Solucionar el error "Categoría no escaneable = Error de mensaje, Motivo no escaneable = Error de archivo: Se superó el límite de tamaño total de los archivos no archivados" en un ESA

Contenido

Introducción

Este documento describe cómo resolver el error "Categoría no escaneable = Error de mensaje, Motivo no escaneable = Error de archivo: Se superó el límite de tamaño total de los archivos no archivados" en un dispositivo de seguridad de correo electrónico (ESA).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- ESA
- Protección frente a malware avanzado (AMP) de Cisco

Componentes Utilizados

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

- ESA AsyncOS 11.1.2-023.
- ESA AsyncOS 12.0.0-419.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

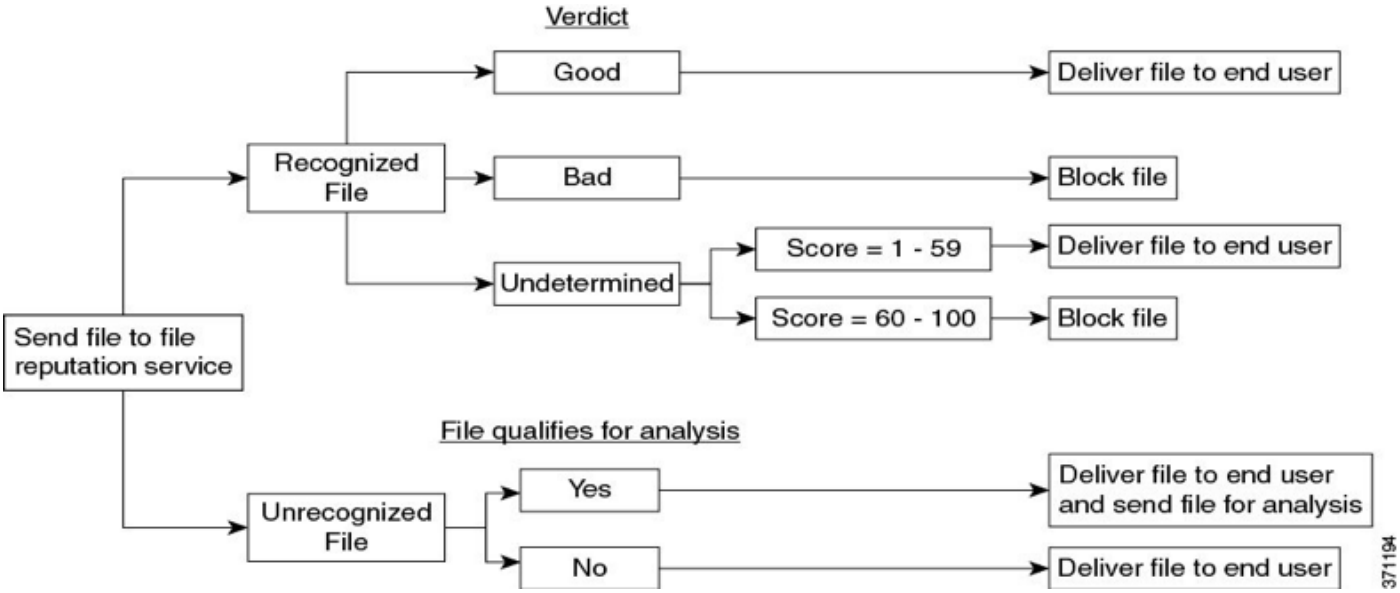
Antecedentes

Cuando un mensaje con datos adjuntos llega a AMP en la canalización, ESA intenta analizar los datos adjuntos del mensaje y comprueba los encabezados de los mensajes (compruebe la conformidad con RFC 2045). Incluso si el mensaje no es totalmente compatible, el ESA sigue haciendo el mejor esfuerzo para analizar el adjunto.

El siguiente paso es verificar si un archivo adjunto es un archivo de almacenamiento y si es así, ESA intenta desempaquetarlo, considera múltiples factores para determinar el tamaño del archivo comprimido para asegurarse de que el archivo adjunto es legítimo y no un archivo zip.

Cuando no se encuentra la reputación de un archivo y este cumple los criterios de análisis, se pone en cuarentena y se carga en el sandbox.

A continuación, el ESA abre una conexión con los servidores de AMP, carga el archivo y espera las actualizaciones del veredicto, como se muestra en la imagen:



ESA proporciona un veredicto basado en estos escenarios:

- Si uno de los archivos extraídos es malicioso, el servicio de reputación de archivos devuelve un veredicto de malicioso para el archivo comprimido o el archivo de almacenamiento.
- Si el archivo comprimido o de archivo comprimido es malicioso y todos los archivos extraídos están limpios, el servicio de reputación de archivos devuelve un veredicto de Malintencionado para el archivo comprimido o de archivo comprimido.
- Si el veredicto de alguno de los archivos extraídos es desconocido, los archivos extraídos se envían opcionalmente (si están configurados y el tipo de archivo es compatible con el análisis de archivos) para su análisis.
- Si el veredicto de alguno de los archivos o archivos adjuntos extraídos es de bajo riesgo, el archivo no se envía para su análisis.
- Si la extracción de un archivo falla cuando se descomprime y, a continuación, se comprime o es un archivo de almacenamiento, el servicio de reputación de archivos devuelve un veredicto de Unscannable para el archivo comprimido o el archivo de almacenamiento. Tenga en cuenta que, en este escenario, si uno de los archivos extraídos es malicioso, el servicio de

reputación de archivos devuelve un veredicto de malicioso para el archivo comprimido o el archivo de almacenamiento (el veredicto malicioso tiene prioridad sobre el veredicto no escaneable).

