将 Cisco Secure Email Gateway 与威胁防御集成

本章包含以下部分：

威胁防御连接器概述

威胁防御连接器客户端将安全邮件云网关与安全电子邮件威胁防御连接起来，以扫描邮件是否存在高级网络钓鱼和欺骗行为。执行基于云的高级威胁扫描的能力有助于组织：

- 获取高级网络钓鱼和欺骗解决方案，以及
- 以比以往更快的速度利用安全解决方案来应对不断变化的网络钓鱼问题。

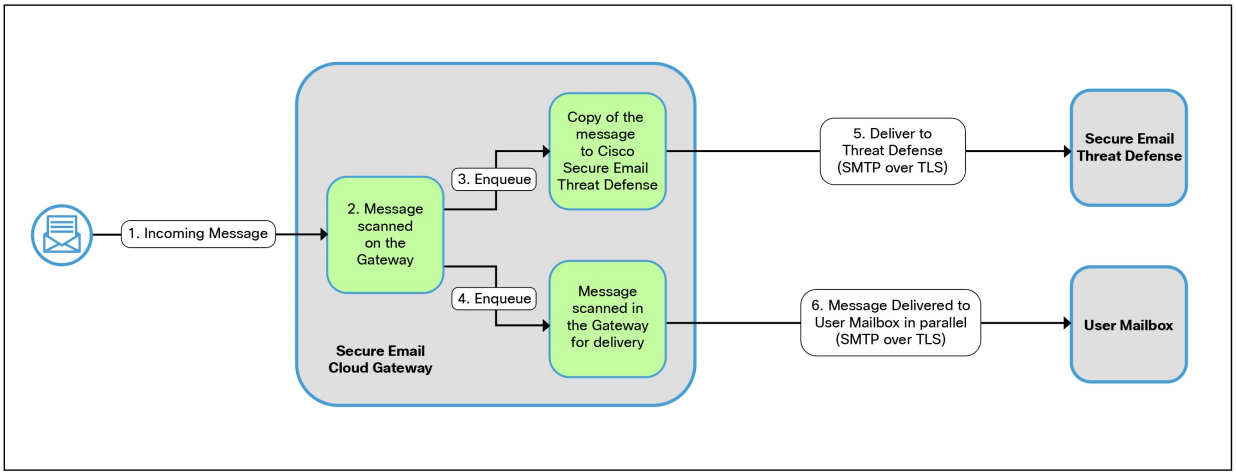
配置威胁防御连接器时，安全邮件云网关会以日志格式将实际邮件的副本作为附件发送到威胁防御门户的邮件接收地址。

一旦邮件被安全电子邮件云网关中的所有扫描引擎扫描并且可以安全传送，则就会复制该邮件。邮件副本将作为 RFC 822 格式的附件排队发送到安全邮件威胁防御系统进行高级扫描。原始邮件将传送到原始收件人。

邮件云网关根据安全邮件威胁防御对 SMTP 会话的要求，通过标准 SMTP 接口发送要进行高级威胁扫描的邮件。威胁防御系统会扫描邮件，并对最初发送到用户邮箱的邮件采取适当的补救措施。

注释 使用威胁防御连接器进行高级威胁扫描仅适用于接收到的邮件。

图 *1:* 威胁防御连接器概述



相关主题

- 如何配置邮件网关以使用威胁防御连接器， 第 2 页

如何配置邮件网关以使用威胁防御连接器

请按顺序执行下列步骤：

步骤	相应操作	更多信息
第 1 步	[关于安全邮件威胁防御]设置安全邮件威胁防御门户，以接收来自安全邮件云网关的邮件。	《思科安全邮件威胁防御用户指南》中的设置安全邮件威胁防御。
第 2 步	从安全邮件威胁防御门户获取邮件接收地址。	思科安全邮件威胁防御用户指南。
第 3 步	在安全邮件云网关上启用和配置威胁防御连接器	在邮件云网关上启用威胁防御连接器， 第 3 页
（可选）步骤 4	为单个邮件策略启用或禁用威胁防御连接器。	为威胁防御连接器配置传入邮件策略， 第 4 页

设置威胁防御门户以从安全邮件云网关接收邮件

作为邮件管理员，您需要设置思科安全邮件威胁防御，以接收来自思科安全邮件云网关的邮件。有关更多信息，请参阅《思科安全邮件威胁防御用户指南》中的设置安全邮件威胁防御一章。

获取邮件接收地址

您的邮件接收地址显示在“安全邮件威胁防御”(Secure Email Threat Defense) 设置页面上。如果您需要在初始设置后找到它，您可以在“帐户详细信息”(Account Details) 部分的**设置 (Settings)**（齿轮图标）> **管理 (Administration)** > **业务 (Business)** 页面上找到它。有关详细信息，请参阅安全邮件威胁防御常见问题。

