配置安全邮件网关每策略日志以保护邮件威胁防御

目录

简介

本文档介绍配置安全邮件网关(SEG)以执行针对安全邮件威胁防御(SETD)的每策略日志记录的步骤。

先决条件

事先了解思科安全邮件网关(SEG)常规设置和配置会很有用。

使用的组件

此设置需要两者；

- 思科安全邮件网关(SEG) AsyncOS 15.5.1及更高版本
- 思科邮件威胁防御(SETD)实例。
- 威胁防御连接器(TDC)。“两种技术之间明确的连接。”

"本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。”

概述

Cisco SEG能够与SETD集成，以提供额外的保护。

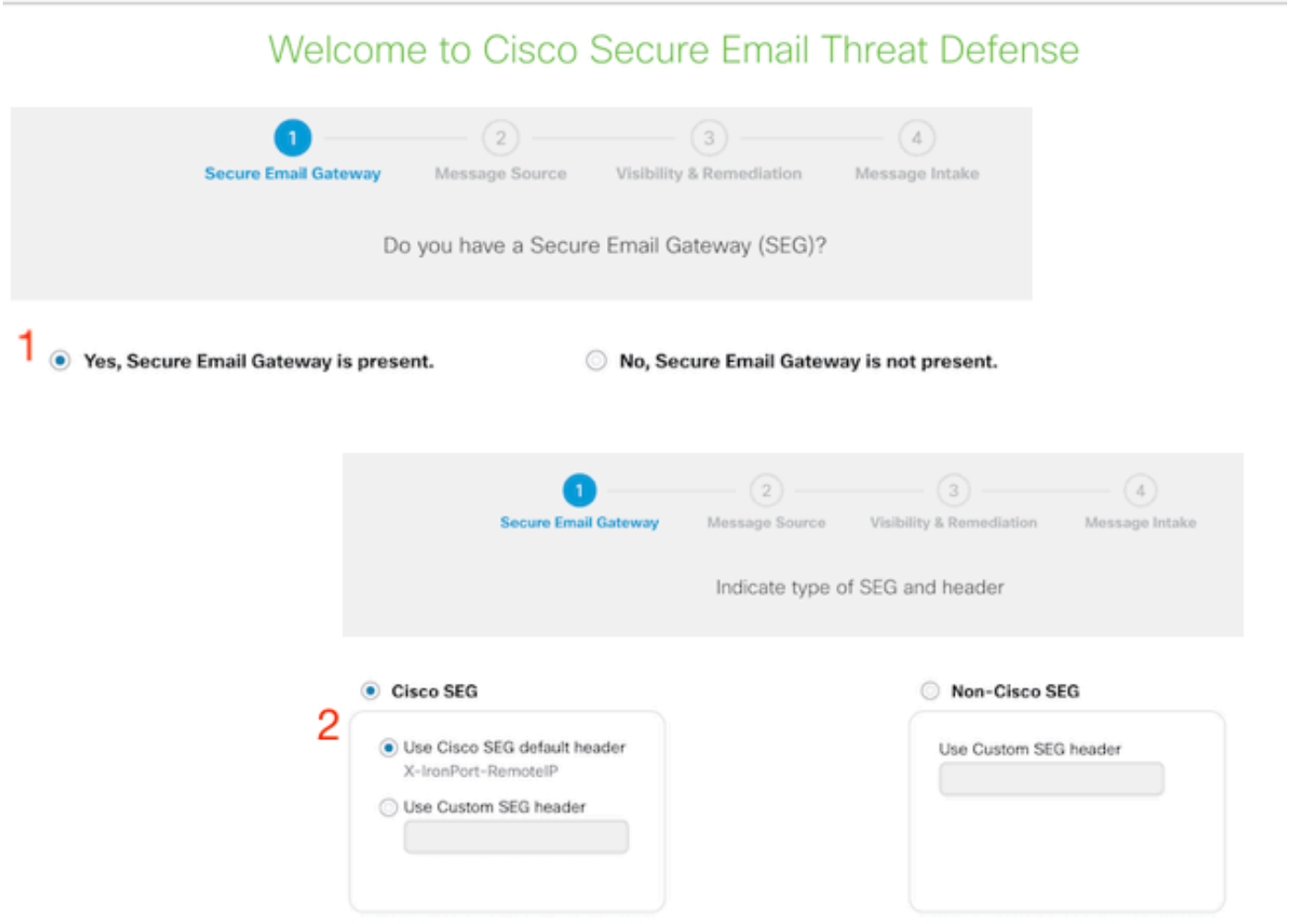
- SEG日志操作会传输所有正常邮件的完整邮件。
- SEG提供了根据每邮件策略匹配选择性地选择传入邮件流的选项。
- SEG Per Policy选项允许3种选择：No Scan、Default Message Inceive Address或Custom Message Inceive Address。
    - “默认接收地址”表示接受特定帐户实例邮件的主SETD帐户。

