

# Configurar el escaneo de amenazas según la política para SEG

## Contenido

---

[Introducción](#)

[Prerequisites](#)

[Componentes Utilizados](#)

[Overview](#)

[Configurar](#)

[Configuración de interfaz web](#)

[Configuración de interfaz de línea de comandos](#)

[Verificación](#)

[Información Relacionada](#)

---

## Introducción

Este documento describe el servicio y la configuración de la integración de Threat Scanner (TS) por política para Cisco Secure Email Gateway (SEG).

## Prerequisites

Se requiere conocer las configuraciones generales de SEG.

## Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software:

- Cisco Secure Email Gateway (SEG) AsyncOS 15.5.1 y versiones posteriores.
- Servicio de graymail.
- Servicio antispam.
- Políticas de correo entrante.

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 tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

## Overview

Threat Scanner (TS), un subcomponente recién activado del servicio de graymail, se ha integrado con Antispam CASE para proporcionar una detección antispam más eficaz.

Una vez que se ha activado el servicio de graymail, las opciones para activar Threat Scanner se activan en cada configuración AntiSpam de política de correo entrante. Una vez habilitada, TS mejora la detección antispam general, haciendo hincapié en la detección de contrabando de HTML:

- Análisis de HTML y detección de scripts maliciosos
- Análisis de URL y detección de redirección

El motor antispam CASE controla los dos servicios, gestionando las actualizaciones y las condenas de spam.

TS tiene una configuración visible de activación/desactivación dentro de cada configuración de antispam de política de correo entrante.

TS influye en los veredictos, lo que aumenta el peso del veredicto final de CASE antispam.

## Configurar


La configuración consta de dos acciones: Habilitar la detección de graymail y Habilitar TS dentro de las políticas de correo entrante.


- El servicio global de graymail debe estar habilitado para activar TS.
- La opción "Antispam" de la política de correo entrante para "Habilitar Threat Scanner" estará disponible una vez que Graymail se haya habilitado globalmente.

## Configuración de interfaz web

Para habilitar Graymail en la interfaz de usuario web:

- Vaya a Servicios de seguridad
  - IMS y Graymail
    - Configuración global de graymail
      - Editar configuración de graymail.
        - Seleccione la opción para activar la detección de graymail.
- Envíe y confirme los cambios para finalizar la acción.

Graymail Global Settings	
Graymail Detection	Disabled 
Safe Unsubscribe	Disabled
<a href="#">Edit Graymail Settings</a>	


Anti-Spam Settings	
Policy:	Default
Enable Anti-Spam Scanning for This Policy:	<input checked="" type="radio"/> Use IronPort Anti-Spam service <input checked="" type="checkbox"/> Enable Threat Scanner  <i>You must enable Graymail Global Settings to enable Threat Scanner.</i> <input type="radio"/> Use IronPort Intelligent Multi-Scan <i>Spam scanning built on IronPort Anti-Spam.</i> <input type="radio"/> Disabled


La vista anterior a la configuración

Una vez que se ha habilitado Graymail, el cuadro de selección de Threat Scanner estará disponible para cada política de correo entrante.

Para habilitar Threat Scanner en la interfaz de usuario web:

- Desplácese hasta Políticas de correo
  - Políticas de correo entrante
    - Seleccione la política de correo que desee
      - Seleccione Anti-Spam.
        - En la parte superior de la página de configuración se muestra la casilla de verificación Activar Threat Scanner.
- Enviar y confirmar los cambios para finalizar la configuración

Graymail Global Settings	
Graymail Detection	Enabled 
Safe Unsubscribe	Disabled
Automatic Updates (?)	Enabled
<a href="#">Edit Graymail Settings</a>	

Anti-Spam Settings	
Policy:	Default
Enable Anti-Spam Scanning for This Policy:	<input checked="" type="radio"/> Use IronPort Anti-Spam service <input checked="" type="checkbox"/> Enable Threat Scanner  <input type="radio"/> Use IronPort Intelligent Multi-Scan <i>Spam scanning built on IronPort Anti-Spam.</i> <input type="radio"/> Disabled

Opción de Threat Scanner en Antispam

## Configuración de interfaz de línea de comandos

Habilite el servicio de graymail mediante los comandos CLI.

- `imsandgraymailconfig`
  - `graymail`
    - configuración
      - ¿Desea utilizar la detección de graymail? [Y] >
        - ¿Desea habilitar las actualizaciones automáticas para el motor de graymail? [Y]>
  - Complete los mensajes restantes para volver al mensaje principal del equipo.
- Confirmar + añadir los comentarios deseados > Completar la acción pulsando la tecla "Volver".

Activación o desactivación de Threat Scanner en una política desde la CLI.

- `CLI> policyconfig`

¿Desea configurar la política de correo entrante o las políticas de correo saliente o la prioridad de coincidencia de encabezados?

