Troubleshooting Unwanted Outbound Emails

Contents

Introduction

Prerequisites

- Components Used

Troubleshoot

- Workqueue Checks
- Sender or Subject of Emails in the Workqueue is Known
- Delivery QueueCheck
- Proactive Monitoring and Action

Related Information

Introduction

This guide helps you investigate and resolve incidents where your ESA is sending unexpected or unwanted outbound emails. It outlines practical steps and commands to identify the source and stop the behavior.

Prerequisites

Components Used

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Troubleshoot

If you know which account is sending spam, it is recommended to immediately lock down that account. If the account is not known, conduct an investigation using the ESA to identify the responsible account and then proceed to lock it down.

Workqueue Checks

If you observe a high number of emails in the workqueue and the incoming email rate significantly exceeds the outgoing rate, this indicates an issue with the workqueue. You can use the `workqueue` command to review the status and details.

```
<#root>

C370.lab>

workqueue status


Status as of:  Thu Feb 06 12:48:02 2014 GMT
Status:        Operational
```

```
Messages:
48654


C370.lab>
workqueue rate 5


Type Ctrl-C to return to the main prompt.

Time      Pending    In   Out
12:48:04    48654
48

 2
12:48:09    48700
31

 0
```

Sender or Subject of Emails in the Workqueue is Known

If you know the sender or subject of the emails affecting the workqueue, it is recommended to use a message filter. Applying a message filter allows the ESA to process and take action on these emails earlier in the workqueue, making their removal more efficient.

You can use the following filter to accomplish this:

```
<#root>

C370.lab>
filters



Choose the operation you want to perform:
- NEW - Create a new filter.
- DELETE - Remove a filter.
- IMPORT - Import a filter script from a file.
- EXPORT - Export filters to a file
- MOVE - Move a filter to a different position.
- SET - Set a filter attribute.
- LIST - List the filters.
- DETAIL - Get detailed information on the filters.
- LOGCONFIG - Configure log subscriptions used by filters.
- ROLLOVERNOW - Roll over a filter log file.
[]>
new


Enter filter script.  Enter '.' on its own line to end.


FilterName:
if (mail-from == 'user@example.com')
```

```
{
drop();
}
.
```

OR

```
FilterName:
if (subject == "^SUBJECT NAME$")
{
drop();
}
.
```

Delivery Queue Check

The **tophosts** command displays the hosts currently affected. In a live environment, you may notice that a recipient host (such as **example.com**) has a large number of active recipients in its delivery queue, indicating impact.

<#root>

C370.lab>

tophosts

```
Sort results by:

1. Active Recipients
2. Connections Out
3. Delivered Recipients
4. Hard Bounced Recipients
5. Soft Bounced Events
[1]>  1

Status as of:                   Thu Feb 06 12:52:17 2014 GMT
Hosts marked with '*' were down as of the last delivery attempt.

                                Active  Conn.     Deliv.       Soft       Hard
#   Recipient Host              Recip.    Out     Recip.    Bounced    Bounced

1
example.com           321550     50        440      75568       8984

2   the.euq.queue                    0      0          0          0          0
3   the.euq.release.queue            0      0          0          0          0
```

If the impacted host is an unfamiliar recipient domain and you need more information before removing all emails, you can use the commands **showrecipients**, **showmessage**, and **deleterecipients**. The **showrecipients**command provides details such as the Message ID (MID), message size, number of delivery attempts, envelope sender, envelope recipient(s), and the subject of the email.

<#root>

C370.lab>

showrecipients

Please select how you would like to show messages:
1. By recipient host.
2. By Envelope From address.
3. All.
[1]>

1

Please enter the hostname for the messages you wish to show.
>

example.com

In the event that the suspected MID in the delivery queue looks legitimate, you can use the **showmessage** command in order to display the message source before you take any action.

<#root>

C370.lab>

showmessage

Enter the MID to show.
[]>

123456789

Once the emails are confirmed as spam, you can remove them using the **deleterecipients**command. This command offers three options for deleting emails from the delivery queue: by envelope sender, by recipient host, or all emails in the delivery queue.

<#root>

C370.lab>

deleterecipients

Please select how you would like to delete messages:
1. By recipient host.
2. By Envelope From address.
3. All.
[1]>

2

Please enter the Envelope From address for the messages you wish to delete.
[]>

```
user@example.com
```

Proactive Monitoring and Action

Header Repeats Rule

The Header Repeats rule evaluates as **true** when, within a one-hour period, a specified number of messages are detected that meet either of the following criteria:

- They have the same subject.
- They are from the same envelope sender.

The rule syntax is: header-repeats(<target>, <threshold> [, <direction>])

To use this rule, log in to the CLI and deploy the appropriate filter. For example, you can create a filter to drop emails or notify an administrator once the defined threshold is reached.

```
<#root>

C370.lab>

filters



Choose the operation you want to perform:
- NEW - Create a new filter.
- DELETE - Remove a filter.
- IMPORT - Import a filter script from a file.
- EXPORT - Export filters to a file
- MOVE - Move a filter to a different position.
- SET - Set a filter attribute.
- LIST - List the filters.
- DETAIL - Get detailed information on the filters.
- LOGCONFIG - Configure log subscriptions used by filters.
- ROLLOVERNOW - Roll over a filter log file.
[]>

new


Enter filter script.  Enter '.' on its own line to end.



FilterName:
if header-repeats('mail-from',1000,'outgoing')
{
drop();
}
.

OR


FilterName:
```

```
if header-repeats('subject',1000,'outgoing')
{
notify('admin@example.com');
}
.
```

Related Information

- **Manually Remove Recipients from the Delivery Queue**
- **Technical Support & Documentation - Cisco Systems**