CSC SSM URL フィルタがインライン ASA で設定されたカットスルー プロキシの認証に失敗する

内容

[概要](#)
[前提条件](#)
[要件](#)
[使用するコンポーネント](#)
[表記法](#)
[状況および環境](#)
[問題](#)
[解決策](#)
[関連情報](#)

概要

このドキュメントでは、適応型セキュリティアプライアンス(ASA)またはCSC-SSMの管理ポートとインターネット間のデバイスでカットスループロキシ認証が設定されている場合に、Content Security and Control Security Services Module(CSC-SSM)でURLフィルタが失敗する問題についてについて説明します。

前提条件

要件

このドキュメントに特有の要件はありません。

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

状況および環境

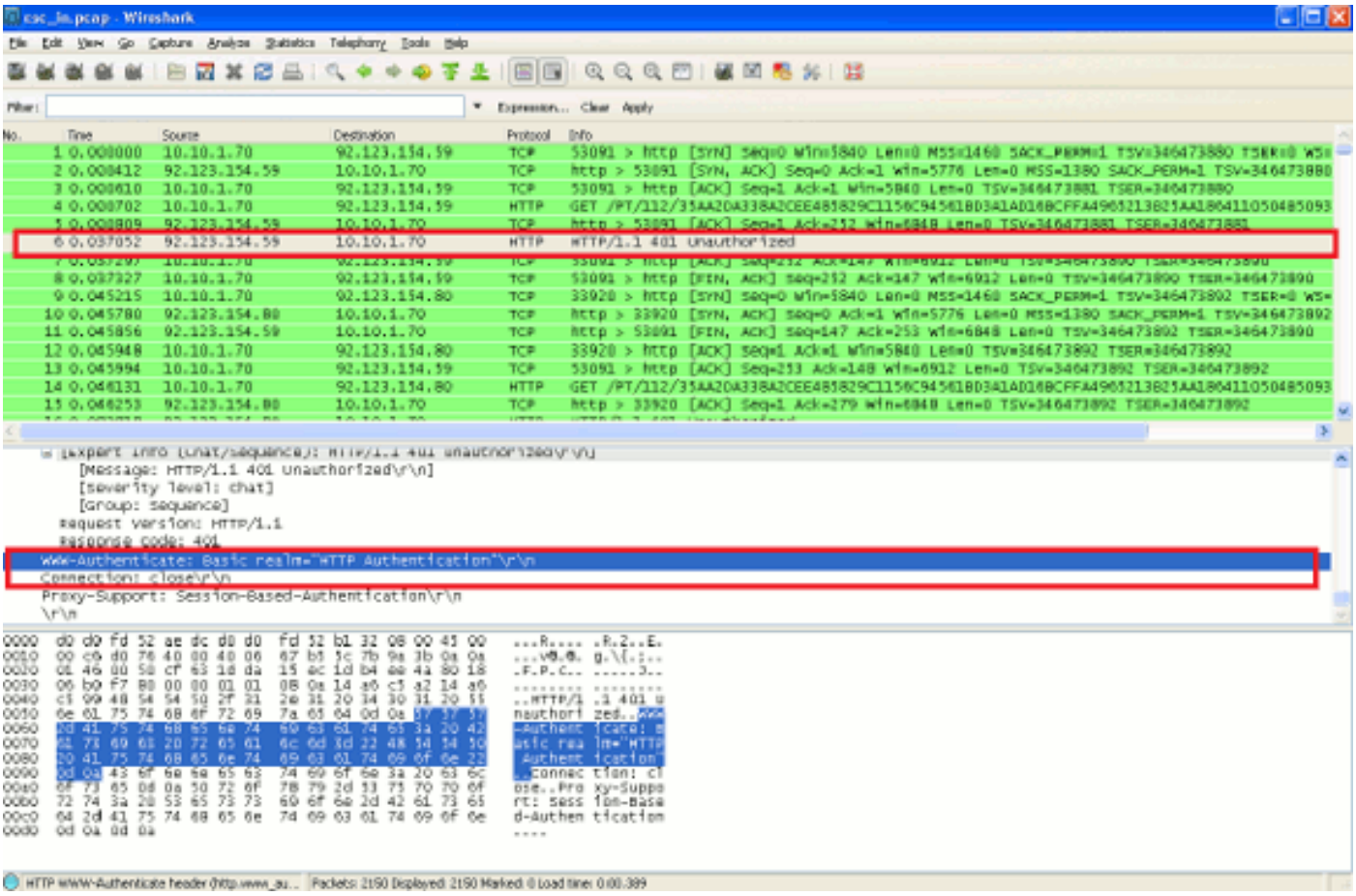
認証、許可、アカウンティング(AAA)カットスループロキシ認証は、CSCモジュールの管理ポートとインターネット間のパスにあるASAで設定されます。

