Spam Gets by the Cisco Email Security Appliance (ESA) into Your Organization

Contents

Introduction

This document describes five methods that spam emails can enter your organization.

Methods

1. Legitimate Message / Marketing Mail

The legitimate message has been opted in by the user or their name has been sold to another organization. In the first case the user will need to take steps to unsubscribe from the list. If it's the latter, submit the message again to spam@access.ironport.com so antispam definitions can be updated globally, improving the overall spam capture rate of your ESA. Enabling Marketing mail at the Incoming mail policy may help change the perception of this message being "Marketing" over "Spam".

2. The Anti-Spam Is Not Being Updated Correctly

Anti-Spam is disabled or the Feature Key has expired. To check and see if Anti-Spam is updating, go to **GUI > Security Services > IronPort Anti-Spam**. Within this panel you should see updates to the rules sets or engine within the last 6 hours. Also from within this tab at the top you can ensure that the Anti-Spam service is enabled. For review of the Feature Key status you can go to the System Administration tab > Feature Key to check on the status of the Anti-Spam key.

3. Mail Policy or Message Filter

Spam can get into your organization if Anti-Spam security engine is disabled for a specific sender or recipient per a customer Mail Policy. Another way to skip spam filtering is via message filters (CLI: **filters** command).

4. Mail Flow Policy

A message is classified using the ICID of the message. In this situation it's likely that the Anti-

Spam Security feature is turned off, which overrides the Mail Policy. You can determine this by looking at the mail logs, within the logs you will first need to review the ICID to understand which SenderGroup the message was classed into. From there review of the associated Mail Flow Policy. If you have a large amount of entries in your AllowList, you may need to review some of the messages that are getting in to see if they were scanned by the AntiSpam engine. Open the headers of a message and look for the header X-IronPort-Spam, the presence of this header means that the message did go through the engine.

5. Message is Spam

The message is actual spam. You've confirmed the message has been scanned by the antispam engine using the Message Tracking feature (in the message tracking, look for "CASE"). If the case verdict is negative and you deem the message to be spam, submit the original message to spam@access.ironport.com. This could be a case of a new Spam threat just being released or an older threat that was re-engineered.

The processing of the Spam submissions is both an automatic and manual process and there is no feedback for your specific submission. At any point you can contact Cisco TAC and request an evaluation and response.