Configureer beveiligde e-mailgateway per beleid voor journalistiek om bedreigingsbescherming voor e-mail te beveiligen

Inhoud

Inleiding

Dit document beschrijft stappen om de Secure Email Gateway (SEG) te configureren om Per-Policy Journaling uit te voeren voor Secure Email Threat Defence (SETD).

Voorwaarden

Voorafgaande kennis van de algemene instellingen en configuratie van Cisco Secure Email Gateway (SEG) is nuttig.

Gebruikte componenten

Voor deze instelling zijn beide nodig:

- Cisco Secure Email Gateway (SEG) AsyncOS 15.5.1 en nieuwer
- Cisco Email Threat Defense (SETD)-instantie.
- Threat Defense Connector (TDC). "De gedefinieerde verbinding tussen de twee technologieën."

"De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, zorg er dan voor dat u de mogelijke impact van elke opdracht begrijpt."

Overzicht

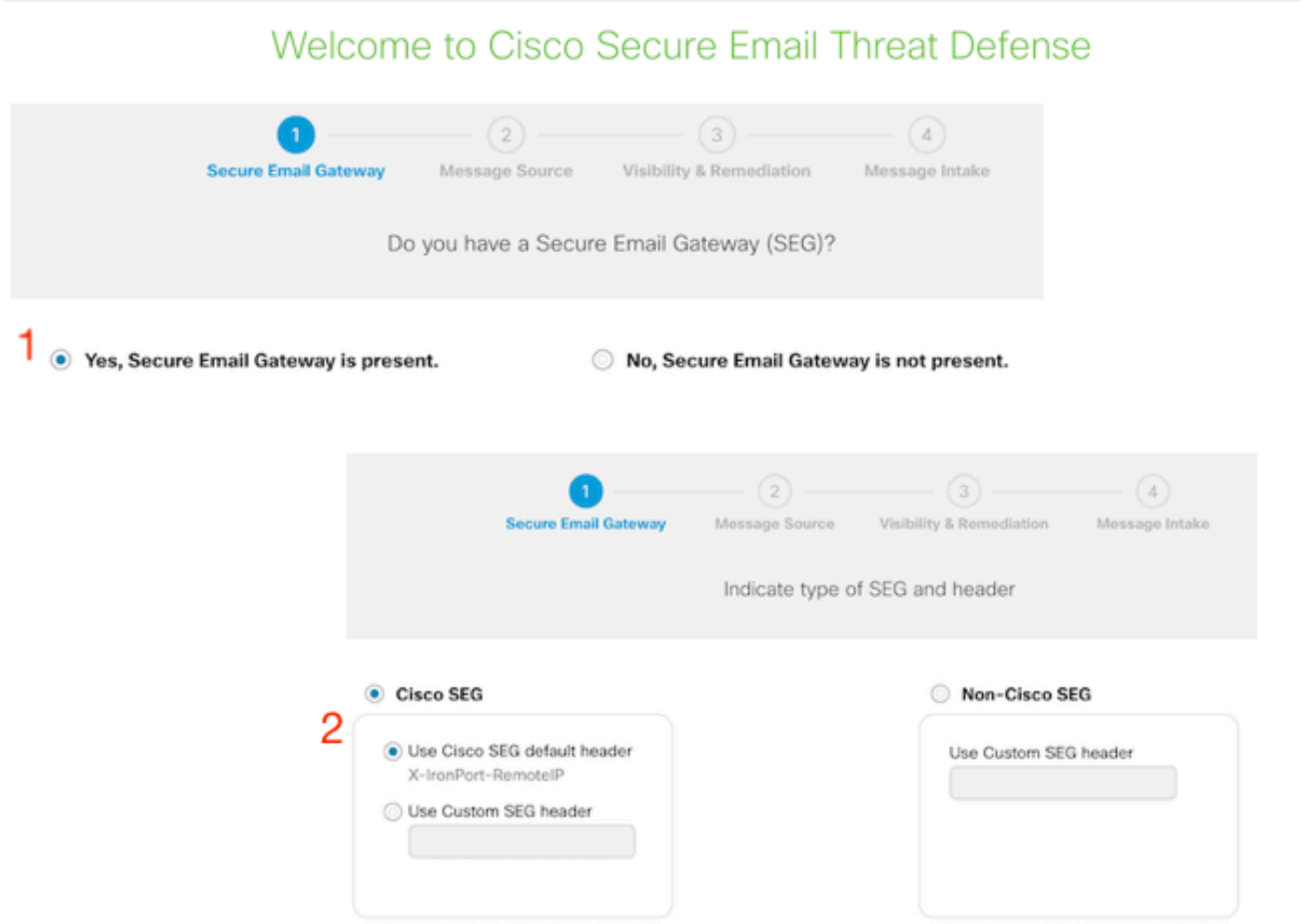
De Cisco SEG is in staat om met SETD te integreren voor extra bescherming.

