Configurer la journalisation par stratégie de la passerelle de messagerie sécurisée pour sécuriser la défense contre les menaces de messagerie

Table des matières

Introduction

Conditions préalables

- Composants utilisés

Aperçu

Configurer

Vérifier

Dépannage

- Comportement de la connexion TDC :

Introduction

Ce document décrit les étapes de configuration de la passerelle de messagerie sécurisée (SEG) pour effectuer la journalisation par stratégie pour la défense contre les menaces de messagerie sécurisée (SETD).

Conditions préalables

Une connaissance préalable des paramètres généraux et de la configuration de la passerelle de messagerie sécurisée Cisco (SEG) est utile.

Composants utilisés

Cette configuration nécessite les deux ;

- Cisco Secure Email Gateway (SEG) AsyncOS 15.5.1 et versions ultérieures
- Instance Cisco Email Threat Defense (SETD).
- Connecteur TDC (Threat Defense Connector). "Le lien défini entre les deux technologies."

"Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est actif, assurez-vous de comprendre l'impact potentiel de toute commande. »

Aperçu

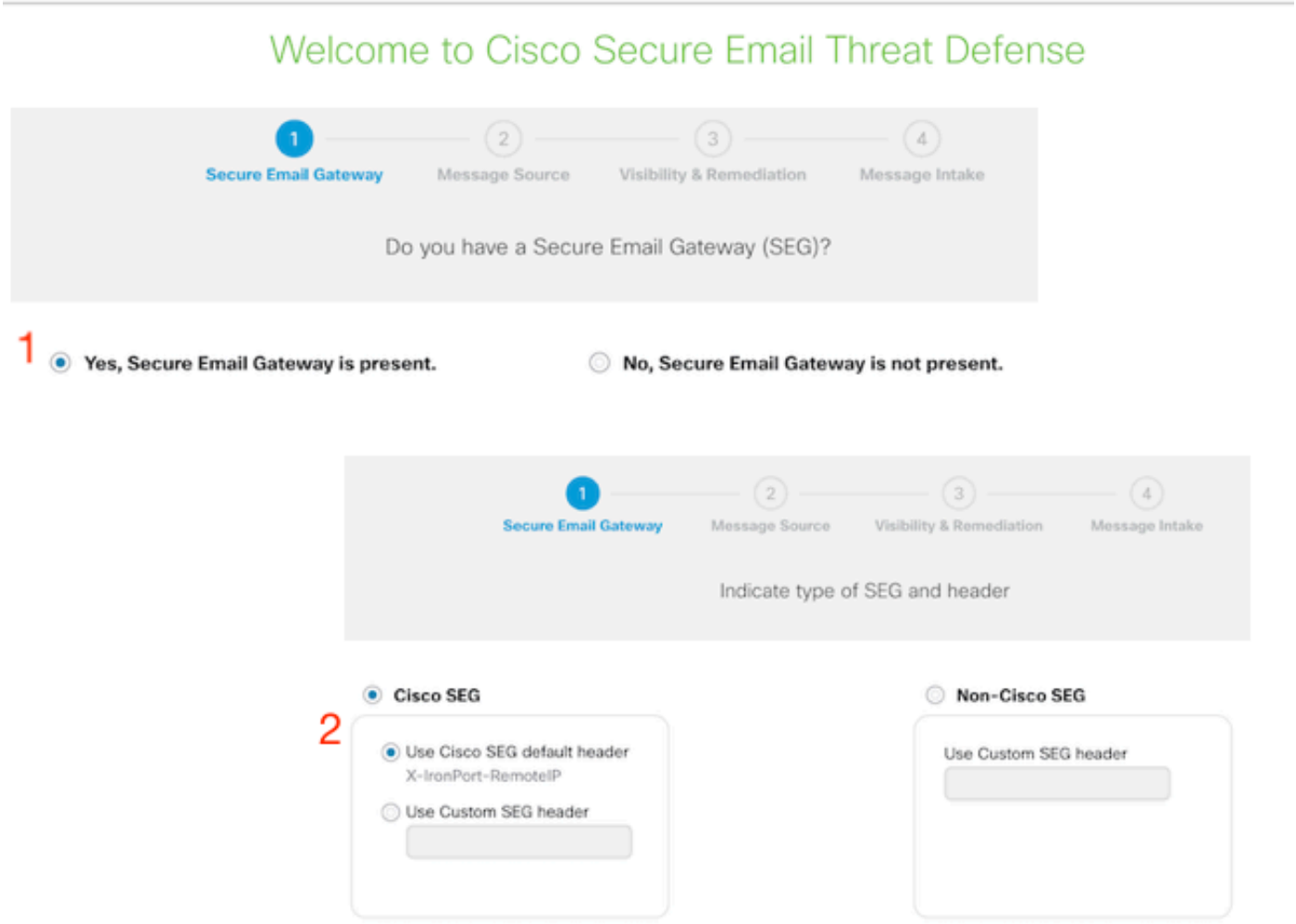
Le SEG Cisco est capable de s'intégrer au SETD pour une protection supplémentaire.

