Configurazione di Secure Email Gateway per-Policy Journaling per la difesa delle minacce di posta elettronica

Sommario

Introduzione

Prerequisiti

- Componenti usati

Panoramica

Configurazione

Verifica

Risoluzione dei problemi

- Comportamento connessione TDC:

Introduzione

In questo documento viene descritto come configurare Secure Email Gateway (SEG) per eseguire il journal per policy per Secure Email Threat Defense (SETD).

Prerequisiti

È utile conoscere in anticipo le impostazioni generali e la configurazione di Cisco Secure Email Gateway (SEG).

Componenti usati

Questa configurazione richiede entrambi i requisiti:

- Cisco Secure Email Gateway (SEG) AsyncOS 15.5.1 e versioni successive
- Istanza di Cisco Email Threat Defense (SETD).
- Threat Defense Connector (TDC). "La connessione definita tra le due tecnologie."

"Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi".

Panoramica

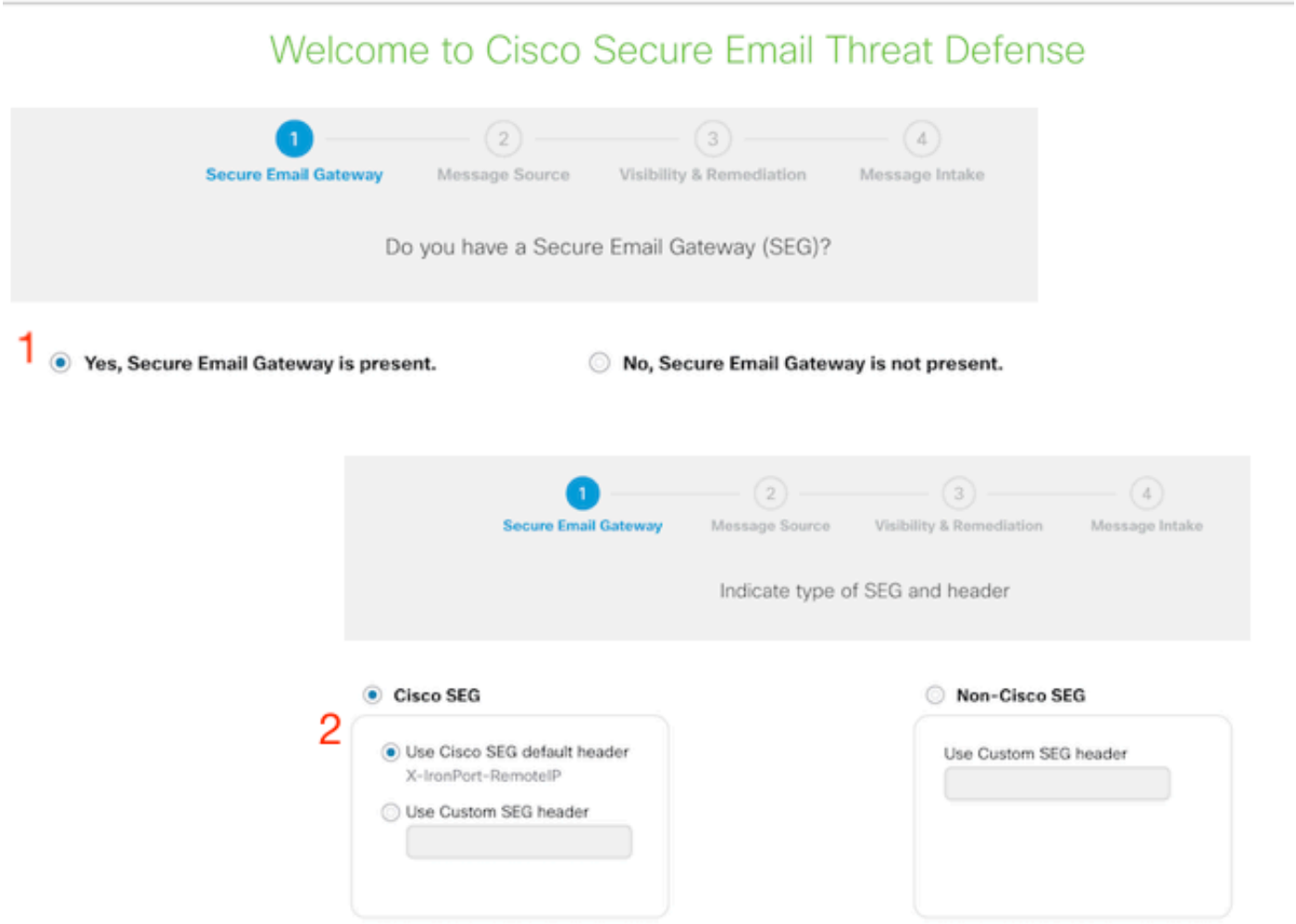
Cisco SEG può integrarsi con SETD per una protezione aggiuntiva.

