セキュリティで保護された電子メール脅威に対する防御を行うためのセキュリティで保護された電子メールゲートウェイのポリシーごとのジャーナリングの設定

内容

はじめに

このドキュメントでは、Secure Email Threat Defense(SETD)のポリシーごとのジャーナリングを実行するようにSecure Email Gateway(SEG)を設定する手順について説明します。

前提条件

Cisco Secure Email Gateway(SEG)の全般的な設定と設定に関する知識があれば役に立ちます。

使用するコンポーネント

この設定では、次の両方が必要です。

- Cisco Secure Email Gateway(SEG)AsyncOS 15.5.1以降
- Cisco Eメール脅威対策(SETD)インスタンス
- 脅威対策コネクタ(TDC)。「2つのテクノロジー間の定義された接続」

"このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください」

概要

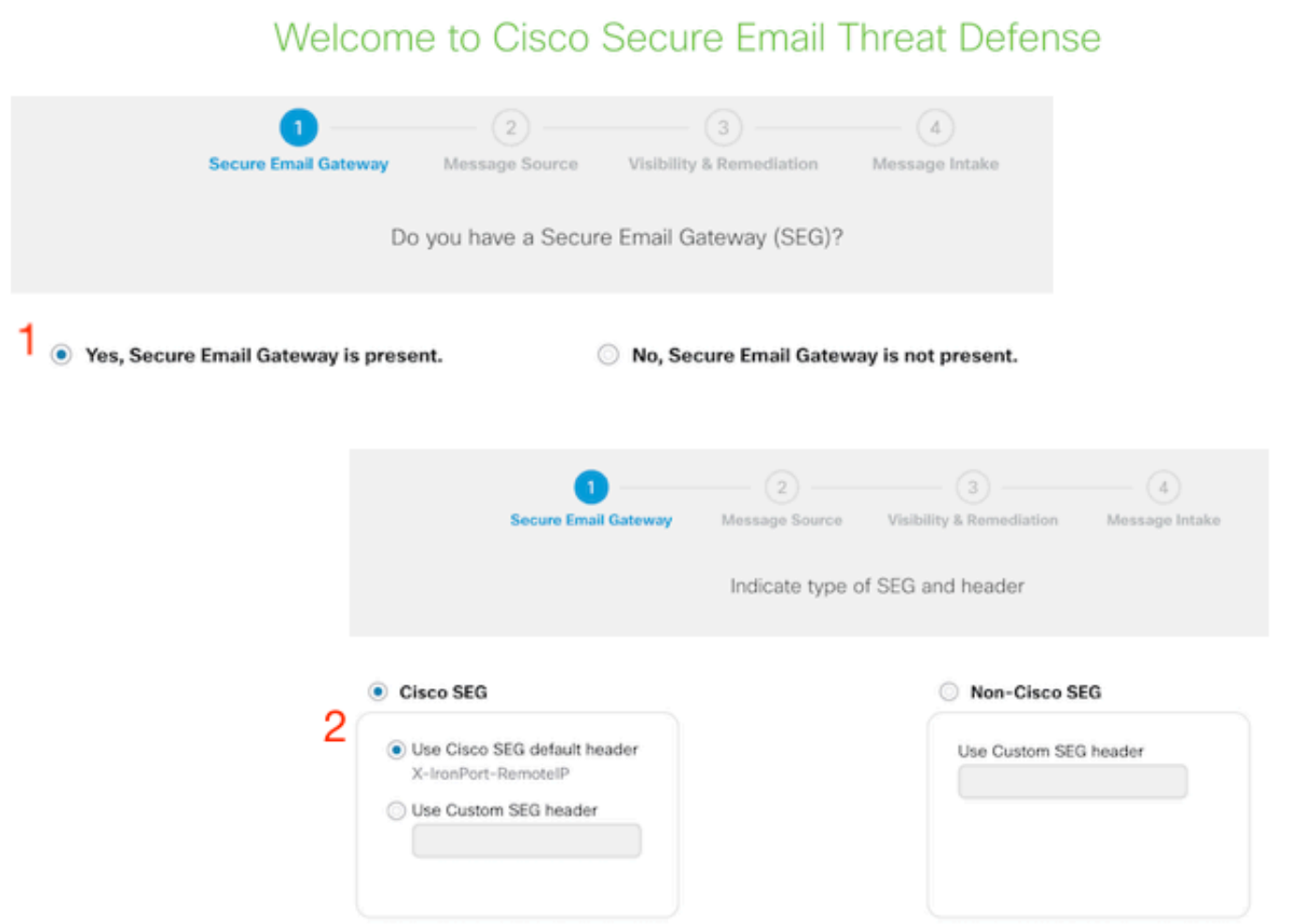
Cisco SEGはSETDと統合して保護を強化できます。

- SEGジャーナルアクションは、すべてのクリーンメッセージの完全な電子メールを転送します。
- SEGは、メールポリシーごとの一致に基づいて着信メールフローを選択的に選択するオプションを提供します。
- ポリシー単位のSEGオプションでは、スキャンなし、デフォルトのメッセージ受信アドレス、またはカスタムメッセージ受信アドレスの3つの選択肢があります。
  - デフォルトの受信アドレスは、特定のアカウントインスタンスのメールを受け取るプライマリSETDアカウントを表します。
  - カスタムメッセージ受信アドレスは、異なる定義済みドメインのメールを受け取る2番目のSETDアカウントを表します。このシナリオは、より複雑なSETD環境に適用されます。
- ジャーナリングされたメッセージには、SEGメッセージID(MID)と宛先接続ID(DCID)があります
- 配信キューには、SETD転送カウンタをキャプチャするためのドメインに似た値「the.tdc.queue」が含まれています。
  - 「the.tdc.queue」アクティブカウンタは、cli>tophosts（非CESの場合）またはSEG Reporting > Delivery Status（非CESの場合）で確認できます。
  - 「.tdc.queue」は、宛先ドメイン名に相当する脅威対策コネクタ(TDC)を表します。