- De dagboekactie SEG brengt de volledige e-mail voor alle schone berichten over.
- De SEG biedt de mogelijkheid om selectief inkomende mailstromen te kiezen op basis van een overeenkomst per-mail-beleid.
- De optie SEG per beleid staat 3 keuzes toe; geen scannen, standaard bericht inname adres, of aangepaste bericht inname adres.
    - Het Default Intake Address staat voor de primaire SETD-account die post voor een specifieke account accepteert.
    - Het Aangepaste Berichtinnameadres staat voor een tweede SETD-account die e-mail voor verschillende gedefinieerde domeinen accepteert. Dit scenario is van toepassing op complexere SETD-omgevingen.
- Journalistieke berichten hebben een SEG Message ID (MID) en een Bestemmings-verbinding-ID (DCID)
- De Leveringswachtrij bevat een waarde die lijkt op een domein, "the.tdc.Queue", om SETD-overdrachttellers op te nemen.
    - De actieve tellers van "the.tdc.row" kunnen hier worden bekeken: cli>tophosts of SEG Reporting > Leveringsstatus (niet-CES).
    - "the.tdc.wachtrij" vertegenwoordigt de Threat Defense Connector (TDC) die equivalent is aan een doeldomeinnaam.

Configureren

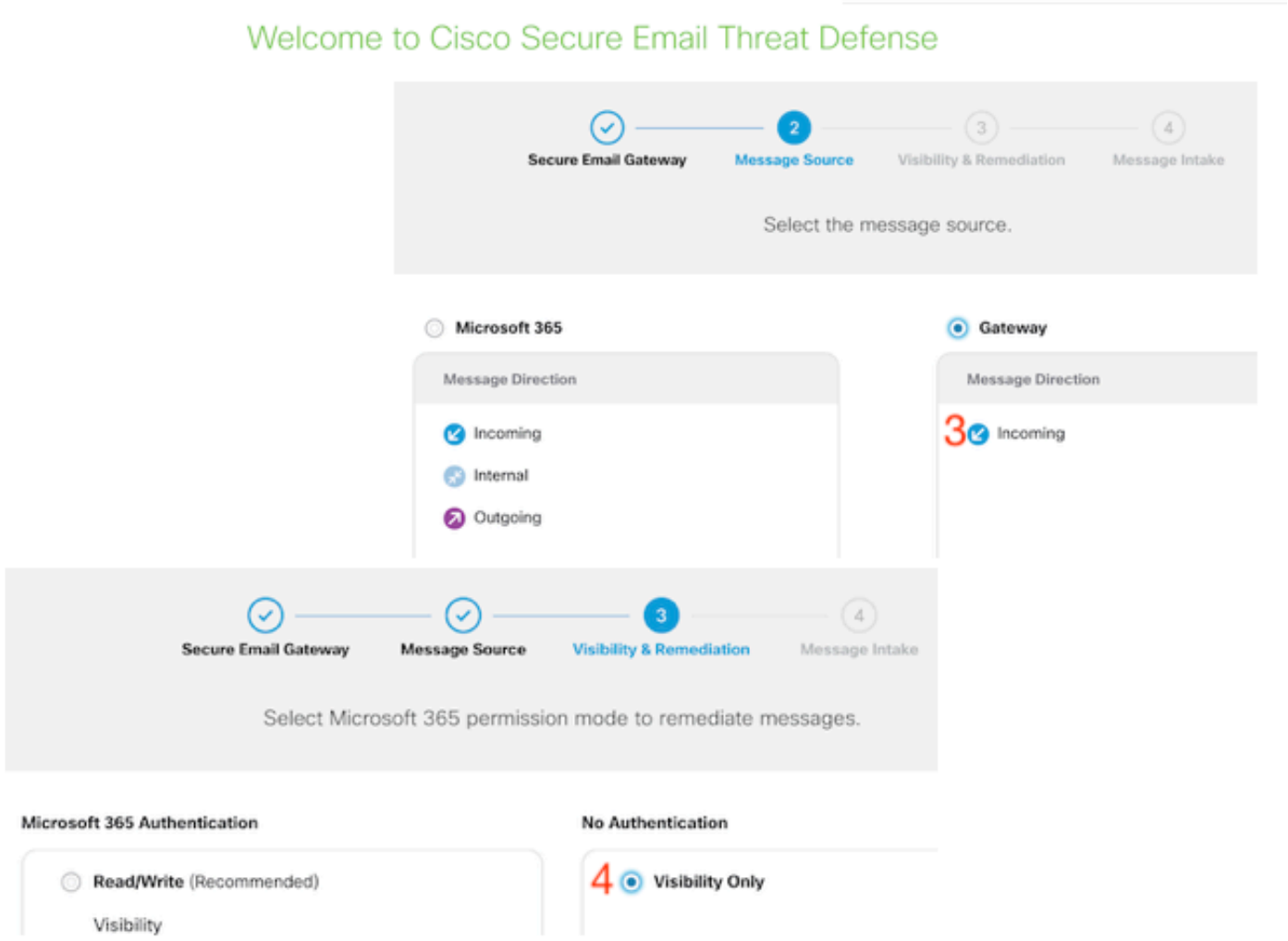
SETD eerste setup-stappen om het "Message Intake Address" te genereren