    - 自定义邮件接收地址表示接受不同已定义域的邮件的第二个SETD帐户。此方案适用于更复杂的SETD环境。
- 日志消息具有SEG消息ID (MID)和目标连接ID DCID
- 传递队列包含类似于域的值“the.tdc.queue”，用于捕获SETD传输计数器。
    - 在此处可查看“the.tdc.queue”活动计数器：cli>tophosts或SEG Reporting > Delivery Status (non-CES)。
    - “the.tdc.queue”表示相当于目标域名的威胁防御连接器(TDC)。

配置

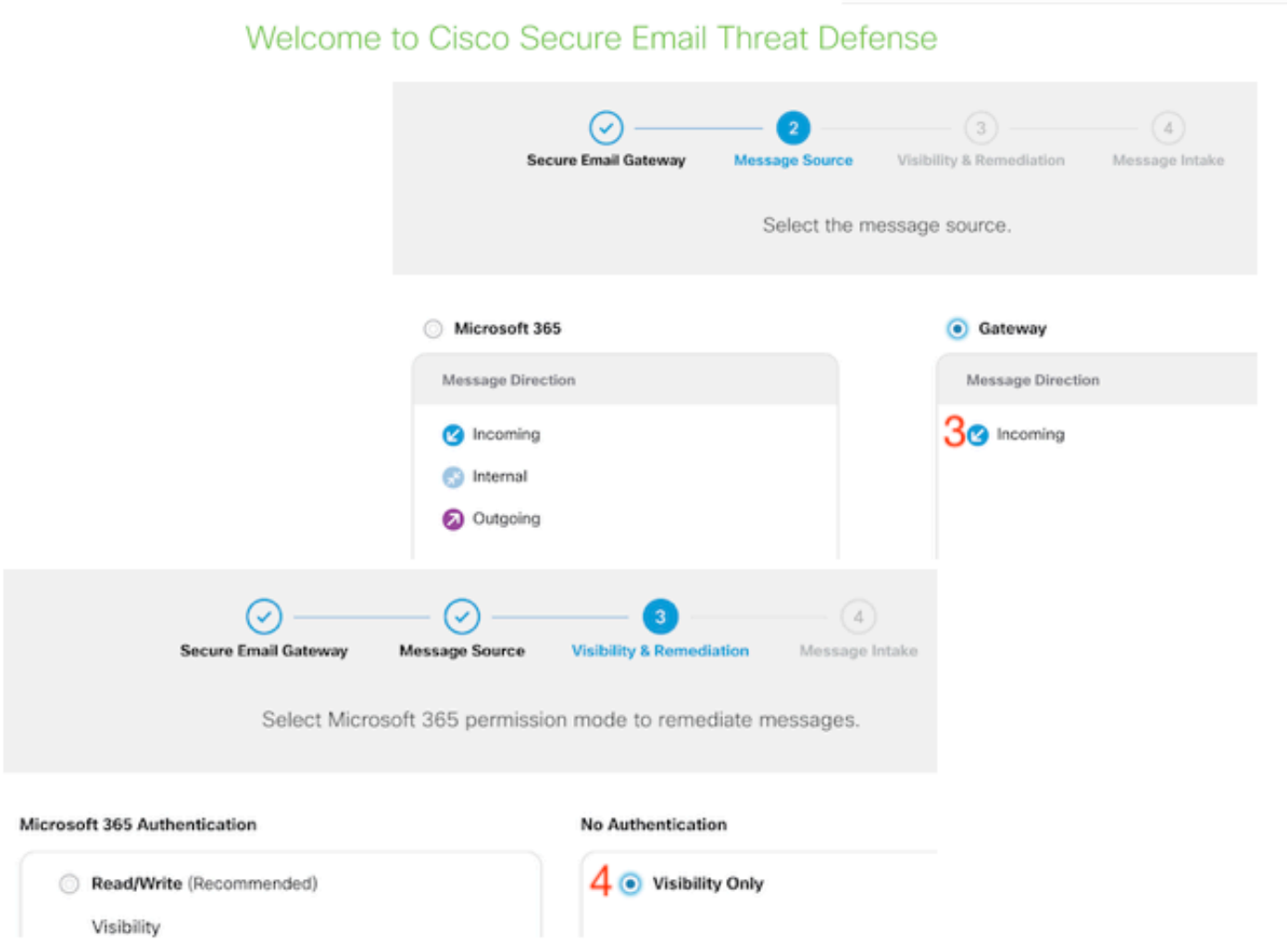
SETD初始设置步骤生成“邮件接收地址”(Message Inceive Address)。