設定

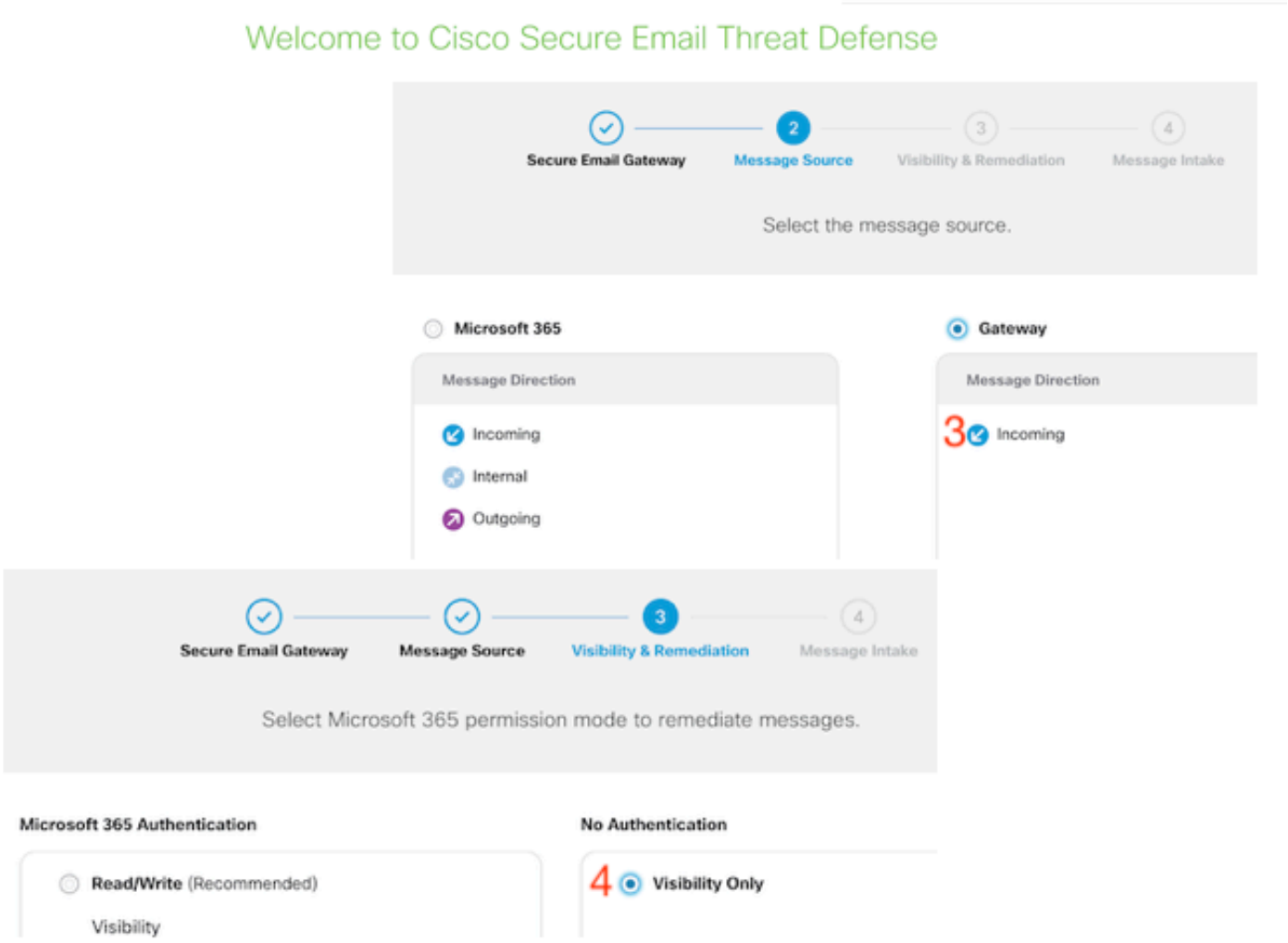
「メッセージ受信アドレス」を生成するためのSETDの初期セットアップ手順。

1. はい、セキュアEメールゲートウェイが存在します。
2. シスコのSEG

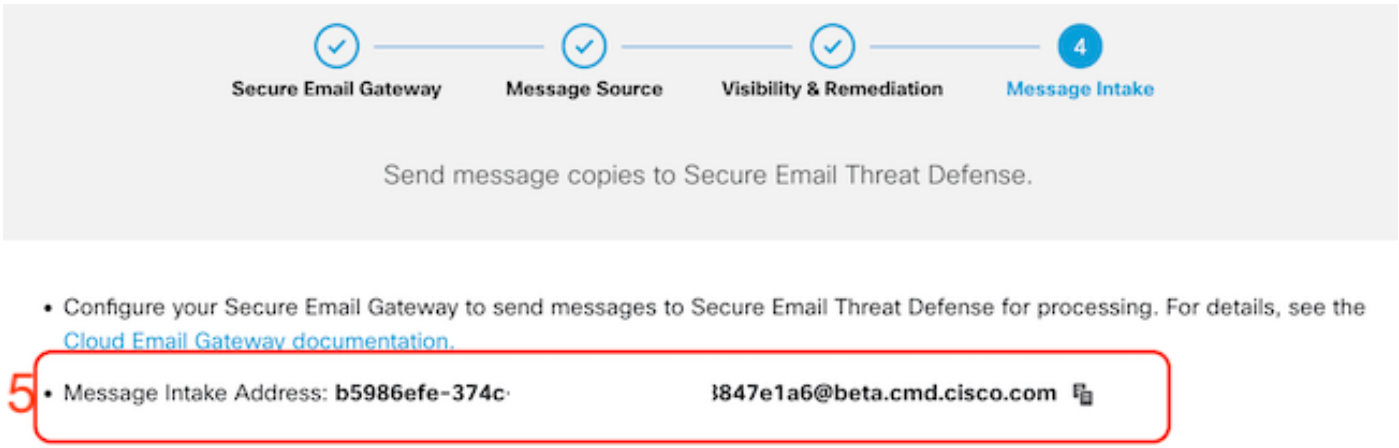


