Konfigurieren der ESA zum Überspringen des Uploads von unbekannten MIME-Typdateien auf den Datei-Analyse-Server

Inhalt

Einleitung

In diesem Dokument werden die Schritte zum Überspringen des Uploads von unbekannten MIME-Type-Dateien (Application/Oktett-Stream) auf den File Analysis Server in Cisco ESA beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- So funktioniert Advanced Malware Protection (AMP) in der ESA.
- Grundkenntnisse der Datei-MIME-Typen.

Cisco empfiehlt Folgendes:

- Physische oder virtuelle ESA installiert.
- Lizenz aktiviert oder installiert.
- Der Setup-Assistent ist abgeschlossen.

- Administrator-Zugriff auf die ESA-Befehlszeilenschnittstelle (CLI)

Verwendete Komponenten

Dieses Dokument gilt für AsyncOS 15.5.1, 15.0.2 und höher.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

MIME-Typen

Ein Medientyp, auch als MIME-Typ (Multipurpose Internet Mail Extensions) bezeichnet, dient zur Identifizierung von Zeichen und Struktur eines Dokuments, einer Datei oder einer Sammlung von Bytes. Die Spezifikationen für MIME-Typen werden in der Internet Engineering Task Force (IETF) RFC 6838 festgelegt und vereinheitlicht.

Unbekannte Untertypen von "text" müssen als Untertyp "plain" behandelt werden, solange die MIME-Implementierung weiß, wie sie mit dem Zeichensatz umgeht. Nicht erkannte Untertypen, die auch einen nicht erkannten Zeichensatz angeben, müssen als "application/octet-stream" behandelt werden.

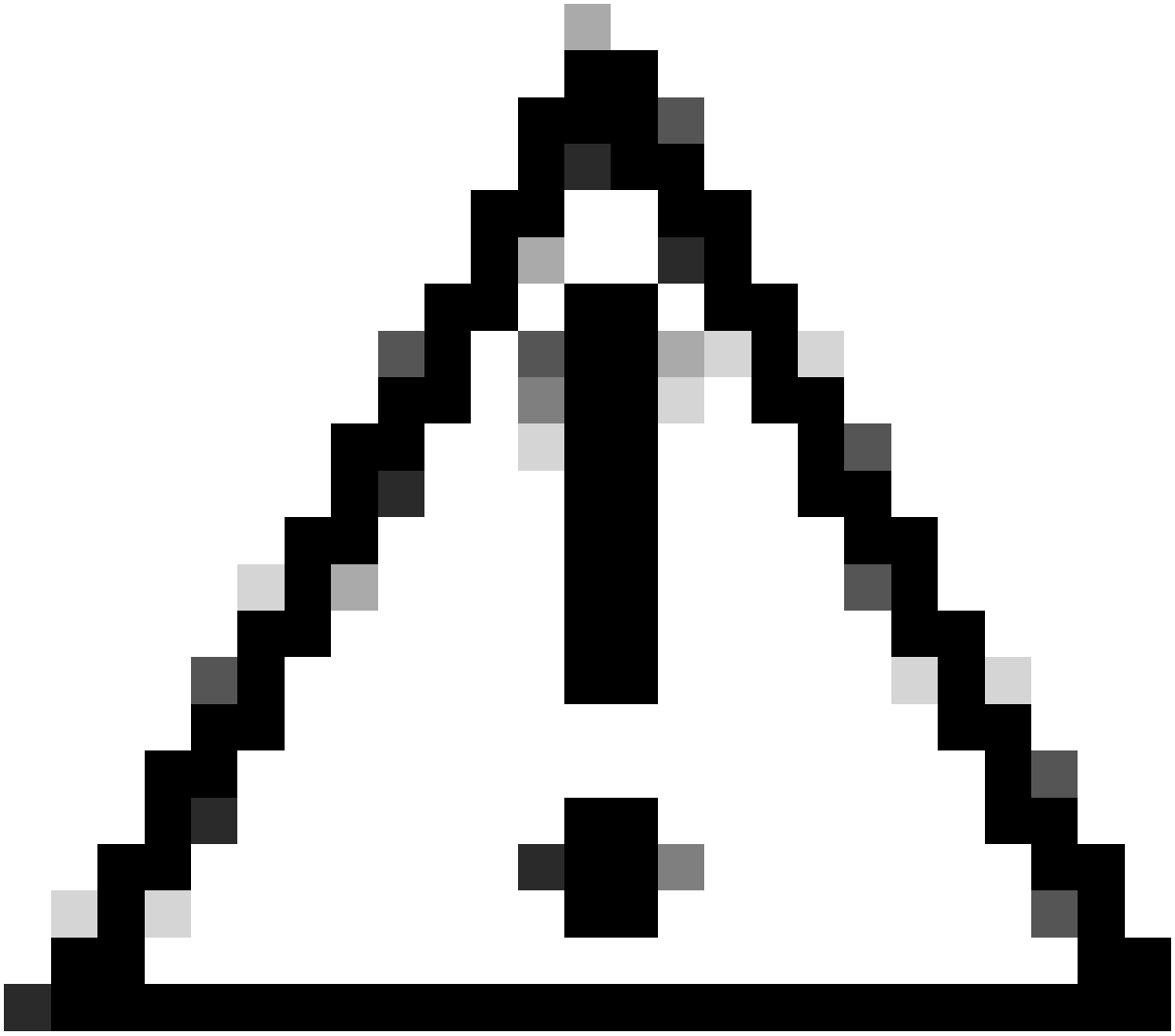
Weitere Informationen finden Sie unter RFC 2046 - Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types

