根據策略配置安全郵件網關日誌記錄以保護郵件威脅防禦

目錄

簡介

本文檔介紹配置安全郵件網關(SEG)以執行安全郵件威脅防禦(SETD)的按策略日誌記錄的步驟。

必要條件

事先瞭解思科安全郵件網關(SEG)的一般設定和配置是有益的。

採用元件

此設定需要兩者；

- Cisco Secure Email Gateway (SEG) AsyncOS 15.5.1及更高版本
- 思科電子郵件威脅防禦(SETD)例項。
- 威脅防禦聯結器(TDC)。 「這兩個技術之間明確的聯絡。」

"本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路處於活動狀態，請確保您瞭解所有命令的潛在影響。」

概觀

Cisco SEG能夠與SETD整合，以提供額外的保護。

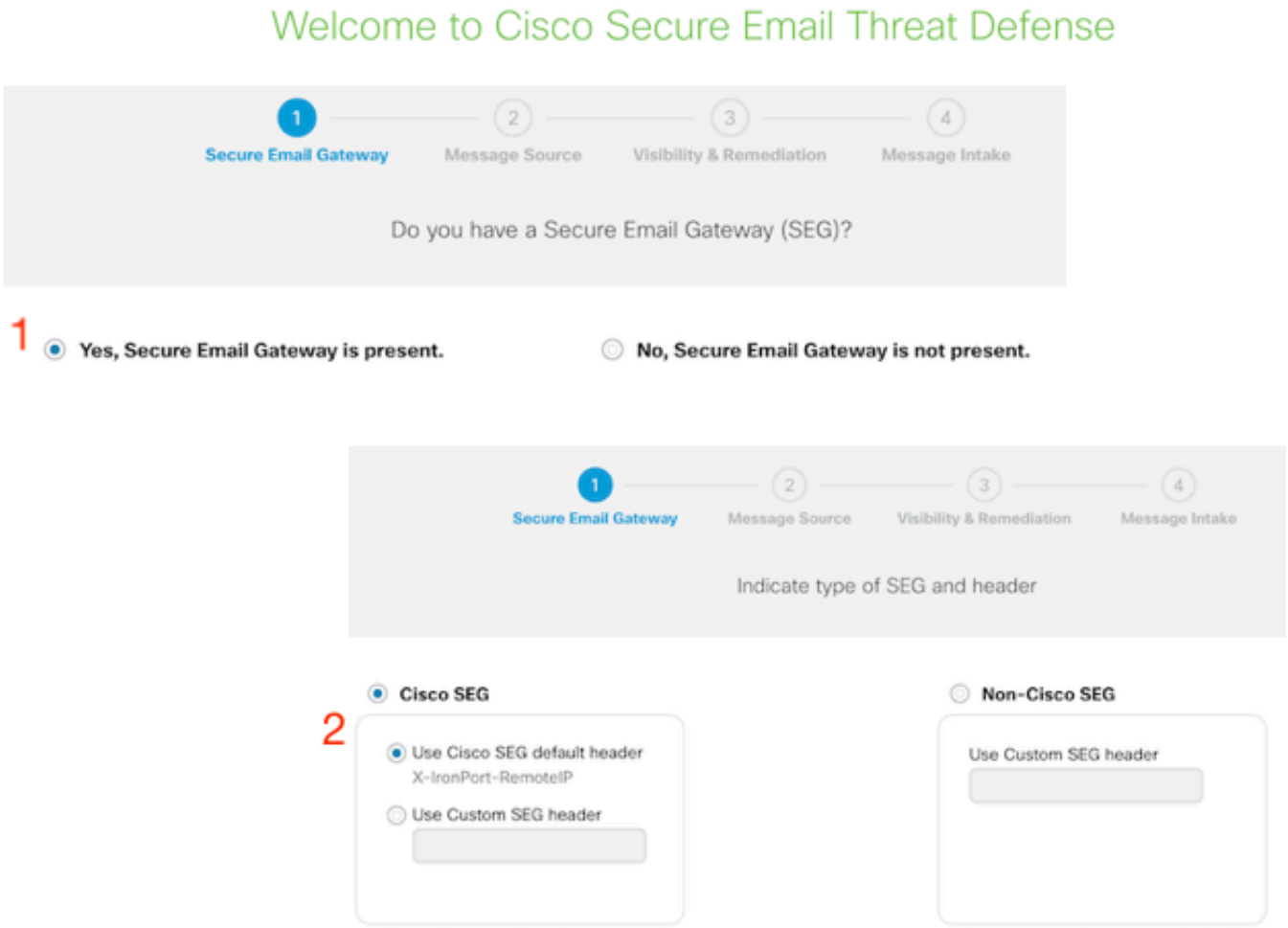
- SEG日誌操作會傳輸所有正常郵件的完整電子郵件。
- SEG提供了根據郵件策略匹配選擇傳入郵件流的選項。
- SEG Per Policy選項允許3種選擇：無掃描、預設郵件接收地址或自定義郵件接收地址。
    - 預設接收地址表示接受特定帳戶例項郵件的主SETD帳戶。
    - 自訂訊息接收位址代表接受不同定義網域郵件的第二個SETD帳戶。此案例適用於較複雜的SETD環境。

