Configurar o Registro em Diário por Política do Secure Email Gateway para Proteger o Email Threat Defense

Contents

Introdução

Este documento descreve as etapas para configurar o Secure Email Gateway (SEG) para executar o Diário por Política para Secure Email Threat Defense (SETD).

Pré-requisitos

Conhecimento prévio das configurações gerais do Cisco Secure Email Gateway (SEG) é útil.

Componentes Utilizados

Esta configuração requer ambos;

- Cisco Secure Email Gateway (SEG) AsyncOS 15.5.1 e mais recente
- Instância do Cisco Email Threat Defense (SETD).
- Threat Defense Connector (TDC). "A conexão definida entre as duas tecnologias."

"As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que você compreende o impacto potencial de qualquer comando."

Overview

O Cisco SEG é capaz de integrar-se com o SETD para proteção adicional.

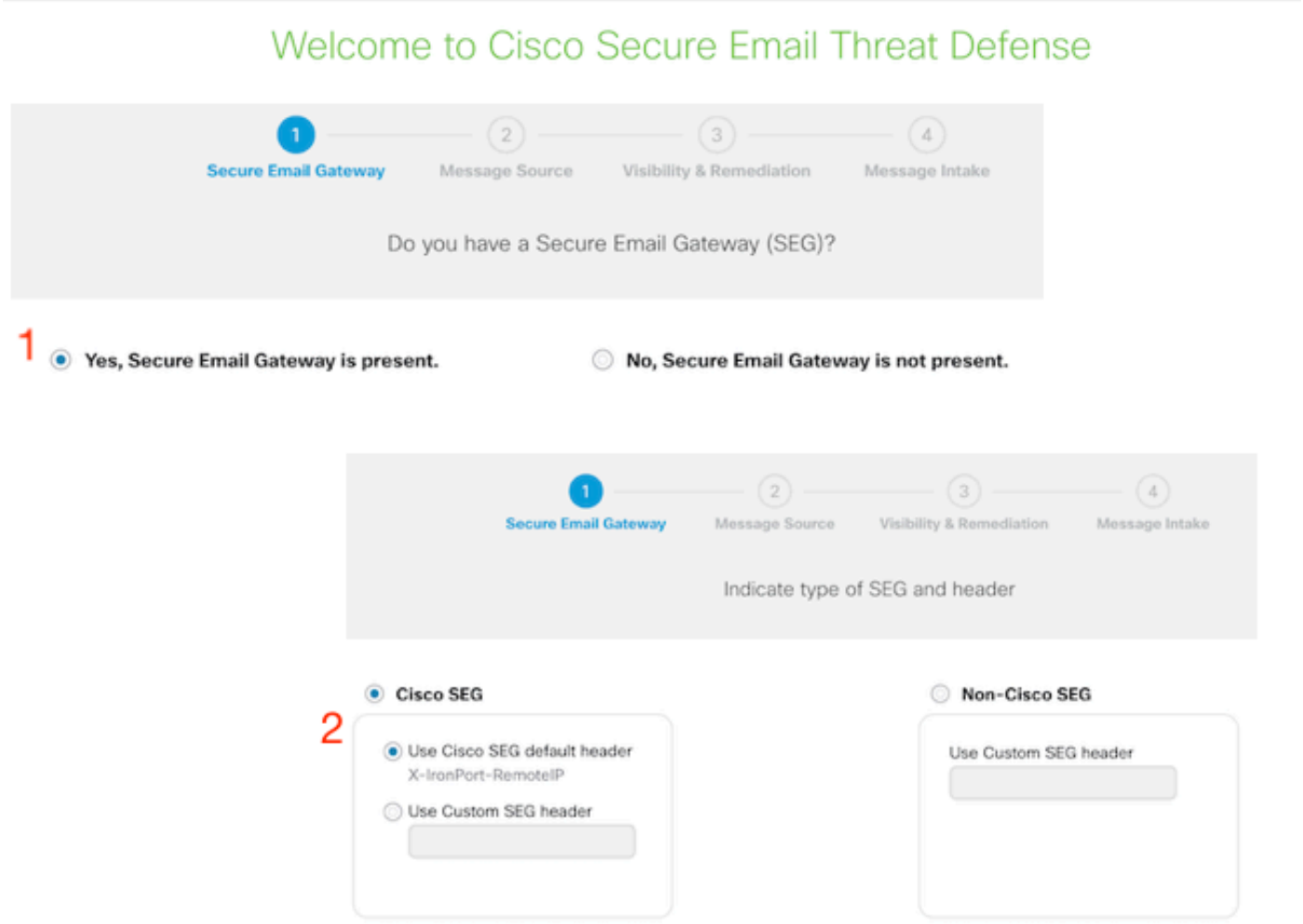
- A ação do diário SEG transfere o email completo para todas as mensagens limpas.