問題

Webサイトは、CSC-SSMおよびCSC-SSM HTTPでURLフィルタリングされません。ログには、次のようなメッセージが表示されます。

```
2011/04/28 14:55:04 GMT+01:00  <6939-1376041904> Get URL Category returned [-1],
    with category 0 = [0] and rating = [0]
2011/04/28 14:55:04 GMT+01:00  <6939-1376041904> URLFilteringScanTask:PerformPreScanTask
    - URL rating failed, has to let it go
2011/04/28 14:55:04 GMT+01:00  <6939-1376041904> add result=1 server=
```

この問題は、ASA内部インターフェイスのCSC-SSM管理ポートとの間でパケットキャプチャが収集された後に簡単に特定できます。次の例では、内部ネットワークのIPアドレスは10.10.1.0/24、CSCモジュールのIPアドレスは10.10.1.70です。IPアドレス92.123.154.59は、Trend Micro Classificationサーバの1つのIPアドレスです。



CSCモジュールが特定のURLが分類されるカテゴリを判別する場合、CSCモジュールはTrend Micro Classificationサーバに対し、その特定のURLに関する情報を要求する必要があります。CSC-SSMは、自身の管理IPアドレスからこの接続を発信し、通信にTCP/80を使用します。上記の画面では、Trend Micro ClassificationサーバとCSC-SSMの間で3ウェイハンドシェイクが正常

に完了します。CSC-SSMはサーバにGET要求を送信し、カットスループロキシを実行するASA（またはその他のインラインネットワークデバイス）によって生成された「HTTP/1.1 401 Unauthorized」メッセージを受信します。

この例のASAでは、AAAカットスループロキシ認証が次のコマンドで設定されています。

```
aaa authentication match inside_authentication inside AUTH_SERV
access-list inside_authentication extended permit tcp any any
```

これらのコマンドを使用するには、ASAが（認証ACLの「tcp any any」が原因で）内部のすべてのユーザに対して、任意のWebサイトへの認証を要求する必要があります。CSC-SSMの管理IPアドレスは10.10.1.70で、これは内部ネットワークと同じサブネットに属し、このポリシーの対象になります。その結果、ASAはCSC-SSMを内部ネットワークの別のホストと見なし、ユーザ名とパスワードの入力にチャレンジします。残念ながら、CSC-SSMは、URLの分類のためにTrend Micro Classificationサーバに到達しようとする際に、認証を提供するように設計されていません。CSC-SSMは認証に失敗するため、ASAは「HTTP/1.1 401 Unauthorized」メッセージをモジュールに送信します。接続が閉じ、問題のURLがCSCモジュールによって正しく分類されません。

解決策

このソリューションを使用して、問題を解決してください。

CSC-SSMの管理IPアドレスを認証から除外するには、次のコマンドを入力します。

```
access-list inside_authentication extended deny tcp host 10.10.1.70 any
access-list inside_authentication extended permit tcp any any
```

CSC-SSMの管理ポートは、インターネットへの完全な障害のないアクセスを持っている必要があります。インターネットへのアクセスを妨げる可能性のあるフィルタやセキュリティチェックを通過してはなりません。また、インターネットへのアクセスを取得するために認証を行う必要はありません。

関連情報

- テクニカル サポートとドキュメント – Cisco Systems