

Solucionar problemas de mensajes en varias cuarentenas

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Tipos de cuarentena](#)

[Información Relacionada](#)

Introducción

Este documento describe cómo un mensaje en un dispositivo de seguridad Cisco Email Security Appliance (ESA) puede residir en varias cuarentenas. Las cuarentenas son repositorios de correo temporales que contienen mensajes para su procesamiento posterior.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco Secure Email Gateway AsyncOS versión 16.x
- Cuarentenas de brotes, virus y políticas

La información de este documento se originó a partir de dispositivos dentro de un ambiente de laboratorio específico. Todos los dispositivos utilizados en este documento se iniciaron con una configuración desactivada (predeterminada). Si la red está activa, asegúrese de que se entienda el impacto potencial de cualquier comando antes de utilizar el comando.

Tipos de cuarentena

En función de las funciones con licencia, un Cisco ESA se puede configurar inicialmente con hasta tres cuarentenas.

- **Outbreak:** cuarentena utilizada por Virus Outbreak Filters, creada cuando la clave de licencia de Virus Outbreak Filters está habilitada.
- **Virus:** cuarentena que utiliza el motor antivirus y que se crea cuando se habilita la clave de licencia antivirus.
- **Política:** una cuarentena predeterminada (por ejemplo, puede utilizarla para almacenar mensajes que requieren revisión legal).
- **Análisis de archivos:** contiene los mensajes que se envían para el análisis de archivos hasta que se devuelve un veredicto.

Un mensaje puede terminar en más de una cuarentena por una variedad de razones. Por ejemplo, se puede crear un filtro para poner en cuarentena el correo electrónico que contiene material ofensivo para la cuarentena de 'Política'. Si un mensaje recibido coincide con ese filtro y también incluye un archivo adjunto cifrado que no se puede analizar en busca de virus, el mensaje se coloca tanto en la cuarentena de 'Virus' como en la de 'Política'.

Mensaje de ejemplo de mail_logs:

```
Sat Jul 25 00:56:03 2026 Info: MID 14712 ready 1352 bytes from <user@example.com>
Sat Jul 25 00:56:03 2026 Info: MID 14712 attachment 'encryptedfile.zip'
Sat Jul 25 00:56:03 2026 Info: ICID 14971 close
Sat Jul 25 00:56:03 2026 Info: MID 14712 matched all recipients for per-recipient policy DEFAULT in the
Sat Jul 25 00:56:03 2026 Info: MID 14712 interim verdict using engine: CASE spam negative
Sat Jul 25 00:56:03 2026 Info: MID 14712 using engine: CASE spam negative
Sat Jul 25 00:56:03 2026 Info: MID 14712 interim AV verdict using Sophos ENCRYPTED
Sat Jul 25 00:56:03 2026 Info: MID 14712 antivirus encrypted
Sat Jul 25 00:56:03 2026 Info: MID 14712 quarantined to "Policy" (content filter:Quarantine)
Sat Jul 25 00:56:03 2026 Info: MID 14712 quarantined to "Virus" (a/v verdict:ENCRYPTED)
Sat Jul 25 00:56:03 2026 Info: Message finished MID 14712 done
```

Los mensajes que residen en varias cuarentenas no se entregan hasta que se liberan de todas las cuarentenas en las que residen.

Ejemplo de registro de versión:

El resultado esperado es que el mensaje se entrega solo después de que se libera de ambas

cuarentenas.

Sat Jul 25 00:57:00 2026 Info: MID 14712 released from quarantine "Virus" (manual) t=57
Sat Jul 25 00:57:49 2026 Info: MID 14712 released from quarantine "Policy" (manual) t=106
Sat Jul 25 00:57:49 2026 Info: MID 14712 released from all quarantines

Información Relacionada

- [Cisco Secure Email Gateway - Guías para el usuario final](#)
- [Soporte técnico y descargas de Cisco](#)

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).