- O SEG oferece a opção de escolher seletivamente os fluxos de e-mail de entrada com base em uma correspondência por política de e-mail.
- A opção SEG por política permite 3 opções: Sem verificação, Endereço de entrada de mensagem padrão ou Endereço de entrada de mensagem personalizado.
    - O endereço de entrada padrão representa a conta SETD principal que aceita e-mails para uma instância de conta específica.
    - O endereço de entrada de mensagem personalizado representa uma segunda conta SETD que aceita e-mails para diferentes domínios definidos. Este cenário se aplica a ambientes SETD mais complexos.
- As mensagens registradas no diário têm um ID de mensagem SEG (MID) e um ID de conexão de destino DCID
- A Fila de entrega contém um valor semelhante a um domínio, "the.tdc.queue", para capturar contadores de transferência SETD.
    - Os contadores ativos do "the.tdc.queue" podem ser visualizados aqui: cli>tophosts ou SEG Reporting > Delivery Status (non-CES).
    - "the.tdc.queue" representa o Threat Defense Connector (TDC) equivalente a um nome de domínio de destino.

Configurar

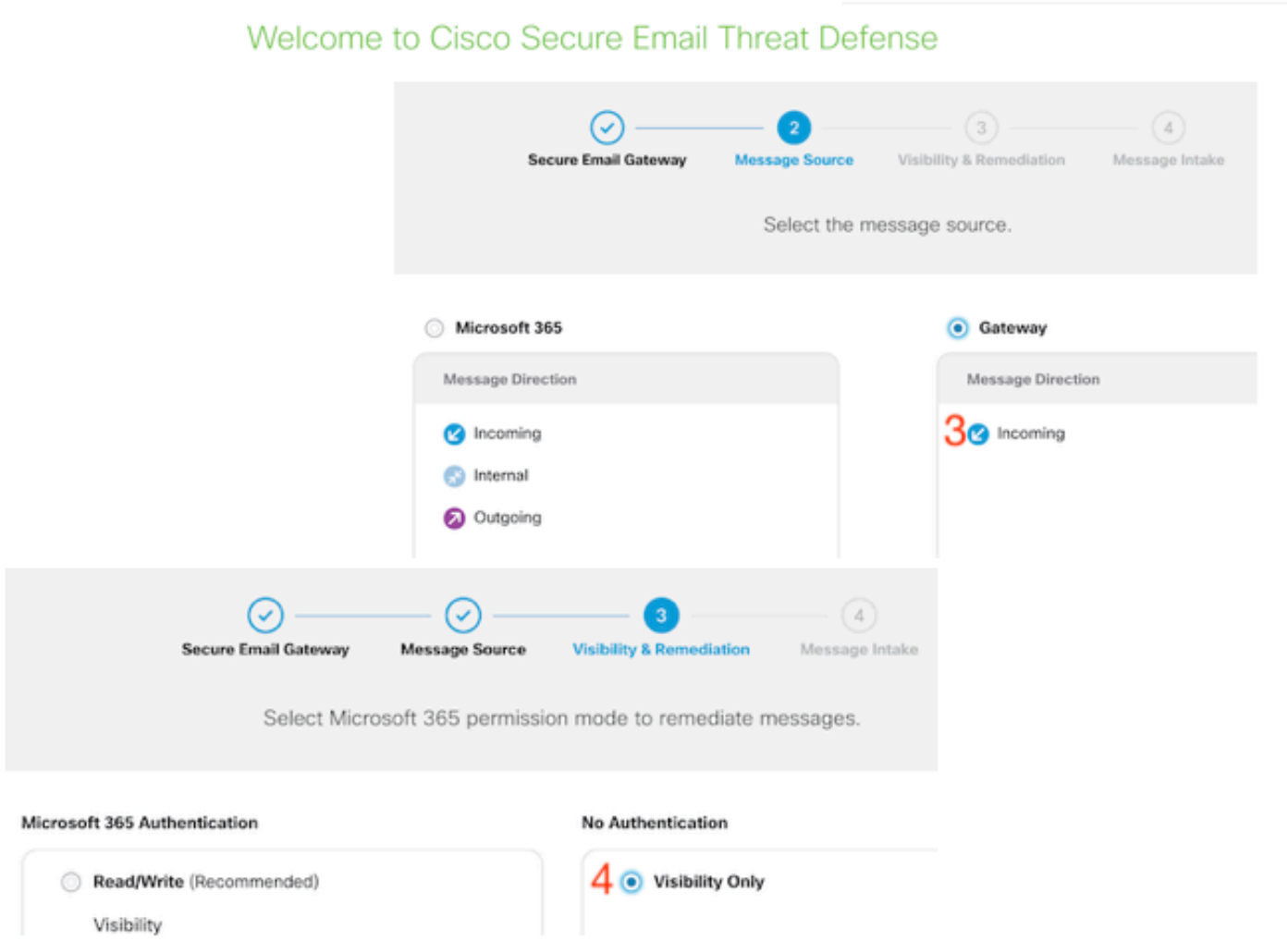
Etapas de configuração inicial do SETD para gerar o "Endereço de entrada de mensagem".

