Configuración del Filtro Entrante Basada en la Verificación DKIM en ESA

Introducción

Este documento describe cómo configurar el dispositivo de seguridad de correo electrónico (ESA) para realizar cualquier acción sobre la verificación de correo electrónico identificado con claves de dominio (DKIM) a través de un filtro de contenido entrante o una configuración de filtro de mensajes.

prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- ESA
- Conocimiento básico de la configuración del filtro de contenido
- Conocimiento básico de la configuración de filtros de mensajes
- Centralización del conocimiento de configuración de cuarentenas de brotes, virus y políticas

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

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.

Configurar

Paso 1. Configuración de la verificación DKIM

Asegúrese de que la verificación DKIM esté habilitada. Navegue hasta **Políticas de correo > Políticas de flujo de correo**.

Para configurar la verificación DKIM en el ESA es similar a la verificación SPF. En los **Parámetros de Política Predeterminados** de Políticas de Flujo de Correo, simplemente active **On** DKIM Verification.

Paso 2. Verificar acción final

En primer lugar, determinar las medidas que deben adoptarse en relación con la verificación

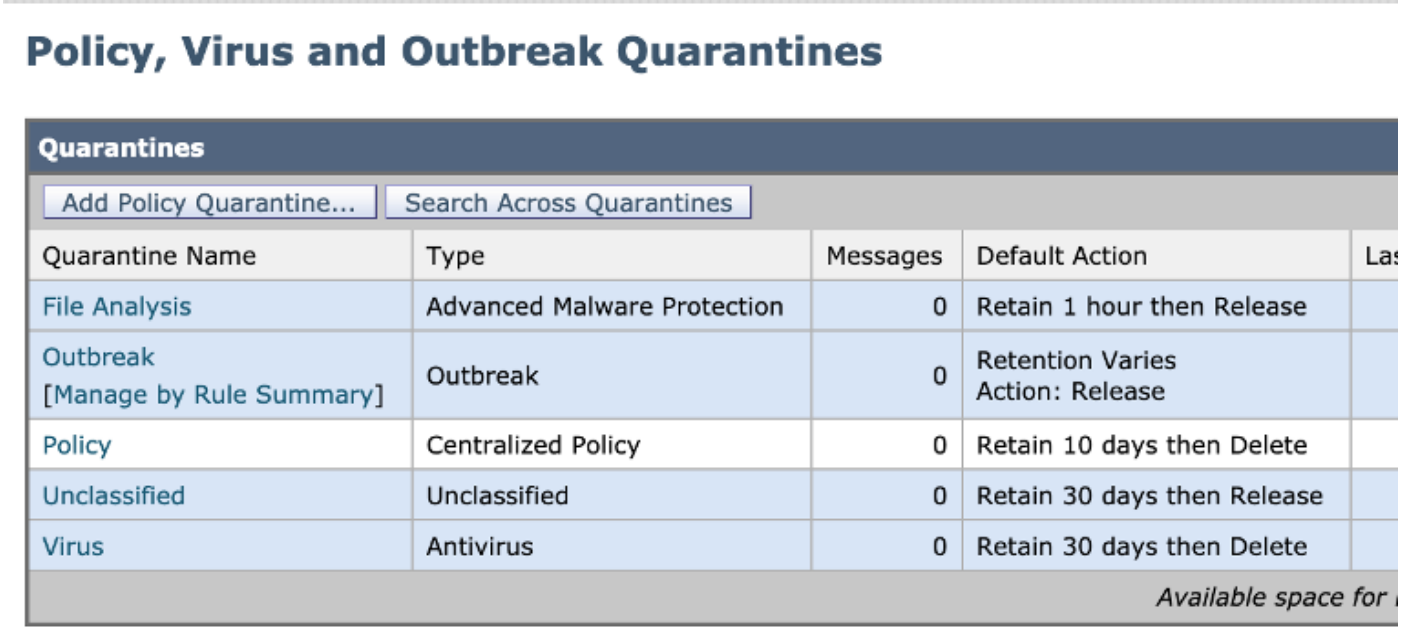
DKIM. Por ejemplo: colocar, agregar una etiqueta o poner en cuarentena. Si la acción final es poner en cuarentena el correo, revise las cuarentenas configuradas.

