ESA에서 악의적인 발신자 또는 문제 발신자 차단

목차

소개

이 문서에서는 Cisco ESA(Email Security Appliance)의 차단 목록에 악성 IP 주소 또는 도메인 이름을 추가하는 방법에 대해 설명합니다.

악의적인 발신자 또는 문제 발신자 차단

발신자를 차단하는 가장 쉬운 방법은 ESA HAT(Host Access Table) 내의 BLOCKED_LIST 발신자 그룹에 IP 주소 또는 도메인 이름을 추가하는 것입니다. BLOCKED_LIST 발신자 그룹은 액세스 규칙이 REJECT인 $BLOCKED 메일 플로우 정책을 사용합니다.

참고: IP 주소 또는 도메인 이름은 발신 메일 서버에서 가져온 것입니다. 발신 메일 서버의 IP 주소는 메시지 추적에서 캡처할 수도 있고 알 수 없는 경우 메일 로그에서 캡처할 수도 있습니다.

GUI를 통해 발신자 차단

GUI를 통해 발신자를 차단하려면 다음 단계를 완료하십시오.

1. Mail Policies(메일 정책)를 클릭합니다.
2. HAT Overview(HAT 개요)를 선택합니다.
3. ESA에 여러 리스너가 구성된 경우 InboundMail 리스너가 현재 선택되어 있는지 확인합니다.
4. Sender Group 열에서 BLOCKED_LIST를 선택합니다.
5. 발신인 추가...를 클릭합니다.
6. 차단할 IP 주소 또는 도메인 이름을 입력합니다. 다음 형식을 사용할 수 있습니다.
    - IPv6 주소(예: 2001:420:80:1::5)
    - IPv6 서브넷(예: 2001:db8::/32)
    - IPv4 주소(예: 10.1.1.0)

- IPv4 서브넷(예: 10.1.1.0/24 또는 10.2.3.1)
- IPv4 및 IPv6 주소 범위(예: 10.1.1.10-20, 10.1.1-5 또는 2001::2-2001::10)
- 호스트 이름(예: example.com)
- 부분 호스트 이름(예: .example.com)

7. 항목을 추가한 후 제출을 클릭합니다.

8. 컨피그레이션 변경을 완료하려면 Commit Changes를 클릭합니다.

CLI를 통해 발신자 차단

다음은 CLI를 통해 도메인 이름 및 IP 주소로 발신자를 차단하는 방법을 보여 주는 예입니다.

```
<#root>

myesa.local>

listenerconfig



Currently configured listeners:
1. Bidirectional (on Management, 192.168.1.x) SMTP TCP Port 25 Public

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: Bidirectional
Type: Public
Interface: Management (192.168.1.x/24) TCP Port 25
Protocol: SMTP
Default Domain: example.com
Max Concurrent Connections: 50 (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
Heading: None
SMTP Call-Ahead: Disabled
LDAP: Off
```

```
Choose the operation you want to perform:
- NAME - Change the name of the listener.
- INTERFACE - Change the interface.
- CERTIFICATE - Choose the certificate.
- 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.
- LDAPACCEPT - Configure an LDAP query to determine whether a recipient address
  should be accepted or bounced/dropped.
- LDAPGROUP - Configure an LDAP query to determine whether a sender or recipient
  is in a specified group.
[]>
```

hostaccess

```
Default Policy Parameters
==========================
Maximum Message Size: 10M
Maximum Number Of Concurrent Connections From A Single IP: 10
Maximum Number Of Messages Per Connection: 10
Maximum Number Of Recipients Per Message: 50
Directory Harvest Attack Prevention: Enabled
Maximum Number Of Invalid Recipients Per Hour: 25
Maximum Number Of Recipients Per Hour: Disabled
Maximum Number of Recipients per Envelope Sender: Disabled
Use SenderBase for Flow Control: Yes
Allow TLS Connections: No
Allow SMTP Authentication: No
Require TLS To Offer SMTP authentication: No
DKIM/DomainKeys Signing Enabled: No
DKIM Verification Enabled: No
S/MIME Public Key Harvesting Enabled: Yes
S/MIME Decryption/Verification Enabled: Yes
SPF/SIDF Verification Enabled: Yes
 Conformance Level: SIDF compatible
 Downgrade PRA verification: No
 Do HELO test: Yes
 SMTP actions:
 For HELO Identity: Accept
 For MAIL FROM Identity: Accept
 For PRA Identity: Accept
 Verification timeout: 40
DMARC Verification Enabled: No
Envelope Sender DNS Verification Enabled: No
Domain Exception Table Enabled: Yes

There are currently 6 policies defined.
There are currently 7 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.
- RESET - Remove senders and set policies to system default.
[]>
```

edit

```
1. Edit Sender Group
2. Edit Policy
[1]>
```

1

```
Currently configured HAT sender groups:
1. ALLOWSPOOF
2. MY_INBOUND_RELAY
3. WHITELIST (My trusted senders have no anti-spam scanning or rate limiting)
4. BLOCKED_LIST (Spammers are rejected)
5. SUSPECTLIST (Suspicious senders are throttled)
6. UNKNOWNLIST (Reviewed but undecided, continue normal acceptance)
7. (no name, first host = ALL) (Everyone else)
Enter the sender group number or name you wish to edit.
[]>
```

4

```
Choose the operation you want to perform:
- NEW - Add a new host.
- DELETE - Remove a host.
- POLICY - Change the policy settings and options.
- PRINT - Display the current definition.
- RENAME - Rename this sender group.
[]>
```

new

```
Enter the senders to add to this sender group. A sender group entry can be
any of the following:
- an IP address
- a CIDR address such as 10.1.1.0/24 or 2001::0/64
- an IP range such as 10.1.1.10-20, 10.1.1-5 or 2001:db8::1-2001:db8::10.
- an IP subnet such as 10.2.3.
- a hostname such as crm.example.com
- a partial hostname such as .example.com
- a range of SenderBase Reputation Scores in the form SBRS[7.5:10.0]
- a SenderBase Network Owner ID in the form SBO:12345
- a remote blocklist query in the form dnslist[query.blocklist.example]
Separate multiple entries with commas.
[]>
```

badhost.example.org, 10.1.1.10

참고: 기본 CLI에서 변경한 모든 사항을 커밋해야 합니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.