¿Cómo se evalúa la condición de verificación SPF con el uso de filtros de contenido?

Contenido

Introducción

Este documento proporciona una explicación de cómo se evalúa actualmente la condición de filtro de contenido de verificación de Sender Policy Framework (SPF).

El término de trabajo indicado se aplica solamente a todas las versiones del sistema operativo asíncrono admitidas actualmente (10.x y superiores).

Condición de filtro de contenido de verificación SPF

SPF es un simple sistema de validación de correo electrónico diseñado para detectar la suplantación de correo electrónico al proporcionar un mecanismo para permitir que los intercambiadores de correo reciban el correo entrante de un dominio que se envía desde un host autorizado por los administradores de ese dominio.

En Cisco Email Security Appliance (ESA), SPF está habilitado para los mensajes entrantes en las políticas de flujo de correo. Se puede crear un filtro de contenido para tomar medidas sobre el veredicto de SPF obtenido que pondrá en cuarentena o descartará los mensajes según el requisito.

Conditions

Add Condition...

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

Actions

Add Action...

Order	Action	Rule
1	Quarantine	quarantine("Policy")

Los registros de correo o el seguimiento de mensajes muestran estos detalles:

```
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>
```

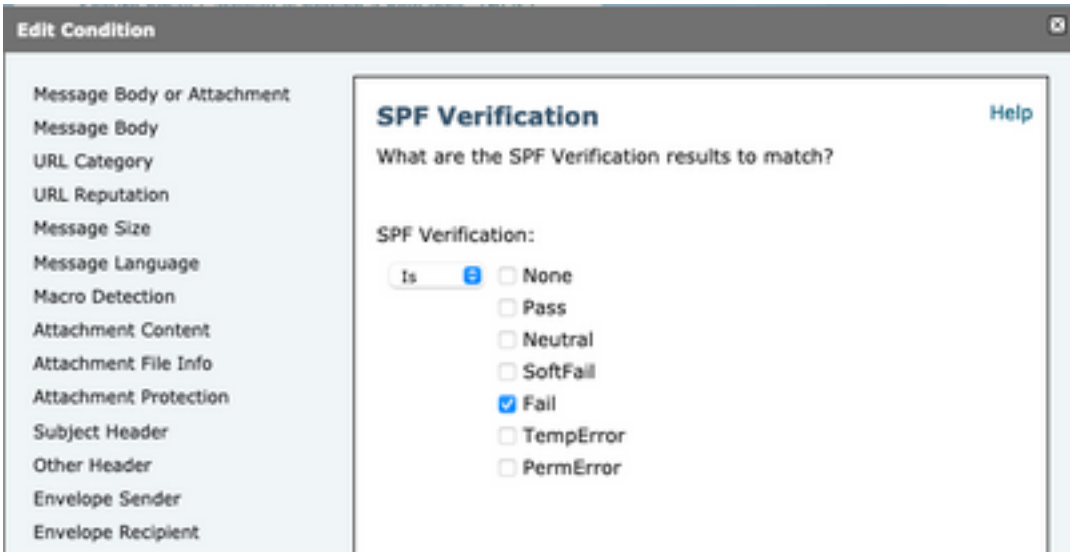
Hay tres tipos de comprobaciones de identidad SPF-Status:

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

En las versiones anteriores (9.7 y anteriores), los filtros de contenido evaluaron solamente los resultados de PRA que fueron rastreados bajo CSCuw56673 y corregidos en Async OS 9.7.2 y superiores.

En todas las versiones más recientes, los filtros de contenido revisan las tres identidades SPF antes de realizar una acción.

Por lo tanto, la condición de filtro de contenido spf-status = "fail" verificaría las tres identidades para ver si alguna tiene un veredicto de falla de SPF.



Los filtros de contenido todavía no permiten verificaciones específicas de una identidad individual, por lo que si un administrador quisiera verificar el correo solo y no de los otros dos, necesitaría el uso de filtros de mensajes.

Solo los filtros de mensajes pueden comprobar las reglas de estado SPF con las identidades 'HELO', 'MAILFROM' y 'PRA' individualmente.

Un filtro de mensaje se vería así:

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

Un filtro de mensajes hace que sea más granular en qué tipo de veredictos SPF el usuario necesita poner en cuarentena, mientras que los filtros de contenido no tienen tantas opciones.

Este es el filtro de mensajes tomado de la guía del usuario avanzada de AsyncOS y utiliza diferentes reglas de estado SPF para diferentes identidades:

```
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");

}

}

}
```

Información Relacionada

- Dispositivo de seguridad Cisco Email Security Appliance - Guías de usuario final
- Soporte Técnico y Documentación - Cisco Systems