

Gibt es eine Filterbedingung, die mit der Dateigröße einzelner Anlagen anstatt der Nachrichtengröße übereinstimmt?

Inhalt

[Einführung](#)

[Gibt es eine Filterbedingung, die mit der Dateigröße einzelner Anlagen anstatt der Nachrichtengröße übereinstimmt?](#)

[Zugehörige Informationen](#)

Einführung

In diesem Dokument wird eine Lösung beschrieben, die der Dateigröße von Anhängen in einer Filterbedingung zugeordnet werden kann.

Gibt es eine Filterbedingung, die mit der Dateigröße einzelner Anlagen anstatt der Nachrichtengröße übereinstimmt?

Auf der Cisco E-Mail Security Appliance (ESA) gibt es keine Option in Nachrichtenfiltern oder Content-Filtern, die der Dateigröße von Anhängen in einer Filterbedingung entsprechen kann. Die einzige Größenbedingung ist die *Nachrichtengröße*, wobei die Größe der gesamten Nachricht berücksichtigt wird.

Die Lösung besteht in der Verwendung der *\$filesize* Action Variable, die eine kommagetrennte Liste der Dateigröße aller Anhänge enthält, die in einer Nachricht enthalten sind. Wenn der Nachricht ein X-Header mit dem Wert *\$filesize* hinzugefügt wird, kann ein Regular Expression (RegEx) so konstruiert werden, dass er übereinstimmt, wenn eine der enthaltenen Zahlen (Dateigrößen) einen bestimmten Wert überschreitet.

Im folgenden Beispiel wird die Einrichtung eines Inhaltsfilters veranschaulicht, der eine Nachricht verwirft, wenn die Größe der Anlagen 10.000 Byte oder mehr beträgt:

1. Erstellen Sie einen Content-Filter, um den Wert der Aktionsvariable "\$filesize" in einem X-Header hinzuzufügen:

Content Filter Settings	
Name:	AddFileSizeHeader
Currently Used by Policies:	No policies currently use this rule.
Description:	Adds X-fileSizes header to messages containing a comma separated list of attachment file sizes using \$filesizes action variable
Order:	1 (of 9)

Conditions
Add Condition...
There are no conditions, so actions will always apply.

Actions			
Add Action...			
Order	Action	Rule	Delete
1	Add Header	insert-header("X-fileSizes", "\$filesizes")	

2. Erstellen Sie einen weiteren Content-Filter, der den Dateigrößen im neuen X-Header entspricht, und löschen Sie die Nachricht, wenn eine der Dateien 10.000 Byte oder mehr entspricht:

Content Filter Settings	
Name:	DropOnBigAttachments
Currently Used by Policies:	No policies currently use this rule.
Description:	Drops messages when one or more attachments equals or exceeds a size of 10000 bytes
Order:	2 (of 9)

Conditions			
Add Condition...			
Order	Condition	Rule	Delete
1	Other Header	header("X-fileSizes") == "[1-9][0-9]{4,}"	

Actions			
Add Action...			
Order	Action	Rule	Delete
1	Strip Header	strip-header("X-fileSizes")	
Final	Drop (Final Action)	drop()	

3. Aktivieren Sie die beiden neuen Content-Filter für alle relevanten Mail-Policys in der oben angegebenen Reihenfolge.

Hinweis: Die Aktionsvariable "\$filesize" ist die Anzahl der Bytes der Anlage. Dies hängt nicht von der *Nachrichtengrößenbedingung* ab. Auch "[1-9][0-9]{4,}" ist ein regulärer Ausdruck, der auf einer beliebigen Zahl ab 10.000 übereinstimmt. Wenn eine weitere Beschränkung erforderlich ist, sollte der Ausdruck entsprechend geändert werden. Beispiel:

Größe => 20000: [2-9][0-9]{4,}
 Größe => 25000: (2[5-9][0-9]{3}|[3-9][0-9]{4,})

Zugehörige Informationen

- [AsyncOS E-Mail-Benutzerhandbuch](#)
- [Kontaktdaten des GLO-Supports](#)
- [Technischer Support und Dokumentation - Cisco Systems](#)