Configurer ESA pour ignorer le téléchargement de fichiers de type MIME inconnu vers le serveur d'analyse de fichiers

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés

Types MIME

L'appliance ESA a dépassé la limite de téléchargement

Exclure les types MIME d'application/flux d'octets à télécharger dans l'analyse de fichiers

Défauts et améliorations liés

Références

Introduction

Ce document décrit les étapes à suivre pour ignorer le téléchargement de fichiers de type MIME inconnus (Application/flux d'octets) vers le serveur d'analyse de fichiers dans Cisco ESA.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Fonctionnement d'Advanced Malware Protection (AMP) dans ESA.
- Connaissance de base des types MIME de fichiers.

Cisco recommande que vous ayez :

- ESA physique ou virtuel installé.
- Licence activée ou installée.
- L'Assistant de configuration est terminé.

- Accès administratif à l'interface de ligne de commande (CLI) ESA.

Composants utilisés

Ce document s'applique à AsyncOS 15.5.1, 15.0.2 et versions ultérieures.

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 votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Types MIME

Un type de support, également appelé MIME (Multipurpose Internet Mail Extensions), sert à identifier le caractère et la structure d'un document, d'un fichier ou d'une collection d'octets. Les spécifications des types MIME sont établies et uniformisées dans le document RFC 6838 de l'IETF (Internet Engineering Task Force).

Les sous-types non reconnus de « text » doivent être traités comme des sous-types « plain » tant que l'implémentation MIME sait comment gérer le jeu de caractères. Les sous-types non reconnus qui spécifient également un jeu de caractères non reconnu doivent être traités comme « application/octet-stream ».

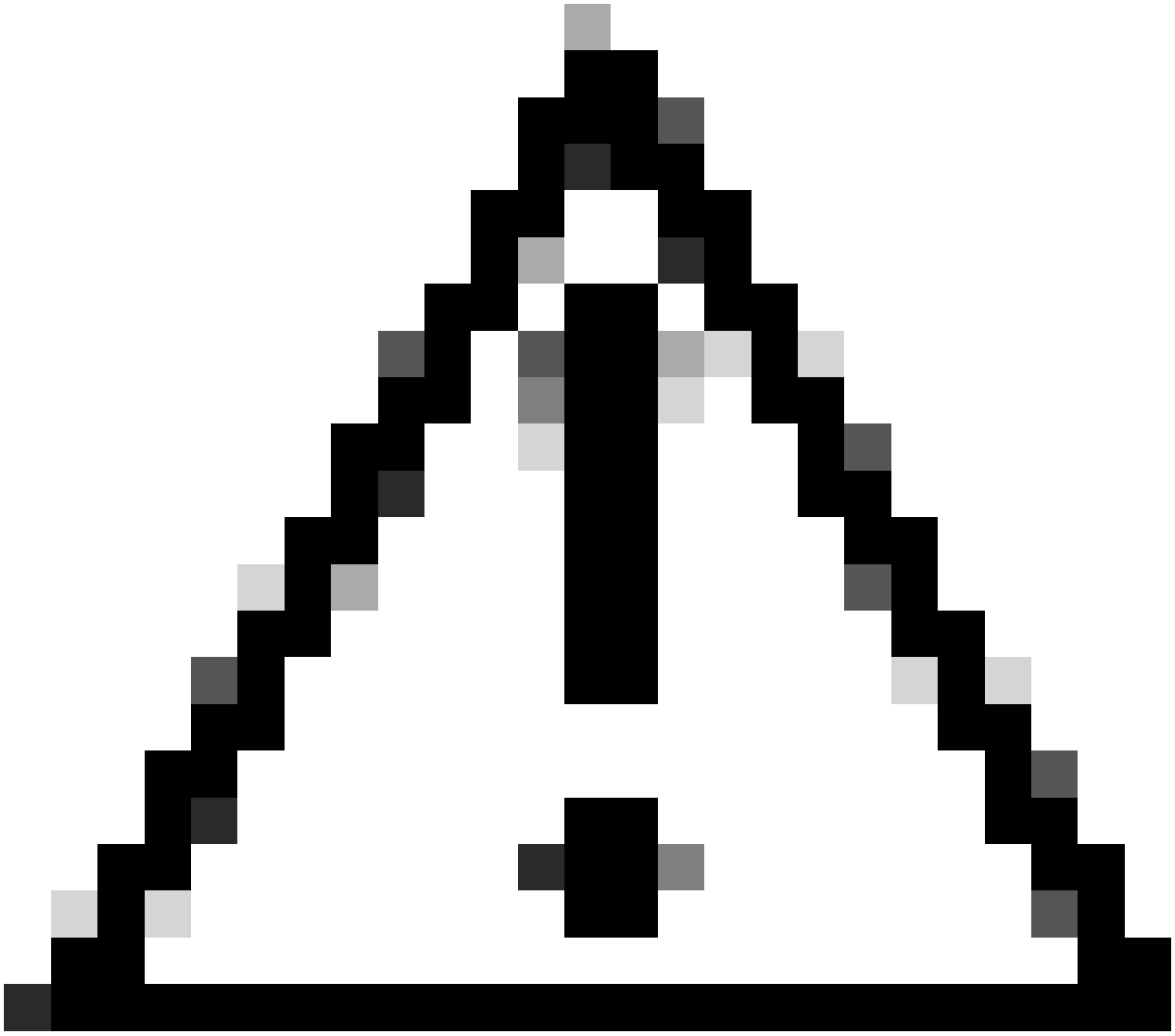
Pour plus d'informations, veuillez vous reporter à RFC 2046 - Multipurpose Internet Mail Extensions (MIME) Part Two : Types de support

