Hoe wordt de gezondheidstoestand van de SPF beoordeeld met het gebruik van inhoudfilters?

Inhoud

Inleiding

In dit document wordt uitgelegd hoe de filtervoorwaarde van het verificatiefilter van het Sender Policy Framework (SPF) momenteel wordt geëvalueerd.

Het aangegeven werk is alleen van toepassing op alle momenteel ondersteunde Async OS-versies (10.x en hoger).

SPF-verificatie contentfilterconditionering

SPF is een eenvoudig e-mailvalideringssysteem dat bedoeld is om e-mailspoofing te detecteren door middel van een mechanisme dat ontvangende mail-uitwisselaars toestaat om te controleren of inkomende e-mail vanuit een domein wordt verzonden vanuit een host die door de beheerders van dat domein is geautoriseerd.

Op de Cisco Email Security Appliance (ESA) is SPF ingeschakeld voor inkomende berichten in een Mail Flow-beleid. Er kan een contentfilter worden gemaakt om actie te ondernemen tegen het verkregen SPF-vonnis, dat in quarantaine wordt geplaatst of de berichten op basis van de vereiste laat vallen.

Conditions

Add Condition...

Order	Condition	Rule
1	SPF Verification	spf-status == "fail"

Actions

Add Action...

Order	Action	Rule
1	Quarantine	quarantine("Policy")

De post logbestanden of het bericht volgen toont deze details:

```
Sat Feb 20 17:27:37 2021 Info: MID 6153849 SPF: helo identity postmaster@example None
Sat Feb 20 17:27:37 2021 Info: MID 6153849 SPF: mailfrom identity
user@example.com Fail (v=spf1)
Sat Feb 20 17:28:15 2021 Info: MID 6153849 SPF: pra identity user@example.com
None headers from Sat Feb 20 17:28:15 2009 Info: MID 6153849 ready 197 bytes
from <user@example.com>
```

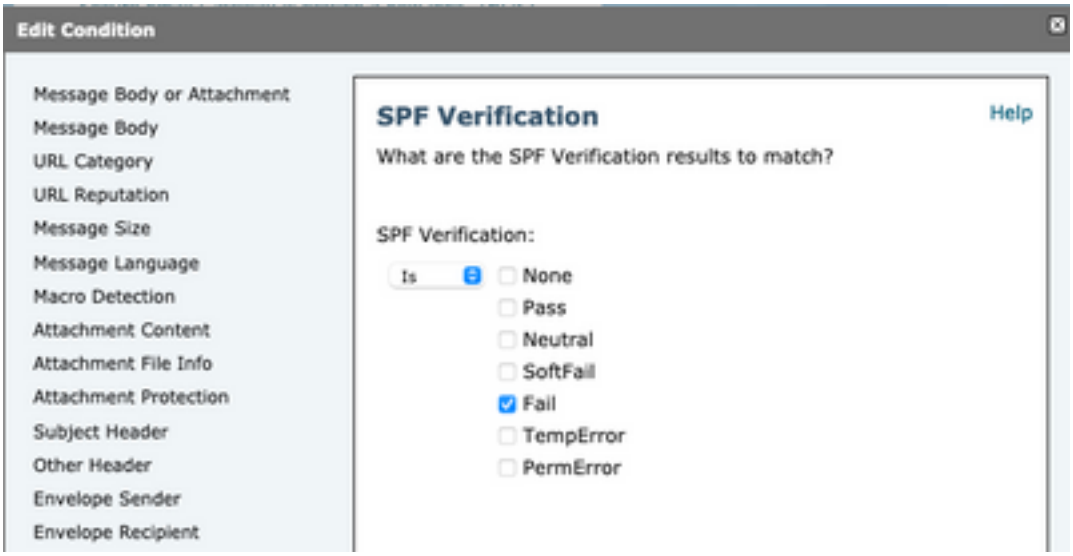
Er zijn drie soorten identiteitscontroles van de SPF-status:

1. SPF-status("mailfrom") IDENTITY
2. SPF-status("pra") IDENTITEIT
3. SPF-status("helo") IDENTITEIT

Bij oudere releases (9.7 en ouder) evalueerden de inhoud-filters alleen PRA-resultaten die werden getraceerd onder CSCuw5673 en zijn vastgelegd op Async OS 9.7.2 en hoger.

Bij alle nieuwere versies bekijken de contentfilters alle drie de SPF-identiteiten voordat ze een actie hebben uitgevoerd.

Dus de inhoud filter conditie spf-status = "fail" zou alle drie identiteiten controleren om te zien of een SPF geen oordeel had.



Content filters staan nog steeds geen specifieke controles tegen een individuele identiteit toe, dus als een admin het mailadres alleen wilde controleren en niet de twee andere, zou hij het gebruik van berichtfilters nodig hebben.

Alleen berichtfilters kunnen de SPF-status regels toetsen aan 'HELO', 'MAILVAN' en 'PRA' identiteiten.

Een berichtfilter ziet er zo uit:

```
if (spf-status("pra") == "Fail") AND(spf-status("mailfrom") == "Fail") AND
(spf-status ("helo") == "Fail")
```

Een berichtfilter maakt het korter op welk type SPF-vonnissen de gebruiker moet quarantaine uitvoeren, terwijl de inhoud-filters niet zoveel opties hebben.

Dit is het berichtfilter dat is genomen uit de AsyncOS geavanceerde gebruikersgids en gebruikt verschillende SPF-statusregel voor verschillende identiteiten:

```
quarantine-spf-failed-mail:

if (spf-status("pra") == "Fail") {

if (spf-status("mailfrom") == "Fail"){

# completely malicious mail

quarantine("Policy");

} else {

if(spf-status("mailfrom") == "SoftFail") {

# malicious mail, but tempting

quarantine("Policy");

}

}

} else {

if(spf-status("pra") == "SoftFail"){

if (spf-status("mailfrom") == "Fail"

or spf-status("mailfrom") == "SoftFail"){

# malicious mail, but tempting

quarantine("Policy");

}

}

}
```

Gerelateerde informatie

- Cisco e-mail security applicatie – eindgebruikershandleiding
- Technische ondersteuning en documentatie – Cisco Systems