ESA contentfilters voor e-mailberichten met meerdere Attachments

Inhoud

Inleiding

Dit document beschrijft hoe de negatieve beeldfilteromstandigheden werken voor e-mailberichten die meerdere bijlagen bevatten op de Cisco e-mail security applicatie (ESA).

Probleem

U gebruikt een contentfilter dat bepaalde soorten bijlagen bij e-mail toestaat, terwijl andere soorten bijlagen voor quarantaine moeten worden gemarkeerd. Als er een e-mailbericht arriveert met meerdere bijlagen, een bericht dat moet worden toegestaan en een bericht dat voor quarantaine moet worden gemarkeerd, identificeert het filter het gehele bericht zoals *toegestaan.*

Hier is het inhoudsfilter dat wordt gebruikt:

```
if attachment filename != (list of attachments), then quarantine
```

Deze voorwaarde en actie werken zoals bedoeld als het e-mailbericht één bijlage heeft, maar niet goed werkt voor berichten met meerdere, verschillende bijlagen.

Bijvoorbeeld scenario

Dit zijn de toegestane typen bijlagen:

- raster
- pdf
- jpg

Alle andere toebehoren moeten naar quarantaine worden gestuurd, zoals aangegeven door de filterconditie en de werking.

Filterconditionering

Hier is de filtermodus die wordt gebruikt:

```
if attachment filename != (rar|pdf|jpg)
```

Filteractie

Hier wordt het filter gebruikt:

```
quarantine
```

De verwachting is doorgaans dat als het e-mailbericht een **pdf-**bijlage en een tekstbijlage bevat, het in quarantaine moet worden geplaatst vanwege de tekst-bijlage omdat het niet in de lijst met toegestane bijlagen staat. Dit contentfilter werkt echter niet zoals bedoeld, omdat het overeenkomt met de **pdf-**bijlage in het bericht en deze rechtstreeks toestaat, ook al heeft het een **tekstbijlage**.

Oplossing

Om deze redenen kan het e-mailadres niet in quarantaine worden geplaatst met de **tekst** bijschrift:

- De koppelingsvoorwaarden zijn voor **alle** bijlagen die in een bericht zijn opgenomen.
- De negatieve vergelijking verifieert of **een** van de bijlagen overeenkomt.

Zoals beschreven, als **een** van de bijlagen is toegestaan, zoals wanneer deze overeenkomen met de **bijlage!=**, dan wordt het gehele bericht *toegestaan*. Er is geen manier om dit te doen; het is gewoon de manier waarop deze voorwaarden werken .

De enige andere oplossing is om de logica om te keren en specifieke bijlagen te blokkeren, niet alleen elke bijlage die niet op de witte lijst staat.