

ESAでの悪意のある送信者または問題のある送信者のブロック

内容

[はじめに](#)

[悪意のある送信者または問題のある送信者のブロック](#)

[GUIを使用した送信者のブロック](#)

[CLIを使用した送信者のブロック](#)

はじめに

このドキュメントでは、Cisco Eメールセキュリティアプライアンス(ESA)のブロックリストに悪意のあるIPアドレスまたはドメイン名を追加する方法について説明します。

悪意のある送信者または問題のある送信者のブロック

送信者をブロックする最も簡単な方法は、IPアドレスまたはドメイン名をESAホストアクセステーブル(HAT)内のBLOCKED_LIST送信者グループに追加することです。BLOCKED_LIST送信者グループは、アクセスルールがREJECTである\$BLOCKEDメールフローポリシーを使用します。

 注:IPアドレスまたはドメイン名は、送信側のメールサーバからのものです。送信元のメールサーバからのIPアドレスは、メッセージトラッキングからキャプチャするか、不明な場合はメールログでキャプチャできます。

GUIを使用した送信者のブロック

GUIを介して送信者をブロックするには、次の手順を実行します。

1. Mail Policiesをクリックします。
2. HAT Overviewを選択します。
3. ESAで複数のリスナーが設定されている場合は、InboundMailリスナーが現在選択されていることを確認します。
4. Sender GroupカラムからBLOCKED_LISTを選択します。
5. Add Sender...をクリックします。
6. ブロックするIPアドレスまたはドメイン名を入力します。次の形式を使用できます。

- IPv6アドレス(2001:420:80:1::5など)
- IPv6サブネット(2001:db8::/32など)
- IPv4アドレス(10.1.1.0など)
- IPv4サブネット(10.1.1.0/24や10.2.3.1など)
- IPv4およびIPv6アドレスの範囲(10.1.1.10-20、10.1.1-5、2001::2-2001::10など)
- ホスト名(example.comなど)
- ホスト名の一部(.example.comなど)

7. エントリを追加したら、Submitをクリックします。

8. Commit Changesをクリックして、設定の変更を完了します。

CLIを使用した送信者のブロック

次の例は、CLIを使用してドメイン名とIPアドレスで送信者をブロックする方法を示しています。

```
<#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

 注：メインCLIから行ったすべての変更をコミットすることを忘れないでください。

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。