- L'azione del giornale di registrazione SEG trasferisce l'e-mail completa per tutti i messaggi puliti.
- Il SEG consente di scegliere in modo selettivo i flussi di posta in arrivo in base a una corrispondenza Per-Mail-Policy.
- L'opzione SEG per criterio consente 3 scelte: Nessuna scansione, Indirizzo di immissione messaggio predefinito o Indirizzo di immissione messaggio personalizzato.
    - L'indirizzo di input predefinito rappresenta l'account SETD primario che accetta la posta per un'istanza di account specifica.
    - L'indirizzo di ricezione del messaggio personalizzato rappresenta un secondo account SETD che accetta la posta per diversi domini definiti. Questo scenario si applica ad ambienti SETD più complessi.
- I messaggi inseriti nel journal hanno un ID messaggio SEG (MID) e un ID connessione di destinazione DCID
- La coda di recapito contiene un valore simile al dominio "the.tdc.queue" per acquisire i contatori di trasferimento SETD.
    - I contatori attivi "the.tdc.queue" possono essere visualizzati qui: cli>tophosts o SEG Reporting > Delivery Status (non CES).
    - "the.tdc.queue" rappresenta il connettore TDC (Threat Defense Connector) equivalente a un nome di dominio di destinazione.

Configurazione

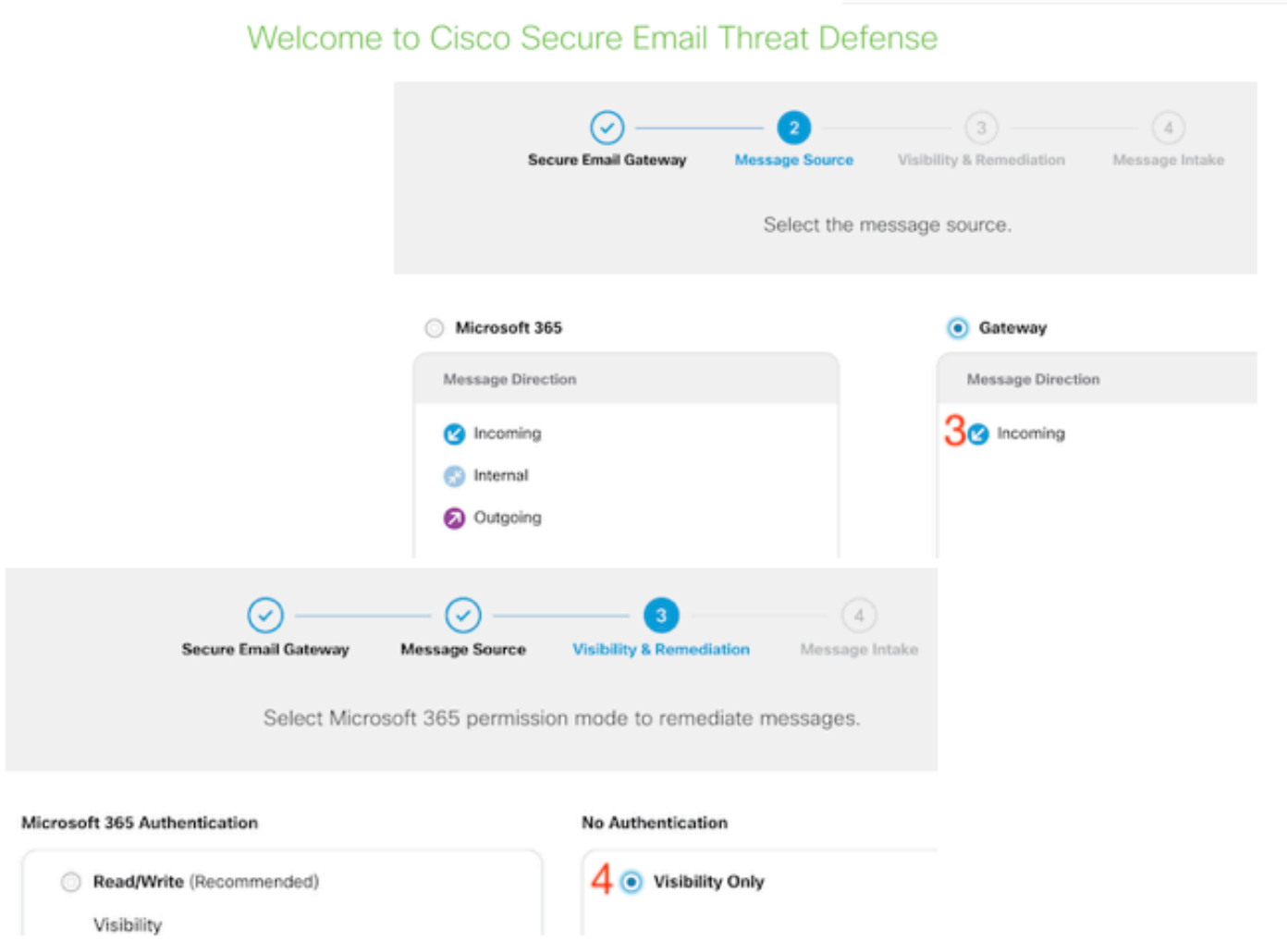
SETD esegue la procedura di impostazione iniziale per generare l'indirizzo di immissione del messaggio.

