将邮件网关配置为使用外部威胁源

本章包含以下部分：

外部威胁源概述

借助外部威胁源 (ETF) 框架，邮件网关可以使用以下格式的外部威胁信息：

- 通过 TAXII 协议传输的 STIX 格式。
- 来自思科 SecureX 威胁响应门户的 JavaScript 对象表示法 (JSON) 格式。

能够在邮件网关中使用外部威胁信息，这有助于组织：

- 主动应对网络威胁，例如恶意软件、勒索软件、网络钓鱼攻击和有针对性的攻击。
- 订用本地和第三方威胁情报源。
- 提高邮件网关的效率。

您需要有效的功能密钥才能在邮件网关上使用 ETF 功能。有关如何获取功能密钥的信息，请联系您的思科销售代表。

STIX （结构化威胁信息表达式）是表示网络威胁信息的行业标准结构化语言。STIX 源包含一个指示器，其中包含用于检测恶意或可疑网络活动的模式。

TAXII （可信任的指标信息自动交换）定义了一组用于通过不同组织或产品系列的服务（TAXII 服务器）交换网络威胁信息的规范。

此版本（含 TAXII 1.1 的 STIX 1.1.1 和 1.2）支持以下版本的 STIX/TAXII。

通过思科 SecureX 威胁响应门户，您可以为可观察对象的持续收集创建自定义源，并使用源 URL 在邮件网关中使用这些源。源是 JSON 格式的可观察对象的简单列表。源可在 SecureX 威胁响应门户的**情报 (Intelligence)** > **源 (Feeds)** 页面中创建和管理。

以下是此版本支持的 STIX 和 SecureX 威胁响应感染指标 (IOC) 的列表：

- 文件散列监视列表（描述一组可疑恶意文件的散列）
- IP 监视列表（描述一组可疑的恶意 IP 地址）
- 域监视列表（描述一组可疑的恶意域）
- URL 监视列表（描述一组可疑的恶意 URL）

如何将邮件网关配置为使用外部威胁源

请按顺序执行下列步骤：

步骤	相应操作	更多信息
第 1 步	获取外部威胁源功能密钥。	获取外部威胁源功能密钥 ， 第 4 页
第 2 步	在邮件网关上启用 ETF 引擎。	在邮件网关中启用外部威胁源引擎 ， 第 5 页
第 3 步	配置 ETF 来源，以允许邮件网关从 TAXII 服务器获取 STIX 格式的威胁源。	配置外部威胁源来源 ， 第 6 页

步骤	相应操作	更多信息
[仅适用于SecureX威胁响应源设置]步骤 4	[在 SecureX 威胁响应门户上]：创建一个源 URL。 注释 创建源 URL 时，请确保将源 URL 的输出仅选择为“可观察对象”。	有关如何创建源 URL 的详细信息，请参阅“SecureX 威胁响应帮助”页面，网址为： • https://visibility.amp.cisco.com/help/create-feed-url [适用于美洲用户] • https://visibility.eu.amp.cisco.com/help/create-feed-url [适用于欧盟 (EU) 用户] • https://visibility.apjc.amp.cisco.com/help/create-feed-url [适用于亚太、日本和中国用户]
[仅适用于SecureX威胁响应源设置]步骤 5	[在 SecureX 威胁响应门户上]：查看并复制步骤4在系统中创建的源 URL 的详细信息。 注释 源 URL 的详细信息用于创建SecureX威胁响应源来源。	有关如何查看步骤4中创建的源 URL 的详细信息，请参阅“SecureX 威胁响应帮助”页面，网址如下： • https://visibility.amp.cisco.com/help/intelligence-view-feeds [适用于美洲用户] • https://visibility.eu.amp.cisco.com/help/intelligence-view-feeds [适用于欧盟 (EU) 用户] • https://visibility.apjc.amp.cisco.com/help/intelligence-view-feeds [适用于亚太、日本和中国用户]
[仅适用于SecureX威胁响应源设置]步骤 6	配置 SecureX 威胁响应源来源，以允许邮件网关从 SecureX 威胁响应门户获取 SecureX 威胁响应源。	配置 SecureX 威胁响应源来源，第 8 页
第 7 步	使用以下内容处理包含威胁的邮件： • HAT • 内容或邮件过滤器	处理包含威胁的邮件，第 12 页

步骤	相应操作	更多信息
第 8 步	将配置的内容过滤器附加到传入邮件策略中，以检测邮件中的恶意域、URL 或文件散列。	将内容过滤器附加到传入邮件策略，第 20 页

获取外部威胁源功能密钥

使用经典许可模式管理邮件网关

如果您是使用经典许可模式的现有用户，并且您没有外部威胁源功能密钥，请按照指定的步骤与思科全球许可运营 (GLO) 团队联系以获取功能密钥：

过程

步骤 1 向 GLO 团队（licensing@cisco.com）发送一封电子邮件，其邮件主题为“Request for External Threat Feeds Feature Key”。