3. メッセージの方向=着信。

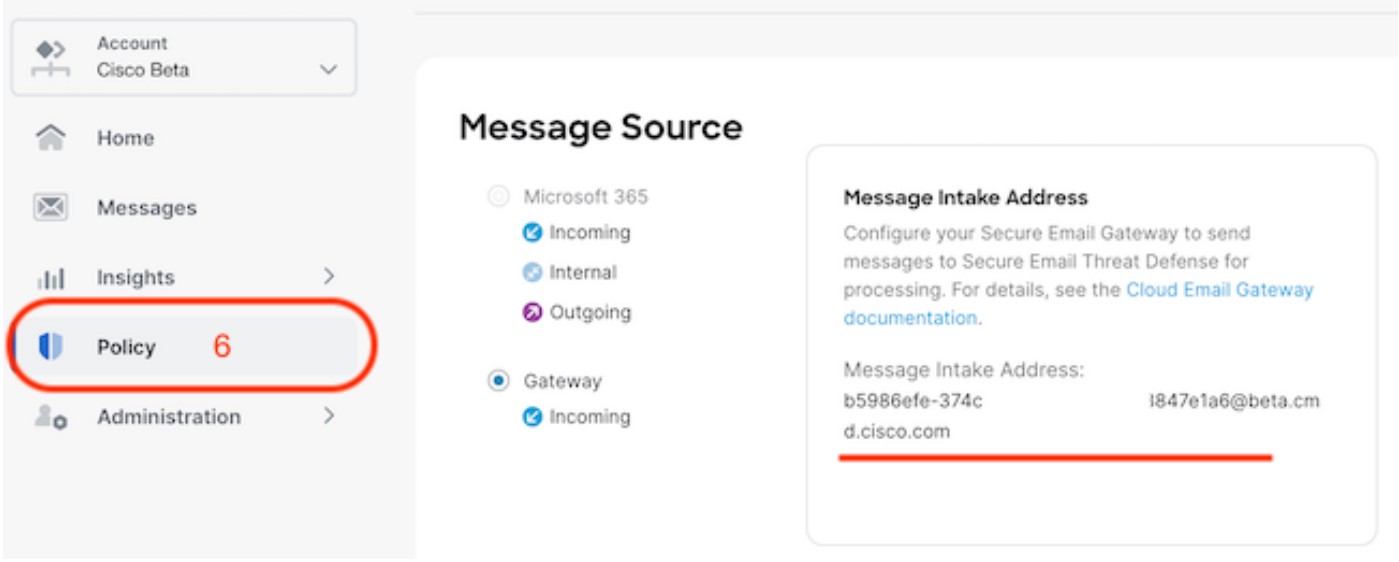
4. 認証なし=表示のみ。



5. メッセージの受信アドレスは、ステップ4が受け入れられた後で表示されます。