- L'action de journal SEG transfère l'e-mail complet pour tous les messages sains.
- Le SEG offre la possibilité de choisir de manière sélective les flux de messages entrants en fonction d'une correspondance par stratégie de messagerie.
- L'option SEG Per Policy permet 3 choix : No Scan, Default Message Intake Address ou Custom Message Intake Address.
    - L'adresse d'entrée par défaut représente le compte SETD principal acceptant le courrier pour une instance de compte spécifique.
    - L'adresse d'entrée de message personnalisée représente un second compte SETD acceptant le courrier pour différents domaines définis. Ce scénario s'applique à des environnements SETD plus complexes.
- Les messages journalisés ont un ID de message SEG (MID) et un ID de connexion de destination DCID
- La file d'attente de remise contient une valeur similaire à un domaine, « the.tdc.queue », pour capturer les compteurs de transfert SETD.
    - Les compteurs actifs "the.tdc.queue" peuvent être affichés ici : cli>tophosts ou SEG Reporting > Delivery Status (non-CES).
    - « the.tdc.queue » représente le connecteur de défense contre les menaces (TDC) équivalent à un nom de domaine de destination.

Configurer

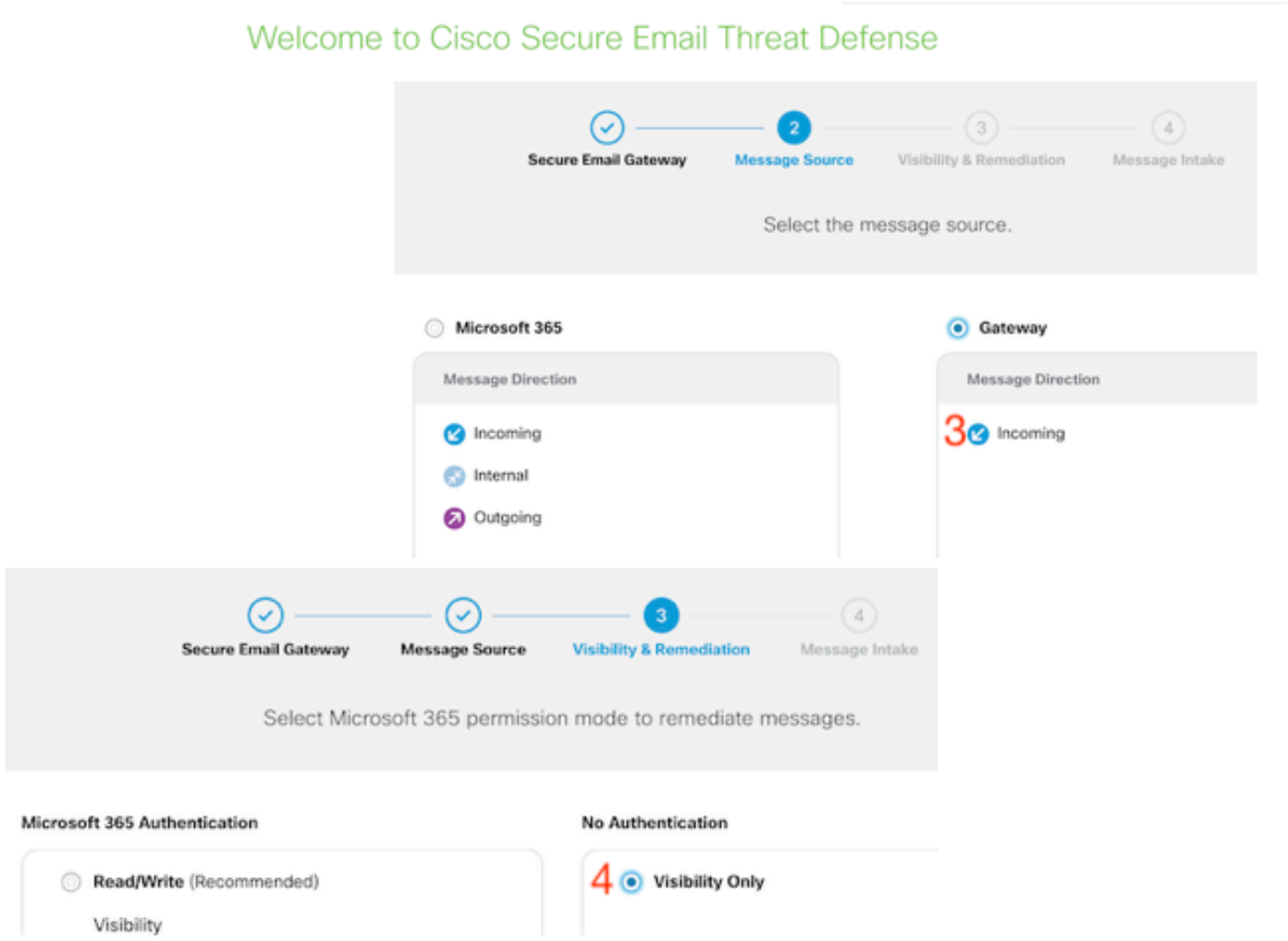
Étapes de configuration initiale SETD pour générer l'« adresse d'entrée de message ».