步骤 2 在邮件中提供您的产品授权密钥 (PAK) 文件和采购订单 (PO) 详细信息。

GLO 团队手动部署功能密钥，并向您发送一封包含许可证密钥的电子邮件，以便在邮件网关上安装。

下一步做什么

注释

- 如果您是使用硬件或虚拟邮件网关型号的现有用户，并且可以直接从思科服务器获取功能密钥或软件许可证，则系统会自动为您提供外部威胁源功能密钥。
- 如果您是使用虚拟邮件网关型号的现有用户，并且无法直接从思科服务器获取功能密钥或许可证，请执行以下步骤以获取外部威胁源功能密钥：
  1. 使用您的 LRP 用户账号凭证登录到许可证注册门户 (LRP)。
  2. 选择“获取许可证”(Get License)。
  3. 选择“迁移”(Migration)。
  4. 选择“安全产品”(Security Products)
  5. 选择“邮件安全 (ESA)”(Email Security (ESA))
  6. 输入 VLN 编号并生成许可证文件。

     生成的许可证文件包含 ETF 功能。您需要在邮件网关中安装新的许可证文件，才能使用 ETF 功能。

注释 如果您无法登录自己的 LRP 帐户，请联系 GLO 团队 (licensing@cisco.com) 以生成许可证文件。

使用智能软件许可模式来管理邮件网关

如果您是在邮件网关上使用智能许可模式的现有或新用户，则系统会自动提供外部威胁源功能密钥。

在邮件网关中启用外部威胁源引擎

开始之前

请确保您具有有效的功能密钥，以便在邮件网关上使用 ETF 功能。

过程

步骤 1 单击**安全服务 (Security Services) > 外部威胁源 (External Threat Feeds)**。

步骤 2 单击**启用 (Enable)**。

步骤 3 滚动到许可协议页面底部，并单击**接受 (Accept)** 以接受该协议。

注释 如果您不接受许可协议，则不会在思科邮件安全网关上启用 ETF。

步骤 4 单击**启用外部威胁源 (Enable External Threat Feeds)**。

步骤 5 （可选）选择**是**将自定义信头添加到由于 ETF 引擎查找失败而未被 ETF 引擎进行威胁扫描的所有邮件。

步骤 6 提交并确认更改。

下一步做什么

配置 ETF 源。请参阅配置外部威胁源来源，第 6 页。

配置外部威胁源来源

ETF 源用于下载有关 TAXII 服务器上可用的威胁集合的信息。您需要配置 ETF 来源，以允许邮件网关从 TAXII 服务器获取 STIX 格式的威胁源。

注释 您可以在邮件网关上配置最多 8 个 ETF 源。

您可以使用由“轮询路径”和“集合名称”组成的轮询服务来配置 ETF 源。

开始之前

- 请确保您已在邮件网关上启用 ETF 功能。
- 请确保在防火墙上打开端口 80 HTTP 和 443 HTTPS，以允许网关使用外部威胁源。有关详细信息，请参阅防火墙资讯。

过程

步骤 1 单击**邮件策略 (Mail Policies)** > **外部威胁源管理器 (External Threat Feeds Manager)**。

步骤 2 单击**添加源 (Add Source)**。

步骤 3 输入下表中描述的所需参数，以配置 ETF 源。

参数源详细信息	说明
源名称	输入 CRL 源的名称。
说明	输入 ETF 源的说明。
TAXII 详细信息	
主机名	输入完全限定域名的主机名或TAXII 服务器的 IP 地址。

参数源详细信息	说明
轮询路径	输入用于识别 TAXII 服务器中的轮询服务的轮询路径，例如 /taxii-data。
集合名称	输入托管在 TAXII 服务器上的威胁源集合的名称，例如 Abuse_ch。
轮询间隔	输入轮询间隔，以定义从 TAXII 服务器获取威胁源的频率。最小值为 5 分钟，默认值为 60 分钟。
威胁源到期时间	输入可以从 TAXII 服务器获取威胁源的最大时间长度。期限值必须介于 1 到 365 天之间。
轮询网段的时间范围	输入每个轮询网段的时间范围。 单个轮询网段的最短时间范围为 1 天。单个轮询网段的最长时间范围为“威胁源到期时间”字段中输入的值。 您可以在以下场景中使用“轮询网段的时间范围”选项： • 如果 TAXII 服务器的威胁源到期时间没有已知限制，请使用在“威胁源到期时间”选项中输入的值。 • 如果 TAXII 服务器的威胁源到期时间存在已知限制，请使用已知限制值。 • 如果您不知道 TAXII 服务器的威胁源到期时间的已知限制，请使用默认值 30 天。 • 如果 TAXII 服务器不支持在 "威胁源到期时间" 选项中输入的值，则可以根据输入的时间范围将威胁源到期时间分为不同的轮询网段。 例如，如果威胁源到期时间为 100 天，并且 TAXII 服务器对威胁源到期时间具有固定限制（例如“40 天”），请输入 40 作为轮询网段的时间范围 **注释** 如果轮询网段的时间范围为较小的值（例如“5 天”），则威胁源来源的轮询可能需要很长时间才能完成，这可能会影响网关的性能。
使用 HTTPS	如果要使用 HTTPS 连接到 TAXII 服务器，请选择**是** 。