1. 是，安全邮件网关存在。
2. 思科SEG

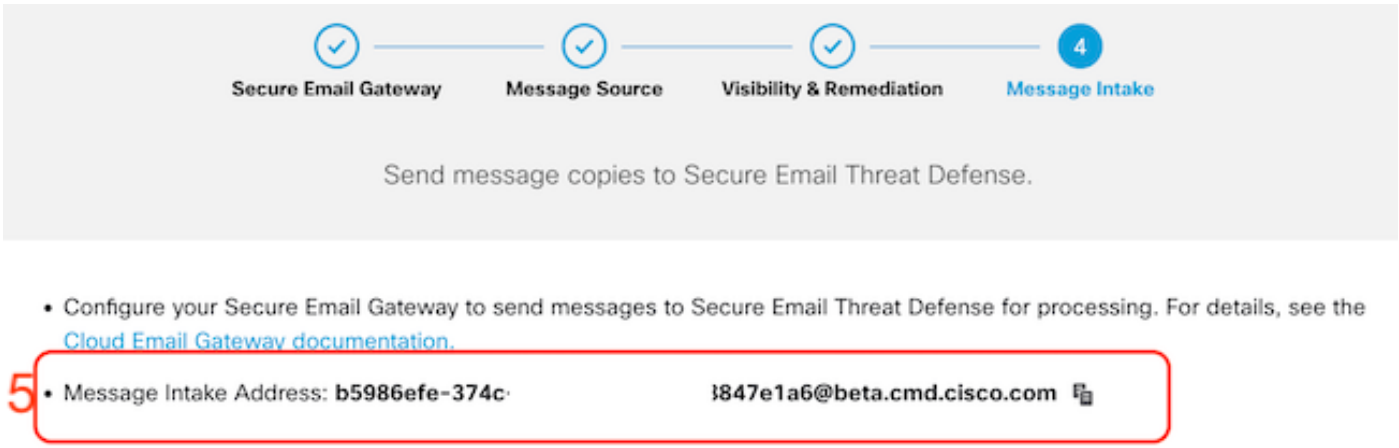


3. 消息方向=传入。

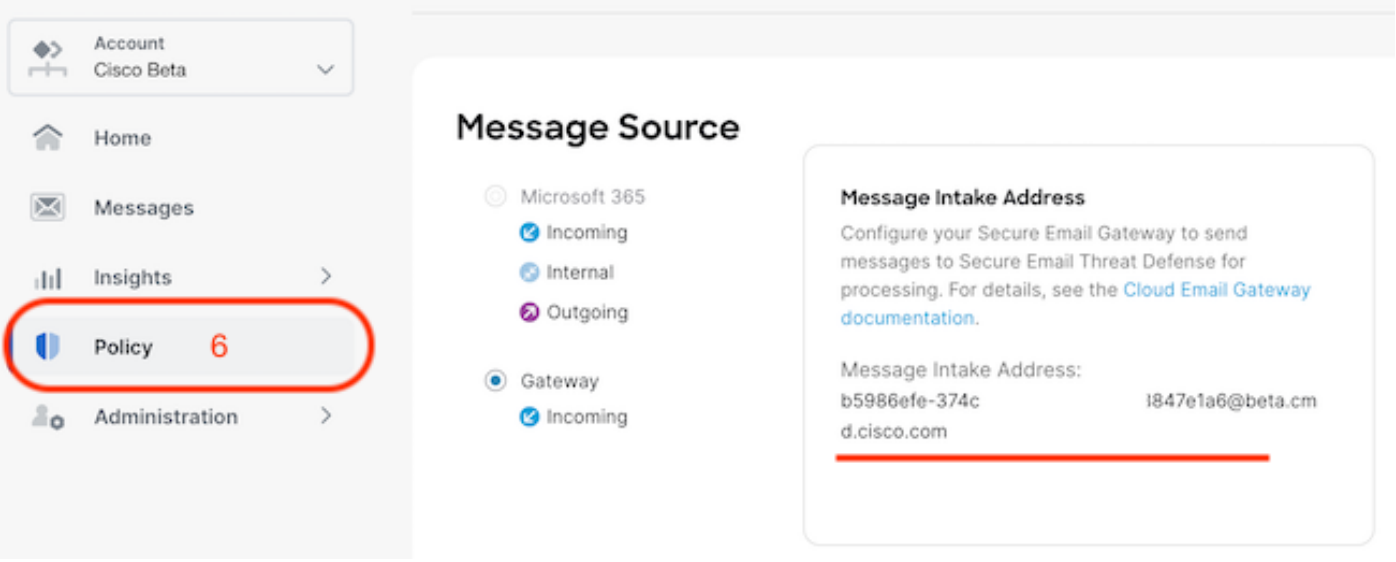
4. 无身份验证=仅可视性。



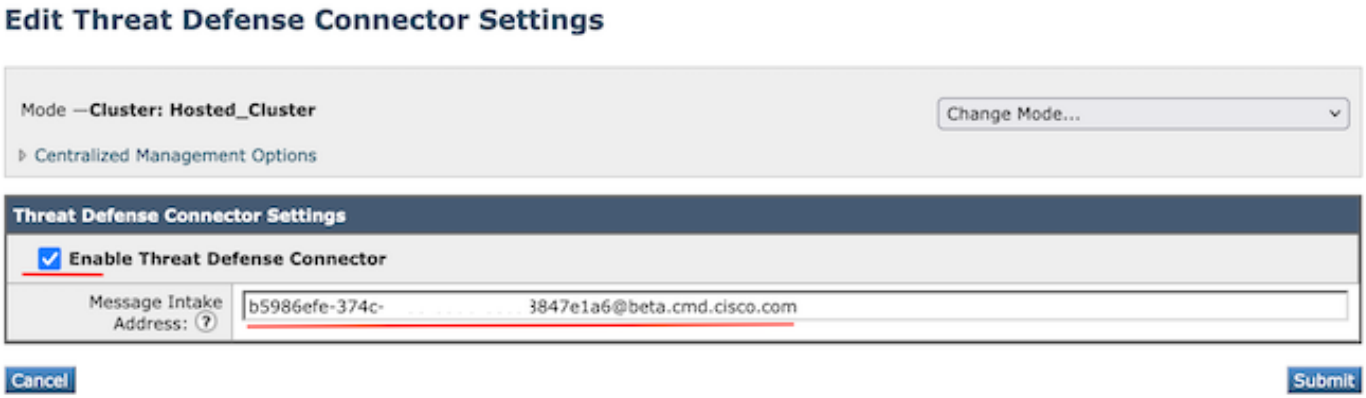
