

Hoe vat en blokkeer ik ingesloten hyperlinks die uitvoerbaar zijn?

Inhoud

[vraag](#)

[Antwoord](#)

vraag

Hoe vat en blokkeer ik ingesloten hyperlinks die uitvoerbaar zijn?

Antwoord

U kunt een berichtfilter gebruiken om het lichaam en alle HTML-bijlagen te scannen. Deze e-mails worden meestal verzonden naar HTML-e-mails. Om de scanmachine te kunnen detecteren, dient u de toestand van het lichaam te gebruiken. Als je alleen uitgaande mail verwerkt, dan kan je 'only-body-Bevat' conditie gebruiken.

Het volgende berichtfilter zal op elke lengte hyperlink zoeken die met een uitvoerbaar document eindigt. Wanneer aan de voorwaarde is voldaan, zullen twee acties in werking treden. De eerste actie is om de lokale beheerder op de hoogte te stellen door een e-mail naar `admin@example.com` te verzenden.

Het tweede is een laatste handeling waarmee je de e-mail stopt. De e-mail hoeft niet te worden gestopt, maar kan in plaats daarvan in quarantaine worden geplaatst. Het verwijderen van de actie hieronder van `'drop();'` kan worden vervangen door `'quarantaine('beleid');'`.

De quarantaine moet worden vastgesteld, anders zal de filtermachine het filter niet toelaten. U kunt de standaardquarantaine gebruiken, of uw eigen quarantaine maken (raadpleeg de quarantaine in de handleiding om quarantaine te maken of te verwijderen).

```
Block_exe_urls: if body-contains("://\\S*\\.exe(\\s|\\b|$)")
{
  notify ("admin@example.com");
  drop();
}
```

U kunt ook deze versie gebruiken die de slechte URL's uit het lichaam heeft verwijderd en deze door URL REMOVED heeft vervangen.

```
remove_exe_urls: if body-contains("://\\S*\\.exe(\\s|\\b|$)")
{
edit-body-text("://\\S*\\.exe(\\s|\\b|$)", "URL REMOVED");
}
```

Voor gedetailleerdere instructies hoe u een berichtfilter moet invoeren, raadpleegt u [Hoe u een nieuw berichtfilter aan mijn Cisco IronPort-applicatie toevoegt?](#)

Raadpleeg de sectie Cisco ESA AsyncOS GEAVANCEERDE GEBRUIKERSHANDLEIDING voor e-mail security applicaties genaamd Beleidshandhaving om berichtfilters te bekijken.