参数源详细信息	说明
配置凭证	如果要使用您在 TAXII 服务器中创建的用户凭证访问 TAXII 服务器，请选择**是**。 输入用户名和密码。
代理详细信息	
使用全局代理	如果您希望邮件网关通过代理服务器连接到TAXII服务器，请选择**是 (Yes)**。 可以通过以下任何一种方式配置代理服务器： • Web 界面中的“安全服务 (Security Services) > 服务更新 (Service Updates)”页面 • CLI 中的 `updateconfig` 命令 如果选择**否 (No)**，则邮件网关会直接连接到 TAXII 服务器。

步骤 4 提交并确认更改。

配置 ETF 源后，邮件网关开始从 TAXII 源获取威胁源。

下一步做什么

- 您还可以在 CLI 中使用 **`threatfeedsconfig > sourceconfig`** 子命令配置 ETF 源。
- （可选）单击“邮件策略 (Mail Policies) > 外部威胁源管理器 (External Threat Feeds Manager)”页面中的**暂停轮询 (Suspend Polling)** ( ) 图标，为已配置的 ETF 源暂停轮询服务。
- （可选）单击“邮件策略 (Mail Policies) > 外部威胁源管理器 (External Threat Feeds Manager)”页面中的**恢复轮询 (Resume Polling)** ( ) 图标，为已配置的 ETF 源恢复轮询服务。
- （可选）单击“邮件策略 (Mail Policies) > 外部威胁源管理器 (External Threat Feeds Manager)”页面中的**立即轮询**，以立即从上一次成功轮询间隔中获取威胁源。
- 请参阅处理包含威胁的邮件，第 12 页。

配置 SecureX 威胁响应源来源

SecureX 威胁响应源来源用于下载有关 SecureX 威胁响应门户上可用威胁集合的信息。您需要配置 SecureX 威胁响应源来源，以允许邮件网关从 SecureX 威胁响应门户获取威胁源。

注释 您可以在邮件网关上配置最多 8 个 SecureX 威胁响应源来源。

开始之前

确保您已满足下列前提条件：

- 已在邮件网关上启用 ETF 引擎。
- 已打开防火墙上的端口 - 80 HTTP 和 443 HTTPS，以允许网关使用 SecureX 威胁响应源。有关详细信息，请参阅 防火墙资讯。
- 在思科 SecureX 中创建了一个具有管理员访问权限的用户账号。要创建新用户账号，请使用 URL https://securex.us.security.cisco.com/login转至**思科 SecureX 登录 (Cisco SecureX login)**页面，然后在登录页面中单击**创建 SecureX 登录帐户 (Create a SecureX Sign-on Account)**。如果您无法创建新用户账号，请联系思科 TAC 寻求帮助。
- 在 SecureX 威胁响应门户中创建了源 URL。有关详细信息，请参阅 SecureX 威胁响应帮助页面：
  - https://visibility.amp.cisco.com/help/create-feed-url [适用于美洲用户]
  - https://visibility.eu.amp.cisco.com/help/create-feed-url [适用于欧盟 (EU) 用户]
  - https://visibility.apjc.amp.cisco.com/help/create-feed-url [适用于亚太、日本和中国用户]
- 查看并复制了在系统的 SecureX 威胁响应门户中创建的源 URL 的详细信息。有关详细信息，请参阅 SecureX 威胁响应帮助页面：
  - https://visibility.amp.cisco.com/help/intelligence-view-feeds [适用于美洲用户]
  - https://visibility.eu.amp.cisco.com/help/intelligence-view-feeds [适用于欧盟 (EU) 用户]
  - https://visibility.apjc.amp.cisco.com/help/intelligence-view-feeds [适用于亚太、日本和中国用户]