Los archivos altamente comprimidos como csv, xml y txt pueden exceder el tamaño máximo de archivo codificado en ESA, los algoritmos de compresión, como Lempel-Ziv, generan un mapa digital que cuenta el número y la posición de caracteres dentro del documento completo y esto produce tamaños de archivo muy pequeños.

Por otro lado, los archivos que contienen gráficos, formato de texto como pdf, jpg, png, no se comprimen de la misma manera, por lo que mantienen casi el tamaño del archivo original.

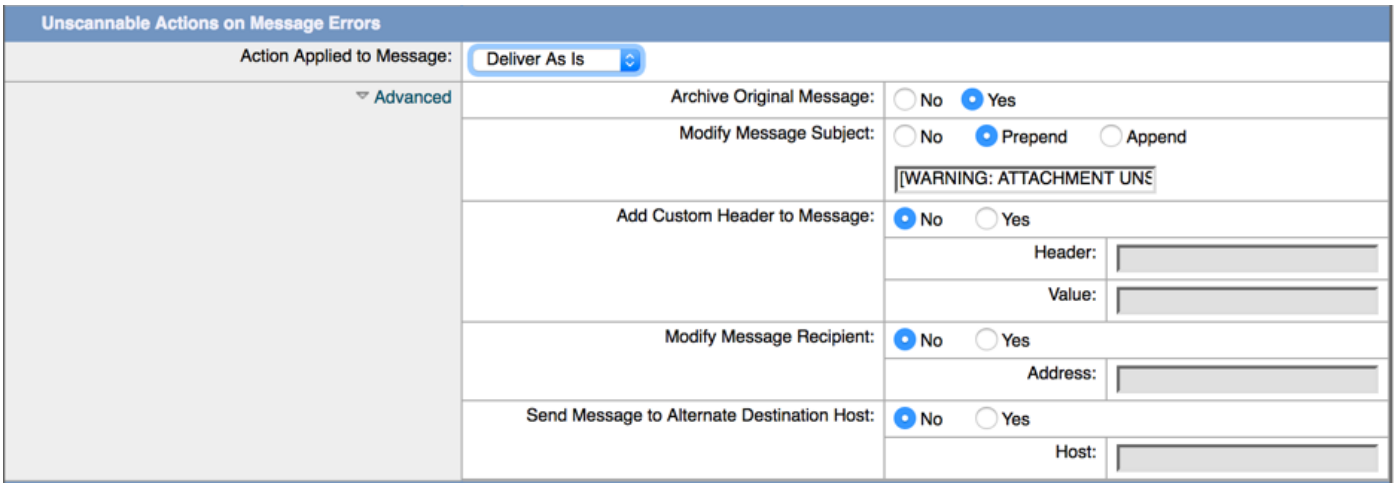
Problema

Cuando el ESA recibe un correo electrónico dentro de un adjunto que está comprimido y esto excede el ratio de compresión máximo y el ESA no puede calcular el tamaño del archivo adjunto, la consecuencia es este registro de errores:

"Mie Feb 13 20:03:47 2019 Info: No se pudo analizar el archivo adjunto. Nombre de archivo = 'ACTS Chopped ISO 88591 encod_NoSchema.XML.zip', MID = 226, SHA256 =7efa6154b7519872055cff10a69067dcad88562f708b284a390a9abcf5e99b8f, Categoría no escaneable = Error de mensaje, Motivo no escaneable = Error de archivo: Se ha superado el límite de tamaño total de los archivos no archivados"

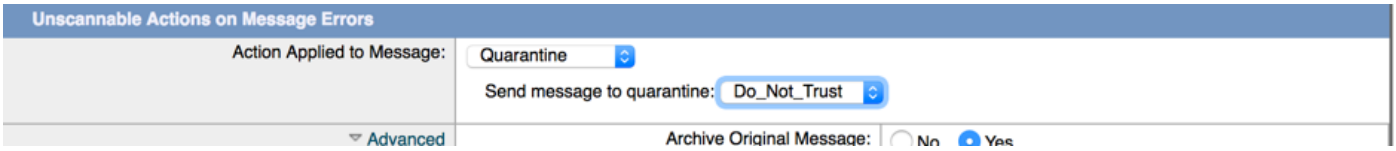
Solución 1

Anteponer los mensajes no escaneables en Asunto para avisar a los usuarios de que los servicios de AMP no han analizado el archivo, como se muestra en la imagen.



Solución 2

Cuarentena no escaneable en cuarentenas de brotes y virus de políticas (PVO) para su posterior análisis. como se muestra en la imagen.



Información Relacionada

- Guía del usuario de AsyncOS 12.0 para los dispositivos Cisco Email Security: GD (implementación general)
- Habilitación de AMP en productos de seguridad de contenido (ESA/WSA)
- Verificar cargas de análisis de archivos en ESA
- Soporte Técnico y Documentación - Cisco Systems

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).