1. Ja, Secure Email Gateway is aanwezig.
2. Cisco SEG

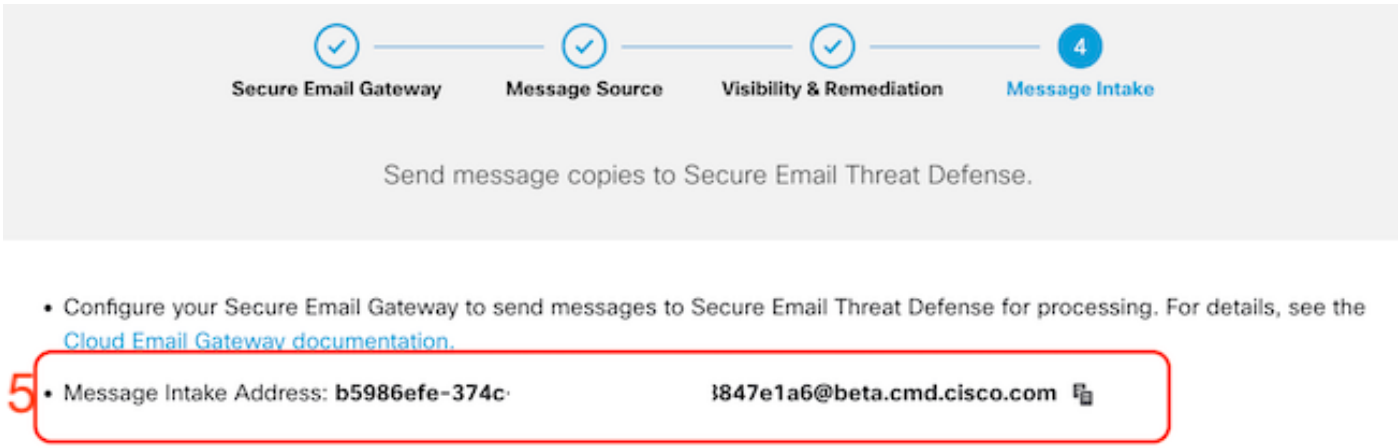


3. Richting bericht = inkomend.

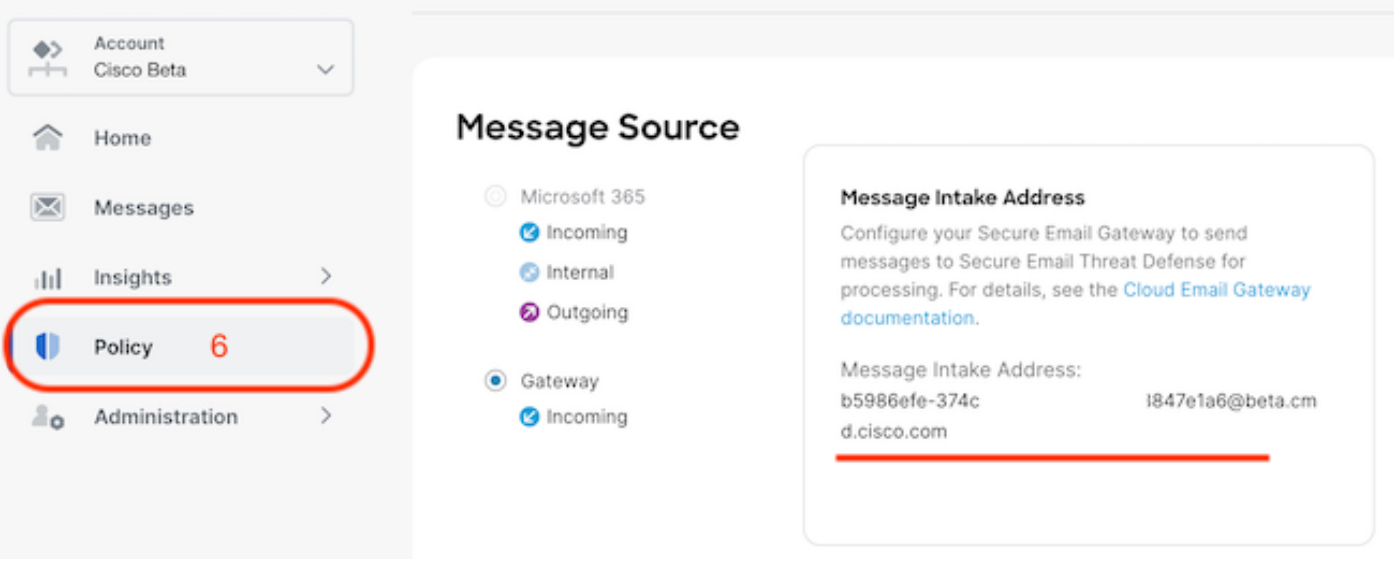