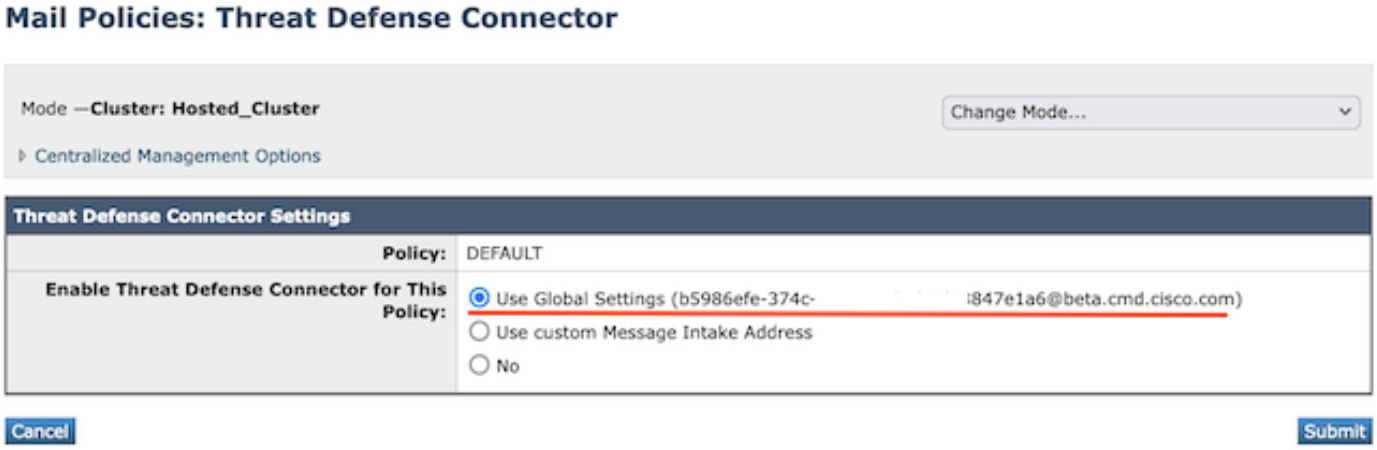
6. セットアップ後にメッセージ受信アドレスを取得する必要がある場合は、[ポリシー]メニューに移動します。



SEG WebUIに移行し、Security Services > Threat Defense Connector Settingsに移動します。