1. Oui, la passerelle de messagerie sécurisée est présente.
2. SEG Cisco

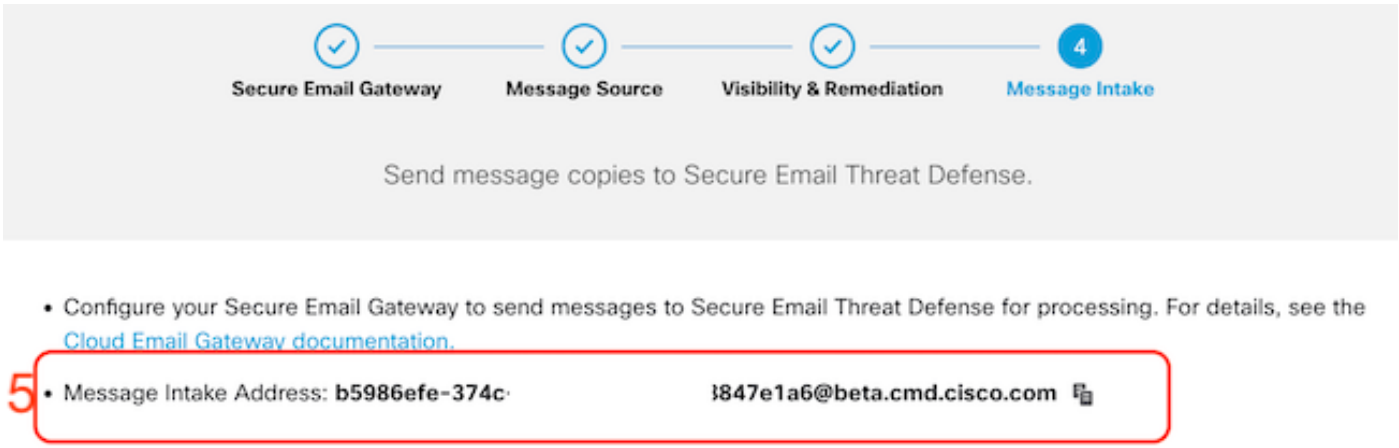


3. Direction du message = Entrant.

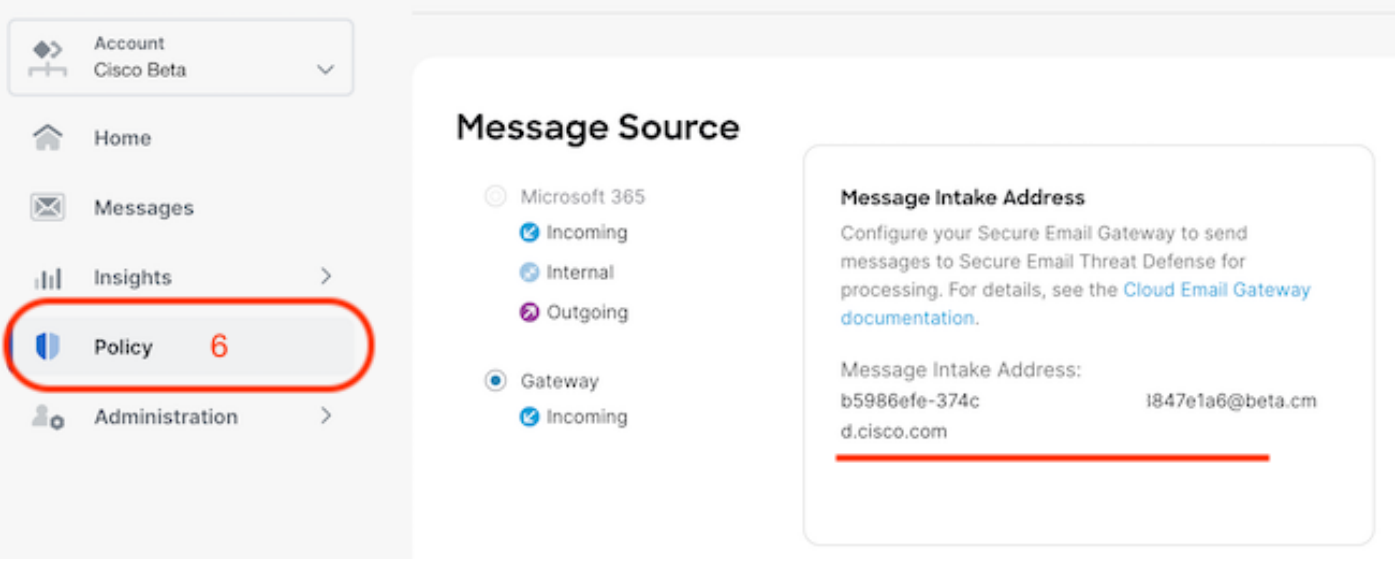
4. Aucune authentification = Visibilité uniquement.