1. Sim, o Secure Email Gateway está presente.
2. SEG da Cisco

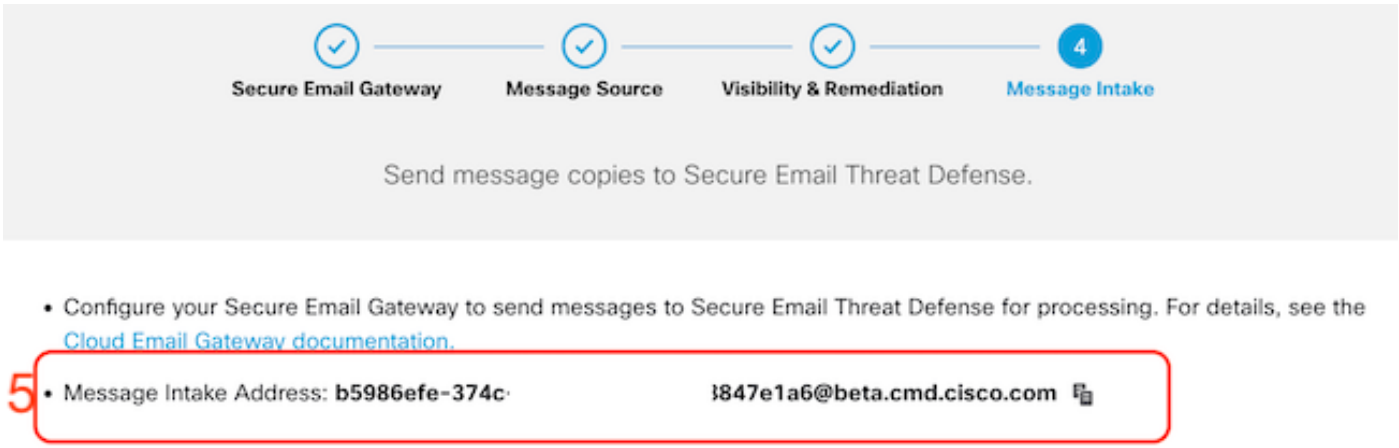


3. Direção da Mensagem = Entrada.

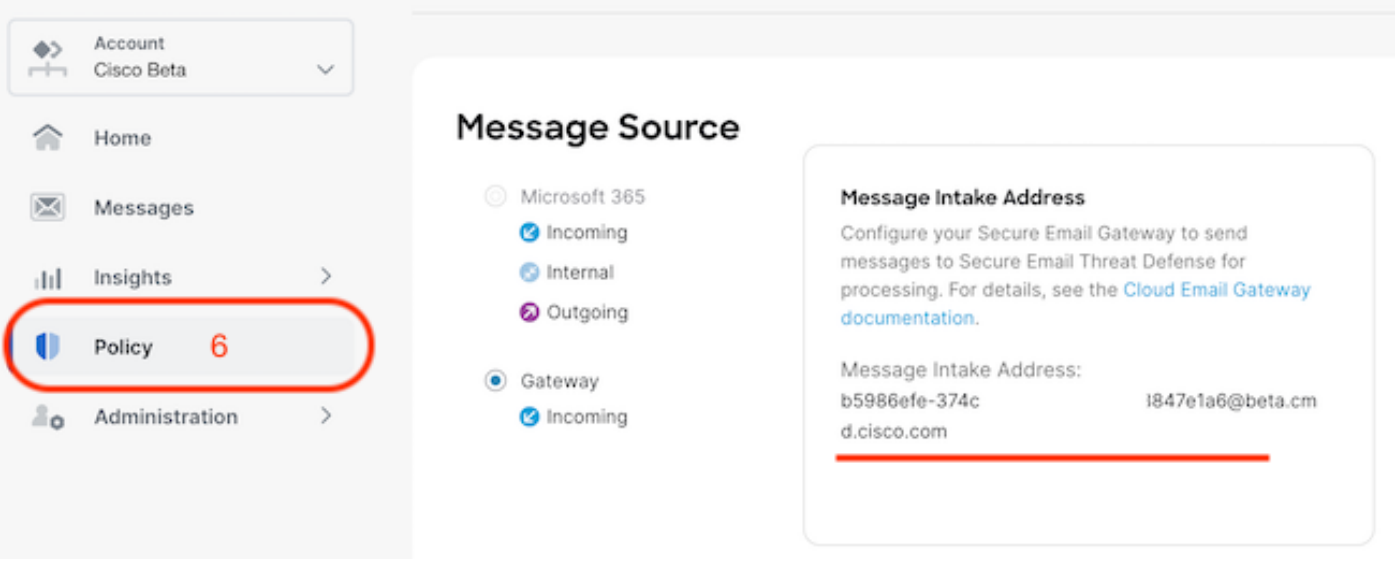
