# Identificeer en sta arme SBRS-mailservers (SenderBase Reputation Score) toe

## Inhoud

[Inleiding](#)
[Achtergrondinformatie](#)
[Probleem](#)
[Oplossing](#)
[Identificeer de slechte SBRS-mailserver](#)
[Geef de arme SBRS-mailserver door de ESA](#)
[Gerelateerde informatie](#)

## Inleiding

In dit artikel wordt beschreven hoe u mailservers met een slechte SenderBase Reputation Score (SBRS) kunt identificeren en tijdelijk toestaan via de E-mail security applicatie (ESA).

## Achtergrondinformatie

Sender reputatie-filtering is de eerste laag van spambescherming, waardoor je de berichten kunt controleren die door de e-mailpoort komen op basis van de betrouwbaarheid van de afzender zoals bepaald door SBRS. E-mailservers met slechte SBRS kunnen hun verbindingen verworpen krijgen, of hun berichten kunnen worden geblokkeerd, gebaseerd op uw voorkeuren.

## Probleem

Een mailserver sluit zich aan op de ESA en wordt gemeld als slechte SBRS en e-mails worden vertraagd door een 554 mtd-reactie die door de verbindingsserver wordt ontvangen.

Steekproef 554 respons:

```
-----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.
```

# Oplossing

## Identificeer de slechte SBRS-mailserver

Gebruik de Opdracht Line Interface (CLI) als het bericht dat de grafische User Interface (GUI) heeft geplaatst geen afgewezen verbindingen standaard opneemt.

> Opmerking: Tracking van afgekeurde verbindingen kan worden ingeschakeld bij **GUI > Security Services > Message Tracking > Schakel "Rejected Connection Handling" in**

Gebruik **grep** tegen het domein om alle verwante loggegevens tegen dat domein te trekken. Voor deze uitvoer is het gebruikte voorbeelddomein *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
```

**grep** dan de inkomende verbinding ID (ICID) om de informatie over de mailhost te extraheren. De ICID is logging gebruikt om alle informatie te onthullen, zoals: het verzenden van IP-adres van de host, de DNS-gecontroleerde hostname (indien beschikbaar), sendergroup matching en de bijbehorende SBRS-score:

```
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
```

## Geef de arme SBRS-mailserver door de ESA

1. Vanuit de GUI, navigeer naar **Mail Policy > HAT overview**.
2. Klik **Zender groep toevoegen...**
3. Geef de zender Group een betekenisvolle naam.
4. Selecteer de opdracht zodat deze boven de BLACKLIST Sender Group staat.
5. Selecteer een van de e-mailregels, **AANVAARD** of **OMGEKEERD**.
6. Laat alle andere velden leeg.
7. Klik op **Senders indienen en toevoegen**
8. Voeg het IP-adres of de DNS-hostnaam van de getroffen host(s) toe zoals onder de grep-opdracht.
9. Klik op **Inzenden**
10. Bekijk het HAT-overzicht en controleer of de nieuwe verzendgroep correct is geordend.
11. Klik tot slot op **Commit** om alle configuratiewijzigingen op te slaan.

Voor verzendadres zijn de volgende bestandsindelingen toegestaan:

- IPv6-adressen zoals 2001:420:80:1:5
- IPv4-adressen zoals 10.1.1.0
- IPv4- of IPv6-subnetten zoals 10.1.1.0/24, 2001:db8:/32
- IPv4- of IPv6-adresbereiken zoals 10.1.1.10-20, 10.1.1-5 of 2001:db8::1-2001:db8:10
- Hostnamen zoals voorbeeld.com
- Deelstaathostnamen zoals .voorbeeld.com.

In het voorbeeld zoals hierboven wordt getoond, zou, om enige andere informatie van de mailserver die met *test.com* eindigt, dit als volgt zijn geconfigureerd:

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

# Gerelateerde informatie

Over Cisco SenderBase