Contents

Introduction

This article describes how to identify and temporarily allow mail servers with poor SenderBase Reputation Score (SBRS) through the Email Security Appliance (ESA).

Background Information

Sender reputation filtering is the first layer of spam protection, allowing you to control the messages that come through the email gateway based on sender's trustworthiness as determined by SBRS. Email servers with poor SBRS can have their connections rejected, or their messages bounced, based on your preferences.

Problem

A mail server connects to the ESA and is reported as poor SBRS and emails are delayed due to a 554 SMTP response received by the connecting server.

Sample 554 Response:

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

Solution

Identify the poor SBRS mail server

Use the Command Line Interface (CLI) as the Graphical User Interface's (GUI) message tracking

does not record rejected connections by default.

> **Note**: Tracking of Rejected connections can be enabled at **GUI > Security Services > Message Tracking > Enable "Rejected Connection Handling"**

Use **grep** against the domain in order to pull all related logging data against that domain. For this output, the example domain used is *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
```

Then **grep** the Incoming Connection ID (ICID) to extract the mail host information. The ICID is logging is used in order to reveal all information such as: sending host IP address, the DNS verified hostname (if available), sendergroup matching and the associated 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
```

Allow the poor SBRS mail server through the ESA

1. From the GUI, navigate to **Mail Policies > HAT overview**.
2. Click **Add Sender Group...**
3. Name the Sender Group with a meaningful name.
4. Select the Order so that it will be above the BLACKLIST Sender Group.
5. Select either mail policy, **ACCEPTED** or **THROTTLED**.
6. Leave all other fields empty.
7. Click **Submit and Add Senders**
8. Add either the IP address or DNS hostname of the affected host(s) as located from the grep command.
9. Click **Submit**
10. Review the HAT overview and ensure that the new Sender Group is ordered correctly.
11. Finally, click **Commit** to save all configuration changes.

For Sender address, the following formats are allowed:

- IPv6 addresses such as 2001:420:80:1::5
- IPv4 addresses such as 10.1.1.0
- IPv4 or IPv6 subnets such as 10.1.1.0/24, 2001:db8::/32
- IPv4 or IPv6 address ranges such as 10.1.1.10-20, 10.1.1-5, or 2001:db8::1-2001:db8::10
- Hostnames such as example.com
- Partial hostnames such as .example.com.

In the example as shown above, in order to allow any other mail server information ending with *test.com*, this would have been configured as:

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

Related Information

About Cisco SenderBase