

Configuración del registro por política de gateway de correo electrónico seguro para proteger la defensa frente a amenazas del correo electrónico

Contenido

[Introducción](#)

[Prerequisites](#)

[Componentes Utilizados](#)

[Overview](#)

[Configurar](#)

[Verificación](#)

[Troubleshoot](#)

[Comportamiento de la conexión TDC:](#)

Introducción

Este documento describe los pasos para configurar Secure Email Gateway (SEG) para realizar el registro por política para Secure Email Threat Defence (SETD).

Prerequisites

El conocimiento previo de la configuración y los parámetros generales de Cisco Secure Email Gateway (SEG) resulta beneficioso.

Componentes Utilizados

Esta configuración requiere ambos:

- Cisco Secure Email Gateway (SEG) AsyncOS 15.5.1 y versiones posteriores
- Instancia de Cisco Email Threat Defence (SETD).
- Conector de defensa frente a amenazas (TDC). "La conexión definida entre las dos tecnologías".

"La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si su red está activa, asegúrese de comprender el impacto potencial de cualquier comando".

Overview

El SEG de Cisco puede integrarse con SETD para obtener una protección adicional.

- La acción de diario SEG transfiere el correo electrónico completo para todos los mensajes limpios.
- El SEG ofrece la opción de elegir de forma selectiva los flujos de correo entrante en función de una coincidencia por política de correo.
- La opción SEG Per Policy (SEG por directiva) permite 3 opciones: No Scan (Sin análisis), Default Message Intake Address (Dirección de entrada de mensajes predeterminada) o Custom Message Intake Address (Dirección de entrada de mensajes personalizada).
 - La dirección de entrada predeterminada representa la cuenta SETD principal que acepta correo para una instancia de cuenta específica.
 - La dirección de entrada de mensaje personalizada representa una segunda cuenta SETD que acepta correo para diferentes dominios definidos. Este escenario se aplica a entornos SETD más complejos.
- Los mensajes registrados tienen un [ID de mensaje SEG \(MID\) e ID de conexión de destino DCID](#)
- La cola de entrega contiene un valor similar a un dominio, "the.tdc.queue", para capturar contadores de transferencia SETD.
 - Los contadores activos "the.tdc.queue" se pueden ver aquí: cli>tophosts o Informes SEG > Estado de entrega (no CES).
 - "the.tdc.queue" representa el conector de defensa frente a amenazas (TDC) equivalente a un nombre de dominio de destino.

Configurar

Los pasos de configuración inicial de SETD para generar la "Dirección de entrada de mensaje".

1. Sí, Secure Email Gateway está presente.
2. Cisco SEG

Welcome to Cisco Secure Email Threat Defense

1 Secure Email Gateway 2 Message Source 3 Visibility & Remediation 4 Message Intake

Do you have a Secure Email Gateway (SEG)?

- 1 Yes, Secure Email Gateway is present. No, Secure Email Gateway is not present.