5. 接受第4步后显示消息接收地址。



6. 如果需要检索设置后的消息接收地址，请定位至“策略”菜单。

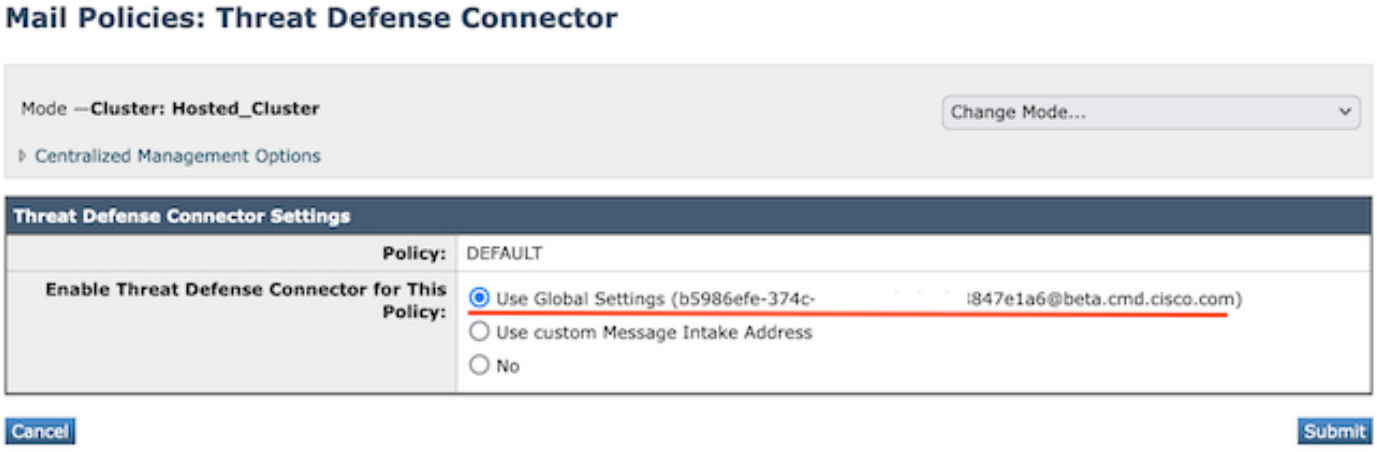


过渡到SEG WebUI，导航至Security Services（安全服务）> Threat Defense