4. Sem Autenticação = Somente Visibilidade.



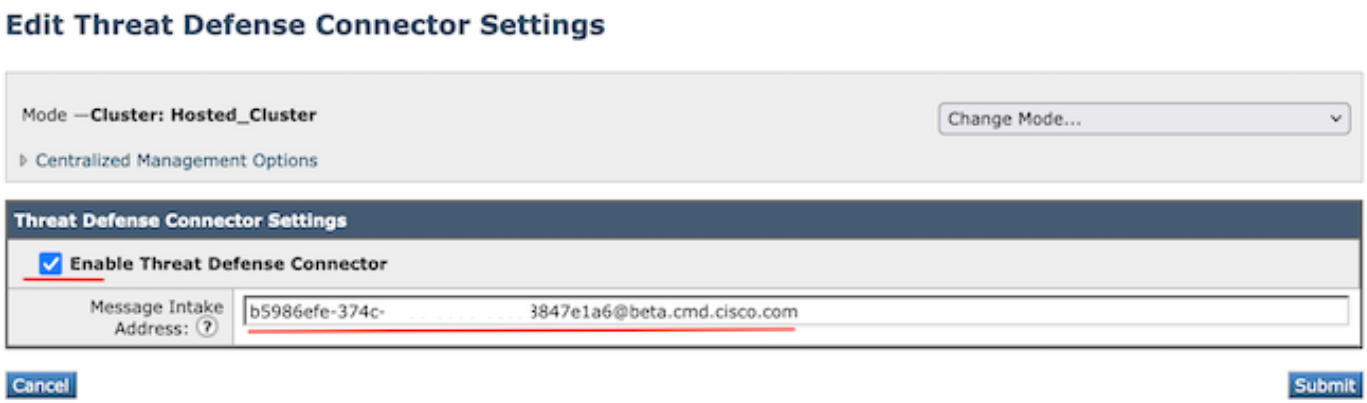
5. O Endereço de Entrada de Mensagem é apresentado após a etapa 4 ter sido aceita.



