Integrating Secure Email Gateway with Threat Defense

This chapter contains the following sections:

- Overview of Threat Defense Connector, on page 1
- How to Configure Email Gateway to use Threat Defense Conncetor, on page 2
- Setting up the Threat Defense Portal to Receive Messages from Secure Email Cloud Gateway, on page 3
- Obtaining the Message Intake Address, on page 3
- Enabling Threat Defense Connector on Email Cloud Gateway, on page 3
- Disabling Threat Defense Connector on Email Cloud Gateway, on page 3
- Threat Defense Connector and Clusters, on page 4
- Monitoring Threat Defense Connector Reports, on page 4
- Viewing Logs, on page 4

Overview of Threat Defense Connector

The Threat Defense Connector client connects the Secure Email Cloud Gateway with the Secure Email Threat Defense to scan messages for Advanced Phishing and Spoofing. The ability to perform cloud-based advanced threat scanning helps an organization to:

- Get an advanced phishing and spoofing solution, and
- Avail security solutions to ever-changing phishing problems much faster than ever before.

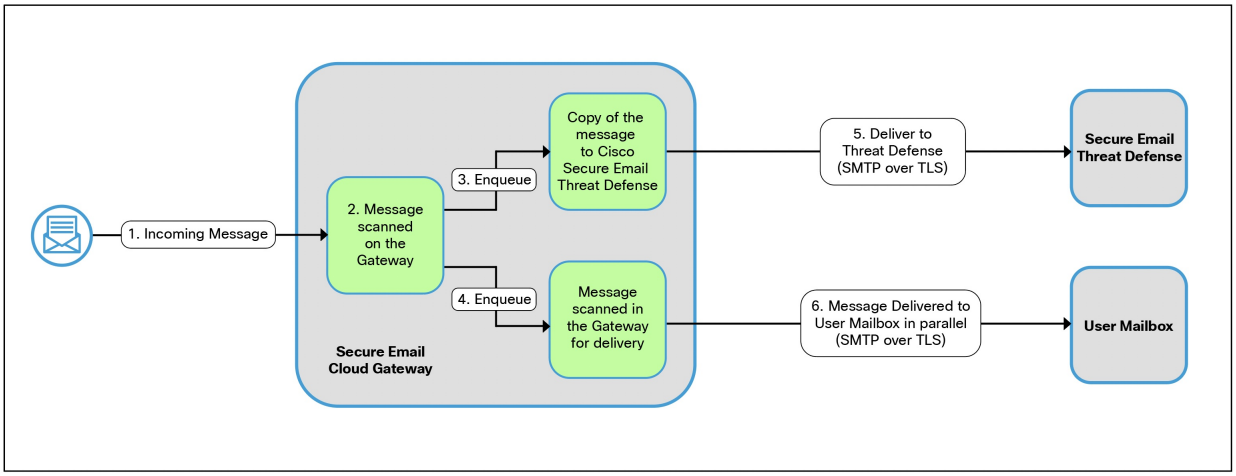
When you configure the Threat Defense Connector, the Secure Email Cloud Gateway sends a copy of the actual message as an attachment to the Threat Defense portal's message intake address in journaled format.

Once a message is scanned by all the scanning engines in the Secure Email Cloud Gateway and the message is safe to be delivered, the message is duplicated. A copy of the message is queued to be sent as an attachment in RFC 822 format to the Secure Email Threat Defense for advanced scanning. The original message gets delivered to the original recipient.

Email Cloud Gateway sends emails that are meant for advanced threat scanning over the standard SMTP interface using a minimum of TLS 1.2 as required on the Secure Email Threat Defense for the SMTP conversation. Threat Defense scans the messages and appropriate remediation action is taken on the message originally delivered to the user mailbox.

Note Advanced threat scanning using Threat Defense Connector is applicable only for incoming messages.

