ESA Understanding SLBL evaluation of email addresses

Contents

[Introduction](#)
[Prerequisites Requirements](#)
[Components Used](#)
[Understanding working of SLBL](#)
[Troubleshoot](#)
[Related Information](#)

Introduction

This article explains how Safelist Blocklist (SLBL) evaluates on the Email Security Appliance (ESA) against envelope sender (mail from) and display From header (From) of an email.
Contributed by Soren Petersen, Libin Varghese, Cisco TAC Engineers

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco ESA
- AsyncOS
- Cisco ESA Anti-Spam feature
- Configuring SLBL

Components Used

The information in this document is based on these software and hardware versions:
All AsyncOS versions

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Understanding working of SLBL

SLBL list for a recipient evaluates against both mail from and display From address of an email.

A sender’s being on asafelistor blocklist does not prevent theappliancefrom scanning a message for viruses or determining if the message meets the criteria for a content-related mail policy. Even if the sender of a message is on the recipient’ssafelist, the message may not be delivered to the end user depending on other scanning settings and results.

When you enablesafelists and blocklists, theappliancescans the messages against thesafelist/blocklist database immediately before anti-spam scanning. If theappliancedetects a sender or domain that matches asafelistor blocklist entry, the message will be splintered if there are multiple recipients (and the recipients have differentsafelist/blocklist settings).

> **Note**: When an end user selects "Release and add to Safelist" for an email in their quarantine, if the envelope sender and From header are different both would be added to users Safelist.

> **Note:** Adding to Safelist may fail if entry already exists in the users Blocklist.

The SLBL feature evaluates messages on both envelope "mail from" and on "From" header in the following sequence:

1. Full email address in "From" header
2. Domain part of email address in "From" header
3. Full email address in envelope "mail from"
4. Domain part of email address in envelope "mail from"

The message is processed until the first match is met.

Configuration 1:
User A@cisco.com has test@gmail.com added to Safelist.

Results: Recipient: A@cisco.com, mail from: random@yahoo.com From: test@gmail.com SLBL spam negative and SLBL graymail negative
Recipient: A@cisco.com, mail from: test@gmail.com From: random@yahoo.com SLBL spam negative and SLBL graymail negative

Configuration 2:
User A@cisco.com has example@gmail.com added to Blocklist

Results: Recipient: A@cisco.com, mail from: random@yahoo.com From: example@gmail.com SLBL spam positive and SLBL graymail positive
Recipient: A@cisco.com, mail from: example@gmail.com From: random@yahoo.com SLBL spam positive and SLBL graymail positive

Configuration 3:
User A@cisco.com has test@gmail.com added to Safelist and gmail.com added to Blocklist

Results: Recipient: A@cisco.com, mail from: random@gmail.com From: test@gmail.com SLBL spam negative and SLBL graymail negative
Recipient: A@cisco.com, mail from: test@gmail.com From: random@gmail.com SLBL spam positive and SLBL graymail positive

Configuration 4:
User A@cisco.com has gmail.com added to Safelist and test@gmail.com added to Blocklist

Results: Recipient: A@cisco.com, mail from: random@gmail.com From: test@gmail.com SLBL spam

```
positive and SLBL graymail positive
Recipient: A@cisco.com, mail from: test@gmail.com From: random@gmail.com SLBL spam negative and
SLBL graymail negative
```

Troubleshoot

Changes made to SLBL are not effective immediately and may need a few minutes to sync.

Related Information

Cisco Secure Email Gateway End-User Guides
Cisco Secure Email Gateway Release Notes
Modifying end user Safelist Blocklist
Using telnet to test SMTP email
Testing Anti-Spam feature on ESA