メールポリシーに移動します。

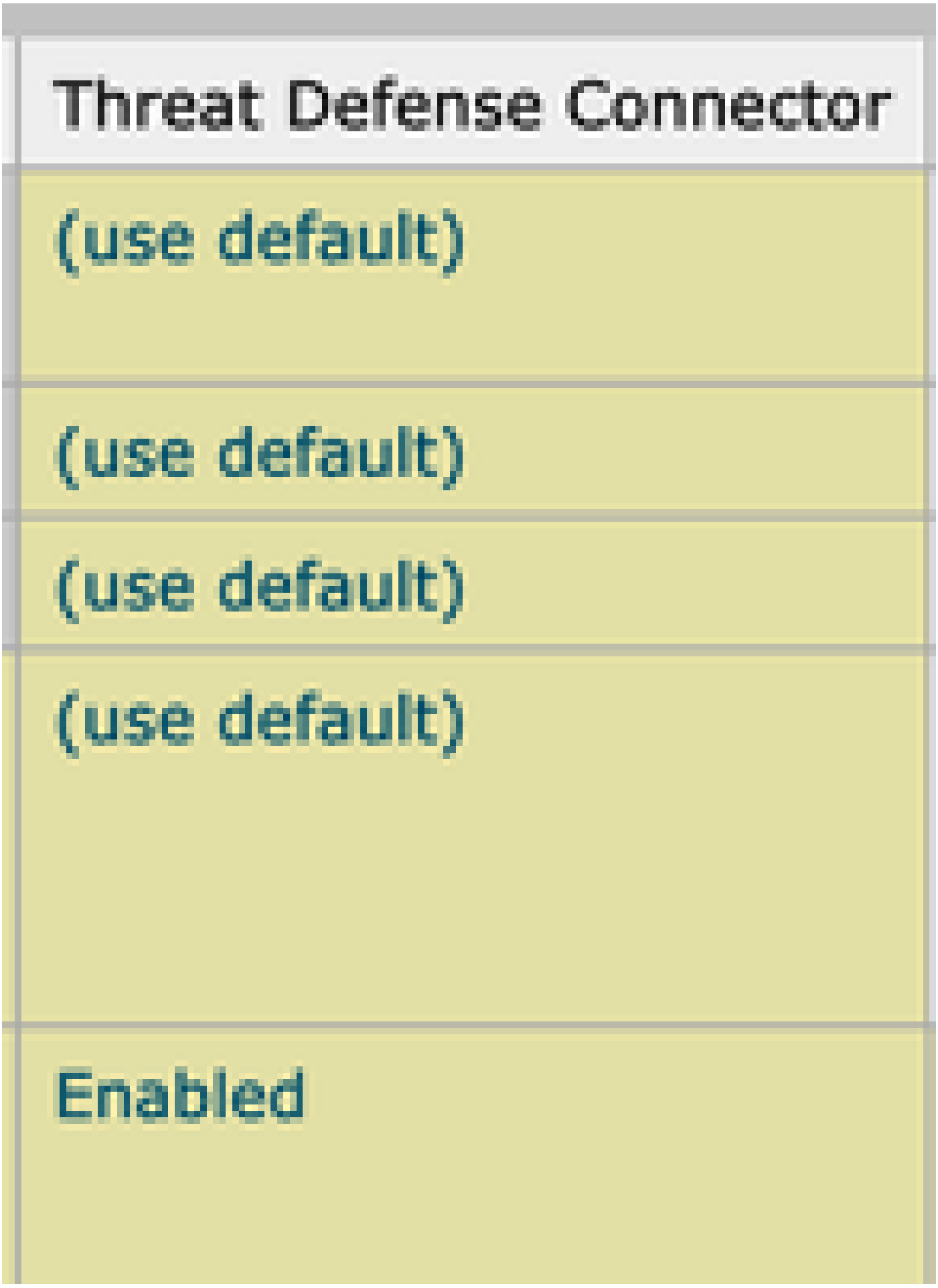
- 受信メール ポリシー
  - 右側の最後のサービスは「脅威対策コネクタ」です。
- 設定リンクには、初めて設定する場合は「Disabled」と表示されます。