Connector Settings（威胁防御连接器设置）。



导航至Mail Policies（邮件策略）：

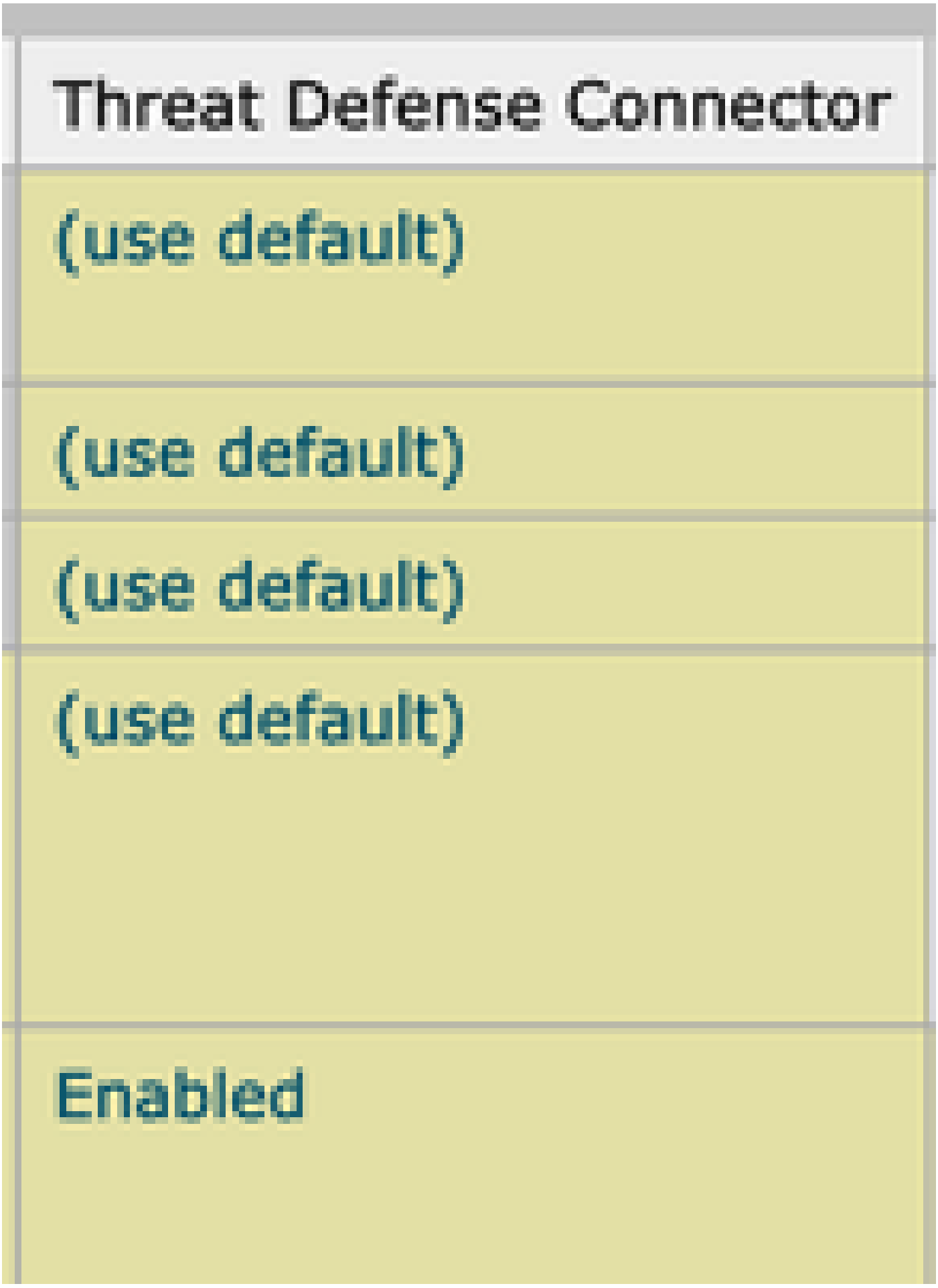
- 传入邮件策略
  - 右侧的最后一项服务是“Threat Defense Connector”。
- 设置链接首次显示“已禁用”。



