コンテンツフィルタを使用してSPF検証条件をどのように評価しますか。

内容

概要

このドキュメントでは、Sender Policy Framework(SPF)の検証コンテンツフィルタ条件が現在評価されている方法について説明します。

記載されている作業は、現在サポートされているすべてのAsync OSバージョン（10.x以降）にのみ適用されます。

SPF検証コンテンツフィルタ条件

SPFは、メール交換機を受信して、ドメインの管理者によって承認されたホストからドメインからの着信メールが送信されていることを確認するメカニズムを提供することで、電子メールのスプーフィングを検出するように設計されたシンプルな電子メール検証システムです。

Cisco Eメールセキュリティアプライアンス(ESA)では、メールフローポリシーの着信メッセージに対してSPFが有効になっています。コンテンツフィルタを作成して、要求に基づいてメッセージを検疫またはドロップするSPF判定に対するアクションを実行できます。

Conditions

Add Condition...

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

Actions

Add Action...

Order	Action	Rule
1	Quarantine	quarantine("Policy")

メールログまたはメッセージトラッキングには、次の詳細が表示されます。

```
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>
```

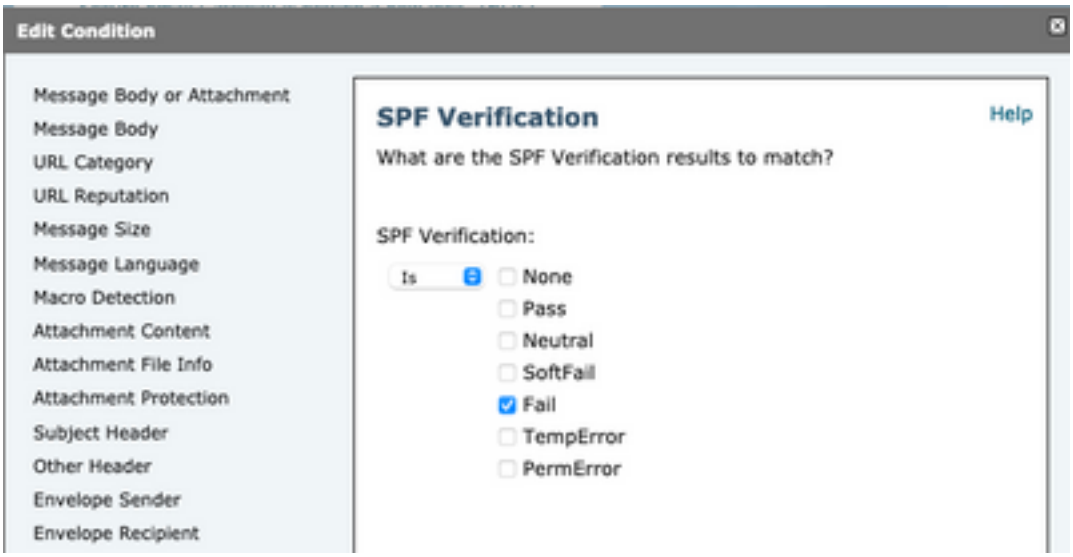
SPF-Status IDチェックには、次の3種類があります。

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

古いリリース（9.7以前）では、コンテンツフィルタはPRAの結果のみを評価し、CSCuw56673で追跡され、Async OS 9.7.2以降で修正されました。

すべての新しいリリースでは、コンテンツフィルタは、アクションを実行する前に3つのSPF IDすべてを確認します。

したがって、コンテンツフィルタ条件spf-status = "fail"は、3つのアイデンティティすべてをチェックして、SPFの失敗判定が行われたかどうかを確認します。



コンテンツフィルタでは、個々のアイデンティティに対する特定のチェックは許可されないため、管理者がメールを単独でチェックし、他の2つのアイデンティティをチェックしない場合は、メッセージフィルタの使用が必要になります。

メッセージフィルタだけが、「HELO」、「MAILFROM」、および「PRA」のIDに対して個別にSPFステータスルールをチェックできます。

メッセージフィルタは次のようになります。

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

メッセージフィルタを使用すると、ユーザが検疫する必要があるSPF判定のタイプに関してより詳細に設定できます。一方、コンテンツフィルタにはそれほど多くのオプションはありません。

これは、『AsyncOS Advanced User Guide』から取得したメッセージフィルタであり、異なるIDに異なるSPFステータスルールを使用します。

```
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");

}

}

}
```

関連情報

- Cisco E メール セキュリティ アプライアンス：エンドユーザ ガイド
- テクニカル サポートとドキュメント – Cisco Systems