Utilizzo dei filtri messaggi

Sommario

[Introduzione](#)
[Prerequisiti](#)
[Vantaggi dell'utilizzo dei filtri messaggi](#)
[Informazioni correlate](#)

Introduzione

In questo articolo vengono illustrate le best practice e l'implementazione dei filtri messaggi in Email Security Appliance (ESA). I filtri messaggi consentono di creare regole speciali per gestire i messaggi che soddisfano condizioni specifiche nel momento in cui vengono ricevuti ed elaborati dall'ESA.

Prerequisiti

- Conoscenze base del funzionamento dei filtri ESA
- Familiarità con l'interfaccia della riga di comando (CLI) sull'ESA

Vantaggi dell'utilizzo dei filtri messaggi

L'utilizzo di filtri messaggi rispetto a filtri contenuti presenta due vantaggi principali:

1. Vengono applicati ai messaggi verso l'inizio della pipeline di elaborazione della coda di lavoro. Per questo motivo, è possibile risparmiare un numero elevato di risorse filtrando i messaggi prima di utilizzare i principali motori di scansione (ad esempio: Antispam, Antivirus, AMP, Ecc.).
2. Le azioni verranno eseguite sul traffico in entrata e in uscita, mentre per i filtri contenuti sarà necessario crearne uno per il traffico in entrata e uno per quello in uscita.

Inoltre, esistono alcune condizioni che non possono essere configurate utilizzando i filtri contenuti, che possono essere eseguiti solo tramite i filtri messaggi.

Esempio: Se è necessario definire condizioni basate sul gruppo Mittente dell'ESA, tale opzione è disponibile solo nei filtri messaggi.

> **Nota:** Le operazioni filtro messaggi non finali sono cumulative. Se un messaggio corrisponde a più filtri in cui ogni filtro specifica un'azione diversa, tutte le azioni vengono accumulate e applicate. Tuttavia, se un messaggio corrisponde a più filtri che specificano la stessa azione, le azioni precedenti vengono ignorate e viene applicata l'operazione filtro finale.

Operazioni dei filtri messaggi

Quando AsyncOS elabora i filtri messaggi, il contenuto analizzato da AsyncOS, l'ordine di elaborazione e le azioni intraprese si basano su diversi fattori:

- I filtri messaggi vengono elaborati nell'ordine in cui sono configurati (dall'alto in basso, da primo a ultimo)
- Un filtro Messaggio verrà elaborato sul contenuto del messaggio nel momento in cui raggiunge il filtro.
- Quando si confronta un'espressione regolare, si configura un "punteggio" per calcolare il numero di volte in cui una corrispondenza deve verificarsi prima di eseguire un'operazione filtro. Ciò consente di "valutare" le risposte in base a termini diversi.
- Le principali alternative nelle condizioni di collegamento di un filtro messaggi sono: **(AND / OR / IF / ELSE)**

Creazione dei filtri messaggi

```
partha.cisco.com> filters


Choose the operation you want to perform:
- NEW - Create a new filter.
- DELETE - Remove a filter.
- IMPORT - Import a filter script from a file.
- EXPORT - Export filters to a file
- MOVE - Move a filter to a different position.
- SET - Set a filter attribute.
- LIST - List the filters.
- DETAIL - Get detailed information on the filters.
- LOGCONFIG - Configure log subscriptions used by filters.
- ROLLOVERNOW - Roll over a filter log file.
[]>
```

In primo luogo, usare i **filtri** dei comandi dalla CLI per accedere alla modalità di configurazione dei filtri messaggi. Le opzioni sono:

- **NOVITÀ**: Questa opzione consente di iniziare la creazione di un nuovo filtro. La selezione di questa opzione è seguita da Nome filtro e quindi dalla sintassi.
- **ELIMINA**: Questa opzione consente di eliminare un filtro esistente in base alle esigenze. Dopo aver eseguito questo comando, è possibile immettere il nome del filtro del numero di sequenza da eliminare
- **IMPORTA**: È possibile importare un file correlato a un filtro salvato nella directory dell'accessorio.
- **ESPORTA**: Questa opzione consente di esportare il file correlato ai filtri per importarlo in un'altra destinazione
- **SPOSTA**: Questa opzione consente di modificare l'ordine di un filtro in base alle preferenze
- **INSIEME**: Questa opzione consente di modificare lo stato di un filtro da Attivo a Inattivo e viceversa

- **ELENCO**: Questa opzione visualizza tutti i filtri creati presenti nell'ESA
- **DETTAGLI**: Questa opzione consente di visualizzare i componenti del filtro creati, ad esempio le condizioni e le azioni definite.
- **LOGCONFIG**: Questa opzione visualizza i nomi dei file di log creati per i filtri messaggi con azioni definite come archivio (‘nome cartella")
- **ROLLOVER**: Questa opzione consente di eseguire il rollover di tutti i log presenti nelle cartelle create a causa dell'azione di archiviazione definita nei filtri messaggi

I filtri possono essere creati in tutte le modalità ESA, ad esempio in modalità **cluster**, **gruppo** o **macchina**.

