ESA FAQ: How can I test the ESA Anti−Spam feature?

Document ID: 117865

Contributed by Valter Pereira da Costa and Robert Sherwin, Cisco TAC Engineers.
Jun 27, 2014

Contents

Introduction
Prerequisites
Requirements
Components Used
How can I test the ESA Anti−Spam feature?
Test Anti−Spam with TELNET
Troubleshoot

Introduction

This document describes how to test the Cisco Email Security Appliance (ESA) Anti−Spam feature.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco ESA
- AsyncOS
- Cisco ESA Anti−Spam feature

Components Used

The information in this document is based on all versions of AsyncOS.

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.

How can I test the ESA Anti−Spam feature?

In order to test the functionality of the ESA Anti−Spam feature, create a new message via TELNET or your email client (Microsoft Outlook, Eudora, Thunderbird, Lotus Notes) and insert one of these headers:

- ***X−Advertisement: Suspect***
- ***X−Advertisement: Spam***
- ***X−Advertisement: Marketing***

You can then send the message through the ESA with the Anti−Spam feature enabled and monitor the results.

Test Anti−Spam with TELNET

This section provides an example that shows how to manually create a test message via the widely−available TELNET utility.

Use the information in the next example in order to create a test message through TELNET. Enter the information shown in ***bold***, and the server should respond as shown:

```
telnet hostname.example.com 25

220 hostname.example.com ESMTP
ehlo localhost
250−hostname.example.com
250−8BITMIME
250 SIZE 10485760
mail from: <sender@example.com>
250 sender <sender@example.com> ok
rcpt to: <recipient@example.com>
250 recipient <recipient@example.com> ok
data
354 go ahead
X−Advertisement: Marketing
from: sender@example.com
to: recipient@example.com
subject: test

test
.
250 ok:  Message 120 accepted
```

Review the ***mail_logs*** and verify the outcome of the anti−spam scanning in order to assure that the message is treated as written. As per the previous example, the default inbound mail policy detects that the mail is Marketing:

```
Thu Jun 26 22:21:56 2014 Info: New SMTP DCID 66 interface 172.11.1.111 address
 111.22.33.111 port 25
Thu Jun 26 22:21:58 2014 Info: DCID 66 TLS success protocol TLSv1 cipher
 RC4−SHA
Thu Jun 26 22:21:58 2014 Info: Delivery start DCID 66 MID 119 to RID [0]
Thu Jun 26 22:21:59 2014 Info: Message done DCID 66 MID 119 to RID [0]
Thu Jun 26 22:21:59 2014 Info: MID 119 RID [0] Response '2.0.0 s5R2LhnL014175
 Message accepted for delivery'
Thu Jun 26 22:21:59 2014 Info: Message finished MID 119 done
Thu Jun 26 22:22:04 2014 Info: DCID 66 close
Thu Jun 26 22:22:53 2014 Info: SDS_CLIENT: URL scanner enabled=0
Thu Jun 26 22:25:35 2014 Info: SLBL: Database watcher updated from snapshot
 20140627T022535−slbl.db.
Thu Jun 26 22:26:04 2014 Info: Start MID 120 ICID 426
Thu Jun 26 22:26:04 2014 Info: MID 120 ICID 426 From: <sender@example.com>
Thu Jun 26 22:26:10 2014 Info: MID 120 ICID 426 RID 0 To:
 <recipient@example.com>
Thu Jun 26 22:26:20 2014 Info: MID 120 Subject 'test'
Thu Jun 26 22:26:20 2014 Info: MID 120 ready 201 bytes from <sender@example.com>
Thu Jun 26 22:26:20 2014 Info: MID 120 matched all recipients for per−recipient
 policy DEFAULT in the inbound table
Thu Jun 26 22:26:21 2014 Info: MID 120 interim verdict using engine:
 CASE marketing
Thu Jun 26 22:26:21 2014 Info: MID 120 using engine: CASE marketing
Thu Jun 26 22:26:21 2014 Info: MID 120 interim AV verdict using Sophos CLEAN
Thu Jun 26 22:26:21 2014 Info: MID 120 antivirus negative
Thu Jun 26 22:26:21 2014 Info: Message finished MID 120 done
```

```
Thu Jun 26 22:26:21 2014 Info: MID 121 queued for delivery
Thu Jun 26 22:26:21 2014 Info: New SMTP DCID 67 interface 172.11.1.111 address
 111.22.33.111 port 25
Thu Jun 26 22:26:21 2014 Info: DCID 67 TLS success protocol TLSv1 cipher RC4-SHA
Thu Jun 26 22:26:21 2014 Info: Delivery start DCID 67 MID 121 to RID [0]
Thu Jun 26 22:26:22 2014 Info: Message done DCID 67 MID 121 to RID [0]
Thu Jun 26 22:26:22 2014 Info: MID 121 RID [0] Response '2.0.0 s5R2QQso009266
 Message accepted for delivery'
Thu Jun 26 22:26:22 2014 Info: Message finished MID 121 done
Thu Jun 26 22:26:27 2014 Info: DCID 67 close
```

Troubleshoot

If the message is not detected as Spam, Suspected Spam, or Marketing, review the ***Mail Polcies*** > ***Incoming Mail Policies*** or ***Mail Policies > Outgoing Mail Policies***. Choose the Default Policy or Policy Name, and click the hyperlink in the the Anti−Spam column in order to verify the Anti−Spam settings and configuration for the policy.

Cisco recommends that you enable the ***Positively−Identified Spam Settings***, the ***Suspected Spam Settings***, and/or the ***Marketing Email Settings*** as desired.

Updated: Jun 27, 2014 Document ID: 117865