Configure o ESA para ignorar o upload de arquivos do tipo MIME desconhecido para o servidor de análise de arquivos

Contents

Introdução

Este documento descreve as etapas para ignorar o upload de arquivos do tipo MIME desconhecidos (Application/octet-stream) para o File Analysis Server no Cisco ESA.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Como funciona a AMP (Advanced Malware Protection, Proteção avançada contra malware) no ESA.
- Conhecimento básico dos tipos MIME de arquivos.

A Cisco recomenda que você:

- ESA físico ou virtual instalado.
- Licença ativada ou instalada.
- O assistente de instalação foi concluído.

- Acesso administrativo à interface de linha de comando (CLI) do ESA.

Componentes Utilizados

Este documento se aplica ao AsyncOS 15.5.1, 15.0.2 e versões posteriores.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Tipos de MIME

Um tipo de mídia, também conhecido como MIME (Multipurpose Internet Mail Extensions), serve para identificar o caractere e a estrutura de um documento, arquivo ou coleção de bytes. As especificações para os tipos MIME são estabelecidas e uniformes na Internet Engineering Task Force (IETF) RFC 6838.

Subtipos não reconhecidos de "text" devem ser tratados como subtipo "plain", desde que a implementação MIME saiba como lidar com o conjunto de caracteres. Subtipos não reconhecidos que também especificam um conjunto de caracteres não reconhecido devem ser tratados como "aplicação/fluxo de octetos".

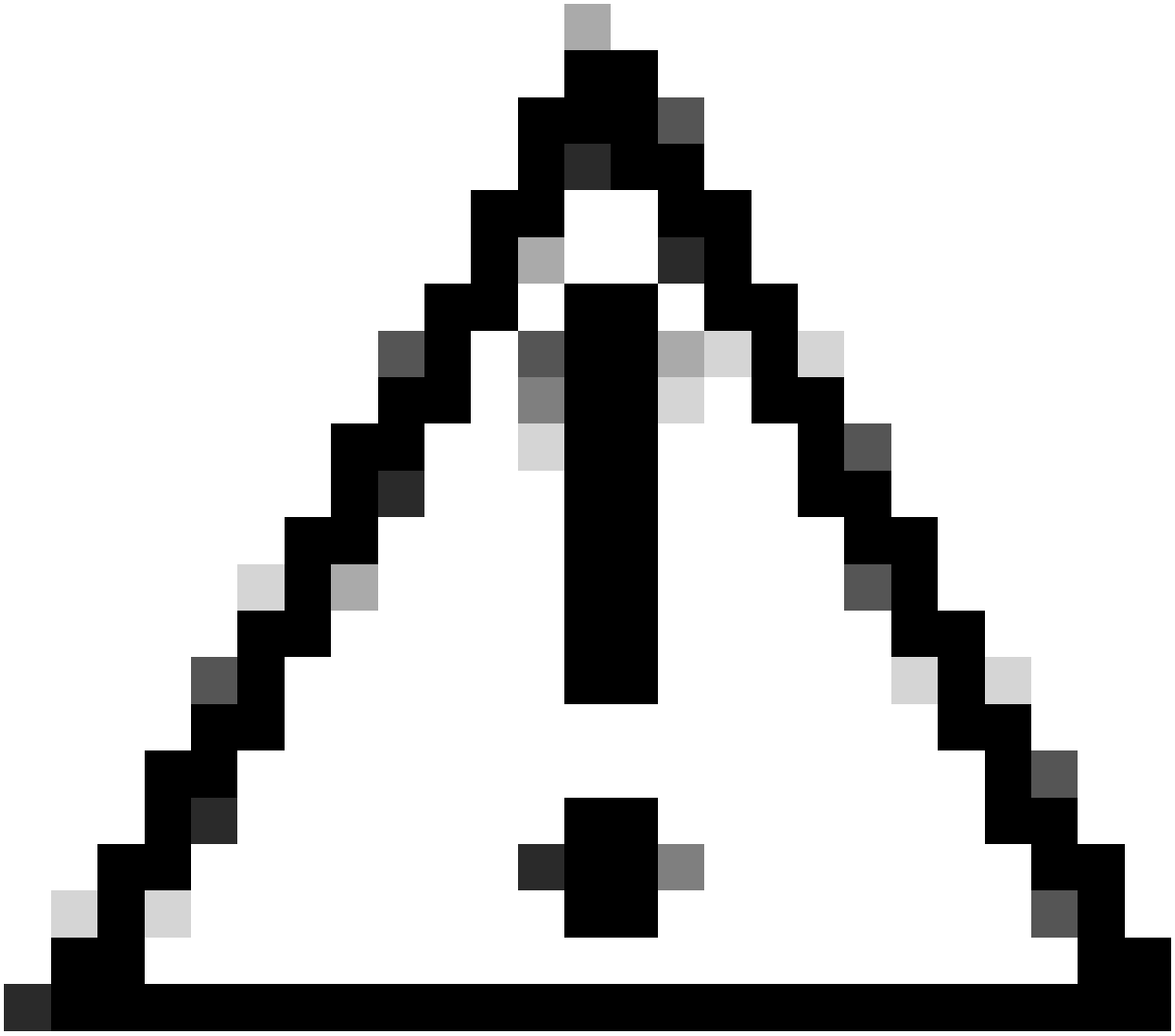
Para obter mais informações, consulte a RFC 2046 - Multipurpose Internet Mail Extensions (MIME) Parte Dois: tipos de mídia

