

Bypass SBRS for Specific Hosts and Continue to Scan for SPAM



Document ID: 118566

Contributed by Ben Robson and Stephan Bayer, Cisco TAC Engineers.

Oct 13, 2014

Contents

Introduction

Symptoms

Procedure

Introduction

This document describes how to bypass SBRS for specific hosts and continue to scan for SPAM.

Symptoms

- Sender using a public MTA is being rejected due to SBRS reputation score
- <http://senderbase.org> shows a SBRS score of "poor" for the sending IP address

A GREYLIST is useful to bypass SBRS filtering for a specific host, in the case the host name or sending MTA may encompass other senders other than your specific trusted user. When using this GREYLIST, the mail is still scanned for SPAM which differs from using the WHITELIST which bypasses SPAM scanning.

Procedure

To setup a GREYLIST in the GUI:

1. Navigate to *GUI > Mail Policies -> HAT Overview -> Add Sender Group*.
2. Name the group GREYLIST and select an order of "1".
3. Choose the "ACCEPTED" mail flow policy.
4. Leave all other settings at their defaults.
5. Click *Submit and Add Senders*.
6. Enter the IP address or hostname of the sender.
7. Submit this page.
8. If needed, click *Add Sender* and keep adding any additional IP addresses.
9. *Commit* the changes.