Configurare ESA in modo da ignorare il caricamento di file di tipo MIME sconosciuti in File Analysis Server

Sommario

Introduzione

In questo documento viene descritto come ignorare il caricamento di file MIME-Type sconosciuti (Application/ottet-stream) in File Analysis Server in Cisco ESA.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Come funziona Advanced Malware Protection (AMP) in ESA.
- Conoscenze base dei tipi MIME dei file.

Cisco raccomanda:

- ESA fisica o virtuale installata.
- Licenza attivata o installata.
- Installazione guidata completata.

- Accesso amministrativo all'interfaccia della riga di comando (CLI) dell'ESA.

Componenti usati

Questo documento è valido per AsyncOS 15.5.1, 15.0.2 e versioni successive.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Tipi MIME

Un tipo di supporto, noto anche come tipo MIME (Multipurpose Internet Mail Extensions), consente di identificare il carattere e la struttura di un documento, un file o una raccolta di byte. Le specifiche per i tipi MIME sono stabilite e rese uniformi nella RFC 6838 dell'Internet Engineering Task Force (IETF).

I sottotipi non riconosciuti di "text" devono essere trattati come sottotipo "plain" a condizione che l'implementazione MIME sappia come gestire il set di caratteri. I sottotipi non riconosciuti che specificano anche un set di caratteri non riconosciuto devono essere considerati come "application/octet-stream".

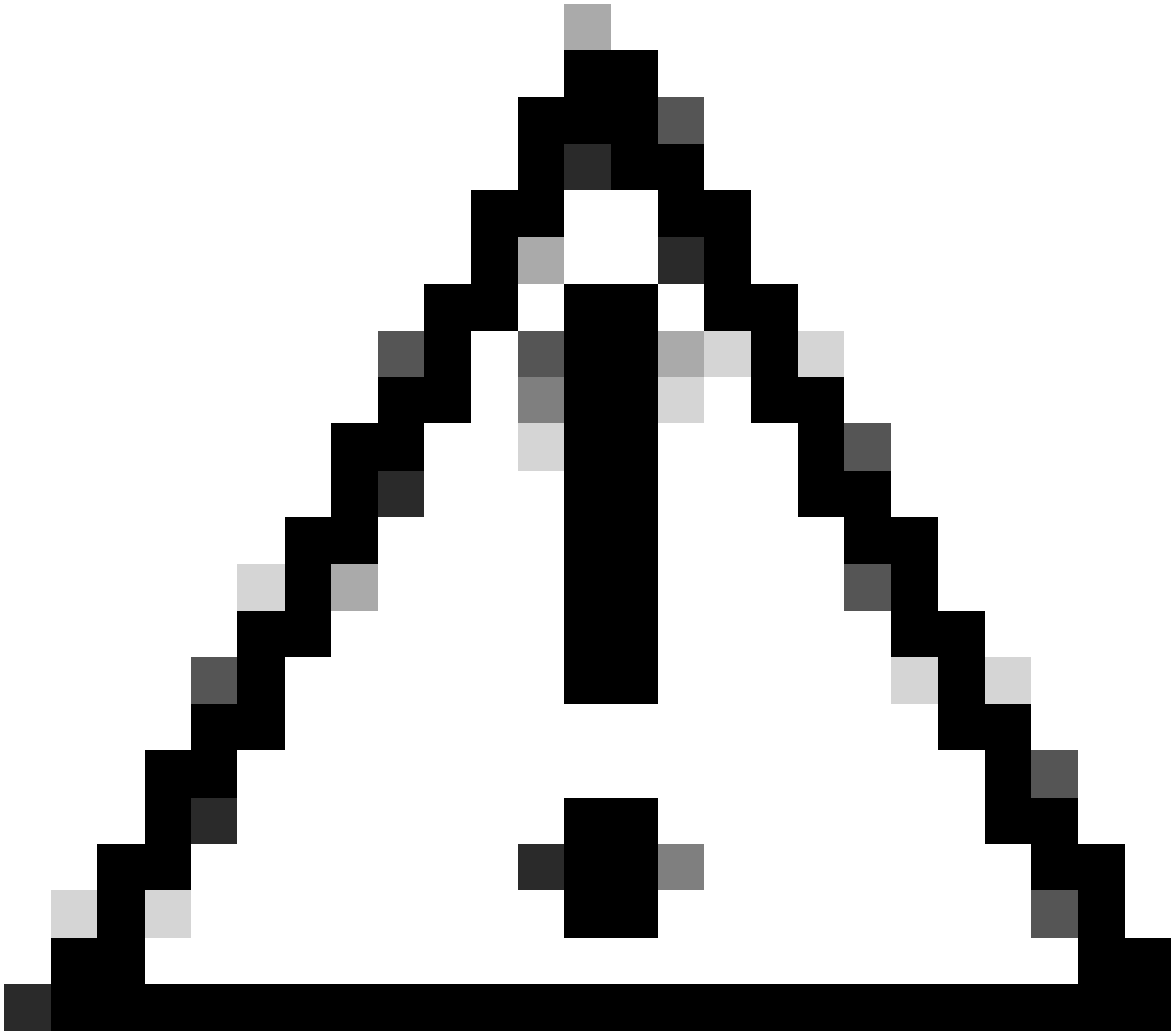
Per ulteriori informazioni, fare riferimento alla RFC 2046 - Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types