Figure 1: Overview of Threat Defense Connector



Related Topics

- How to Configure Email Gateway to use Threat Defense Conncetor, on page 2

How to Configure Email Gateway to use Threat Defense Conncetor

Perform these steps in order:

Steps	Do This	More Information
Step 1	[On Secure Email Threat Defense] Set up the Secure Email Threat Defense portal to receive emails from Secure Email Cloud Gateway.	Set up Secure Email Threat Defense on Cisco Secure Email Threat Defense User Guide.
Step 2	Obtain the message intake address from the Secure Email Threat Defense portal.	Cisco Secure Email Threat Defense User Guide.
Step 3	Enable and configure Threat Defense Connector on Secure Email Cloud Gateway	Enabling Threat Defense Connector on Email Cloud Gateway, on page 3

Setting up the Threat Defense Portal to Receive Messages from Secure Email Cloud Gateway

As an email administrator, you need to set up the Secure Email Threat Defense to receive messages from Secure Email Cloud Gateway. For more information, see the Set up Secure Email Threat Defense chapter on the Secure Email Threat Defense User Guide.

Obtaining the Message Intake Address

Your message intake address is shown on the Secure Email Threat Defense setup page. If you need to find it after your initial setup, you can locate it on the **Settings** (gear icon) > **Administration** > **Business** page in the Account Details section. For more information, see Secure Email Threat Defense FAQ.

Enabling Threat Defense Connector on Email Cloud Gateway

Before you begin

Make sure that you have received the message intake address from Secure Email Threat Defense. Also, ensure that mail deliveries to this domain and recipient address are allowed.

Note If you use custom SMTP routes for mail deliveries, make sure that you use DNS for deliveries to the message intake address domain. For example, by using "USEDNS" for the domain in the SMTP Routes.

Procedure

Step 1 Click **Security Services** > **Threat Defense Connector**.

Step 2 Click **Enable**.

Step 3 Select the **Enable Threat Defense Connector** checkbox.

Step 4 Enter the message intake address retrieved from the Email Threat Defense portal.

Step 5 Click **Submit** and commit your changes.

Disabling Threat Defense Connector on Email Cloud Gateway

Procedure

Step 1 Click **Security Services** > **Threat Defense Connector**.

Step 2 Click **Edit Global Settings**.

Step 3 Clear the **Enable Threat Defense Connector** checkbox.

Step 4 Click **Submit** and commit your changes.

Threat Defense Connector and Clusters

If you use centralized management, you can enable the Threat Defense Connector at the cluster, group, and machine levels.

Note When you disable the Threat Defense Connector at the machine level, the same is disabled on the group and cluster levels.

Monitoring Threat Defense Connector Reports

You need to log in to Cisco Secure Threat Defense portal for viewing advanced scanning reports of Threat Defense Connector. For more information, see Cisco Secure Email Threat Defense User Guide.

You can view the the delivery status of outgoing emails under **Monitor** > **Delivery Status**. The Delivery Status Page provides monitoring information about email operations relating to a specific recipient domain. When Threat Defense Connector is enabled, you can view the delivery status of emails to the message intake address under the **the.tdc.queue** destination domain.

Related Topics

- Delivery Status Page

Viewing Logs

The Threat Defense Connector information is posted to the Mail Logs with a prefix 'TDC'.

Examples of Threat Defense Connector Log Entries

- Message Delivery Failed - TLS Error, on page 4

Message Delivery Failed - TLS Error

In this example, the log shows a message that was not delivered because of TLS error when communicating with Threat Defense.

```
17 Aug 2022 05:52:04 (GMT +00:00) Message 3 queued for delivery.
17 Aug 2022 05:52:04 (GMT +00:00) (DCID O) Delivery started for message 3 to
astra_victim@astra-cs.com.
17 Aug 2022 05:52:04 (GMT +00:00) (CID O) Delivery details: Message 3 sent to astra
victim@astra-cs.com
17 Aug 2022 05:52:04 (GMT +00:00) Incoming connection (ICID 3) lost.
17 Aug 2022 05:52:04 (GMT +00:00) Message 3 to astra_victim@astra-cs.com received remote
SMTP response "/dev/null'
```

```
17 Aug 2022 05:52:04 (GMT +00:00) TDC: Message 4 delivery failed to Cisco Secure Email
Threat Defense: TLS Error.
```

Solution

To investigate further and fix this error, contact Cisco Technical Assistance Center (TAC).