- Si no utiliza la administración centralizada:

Vaya a **ESA >Monitor> Cuarentenas de políticas, virus y brotes**.

- Si ha configurado la administración centralizada (SMA):

Vaya a **SMA >Correo electrónico >Cuarentena de mensajes >Cuarentenas de brotes, virus y políticas**, como se muestra en la imagen:

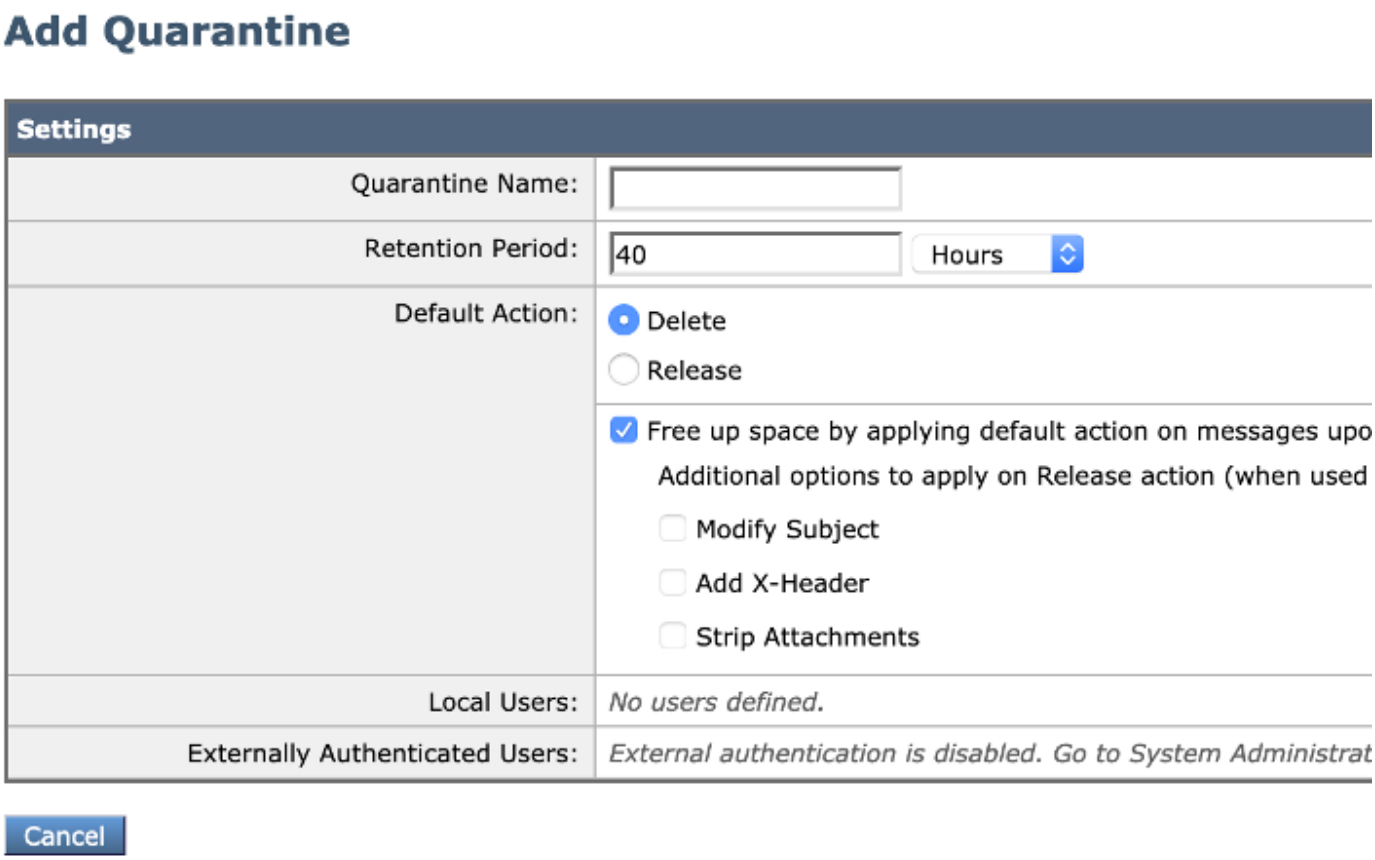


Si no hay cuarentena específica para los servicios **DKIM**/Autenticación de mensajes basada en dominio, notificación y conformidad (DMARC)/Marco de políticas de remitente (SPF). Se recomienda crear uno.