自定义邮件接收地址将使用辅助SETD实例填充。

注意：使用自定义接收地址配置邮件策略匹配条件以捕获正确的域流量时，这一点非常重要。

设置的最终视图显示已配置服务的“已启用”值。


Threat Defense Connector
(use default)
(use default)
(use default)
(use default)
Enabled

验证

完成所有步骤后，邮件会填充SETD控制面板。

SEG CLI命令> tophosts显示活动传递的.tdc.queue计数器。

```
(Machine esa1.myesa.com)> tophosts

Status as of:                  Fri Feb 16 19:55:34 2024 CST
Hosts marked with '*' were down as of the last delivery attempt.

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

5   the.tdc.queue                   1      0    104,163          0          0
```

故障排除

TDC连接行为：

- 当目标队列中存在条目时，至少会打开3个连接
- 对于常规邮件目标队列，使用相同的逻辑动态生成更多连接。
- 一旦队列变为空或目标队列中没有足够的条目，打开的连接就会关闭。
- 根据表中的值执行重试。
- 在重试被耗尽或消息在队列中的时间过长（120秒）时，消息将从队列中删除

威胁防御连接器重试机制

错误案例	重试完成	重试次数
SMTP 5xx错误（503/552除外）	无	不适用
SMTP 4xx错误（包括503/552）	Yes	1
TLS错误	无	不适用
常规网络\连接错误、DNS错误等。	Yes	1

基于传送结果的TDC邮件日志示例

与TDC相关的日志条目包含日志文本之前的TDC：值。

样本呈现正常的TDC传输。

```
Fri Feb 16 21:19:22 2024 Info: TDC: MID 14501404 with Message-ID '<O7afv777xxreILg2OQ@gostrt-sstp-0>' e
Fri Feb 16 21:19:23 2024 Info: TDC: New SMTP DCID 4566150 interface 10.13.0.99 address 10.10.55.171 por
Fri Feb 16 21:19:23 2024 Info: DCID 4566150 TLS success protocol TLSv1.2 cipher ECDHE-RSA-AES128-GCM-SH
```

```
Fri Feb 16 21:19:23 2024 Info: TDC: Delivery start DCID 4566150 MID 14501404
Fri Feb 16 21:19:24 2024 Info: TDC: MID 14501404 successfully delivered for scanning with Cisco Secure
Fri Feb 16 21:19:24 2024 Info: Message finished MID 14501404 done
```

该示例在120秒超时后由于无法传送的消息而出现传送错误

```
Wed Nov 29 09:03:05 2023 Info: TDC: Connection Error: DCID 36 domain: the.tdc.queue IP: 10.10.0.3 port:
```

示例显示由于TLS错误而导致的传递错误。

```
Fri Feb 14 04:10:14 2024 Info: TDC: MID 1450012 delivery failed to Cisco Secure Email Threat Defense:TL
```

此示例显示的SETD日记帐地址无效，导致硬退回。

```
Wed Nov 29 09:07:16 2023 Info: TDC: MID 171 with Message-ID '<20231129090720.24911.11947@vm21bsd0050.cs
dress test@esa.example.com
Wed Nov 29 09:07:16 2023 Info: DNS Error esa.example.com MX - NXDomain
Wed Nov 29 09:07:16 2023 Info: TDC: Hard bounced - 5.1.2 - Bad destination host ('000', 'DNS Hard Error
Wed Nov 29 09:07:16 2023 Info:
TDC: MID 171 delivery failed to Cisco Secure Email Threat Defense: Hard Bounced.
Wed Nov 29 09:07:16 2023 Info: Bounced: DCID 0 MID 171 to RID 0 - Bounced by destination server with re
(MX) :
```

“邮件跟踪”(Message Tracking)仅显示指示邮件成功传递到SETD的单个行。

此示例显示由于TLS错误而导致的传送错误。

2024年2月16日21:19:24 (GMT -06:00)	TDC：邮件14501404已成功传送给使用思科安全邮件威胁防御进行扫描。

相关信息

- 邮件安全设置指南
- 支持指南的思科安全电邮网关发布页面
- ETD用户指南

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。