

阻止ESA上的恶意或问题发送程序

目录

[简介](#)

[阻止恶意发件人或问题发件人](#)

[通过GUI阻止发件人](#)


[通过CLI阻止发件人](#)

简介

本文档介绍如何向思科邮件安全设备(ESA)上的阻止列表添加恶意IP地址或域名。

阻止恶意发件人或问题发件人

阻止发件人的最简单方法是将其IP地址或域名添加到ESA主机访问表(HAT)中的BLOCKED_LIST发件人组。BLOCKED_LIST发件人组使用\$BLOCKED邮件流策略，该策略的访问规则为REJECT。

 注:IP地址或域名来自发送邮件服务器。如果不知道发送邮件服务器的IP地址，可以从邮件跟踪或邮件日志中捕获该地址。

通过GUI阻止发件人

要通过GUI阻止发件人，请完成以下步骤：

1. 单击邮件策略。
2. 选择HAT概述。
3. 如果在ESA上配置了多个侦听程序，请确保当前已选择InboundMail侦听程序。
4. 从Sender Group列中选择BLOCKED_LIST。
5. 单击Add Sender...
6. 输入要阻止的IP地址或域名。允许以下格式：
 - IPv6地址，例如2001:420:80:1::5
 - IPv6子网，例如2001:db8::/32
 - IPv4地址，例如10.1.1.0
 - IPv4子网，例如10.1.1.0/24或10.2.3.1
 - IPv4和IPv6地址范围，例如10.1.1.10-20、10.1.1-5或2001::2-2001::10
 - 主机名，例如example.com

- 部分主机名，例如.example.com

7. 添加条目后，单击Submit。

8. 单击Commit Changes以完成配置更改。

通过CLI阻止发件人

以下示例展示如何通过CLI按域名和IP地址阻止发件人：

```
<#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：请记住提交从主CLI所做的所有更改。

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。