1. Sì, è presente Secure Email Gateway.
2. Cisco SEG

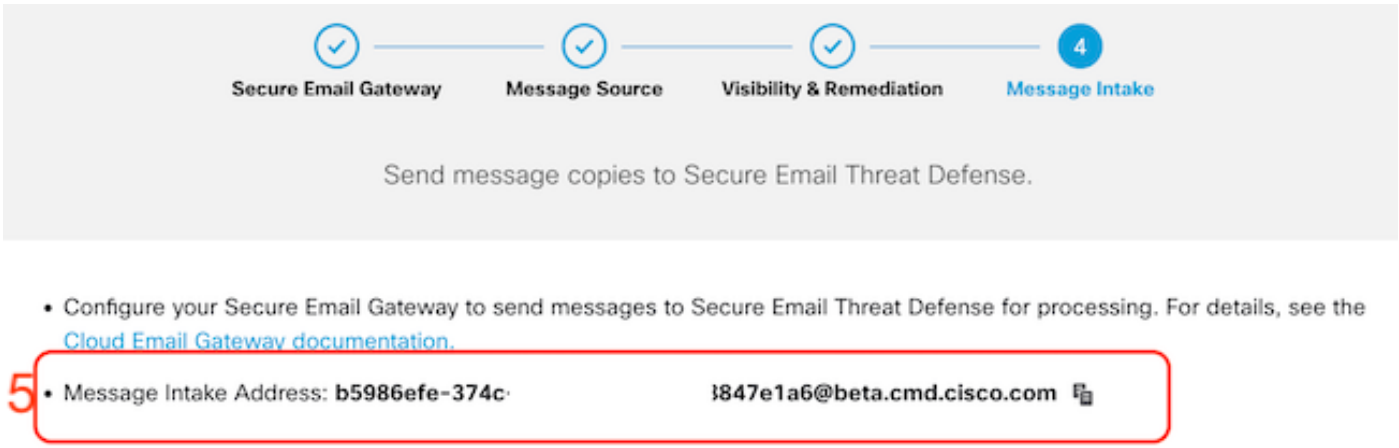


3. Direzione messaggio = In ingresso.

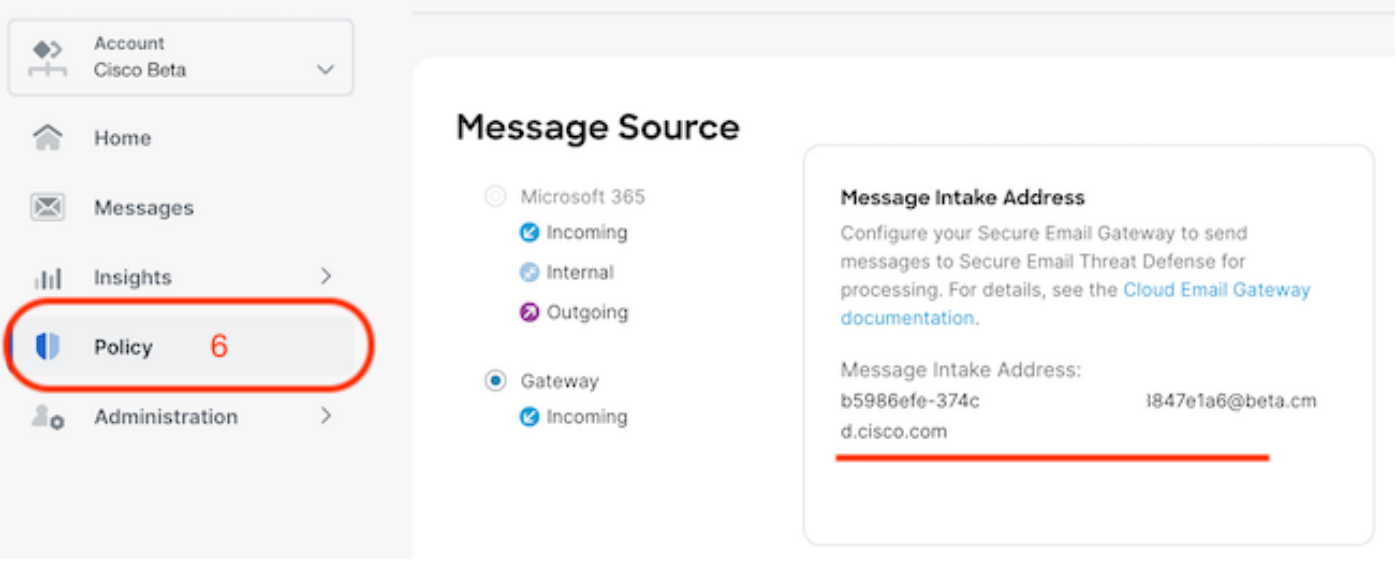
4. No Authentication = Solo visibilità.



