ESA Advanced Malware Protection (AMP) Test

Document ID: 118511

Contributed by Robert Sherwin, Cisco TAC Engineer.
Nov 14, 2014

Contents

Introduction

This document describes how to test and verify the Advanced Malware Protection (AMP) features of the Cisco Email Security Appliance (ESA).

Test AMP on the ESA

With the release of AsyncOS 8.5 for the ESA, AMP performs file reputation scans and file analysis in order to detect malware in attachments.

Feature Keys

In order to implement AMP, you must have a valid and active feature key for both ***File Reputation*** and ***File Analysis*** on your ESA. Visit ***System Administration> Feature Keys*** on the GUI, or use ***featurekeys*** on the CLI, in order to verify the feature keys.

Security Services

In order to enable the service from the GUI, navigate to ***Security Services > File Reputation and Analysis***. From the CLI, you can run ***ampconfig***. Submit and commit your changes to the configuration.

Incoming Mail Policies

Once you have enabled the service, you must have this service tied to an incoming mail policy.

1. Navigate to ***Mail Policies > Incoming Mail Policies***.

2. Select your ***Default Policy*** or preconfigured policy as needed. The ***Advanced Malware Protection*** column on the Incoming Mail Polices page displays.

3. Select the ***Disabled*** link for the column, and ***Enable File Reputation*** and ***Enable File Analysis*** on the options page.

4. You can make any further configuration enhancements to message scanning, actions for un−scannable attachments, and actions for positively identified messages, as needed.

5. Submit and commit your changes to the configuration.

Test

At this time, your incoming mail policy is enabled to scan and detect malware. You must have a true malware sample with which to test. If you need valid examples, visit the European Institute for Computer Antivirus Research (eicar) downloads page.

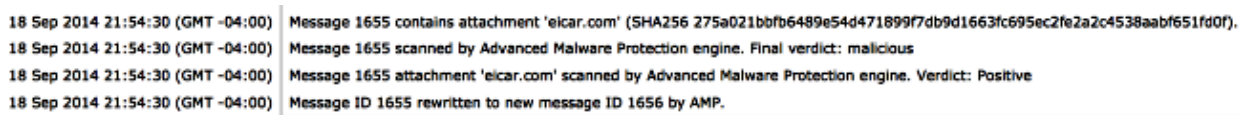
Caution: Cisco cannot be held responsible when these files or your AV scanner in combination with these files cause any damage to your computer or network environment. YOU DOWNLOAD THESE FILES AT YOUR OWN RISK. Download these files only if you are sufficiently secure in the usage of your AV scanner, computer settings, and network environment. This information is provided as a courtesy for test and reproduction purposes.

With the use of a valid a preconfigured email account, send the attachment through your ESA and normal processing. You can use the CLI of the ESA, and ***tail mail_logs*** in order to monitor the mail as it processes. You will see the Message ID (MID) listed in the mail logs. Output similar to this displays:

```
Thu Sep 18 16:17:38 2014 Info: New SMTP ICID 16488 interface Management
(192.168.0.199) address 65.55.116.95 reverse dns host blu004−omc3s20.hotmail.com
verified yes
Thu Sep 18 16:17:38 2014 Info: ICID 16488 ACCEPT SG UNKNOWNLIST match sbrs
[−1.0:10.0] SBRS 5.5
Thu Sep 18 16:17:38 2014 Info: Start MID 1653 ICID 16488
Thu Sep 18 16:17:38 2014 Info: MID 1653 ICID 16488 From: <joe_user@hotmail.com>
Thu Sep 18 16:17:38 2014 Info: MID 1653 ICID 16488 RID 0 To:
<any.one@mylocal_domain.com>
Thu Sep 18 16:17:38 2014 Info: MID 1653 Message−ID '<BLU437−SMTP10E1315A60354F2
906677B9DB70@phx.gbl>'
Thu Sep 18 16:17:38 2014 Info: MID 1653 Subject 'Your Daily Update''
Thu Sep 18 16:17:38 2014 Info: MID 1653 ready 2313 bytes from
<joe_user@hotmail.com>
Thu Sep 18 16:17:38 2014 Info: MID 1653 matched all recipients for per−recipient
policy DEFAULT in the inbound table
Thu Sep 18 16:17:38 2014 Info: ICID 16488 close
Thu Sep 18 16:17:39 2014 Info: MID 1653 interim verdict using engine:
CASE spam negative
Thu Sep 18 16:17:39 2014 Info: MID 1653 using engine: CASE spam negative
Thu Sep 18 16:17:39 2014 Info: MID 1653 AMP file reputation verdict : MALWARE
Thu Sep 18 16:17:39 2014 Info: Message aborted MID 1653 Dropped by amp
Thu Sep 18 16:17:39 2014 Info: Message finished MID 1653 done
```

The previous example shows that AMP detected the malware attachment and ***dropped*** as the final action per the default settings.

