如何使用内容过滤器评估SPF验证条件？

目录

简介

本文档提供有关当前如何评估发件人策略框架(SPF)验证内容过滤条件的说明。

工作说明仅适用于当前支持的所有异步操作系统版本（10.x及更高版本）。

SPF验证内容过滤器条件

SPF是一个简单的电子邮件验证系统，旨在通过提供允许接收邮件交换器检查从域的传入邮件是否来自该域管理员授权的主机来检测电子邮件欺骗。

在思科邮件安全设备(ESA)上，为邮件流策略上的传入邮件启用SPF。可以创建内容过滤器以对获取的SPF裁决采取操作，该裁决将根据要求隔离或丢弃邮件。

Conditions

Add Condition...

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

Actions

Add Action...

Order	Action	Rule
1	Quarantine	quarantine("Policy")

邮件日志或邮件跟踪显示以下详细信息：

```
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>
```

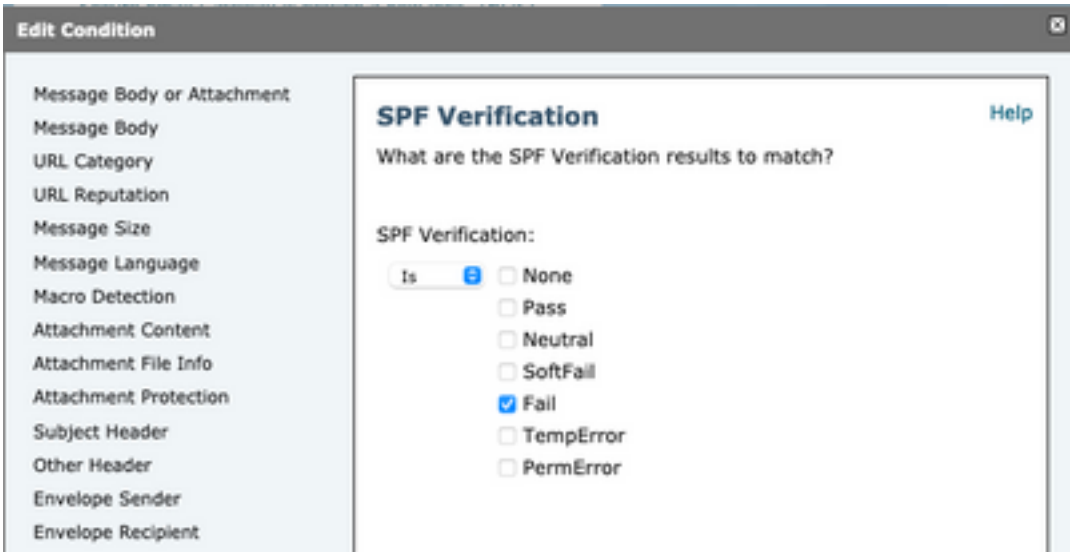
SPF状态身份检查有三种类型：

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

在较旧版本（9.7及更旧版本）上，内容过滤器仅评估PRA结果，这些结果在CSCuw56673下进行跟踪，并在Async OS 9.7.2及更高版本上进行了修复。

在所有较新版本上，内容过滤器在执行操作之前检查所有三个SPF身份。

因此，内容过滤条件spf-status = "fail"将检查所有三个身份，以查看是否有SPF失败裁决。



内容过滤器仍不允许针对单个身份进行特定检查，因此，如果管理员想单独检查邮件，而不是检查另外两个邮件，则需要使用邮件过滤器。

只有邮件过滤器可以针对“HELO”、“MAILFROM”和“PRA”身份逐个检查SPF状态规则。

邮件过滤器如下所示：

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

邮件过滤器可更精细地显示用户需要隔离的SPF判定类型，而内容过滤器没有太多选项。

这是从AsyncOS高级用户指南获取的邮件过滤器，对不同身份使用不同的SPF状态规则：

```
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");

}

}

}
```

相关信息

- 思科邮件安全设备 — 最终用户指南
- 技术支持和文档 - Cisco Systems