Como a condição de verificação SPF é avaliada com o uso de filtros de conteúdo?

Contents

Introduction

Este documento fornece uma explicação sobre como a condição do filtro de conteúdo de verificação do Sender Policy Framework (SPF) é avaliada no momento.

O estado de funcionamento indicado aplica-se apenas a todas as versões Async OS atualmente suportadas (10.x e superiores).

Condição do filtro de conteúdo de verificação SPF

SPF é um sistema de validação de e-mail simples projetado para detectar falsificação de e-mail fornecendo um mecanismo que permite que os corretores de e-mail de recepção verifiquem se os e-mails de entrada de um domínio estão sendo enviados de um host autorizado pelos administradores desse domínio.

No Cisco Email Security Appliance (ESA), o SPF é ativado para mensagens recebidas em Políticas de fluxo de e-mail. Um filtro de conteúdo pode ser criado para agir no veredito SPF obtido que colocará em quarentena ou soltará as mensagens com base no requisito.

Conditions

Add Condition...

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

Actions

Add Action...

Order	Action	Rule
1	Quarantine	quarantine("Policy")

Os logs de e-mail ou o rastreamento de mensagens mostram estes detalhes:

```
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>
```

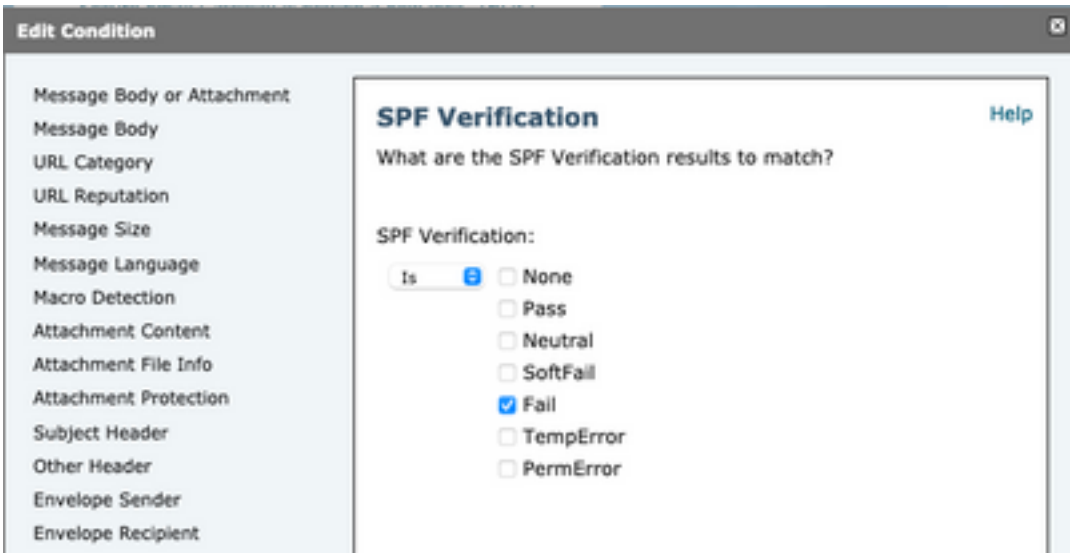
Há três tipos de verificações de identidade SPF-Status:

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

Em versões mais antigas (9.7 e mais antigas), os filtros de conteúdo avaliaram somente os resultados do PRA que foram rastreados no CSCuw56673 e fixos no Async OS 9.7.2 e mais recente.

Em todas as versões mais recentes, os filtros de conteúdo revisam todas as três identidades SPF antes de executar uma ação.

Portanto, a condição de filtro de conteúdo spf-status = "falha" verificaria todas as três identidades para ver se houve algum erro de SPF.



Os filtros de conteúdo ainda não permitem verificações específicas em relação a uma identidade individual, portanto, se um administrador quisesse verificar o correio sozinho e não os dois outros, seria necessário usar filtros de mensagem.

Somente filtros de mensagem podem verificar as regras de status SPF em relação às identidades 'HELO', 'MAILFROM' e 'PRA' individualmente.

Um filtro de mensagem seria semelhante a este:

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

Um filtro de mensagens torna-o mais granular em que tipo de veredito SPF o usuário precisa colocar em quarentena, enquanto os filtros de conteúdo não têm muitas opções.

Este é o filtro de mensagens extraído do AsyncOS Advanced User Guide e usa uma regra de status SPF diferente para identidades diferentes:

```
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");

}

}

}
```

Informações Relacionadas

- Cisco Email Security Appliance – Guias do usuário final
- Suporte Técnico e Documentação - Cisco Systems