Condición de autenticación SMTP de ESA para evitar la suplantación

Contenido

Introducción

Este documento describe cómo crear un filtro basado en el usuario autenticado del protocolo simple de transferencia de correo (SMTP) y registrar el nombre de usuario en un encabezado X.

Prerequisites

Cisco recomienda que tenga conocimiento de AsyncOS versión 6.5 y posteriores.

Antecedentes

La función de autenticación SMTP permite a los clientes utilizar la autenticación SMTP para sus clientes con el fin de conectarse y enviar correo desde los dispositivos de seguridad de correo electrónico (ESA). Dado que la función permite al usuario autenticado retransmitir, es posible que los usuarios falsifiquen el campo "De:" en correos electrónicos que envían a través de Cisco ESA. Para evitar que los usuarios falsifiquen, ESA AsyncOS versión 6.5 y posteriores ahora contienen una condición de filtro de mensajes que permite comparaciones con el nombre de usuario de usuario SMTP autenticado y la dirección de correo **Desde**.

Crear un filtro

La condición de filtro de mensajes permite que un administrador escriba un filtro similar a la regla de ejemplo en la siguiente sección que compara los correos electrónicos que se retransmiten de salida a través de una sesión de autenticación SMTP. Si las credenciales SMTP están comprometidas, la máquina que envía los correos electrónicos generalmente genera varias direcciones para ser utilizadas como el correo **De:** encabezado. La condición de filtro de mensajes sólo permite que los correos electrónicos salgan si el nombre de usuario y el correo **De:** los encabezados coinciden. De lo contrario, el correo electrónico se considera un correo falsificado

Desde: y se activa la acción de filtro de mensajes. La acción de filtro de mensajes puede ser cualquier acción final; la regla de ejemplo muestra una acción de cuarentena. La condición de filtro tiene esta sintaxis:

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

El filtro permite una comparación con uno de estos objetivos:

- **SobreDe:** Compara la dirección especificada en **Correo de:** en la conversación SMTP.
- **Dirección de origen:** Compara las direcciones analizadas desde el **origen:** encabezado. Dado que se permiten varias direcciones en el **campo Desde:** , sólo uno debe coincidir.
- **Remitente:** Compara la dirección especificada en el **remitente:** encabezado.
- **Cualquiera:** Coincide con los mensajes creados durante una sesión SMTP autenticada (independientemente de la identidad).
- **Ninguno:** Coincide con los mensajes que no se crearon durante una sesión SMTP autenticada (por ejemplo, cuando se **prefiere** la autenticación SMTP).

ID de autenticación SMTP	SIEVE CHAR	DIRECCIÓN DE COMPARACIÓN	¿COINCIDENCIAS?
someuser		otheruser@example.com	No
someuser		someuser@example.com	Yes
someuser		someuser@face.localhost	Yes
AlgunosUsuarios		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 sustitución de variable, **$SMTPAuthID**, se creó para permitir la inclusión en los encabezados de las credenciales de autenticación originales usadas para retransmitir.

Regla de ejemplo

```
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");
   }
}
```

Nota: Este filtro asume que tiene una cuarentena llamada **falsificada**.

Información Relacionada

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