S/MIME Encrypted Emails Lose their Content after ESA/CES Tags

Contents

Introduction

This document describes why Secure/Multipurpose Internet Mail Extensions (S/MIME) emails received in recipients inbox contains no contents after passing through the Email Security Appliance (ESA) or Cloud Email Security (CES).

Problem: Emails lose their Content after the ESA/CES Tags.

An organization has configured its emails to be signed or encrypted by S/MIME certificates and after being sent through a Cisco ESA/CES device, the email appears to have lost it's content when it arrives in the end recipients inbox. This behavior generally occurs when the ESA/CES is configured to modify the contents of the email, the typical modification from the ESA/CES is disclaimer tagging.

When an email is signed or encrypted with S/MIME, all the body content is hashed to protect its integrity. When any mail servers tamper with the content by modifying the body, the hash no longer matches that which was signed/encrypted and in turn causes the body content to be lost.

Furthermore, emails that are encrypted with S/MIME or use 'opaque' S/MIME signing (i.e. p7m files) may not be automatically recognized by S/MIME software on the receiving end if they are modified. In the case of a p7m S/MIME email, the contents of the email, including attachments, are contained within the .p7m file. If the structure is re-organized when the ESA/CES adds the disclaimer stamping, this .p7m file may no longer be in a place where the MUA software that handles the S/MIME can properly understand it.

Typically emails that are signed or encrypted by S/MIME should not be altered at all. When the ESA/CES is the gateway configured to sign/encrypt an email, this should be done after any modification of the email is required, and generally when the ESA/CES is the last hop which handles the email before sending it to the recipient's mail server.

Solution

In order to avoid the ESA/CES manipulation or modification of incoming emails from the internet which are S/MIME encrypted, configure a message filter to locate the email to add an **X-Header** and skip any remaining message filters, followed by creating a content filter to locate this X-Header and skip the remaining content filters which may alter the body/attachment contents.

> **Caution**: When working with skip-filters(); action or Skip Remaining Content Filters (Final Action) the order of the filters is very critical. Setting a skip filter in an incorrect order may allow the message to skip some filters unintended.

This includes but not limited to:

- URL filtering rewrites, both defang and secure proxy rewrites.
- Disclaimer tagging onto the email.
- Email body scan and replace.

> **Note**: To get access to the CES Solution command line, please refer to the **CES CLI Guide**.

In order to configure a message filter, log in to the ESA/CES from the CLI:

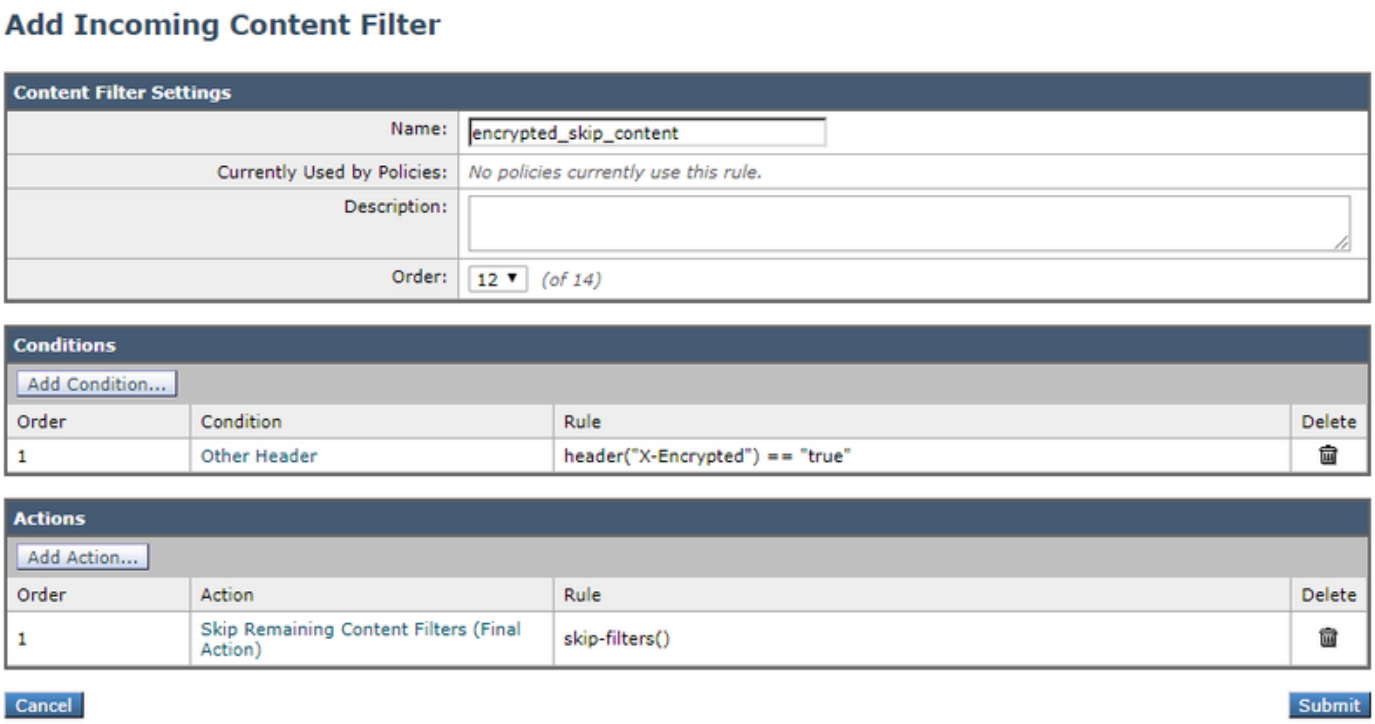
```
C680.esa.lab> filters


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.
```

> **Note**: Cisco Virus Outbreak Filters when set with **Message Modification** also causes the S/MIME signing/encryption hash to fail. In the event the mail policy has Virus Outbreak Filters enabled with message modification, it is recommended to disable message modification on the matching mail policy or skip outbreak filtering as well with a message filter action of **skip-outbreakcheck(); .**

After the message filter is configured to tag encrypted emails with an X-Header, create a content filter to locate this header and apply the skip remaining content filter action.



Configure this content filter into your existing incoming mail policies where the encrypted emails should skip the content filters that remain.

Related Information

- **How to verify messages sent with S/MIME Sending Profile on ESA**
- **How to verify messages received with S/MIME on ESA**
- **Technical Support & Documentation - Cisco Systems**
- **Cisco Email Security Appliance - User Guides**