过程

步骤 1 单击**邮件策略 (Mail Policies)** > **外部威胁源管理器 (External Threat Feeds Manager)**。

步骤 2 单击**添加源 (Add Source)**。

步骤 3 输入下表中描述的所需参数，以配置 SecureX 威胁响应源来源。

参数源详细信息	说明
源名称	输入 SecureX 威胁响应源来源的名称。
说明	输入 SecureX 威胁响应源来源的说明。

参数源详细信息	说明
TAXII 详细信息 SecureX 威胁响应源来源与典型的 TAXII 源来源有所不同。但是，要启用来自 SecureX 威胁响应服务器的可观察对象的轮询，则必须将 SecureX 威胁响应源 URL 映射到以下 TAXII 来源参数。 • 主机名 • 轮询路径 • 集合名称 **例如**：以下是在 SecureX 威胁响应门户中创建的示例 SecureX 威胁响应源 URL。 *<https://private.intel.amp.cisco.com/ctia/feed/feed-d78e1eba-cbe6-5* *e13-8d47-197b344e41c9/view.txt?s=e8f3f519-9170-4b76-8b58 bda0be540ff3>* 您可以将示例 SecureX 威胁响应源 URL 详细信息映射到以下 TAXII 来源参数： • **主机名** - 包含 SecureX 威胁响应源 URL 的“*private.intel.amp.cisco.com*”部分。 • **轮询路径** - 包含 SecureX 威胁响应源 URL 的“*/ctia/feed/feed-d78e1eba-cbe6-5e13-8d47-197b344e41c9/view*”部分。 **注释** 请勿在轮询路径中包含 SecureX 威胁响应源 URL 的“*.txt*”部分。 • **集合名称** - 包含 SecureX 威胁响应源 URL 的“*e8f3f519-9170-4b76-8b58-bda0be540ff3*”部分。 使用上述示例，您可以配置“主机名”、“轮询路径”和“集合名称”参数。有关如何配置这些参数的详细信息，请参阅下文。	
主机名	输入基于您的 SecureX 威胁响应服务器区域的 SecureX 威胁响应源 URL 的主机名。 以下是您可以根据 SecureX 威胁响应服务器区域选择的主机名： • `private.intel.amp.cisco.com` [适用于美洲用户] • `private.intel.eu.amp.cisco.com` [适用于欧盟用户] • `private.intel.apjc.amp.cisco.com` [适用于亚太、日本和中国用户]
轮询路径	输入在 SecureX 威胁响应服务器中标识轮询服务的轮询路径。 例 如：/ctia/feed/feed-d78e1eba-cbe6-5e13-8d47-197b344e41c9/view

参数源详细信息	说明
集合名称	输入在 SecureX 威胁响应服务器上托管的 SecureX 威胁响应源的集合名称。 例如：e8f3f519-9170-4b76-8b58-bda0be540ff3
轮询间隔	输入轮询间隔，以定义从 SecureX 威胁响应服务器获取 SecureX 威胁响应源的频率。最小值为 5 分钟，默认值为 60 分钟。 **注释** 完整轮询的最大限制为 100 mb，如果源可观察对象的大小超过最大限制，则邮件网关会在 ETF 日志中显示错误消息。
威胁源到期时间，轮询网段的时间范围	配置 SecureX 威胁响应源来源时不需要这些参数，因为来自 SecureX 威胁响应服务器的可观察对象的轮询并不基于时间间隔。完整轮询方法用于获取可观察对象。
使用 HTTPS	选择**是 (Yes)** 以使用 HTTPS 连接到 SecureX 威胁响应服务器。
配置凭证	配置 SecureX 威胁响应源来源时不需要此参数。
代理详细信息	
使用全局代理	如果您希望邮件网关通过代理服务器连接到 SecureX 威胁响应服务器，请选择**是 (Yes)**。 可以通过以下任何一种方式配置代理服务器： • Web 界面中的“安全服务 (Security Services) > 服务更新 (Service Updates)”页面 • CLI 中的 *updateconfig* 命令 如果选择**否 (No)**，则邮件网关会直接连接到 SecureX 威胁响应服务器。

步骤 4 提交并确认更改。

配置 SecureX 威胁响应源来源后，邮件网关会开始从 SecureX 威胁响应来源获取威胁源。

下一步做什么

- 您还可以在 CLI 中使用 **threatfeedsconfig > sourceconfig** 子命令配置 SecureX 威胁响应源来源。

- （可选）单击“邮件策略 (Mail Policies) > 外部威胁源管理器 (External Threat Feeds Manager)”页面中的**暂停轮询 (Suspend Polling)** ( ) 图标，为已配置的 SecureX 威胁响应源来源暂停轮询服务。
- （可选）单击“邮件策略 (Mail Policies) > 外部威胁源管理器 (External Threat Feeds Manager)”页面中的**恢复轮询 (Resume Polling)** ( ) 图标，为已配置的 SecureX 威胁响应源来源恢复轮询服务。
- （可选）单击“邮件策略 (Mail Policies) > 外部威胁源管理器 (External Threat Feeds Manager)”页面中的**立即轮询 (Poll Now)**，以立即从上一次成功轮询间隔中获取 SecureX 威胁响应源。
- 请参阅处理包含威胁的邮件 ， 第 12 页。