Dispositivo ESA excedeu o limite de carregamento

Se você tiver habilitado o serviço de Análise de arquivo e o serviço de reputação não tiver informações sobre o arquivo, e o arquivo atender aos critérios para arquivos que podem ser analisados, a mensagem poderá ser colocada em quarentena e o arquivo enviado para análise. Se você não tiver configurado o equipamento para colocar mensagens em quarentena quando os anexos forem enviados para análise ou o arquivo não for enviado para análise, a mensagem será liberada para o usuário.

Para obter mais informações, consulte o Guia do usuário. Guia do usuário do AsyncOS 15.0 para Cisco Secure Email Gateway - GD (General Deployment) - Filtragem de reputação de arquivo e análise de arquivo [Cisco Secure Email Gateway] - Cisco

Introduzimos um novo comando CLI para resolver o problema de dispositivos com cotas de envio de arquivos limitadas que atingem prematuramente a capacidade máxima de upload devido ao ESA ter enviado arquivos excessivos para inspeção, . Esse aprimoramento foi implementado a partir da versão 15.5.1 e também está sendo incorporado à versão de manutenção (MR) 15.0.2 e às versões subsequentes.



Cuidado: para aumentar a segurança, recomendamos que todos os arquivos sejam carregados conforme recomendado. No entanto, se você considerar essencial ignorar esta etapa para tipos de arquivos específicos, o comando fornecido permitirá que a opção faça isso a seu critério. Prossiga com cuidado, compreendendo os possíveis riscos envolvidos.