The same details are also seen in Message Tracking from the GUI:



If you choose to deliver positively identified malware, or other advanced options in the AMP configuration from the Incoming Mail Policies, you might see this mail processing outcome:

```
Thu Sep 18 21:54:30 2014 Info: MID 1655 AMP file reputation verdict : MALWARE
Thu Sep 18 21:54:30 2014 Info: MID 1655 rewritten to MID 1656 by AMP
```

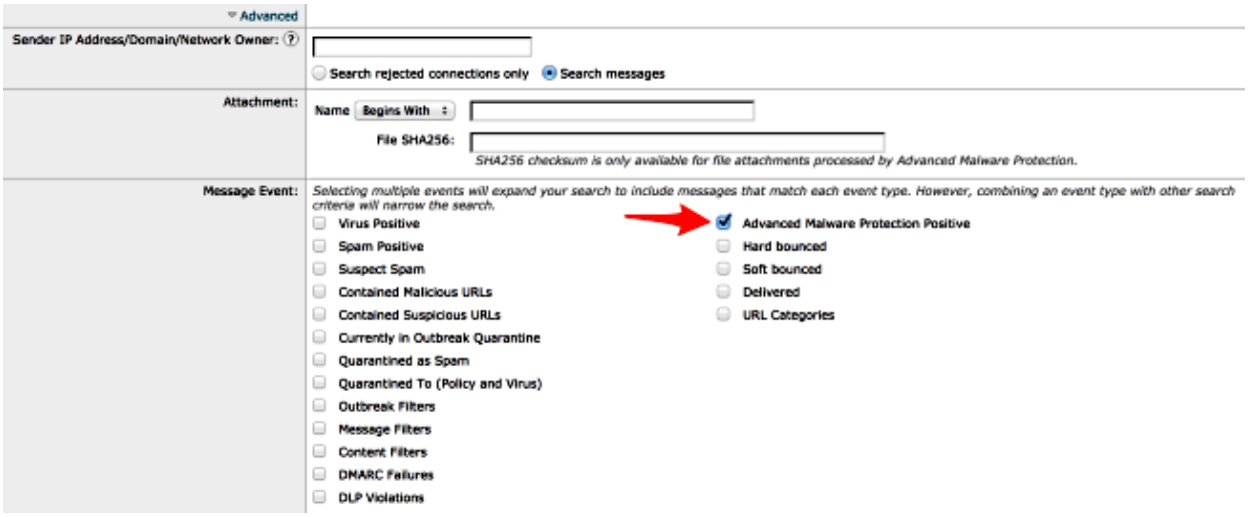
The reputation verdict is still positive for ***MALWARE*** as shown. The rewritten action is per the message modification actions and subject line prepending of ***[WARNING: MALWARE DETECTED]***.

A clean file, or a file that has not been identified at processing time as malware, has this verdict written to the mail logs:

```
Thu Sep 18 21:58:33 2014 Info: MID 1657 AMP file reputation verdict : CLEAN
```

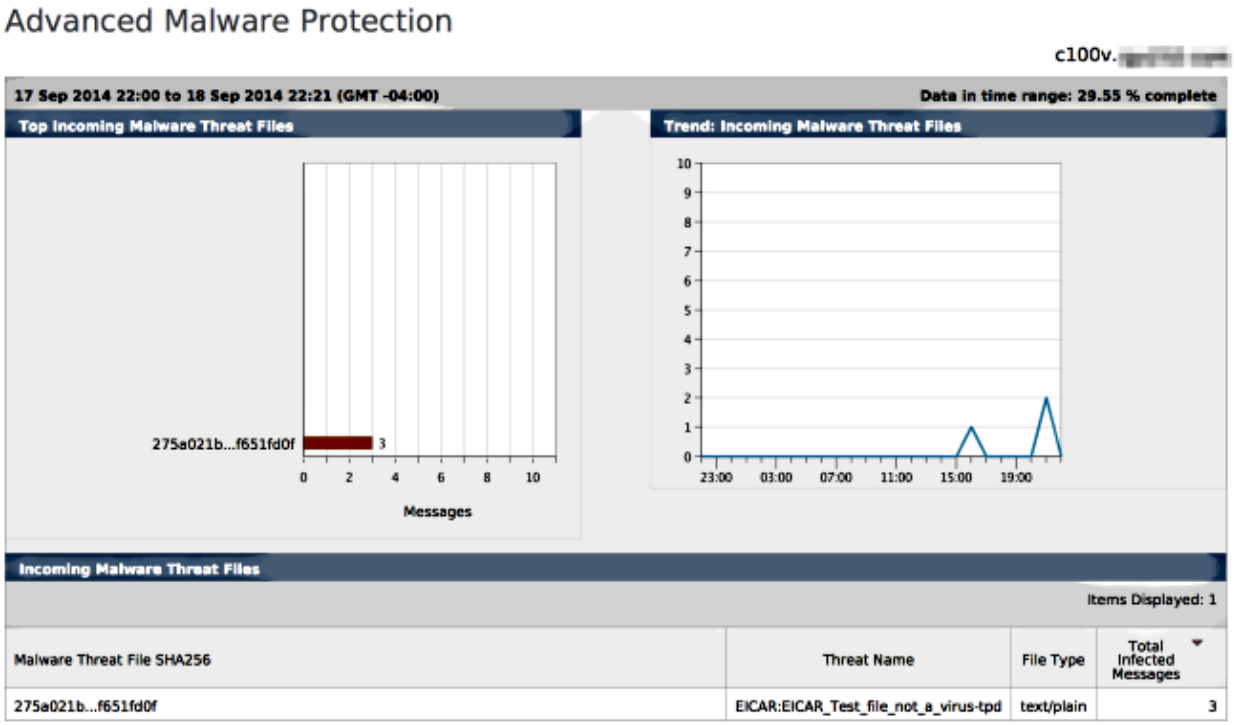
Advanced Message Tracking for AMP+ Messages