处理包含威胁的邮件

您可以使用以下方式处理邮件网关中包含威胁的邮件：

- HAT
- 内容或邮件过滤器

相关主题

- 配置发件人组以处理包含威胁的邮件 ， 第 12 页。
- 配置用于处理包含威胁的邮件的内容或邮件过滤器 ， 第 13 页。

配置发件人组以处理包含威胁的邮件

您可以将现有发件人组配置为使用从 ETF 引擎获取的判定来处理源自恶意 IP 的邮件。

过程

步骤 1 转到**邮件策略 (Mail Policies) > HAT 概述 (HAT Overview)** 页面。
步骤 2 单击要配置以处理包含威胁的邮件的现有发件人组。
步骤 3 单击**编辑设置 (Edit Settings)**。
步骤 4 选择所需的 ETF 源以过滤恶意 IP 地址。
步骤 5 （可选）单击**添加行 (Add Row)** 添加另一个 ETF 源。
步骤 6 提交并确认更改。

配置用于处理包含威胁的邮件的内容或邮件过滤器

您可以配置以下一个或多个内容或邮件过滤器，以根据从 ETF 引擎获取的判定对包含威胁的邮件采取适当的操作：

- URL 信誉 - 用于检测被 ETF 引擎归类为恶意的 URL。
- 域信誉 - 用于检测被 ETF 引擎归类为恶意的域。
- 附件(按文件信息) - 用于检测被 ETF 引擎根据文件散列归类为恶意的文件。

相关主题

- 使用内容过滤器检测邮件中的恶意域，第 13 页。
- 使用邮件过滤器检测邮件中的恶意域，第 14 页
- 使用内容过滤器检测邮件中的恶意 URL，第 15 页
- 使用邮件过滤器检测邮件中的恶意域，第 16 页
- 使用内容过滤器检测邮件附件中的恶意文件，第 18 页。
- 使用邮件过滤器检测邮件附件中的恶意文件。

使用内容过滤器检测邮件中的恶意域

使用“域信誉”内容过滤器可检测 ETF 引擎在邮件中归类为恶意的域，并对此类邮件执行相应的操作。

开始之前

- 可选）创建仅包含域的地址列表。要创建一个，请转到 Web 界面中的**邮件策略 (Mail Policies)** > **地址列表 (Address Lists)** 页面或 CLI 中的 `addresslistconfig` 命令。有关详细信息，请参阅邮件策略。
- （可选）创建域例外列表。有关详细信息，请参阅创建域例外列表。

过程

步骤 1 转到**邮件策略 (Mail Policies)** > **传入内容过滤器 (Incoming Content Filters)**。

步骤 2 单击**添加过滤器 (Add Filter)**。

步骤 3 输入内容过滤器的名称和描述。

步骤 4 单击**添加条件 (Add Condition)**。

步骤 5 单击**域信誉 (Domain Reputation)**。

步骤 6 选择**外部威胁源 (External Threat Feeds)**。

步骤 7 选择要在邮件的信头中检测恶意域的 ETF 源。

步骤 8 选择所需的信头以检查域的信誉。

步骤 9 （可选）选择您不希望邮件网关为此内容过滤器检测威胁的已列入允许列表的域列表。

步骤 10 单击**确定 (OK)**。

步骤 11 单击添加操作，配置要对包含恶意域的邮件执行的相应操作。

步骤 12 提交并确认更改。

创建域例外列表

域例外列表由仅包含域的地址列表组成。如果您希望邮件网关跳过所有已配置的域信誉内容或邮件过滤器的域检查，则可以使用域例外列表。

过程

步骤 1 转到**安全服务 (Security Services) > 域信誉 (Domain Reputation)**。

步骤 2 单击域例外列表下的**编辑设置 (Edit Settings)**。

步骤 3 选择仅包含域的所需地址列表。

步骤 4 提交并确认更改。

下一步做什么

您还可以在 CLI 中使用 domainrepconfig 命令创建域例外列表。有关详细信息，请参阅《适用于思科邮件安全设备的 AsyncOS 12.0 的 CLI 参考指南》。

使用邮件过滤器检测邮件中的恶意域

例如，使用以下邮件过滤器规则语法来检测使用 ETF 引擎的邮件中的恶意域，并对此类邮件执行适当的操作。

语法：

```
quarantine_msg_based_on_ETF: if (domain-external-threat-feeds (['etf_source1'],
 ['mail-from', 'from'], <'domain_exception_list'>)) { quarantine("Policy"); }
```

位置

- ‘`domain-external-threat-feeds`' 是域信誉邮件过滤器规则。
- ‘`etf_source1`' 是用于在邮件的信头中检测恶意域的 ETF 源。
- ‘`mail-from`','`from`' 是用于检查域信誉的所需信头。
- '`domain_exception_list`' 是域例外列表的名称。如果不存在域例外列表，它将显示为 ""。

示例

在以下示例中，如果 ETF 引擎检测到 'Errors To:' 自定义信头中的域为恶意域，则该邮件将被隔离。

```
Quaranting_Messages_with_Malicious_Domains: if domain-external-threat-feeds
(['threat_feed_source'], ['Errors-To'], "")) {quarantine("Policy");}
```

