Condição da autenticação ESA S TP para impedir a falsificação

Índice

Introdução

Este documento descreve como criar um filtro baseado no usuário autenticado do Simple Mail Transfer Protocol (SMTP) e registrar o username em um X-encabeçamento.

Pré-requisitos

Cisco recomenda que você tem o conhecimento da versão 6.5 e mais recente de AsyncOS.

Informações de Apoio

A função da autenticação S TP permite que os clientes usem a autenticação S TP para seus clientes a fim conectar a e enviar o correio das ferramentas de segurança do email (ESA). Desde que a característica permite que o usuário autenticado retransmita, é possível para usuários forjar “de: ” coloque nos email que enviam através de Cisco ESA. A fim impedir usuários do forjamento, a versão 6.5 e mais recente ESA AsyncOS contém agora uma condição do filtro da mensagem que permita comparações contra o username autenticado do usuário S TP e o **correio do** endereço email.

Crie um filtro

A condição do filtro da mensagem permite que um administrador escreva um filtro similar à regra de exemplo na próxima seção que compara os email que são de partida retransmitido através de uma sessão da autenticação S TP. Se as credenciais S TP são comprometidas, a máquina que envia os email gerencie geralmente diversos endereços a ser usados como o correio **de:** encabeçamento. A condição do filtro da mensagem permite somente que os email saam se o username e o correio **de:** fósforo dos encabeçamentos. Se não, o email é considerado um correio forjado **de:** , e a ação do filtro da mensagem ativa. A ação do filtro da mensagem pode ser toda a

ação final; a regra de exemplo mostra uma ação da quarentena. A condição do filtro tem esta sintaxe:

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

O filtro permite uma comparação contra um destes alvos:

- **EnvelopeFrom:** Compara o endereço especificado no **correio de:** na conversação SMTP.
- **FromAddress:** Compara os endereços analisados gramaticalmente fora do **de:** encabeçamento. Desde que os endereços múltiplos são permitidos no **de:** o encabeçamento, somente um deve combinar.
- **Remetente:** Compara o endereço especificado no **remetente:** encabeçamento.
- **Alguns:** Combina as mensagens que foram criadas durante uma sessão de SMTP autenticada (apesar da identidade).
- **Nenhum:** Combina as mensagens que não foram criadas durante uma sessão de SMTP autenticada (por exemplo, quando a autenticação S TP **é preferida**).

AUTH ID S TP	CARVÃO ANIMAL DA PENEIRA	ENDEREÇO DA COMPARAÇÃO	FÓSFORO
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 substituição variável, **$SMTPAuthID**, foi criada a fim permitir a inclusão nos encabeçamentos das credenciais de autenticação originais usadas para retransmitir.

Regra de exemplo

```
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 supõe que você tem uma quarentena chamada **forjada**.

Informações Relacionadas

- Guia de usuário avançado de IronPort AsyncOS para ferramentas de segurança do email de IronPort
- Suporte Técnico e Documentação - Cisco Systems