Configuración de ESA para omitir la carga de archivos de tipo MIME desconocidos en el servidor de análisis de archivos

Contenido

Introducción

Este documento describe los pasos para omitir la carga de archivos MIME-Type desconocidos (Application/octet-stream) en File Analysis Server en Cisco ESA.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cómo funciona la protección frente a malware avanzado (AMP) en ESA.
- Conocimiento básico de MIME-types de archivo.

Cisco recomienda que tenga:

- ESA físico o virtual instalado.
- Licencia activada o instalada.
- El asistente de configuración ha finalizado.

- Acceso administrativo a la interfaz de línea de comandos (CLI) de ESA.

Componentes Utilizados

Este documento es aplicable a AsyncOS 15.5.1, 15.0.2 y versiones posteriores.

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.

Tipos de MIME

Un tipo de medio, también denominado tipo de Extensiones multipropósito de correo Internet (MIME), sirve para identificar el carácter y la estructura de un documento, archivo o colección de bytes. Las especificaciones para los tipos MIME se establecen y se unifican en el RFC 6838 del Grupo de trabajo de ingeniería de Internet (IETF, Internet Engineering Task Force).

Los subtipos de "texto" no reconocidos deben tratarse como subtipos "sin formato", siempre y cuando la implementación MIME sepa cómo manejar el juego de caracteres. Los subtipos no reconocidos que también especifican un conjunto de caracteres no reconocido deben tratarse como "application/octet- stream".

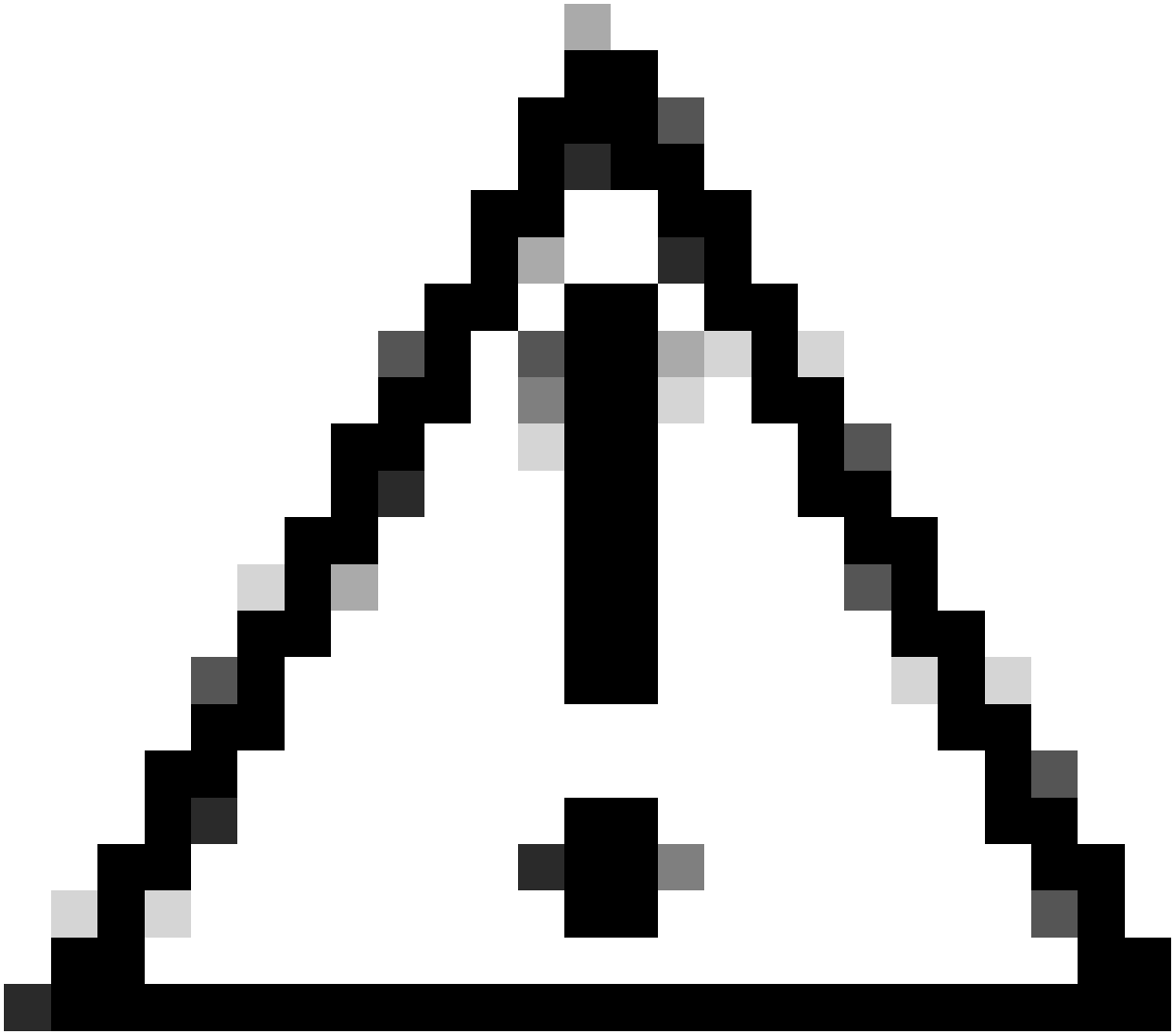
Para obtener más información, consulte RFC 2046 - Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types (Extensiones multipropósito de correo Internet, segunda parte)