L'appliance ESA ha superato il limite di caricamento

Se è stato abilitato il servizio Analisi file e il servizio di reputazione non dispone di informazioni sul file e il file soddisfa i criteri per i file che possono essere analizzati, è possibile mettere in quarantena il messaggio e inviare il file per l'analisi. Se l'accessorio non è stato configurato in modo da mettere in quarantena i messaggi quando gli allegati vengono inviati per l'analisi o se il file non viene inviato per l'analisi, il messaggio verrà rilasciato all'utente.

Per ulteriori informazioni, consultare il Manuale dell'utente. Guida per l'utente di AsyncOS 15.0 per Cisco Secure Email Gateway - GD (General Deployment) - Filtro della reputazione dei file e analisi dei file [Cisco Secure Email Gateway] - Cisco

È stato introdotto un nuovo comando CLI per risolvere il problema dei dispositivi con quote di invio file limitate che raggiungono prematuramente la capacità di caricamento massima a causa dell'invio di file eccessivi da parte dell'ESA per l'ispezione, . Questo miglioramento è stato implementato a partire dalla versione 15.5.1 ed è stato inoltre incorporato nella release di manutenzione 15.0.2 (MR) e nelle versioni successive.



Attenzione: per una maggiore sicurezza, si consiglia di caricare tutti i file come consigliato. Tuttavia, se si ritiene essenziale ignorare questo passaggio per tipi di file specifici, il comando fornito consente di scegliere di eseguire questa operazione a propria discrezione. Procedere con cautela, comprendendo i potenziali rischi coinvolti.