1. Políticas de correo entrante
2. Políticas de correo saliente
3. Coincidir prioridad de encabezados

[1]> 1

configuración de política de correo entrante

1. Norte1
2. LISTA\_DE\_BLOQUEOS
3. LISTA\_PERMITIDA
4. ALLOW\_SPOOF
5. PREDETERMINADO

Introduzca el nombre o el número de la entrada que desea editar:

[]> 1

Elija la operación que desea realizar:

- NOMBRE - Cambiar el nombre de la política
- NUEVO - Agregar una nueva fila de miembro de política
- DELETE - Elimina una fila de miembro de política
- PRINT - Imprimir filas de miembros de políticas
- ANTISPAM - Modificar la política Anti-Spam
- ANTIVIRUS - Modificar la política antivirus
- OUTBREAK - Modificar la política de filtros de brote
- ADVANCEDMALWARE - Modificar la política de protección frente a malware avanzado

- GRAYMAIL - Modificar política de graymail
  - THREATDEFENSECONNECTOR - Modificar conector de Threat Defence
  - FILTROS - Modificar filtros
- []> antispam

Elija la operación que desea realizar:

- DISABLE (Desactivar): desactiva la política antispam (desactiva todas las acciones relacionadas con la política)
  - ENABLE (HABILITAR): habilita la política antispam
- []> enable

Comenzar configuración Anti-Spam

¿Desea utilizar Intelligent Multi-Scan en esta política? [N]>

¿Desea utilizar IronPort Anti-Spam en esta política? [Y]>

Algunos mensajes se identifican positivamente como spam. Algunos mensajes son identificado como spam sospechoso. Puede configurar el IronPort Anti-Spam Sospechoso Spam Umbral inferior.

Las opciones de configuración se aplican a los mensajes identificados POSITIVAMENTE como spam:

¿Desea habilitar un tratamiento especial para el veredicto de Threat Scanner? [N]> y

Continúe con las selecciones del menú para completar las opciones de la política de correo y presione la "tecla de retorno" para aceptar la acción predeterminada para cada opción.

Complete la operación de guardar con los comandos.

- Confirmar + añadir los comentarios deseados > Completar la acción pulsando la tecla "Volver".

## Verificación

Cómo leer e interpretar los registros.

El registro de correo de Threat Scanner solo presenta un veredicto provisional, mientras que CASE presenta el veredicto final.

Los registros de correo muestran dos verbos diferentes para los veredictos de Threat Scanner limpios frente a los condenados

- Si el veredicto provisional de Threat Scanner está limpio, el registro se presenta de forma similar a estas muestras.
  - Información: veredicto provisional de graymail - LEGIT (0) <Clean message>
  - Información: veredicto provisional sobre graymail - MCE (11) <Campaña de correo electrónico diversa>

- Si el veredicto provisional de Threat Scanner se va a condenar, el registro se presenta de forma similar a estas muestras.
  - Información: veredicto provisional de ThreatScanner - PHISHING (101)
  - Información: veredicto provisional de ThreatScanner - VIRUS (2)

Ejemplo de registros de correo: el veredicto de Threat Scanner Clean utiliza otro lenguaje: el veredicto de graymail.

<#root>

Wed Jan 31 08:19:32 2024 Info: MID 3189755

interim graymail verdict - LEGIT (0) <Clean message>


Wed Jan 31 08:19:33 2024 Info: MID 3189755 interim verdict using engine: CASE negative

Wed Jan 31 08:19:33 2024 Info: MID 3189755 using engine: CASE spam negative

El rastreo de mensajes no muestra la entrada de registro de Threat Scanner, solo el caso: veredicto final.

Estos ejemplos de Threat Scanner (TS) presentan los cuatro escenarios de veredicto.

---

 Nota: Las categorías de TS de "PHISHING" y "VIRUS" son la única detección que aumenta el peso del veredicto del CASO

---

Ejemplo de registros de correo: PHISHING TS Conviction y AntiSpam Conviction están presentes

<#root>

Thu Jan 25 09:05:23 2024 Info: MID 3057397

interim

ThreatScanner verdict - PHISHING (101)

<Message detected as phishing either by heuristic analysis or by detecting the link as fraudulent>

Thu Jan 25 09:05:23 2024 Info: MID 3057397 interim verdict using engine: CASE spam positive

Thu Jan 25 09:05:23 2024 Info: MID 3057397

using engine: CASE spam positive

Thu Jan 25 09:05:23 2024 Info: Message aborted MID 3057397 Dropped by CASE

Muestra de seguimiento: la condena de SUPLANTACIÓN DE IDENTIDAD ESTÁ ausente y la condena de CASE está presente.

```
25 Jan 2024 07:05:23 (GMT -08:00) Message 3057397 matched per-recipient policy DEFAULT for inbound mail policies.
25 Jan 2024 07:05:23 (GMT -08:00) Message 3057397 scanned by Anti-Spam engine: CASE. Interim verdict: Positive
25 Jan 2024 07:05:23 (GMT -08:00) Message 3057397 scanned by Anti-Spam engine: CASE. Final verdict: Positive
```

PHISHING TS Rastreo de condenados y de condenados por antisпам

Ejemplo de registros de correo: PHISHING TS Conviction y AntiSpam Negative están presentes.