Die ESA-Appliance überschreitet den Upload-Grenzwert

Wenn Sie den Dateianalysedienst aktiviert haben und der Reputationsdienst über keine Informationen zu der Datei verfügt und die Datei die Kriterien für Dateien erfüllt, die analysiert werden können, kann die Nachricht in Quarantäne verschoben und die Datei zur Analyse gesendet werden. Wenn Sie die Appliance nicht so konfiguriert haben, dass sie Nachrichten unter Quarantäne stellt, wenn Anhänge zur Analyse gesendet werden, oder wenn die Datei nicht zur Analyse gesendet wird, wird die Nachricht an den Benutzer freigegeben.

Weitere Informationen finden Sie im Benutzerhandbuch. Benutzerhandbuch für AsyncOS 15.0 für Cisco Secure Email Gateway - GD (Allgemeine Bereitstellung) - Dateireputationsfilterung und Dateianalyse [Cisco Secure Email Gateway] - Cisco

Wir haben einen neuen CLI-Befehl eingeführt, um das Problem von Geräten mit begrenzten Dateiübertragungsquoten zu lösen, die vorzeitig die maximale Upload-Kapazität erreichen, da die ESA zu viele Dateien zur Überprüfung einreicht. Diese Erweiterung wurde ab Version 15.5.1 implementiert und wird auch in die Maintenance Release 15.0.2 und Folgeversionen integriert.



Vorsicht: Zur Erhöhung der Sicherheit wird dringend empfohlen, alle Dateien wie empfohlen hochzuladen. Wenn Sie es jedoch für notwendig erachten, diesen Schritt für bestimmte Dateitypen zu umgehen, aktiviert der angegebene Befehl die Option, dies nach eigenem Ermessen zu tun. Seien Sie vorsichtig, und beachten Sie die potenziellen Risiken.

