Comment la condition de vérification SPF est-elle évaluée avec l'utilisation de filtres de contenu ?

Contenu

Introduction

Ce document explique comment la condition de filtre de contenu de vérification SPF (Sender Policy Framework) est actuellement évaluée.

La déclaration de travail ne s'applique qu'à toutes les versions d'Async OS actuellement prises en charge (10.x et ultérieures).

Condition de filtre de contenu de vérification SPF

SPF est un système simple de validation des e-mails conçu pour détecter l'usurpation d'e-mails en fournissant un mécanisme permettant aux échangeurs de messagerie de réception de vérifier que le courrier entrant d'un domaine est envoyé par un hôte autorisé par les administrateurs de ce domaine.

Sur le dispositif de sécurité de la messagerie Cisco (ESA), SPF est activé pour les messages entrants sur les stratégies de flux de messagerie. Un filtre de contenu peut être créé pour effectuer une action sur le verdict SPF obtenu qui mettra en quarantaine ou supprimera les messages en fonction de la condition requise.

Conditions

Add Condition...

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

Actions

Add Action...

Order	Action	Rule
1	Quarantine	quarantine("Policy")

Les journaux de messagerie ou le suivi des messages affichent ces détails :

```
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>
```

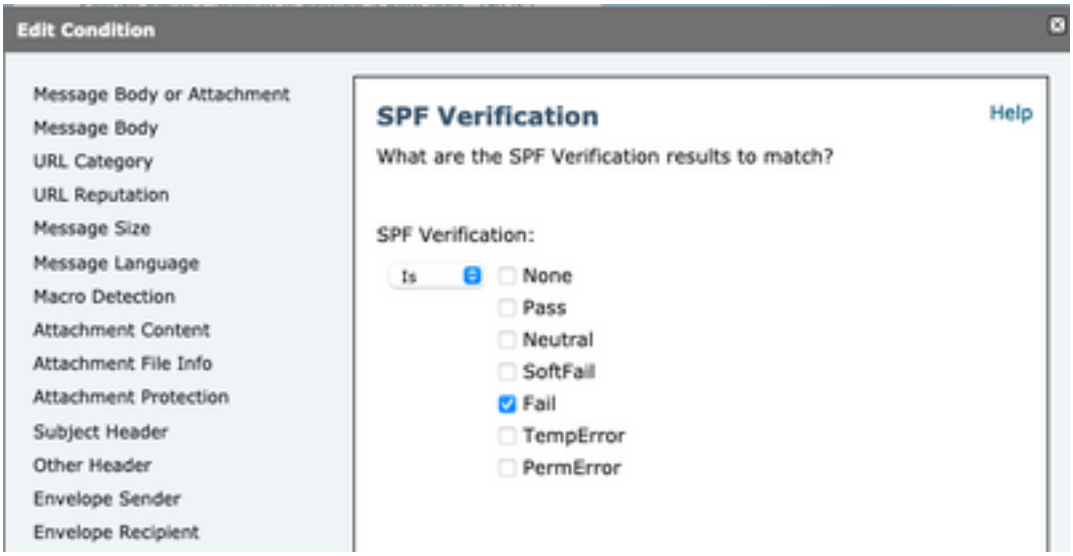
Il existe trois types de vérifications d'identité SPF-Status :

1. spf-status(« mailfrom ») IDENTITÉ
2. spf-status(« pra ») IDENTITÉ
3. spf-status(« helo ») IDENTITÉ

Sur les versions antérieures (9.7 et ultérieures), les filtres de contenu n'ont évalué que les résultats PRA qui ont été suivis sous CSCuw56673 et corrigés sur Async OS 9.7.2 et les versions ultérieures.

Sur toutes les nouvelles versions, les filtres de contenu examinent les trois identités SPF avant d'effectuer une action.

Ainsi, la condition de filtre de contenu spf-status = « fail » vérifierait les trois identités pour voir si un verdict d'échec SPF a été prononcé.



Les filtres de contenu ne permettent toujours pas de vérifications spécifiques d'une identité individuelle, donc si un administrateur voulait vérifier le courrier seul et non les deux autres, il aurait besoin d'utiliser des filtres de message.

Seuls les filtres de messages peuvent vérifier individuellement les règles d'état SPF par rapport aux identités HELO, MAILFROM et PRA.

Un filtre de message ressemblerait à ceci :

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

Un filtre de messages le rend plus précis sur le type de verdicts SPF que l'utilisateur doit mettre en quarantaine, alors que les filtres de contenu n'ont pas autant d'options.

Il s'agit du filtre de message extrait du Guide de l'utilisateur avancé AsyncOS et utilise une règle

d'état SPF différente pour différentes identités :

```
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");

}

}

}
```

Informations connexes

- Cisco Email Security Appliance - Guides de l'utilisateur final
- Support et documentation techniques - Cisco Systems