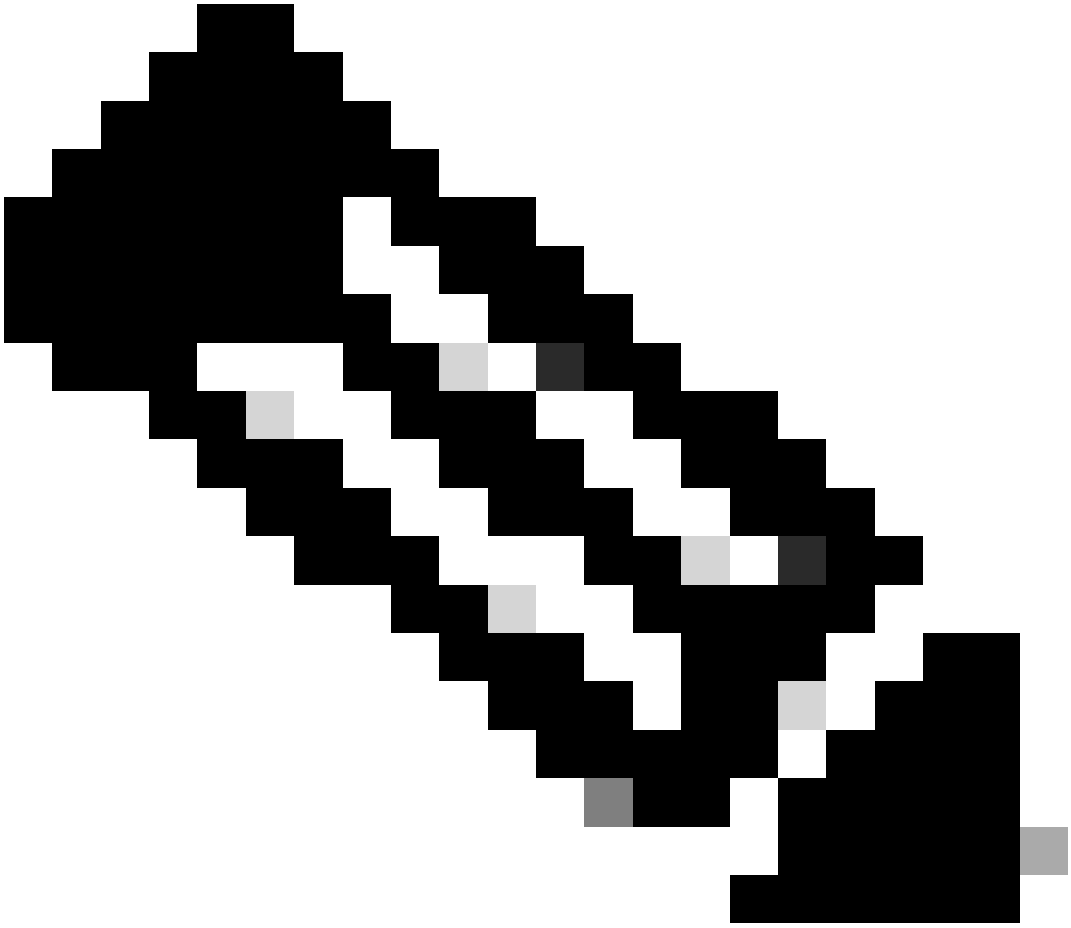
Escludi tipi MIME applicazione/flusso di ottetti da caricare nell'analisi file

Per escludere i tipi MIME application/octet-stream da caricare in File Analysis Server per la scansione, attenersi alla seguente procedura:

Passaggio 1. Accedere alla CLI.

Passaggio 2. eseguire il comando ampconfig

Passaggio 3. Digitare unknown mimeoverride e premere Invio



Nota: unknown nmimeoverride è un comando nascosto.

Passaggio 4. Digitare N in risposta a "Inviare MIME sconosciuto per l'analisi solo se le relative estensioni sono selezionate? [N]> "

Passaggio 5. Premere Invio per uscire dalla procedura guidata.

Passaggio 6. Conferma modifiche

```
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
```

Miglioramenti e difetti collegati

Questa nuova funzione è stata introdotta a causa delle seguenti richieste e difetti:

- Il cambiamento di comportamento nei file HTML e Octet-stream caricati in File Analysis confonde i clienti. ID bug Cisco CSCwh61317
- I file p7s vengono caricati in Analisi file anche se il tipo di file non è selezionato. ID bug Cisco CSCwh70476

Riferimenti

Guida per l'utente di AsyncOS 15.0 per Cisco Secure Email Gateway - GD (General Deployment) - Filtro della reputazione dei file e analisi dei file [Cisco Secure Email Gateway] - Cisco

RFC 2046 - MIME (Multipurpose Internet Mail Extensions) seconda parte: Tipi di supporto

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).