El dispositivo ESA superó el límite de carga

Si ha activado el servicio de análisis de archivos y el servicio de reputación no tiene información sobre el archivo, y el archivo cumple los criterios para los archivos que se pueden analizar, el mensaje se puede poner en cuarentena y el archivo se envía para su análisis. Si no ha configurado el dispositivo para poner en cuarentena los mensajes cuando se envían archivos adjuntos para su análisis, o el archivo no se envía para su análisis, el mensaje se envía al usuario.

Para obtener más información, consulte la guía del usuario. Guía del usuario de AsyncOS 15.0 para Cisco Secure Email Gateway - GD (implementación general) - Filtrado de reputación de archivos y análisis de archivos [Cisco Secure Email Gateway] - Cisco

Hemos introducido un nuevo comando CLI para abordar el problema de los dispositivos con cuotas limitadas de envío de archivos que alcanzan prematuramente la capacidad máxima de carga debido a que el ESA envía archivos excesivos para inspección, . Esta mejora se ha implementado a partir de la versión 15.5.1 y también se está incorporando a la versión de mantenimiento (MR) 15.0.2 y versiones posteriores.



Precaución: para mejorar la seguridad, se recomienda encarecidamente cargar todos los archivos como se recomienda. Sin embargo, si considera esencial omitir este paso para tipos de archivo específicos, el comando proporcionado habilita la opción de hacerlo a su discreción. Proceda con cautela, comprendiendo los riesgos potenciales implicados.

