How do I troubleshoot why a message was not received by the Cisco Secure Email Gateway?

Contents

Introduction

This document describes why a message is not recevied by the Cisco Secure Email Gateway and options to troubleshoot the issue.

How do I troubleshoot why a message was not received by the Cisco Secure Email Gateway?

In order to troubleshoot message reception, you need to know the IP addresses used to send mail by the organization that sent the mail. Usually, the most accurate way to obtain this information is to contact the sender organization's mail administrator. In the absence of this resource, you can use one of these other options:

- **SenderBase** - If you enter a domain in the search box at http://www.senderbase.org, you will receive a list of known sending IP addresses for that domain.
- **Mail Logs** - If you have successfully received mail from the domain in the past, you can look in mail logs for one of those successful deliveries.
- **Domain Name System (DNS)** - You can look up the mail exchanger (MX) records for the domain. Most smaller organizations use the same inbound and outbound servers. For larger or more segmented organizations, this option will not likely reveal the needed information.

Once you know the IP addresses, you will need to search the mail logs. The grep utility is a good tool for this purpose. If you run Microsoft Windows, you can use Find in Word Pad or Notepad or download a grep utility from the Internet. Unix and Mac OSX have grep built in and can be accessed from a shell. The grep command line will look like this, where '10.2.3.4' is the IP address to search for:

```
host> grep '10.2.3.4' file.log
```

If the sender's server successfully connects to your server, you will see a line similar to this example when you search for their IP address(es):

```
Wed Feb  2 23:43:11 2008 Info: New SMTP ICID 6 interface Management (10.0.0.1)
address 10.2.3.4 reverse dns host test.ironport.com verified no
```

You can then search for all the lines that involve the Incoming Connection ID (ICID). The lines you find will tell you if they sent From information, if they sent To Information, and the Message IDs (MIDs) linked with the connection. A search on the MID(s) will show you if the message was

accepted by the system, the scan results, and whether delivery was attempted.

Another troubleshooting tool available is the **Injection Debug Logs**. You will need the IP address of the sending server(s) first. Once you have this, use the **logconfig** commands and select this log type. Once the log is configured and committed, you can have the user send a test message and (assuming their server connects to your Cisco Secure Email Gateway) the Cisco Secure Email Gateway will log the entire SMTP conversation. This allows you to see the point of breakdown in communication.

If there are still no connections and thus no messages received, the next step is to have the sending servers administrator check their logs and/or use telnet to manually test sending a message from the mail server. This will mimic the server attempting to deliver to your Cisco Secure Email Gateway and your Cisco Secure Email Gateway will react the same as if the sending servers application sent it.

If the test goes through, but the server application fails when it tries to send mail, this indicates delivery issues on the remote server. The remote server administrator will need to review the logs in order to diagnose the errors.

One common cause of delayed or failed receipt of messages is that the sending server's IP address does not have reverse DNS configured properly, which causes a long delay (30+ seconds) for the Cisco Secure Email Gateway to provide an SMTP banner. Some server applications will reach their configured timeout and close the session before it sends mail because of the delayed banner. The solution in this case is to extend the timeout or implement reverse DNS. The recommended action is to implement reverse DNS for all mail servers that deliver to other Internet mail servers. It is considered proper Internet etiquette and allows mail servers to confirm the identity of the server at a very basic level.