ESA X−Headers Removed from Messages to Microsoft Exchange 2013

Document ID: 118900

Contributed by Robert Sherwin, Cisco TAC Engineer.
Apr 03, 2015

Contents

Introduction

This document describes the reason that X−headers and custom X−headers might not appear for email messages that are sent through a Cisco Email Security Appliance (ESA) to a Microsoft Exchange 2013 mail server and how to resolve the issue.

Background Information

On the ESA, Cisco uses and injects X−headers for specific features that are associated to the ESA. These headers are used in order to record the values and outputs of these features.

Here are some examples of X−headers:

X−header	***Feature***	***Value Examples***
X−Ironport−Anti−Spam−Filtered	Anti−Spam	True/False
X−Ironport−Anti−Spam−Result	Anti−Spam	<hashed result>
X−Ironport−AV	Anti−Virus	encoded details pertaining to AV scanning
X−Amp−Result	Advanced Malware	Clean/Malicious/Unscannalbe
X−Amp−Original−Verdict	Advanced Malware	File unknown/Verdict unknown
X−Amp−File−Uploaded	Advanced Malware	True/False
X−IronPort−Outbreak−Status	Virus Outbreak Filtering	$threat_verdict
X−IronPort−Outbreak−Description	Virus Outbreak Filtering	$threat_description

Tip: There are various other X−headers that are used by these and other features. Refer to the ESA End User Guide for additional information.

From the ESA, the primary X−headers of concern are usually the ***X−Ironport−AV*** headers and the ***X−Ironport−Anti−Spam*** headers:

```
X-Ironport-Av: E=Sophos;i="5.11,502,1422939600"; d="scan'208,217";a="54"
X-Ironport-Av: E=Sophos;i="5.11,502,1422921600"; d="scan'208,217";a="408151624"
X-Ironport-Anti-Spam-Result: A0DdCADh5RpV/5RdJa1cgkNDUlwFtDiPCYI0hXcCgUhMAQEBAQE
```

```
 BeQSEGxlyAQsBAnInBIhCpTCpC4xhh3QFgzONL4l1iziJAyKBRQyCHW+BRH8BAQE
X-Ironport-Anti-Spam-Filtered: true
```

These headers are used when spam and false positive messages are submitted directly to Cisco for further review, and they contain the values of the features that are used in order to process the message when originally presented to, or from, the ESA.

Problem

The X−headers do not appear for some email messages that are processed through the ESA to Microsoft Exchange 2013.

In Microsoft Exchange, there is a "Header firewall option that removes specific header fields from inbound and outbound messages." This is observed when the X−headers, as injected from the ESA, are stripped and removed, which results in routing and processing issues on the Cisco Services end.

Here is a description of the issue, as found in the Header firewall section of Microsoft TechNet:

> Header firewall prevents the spoofing of these Exchange−related X−headers by removing them from inbound messages that enter the Exchange organization from untrusted sources. Header firewall prevents the disclosure of these Exchange−related X−headers by removing them from outbound messages sent to untrusted destinations outside the Exchange organization. Header firewall also prevents the spoofing of standard routing headers that are used to track the routing history of a message.

Solution

In order to resolve this issue, Cisco recommends that you review the options and configurations for your Microsoft Exchange 2013 environment in order to ensure that the Header Firewall option is not enabled.

Also, verify that the header information is input correctly. Messages that are processed through an ESA and Microsoft Exchange environment should have raw headers written correctly for each message. Dependent upon the email application that is used by an end−user, there can be various methods used in order to view these headers.

Tip: Refer to the How to Get Email Headers MXToolBox document for additional information.

Related Information

- ***Cisco Email Security Appliance End User Guides***
- ***How do I decode the X−IronPort−AV header on the ESA?***
- ***Technical Support & Documentation − Cisco Systems***

Updated: Apr 03, 2015 Document ID: 118900