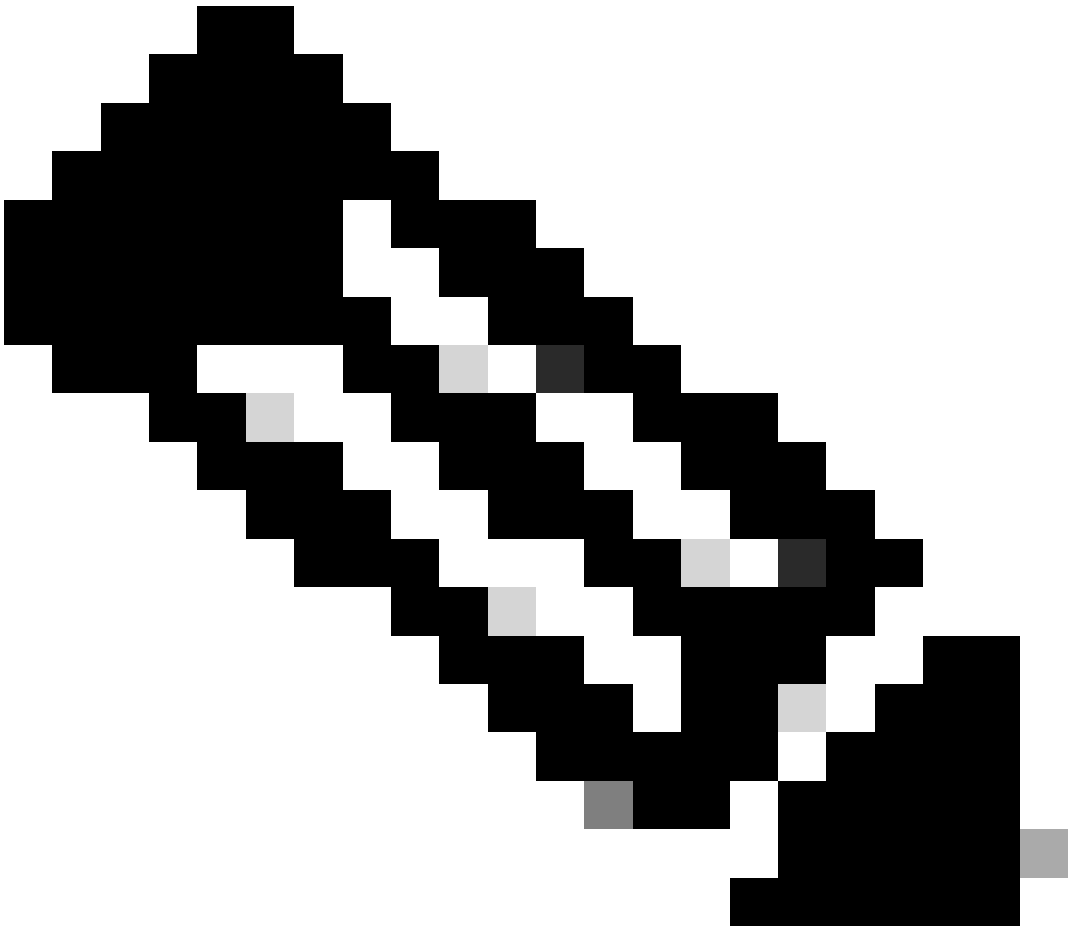
Excluir tipos MIME de aplicativo/fluxo de octetos para carregar na análise de arquivo

Para excluir os tipos MIME de aplicativo/fluxo de octeto para carregar no servidor de análise de arquivo para varredura, use estas etapas:

Etapa 1. Faça login na CLI.

Etapa 2. execute o comando ampconfig

Etapa 3. Digite unknownmimeoverride e pressione enter



Observação: unknownmimeoverride é um comando oculto.

Etapa 4. Digite N em resposta para "Deseja enviar mime desconhecido para análise somente se suas extensões forem selecionadas? [N]>

Etapa 5. Pressione Enter para sair do assistente.

Etapa 6. Confirmar alterações

```
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
```

Defeitos e aprimoramentos vinculados

Este novo recurso é introduzido devido a estas Solicitações e Defeitos de Recurso:

- A alteração de comportamento em arquivos HTML e de fluxo de octetos carregados na análise de arquivos confunde os clientes. ID de bug da Cisco CSCwh61317
- Os arquivos p7s são carregados para a Análise de arquivo mesmo que o tipo de arquivo não esteja selecionado. ID de bug da Cisco CSCwh70476

Referências

Guia do usuário do AsyncOS 15.0 para Cisco Secure Email Gateway - GD (General Deployment) - Filtragem de reputação de arquivo e análise de arquivo [Cisco Secure Email Gateway] - Cisco

RFC 2046 - Multipurpose Internet Mail Extensions (MIME) Parte Dois: tipos de mídia

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.