L'appliance ESA a dépassé la limite de téléchargement

Si vous avez activé le service d'analyse de fichiers et que le service de réputation ne dispose d'aucune information sur le fichier, et que le fichier répond aux critères des fichiers pouvant être analysés, le message peut être mis en quarantaine et le fichier envoyé pour analyse. Si vous n'avez pas configuré la solution matérielle-logicielle pour mettre en quarantaine les messages lorsque les pièces jointes sont envoyées pour analyse, ou si le fichier n'est pas envoyé pour analyse, le message est alors libéré pour l'utilisateur.

Pour plus d'informations, consultez le Guide de l'utilisateur. Guide de l'utilisateur d'AsyncOS 15.0 pour Cisco Secure Email Gateway - GD (General Deployment) - File Reputation Filtering and File Analysis [Cisco Secure Email Gateway] - Cisco

Nous avons introduit une nouvelle commande CLI pour résoudre le problème des périphériques avec des quotas limités de soumission de fichiers atteignant prématurément la capacité de chargement maximale en raison de l'ESA soumettant des fichiers excessifs pour inspection, . Cette amélioration a été implémentée à partir de la version 15.5.1 et est également incorporée à la version de maintenance 15.0.2 (MR) et aux versions ultérieures.



Mise en garde : Pour une sécurité renforcée, nous vous conseillons vivement de télécharger tous les fichiers comme recommandé. Cependant, si vous jugez essentiel de contourner cette étape pour des types de fichiers spécifiques, la commande fournie permet de le faire à votre discrétion. Veuillez procéder avec prudence et comprendre les risques potentiels.

