

Pourquoi les messages obtiennent-ils livré même si la vérification SPF échoue ?

Contenu

[Introduction](#)

[Pourquoi les messages obtiennent-ils livré même si la vérification SPF échoue ?](#)

[Informations connexes](#)

Introduction

Ce document fournit une explication quant à pourquoi des messages électroniques sont fournis même lorsque la validation de Sender Policy Framework (SPF) échoue.

Pourquoi les messages obtiennent-ils livré même si la vérification SPF échoue ?

La SPF est un système simple de validation d'email conçu pour détecter la mystification d'email en fournissant un mécanisme pour permettre recevoir des messages pour vérifier que la messagerie entrante d'un domaine est envoyée d'un hôte autorisé par les administrateurs de ce domaine.

Sur l'appliance de sécurité du courrier électronique de Cisco (ESA), la vérification SPF est activée pour tous les messages entrant sur des stratégies de flux de courrier. Un filtre satisfait existe qui mettra en quarantaine ou relâchera les messages si la SPF-vérification échoue, utilisant le == de SPF-*vérification* et de SPF-état de condition « échouer », avec l'action de la *quarantaine* :

La messagerie se connecte ou le cheminement de message affiche les détails suivants :

```
Thu Aug 20 17:27:37 2009 Info: MID 6153849 SPF: helo identity postmaster@example None
Thu Aug 20 17:27:37 2009 Info: MID 6153849 SPF: mailfrom identity
user@example.com Fail (v=spf1)
Thu Aug 20 17:28:15 2009 Info: MID 6153849 SPF: pra identity user@example.com
None headers from Thu Aug 20 17:28:15 2009 Info: MID 6153849 ready 197 bytes
from <user@example.com>
```

Cependant, le message est traité et fourni normalement.

Il y a trois types de contrôles d'identité de SPF-état :

1. IDENTITÉ de SPF-état (« mailfrom »)
2. IDENTITÉ de SPF-état (« pra »)
3. IDENTITÉ de SPF-état (« hélicoptère »)

Seulement les filtres de message peuvent vérifier des règles de SPF-état contre « HÉLICOPTÈRE », « MAILFROM », et des identités « PRA ».

Dans des filtres satisfaits, seulement le résultat d'identité PRA est vérifié. Un filtre semblable de message ressemblerait à ceci :

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

Un filtre de message le rend plus granulaire sur quel type de besoin de l'utilisateur de verdicts SPF de mettre en quarantaine, alors que les filtres satisfaits n'ont pas que beaucoup d'options.

Le filtre de message suivant pris du guide d'utilisateur avancé d'AsyncOS utilise la règle différente de SPF-état pour différentes identités :

```
quarantine-spf-failed-mail:
if (spf-status("pra") == "Fail") {
  if (spf-status("mailfrom") == "Fail") { quarantine("Policy");}
  else {
    if(spf-status("mailfrom") == "SoftFail") { quarantine("Policy")}
  }
} else {
  if(spf-status("pra") == "SoftFail"){
    if (spf-status("mailfrom") == "Fail" or spf-status("mailfrom") == "SoftFail")
    { quarantine("Policy");}
  }
}
```

[Informations connexes](#)

- [Appliance de sécurité du courrier électronique de Cisco - Guides d'utilisateur](#)
- [Support et documentation techniques - Cisco Systems](#)