How is SPF verification condition evaluated with the use of content filters?

Contents

Introduction

This document provides an explanation as to how the Sender Policy Framework (SPF) verification content filter condition is currently evaluated.

The working stated applies only to all currently supported Async OS versions (10.x and above).

SPF Verification Content Filter Condition

SPF is a simple email validation system designed to detect email spoofing by providing a mechanism to allow receiving mail exchangers to check that incoming mail from a domain is being sent from a host authorized by that domain's administrators.

On the Cisco Email Security Appliance (ESA), SPF is enabled for incoming messages on Mail Flow Policies. A content filter can be created to take action on the SPF verdict obtained which will quarantine or drop the messages based on the requirement.

Conditions

Add Condition...

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

Actions

Add Action...

Order	Action	Rule
1	Quarantine	quarantine("Policy")

Mail logs or message tracking shows these details:

```
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>
```

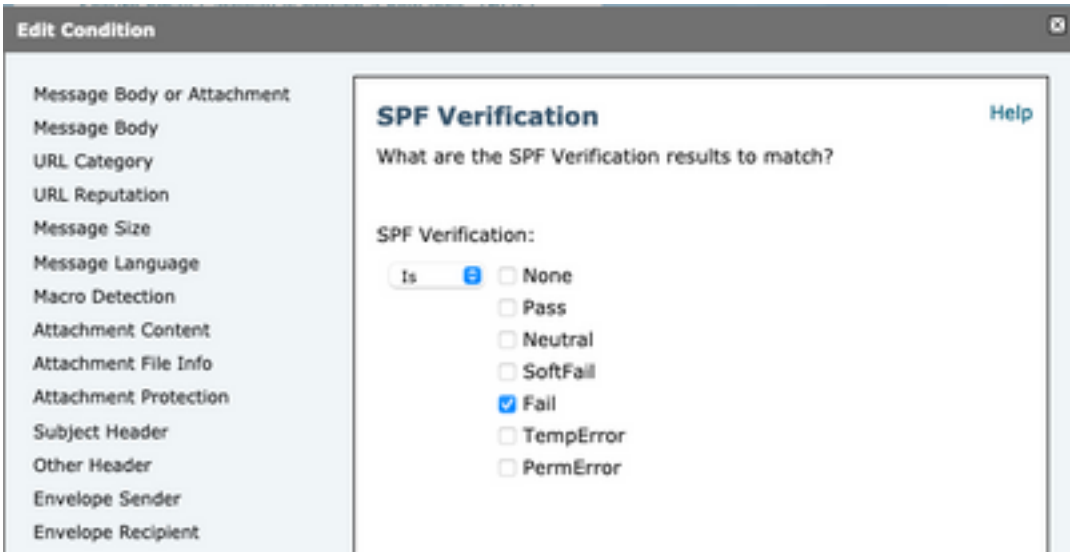
There are three types of SPF-Status identity checks:

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

On older releases (9.7 and older), content filters evaluated only PRA results which were tracked under CSCuw56673 and fixed on Async OS 9.7.2 and above.

On all newer releases, content filters review all three SPF identities before they performed an action.

So content filter condition spf-status = "fail" would check all three identities to see if any had an SPF fail verdict.



Content filters still do not allow for specific checks against an individual identity, so if an admin wanted to check mailfrom alone and not the two others it would require the use of message filters.

Only message filters can check SPF-status rules against 'HELO', 'MAILFROM', and 'PRA' identities individually.

A message filter would look like this:

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

A message filter makes it more granular on what type of SPF verdicts user need to quarantine, while content filters do not have that many options.

This is the message filter taken from the AsyncOS Advanced User Guide and uses different SPF-status rule for different identities:

```
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");

}

}

}
```

Related Information

- **Cisco Email Security Appliance - End-User Guides**
- **Technical Support & Documentation - Cisco Systems**