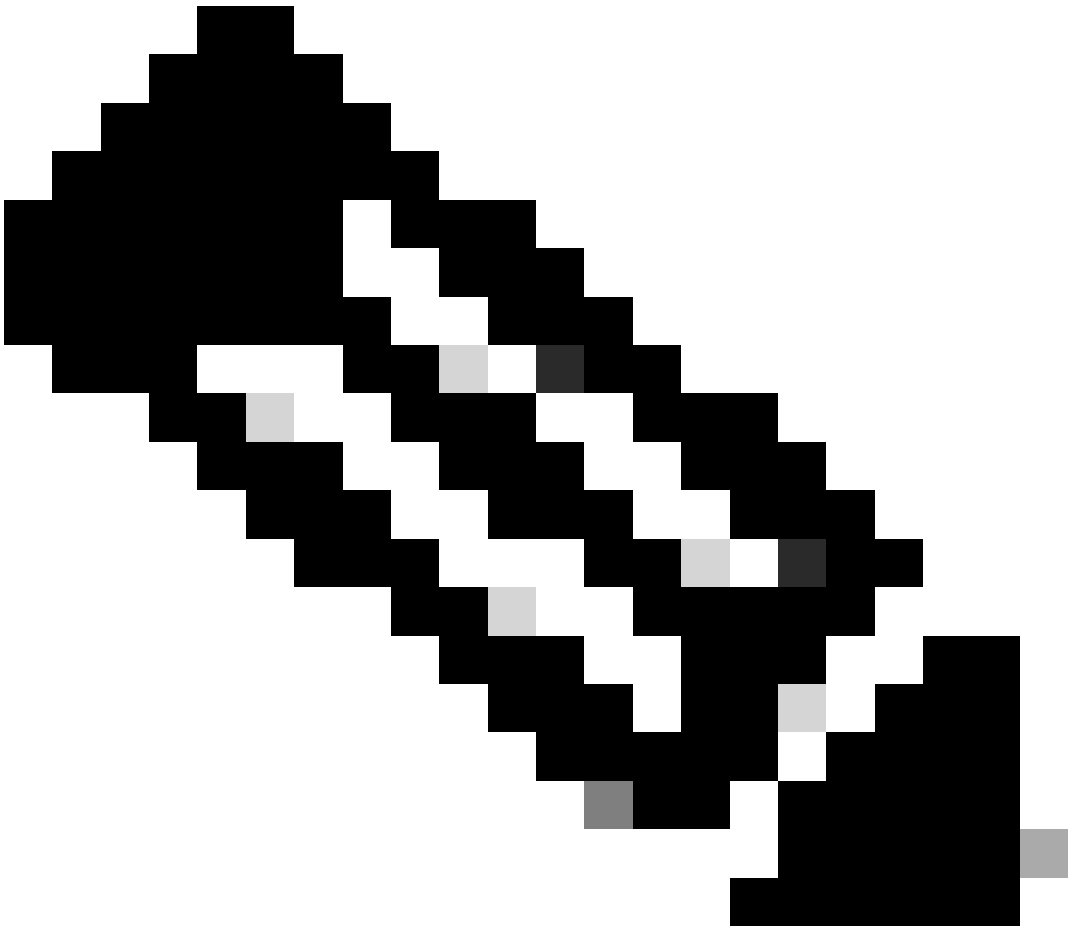
Exclure les types MIME d'application/flux d'octets à télécharger dans l'analyse de fichiers

Pour exclure les types MIME d'application/flux d'octets à télécharger sur le serveur d'analyse de fichiers pour l'analyse, procédez comme suit :

Étape 1. Connectez-vous à l’interface de ligne de commande

Étape 2 : exécutez la commande ampconfig

Étape 3. Tapez unknown imeoverride et appuyez sur Entrée



Remarque : unknownmimeoverride est une commande masquée.

Étape 4. Tapez N en réponse à « Voulez-vous envoyer des MIME inconnus pour analyse uniquement si leurs extensions sont sélectionnées ? [N]> "

Étape 5. Appuyez sur Entrée pour quitter l'assistant.

Étape 6. Valider les modifications

```
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
```

Défauts et améliorations liés

Cette nouvelle fonctionnalité est introduite en raison des requêtes et des défauts suivants :

- Le changement de comportement dans les fichiers HTML et les fichiers de flux d'octets chargés dans l'analyse de fichiers perturbe les clients. ID de bogue Cisco CSCwh61317
- Les fichiers p7s sont téléchargés dans l'analyse de fichier même si le type de fichier n'est pas sélectionné. ID de bogue Cisco CSCwh70476

Références

Guide de l'utilisateur d'AsyncOS 15.0 pour Cisco Secure Email Gateway - GD (General Deployment) - Filtrage par réputation de fichiers et analyse de fichiers [Cisco Secure Email Gateway] - Cisco

RFC 2046 - Multipurpose Internet Mail Extensions (MIME) - Deuxième partie : Types de support

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.