Mientras se encuentra en cuarentenas de brotes, virus y políticas, seleccione **Agregar cuarentena de políticas**:

Aquí puede configurar:

- Nombre de cuarentena: por ejemplo, **DkimQuarantine**
- Período de retención: Depende de usted y de las necesidades de su organización, así como de la acción predeterminada. Tras el período de retención del correo electrónico, se eliminará o se liberará y entregará, según la selección realizada, como se muestra en la imagen:



Paso 3. Filtro entrante para ESA

a. Cree un filtro de contenido entrante para ESA:

Vaya a **ESA > Políticas de correo > Filtros de contenido entrante > Agregar filtro**.

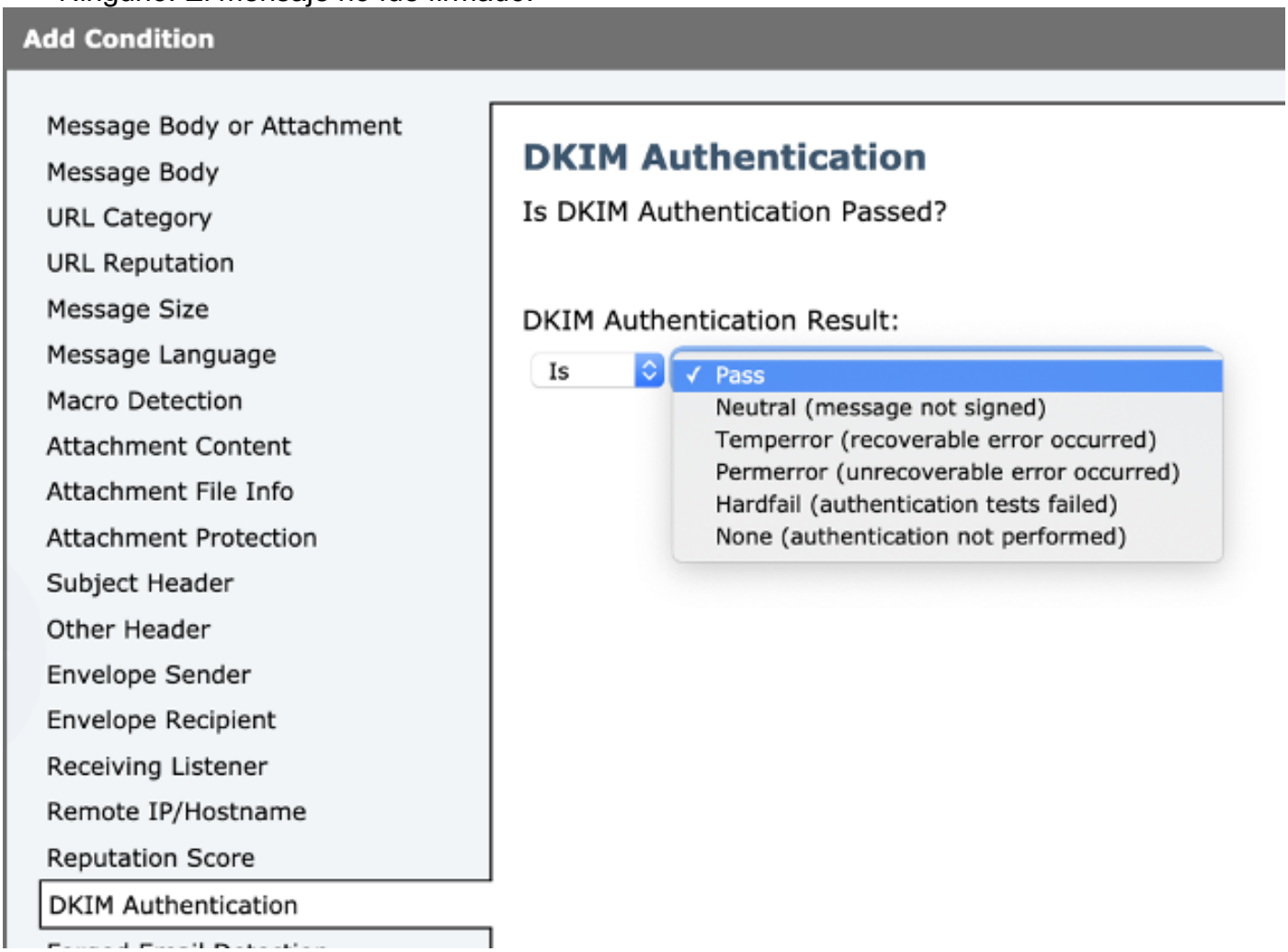
- Primera sección: Puede configurar el **Nombre**, **Descripción** y **Orden** del filtro:

- Segunda sección: Agregar condición. Puede agregar más de una condición y puede configurar más filtros de contenido para tomar medidas en la verificación DKIM:

Autenticación: resultados esperados y significado:

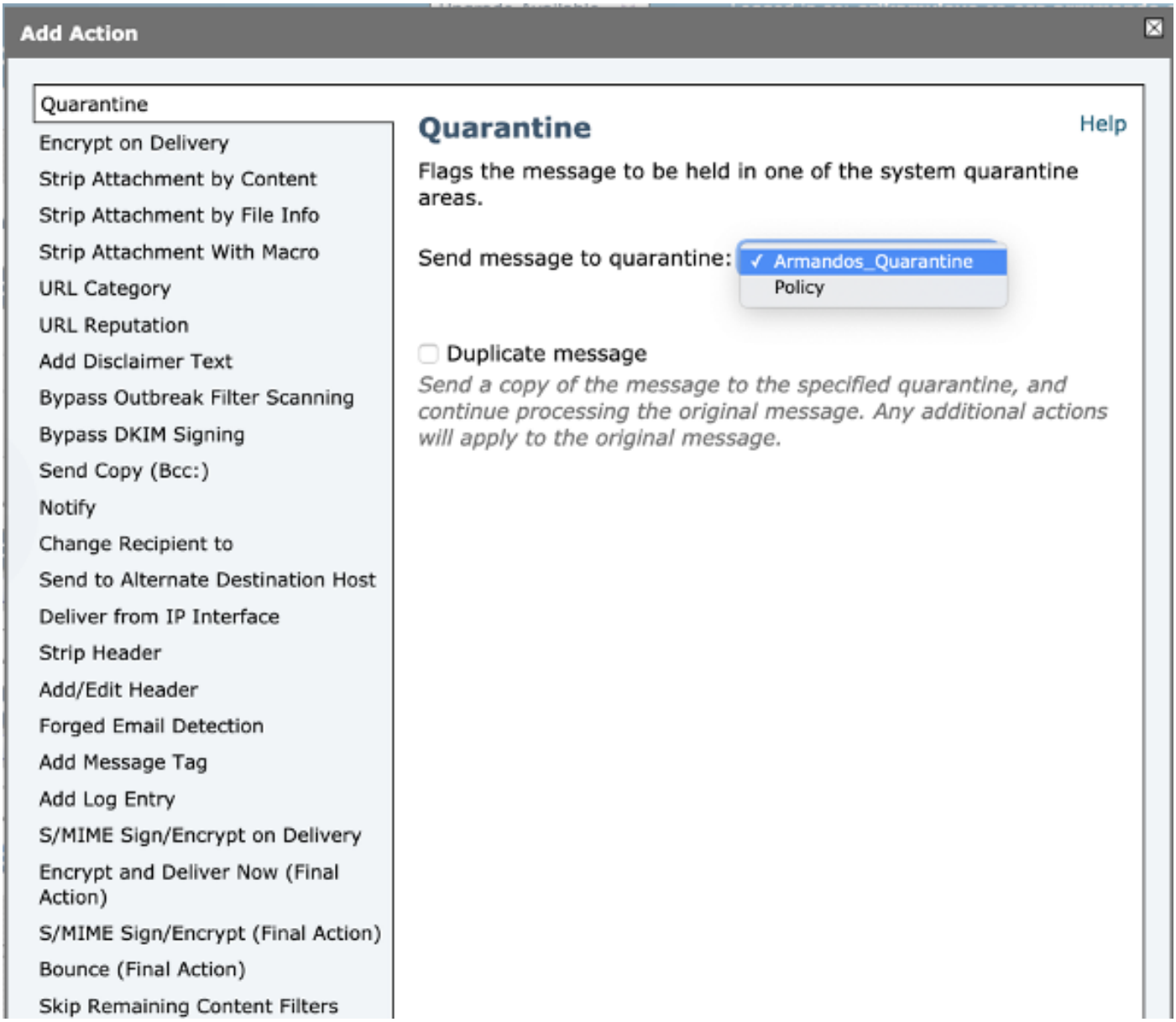
- Pass: El mensaje pasó las pruebas de autenticación.