5. L'indirizzo di ricezione del messaggio viene presentato dopo che il passo 4 è stato accettato.



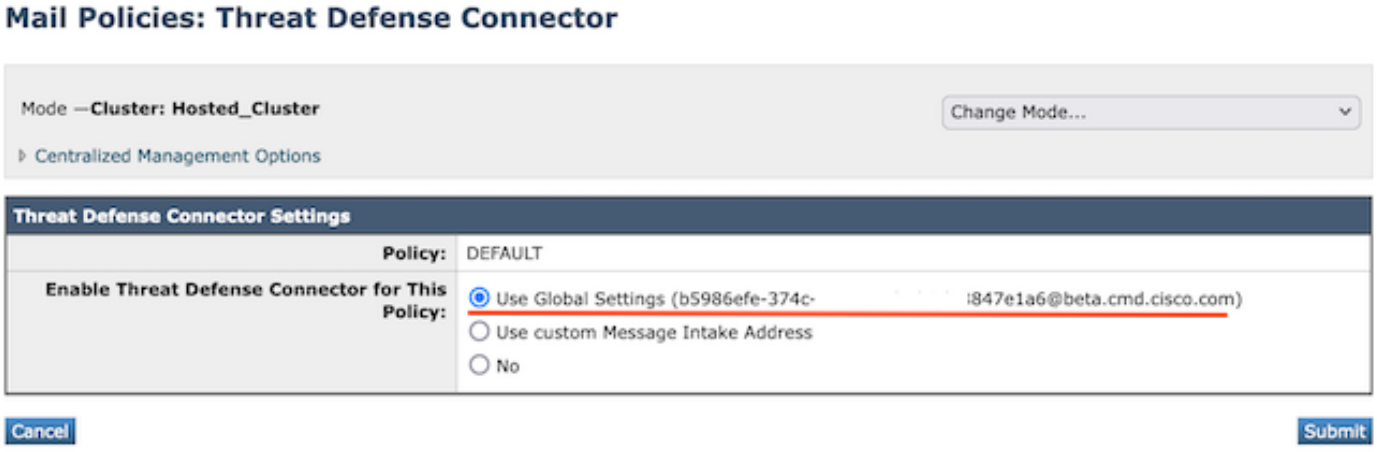
6. Se è necessario recuperare l'indirizzo di ricezione del messaggio dopo l'impostazione, passare al menu Criteri.