4. Geen verificatie = alleen zichtbaarheid.



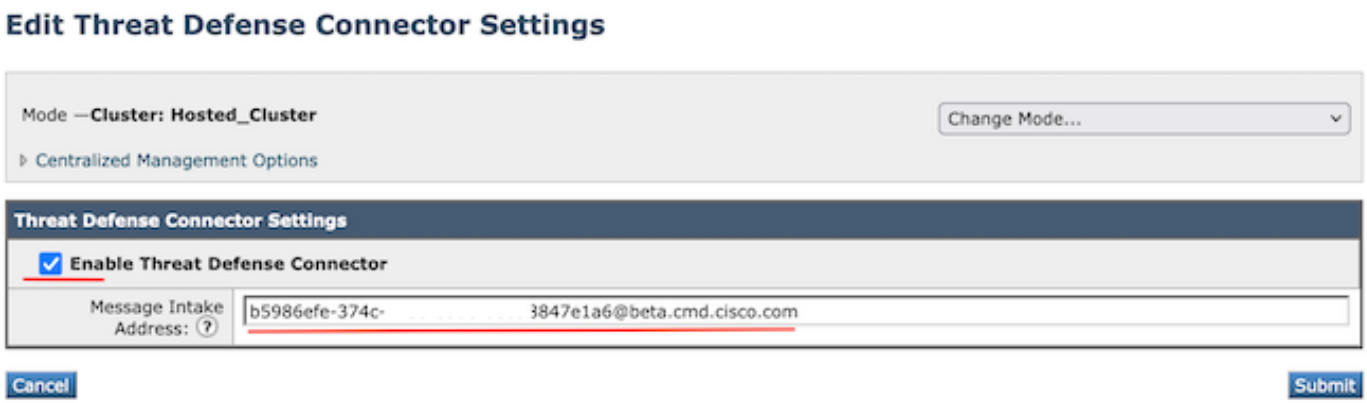
5. Het Berichtinnameadres wordt weergegeven nadat stap 4 is aanvaard.



