

列入黑名单在ESA的一有恶意或问题发送方

目录

[简介](#)

[列入黑名单一有恶意或问题发送方](#)

[通过GUI列入黑名单发送方](#)

[通过CLI列入黑名单发送方](#)

简介

本文如何描述添加一个有恶意的IP地址或域名到您的在思科电子邮件安全工具(ESA)的黑名单。

列入黑名单有恶意或问题发送方

列入黑名单发送方的简便的方法是添加他们的IP地址或域名给在ESA主机访问表(帽子)内的黑名单发送方组。黑名单发送方组使用\$BLOCKED邮件流量策略，有拒绝一个访问规则。

注意：IP地址或域名是从发送的邮件服务器。从发送的邮件服务器的IP地址可以捕获从消息跟踪或在邮件日志，如果没已知。

通过GUI列入黑名单发送方

完成这些步骤为了通过GUI列入黑名单发送方：

1. 点击邮件“Policies”。
2. 选择帽子概述。
3. 如果有在ESA配置的广泛监听程序，请保证*InboundMail*监听程序当前选择。
4. 选择从发送方组列的**黑名单**。
5. 单击添加发送方....
6. 输入您希望列入黑名单的IP地址或域名。这些格式允许：

IPv6地址，例如2001:420:80:1::5IPv6子网，例如2001:db8::/32IPv4地址，例如10.1.1.0IPv4子网，例如10.1.1.0/24或10.2.3.1IPv4和IPv6地址范围，例如10.1.1.10-20，10.1.1-5或者2001::2-2001::10主机名，例如example.com部分主机名，例如.example.com

7. 在您添加了您的条目后，请单击**提交**。

8. 单击**进行更改**为了完成配置更改。

通过CLI列入黑名单发送方

这是显示如何由域名和IP地址列入黑名单发送方通过CLI的示例：

```
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**

注意：切记确认由主CLI做的任意变动。