カスタムメッセージ受信アドレスは、セカンダリSETDインスタンスを使用して入力されます。

注：カスタム受信アドレスを使用してメールポリシーの一致基準を設定し、正しいドメイントラフィックをキャプチャする場合は、これが重要です。

設定の最終的なビューには、設定済みサービスの値「Enabled」が表示されます。


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

確認

すべての手順が完了すると、電子メールがSETDダッシュボードに入力されます。

SEG CLIコマンド> tophostsは、アクティブな配信の.tdc.queueカウンタを表示します。

```
(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
```

トラブルシュート

TDC接続動作：

- 宛先キューにエントリが存在する場合、少なくとも3つの接続が開かれます
- それ以降の接続は、通常の電子メール宛先キューと同じロジックを使用して動的に生成されます。
- 開いている接続は、キューが空になるか、宛先キューに十分なエントリがなくなると閉じられます。
- 再試行は、テーブル内の値に従って実行されます。
- 再試行が終わった後、またはメッセージがキューに長すぎる時間（120秒）入っている場合、メッセージはキューから削除されます

脅威対策コネクタの再試行メカニズム

エラーケース	再試行が完了	再試行回数
SMTP 5xxエラー（503/552を除く）	いいえ	N/A
SMTP 4xxエラー（503/552を含む）	Yes	1
TLSエラー	いいえ	N/A
一般的なネットワーク\接続エラー、DNSエラーなど。	Yes	1

配信結果に基づくTDCメールログのサンプル

TDC関連のログエントリには、ログテキストの前にTDC：値が含まれています。

サンプルは正常なTDC配信を示しています。

```
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
```

このサンプルでは、120秒のタイムアウトが経過した後に配信不能メッセージが原因で配信エラーが発生します

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

サンプルでは、TLSエラーが原因の配信エラーが示されています。

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

このサンプルでは、無効なSETDジャーナルアドレスが示され、ハードバウンスが発生します。

```
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) :
```

メッセージトラッキングには、SETDへのメッセージの配信が成功したことを示す1行だけが表示されます。

このサンプルでは、TLSエラーによる配信エラーが示されています。

2024年2月16日21:19:24 (GMT -06:00)	TDC：メッセージ14501404が、Cisco Secure Email Threat Defenseによるスキャン用に正常に配信されました。

関連情報

- Eメールセキュリティ設定ガイド
- サポートガイドへのCisco Secure Email Gateway起動ページ
- ETDユーザガイド

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。