- 日誌消息具有SEG消息ID(MID)和目標連線ID DCID
- 傳遞佇列包含類似網域「the.tdc.queue」的值，以擷取SETD傳輸計數器。
  - 在此處可檢視「the.tdc.queue」活動計數器：cli>tophosts或SEG Reporting > Delivery Status（非CES）。
  - 「the.tdc.queue」表示相當於目標域名的威脅防禦聯結器(TDC)。

設定

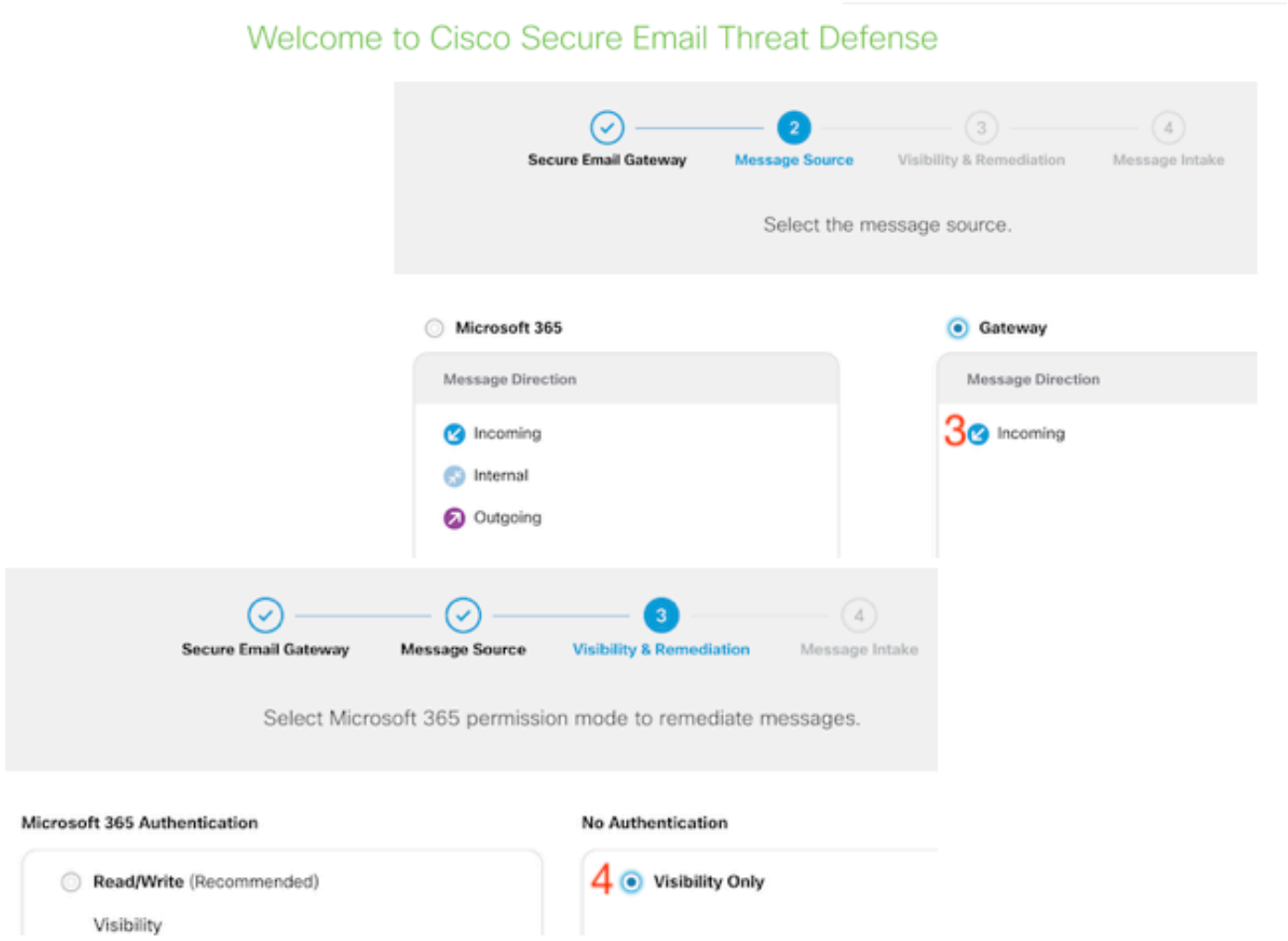
SETD初始設定步驟以生成「郵件接收地址」。

1. 是，安全電子郵件網關存在。
2. Cisco SEG

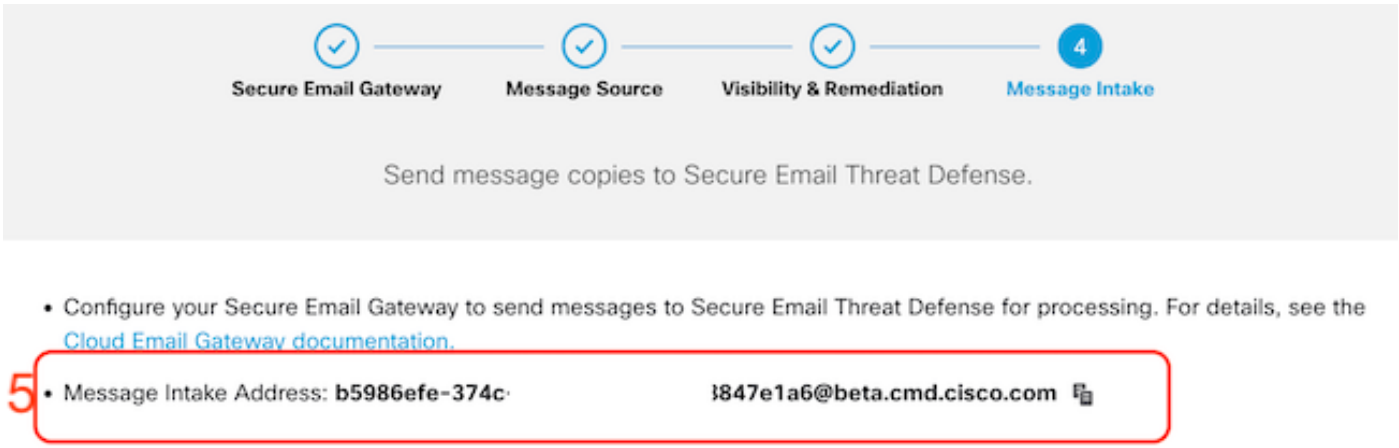


3. 消息方向=傳入。

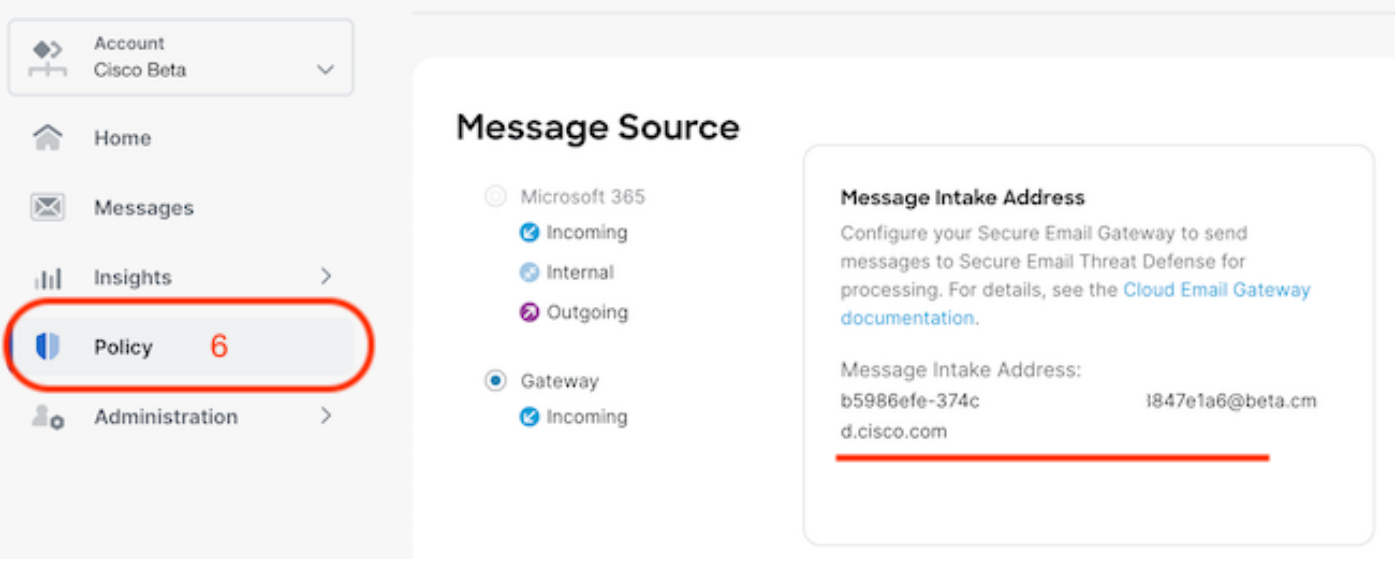
