콘텐츠 필터를 사용하여 SPF 확인 조건을 어떻게 평가합니까?

목차

소개

이 문서에서는 SPF(Sender Policy Framework) 확인 콘텐츠 필터 조건이 현재 평가되는 방법에 대한 설명을 제공합니다.

작업 설명은 현재 지원되는 모든 Async OS 버전(10.x 이상)에만 적용됩니다.

SPF 확인 콘텐츠 필터 조건

SPF는 이메일 스푸핑을 탐지하는 간단한 이메일 검증 시스템으로, 도메인에서 들어오는 메일이 해당 도메인의 관리자가 승인한 호스트에서 전송되고 있는지 확인하는 메일 교환기를 제공합니다.

Cisco ESA(Email Security Appliance)에서 메일 플로우 정책의 수신 메시지에 대해 SPF가 활성화됩니다. 요구 사항에 따라 메시지를 격리 또는 삭제하는 SPF 판정에 대해 조치를 취하도록 콘텐츠 필터를 생성할 수 있습니다.

Conditions

Add Condition...

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

Actions

Add Action...

Order	Action	Rule
1	Quarantine	quarantine("Policy")

메일 로그 또는 메시지 추적에는 다음 세부 정보가 표시됩니다.

```
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
```

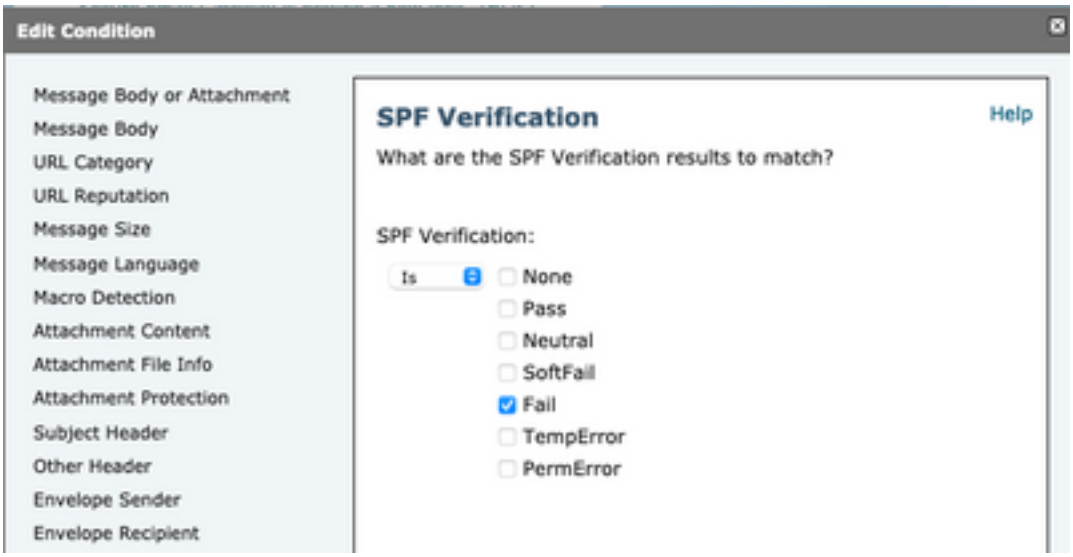
```
None headers from Sat Feb 20 17:28:15 2009 Info: MID 6153849 ready 197 bytes
from <user@example.com>
```
SPF-Status ID 확인에는 세 가지 유형이 있습니다.

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

이전 릴리스(9.7 이상)에서 콘텐츠 필터는 CSCuw56673에서 추적되고 Async OS 9.7.2 이상에서 수정된 PRA 결과만 평가했습니다.

모든 최신 릴리스에서 콘텐츠 필터는 작업을 수행하기 전에 세 SPF ID를 모두 검토합니다.

따라서 콘텐츠 필터 조건 spf-status = "fail"은 세 ID 모두를 검사하여 SPF 실패 판정을 받았는지 확인합니다.



콘텐츠 필터는 여전히 개별 ID에 대한 특정 확인을 허용하지 않으므로 관리자가 단독으로 메일을 확인하고 다른 두 ID가 아닌 다른 ID를 검사하려면 메시지 필터를 사용해야 합니다.

메시지 필터만 'HELO', 'MAILFROM' 및 'PRA' ID에 대해 SPF 상태 규칙을 개별적으로 확인할 수 있습니다.

메시지 필터는 다음과 같습니다.

```
if (spf-status("pra") == "Fail") AND(spf-status("mailfrom") == "Fail") AND
(spf-status ("helo") == "Fail")
```
메시지 필터를 사용하면 사용자가 격리해야 하는 SPF 판정 유형에 대해 더 세부적으로 파악할 수 있지만, 콘텐츠 필터에는 해당 옵션이 많지 않습니다.

AsyncOS Advanced User Guide에서 가져온 메시지 필터이며 여러 ID에 대해 서로 다른 SPF 상태 규칙을 사용합니다.

```
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");

}

}

}
```

관련 정보

- Cisco Email Security Appliance – 엔드 유저 가이드
- 기술 지원 및 문서 – Cisco Systems