Solucionar problemas relacionados con "Detenido por filtrado de reputación de IP"

Contenido

Introducción

Este documento describe una consulta común sobre informes que indican correos electrónicos detenidos por "filtrado de reputación IP".

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Dispositivo Cisco Secure Email

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Dispositivo Cisco Secure Email

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

El filtrado de reputación IP es la primera capa de protección frente a spam que permite controlar los mensajes que pasan a través del gateway de correo electrónico en función de la fiabilidad del remitente, según determine el servicio de reputación IP del remitente. Este artículo trata sobre cómo abordar los problemas relacionados con el filtrado de reputación de IP.

Problema

Al acceder a los informes en el dispositivo ESA/CES navegando hasta Monitor > Correo entrante, ciertos correos electrónicos parecen estar bloqueados por el "filtrado de reputación IP". En algunos casos, el número total de intentos de correo electrónico coincide con los detenidos por el filtrado de reputación de IP, lo que plantea dudas sobre su precisión. Además, puede resultar difícil localizar correos electrónicos específicos que se bloquearon.

Una preocupación común es la incapacidad de generar una lista de correos electrónicos bloqueados por el filtrado de reputación de IP, lo que genera confusión sobre si los correos electrónicos legítimos se filtraron por error.

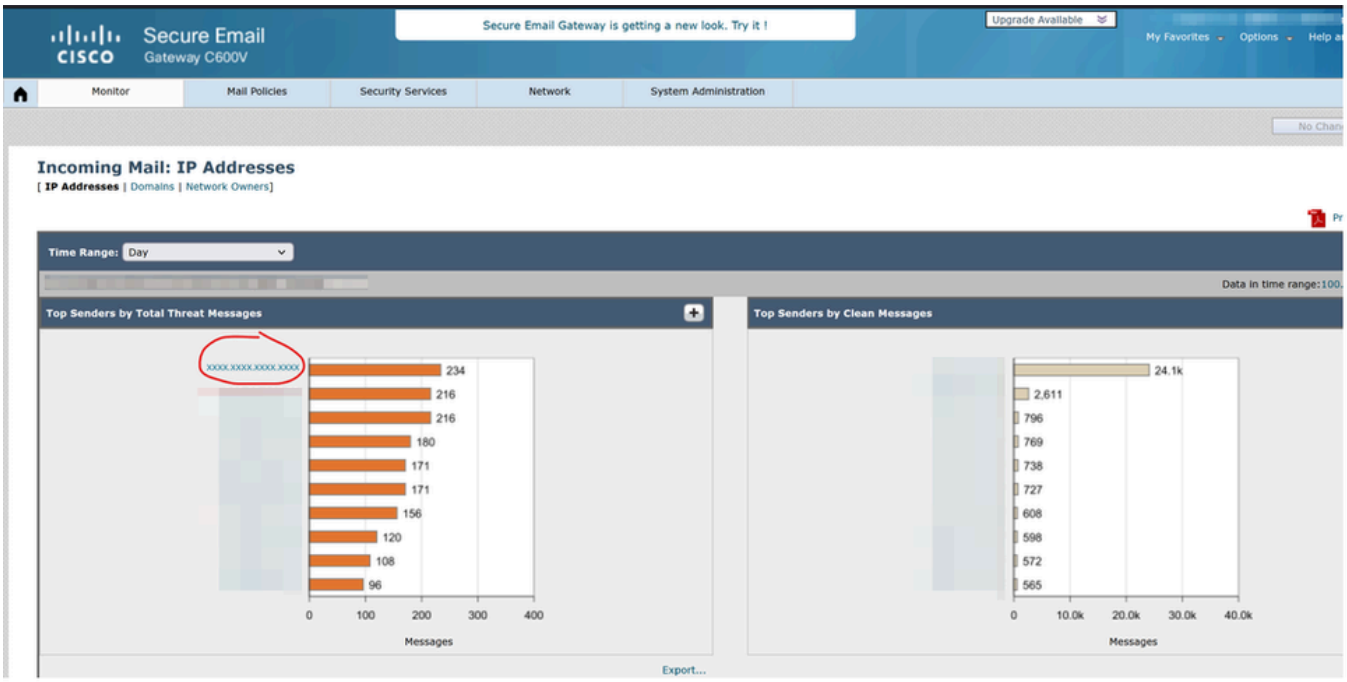
Solución

Funciones de filtrado de reputación de IP similares a las puntuaciones de reputación de Sender Base (SBRS) en dispositivos ESA, mediante un método de cálculo comparable.

