ESA で悪意のある（または問題となる）送信者をブラックリストに載せる

目次

概要

この資料に Cisco E メール セキュリティ アプライアンス（ESA）のブラックリストに悪意のある IP アドレスかドメイン名を追加する方法を記述されています。

悪意のあるまたは問題送信側をブラックリストに載せて下さい

送信側をブラックリストに載せる最も簡単な方法は ESA ホスト アクセス 表（帽子）内のブラックリスト送信側 グループへ IP アドレスかドメイン名を追加することです。 ブラックリスト送信側 グループは $BLOCKED メール フロー ポリシーを使用します、リジェクトのアクセス規則がある。

> **注:** IP アドレスかドメイン名は送信 メール サーバからあります。 既知 送信 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 することができますまたはメールで記録 します。

GUI によって送信側をブラックリストに載せて下さい

GUI によって送信側をブラックリストに載せるためにこれらのステップを完了して下さい:

1. **メール「Policies」を**クリックして下さい。
2. **帽子外観を**選択して下さい。
3. ESA で設定される複数のリスナーがある場合 *InboundMail* リスナーが現在選択されるようにして下さい。
4. *送信側 Group カラム*から**ブラックリストを**選択して下さい。

5. 『Add』 をクリック して下さい**送信側を....**

6. ブラックリストに載せたいドメイン・ネームか IP アドレスを入力して下さい。 これらの形式は許可されます:

   2001:420:80:1::5 のような IPv6 アドレス、*2001:db8::/32* のような IPv6 サブネット、*10.1.1.0* のような IPv4 アドレス、*10.1.1.0/24* か *10.2.3.1* のような IPv4 サブネット、*10.1.1.10-20*、*10.1.1-5*、か *2001::2-2001::10* のような IPv4 および IPv6 アドレス範囲、*example.com* のようなホスト名、*.example.com* のような部分的なホスト名、

7. エントリを追加した後『SUBMIT』 をクリック して下さい。

8. コンフィギュレーション変更を完了するために**保存します変更を**クリックして下さい。

CLI によって送信側をブラックリストに載せて下さい

ドメイン名によって送信側および CLI によって IP アドレスをブラックリストに載せる方法を示す例はここにあります:

```
myesa.local> listenerconfig

Currently configured listeners:
1. Bidirectional (on Management, 172.18.249.222) 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 (172.18.249.222/24) 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. BLACKLIST (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 blacklist query in the form dnslist[query.blacklist.example]
Separate multiple entries with commas.
[]> badhost.example.org, 10.1.1.10
```

注: 主要な CLI から行うありとあらゆる変更を**保存することを**忘れないようにして下さい。