6. Se precisar recuperar a configuração de postagem do Endereço de Entrada de Mensagem, navegue até o menu Política.

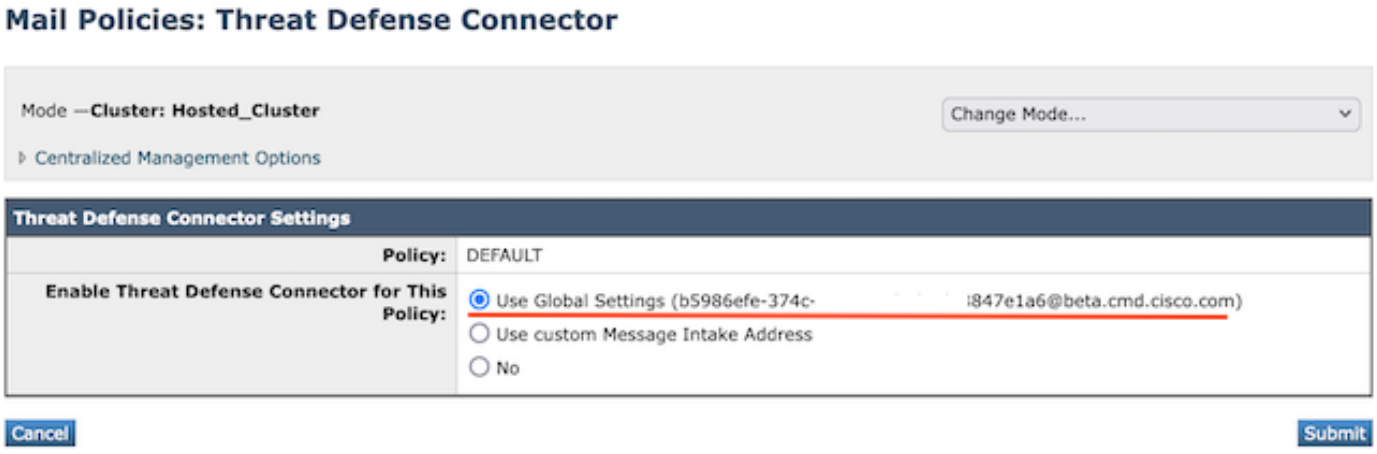


Fazendo a transição para o SEG WebUI, navegue para Serviços de segurança > Configurações do conector Threat Defense.



Navegue até Políticas de e-mail:

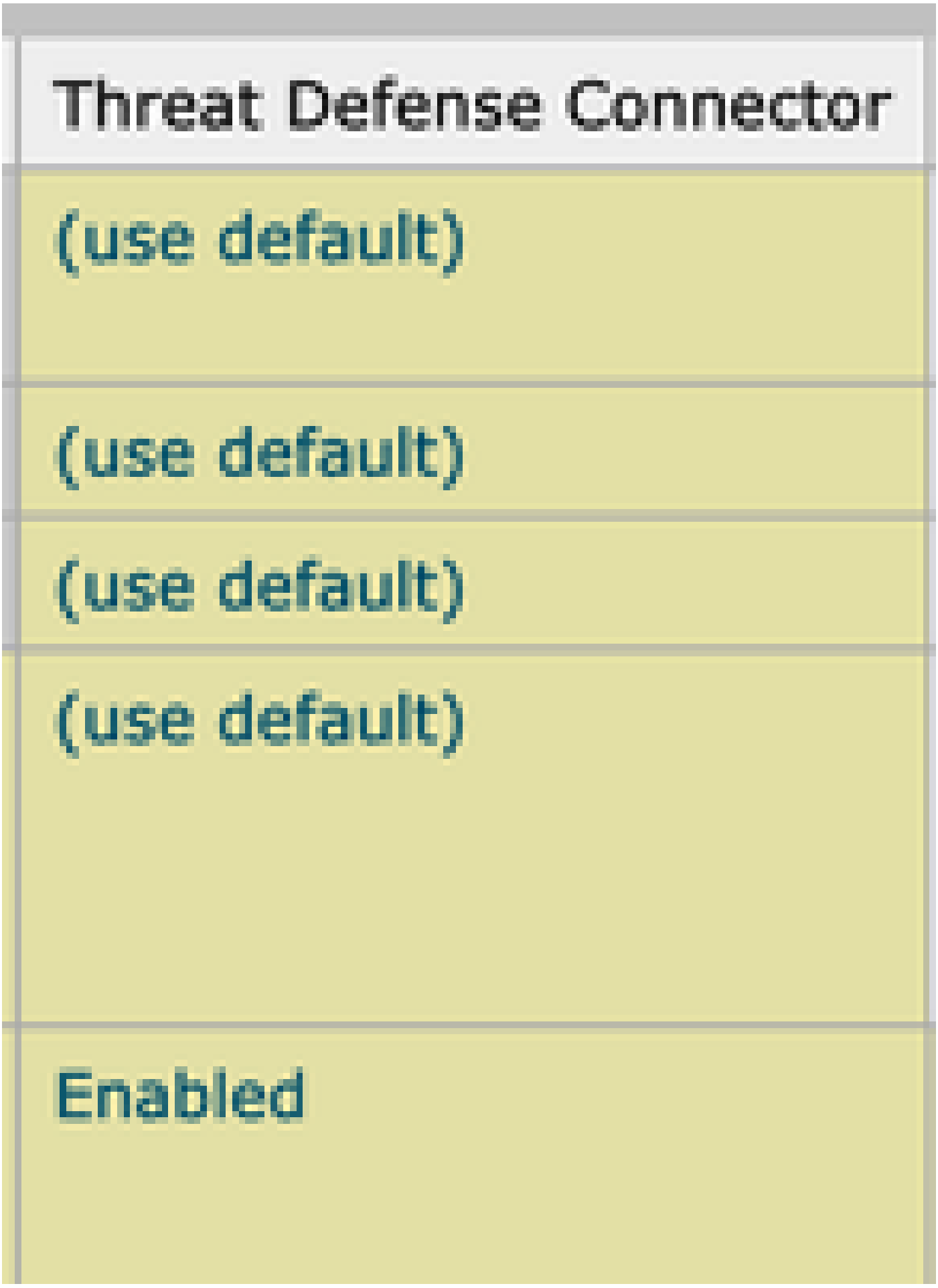
- Políticas de recebimento de e-mail
  - O último serviço à direita é o "Threat Defense Connector".
- O link de configurações exibe "Desabilitado" para a primeira configuração.