使用内容过滤器检测邮件中的恶意 URL

使用“URL 信誉”内容过滤器可检测被 ETF 引擎归类为恶意的邮件中的 URL，并对此类邮件执行适当的操作。

您可以通过以下任何一种方式配置 ETF 的“URL 信誉”内容过滤器：

- 请将“URL 信誉”条件与任何适当的操作结合使用。
- 将“URL 信誉”操作与任何或不条件结合使用。
- 将“URL 信誉”条件和操作结合使用。

以下过程用于使用“URL 信誉”条件和操作检测恶意 URL：

注释

- 如果您只想将“URL 信誉”条件与任何适当的操作结合使用，请勿执行该过程的步骤 11-20。
- 如果您只想将“URL 信誉”操作与任何条件结合使用或不与任何条件结合使用，请勿执行该过程的步骤 4-10。

开始之前

- 确保您已在邮件网关上启用 URL 过滤。要启用 URL 过滤，请转到 Web 界面中的安全服务 *(Security Services)* > *URL* 过滤 *(URL Filtering)* 页面。有关详细信息，请参阅防御恶意或不需要的 URL。
- 确保您已在邮件网关上启用爆发过滤器。要启用病毒爆发过滤器，请转到 Web 界面中的安全服务 *(Security Services)* > 病毒爆发过滤器 *(Outbreak Filters)*页面。有关详细信息，请参阅病毒爆发过滤器。
- 确保您已在邮件网关上启用反垃圾邮件引擎。要启用反垃圾邮件引擎，请转到 Web 界面中的安全服务 *(Security Services)* > 反垃圾邮件 *(Anti-Spam)*页面。有关详细信息，请参阅管理垃圾邮件和灰色邮件。
- （可选）创建 URL 列表。要创建一个，请转到 Web 界面中的邮件策略 *(Mail Policies)* > *URL* 列表 *(URL Lists)* 页面。有关详细信息，请参阅防御恶意或不需要的 URL。

过程

步骤 1 转到**邮件策略 (Mail Policies)** > **传入内容过滤器 (Incoming Content Filters)**。

步骤 2 单击**添加过滤器 (Add Filter)**。

步骤 3 输入内容过滤器的名称和描述。

步骤 4 单击**添加条件 (Add Condition)**。

步骤 5 单击 **URL 信誉 (URL Reputation)**。

步骤 6 选择**外部威胁源 (External Threat Feeds)**。

步骤 7 选择要检测恶意 URL 的 ETF 源。

步骤 8 （可选）选择您不希望邮件网关检测威胁的已列入允许列表的 URL 列表。

步骤 9 选择所需的**检查 URL** 选项，以检测“邮件正文和主题”和/或“邮件附件”中的恶意 URL。

步骤 10 单击**确定 (OK)**。

步骤 11 单击**添加操作 (Add Action)**。

步骤 12 单击 **URL 信誉 (URL Reputation)**。

步骤 13 选择**外部威胁源 (External Threat Feeds)**。

步骤 14 请确保选择您在条件中所选（第7步）的相同 ETF 源。

步骤 15 （可选）选择您在第 8 步中所选的已列入允许列表的相同 URL 列表。

步骤 16 选择所需的**检查 URL** 选项，以检测“邮件正文和主题”和/或“邮件附件”中的恶意 URL

步骤 17 在邮件正文、主题和/或邮件附件中，选择要在 URL 上执行的所需操作。

注释 在第 16 步中，如果您将“检查 URL”选项选择为“附件”，则只能删除该邮件的附件。

步骤 18 选择是否要对所有邮件或未签名的邮件执行操作。

步骤 19 单击**确定 (OK)**。

步骤 20 提交并确认更改。

注释 如果您在邮件网关上为基于 Web 信誉得分 (WBRS) 和 ETF 配置了“URL 信誉”内容过滤器，建议将 WBRS URL 信誉内容过滤器的顺序设置为高于 ETF URL 信誉过滤器的顺序，以提高邮件网关的性能。

使用邮件过滤器检测邮件中的恶意域

例如，使用“URL 信誉”邮件过滤器规则语法来检测使用 ETF 引擎的邮件中的恶意 URL，并去除该 URL。

语法：

```
defang_url_in_message: if (url-external-threat-feeds (['etf_source1'],
<'URL_allowedlist'>,
<’ message_attachments'> , <’ message_body_subject’ > ,))
```

```
 { url-etf-defang(['etf-source1'], "", 0); } <’ URL_allowedlist’> ,
<’ Preserve_signed’>)}
```

位置

- ‘url-external-threat-feeds’ 是 URL 信誉规则。
- ‘etf_source1’ 是用于检测邮件或邮件附件中的恶意 URL 的 ETF 源。
- “URL_allowedlist”是 URL 允许列表的名称。如果 URL 允许列表不存在，则显示为“”。
- ‘message_attachments’ 用于检查邮件附件中是否存在恶意 URL。值 "1" 用于检测邮件附件中的恶意 URL。
- ‘message_body_subject’ 用于检查邮件正文和主题中是否存在恶意 URL。值“1”用于检测邮件正文和主题中的恶意 URL。

