In che modo viene valutata la condizione di verifica SPF con l'utilizzo dei filtri contenuti?

Sommario

Introduzione

In questo documento viene spiegato come viene attualmente valutata la condizione di filtro del contenuto di verifica di Sender Policy Framework (SPF).

Il funzionamento descritto si applica solo a tutte le versioni Async OS attualmente supportate (10.x e successive).

Condizione filtro contenuto verifica SPF

SPF è un semplice sistema di convalida della posta elettronica progettato per rilevare lo spoofing della posta elettronica fornendo un meccanismo che consente agli scambiatori di posta di ricevere la posta in arrivo da un dominio e di controllare che la posta in arrivo da un host autorizzato dagli amministratori di quel dominio.

In Cisco Email Security Appliance (ESA), SPF è abilitato per i messaggi in arrivo nei criteri di flusso della posta. È possibile creare un filtro contenuti per eseguire un'azione sul verdetto SPF ottenuto che metterà in quarantena o eliminerà i messaggi in base ai requisiti.

Conditions

Add Condition...

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

Actions

Add Action...

Order	Action	Rule
1	Quarantine	quarantine("Policy")

Nei log di posta o nella verifica dei messaggi vengono visualizzati i dettagli seguenti:

```
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>
```

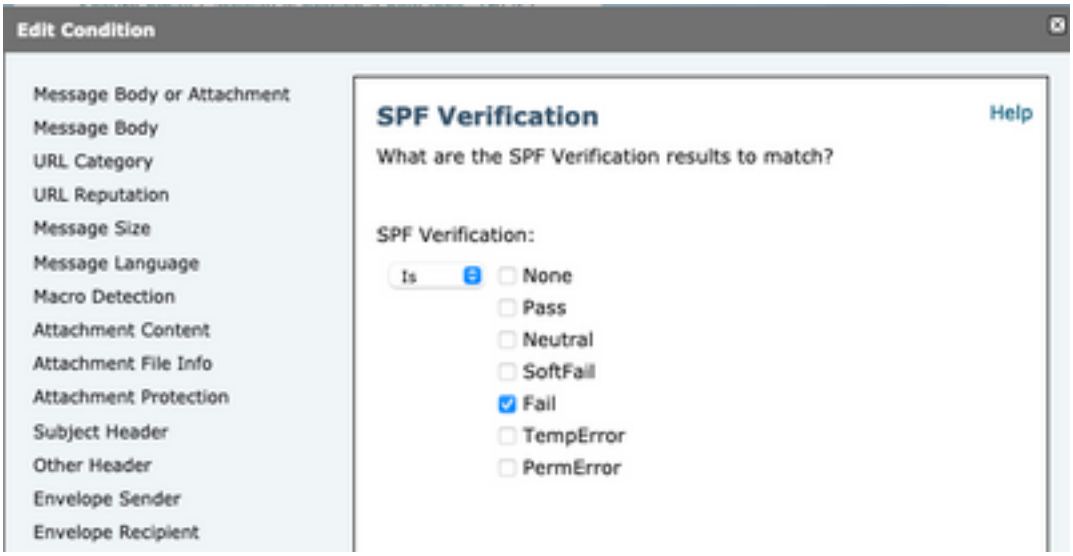
Esistono tre tipi di controlli di identità SPF-Status:

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

Nelle versioni precedenti (9.7 e precedenti), i filtri dei contenuti valutavano solo i risultati PRA che erano stati tracciati in CSCuw56673 e corretti in Async OS 9.7.2 e versioni successive.

In tutte le nuove versioni, i filtri dei contenuti esaminano tutte e tre le identità SPF prima di eseguire un'azione.

Pertanto, la condizione del filtro dei contenuti spf-status = "fail" (non riuscito) controllerà tutte e tre le identità per verificare se esiste un verdetto di errore SPF.



I filtri contenuti non consentono ancora controlli specifici su una singola identità, quindi se un amministratore desidera controllare la posta da solo e non dalle altre due, è necessario utilizzare i filtri messaggi.

Solo i filtri messaggi possono controllare le regole di stato SPF in base alle identità 'HELO', 'MAILFROM' e 'PRA' singolarmente.

Un filtro messaggi sarebbe simile al seguente:

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

Un filtro messaggi rende più granulare il tipo di verdetti SPF che l'utente deve mettere in quarantena, mentre i filtri contenuti non hanno così tante opzioni.

Questo è il filtro messaggi tratto dalla AsyncOS Advanced User Guide e utilizza una regola di stato SPF diversa per identità diverse:

```
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");

}

}

}
```

Informazioni correlate

- Cisco Email Security Appliance - Guide per l'utente
- Documentazione e supporto tecnico – Cisco Systems