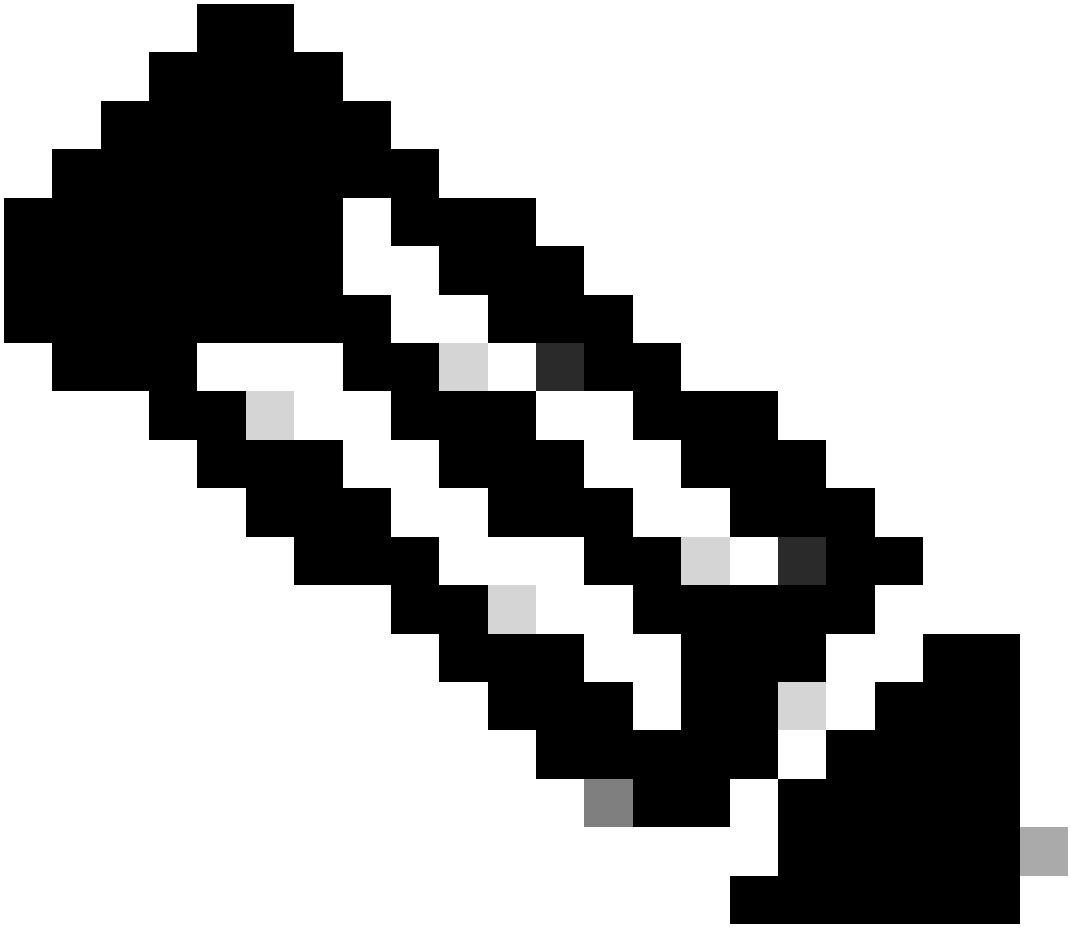
Ausschließen von Anwendungs-/Oktett-Stream-MIME-Typen, die in Dateianalyse hochgeladen werden sollen

So schließen Sie die Anwendungs-/Oktett-Stream-MIME-Typen aus, die zum Scannen auf den Dateianalyseserver hochgeladen werden:

Schritt 1: Melden Sie sich bei CLI an.

Schritt 2: Ausführen des Befehls ampconfig

Schritt 3: Geben Sie unknown mimeoverride ein, und drücken Sie die Eingabetaste.



Hinweis: unknown wnmimeoverride ist ein versteckter Befehl.

Schritt 4: Geben Sie N als Antwort auf "Möchten Sie unbekannte MIME nur dann zur Analyse senden, wenn deren Durchwahlen ausgewählt sind? [N]> "

Schritt 5: Drücken Sie die Eingabetaste, um den Assistenten zu beenden.

Schritt 6: Änderungen bestätigen

```
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
```

Verknüpfte Fehler und Verbesserungen

Diese neue Funktion wird aufgrund der folgenden Funktionsanforderungen und -fehler eingeführt:

- Verhaltensänderungen bei HTML- und Oktett-Stream-Dateien, die in die Dateianalyse hochgeladen werden, verwirren Kunden. Cisco Bug-ID CSCwh61317
- p7s-Dateien werden in die Dateianalyse hochgeladen, auch wenn der Dateityp nicht ausgewählt ist. Cisco Bug-ID CSCwh70476

Referenzen

Benutzerhandbuch für AsyncOS 15.0 für Cisco Secure Email Gateway - GD (Allgemeine Bereitstellung) - Dateireputationsfilterung und Dateianalyse [Cisco Secure Email Gateway] - Cisco

RFC 2046 - Multipurpose Internet Mail Extensions (MIME) Teil 2: Medientypen

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.