

El Spam pasa el dispositivo de seguridad del correo electrónico de Cisco (ESA) en su organización

Contenido

[Introducción](#)

[Métodos](#)

1. [Correo legítimo del mensaje/del márketing](#)
2. [El Anti-Spam no se está poniendo al día correctamente](#)
3. [Filtro de la directiva o del mensaje del correo](#)
4. [Directiva del flujo de correo](#)
5. [El mensaje es Spam](#)

Introducción

Este documento describe cinco métodos que los email del Spam puedan ingresar su organización.

Métodos

1. Correo legítimo del mensaje/del márketing

El mensaje legítimo ha sido optado adentro por el usuario o su nombre se ha vendido a otra organización. En el primer caso el usuario necesitará tomar las medidas para desinscribir de la lista. Si es este último, someta el mensaje otra vez a spam@access.ironport.com así que las definiciones del antispam se pueden poner al día global, mejorando el índice total de la captura del Spam de su ESA. Habilitar el correo del márketing en la directiva del correo entrante puede ayudar a cambiar la opinión de este mensaje “que comercializa” sobre el “Spam”.

2. El Anti-Spam no se está poniendo al día correctamente

Se inhabilita el Anti-Spam o las teclas de función han expirado. Para marcar y ver si el Anti-Spam se está poniendo al día, vaya a los **servicios del > Security (Seguridad) GUI > al Anti-Spam de IronPort**. Dentro del este panel usted debe ver las actualizaciones a los conjuntos de las reglas o el motor dentro del último 6 horas. También dentro de esta lengüeta en el top usted puede asegurarse de que el servicio del Anti-Spam esté habilitado. Para el estudio del estatus de las teclas de función usted puede ir a la lengüeta > a las teclas de función de la administración del sistema a comprobar el estatus de la clave del Anti-Spam.

3. Filtro de la directiva o del mensaje del correo

El Spam puede conseguir en su organización si el motor de la Seguridad del Anti-Spam se inhabilita para un remitente o un beneficiario específico por una directiva del correo del cliente. Otra manera de saltar la filtración del Spam está vía el mensaje filtra (CLI: comando de los **filtros**).

4. Directiva del flujo de correo

Un mensaje se clasifica usando el ICID del mensaje. En esta situación es probable que la función de seguridad del Anti-Spam esté apagada, que reemplaza la directiva del correo. Usted puede determinar esto mirando los registros del correo, dentro de los registros que usted primero necesitará revisar el ICID para entender en qué SenderGroup fue clasificado el mensaje. Allí del estudio de la directiva asociada del flujo de correo. Si usted tiene una gran cantidad de entradas en su lista blanca, usted puede necesitar revisar algunos de los mensajes que están entrando considerar si fueron analizados por el motor de AntiSpam. Abra las encabezados de un mensaje y busque el X-IronPort-Spam de la encabezado, la presencia de esta encabezado significa que el mensaje pasó a través del motor.

5. El mensaje es Spam

El mensaje es Spam real. Usted ha confirmado el mensaje ha sido analizado por el motor del antispam usando Seguimiento de mensajes la característica (en Seguimiento de mensajes, busque el "CASO"). Si el veredicto del caso es negativo y usted juzga el mensaje para ser Spam, presente el mensaje original a spam@access.ironport.com. Éste podría ser un caso de una nueva amenaza del Spam apenas que era liberada o de una más vieja amenaza que fue rediseñada.

El proceso de las presentaciones del Spam es un automático y el Proceso manual y allí no es ningún feedback para su presentación específica. En cualquier momento usted puede entrar en contacto el TAC de Cisco y pedir una evaluación y una respuesta.