# Identifique y permita los servidores pobres del correo de la calificación de la reputación de SenderBase (SBR)

## Contenido



## Introducción

Este artículo describe cómo identificar y permitir temporalmente los servidores del correo con la calificación pobre de la reputación de SenderBase (SBR) a través del dispositivo de seguridad del correo electrónico (ESA).

## Antecedentes

La filtración de la reputación del remitente es la primera capa de protección del Spam, permitiendo que usted controle los mensajes que vienen con gateway de correo electrónico basado en la fiabilidad del remitente según lo determinado por los SBR.  Los servidores de correo electrónico con los SBR pobres pueden hacer sus conexiones rechazaas, o sus mensajes ser despedido, sobre la base de sus preferencias.

## Problema

Un mail server conecta con el ESA y está señalado pues los SBR pobres y los correos electrónicos son retrasado debido a una respuesta de 554 S TP recibida por el servidor de conexión.

Respuesta de la muestra 554:

```
-----Original Message-----
From: Mail Delivery System [mailto:Mailer-Daemon@example.domain.com]
Sent: 25 April 2013 23:23
To: user@companyx.com
Subject: Mail delivery failed: returning message to sender

This message was created automatically by mail delivery software.

A message that you sent could not be delivered to one or more of its
recipients. This is a permanent error. The following address(es) failed:
```

```
person@example.domain.com
SMTP error from remote mail server after initial connection:
host gatekeeper.companyx.com [195.195.195.1]: 554-gatekeeper1.companyx.com
554 Your access to this mail system has been rejected due to the sending
MTA's poor reputation. If you believe that this failure is in error, please
contact the intended recipient via alternate means.
```

# Solución

## Identifique el mail server pobre SBR

Utilice el comando line interface(cli) pues la interfaz delusuario (GUI) Seguimiento de mensajes no registra las conexiones rechazadas por abandono.

> Nota: El seguimiento de las conexiones rechazadas se puede habilitar en los **servicios del > Security (Seguridad) GUI > Seguimiento de mensajes > permiso "dirección rechazada de la conexión"**

Utilice el **grep** contra el dominio para tirar de todos los datos de registro relacionados contra ese dominio. Para esta salida, el dominio del ejemplo usado es *test.com*:

```
myesa.local> grep "test.com" mail_logs

Info: New ICID 1512 to Management (10.0.0.1) from 198.51.100.1 connecting host reverse DNS
hostname: smtp1. test.com
Info: MID 6531 ICID 1512 From: test@test.com
```

Entonces **grep la** conexión entrante ID (ICID) para extraer la información del host de correo. El ICID está registrando se utiliza para revelar toda la información por ejemplo: enviando la dirección IP del host, el DNS verificó el nombre de host (si está disponible), corresponder con del sendergroup y la calificación asociada SBR:

```
myesa.local> grep "ICID 1512" mail_logs


Tue Mar 10 12:04:29 2015 Info: New SMTP ICID 1512 interface Management (10.0.0.1) address
198.51.100.1 reverse dns host unknown verified smtp1.test.com
Tue Mar 10 12:04:29 2015 Info: ICID 1512 REJECT SG BLACKLIST match sbrs[-10:-3] SBRS -4.0
```

## Permita el mail server pobre SBR con el ESA

1. Del GUI, navegue **para enviar las directivas > la descripción del SOMBRERO**.
2. El tecleo **agrega el grupo del remitente…**
3. Nombre el grupo del remitente con un nombre significativo.
4. Seleccione la orden de modo que esté sobre el grupo del remitente de la LISTA NEGRA.
5. Seleccione cualquier directiva del correo, **VALIDADA** o **ESTRANGULAMIENTA**.
6. Deje el resto de los campos vacíos.
7. El tecleo **somete y agrega los remitentes**
8. Agregue la dirección IP o el nombre del host de DNS de los host afectados según lo situado del comando grep.
9. El tecleo **somete**
10. Revise la descripción del SOMBRERO y asegúrese de que el nuevo grupo del remitente está pedido correctamente.
11. Finalmente, **cometer del** tecleo para salvar todos los cambios de configuración.

Para el direccionamiento del remitente, se permiten los formatos siguientes:

- Direccionamientos del IPv6 tales como 2001:420:80:1::5
- Direccionamientos del IPv4 tales como 10.1.1.0
- Subredes del IPv4 o del IPv6 tales como 10.1.1.0/24, 2001:db8::/32
- Intervalos de direcciones del IPv4 o del IPv6 tales como 10.1.1.10-20, 10.1.1-5, o 2001:db8::1-2001:db8::10
- Nombres de host tales como example.com
- Nombres de host parciales tales como .example.com.

En el ejemplo como se muestra arriba, para permitir cualquier otra conclusión de la información del mail server con *test.com*, esto habría sido configurada como:

```
198.51.100.1
smtp1.test.com
.test.com
```

# Información Relacionada

Sobre Cisco SenderBase