I messaggi di posta elettronica crittografati S/MIME perdono il contenuto dopo i tag ESA/CES

Sommario

Introduzione

In questo documento viene illustrato il motivo per cui i messaggi di posta elettronica S/MIME (Secure/Multipurpose Internet Mail Extensions) ricevuti nella cartella Posta in arrivo dei destinatari non contengono contenuti dopo essere passati attraverso Email Security Appliance (ESA) o Cloud Email Security (CES).

Problema: Le e-mail perdono il loro contenuto dopo i tag ESA/CES.

Un'organizzazione ha configurato i propri messaggi di posta elettronica in modo che vengano firmati o crittografati tramite certificati S/MIME e, dopo l'invio tramite un dispositivo Cisco ESA/CES, il contenuto dell'e-mail sembra essere stato perso quando arriva nella cartella Posta in arrivo dei destinatari finali. Questo comportamento si verifica in genere quando l'ESA/CES è configurato per modificare il contenuto dell'e-mail; la modifica tipica dell'ESA/CES è l'etichettatura di esclusione di responsabilità.

Quando un messaggio e-mail viene firmato o crittografato con S/MIME, viene eseguito l'hashing di tutto il contenuto del corpo per proteggerne l'integrità. Quando i server di posta alterano il contenuto modificandone il corpo, l'hash non corrisponde più a quello firmato/crittografato e a sua volta causa la perdita del contenuto del corpo.

Inoltre, i messaggi di posta elettronica crittografati con S/MIME o che utilizzano la firma S/MIME 'opaca' (ovvero i file p7m) potrebbero non essere riconosciuti automaticamente dal software S/MIME sul lato ricevente se vengono modificati. Nel caso di un'e-mail p7m S/MIME, il contenuto dell'e-mail, inclusi gli allegati, è contenuto nel file .p7m. Se la struttura viene riorganizzata quando l'ESA/CES aggiunge il timbro di esclusione di responsabilità, questo file .p7m potrebbe non trovarsi più in una posizione in cui il software MUA che gestisce l'S/MIME possa comprenderlo correttamente.

In genere i messaggi di posta elettronica firmati o crittografati da S/MIME non devono essere modificati. Quando l'ESA/CES è il gateway configurato per firmare/criptare un'e-mail, questa operazione deve essere eseguita dopo ogni modifica dell'e-mail, e in genere quando l'ESA/CES è l'ultimo hop che gestisce l'e-mail prima di inviarla al server di posta del destinatario.

Soluzione

Per evitare la manipolazione ESA/CES o la modifica dei messaggi e-mail in arrivo da Internet che sono crittografati con S/MIME, configurare un filtro messaggi per individuare l'e-mail per aggiungere un'intestazione **X-Header** e ignorare eventuali filtri messaggi rimanenti, quindi creare un filtro contenuti per individuare questa intestazione X-Header e ignorare i filtri contenuti rimanenti che potrebbero alterare il contenuto del corpo/degli allegati.

> **Attenzione:** Quando lavorate con skip-filters(); o Skip Remaining Content Filters (Final Action) l'ordine dei filtri è molto critico. L'impostazione di un filtro di omissione in un ordine non corretto può consentire al messaggio di ignorare alcuni filtri involontariamente.

Ciò include, a titolo esemplificativo:

- Il filtro URL riscrive, sia disinnesca che protetta.
- Etichettatura dell'esclusione di responsabilità nell'e-mail.
- Scansione e sostituzione del corpo dell'e-mail.

> **Nota:** Per accedere alla riga di comando della soluzione CES, consultare la Guida CLI di CES.

