 메일 플로우 정책)에는 Connection behavior of Accept(수락의 연결 동작)가 있습니다(수신 이메일의 다른 메일 플로우 정책의 동작과 유사).

발신자가 비즈니스 요구 사항에 대해 신뢰할 수 있는 경우 안티바이러스 및 안티스팸 검사를 비활성화하도록 선택할 수 있습니다.이렇게 하면 신뢰할 수 있는 소스에서 온 이메일이 아닌 이메일을 스캔하는 동안 두 스캐닝 엔진의 추가 처리 로드를 줄일 수 있습니다.

> **참고:**Anti-spam 및 Anti-virus 엔진이 비활성화되면 ESA에서 수신 이메일에 대한 스팸 또는 바이러스 관련 스캔을 건너뜁니다.이 작업은 신뢰할 수 있는 발신자에 대한 스캔을 건너뛰는 것이 위험하지 않다고 완전히 확신하는 경우에만 수행해야 합니다.

엔진을 비활성화할 수 있는 Option(옵션)은 Mail Flow Policies(메일 플로우 정책)의 Security Features(보안 기능) 탭에서 사용할 수 있습니다.동일한 경로의 경로는 **GUI > Mail Policies > Mail Flow Policies입니다**.TRUSTEDMail **flow 정책**을 클릭하고 아래로 스크롤하여 다음 페이지**의 Security Features(보안 기능)**로 이동합니다.

원하는 대로 수정한 후 변경 사항을 커밋해야 합니다.



신뢰할 수 있는 발신자를 허용 목록에 추가

최종 사용자 허용 목록 및 차단 목록은 최종 사용자가 만들고 스팸 방지 검사 전에 확인되는 데이터베이스에 저장됩니다. 각 최종 사용자는 스팸으로 항상 처리하거나 스팸으로 처리하지 않으려는 도메인, 하위 도메인 또는 전자 메일 주소를 식별할 수 있습니다.발신자 주소가 최종 사용자 허용 목록의 일부인 경우 안티스팸 검사를 건너뜁니다.

이 설정을 사용하면 최종 사용자가 안티스팸 검사를 제외하기 위한 요구 사항에 따라 발신자를 허용 목록에 추가할 수 있습니다.이메일 파이프라인의 안티바이러스 스캐닝 및 기타 스캔은 이 설정을 통해 그대로 유지되며 메일 정책의 컨피그레이션에 따라 계속 진행됩니다.이러한 설정은 최종 사용자가 발신자에 대한 스팸 검사를 면제해야 할 때마다 관리자의 참여를 줄여줍니다.

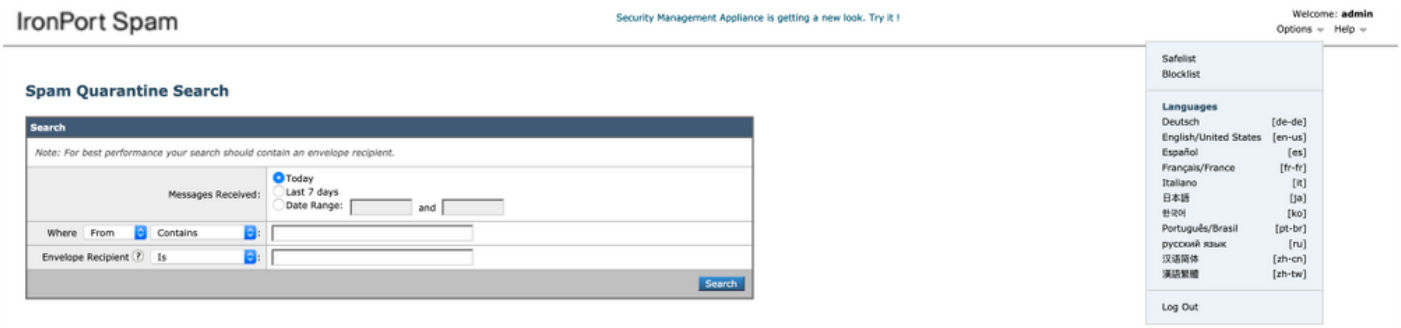
허용 목록의 경우 최종 사용자 및 최종 사용자 허용 목록/차단 목록에 대해 최종 사용자 격리 액세스를 활성화(ESA 또는 SMA에서 모두)로 설정해야 합니다. 이렇게 하면 스팸 쿼런틴 포털에 액세스할 수 있으며 격리된 이메일의 **릴리스/삭제**와 함께 허용 목록의 발신자 **추가/삭제**를 수행할 수도 있습니다.