4. 無驗證=僅限可見性。



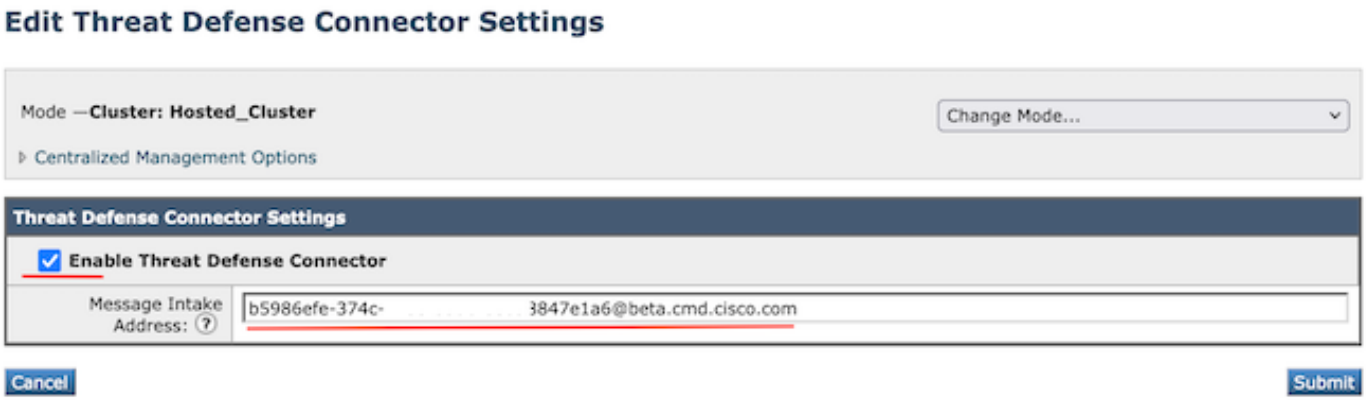
5. 接受步驟4後會顯示「訊息接收地址」。



6. 如果您在設定後需要擷取「訊息接收地址」，請切換作業選項至「政策」功能表。

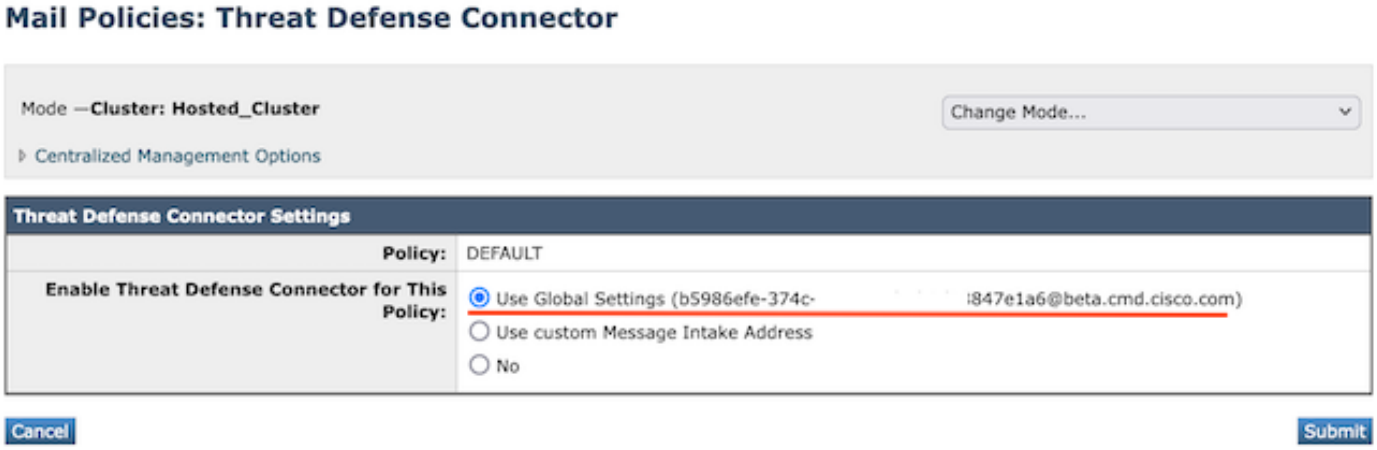


正在過渡到SEG WebUI，請導航到Security Services > Threat Defense Connector Settings。



導航至「郵件策略」：

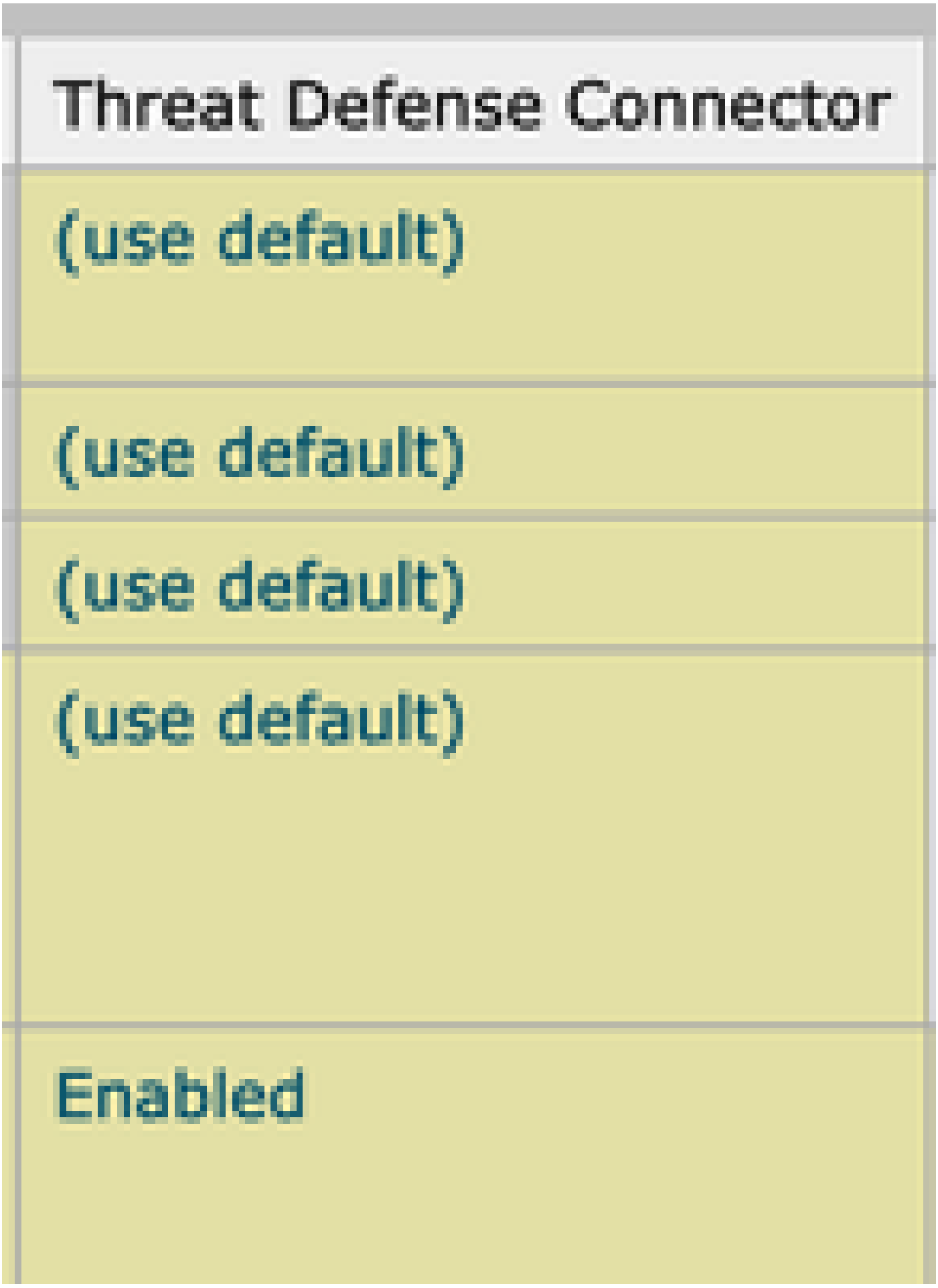
- 傳入郵件策略
  - 右邊的最後一項服務是「威脅防禦聯結器」。
- 設定連結首次顯示「已停用」。



自定義消息接收地址將使用輔助SETD例項填充。