- Neutra: La autenticación no se realizó.
- Temperror: Se ha producido un error recuperable.
- Permerror: Se ha producido un error irrecuperable.
- Falla dura: Las pruebas de autenticación fallaron.
- Ninguno. El mensaje no fue firmado.



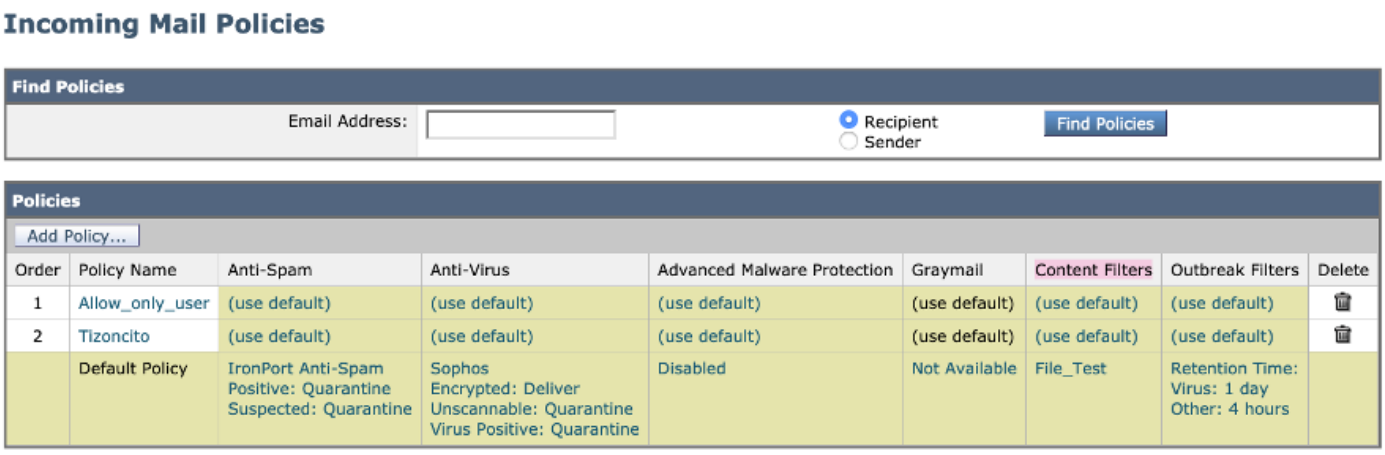
Nota: Requisitos de verificación DKIM: El remitente debe firmar el mensaje antes de que pueda verificarse. El dominio de envío debe tener una clave pública disponible en DNS para la verificación.

- Tercera sección: Seleccione una acción. Puede agregar más de una acción como agregar una entrada de registro, enviar a cuarentena, dejar el correo electrónico, notificar, etc. En este caso, seleccione la cuarentena configurada previamente, como se muestra en la imagen:



Agregar nuevo filtro a la política de flujo de correo:

Una vez creado el filtro. Desde ESA, agregue el filtro en cada política de flujo de correo donde desea verificar DKIM con una acción final. Navegue hasta **ESA> Políticas de correo >Políticas de correo entrante**, como se muestra en la imagen:



Haga clic en la columna **Filtros de contenido** y en la fila **Política de flujo de correo.**

Nota: (use default) no significa que esté configurado como configuración de política predeterminada. Configure cada política de flujo de correo con los filtros necesarios.

b. Cree un filtro de mensaje para ESA:

Todo el filtro de mensajes se configura desde ESA CLI. Ingrese el comando **Filters** y siga las instrucciones:

```
ESA. com> filters
Choose the operation you want to perform:
- NEW - Create a new filter.
- IMPORT - Import a filter script from a file.
[]> NEW
Enter filter script.  Enter '.' on its own line to end.
DKIM_Filter:
If (dkim-authentication == "hardfail" )
{
quarantine("DkimQuarantine");
}
.
1 filters added.
```

Una vez creado el filtro, revise la leyenda: **1 filtros agregados**.

