How do I audit positvely−identified or suspect spam, marketing email for false positives?

Document ID: 118024

Contributed by Robert Sherwin, Cisco TAC Engineers.

Jul 22, 2014

Contents

Introduction
Related Information

Introduction

This document describes how to audit positvely−identified or suspect spam, marketing email for false positives.

How do I audit positvely−identified or suspect spam, marketing email for false positives?

The Cisco IronPort Email Appliance (ESA) provides several options that allow you to store messages and examine for false positive anti−spam verdicts.

In the GUI, ***Mail Policies > Incoming Mail Policies*** or ***Outgoing Mail Policies***, choosing the Anti−Spam settings for the mail policy, you can choose to send positvely−identified spam, suspect spam, or marketing email to an alternate host, or to send the IronPort Spam Quarantine (ISQ).

Using an alternate host address can allow an administrator to review positvely−identified spam, suspect spam, or marketing email and report any false positives.

The ISQ allows both administrators and end recipients to review positvely−identified spam, suspect spam, or marketing email before choosing to delete or release them.

If false positives are detected, please report those to ham@access.ironport.com.

Related Information

- ESA FAQ: How do you report Content Security Anti−Spam false positives or missed spam?