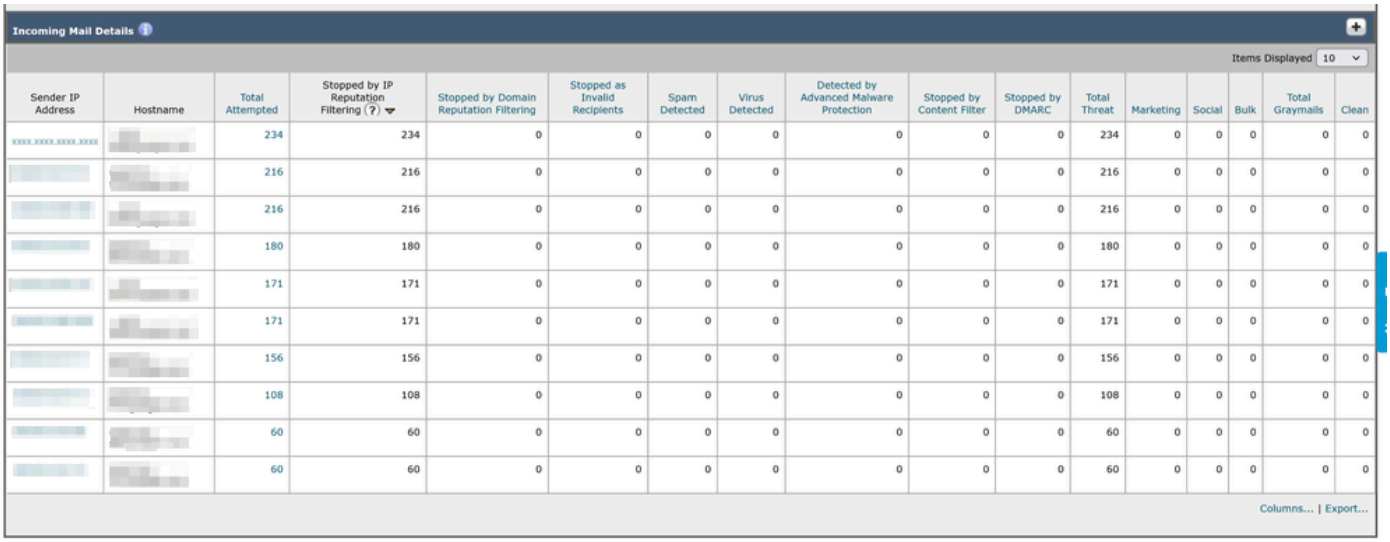
Comprender el filtrado de reputación de IP

El filtrado de reputación de IP de remitente es la primera capa de protección frente a spam, que permite controlar los mensajes que llegan a través del gateway de correo electrónico en función de la fiabilidad de los remitentes determinada por el servicio de reputación de IP de remitente. El Servicio de Reputación IP, utilizando datos globales de la red de afiliados de Talos, asigna una puntuación de reputación IP (IPRS) a los remitentes de correo electrónico en función de las tasas de quejas, las estadísticas de volumen de mensajes y los datos de las listas de bloqueos públicos y las listas de proxy abiertas. La puntuación de reputación de IP ayuda a diferenciar a los remitentes legítimos de las fuentes de spam. Puede determinar el umbral para bloquear mensajes de remitentes con puntuaciones de reputación bajas. Talos intelligence (Talos Intelligence) proporciona una descripción general global de las últimas amenazas basadas en la Web y en el correo electrónico, muestra el volumen actual del tráfico de correo electrónico por país y le permite consultar las puntuaciones de reputación en función de la dirección IP, el URI o el dominio.

El ejemplo explica el funcionamiento del filtrado de reputación de IP:

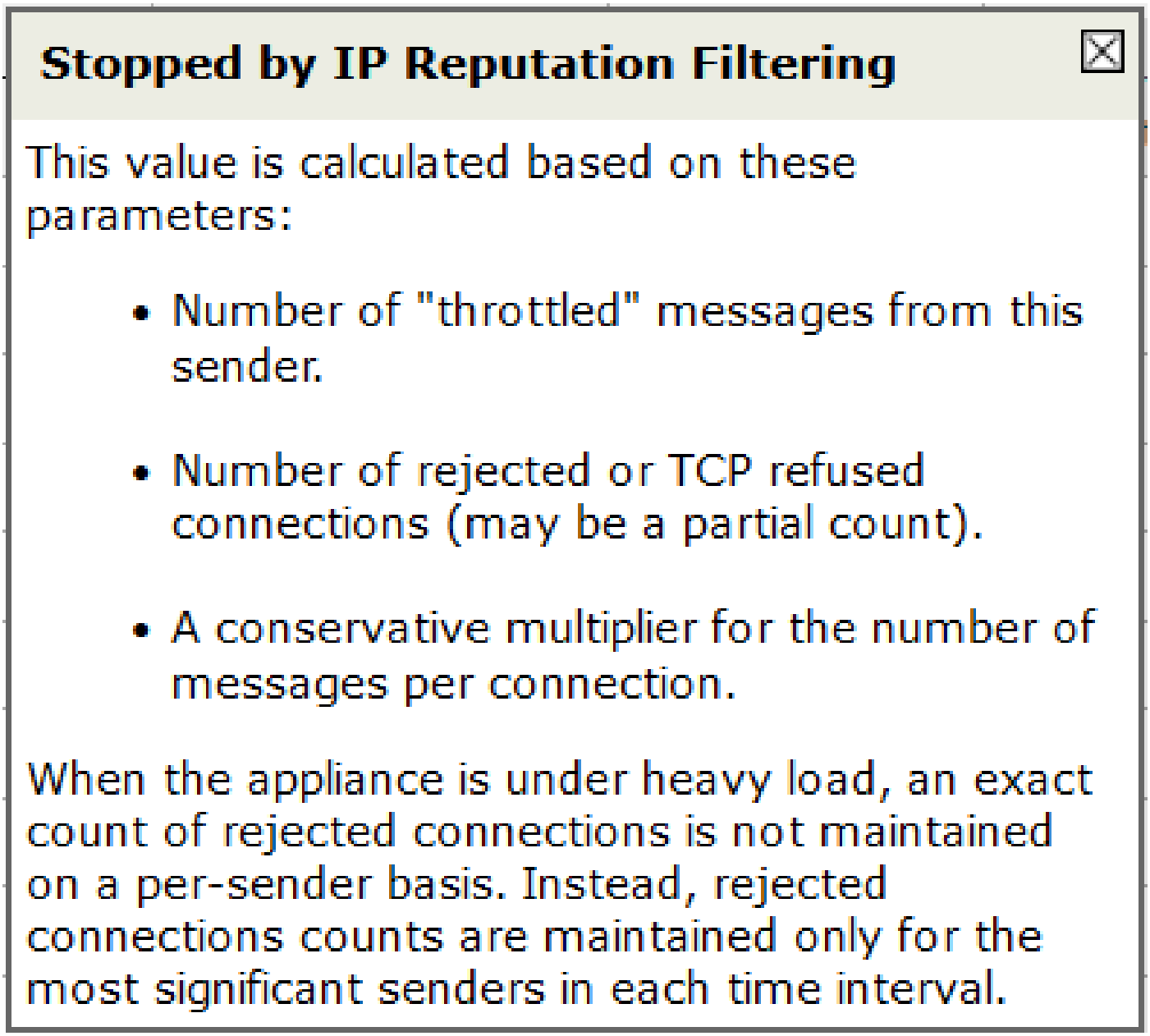


Principales remitentes



Detalles del correo entrante

IP XXXX.XXXX.XXXX.XXXX ha enviado 234 mensajes de correo electrónico, todos los cuales parecen haber sido bloqueados por el filtrado de reputación de IP. Sin embargo, un análisis del rastreo de mensajes y mail_logs dentro del dispositivo muestra que los correos electrónicos de esta IP se entregaron correctamente, sin evidencia de bloqueo por el filtrado de reputación de IP.



Condiciones aplicables al filtrado de reputación de IP

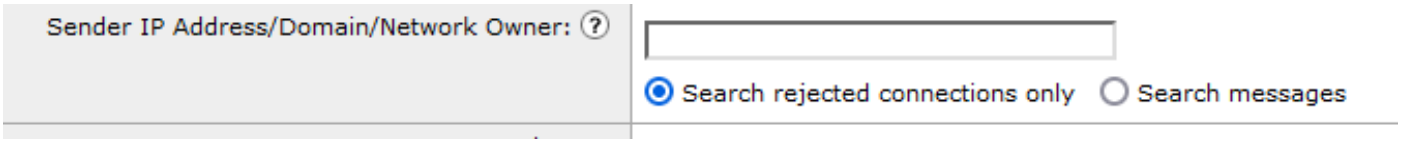
El filtrado de reputación de IP se calcula en función de parámetros específicos, como se muestra en la captura de pantalla mencionada. En algunos casos, los correos electrónicos pueden ajustarse a la tercera condición: un multiplicador conservador para el número de mensajes por conexión. Los registros de rechazo solo son visibles si los correos electrónicos cumplen las dos primeras condiciones. Sin embargo, el dispositivo puede mostrar un número estimado de mensajes basándose en este multiplicador.

El informe puede reflejar un número aproximado de conexiones, algunas de las cuales no pueden llegar realmente al dispositivo. Por ejemplo, se establece una conexión SMTP (protocolo simple de transferencia de correo), pero se descarta más tarde debido a un problema de red. La tercera condición tiene en cuenta estos escenarios, proporcionando un análisis estimado de si la conexión pasó o no la verificación de reputación de IP. Esto no indica necesariamente que todos los mensajes enumerados fueron bloqueados por el filtrado de reputación IP.

Verificar correos electrónicos bloqueados

Para determinar si los mensajes se bloquearon realmente:

- Comprobar grupo de remitentes de lista de bloqueo: Los mensajes bloqueados por el filtrado de reputación IP se clasifican en el grupo de remitentes de la lista de bloqueo.
- Usar rastreo de mensajes: Navegue hasta Opciones avanzadas, ingrese la dirección IP para buscar y seleccione Buscar sólo conexiones rechazadas.



Buscar conexiones rechazadas en rastreo de mensajes

- Revisar registros de correo: Los correos electrónicos bloqueados por el grupo de remitentes de la lista de bloqueo se pueden identificar en mail_logs.
- Rechazo de HAT retrasado: El filtrado de IP se aplica en el nivel de conexión SMTP y la función de rechazo de la tabla de acceso de host retrasado (HAT) en ESA se puede utilizar para comprender la causa.

Información Relacionada

- Preguntas frecuentes sobre rechazo retrasado de HAT
- Guía del usuario de Cisco ESA
- Soporte técnico y descargas de Cisco

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).