如何使用內容過濾器評估SPF驗證條件？

目錄

簡介

本文說明如何目前評估傳送者原則架構(SPF)驗證內容篩選條件。

所述工作狀態僅適用於當前支援的所有非同步OS版本（10.x及更高版本）。

SPF驗證內容篩選器條件

SPF是一種簡單的電子郵件驗證系統，旨在通過提供一種機制來檢測電子郵件欺騙，該機制允許接收郵件交換器檢查來自域的傳入郵件是否正由該域管理員授權的主機傳送。

在思科郵件安全裝置(ESA)上，對郵件流策略上的傳入郵件啟用SPF。可以建立內容篩選器對獲取的SPF裁決執行操作，這將根據需要隔離或丟棄郵件。

Conditions

Add Condition...

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

Actions

Add Action...

Order	Action	Rule
1	Quarantine	quarantine("Policy")

郵件日誌或郵件跟蹤顯示以下詳細資訊：

```
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>
```

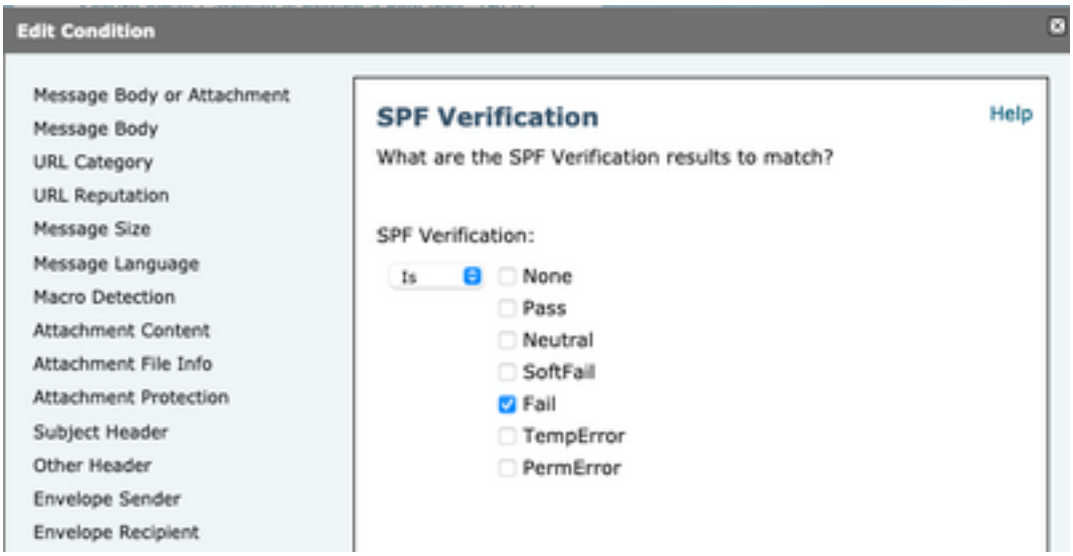
有三種型別的SPF狀態身份檢查：

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

在較早版本（9.7及更高版本）上，內容過濾器僅評估PRA結果，這些結果在CSCuw5673下被跟蹤，並在Async OS 9.7.2及更高版本上被修復。

在所有較新版本中，內容過濾器在執行操作之前會檢查所有三個SPF標識。

因此，內容過濾器條件spf-status =「fail」將檢查所有三個身份，以確定是否有任何SPF失敗判定結果。



內容過濾器仍不允許對單個身份進行特定檢查，因此，如果管理員想要單獨檢查郵件而不是檢查另外兩個郵件，則需要使用郵件過濾器。

只有郵件過濾器可以針對「HELO」、「MAILFROM」和「PRA」標識分別檢查SPF狀態規則。

郵件過濾器將如下所示：

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

郵件過濾器可以更精確地確定使用者需要隔離的SPF型別，而內容過濾器沒有那麼多的選項。

這是從《AsyncOS高級使用手冊》中獲取的郵件過濾器，它針對不同的身份使用不同的SPF狀態規則：

```
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");

}

}

}
```

相關資訊

- Cisco Email Security Appliance — 最終使用手冊
- 技術支援與文件 - Cisco Systems