S/MIME-verschlüsselte E-Mails verlieren ihre Inhalte nach ESA/CES-Tags

Inhalt

Einführung

In diesem Dokument wird erläutert, warum E-Mails mit sicheren/mehrseitigen Internet-Mail-Erweiterungen (S/MIME), die im Posteingang der Empfänger eingehen, nach dem Durchlaufen der E-Mail Security Appliance (ESA) oder Cloud Email Security (CES) keinen Inhalt enthalten.

Problem: E-Mails verlieren ihre Inhalte nach den ESA/CES Tags.

Eine Organisation hat ihre E-Mails so konfiguriert, dass sie mit S/MIME-Zertifikaten signiert oder verschlüsselt werden. Nachdem sie über ein Cisco ESA/CES-Gerät gesendet wurden, scheint die E-Mail den Inhalt verloren zu haben, wenn sie im Posteingang der Endempfänger eingeht. Dieses Verhalten tritt im Allgemeinen auf, wenn die ESA/CES so konfiguriert ist, dass der Inhalt der E-Mail geändert wird. Die typische Änderung von der ESA/CES ist das Tagging für Haftungsausschluss.

Wenn eine E-Mail mit S/MIME signiert oder verschlüsselt wird, wird der gesamte Inhalt gehasht, um die Integrität der E-Mail zu schützen. Wenn ein Mailserver den Inhalt manipuliert, indem er den Text ändert, stimmt der Hash nicht mehr mit dem, der signiert/verschlüsselt wurde, überein und führt damit zum Verlust des Textinhalts.

Darüber hinaus können E-Mails, die mit S/MIME verschlüsselt sind oder "opak" S/MIME Signierung (d. h. p7m Dateien) verwenden, von der S/MIME-Software am Empfängerende nicht automatisch erkannt werden, wenn sie geändert werden. Bei einer S/MIME-E-Mail um 0,70 Uhr sind der Inhalt der E-Mail, einschließlich der Anhänge, in der Datei .p7m enthalten. Wenn die Struktur neu organisiert wird, wenn die ESA/CES den Haftungsausschluss-Stempel hinzufügt, ist diese .p7m-Datei möglicherweise nicht mehr an einem Ort, an dem die MUA-Software, die das S/MIME behandelt, sie richtig verstehen kann.

E-Mails, die von S/MIME signiert oder verschlüsselt werden, sollten in der Regel überhaupt nicht geändert werden. Wenn die ESA/CES das für das Signieren/Verschlüsseln einer E-Mail konfigurierte Gateway ist, sollte dies geschehen, nachdem eine Änderung der E-Mail erforderlich ist, und im Allgemeinen, wenn die ESA/CES der letzte Hop ist, der die E-Mail verarbeitet, bevor sie an den Mail-Server des Empfängers gesendet wird.

Lösung

Um zu verhindern, dass E-Mails aus dem Internet, die S/MIME-verschlüsselt sind, manipuliert oder verändert werden, konfigurieren Sie einen Nachrichtenfilter, um die E-Mail zu suchen, um einen **X-Header** hinzuzufügen und alle verbleibenden Nachrichtenfilter zu überspringen. Anschließend wird ein Inhaltsfilter erstellt, um diesen X-Header zu finden, und die übrigen Content-Filter überspringen, die den Text/die Inhalte ändern können.

> **Vorsicht**: Beim Arbeiten mit "skip filter()"; Aktion oder Filter für verbleibende Inhalte überspringen (abschließende Aktion), die Reihenfolge der Filter ist sehr wichtig. Wenn Sie einen Übersprungsfilter in einer falschen Reihenfolge festlegen, kann die Nachricht möglicherweise unbeabsichtigte Filter überspringen.

Dazu gehören u. a.:

- Die URL-Filterung wird umgeschrieben, sowohl das Standard- als auch das sichere Proxy-Rewrites.
- Haftungsausschluss-Tagging in der E-Mail.
- E-Mail-Textprüfung und -Austausch

> **Hinweis**: Informationen zum Zugriff auf die Befehlszeile der CES Solution finden Sie im **CES CLI Guide**.

Um einen Nachrichtenfilter zu konfigurieren, melden Sie sich über die CLI bei der ESA/CES an:

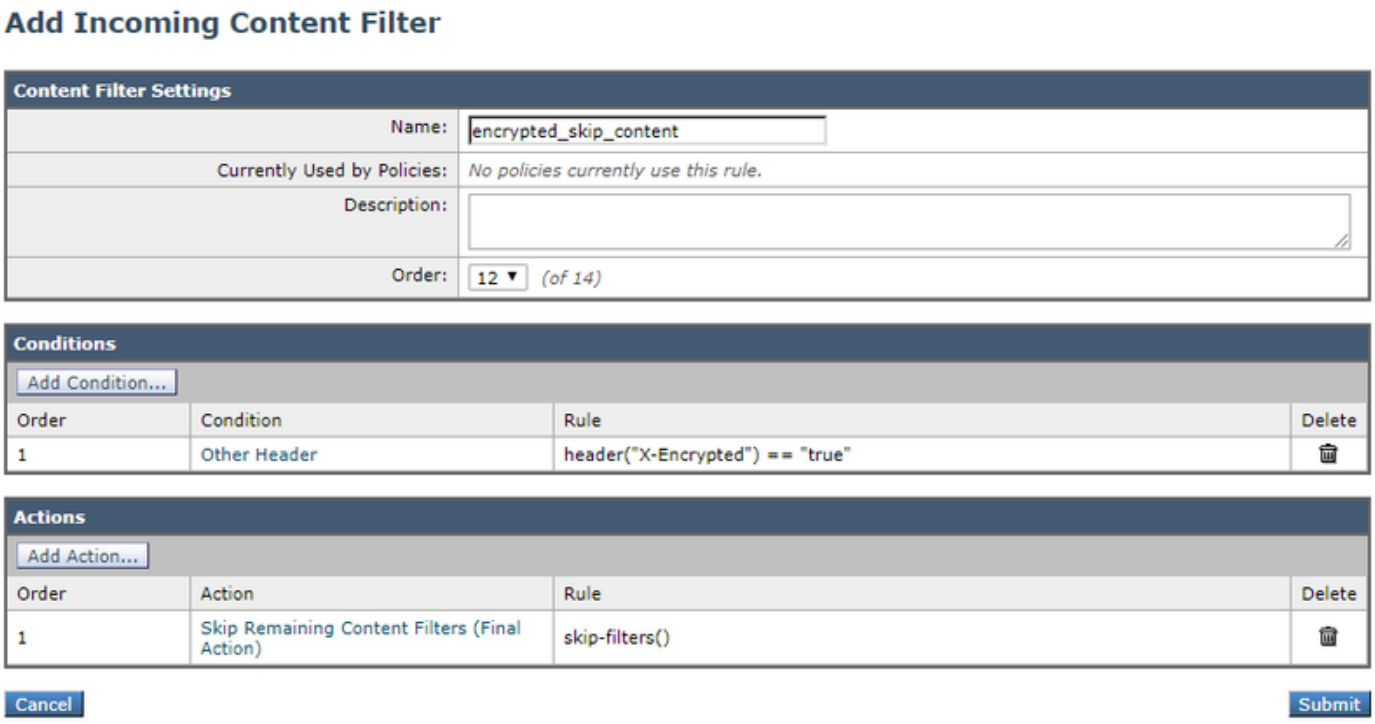
```
C680.esa.lab> filters


Choose the operation you want to perform:
- NEW - Create a new filter.
- DELETE - Remove a filter.
- IMPORT - Import a filter script from a file.
- EXPORT - Export filters to a file
- MOVE - Move a filter to a different position.
- SET - Set a filter attribute.
- LIST - List the filters.
- DETAIL - Get detailed information on the filters.
- LOGCONFIG - Configure log subscriptions used by filters.
- ROLLOVERNOW - Roll over a filter log file.
[]> new

Enter filter script. Enter '.' on its own line to end.
encrypted_skip:
if (encrypted)
{
insert-header("X-Encrypted", "true");
skip-filters();
}
.
1 filters added.
```

> **Hinweis**: Wenn Cisco Virus-Outbreak-Filter mit **Nachrichtenmodifizierung** festgelegt werden, schlägt auch der S/MIME-Signierungs-/Verschlüsselungs-Hash fehl. Falls die Virus-Outbreak-Filter in der Mail-Policy aktiviert sind und die Nachrichtenänderung aktiviert ist, wird empfohlen, die Nachrichtenänderung für die übereinstimmende Mail-Policy zu deaktivieren oder die Outbreak-Filterung sowie eine Nachrichtenfilteraktion von **Skip-OutbreakCheck(); zu** überspringen.

Nachdem der Nachrichtenfilter so konfiguriert ist, dass er verschlüsselte E-Mails mit einem X-Header kennzeichnet, erstellen Sie einen Content-Filter, um diesen Header zu finden und die verbleibende Content-Filter-Aktion zu überspringen.



Konfigurieren Sie diesen Content-Filter in Ihre bestehenden Richtlinien für eingehende E-Mails, in denen die verschlüsselten E-Mails die verbleibenden Content-Filter überspringen sollen.

Zugehörige Informationen

- Überprüfen von Nachrichten, die mit S/MIME-Sendeprofil auf der ESA gesendet wurden
- Überprüfen von Nachrichten, die mit S/MIME auf ESA empfangen wurden
- Technischer Support und Dokumentation - Cisco Systems
- Cisco Email Security Appliance - Benutzerhandbücher