5. L’adresse d’entrée du message est présentée après l’acceptation de l’étape 4.



6. Si vous devez récupérer l'adresse d'entrée du message après la configuration, accédez au menu Stratégie.

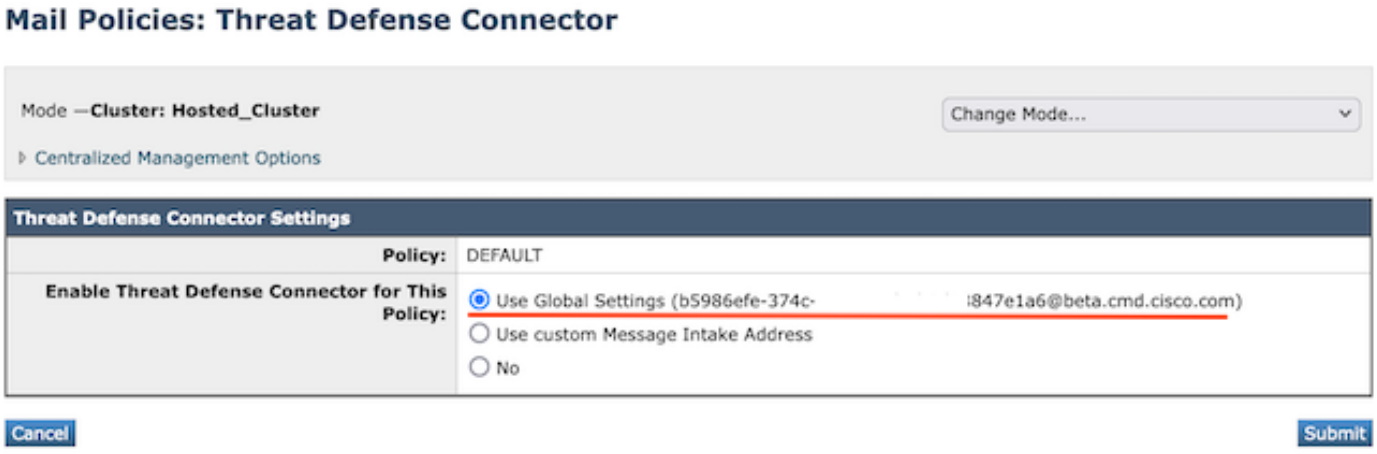


En passant à l'interface utilisateur Web de SEG, accédez à Services de sécurité > Paramètres du connecteur de défense contre les menaces.



Accédez à Politiques de messagerie :

- Stratégies de messages entrants
  - Le dernier service à droite est « Threat Defense Connector ».
- Le lien des paramètres affiche « Désactivé » pour la première configuration.