I criteri delle preferenze di configurazione in cui l'ESA applicherà i filtri alle e-mail saranno i seguenti:

1ª preferenza: Modalità computer

2 ª preferenza: Modalità gruppo

3ª preferenza: Modalità cluster

Per la creazione dei filtri messaggi, è necessaria una combinazione di sintassi per definire le condizioni e le azioni:

Esempio:

```
if (recv-listener == 'InboundMail' or recv-int == 'notmain')

{

skip-filters();

}

else

{

quarantine(“Policy”);

}

.
```

Il filtro sopra illustrato mostra che se il listener ricevente è 'InboundMail' O se l'interfaccia ricevente è 'notmain', l'azione consisterà nell'ignorare i restanti filtri messaggi.

Se le condizioni non corrispondono, mettere in quarantena il criterio. Questo viene definito dopo else.

Suggerimenti utili

In alcuni casi, la sintassi da utilizzare nei filtri messaggi può risultare poco chiara, ma un punto di riferimento semplice potrebbe essere costituito dai filtri contenuti.

Èpossibile creare un filtro contenuti con le condizioni e le azioni desiderate nel filtro messaggi. Dopo aver inviato il filtro, nella pagina successiva vedremo 3 schede nella parte superiore della sezione filtri:

- Descrizione
- Regole
- Criteri

Quando si fa clic sulla scheda **Regole**, viene visualizzata la sintassi utilizzata dal filtro e lo stesso può essere utilizzato per creare i filtri messaggi. Questo è il modo più semplice per restringere la sintassi delle condizioni di filtro in base ai nostri requisiti.

Espressione regolare utilizzata nei filtri messaggi

- **accento circonflesso (^)**: le regole contenenti il simbolo di accento circonflesso (^) corrispondono solo all'inizio della stringa.

Esempio: **^**Corrisponderò Sono un ingegnere

- **Segno di dollaro ($):** Le regole contenenti il simbolo del dollaro ($) corrispondono solo alla fine della stringa

Esempio: **.com$** corrisponderà a google.com e a yahoo.com

- **Carattere punto (.):** Le regole contenenti un punto (.) corrispondono a qualsiasi carattere, ad eccezione di una nuova riga.

Esempio: L'espressione regolare **^...admin$** corrisponde alla stringa macadmin e alla stringa sunadmin ma non alla stringa win32admin.

- **direttiva asterisco (*):** Le regole contenenti un asterisco (*) corrispondono a "zero o più corrispondenze della direttiva precedente". In particolare, la sequenza di un punto e un asterisco (.*) corrisponde a qualsiasi sequenza di caratteri (non contenente una nuova riga).

Esempio: L'espressione regolare **^P.*Piper$** corrisponde a tutte le stringhe seguenti: Piper, Peter Piper, P.Piper

- **Caratteri speciali barra rovesciata (\)**: Il carattere barra rovesciata *consente di ignorare* i caratteri speciali. Pertanto, la sequenza \. corrisponde solo a un punto letterale, la sequenza \$ corrisponde solo a un simbolo del dollaro letterale e la sequenza \^ corrisponde solo a un simbolo di accento circonflesso letterale.

Esempio: L'espressione regolare **^ik\\.ac\\.uk$** corrisponde solo alla stringa ik.ac.uk

- **Senza distinzione tra maiuscole e minuscole (?i))**: Il token (?i) che indica il resto dell'espressione regolare deve essere trattato in modalità senza distinzione tra maiuscole e minuscole.

Esempio: L'espressione regolare **(?i)cisco** corrisponde a Cisco, CISCO e cisco

- **Oppure (|):** L'operatore "or". Se A e B sono espressioni regolari, l'espressione "A|B" corrisponderà a qualsiasi stringa che corrisponda a "A" o "B".

Esempio: L'espressione **"foo|bar"** corrisponderà a **foo o bar**, ma non a foobar.

Informazioni correlate

Cisco Email Security Appliance - Guide per l'utente