Per passare a SEG WebUI, selezionare Security Services > Threat Defense Connector Settings (Servizi di sicurezza > Impostazioni connettore difesa dalle minacce).

Passare a Criteri di posta:

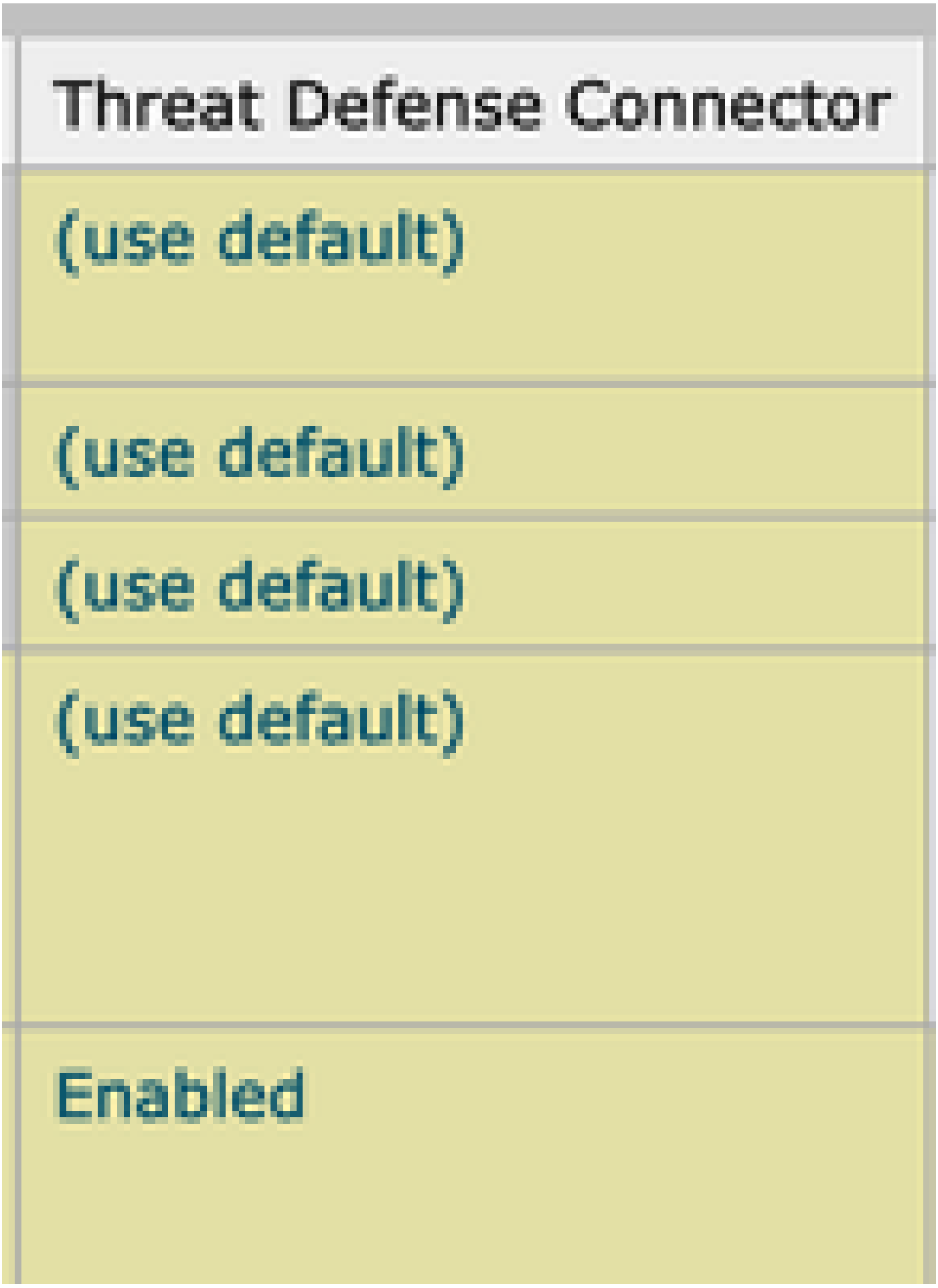
- Criteri posta in arrivo
  - L'ultimo servizio a destra è "Threat Defense Connector".
- Il collegamento delle impostazioni visualizza "Disattivato" per la prima configurazione.