Also from the GUI, when you use Message Tracking and the Advanced drop−down menu, you can choose to search for an Advanced Malware Protection Positive message directly:



Advanced Malware Protection Reports

From the ESA GUI, you also see report tracking for positively identified messages through AMP. Navigate to ***Monitor > Advanced Malware Protection*** and modify the time range as needed. You now see similar, with the previous examples for input:



Troubleshoot

If you do not see a known, true malware file that is positively scanned by AMP, review the mail logs in order to assure that another service did not take action on the message and/or attachment before AMP scanned the message.

From the earlier example used, when Sophos Anti−virus is enabled, it actually catches and takes action on the attachment:

```
Thu Sep 18 22:15:34 2014 Info: New SMTP ICID 16493 interface Management
(192.168.0.199) address 65.55.116.95 reverse dns host blu004-omc3s20.hotmail.com
verified yes
Thu Sep 18 22:15:34 2014 Info: ICID 16493 ACCEPT SG UNKNOWNLIST match sbrs
[-1.0:10.0] SBRS 5.5
Thu Sep 18 22:15:34 2014 Info: Start MID 1659 ICID 16493
Thu Sep 18 22:15:34 2014 Info: MID 1659 ICID 16493 From: <joe_user@hotmail.com>
Thu Sep 18 22:15:34 2014 Info: MID 1659 ICID 16493 RID 0 To:
<any.one@mylocal_domain.com>
Thu Sep 18 22:15:34 2014 Info: MID 1659 Message-ID '<BLU437-SMTP2399199FA50FB
5E71863489DB40@phx.gbl>'
Thu Sep 18 22:15:34 2014 Info: MID 1659 Subject 'Daily Update Final'
Thu Sep 18 22:15:34 2014 Info: MID 1659 ready 2355 bytes from
<joe_user@hotmail.com>
Thu Sep 18 22:15:34 2014 Info: MID 1659 matched all recipients for per-recipient
policy DEFAULT in the inbound table
Thu Sep 18 22:15:35 2014 Info: ICID 16493 close
Thu Sep 18 22:15:35 2014 Info: MID 1659 interim verdict using engine:
CASE spam negative
Thu Sep 18 22:15:35 2014 Info: MID 1659 using engine: CASE spam negative
Thu Sep 18 22:15:37 2014 Info: MID 1659 interim AV verdict using Sophos VIRAL
Thu Sep 18 22:15:37 2014 Info: MID 1659 antivirus positive 'EICAR-AV-Test'
Thu Sep 18 22:15:37 2014 Info: Message aborted MID 1659 Dropped by antivirus
Thu Sep 18 22:15:37 2014 Info: Message finished MID 1659 done
```

The Sophos Anti−virus configuration settings on the incoming mail policy are set to ***drop*** for virus infected messages. In this instance, AMP is never reached to scan or take action on the attachment.

This is not always the case. A review of the mail logs and Message IDs (MIDs) might be needed in order to assure that another service OR a content/message filter did not take action against the MID before AMP processing and an action was reached.

Related Information

- ***Cisco Email Security Appliance − End−User Guides***
- ***Technical Support & Documentation − Cisco Systems***

Updated: Nov 14, 2014 Document ID: 118511