ESA SMTP-Authentifizierungsbedingung zum Verhindern von Spoofing

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie Sie einen Filter erstellen, der auf dem SMTP-authentifizierten Benutzer (Simple Mail Transfer Protocol) basiert, und den Benutzernamen in einen X-Header eingeben.

Voraussetzungen

Cisco empfiehlt, über Kenntnisse von AsyncOS 6.5 und höher zu verfügen.

Hintergrundinformationen

Mit der SMTP-Authentifizierungsfunktion können Kunden SMTP-Authentifizierung für ihre Clients verwenden, um eine Verbindung zu E-Mail-Security-Appliances (ESAs) herzustellen und E-Mails von ihnen zu senden. Da die Funktion die Weiterleitung durch den authentifizierten Benutzer ermöglicht, können Benutzer das Feld "Von" in E-Mails, die sie über die Cisco ESA versenden, nachschlagen. Um das Schmieden von Benutzern zu verhindern, enthält die ESA AsyncOS-Version 6.5 und höher jetzt eine Nachrichtenfilterbedingung, die Vergleiche mit dem authentifizierten SMTP-Benutzernamen und der **E-Mail-**Adresse **"Von"** erlaubt.

Filter erstellen

Die Nachrichtenfilterbedingung ermöglicht es einem Administrator, einen Filter zu schreiben, der der Beispielregel im nächsten Abschnitt ähnelt, der E-Mails vergleicht, die über eine SMTP-Authentifizierungssitzung ausgesendet werden. Wenn die SMTP-Anmeldeinformationen kompromittiert werden, generiert der Computer, der die E-Mails sendet, in der Regel mehrere Adressen, die als E-Mail-**Absender** verwendet werden sollen**:** Header. Die Bedingung für den Nachrichtenfilter erlaubt nur das Hinterlassen von E-Mails, wenn der Benutzername und die E-

Mail-Adresse **Von:** Header übereinstimmen. Andernfalls wird die E-Mail als gefälschte E-Mail **From:** (**Von:**) angesehen, und die Aktion "Nachrichtenfilter" wird aktiviert. Bei der Aktion für den Nachrichtenfilter kann es sich um eine beliebige endgültige Aktion handeln. Die Beispielregel zeigt eine Quarantäneaktion. Die Filterbedingung hat folgende Syntax:

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

Der Filter ermöglicht einen Vergleich mit einem der folgenden Ziele:

- **UmschlagVon:** Vergleicht die unter **Mail From** angegebene Adresse**:** im SMTP-Gespräch.
- **VonAdresse:** Vergleicht Adressen, die aus dem **Formular** geparst wurden**:** Header. Da im **From** mehrere Adressen zulässig sind**:** -Header, nur einer muss übereinstimmen.
- **Absender:** Vergleicht die im **Absender** angegebene Adresse**:** Header.
- **Beliebig:** Gleicht Nachrichten ab, die während einer authentifizierten SMTP-Sitzung erstellt wurden (unabhängig von der Identität).
- **Keine:** Entspricht Nachrichten, die nicht während einer authentifizierten SMTP-Sitzung erstellt wurden (z. B. wenn die SMTP-Authentifizierung **bevorzugt** wird).

SMTP-AUTH-ID	SIEBE KLEINE	VERGLEICHSANSCHRIFT	ÜBEREINSTIMMUNGEN?
Benutzer		otheruser@example.com	Nein
Benutzer		someuser@example.com	Ja
Benutzer		someuser@face.localhost	Ja
Einige Benutzer		someuser@example.com	Ja
Benutzer		someuser+folder@example.com	Nein
Benutzer	+	someuser+folder@example.com	Ja
someUser@example.com		someuser@forged.com	Nein
someUser@example.com		someuser@example.com	Ja
someUser@example.com		someuser@example.com	Ja

Diese Variablenersetzung, **$SMTPAuthID**, wurde erstellt, um die Einbindung in Header der ursprünglichen Authentifizierungsinformationen zu ermöglichen, die zum Relay verwendet werden.

Beispielregel

```
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");
   }
```

```
}
```

Hinweis: Bei diesem Filter wird davon ausgegangen, dass Sie über eine Quarantäne mit dem Namen **gefälscht** verfügen.

Zugehörige Informationen

- IronPort AsyncOS Erweitertes Benutzerhandbuch für IronPort Email Security Appliances
- Technischer Support und Dokumentation - Cisco Systems