O endereço de entrada de mensagem personalizado seria preenchido usando uma instância SETD secundária.

Observação: é importante ao utilizar o endereço de entrada personalizado para configurar os critérios de correspondência da política de e-mail para capturar o tráfego de domínio correto.

A visualização final da configuração apresenta o valor "Habilitado" para o serviço configurado.


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

Verificar

Depois que todas as etapas tiverem sido concluídas, o e-mail preencherá o painel SETD.

O comando SEG CLI > tophosts exibe os contadores .tdc.queue para entregas ativas.

```
(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
```

Troubleshooting

Comportamento da conexão TDC:

- Um mínimo de 3 conexões são abertas quando há entradas presentes na fila de destino
- Outras conexões são geradas dinamicamente usando a mesma lógica para filas de destino de e-mail comuns.
- As conexões abertas são fechadas quando a fila fica vazia ou não há entradas suficientes na fila de destino.
- As novas tentativas são executadas de acordo com o valor na tabela.
- As mensagens são removidas da fila depois que as tentativas são esgotadas ou se a mensagem estiver na fila por muito tempo (120 seg)

Mecanismo de nova tentativa do conector de defesa contra ameaças

Caso de erro	Repetição Concluída	Número de Tentativas
Erros SMTP 5xx (exceto 503/552)	No	N/A
Erros de SMTP 4xx (incluindo 503/552)	Yes	1
Erros de TLS	No	N/A
Rede geral \ Erros de conexão, erros de DNS e assim por diante.	Yes	1

Exemplos de registros de e-mail do TDC com base nos resultados de entrega

As entradas de log relacionadas ao TDC contêm o valor TDC: que precede o texto de log.

A amostra apresenta uma entrega normal de TDC.

```
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
```

A amostra apresenta um erro de entrega devido à mensagem que não pode ser entregue após o tempo limite de 120 segundos expirar

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

O exemplo apresenta um erro de entrega devido a um erro TLS.

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

Este exemplo apresenta um Endereço de Diário SETD inválido, resultando em uma devolução forçada.

```
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) :
```

O Rastreamento de mensagem simplesmente exibe uma única linha indicando a entrega bem-sucedida da mensagem ao SETD.

Este exemplo apresenta um erro de entrega devido a um erro TLS.

16 de fevereiro de 2024 21:19:24 (GMT -06:00)	TDC: A mensagem 14501404 foi entregue com êxito para varredura com o Cisco Secure Email Threat Defense.

Informações Relacionadas

- Guia de configuração do Email Security
- Página inicial do Cisco Secure Email Gateway para guias de suporte

- Guia do usuário do ETD

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.