Per configurare un filtro messaggi, accedere a ESA/CES dalla CLI:

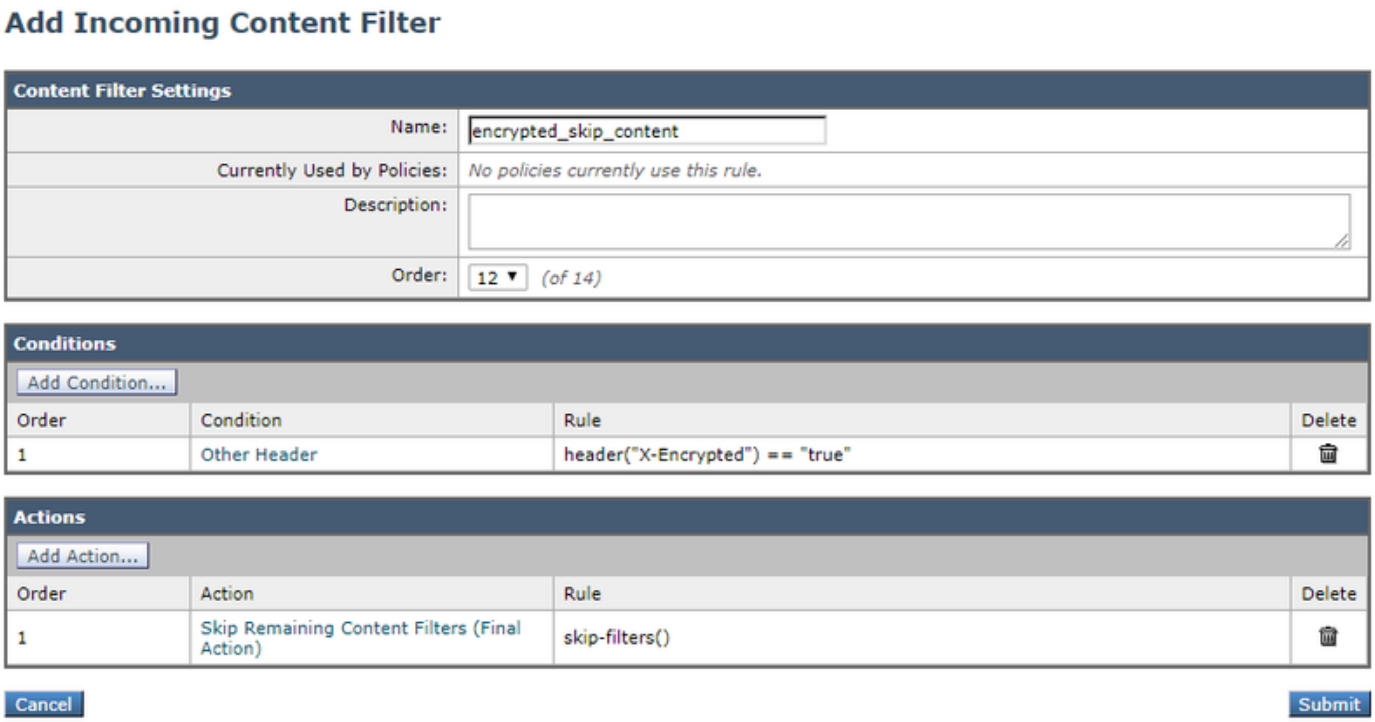
```
C680.esa.lab> filters


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.
```

> **Nota:** Se i filtri epidemie di virus Cisco sono impostati con la **modifica del messaggio**, l'hash di firma/crittografia S/MIME non riesce. Se nel criterio di posta sono attivati i filtri epidemie di virus con la modifica del messaggio, è consigliabile disattivare la modifica del messaggio nel criterio di posta corrispondente o ignorare il filtro epidemie e un'operazione filtro messaggi di **skip-outbreakcheck(); .**

Dopo aver configurato il filtro messaggi per contrassegnare i messaggi di posta elettronica crittografati con un'intestazione X, creare un filtro contenuti per individuare l'intestazione e applicare l'operazione di filtro ignora contenuto rimanente.



Configura questo filtro contenuti nei criteri di posta in arrivo esistenti in cui i messaggi di posta elettronica crittografati devono ignorare i filtri contenuti rimanenti.

Informazioni correlate

- Come verificare i messaggi inviati con S/MIME Sending Profile su ESA
- Come verificare i messaggi ricevuti con S/MIME su ESA
- Documentazione e supporto tecnico – Cisco Systems
- Cisco Email Security Appliance - Guide per l'utente