在邮件云网关上启用威胁防御连接器

开始之前

- 确保您已从思科安全邮件威胁防御收到邮件接收地址。此外，请确保允许向此域和收件人地址传送邮件。
-

注释 如果使用自定义 SMTP 路由传送邮件，请确保使用 DNS 传送到邮件入口地址域。例如，对 SMTP 路由中的域使用“USEDNS”。

过程

步骤 1 点击**安全服务 (Security Services)** > **威胁防御连接器 (Threat Defense Connector)**。

步骤 2 点击**启用 (Enable)**。

步骤 3 选中**启用威胁防御连接器 (Enable Threat Defense Connector)** 复选框。

步骤 4 输入从电子邮件威胁防御门户获取的邮件接收地址。

注释 您也可以为每个传入邮件策略配置威胁防御连接器，并为每个传入邮件策略使用单独的邮件接收地址。确保它们使用与此处使用的全局邮件接收地址相同的域。有关详细信息，请参阅为威胁防御连接器配置传入邮件策略，第 4 页。

步骤 5 点击**提交 (Submit)** 并确认更改。

在邮件云网关上禁用威胁防御连接器

过程

步骤 1 点击**安全服务 (Security Services) > 威胁防御连接器 (Threat Defense Connector)**。

步骤 2 点击**编辑全局设置 (Edit Global Settings)**。

步骤 3 取消选中**启用威胁防御连接器 (Enable Threat Defense Connector)** 复选框。

步骤 4 点击**提交 (Submit)** 并提交您的更改。

威胁防御连接器和集群

如果使用集中管理，则可以在集群、组和计算机级别启用威胁防御连接器。

注释 如果在计算机级别禁用了威胁防御连接器，则也会在组和集群级别禁用相同的功能。

为威胁防御连接器配置传入邮件策略

准备工作

在邮件云网关上启用威胁防御连接器, on page 3

Procedure

步骤 1 依次点击**邮件策略 (Mail Policies) > 传入邮件策略 (Incoming Mail Policies)**。

步骤 2 点击要修改的邮件策略的**威胁防御连接器 (Threat Defense Connector)** 列中的链接。

步骤 3 根据需求，选择以下选项：

- [对于默认策略] **使用全局设置** - 使用在**安全服务 (Security Services) > 威胁防御连接器 (Threat Defense Connector)** 页面中配置的邮件入口地址。
- [对于其他自定义邮件策略] **使用默认策略的设置** - 继承默认策略的威胁防御连接器设置。

  Note 默认情况下，系统会为默认策略禁用威胁防御连接器。如果您在以前的版本中启用了它，则在升级到新版本时将保留这些设置。

- **使用自定义邮件接收地址** - 除了在**安全服务 (Security Services) > 威胁防御连接器 (Threat Defense Connector)** 页面中配置的地址外，您还可以为所选传入邮件策略使用不同的邮件接收地址。确

保对自定义邮件传入地址使用与**安全服务 (Security Services)** > **威胁防御连接器 (Threat Defense Connector)** 页面中配置的全局邮件传入地址相同的域。

在文本框中输入邮件入口地址。

- **否 (No)** - 为选定的传入邮件策略禁用威胁防御连接器。

步骤 4 提交并确认更改。

What to do next

要在 CLI 中配置威胁防御连接器的策略设置，请使用 **policyconfig** 命令。有关详细信息，请参阅《适用于*Cisco Secure Email Gateway*的 *AsyncOS CLI* 参考指南》。

监控威胁防御连接器报告

您需要登录思科安全威胁防御门户才能查看威胁防御连接器的高级扫描报告。有关更多信息，请参阅《思科安全邮件威胁防御用户指南》。

您可以在**监控 (Monitor)** > **传送状态 (Delivery Status)** 下查看外发邮件的传送状态。“传送状态”(Delivery Status) 页面提供与特定收件人域有关的电子邮件操作的监控信息。启用威胁防御连接器后，您可以查看发送到 **.tdc.queue** 目标域下的邮件接收地址的邮件的传送状态。

相关主题

- “传送状态”(Delivery Status) 页面

查看日志

威胁防御连接器信息会被发布到带有前缀“TDC”的邮件日志。

威胁防御连接器日志条目示例

- 邮件发送失败 - TLS 错误，第 5 页

邮件发送失败 - TLS 错误

在此示例中，日志显示在与威胁防御通信时，由于 TLS 错误而未传递信息。

```
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.
```

解决方案

要进一步调查并修复此错误，请联系思科 Technical Assistance Center (TAC)。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。