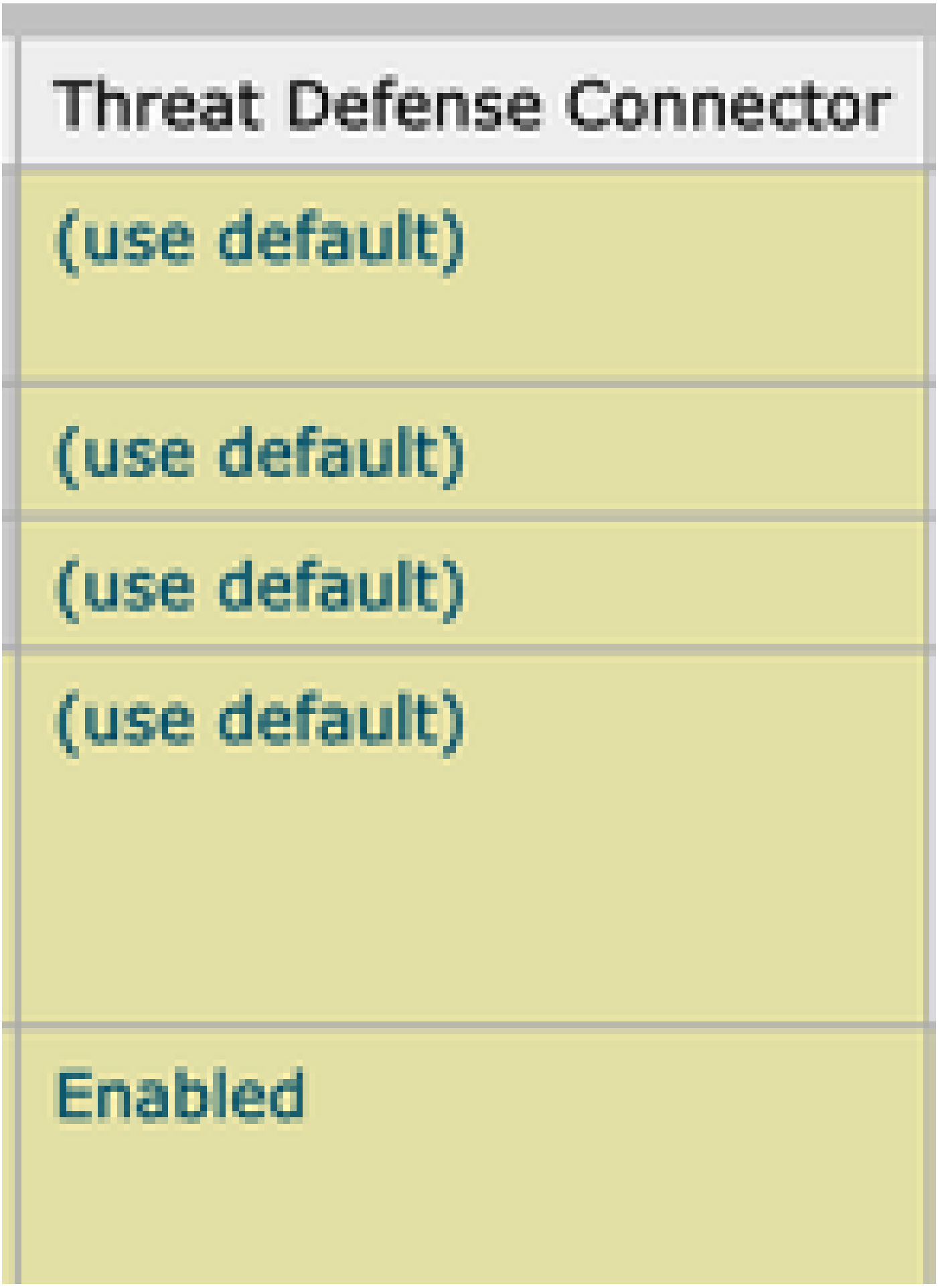


L'adresse d'entrée de message personnalisée doit être renseignée à l'aide d'une instance SETD secondaire.



Remarque : il est important d'utiliser l'adresse d'entrée personnalisée pour configurer les critères de correspondance de la stratégie de messagerie afin de capturer le trafic de domaine correct.

La vue finale du paramètre présente la valeur « Enabled » pour le service configuré.


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

Vérifier

Une fois toutes les étapes terminées, l'e-mail remplit le tableau de bord SETD.

La commande SEG CLI > tophosts affiche les compteurs.tdc.queue pour les livraisons actives.

```
(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
```

Dépannage

Comportement de la connexion TDC :

- Un minimum de 3 connexions sont ouvertes lorsque des entrées sont présentes dans la file d'attente de destination
- D'autres connexions sont générées dynamiquement en utilisant la même logique pour les files d'attente de destination de courrier électronique normales.
- Les connexions ouvertes sont fermées lorsque la file d'attente devient vide ou qu'il n'y a pas assez d'entrées présentes dans la file d'attente de destination.
- Les nouvelles tentatives sont effectuées conformément à la valeur de la table.
- Les messages sont retirés de la file d'attente après l'épuisement des tentatives ou si le message est dans la file d'attente pendant trop longtemps (120 secondes)

Mécanisme de relance du connecteur Threat Defense