1 Secure Email Gateway 2 Message Source 3 Visibility & Remediation 4 Message Intake

Indicate type of SEG and header

2 **Cisco SEG** **Non-Cisco SEG**

Use Cisco SEG default header
X-IronPort-RemoteIP

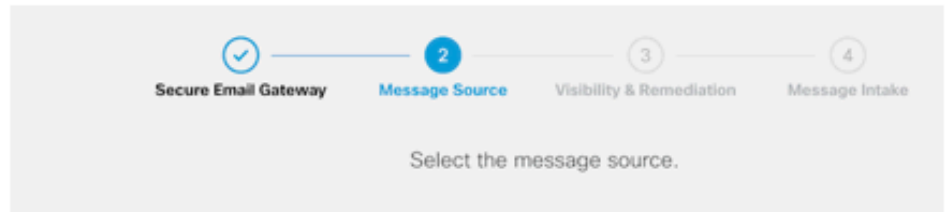
Use Custom SEG header

Use Custom SEG header

3. Dirección del mensaje = Entrante.

4. Sin autenticación = solo visibilidad.

Welcome to Cisco Secure Email Threat Defense



Microsoft 365

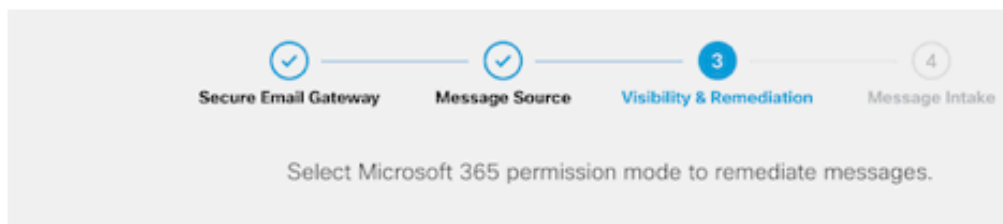
Message Direction

- Incoming
- Internal
- Outgoing

Gateway

Message Direction

3 Incoming



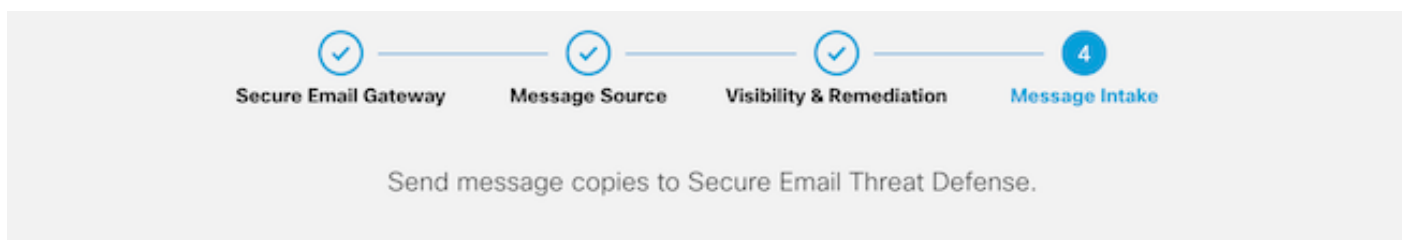
Microsoft 365 Authentication

Read/Write (Recommended)
Visibility

No Authentication

4 Visibility Only

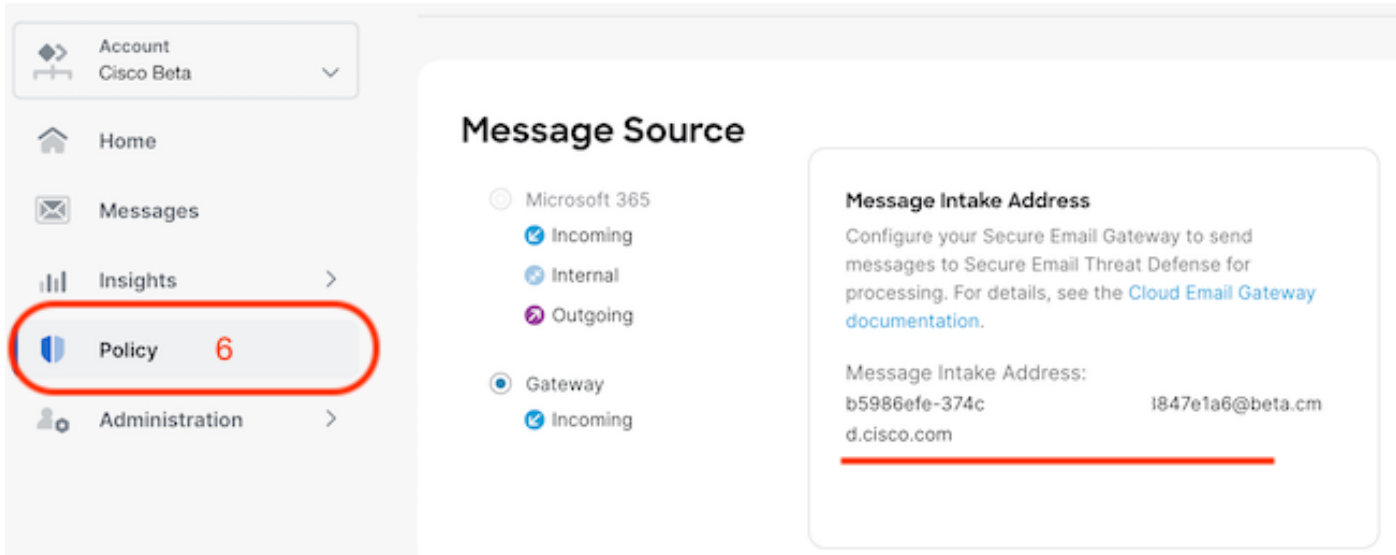
5. La dirección de entrada del mensaje se presenta después de que se haya aceptado el paso 4.



- Configure your Secure Email Gateway to send messages to Secure Email Threat Defense for processing. For details, see the [Cloud Email Gateway documentation](#).