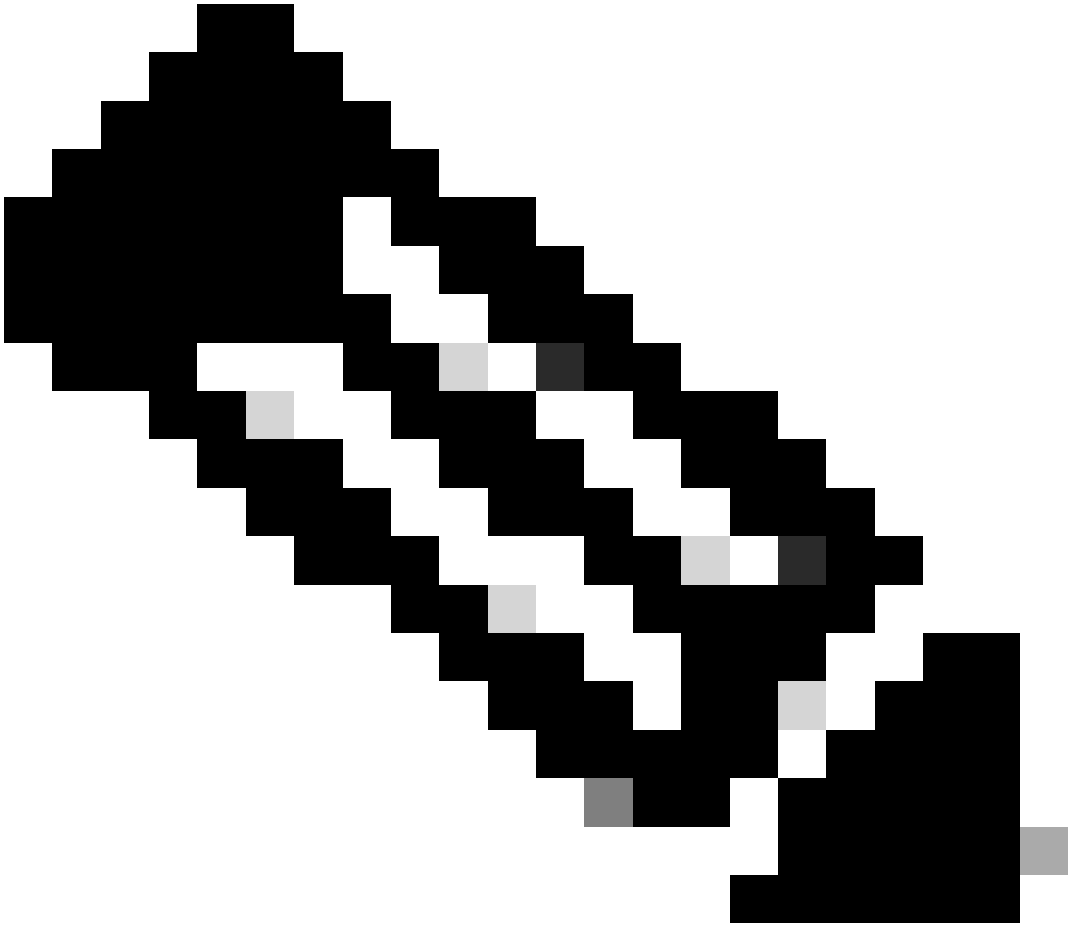
Excluir tipos MIME application/octet-stream para cargarlos en el análisis de archivos

Para excluir los tipos MIME application/octet-stream que se cargarán en el servidor de análisis de archivos para su análisis, siga estos pasos:

Paso 1. Inicie sesión en CLI.

Paso 2. ejecute el comando ampconfig

Paso 3. Escriba unknownmimeoverride y pulse Intro



Nota: unknownmimeoverride es un comando oculto.

Paso 4. Escriba N en respuesta a "¿Desea enviar mime desconocido para análisis sólo si se seleccionan sus extensiones? [N]> "

Paso 5. Pulse Intro para salir del asistente.

Paso 6. Registrar cambios

```
ESA_CLI> ampconfig

File Reputation: Enabled
File Analysis: Enabled
Appliance Group ID/Name: Not part of any group yet


Choose the operation you want to perform:
- SETUP - Configure Advanced-Malware protection service.
- ADVANCED - Set values for AMP parameters (Advanced configuration).
```

```
- SETGROUP - Add this appliance to the group of appliances that can share File Analysis reporting
details.
- CACHESETTINGS - Configure the cache settings for AMP.
[]> unknownmimeoverride

Do you want to send unknown mime for analysis only if their extensions are selected? [Y]> N

ESA_CLI>  commit
```

Defectos y mejoras vinculados

Esta nueva función se introduce debido a estas solicitudes y defectos de funciones:

- El cambio de comportamiento en la carga de archivos HTML y de flujo de octeto en Análisis de archivos confunde a los clientes. ID de bug de Cisco CSCwh61317
- Los archivos p7s se cargan en Análisis de archivos aunque no se haya seleccionado el tipo de archivo. ID de bug de Cisco CSCwh70476

Referencias

Guía del usuario de AsyncOS 15.0 para Cisco Secure Email Gateway - GD (implementación general) - Filtrado de reputación de archivos y análisis de archivos [Cisco Secure Email Gateway] - Cisco

RFC 2046: Extensiones multipropósito de correo de Internet (MIME), segunda parte: tipos de medios

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).