6. Als u de postinstelling van het Berichtinnameadres moet ophalen, navigeer dan naar het menu Beleid.

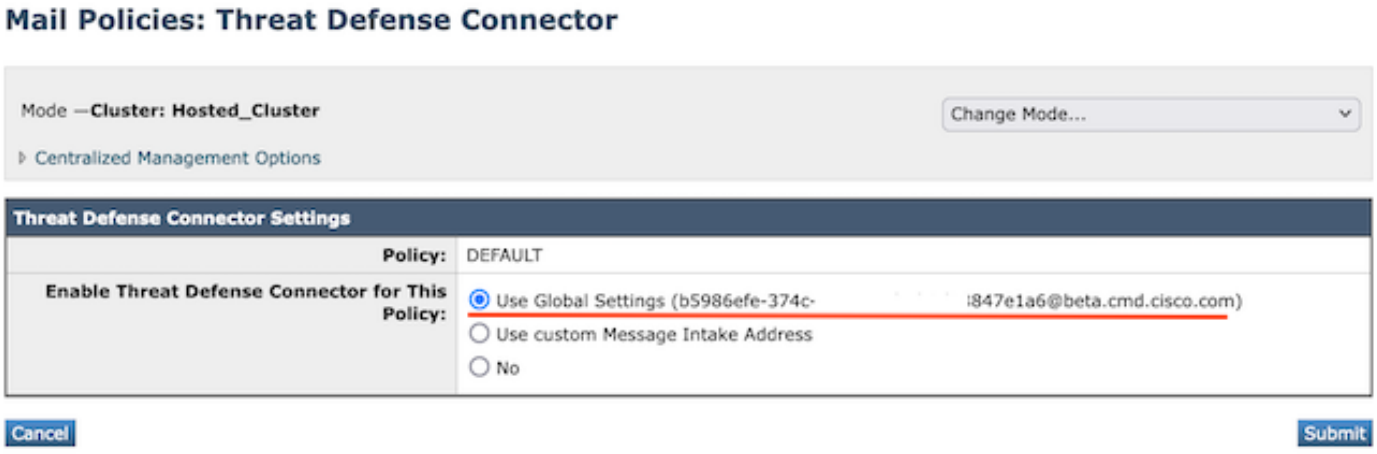


Overgang naar de SEG WebUI, navigeer naar security services > Threat Defense Connector-instellingen.



Naar mailbeleid navigeren:

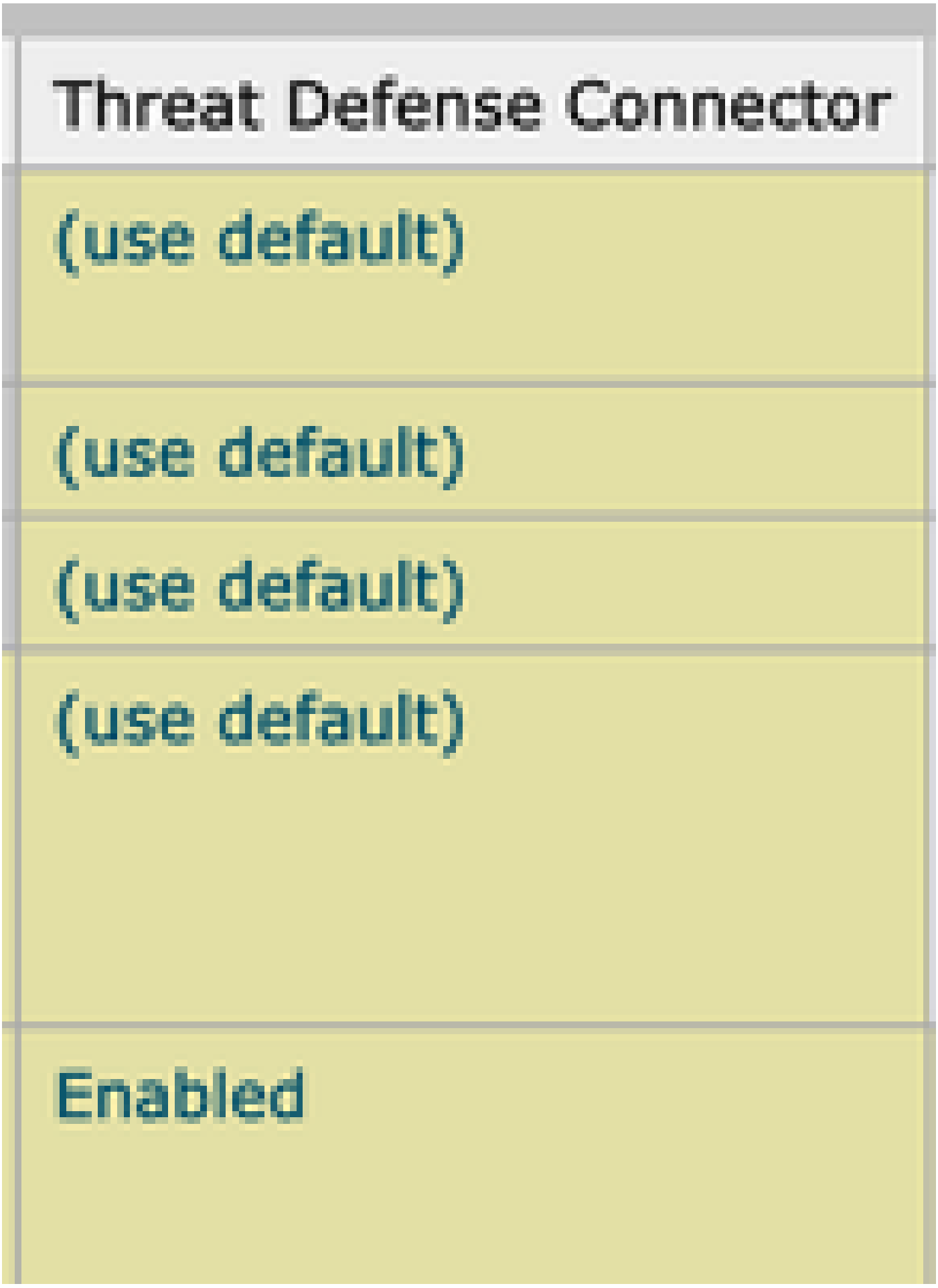
- Beleid voor inkomende e-mail
  - De laatste service rechts is "Threat Defense Connector".
- De instellingen linken displays, "Uitgeschakeld" voor de eerste configuratie.