최종 사용자 격리 액세스는 아래와 같이 활성화할 수 있습니다.

ESA:**GUI > Monitor > Spam Quarantine으로** 이동합니다. **최종 사용자 격리 액세스**에 대한 **라디오** 버튼**을** 체크 인합니다.요구 사항에 따라 액세스할 인증 방법(None/LDAP/SAML/IMAP 또는 POP)을 선택합니다. 이를 게시하고 최종 사용자 허용 목록/차단 목록을 활성화합니다.

SMA:**GUI > Centralized Services(중앙 집중식 서비스) > Spam Quarantine(스팸 격리)으로 이동합니다.최종 사용자 격리 액세스**에 대한 **라디오** 버튼**을 체크 인합니다**.요구 사항에 따라 액세스할 인증 방법(None/LDAP/SAML/IMAP 또는 POP)을 선택합니다. 이를 게시하고 최종 사용자 허용 목록/차단 목록을 활성화합니다.

활성화되면 최종 사용자가 스팸 쿼런틴 포털로 이동하면 오른쪽 상단의 드롭다운 옵션에서 선택한 대로 허용 목록을 **추가/수정할** 수 있습니다.



수신 메일 정책이 있는 신뢰할 수 있는 발신자

또한 Incoming Mail Policy(수신 메일 정책)에서 Trusted Sender(신뢰할 수 있는 발신자)를 추가하고 요구 사항에 따라 **Antivirus/Anti** spam(안티바이러스**/안티스팸** 검사)을 비활성화할 수 있습니다.선택한 대로 Trusted Senders/**Safe Senders** 등과 같은 이름으로 새로운 사용자 지정 메일 정책을 생성한 다음 도메인 이름 또는 발신자 이메일 주소와 같은 발신자 세부사항을 이 사용자 지정 정책에 추가할 수 있습니다.

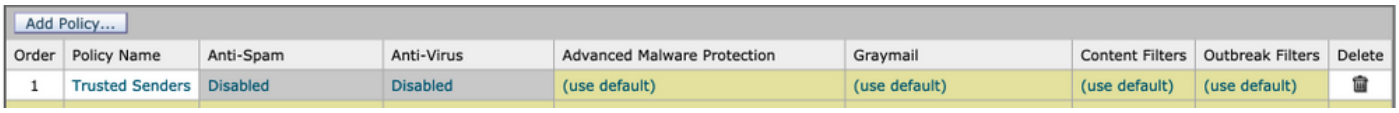
필요한 추가 후 정책을 제출하면 안티스팸 또는 **안티바이러스**의 열을 클릭하고 후속 페이지에서 Disable(비활성화)을 **선택합니다**.

이 설정을 통해 이 메일 정책에 추가된 신뢰할 수 있는 발신자 도메인 또는 이메일 주소는 안티스팸 또는 안티바이러스 스캔에서 제외됩니다.

> **참고:**Anti-spam 및 Anti-virus 엔진이 비활성화되면 이 맞춤형 메일 정책을 통해 처리된 ESA에서 수신 이메일에 대한 스팸 또는 바이러스 관련 스캔을 건너뜁니다.이 작업은 신뢰할 수 있는 발신자에 대한 스캔을 건너뛰는 것이 위험하지 않다고 완전히 확신하는 경우에만 수행해야 합니다.

맞춤형 메일 정책은 ESA **GUI > Mail Policies > Incoming Mail Policies > Add Policy**에서 생성할 수 있습니다.선택 사항에 따라 정책 이름을 입력 한 다음 **Add User를 선택 합니다**.다음 발신자에 대한 라디오 버튼을 **선택합니다.** 상자에 필수 도메인 또는 이메일 주소를 추가하고 확인을 **클릭합니다**.

메일 정책 생성 후 비즈니스 요구 사항에 따라 안티바이러스 및 안티스팸 스캔을 비활성화하도록 선택할 수 있습니다.다음은 예제 스크린샷입니다.


Add Policy...

Order	Policy Name	Anti-Spam	Anti-Virus	Advanced Malware Protection	Graymail	Content Filters	Outbreak Filters	Delete
1	Trusted Senders	Disabled	Disabled	(use default)	(use default)	(use default)	(use default)	

관련 정보

- Cisco Email Security Appliance – 엔드 유저 가이드
- 기술 지원 및 문서 – Cisco Systems