S/MIME によって暗号化されるメールは ESA/CES タグの後で内容を失います

目次

概要

受信者インボックスで受信されたセキュア/Multipurpose Internet Mail Extensions （ S/MIME ）メールが E メール セキュリティ アプライアンス (ESA) またはクラウド E メール セキュリティ (CES) かを通ることの後で内容がなぜ含まれていないかこの資料に記述されています。

問題： メールは ESA/CES タグの後で内容を失います。

組織はメールを署名するために設定しましたまたは S/MIME 証明書によっておよび Cisco ESA/CES デバイスを通って送信の後で暗号化されて、端受信者インボックスで着くときメールはです満足それを失うようです。 この動作は ESA/CES から一般に メールの内容を修正するために ESA/CES が設定されるとき典型的な修正です免責事項 タギング見られます。

メールが S/MIME と署名するか、または暗号化されるとき統合を保護するために、すべての本文内容はハッシュされます。 どのメール サーバでも本文の修正によって内容を不正変更するとき、もはやハッシュ一致はおよび次々と本文内容を署名したり/暗号化されたそれ失いません。

なお、S/MIME か使用「不透明な」S/MIME 署名と暗号化されるメールは受電端の S/MIME ソフトウェアによって (すなわち p7m ファイル) 修正される場合自動的に認識されないかもしれません。 p7m S/MIME メールの場合には、メールの内容は、添付ファイルを含んで .p7m ファイルの内で、含まれています。 ESA/CES が押す免責事項を追加するとき構造が再構成されれば S/MIME を処理するこの .p7m ファイルは MUA ソフトウェアがきちんとそれを理解する場合があるインポートにもはやであるかもしれません。

通常 S/MIME によって署名するか、または暗号化されるメールはまったく変えるべきではありません。 ESA/CES がメール ゲートウェイによって設定される/暗号化署名するときこれは受信者のメール サーバへそれを送信 する前にメールを処理する ESA/CES が最後のホップである時メールのどの修正でも必要となった、一般に後する必要があり。

解決策

暗号化される S/MIME であるインターネットからの着信メールの ESA/CES 操作か修正を避けるためにメールを X **ヘッダを**追加し、コンテンツ フィルタのこの X ヘッダを見つけ、本文/添付ファイル内容を変えるかもしれない残りのコンテンツ フィルターをスキップするために作成に先行している残りのメッセージ フィルターをスキップするために見つけるようにメッセージ フィルターを設定して下さい。

注意： とはたらいた場合スキップしてfilters() 下さい; 操作はまたは残りのコンテンツ フィルタ（最終措置）をフィルターの発注が非常に重要であるスキップします。 不正確な順序で省略フィルタを設定 することはメッセージが故意ではないいくつかのフィルターをスキップするようにするかもしれません。

これはに制限されなくて含んでいます:

- URL フィルタリング書き直しは、プロキシ書き直しの牙を抜き、保護します。
- メールに免責事項 タギング。
- 本文スキャンを E-メールを送り、取り替えて下さい。

注: CES ソリューション コマンド・ラインへのアクセスを得るために、CES CLI ガイドを参照して下さい。

メッセージ フィルターを、ログイン CLI からの ESA/CES に設定するため:

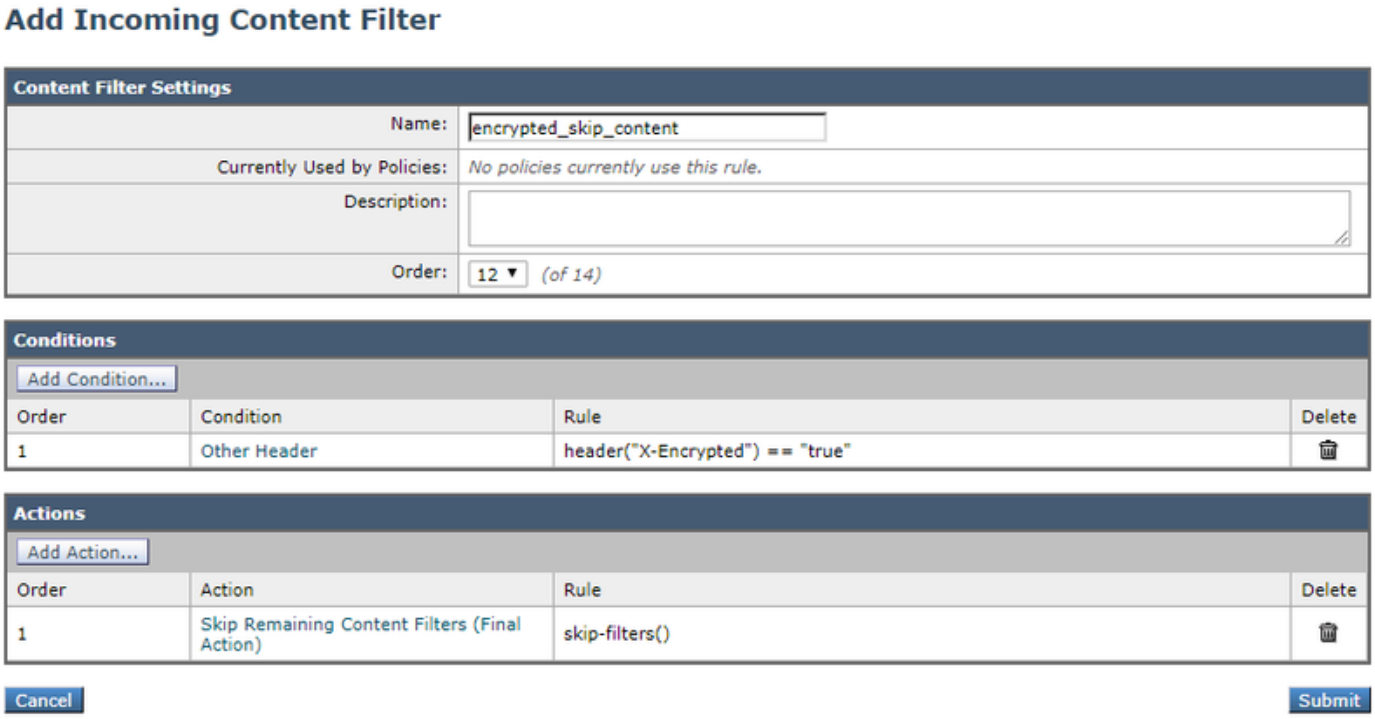
```
C680.esa.lab> filters


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.
```

注: メッセージ修正を用いるセットによりまた失敗するために署名する S/MIME/暗号化ハッシュを引き起こす場合の Cisco ウイルス発生フィルタ。 イベントではメール ポリシーにメッセージ修正と有効に なる ウイルス発生フィルタがありますー致するメール ポリシーのメッセージ修正を無効に することを推奨しますまたはメッセージ フィルター操作と同様にのフィルタリングする発生をスキップするために**スキップしてoutbreakcheck() 下さい;。**

暗号化されたメールを X ヘッダとタグ付けし、このヘッダを見つけるためにコンテンツ フィルタを作成し、省略残りのコンテンツ フィルタ操作を適用するためにメッセージ フィルターが設定された後。



暗号化されたメールが残すコンテンツ フィルターをスキップする必要がある存在来信ポリシーにこのコンテンツ フィルタを設定して下さい。

関連情報

- 方法メッセージを確認する ESA のプロファイルを送信 する S/MIME と送信 しました
- ESA の S/MIME と受け取ったメッセージを確認する方法
- テクニカル サポートとドキュメント – Cisco Systems
- Cisco E メール セキュリティ アプライアンス-ユーザ ガイド