  注释 值“1,1”用于检测邮件正文、主题和邮件附件中的恶意URL。

- ‘url-etf-defang’ 是您可以对包含恶意 URL 的邮件执行的操作之一。

  以下示例是您可以在包含恶意 URL 的邮件上应用的基于 ETF 的操作：

  - url-etf-strip(['etf_source1'], "None", 1)
  - url-etf-defang-strip(['etf_source1'], "None", 1, "Attachment removed")
  - url-etf-defang-strip(['etf_source1'], "None", 1)
  - url-etf-proxy-redirect(['etf_source1'], "None", 1)
  - url-etf-proxy-重定向条（[' etf_source1 ']，"None"，1）
  - url-etf-proxy-redirect-strip(['etf_source1'], "None", 1, " Attachment removed")
  - url-etf-replace(['etf_source1'], "", "None", 1)
  - url-etf-replace(['etf_source1'], "URL removed", "None", 1)
  - url-etf-replace-strip(['etf_source1'], "URL removed ", "None", 1)
  - url-etf-replace-strip(['etf_source1'], "URL removed*", "None", 1, "Attachment removed")

- "Preserve_signed"由 "1" 或 "0" 表示。"1" 表示此操作仅适用于未签名邮件，"0" 表示此操作适用于所有邮件。

在以下示例中，如果邮件附件中的 URL 被 ETF 引擎检测为恶意，则该附件将被删除。

```
Strip_Malicious_URLs: if (true) {url-etf-strip(['threat_feed_source'], "", 0);}
```

使用内容过滤器检测邮件附件中的恶意文件

使用“附件文件信息”内容过滤器可检测被 ETF 引擎归类为恶意的邮件附件中的文件，并对此类邮件执行相应的操作。

注释 ETF 引擎根据文件的文件散列执行查找。

您可以通过以下任何一种方式配置 ETF 的“附件文件信息”内容过滤器：

- 将“附件文件信息”条件与任何适当的操作结合使用。
- 将“按文件信息删除附件”(Strip Attachment by File Info) 操作与任何条件结合使用，或不与任何条件结合使用。
- 使用“附件文件信息”(Attachment File Info) 条件和“按文件信息删除附件”(Strip Attachment by File Info) 操作。

以下程序用于使用 "按文件信息附件"(Attachment by File Info) 条件和 "按文件信息删除附件"(Strip Attachment by File Info) 操作来检测邮件附件中的恶意文件：

注释
- 如果您只想将“附件文件信息”条件用于任何相应的操作，请勿执行该过程的步骤 10-15。
- 如果您只想将“按文件信息删除附件”(Strip Attachment by File Info) 操作与任何条件结合使用，或不与任何条件结合使用，请勿执行该过程的步骤 4-9。

开始之前

可选创建文件散列例外列表。要创建一个，请转到 Web 界面中的 "邮件策略 (Mail Policies) > 文件散列列表 (File Hash Lists)" 页面。有关详细信息，请参阅创建文件散列列表，第 19 页。

过程

步骤 1 转到**邮件策略 (Mail Policies) > 传入内容过滤器 (Incoming Content Filters)**。

步骤 2 单击**添加过滤器 (Add Filter)**。

步骤 3 输入内容过滤器的名称和描述。

步骤 4 单击**添加条件 (Add Condition)**。

步骤 5 单击**附件文件信息 (Attachment File Info)**。

步骤 6 选择**外部威胁源 (External Threat Feeds)**。

步骤 7 选择要使用文件散列检测恶意文件的 ETF 源。

步骤 8 （可选）选择您不希望邮件网关检测威胁的文件散列列表。

步骤 9 单击**确定 (OK)**。

步骤 10 单击**添加操作 (Add Action)**。

步骤 11 单击**按文件信息删除附件 (Strip Attachment by File Info)**。

步骤 12 选择**外部威胁源 (External Threat Feeds)**。

步骤 13 请确保选择您在条件中所选（第7步）的相同 ETF 源。

步骤 14 （可选）选择您在第 8 步中所选的相同文件散列列表。

步骤 15 提交并确认更改。

创建文件散列列表

过程

步骤 1 转到**邮件策略 (Mail Policies) > 文件散列列表 (File Hash Lists)**。

步骤 2 单击**添加文件散列列表 (Add File Hash List)**。

步骤 3 检查所需的文件散列类型：“SHA256”或“MD5”或以上全部。

步骤 4 以逗号分隔或在新行中输入文件散列（在第 3 步中已选择）。

步骤 5 提交并确认更改。

使用邮件过滤器检测邮件附件中的恶意文件

例如，使用以下邮件过滤器规则语法检测被 ETF 引擎归类为恶意的邮件附件中的文件，并对此类邮件执行适当的操作。

语法：

```
Strip_malicious_files: if (file-hash-etf-rule (['etf_source1'], <'file_hash_exception_list'>))

{ file-hash-etf-strip-attachment-action (['etf_source1'], <'file_hash_exception_list>,
 "file stripped from message attachment"); }
```