Cas d'erreur	Nouvelle tentative terminée	Nombre de tentatives
Erreurs SMTP 5xx (sauf 503/552)	Non	S/O
Erreurs SMTP 4xx (y compris 503/552)	Oui	1
Erreurs TLS	Non	S/O
Réseau général \ Erreurs de connexion, erreurs DNS, etc.	Oui	1

Exemples de journaux de messagerie TDC basés sur les résultats de remise

Les entrées de journal relatives au TDC contiennent la valeur TDC : précédant le texte du journal.

L'échantillon présente une livraison TDC normale.

```
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
```

L'exemple présente une erreur de remise due au message non remis après l'expiration du délai d'attente de 120 secondes

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

L'exemple présente une erreur de remise due à une erreur TLS.

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

Cet exemple présente une adresse de journal SETD non valide, ce qui entraîne un renvoi forcé.

```
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) :
```

Le suivi des messages affiche simplement une seule ligne indiquant la livraison réussie du message à SETD.

Cet exemple présente une erreur de remise due à une erreur TLS.

16 février 2024 21:19:24 (GMT -06:00)	TDC : le message 14501404 a été transmis pour analyse avec Cisco Secure Email Threat Defense.

Informations connexes

- Guide de configuration de Email Security
- Guides d'assistance de la page de lancement de Cisco Secure Email Gateway
- Guide utilisateur ETD

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.