¿Por qué los mensajes consiguen entregados incluso si la verificación SPF falla?

Contenido

Introducción

Este documento proporciona una explicación en cuanto a porqué se entregan los correos electrónicos incluso cuando la validación del Marco de políticas del remitente (SPF) falla.

¿Por qué los mensajes consiguen entregados incluso si la verificación SPF falla?

El SPF es correo electrónico simple un sistema de la validación diseñado para detectar el spoofing del email proporcionando a un mecanismo para permitir el recibir de los cambiadores de correo para marcar que el correo entrante de un dominio se está enviando de un host autorizado por los administradores de ese dominio.

En el dispositivo de seguridad del correo electrónico de Cisco (ESA), la verificación SPF se habilita para todos los mensajes entrantes en las directivas del flujo de correo. Un filtro contento existe que quarantine o caerá los mensajes si la SPF-verificación falla, usando el == “fall” de la SPF-*verificación* y del SPF-estatus de la condición, con la acción de la *cuarentena*:

Conditions

Add Condition...

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

Actions

Add Action...

Order	Action	Rule
1	Quarantine	quarantine("Policy")

Envíe los registros o Seguimiento de mensajes muestra los detalles siguientes:

```
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>
```

Sin embargo, el mensaje se procesa y se entrega normalmente.

Hay tres tipos de controles de la identidad del SPF-estatus:

1. IDENTIDAD del SPF-estatus (“mailfrom”)
2. IDENTIDAD del SPF-estatus (“pra”)
3. IDENTIDAD del SPF-estatus (“helicóptero”)

Solamente los filtros del mensaje pueden marcar las reglas del SPF-estatus contra “HELO”, “MAILFROM”, y las identidades del “PRA”.

En los filtros contentos, solamente se marca el resultado de la identidad del PRA. Un filtro similar del mensaje parecería esto:

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

Un filtro del mensaje lo hace más granular en qué tipo de necesidad de usuario de los veredictos SPF de quarantine, mientras que los filtros contentos no tienen que muchas opciones.

El filtro del siguiente mensaje tomado de la guía de usuario avanzado de AsyncOS utiliza diversa regla del SPF-estatus para diversas identidades:

```
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");}
 }
}
```

Información Relacionada

- Dispositivo de seguridad del correo electrónico de Cisco - Guías del usuario final
- Soporte Técnico y Documentación - Cisco Systems