其中：

- ‘`file-hash-etf-rule`' 是附件文件信息邮件过滤器规则
- ‘`etf_source1`' 是用于根据文件散列检测邮件中的恶意文件的 ETF 源。
- '`file_hash_exception_list`' 是文件散列例外列表的名称。如果不存在文件散列例外列表，它将显示为 ""。
- '`file-hash-etf-strip-attachment-action`' 是要应用于包含恶意文件的邮件的操作名称。

在以下示例中，如果邮件包含 ETF 引擎检测为恶意的邮件附件，则该附件将被删除。

```
Strip_Malicious_Attachment: if (true) {file-hash-etf-strip-attachment-action
(['threat_feed_source'], "", “Malicious message attachment has been stripped from
the message.");}
```

将内容过滤器附加到传入邮件策略

您可以将配置的一个或多个内容过滤器附加到传入邮件策略中，以检测邮件中的恶意域、URL 或文件散列。

过程

步骤 1 转到**邮件策略 (Mail Policies)** > **传入邮件策略 (Incoming Mail Policies)**。

步骤 2 单击特定邮件策略的**内容过滤器 (Content Filters)** 下面的链接。

步骤 3 选择**启用内容过滤器(自定义设置) (Enable Content Filters [Customize Settings])**。

步骤 4 选择您创建的用于检测恶意域、URL 或文件散列值的内容过滤器。

步骤 5 提交并确认更改。

下一步做什么

将内容过滤器附加到传入邮件策略后，您的邮件网关开始根据从 ETF 引擎收到的判定对邮件采取操作。

外部威胁源和群集

如果使用集中管理，则可以启用群集、组和计算机级别的 ETF 引擎和邮件策略。

监控外部威胁源引擎更新

如果已启用服务更新，则会从思科更新服务器检索 ETF 引擎更新。但在某些情况下（例如，已禁用自动服务更新或自动服务更新不起作用），您可能需要手动检查 ETF 引擎更新。

您可以通过以下任一方式手动更新 ETF 引擎：

- 转到 Web 界面中的“**安全服务 (Security Services)** > **外部威胁源 (External Threat Feeds)**”页面，然后单击**立即更新 (Update Now)**。
- 在 CLI 中使用 `threatfeedupdate` 命令。

要了解现有 ETF 引擎的详细信息，请参阅 Web 界面中的 "安全服务 (Security Services) > 外部威胁源 (External Threat Feeds)" 页面中的“”外部威胁源引擎更新”(External Threat Feeds Engine Updates) 部分，或在 CLI 中使用 threatfeedstatus 命令。

查看警报

下表包含 AsyncOS 生成的各种系统警报的列表，包括对警报和警报严重性的说明。

组件/警报名称	邮件和描述	参数
ETF 引擎警报	3 次尝试失败后，无法从 $source_name 源获取可观察对象。 失败原因：$reason	‘**source**’ - TAXII 源的名称。 ‘**reason**’ - 轮询失败的原因。
	参考。当从 TAXII 源轮询源失败时发送。	
ETF 引擎警报	可观察对象类型 $type 已超过 $count 可观察对象的存储限制。	**$count** - 每种类型允许的可观察对象数。 **$ type** - 可观察对象的类型。
	参考。当超过允许的可观察对象数量时发送。	

在邮件跟踪中显示威胁详细信息

您可以从所选 ETF 源中查看包含与所选 IOC 对应的威胁的邮件详细信息。

开始之前

- 请确保在邮件网关上启用邮件跟踪功能。要启用邮件跟踪 (Message Tracking)，请转到 Web 界面中的**安全服务 (Security Services) > 集中服务 (Centralized Services) > 邮件跟踪 (Message Tracking)** 页面。
- 用于检测邮件的内容或邮件过滤器可正常运行。

过程

步骤 1 转到**监控 (Monitor) > 邮件跟踪 (Message Tracking)**。

步骤 2 单击**高级 (Advanced)**。

步骤 3 检查“邮件事件”(Message Event) 下的**外部威胁源 (External Threat Feeds)**。

步骤 4 选择所需的 IOC，以跟踪包含与所选 IOC 对应的威胁的邮件。

步骤 5 （可选）选择**所有外部威胁源来源 (All External Threat Feed Sources)**，以根据在邮件网关中配置的可用和已删除 ETF 源来查看包含威胁的邮件。

步骤 6 （可选）选择**当前外部威胁源来源 (Current External Threat Feed Sources)**并选择所需的 ETF 源，以根据在思科邮件安全网关中配置的可用 ETF 源来查看包含威胁的邮件。

步骤 7 （可选）在“外部威胁源源”(External Threat Feed Sources) 字段中输入特定 ETF 源的名称，以根据此 ETF 源来查看包含威胁的邮件。

步骤 8 单击**搜索 (Search)**。