Het Aangepaste Bericht Inname Adres zou bevolken met behulp van een secondaire SETD instantie.

Opmerking: Het is belangrijk om bij gebruik van het Aangepaste Inlaatadres de Mail Policy match criteria te configureren om het juiste domeinverkeer op te nemen.

De definitieve mening van de instelling toont de waarde "Enabled," voor de geconfigureerde service.


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

Verifiëren

Zodra alle stappen zijn voltooid, de e-mail bevolkt het SETD Dashboard.

De opdracht SEG CLI > tophosts geeft de tellers van de wachtrij.tdc.wachtrij weer voor actieve leveringen.

```
(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
```

Problemen oplossen

Gedrag van TDC-verbinding:

- Een minimum van 3 verbindingen worden geopend wanneer er ingangen aanwezig in de bestemmingsrij zijn
- Verdere verbindingen worden dynamisch gegenereerd met dezelfde logica voor reguliere e-mailwachtrijen.
- Open verbindingen worden gesloten zodra de wachtrij leeg wordt of wanneer er niet genoeg items aanwezig zijn in de doelwachtrij.
- Er worden nieuwe pogingen uitgevoerd volgens de waarde in de tabel.
- Berichten worden uit de wachtrij verwijderd nadat opnieuw geprobeerd is of als het bericht te lang in de wachtrij staat (120sec)

Mechanisme voor opnieuw proberen van Threat Defense Connector

Foutcase	Gereed opnieuw proberen	Aantal pogingen
SMTP 5xx-fouten (behalve 503/552)	Nee	N.v.t.
SMTP 4xx-fouten (inclusief 503/552)	Ja	1
TLS-fouten	Nee	N.v.t.
Algemene Network \ Connection-fouten, DNS-fouten, enzovoort.	Ja	1

TDC-maillogbestanden voorbeeldop basis van de leveringsresultaten

TDC-gerelateerde logitems bevatten de TDC: waarde voorafgaand aan de logtekst.

Het monster heeft een normale TDC-levering.

```
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
```

De steekproef presenteert een leveringsfout toe te schrijven aan het undeliverable bericht nadat de 120 tweede onderbreking verliep

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

De Steekproef levert een leveringsfout toe te schrijven aan een Fout van TLS.

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

Deze steekproef presenteert een ongeldig adres van het SETD Journal resulterend in een harde sprong.

```
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) :
```

Berichttracering geeft slechts één regel weer die aangeeft dat het bericht met succes naar SETD is verzonden.

Deze steekproef presenteert een leveringsfout toe te schrijven aan een Fout van TLS.

16 feb. 2024 21:19:24 (GMT -06:00)	TDC: Bericht 14501404 is geleverd voor scannen met Cisco Secure Email Threat Defence.

Gerelateerde informatie

- E-mail security installatiehandleiding
- Cisco Secure Email Gateway-startpagina voor ondersteuningshandleidingen
- ETD-gebruikershandleiding

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.