Wie wird die SPF-Verifizierungsbedingung mithilfe von Content-Filtern bewertet?

Inhalt

Einführung

In diesem Dokument wird erläutert, wie die Filterbedingung für den Verifizierungsinhaltsfilter des Sender Policy Framework (SPF) derzeit evaluiert wird.

Die angegebene Funktion gilt nur für alle aktuell unterstützten asynchronen Betriebssystemversionen (10.x und höher).

Bedingung für SPF-Verifizierung Content-Filter

SPF ist ein einfaches E-Mail-Validierungssystem, das entwickelt wurde, um E-Mail-Spoofing zu erkennen, indem es einen Mechanismus bereitstellt, mit dem Empfänger-Mail-Empfänger überprüfen können, ob eingehende E-Mails aus einer Domäne von einem Host gesendet werden, der von den Administratoren dieser Domäne autorisiert wurde.

Auf der Cisco E-Mail Security Appliance (ESA) ist SPF für eingehende Nachrichten in Mail Flow-Policys aktiviert. Es kann ein Content-Filter erstellt werden, um Maßnahmen bezüglich des gesammelten SPF-Urteils zu ergreifen, das die Nachrichten je nach Anforderung unter Quarantäne stellt oder löscht.

Conditions

Add Condition...

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

Actions

Add Action...

Order	Action	Rule
1	Quarantine	quarantine("Policy")

Mail-Protokolle oder Nachrichtenverfolgung zeigen folgende Details an:

```
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>
```

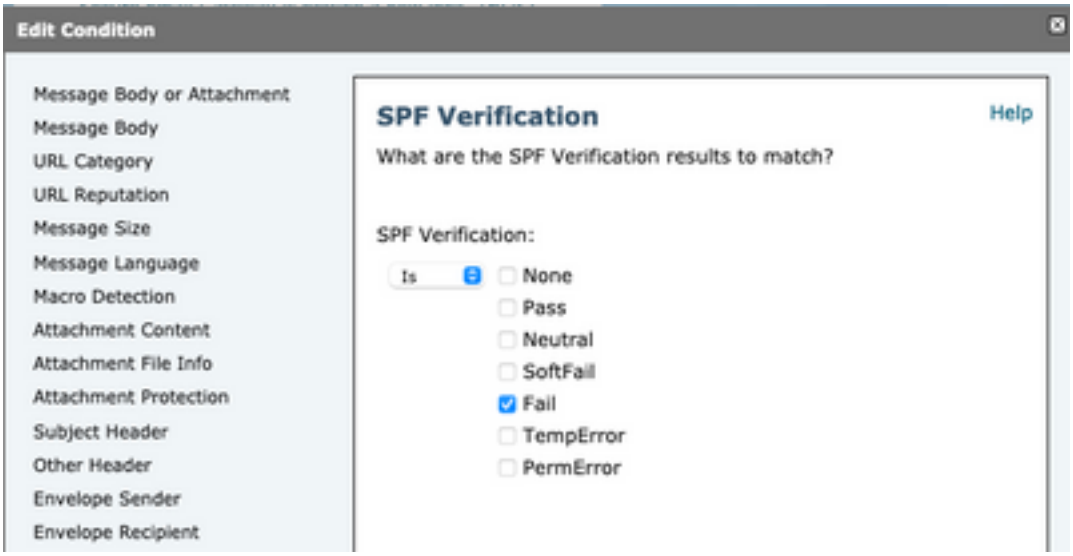
Es gibt drei Arten von SPF-Status-Identitätsprüfungen:

1. SPF-Status("mailfrom")-IDENTITÄT
2. SPF-Status("pra")-IDENTITÄT
3. SPF-Status("helo") IDENTITÄT

Bei älteren Versionen (9.7 und älter) bewerteten Content-Filter nur PRA-Ergebnisse, die unter CSCuw56673 nachverfolgt und auf Async OS 9.7.2 und höher behoben wurden.

Bei allen neueren Versionen überprüfen Content-Filter alle drei SPF-Identitäten, bevor sie eine Aktion ausgeführt haben.

Der Content-Filter-Zustand "spf-status = "fail" (Fehler) überprüft alle drei Identitäten, um festzustellen, ob ein SPF-Failover-Urteil vorliegt.



Content-Filter erlauben immer noch keine spezifischen Prüfungen gegen eine individuelle Identität. Wenn also ein Administrator E-Mails allein und nicht die beiden anderen abrufen möchte, ist die Verwendung von Nachrichtenfiltern erforderlich.

Nur Nachrichtenfilter können SPF-Statusregeln einzeln mit den Identitäten 'HELO', 'MAILFROM' und 'PRA' abgleichen.

Ein Nachrichtenfilter sieht wie folgt aus:

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

Mit einem Nachrichtenfilter kann detaillierter festgelegt werden, welche SPF-Verdicts der Benutzer unter Quarantäne stellen muss, während Content-Filter nicht über so viele Optionen verfügen.

Dies ist der Nachrichtenfilter aus dem AsyncOS Advanced User Guide und verwendet verschiedene SPF-Statusregeln für verschiedene Identitäten:

```
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");

}

}

}
```

Zugehörige Informationen

- Cisco Email Security Appliance - Benutzerhandbücher
- Technischer Support und Dokumentation für Cisco Systeme