<#root>

Thu Jan 25 09:05:47 2024 Info: MID 3057413

interim ThreatScanner verdict - PHISHING (101)

<Message detected as phishing either by heuristic analysis or by detecting the link as fraudulent>

Thu Jan 25 09:05:47 2024 Info: MID 3057413 interim verdict using engine: CASE spam negative

Thu Jan 25 09:05:47 2024 Info: MID 3057413

using engine: CASE spam negative

Seguimiento de la muestra: PHISHING TS Convicted y AntiSpam Negative están presentes.

```
25 Jan 2024 07:05:47 (GMT -08:00) Message 3057413 matched per-recipient policy DEFAULT for inbound mail policies.
25 Jan 2024 07:05:47 (GMT -08:00) Message 3057413 scanned by Anti-Spam engine: CASE. Interim verdict: Negative
25 Jan 2024 07:05:47 (GMT -08:00) Message 3057413 scanned by Anti-Spam engine CASE. Interim verdict: definitely negative.
25 Jan 2024 07:05:47 (GMT -08:00) Message 3057413 scanned by Anti-Spam engine: CASE. Final verdict: Negative
```

Ejemplo Mail Logs: ejemplo VIRUS TS Conviction y AntiSpam Conviction de los registros de correo.

<#root>

Thu Jan 25 13:37:16 2024 Info: MID 3066060 interim

ThreatScanner verdict - VIRUS (2)

<Virus detected by ThreatScanner engine>

Thu Jan 25 13:37:16 2024 Info: MID 3066060 interim verdict using engine: CASE spam positive

Thu Jan 25 13:37:16 2024 Info: MID 3066060

using engine: CASE spam positive

Thu Jan 25 13:37:16 2024 Info: Message aborted MID 3066060 Dropped by CASE

Muestra de seguimiento: ausencia de condena por VIRUS TS y presencia de condena por antisпам.

```
25 Jan 2024 11:37:16 (GMT -08:00) Message 3066060 matched per-recipient policy DEFAULT for inbound mail policies.
25 Jan 2024 11:37:16 (GMT -08:00) Message 3066060 scanned by Anti-Spam engine: CASE. Interim verdict: Positive
25 Jan 2024 11:37:16 (GMT -08:00) Message 3066060 scanned by Anti-Spam engine: CASE. Final verdict: Positive
25 Jan 2024 11:37:16 (GMT -08:00) Message 3066060 aborted: Dropped by CASE
```

Ejemplo Mail Logs: VIRUS TS Conviction y AntiSpam Negative están presentes.

<#root>

Jan 23 21:38:57 2024 Info: MID 3013692

interim ThreatScanner verdict - VIRUS (2)

<Virus detected by ThreatScanner engine>

Jan 23 21:38:58 2024 Info: MID 3013692 interim verdict using engine: CASE spam negative

Jan 23 21:38:58 2024 Info: MID 3013692

using engine: CASE spam negative

Muestra de seguimiento: falta de condena por VIRUS TS y presencia de antiSpam negativo.

```
23 Jan 2024 19:38:57 (GMT -08:00) Message 3013692 matched per-recipient policy DEFAULT for inbound mail policies.
23 Jan 2024 19:38:58 (GMT -08:00) Message 3013692 scanned by Anti-Spam engine: CASE. Interim verdict: Negative
23 Jan 2024 19:38:58 (GMT -08:00) Message 3013692 scanned by Anti-Spam engine: CASE. Final verdict: Negative
```

Los registros de graymail contienen veredicto de Threat Scanner y contenido de apoyo para el análisis de TALOS si se realiza un desafío de falso positivo.

La presencia de los resultados sin procesar de Threat Scanner hizo que el registro de graymail se reiniciara más rápidamente. Para abordar este comportamiento, se han realizado las modificaciones SEG en los registros de graymail.

- AsyncOS 15.5 establece la suscripción de registro predeterminada para los archivos de registro de Graymail en 20 para aumentar la retención de registro.
  - La configuración del archivo de registro no cambia si la configuración es superior a 20 al actualizar.
- Los mensajes convictos de Inbound Graymail Interim muestran los resultados sin procesar del análisis completo, en el nivel de información.
- Los resultados del análisis de graymail para todos los demás mensajes se muestran en el nivel de depuración.

## Información Relacionada

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



## 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).