5 • Message Intake Address: **b5986efe-374c-1847e1a6@beta.cmd.cisco.com** 📧

6. Si necesita recuperar la dirección de entrada de mensaje después de la configuración, acceda al menú Política.



En la transición a la interfaz de usuario web de SEG, vaya a Servicios de seguridad > Configuración del conector de Threat Defence.

Edit Threat Defense Connector Settings

Mode — Cluster: Hosted_Cluster Change Mode...

Centralized Management Options

Threat Defense Connector Settings

Enable Threat Defense Connector

Message Intake Address:

Cancel Submit

Desplácese hasta Políticas de correo:

- Políticas de correo entrante
 - El último servicio de la derecha es el conector de defensa frente a amenazas.
- El enlace de configuración muestra "Desactivado" por primera vez en la configuración.

Mail Policies: Threat Defense Connector

Mode — Cluster: Hosted_Cluster Change Mode...

Centralized Management Options

Threat Defense Connector Settings

Policy: DEFAULT

Enable Threat Defense Connector for This Policy:

Use Global Settings (b5986efe-374c-1847e1a6@beta.cmd.cisco.com)


Use custom Message Intake Address

No

Cancel Submit

La dirección de entrada de mensaje personalizado se rellenaría con una instancia SETD secundaria.

Threat Defense Connector Settings	
	Policy: DEFAULT
Enable Threat Defense Connector for This Policy:	<input type="radio"/> Use Global Settings (b5986efe-374c-47a5-aade-b8d98847e1a6@beta.cmd.cisco.com)
	<input checked="" type="radio"/> Use custom Message Intake Address
	Message Intake Address: (?)
	<input type="text" value="15e1c36b-098c-4e87-590@beta.cmd.cisco.com"/>
	<input type="radio"/> No

 Nota: es importante cuando se utiliza la dirección de entrada personalizada para configurar los criterios de coincidencia de la política de correo para capturar el tráfico de dominio correcto.

La vista final de la configuración presenta el valor "Enabled" (Activado) para el servicio configurado.

Threat Defense Connector

(use default)

(use default)

(use default)

(use default)

Enabled

Verificación

Una vez completados todos los pasos, el mensaje de correo electrónico se rellena en el panel SETD.

El comando CLI de SEG > tophosts muestra los contadores .tdc.queue para las entregas activas.

```
(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.

#   Recipient Host           Active  Conn.  Deliv.  Soft   Hard
#   Recipient Host           Recip.  Out    Recip.  Bounced Bounced
5   the.tdc.queue           1       0      104,163  0       0
```

Troubleshoot

Comportamiento de la conexión TDC:

- Se abren un mínimo de 3 conexiones cuando hay entradas presentes en la cola de destino
- Otras conexiones se generan dinámicamente utilizando la misma lógica para las colas de destino de correo electrónico normales.
- Las conexiones abiertas se cierran cuando la cola se vacía o cuando no hay suficientes entradas presentes en la cola de destino.
- Los reintentos se realizan según el valor de la tabla.
- Los mensajes se quitan de la cola después de que se agoten los reintentos o si el mensaje permanece en la cola durante demasiado tiempo (120 s)

Mecanismo de reintento del conector de Threat Defence

Caso de error	Reintento realizado	Número de reintentos
Errores SMTP 5xx (excepto 503/552)	No	N/A
Errores SMTP 4xx (incluidos 503/552)	Yes	1
Errores de TLS	No	N/A
Red general \ Errores de conexión, errores de DNS, etc.	Yes	1

Registros de correo TDC de muestra basados en los resultados de la entrega

Las entradas de registro relacionadas con TDC contienen el valor TDC: que precede al texto del

registro.

La muestra presenta una entrega normal de TDC.

```
Fri Feb 16 21:19:22 2024 Info: TDC: MID 14501404 with Message-ID '<07afv777xxreILg20Q@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
```

El ejemplo presenta un error de entrega debido al mensaje de no entrega después de que caducara el tiempo de espera de 120 segundos

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

El ejemplo presenta un error de entrega debido a un error de TLS.

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

Este ejemplo presenta una dirección de diario SETD no válida que resulta en un rebote duro.

```
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) :
```

Rastreo de mensajes simplemente muestra una única línea que indica la entrega correcta del mensaje a SETD.

Este ejemplo presenta un error de entrega debido a un error de TLS.

16 de febrero de 2024 21:19:24 (GMT -06:00)	TDC: el mensaje 14501404 se entregó correctamente para su análisis con Cisco Secure Email Threat Defence.
--	---

Información Relacionada

- [Guía de configuración de Email Security](#)
- [Página de inicio de Cisco Secure Email Gateway para las guías de asistencia](#)
- [Guía del usuario de ETD](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).