注意：使用自定義接收地址配置郵件策略匹配條件以捕獲正確的域流量時，這一點非常重要。

設定的最終檢視顯示配置的服務的「已啟用」值。


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

驗證

完成所有步驟後，電子郵件將填充SETD控制台。

SEG CLI命令> tophosts顯示活動傳遞的.tdc.queue計數器。

```
(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
```

疑難排解

TDC連線行為：

- 當目標隊列中存在條目時，至少打開3個連線
- 對於常規電子郵件目標隊列，使用相同的邏輯動態生成更多的連線。
- 當佇列變成空白或目的地佇列中沒有足夠的專案時，開啟的連線就會關閉。
- 會根據表格中的值執行重試。
- 重試用完或訊息在佇列中停留太久（120秒）後，就會從佇列中移除訊息

威脅防禦聯結器重試機制

錯誤案例	重試完成	重試次數
SMTP 5xx錯誤（503/552除外）	否	不適用
SMTP 4xx錯誤（包括503/552）	是	1
TLS錯誤	否	不適用
一般網路\連線錯誤、DNS錯誤等。	是	1

基於傳遞結果的TDC郵件日誌示例

與TDC相關的日誌條目包含TDC：值在日誌文本之前。

樣本呈現正常的TDC傳遞。

```
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
```

在120秒超時到期後，由於無法傳送的消息，該示例顯示傳送錯誤

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

該示例由於TLS錯誤而出現傳送錯誤。

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

此示例顯示導致硬退回的無效SETD日記帳地址。

```
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) :
```

「郵件跟蹤」僅顯示一行，指示郵件成功傳遞到SETD。

這個範例顯示由於TLS錯誤而導致的傳遞錯誤。

2024年2月16日21:19:24 (GMT -06:00)	TDC：已成功傳遞郵件14501404供使用思科安全郵件威脅防禦進行掃描。

相關資訊

- 電子郵件安全設定指南
- 用於支援指南的思科安全郵件網關啟動頁面
- ETD使用者指南

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。