Condición de la autenticación ESA S TP para prevenir el spoofing

Contenido

[Introducción](#)
[prerrequisitos](#)
[Antecedentes](#)
[Cree un filtro](#)
[Ejemplo de regla](#)
[Información Relacionada](#)

Introducción

Este documento describe cómo crear un filtro basado en el usuario autenticado del Simple Mail Transfer Protocol (SMTP) y registrar el nombre de usuario en una X-encabezado.

Prerequisites

Cisco recomienda que usted tiene conocimiento de la versión 6.5 y posterior de AsyncOS.

Antecedentes

La función de la autenticación S TP permite que los clientes utilicen la autenticación S TP para sus clientes para conectar con y enviar el correo de los dispositivos de seguridad del correo electrónico (ESA). Puesto que la característica permite que el usuario autenticado retransmita, es posible que los usuarios forjen “de: ” coloque en los correos electrónicos que envían con Cisco ESA. Para prevenir a los usuarios de la forja, la versión 6.5 y posterior ESA AsyncOS ahora contiene una condición del filtro del mensaje que permita las comparaciones contra el nombre de usuario del usuario autenticado S TP y el **correo de la** dirección de correo electrónico.

Cree un filtro

La condición del filtro del mensaje permite que un administrador escriba un filtro similar al ejemplo de regla en la siguiente sección que compara los correos electrónicos que son salientes retransmitido vía una sesión de la autenticación S TP. Si se comprometen las credenciales S TP, la máquina que envía los correos electrónicos genera generalmente varios direccionamientos que se utilizarán como el correo **de:** encabezado. La condición del filtro del mensaje permite solamente que los correos electrónicos se vayan si el nombre de usuario y el correo **de:** coincidencia de las encabezados. Si no, el correo electrónico se considera un correo forjado **de:** ,

y el mensaje Filter Action (Acción de filtro) activa. El mensaje Filter Action (Acción de filtro) puede ser cualquier última acción; el ejemplo de regla muestra una acción de la cuarentena. La condición del filtro tiene este sintaxis:

```
smtp-auth-id-matches("<target>" [, "<sieve-char>"])
```

El filtro permite una comparación contra una de estas blancos:

- **EnvelopeFrom:** Compara el direccionamiento especificado en el **correo de:** en la conversación SMTP.
- **FromAddress:** Compara el de los analizado los direccionamientos **de:** encabezado. Puesto que permiten a las múltiples direcciones en **de:** la encabezado, solamente una debe hacer juego.
- **Remitente:** Compara el direccionamiento especificado en el **remitente:** encabezado.
- **Ningunos:** Hace juego los mensajes que fueron creados durante una sesión de SMTP autenticada (sin importar la identidad).
- **Ninguno:** Hace juego los mensajes que no fueron creados durante una sesión de SMTP autenticada (por ejemplo, cuando **se prefiere la** autenticación S TP).

S TP AUTH ID	CHAR DEL TAMIZ	DIRECCIONAMIENTO DE LA COMPARACIÓN	¿COINCIDENC
someuser		otheruser@example.com	No
someuser		someuser@example.com	Yes
someuser		someuser@face.localhost	Yes
SomeUser		someuser@example.com	Yes
someuser		someuser+folder@example.com	No
someuser	+	someuser+folder@example.com	Yes
someUser@example.com		someuser@forged.com	No
someUser@example.com		someuser@example.com	Yes
someUser@example.com		someuser@example.com	Yes

Esta substitución variable, **$SMTPAuthID**, fue creada para permitir la inclusión en las encabezados de los credenciales de autenticación originales usados para retransmitir.

Ejemplo de regla

```
Msg_Authentication: if (smtp-auth-id-matches("*Any"))
{
   # Always include the original authentication credentials in a
   # special header.
   insert-header("X-SMTPAUTH", "$SMTPAuthID");

   if (smtp-auth-id-matches("*FromAddress", "+") and
       smtp-auth-id-matches("*EnvelopeFrom", "+"))
   {
       # Username matches.  Verify the domain
       if (header('from') != "(?i)@(?:example\.com|example\.com)" or mail-from !=
"(?i)@(?:example\.com|\.com)"
       {
           # User has specified a domain which cannot be authenticated
           quarantine("forged");
       }
   } else {
       # User claims to be an completely different user
```

```
        quarantine("forged");
    }
}
```

Note: Este filtro asume que usted hace una cuarentena llamada **forjar**.

Información Relacionada

- Guía de usuario avanzado de IronPort AsyncOS para los dispositivos de seguridad del correo electrónico de IronPort
- Soporte Técnico y Documentación - Cisco Systems