

¿Cómo auditoría el Spam positvely-identificado o sospechado, comercializando el correo electrónico para los falsos positivos?

Contenido

[Introducción](#)

[Información Relacionada](#)

Introducción

Este documento describe cómo auditoría el Spam positvely-identificado o sospechado, comercializando el correo electrónico para los falsos positivos.

¿Cómo auditoría el Spam positvely-identificado o sospechado, comercializando el correo electrónico para los falsos positivos?

El dispositivo del correo electrónico de Cisco IronPort (ESA) proporciona varias opciones que permitan que usted salve los mensajes y que los examine para los veredictos del anti-Spam del falso positivo.

En el GUI, las **directivas del correo > las directivas del correo entrante** o las **directivas salientes del correo**, eligiendo las configuraciones del Anti-Spam para la directiva del correo, usted puede elegir enviar el Spam positvely-identificado, el Spam del sospechoso, o el correo electrónico de comercialización a un host alterno, o enviar la cuarentena del Spam de IronPort (ISQ).

Usando el suplente un host address puede permitir que un administrador revise el Spam positvely-identificado, el Spam del sospechoso, o el correo electrónico del márketing y señale cualquier falso positivo.

El ISQ permite que los administradores y los beneficiarios del extremo revisen el Spam positvely-identificado, el Spam del sospechoso, o el correo electrónico del márketing antes de elegir borrarlos o liberar.

Si se detectan los falsos positivos, señale por favor ésos a ham@access.ironport.com.

Información Relacionada

- [ESA FAQ: ¿Cómo usted señala los falsos positivos contenidos del Anti-Spam de la Seguridad o faltado mandó spam?](#)