Las condiciones y acciones que se deben configurar son las mismas que las que utiliza el filtro de contenido entrante.

Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

Filtro de contenido entrante:

- Desde la interfaz de usuario web ESA (WebUI)

a. Compruebe si el filtro está configurado:

Navegue hasta **ESA >Políticas de correo >Filtros de contenido entrante.** El filtro se debe configurar según el orden seleccionado anteriormente en la lista mostrada.

b. Compruebe si se aplica el filtro:

Navegue hasta **ESA>Políticas de correo >Políticas de correo entrante**.

El nombre del filtro se debe mostrar en la columna Filtros de contenido y en la fila Política de flujo de correo. Si la lista es amplia y no puede ver el nombre, haga clic en la lista de filtros para identificar los filtros aplicados a la política.

Filtro de mensaje:

```
From ESA CLI:
ESA. com> filters
Choose the operation you want to perform:
```

```
- NEW - Create a new filter.
- DELETE - Remove a filter.
- IMPORT - Import a filter script from a file.
- EXPORT - Export filters to a file
- MOVE - Move a filter to a different position.
- SET - Set a filter attribute.
- LIST - List the filters.
- DETAIL - Get detailed information on the filters.
- LOGCONFIG - Configure log subscriptions used by filters.
- ROLLOVERNOW - Roll over a filter log file.
[]> list

Num Active Valid Name

  1           Y      Y     DKIM_Filter
```

La lista muestra si el filtro está configurado y activo.

Troubleshoot

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

Verificar configuración:

Debe asegurarse de que:

- La política de flujo de correo tiene dkim: sobre verificación
- Hay una acción configurada en un filtro de contenido o filtro de mensaje
- En el caso de un filtro de contenido, compruebe que el filtro está asociado a un flujo de correo

Verificación del seguimiento de mensajes:

El rastreo de mensajes nos permite observar:

- El resultado de la verificación DKIM, p. ej.: permfail
- La entrada de registro configurada (si se configuró una)
- El filtro aplicado (nombre y acción realizada)

Seguimiento desde ESA:

```
Fri Apr 26 11:33:44 2019 Info: MID 86 ICID 98 From: <user@domain.com>
Fri Apr 26 11:33:44 2019 Info: MID 86 ICID 98 RID 0 To: <userb@domainb.com>
Fri Apr 26 11:33:44 2019 Info: MID 86 Message-ID '<3903af$2r@mgt.esa.domain.com>Fri Apr 26
11:33:44 2019 Info: MID 86 DKIM: permfail body hash did not verify [final]
Fri Apr 26 11:33:44 2019 Info: MID 86 Subject "Let's go to camp!"
Fri Apr 26 11:33:44 2019 Info: MID 86 ready 491 bytes from <user@domain.com>
Fri Apr 26 11:33:44 2019 Info: MID 86 matched all recipients for per-recipient policy
Allow_only_user in the inbound table
Fri Apr 26 11:33:46 2019 Info: MID 86 interim verdict using engine: CASE spam negative
Fri Apr 26 11:33:46 2019 Info: MID 86 using engine: CASE spam negative
Fri Apr 26 11:33:46 2019 Info: MID 86 interim AV verdict using Sophos CLEAN
Fri Apr 26 11:33:46 2019 Info: MID 86 antivirus negative
Fri Apr 26 11:33:46 2019 Info: MID 86 AMP file reputation verdict : UNSCANNABLE
Fri Apr 26 11:33:46 2019 Info: MID 86 using engine: GRAYMAIL negative
Fri Apr 26 11:33:46 2019 Info: MID 86 Custom Log Entry: The content that was found was:
DkimFilter
Fri Apr 26 11:33:46 2019 Info: MID 86 Outbreak Filters: verdict negative
```

```
Fri Apr 26 11:33:46 2019 Info: MID 86 quarantined to "DkimQuarantine" by add-footer filter
'DkimFilter '
Fri Apr 26 11:33:46 2019 Info: Message finished MID 86 done
```

Información Relacionada

- Prácticas recomendadas ESA-SPF-DKIM-DMARC
- Guía del usuario final del dispositivo de seguridad de correo electrónico
- DKIM RFC4871
- RFC8301 DKIM
- DKIM RFC8463
- Soporte Técnico y Documentación - Cisco Systems