L'indirizzo di immissione del messaggio personalizzato viene popolato utilizzando un'istanza SETD secondaria.

Nota: quando si utilizza l'indirizzo di input personalizzato per configurare i criteri di corrispondenza dei criteri di posta in modo da acquisire il traffico di dominio corretto, è importante.

La visualizzazione finale dell'impostazione presenta il valore "Enabled" per il servizio configurato.


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

Verifica

Una volta completati tutti i passaggi, l'e-mail inserisce i dati nel Dashboard SETD.

Il comando SEG CLI > tophosts visualizza i contatori .tdc.queue per le consegne attive.

```
(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
```

Risoluzione dei problemi

Comportamento connessione TDC:

- Almeno 3 connessioni vengono aperte quando sono presenti voci nella coda di destinazione
- Altre connessioni vengono generate dinamicamente utilizzando la stessa logica per le code di destinazione di e-mail normali.
- Le connessioni aperte vengono chiuse quando la coda diventa vuota o non è presente un numero sufficiente di voci nella coda di destinazione.
- I tentativi vengono eseguiti in base al valore nella tabella.
- I messaggi vengono rimossi dalla coda dopo l'esaurimento dei tentativi o se il messaggio rimane nella coda troppo a lungo (120 sec)

Meccanismo di ripetizione dei tentativi del connettore Threat Defense

Caso di errore	Riprova completato	Numero di tentativi
Errori SMTP 5xx (eccetto 503/552)	No	N/D
Errori SMTP 4xx (inclusi 503/552)	Sì	1
Errori TLS	No	N/D
Rete \ Errori di connessione, errori DNS e così via.	Sì	1

Esempi di log di posta TDC basati sui risultati del recapito

Le voci di log relative a TDC contengono il valore TDC: che precede il testo del log.

L'esempio presenta una consegna 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
```

Nell'esempio viene illustrato un errore di recapito causato dal messaggio non recapitato dopo la scadenza del timeout di 120 secondi

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

Nell'esempio viene visualizzato un errore di recapito causato da un errore TLS.

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

In questo esempio viene presentato un indirizzo del journal SETD non valido che determina un rimbalzo a freddo.

```
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) :
```

Verifica messaggi visualizza una sola riga che indica la corretta consegna del messaggio a SETD.

In questo esempio viene illustrato un errore di recapito causato da un errore TLS.

16 feb 2024 21:19:24 (GMT -06:00)	TDC: il messaggio 14501404 è stato recapitato correttamente per la scansione con Cisco Secure Email Threat Defense.

Informazioni correlate

- Guida alla configurazione di Email Security
- Pagina di avvio di Cisco Secure Email Gateway per il supporto delle guide
- Guida per l'utente ETD

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).