Condizione di autenticazione SMTP ESA per impedire lo spoofing

Sommario

Introduzione

In questo documento viene descritto come creare un filtro basato sull'utente autenticato SMTP (Simple Mail Transfer Protocol) e accedere al nome utente in un'intestazione X.

Prerequisiti

Cisco raccomanda la conoscenza di AsyncOS versione 6.5 e successive.

Premesse

La funzione di autenticazione SMTP consente ai clienti di utilizzare l'autenticazione SMTP per connettersi a e inviare posta da Email Security Appliance (ESA). Poiché questa funzione consente all'utente autenticato di inoltrare, è possibile per gli utenti falsificare il campo "Da:" nelle e-mail che inviano tramite Cisco ESA. Per impedire agli utenti di falsificare, ESA AsyncOS versione 6.5 e successive ora contiene una condizione di filtro messaggi che permette confronti con il nome utente utente SMTP autenticato e l'indirizzo e-mail **Da**.

Creare un filtro

La condizione del filtro messaggi consente a un amministratore di scrivere un filtro simile alla regola di esempio della sezione successiva che confronta i messaggi di posta elettronica inoltrati in uscita tramite una sessione di autenticazione SMTP. Se le credenziali SMTP sono compromesse, il computer che invia i messaggi di posta elettronica in genere genera diversi indirizzi da utilizzare come posta **Da:** intestazione. La condizione di filtro messaggi consente di lasciare i messaggi di posta elettronica solo se il nome utente e l'indirizzo di posta elettronica **Da:** le intestazioni corrispondono. In caso contrario, l'e-mail viene considerata un messaggio contraffatto **Da:** e l'operazione filtro messaggi viene attivata. L'operazione filtro messaggi può

essere qualsiasi azione finale; la regola di esempio mostra un'azione di quarantena. La condizione del filtro ha la seguente sintassi:

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

Il filtro consente un confronto con una delle seguenti destinazioni:

- **BustaDa:** Confronta l'indirizzo specificato in **Invia da:** nella conversazione SMTP.
- **Indirizzo mittente:** Confronta gli indirizzi analizzati nel campo **Da:** intestazione. Poiché sono consentiti più indirizzi nel campo **Da:** , solo uno deve corrispondere.
- **Mittente:** Confronta l'indirizzo specificato nel campo **Mittente:** intestazione.
- **Qualsiasi:** Corrisponde ai messaggi creati durante una sessione SMTP autenticata (indipendentemente dall'identità).
- **Nessuna:** Corrisponde ai messaggi che non sono stati creati durante una sessione SMTP autenticata (ad esempio, quando è **preferibile** l'autenticazione SMTP).

ID AUTENTICAZIONE SMTP	SIEVE	INDIRIZZO DI CONFRONTO	CORRISPONDENZE?
utente		otheruser@example.com	No
utente		someuser@example.com	Sì
utente		someuser@face.localhost	Sì
Utente		someuser@example.com	Sì
utente		someuser+folder@example.com	No
utente	+	someuser+folder@example.com	Sì
someUser@example.com		someuser@forged.com	No
someUser@example.com		someuser@example.com	Sì
someUser@example.com		someuser@example.com	Sì

La sostituzione della variabile **$SMTPAuthID** è stata creata per consentire l'inclusione nelle intestazioni delle credenziali di autenticazione originali utilizzate per l'inoltro.

Regola di esempio

```
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: Questo filtro presuppone che si disponga di una quarantena denominata **falsificata**.

Informazioni correlate

- Guida per l'utente avanzata di IronPort AsyncOS per IronPort Email Security Appliance
- Documentazione e supporto tecnico – Cisco Systems