How do I prevent my ESA from being used as an open relay?

Document ID: 117976

Contributed by John Yu and Enrico Werner, Cisco TAC Engineers.
Jul 17, 2014

Contents

Question

How do I prevent my ESA from being used as an open relay?

To secure your ESA from being used as an open relay, make sure that you have specified the recipient domain(s) in the Recipient Access Table (RAT) of your Public listener(s) and that the "ALL" entry is configured to "Reject". RAT entries can be added via the GUI, on the Mail Policies tab. Below is an example showing how to add a domain, "example.com" to the RAT via the CLI.

```
mail.example.com> listenerconfig
Currently configured listeners:
1. InboundMail (on PublicNet, 172.19.1.80) SMTP TCP Port 25 Public
2. OutboundMail (on PrivateNet, 172.19.2.80) SMTP TCP Port 25 Private
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: InboundMail
Type: Public
Interface: PublicNet (172.19.1.80/24) TCP Port 25
Protocol: SMTP
Default Domain:
Max Concurrency: 1000 (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
LDAP: Off

Choose the operation you want to perform:
- NAME - Change the name of the listener.
- INTERFACE - Change the interface.
- 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.
```

```
[]> rcptaccess
Recipient Access Table
There are currently 1 recipients.
Default Access: REJECT<
Choose the operation you want to perform:
- NEW - Create a new entry.
- EDIT - Modify an entry.
- IMPORT - Import a table from a file.
- EXPORT - Export the table to a file.
[]> new
Enter the recipient address for this entry.
Hostnames such as "example.com" and "[1.2.3.4]" are allowed.
Partial hostnames such as ".example.com" are allowed.
Usernames such as "postmaster@" are allowed.
Full email addresses such as "joe@example.com" or "joe@[1.2.3.4]" are allowed.
Separate multiple addresses with commas.
[]> example.com
Select the action to apply to this address:
1. Accept
2. Reject
[1]>
Would you like to specify a custom SMTP response? [N]>
Would you like to bypass receiving control for this entry? [N]>
Recipient Access Table
There are currently 2 recipients.
Default Access: REJECT
Choose the operation you want to perform:
- NEW - Create a new entry.
- EDIT - Modify an entry.
- DELETE - Remove an entry.
- PRINT - Display all entries.
- IMPORT - Import a table from a file.
- EXPORT - Export the table to a file.
- CLEAR - Remove all entries.
[]> print
ironport.com  ACCEPT
ALL  REJECT
```

Notice that the "ALL" entry is configured to "REJECT". This entry causes the system to reject messages from any host that is not specifically configured to be accepted.

Updated: Jul 17, 2014 Document ID: 117976