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

目次

概要

この資料はカットスルー プロキシ認証が（ASA）または CSC-SSM のマネージメントポートとインターネット間のデバイスで適応型セキュリティ アプライアンス（ASA）ソフトウェア設定されるとき URL フィルタがコンテンツ セキュリティおよびコントロール セキュリティ サービス モジュール（CSC-SSM）で失敗するとき問題を記述したものです。

前提条件

要件

このドキュメントに関する固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たものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分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

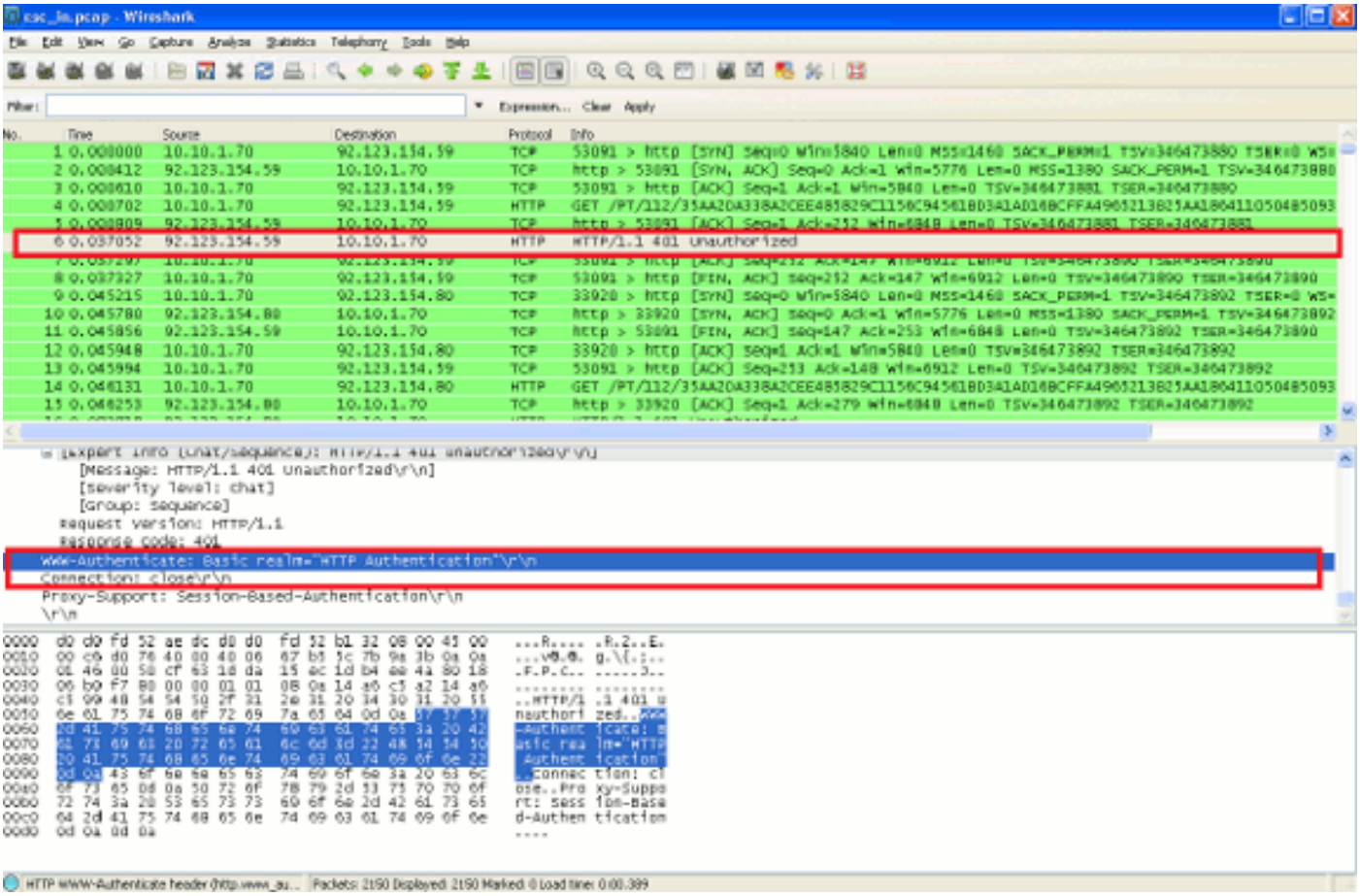
認証、許可、アカウンティング（AAA）カットスルー プロキシ認証は CSC モジュールのマネージメントポートとインターネット間のパスにある ASA で設定されます。

問題

Webサイトは CSC-SSM によって URL フィルタ処理されたおよび CSC-SSM HTTP ではないです。 ログはこれらと同じようなメッセージを表示します:

```
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=
```

問題点は容易にパケットキャプチャが ASA 内部インターフェイスの CSC-SSM のマネージメントポートに出入して集められた後明らかにされます。 下記の例では、内部ネットワーク IP アドレスは 10.10.1.0/24 であり、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 分類サーバの 1 つの IP アドレスです。



ある特定の URL はに下ることカテゴリを判別する CSC モジュール外観がその仕様 URL について情報を、CSC モジュール Trend Micro 分類サーバに頼む必要がある時。 CSC-SSM は自身の管理IPアドレスからこの接続のソースをたどり、通信のために TCP/80 を使用します。 上記の画面表示では三方ハンドシェイクは Trend Micro 分類 サーバと CSC-SSM の間で正常に完了します。 CSC-SSM はサーバに今 GET 要求を送信 し、カットスルー プロキシをする他のインライン ネッ

トワークデバイス）または ASA によって受け取ります（生成される "HTTP/1.1 401 不正 な」メッセージを。

この例 ASA で、AAA カットスルー プロキシ認証はこれらのコマンドで設定されます:

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

これらのコマンドは ASA が認証のための内部のすべてのユーザを（「認証 ACL で」あらゆる TCP による）あらゆる Webサイトに行くためにプロンプト表示するように要求します。 CSC-SSM の管理IPアドレスは 10.10.1.70 です、内部ネットワークのそれがこのポリシーに応じて今あるように同じ サブネットに属する。 その結果、ASA は CSC-SSM が内部ネットワークのありふれたホストであると考慮し、ユーザ名 および パスワードのために挑戦します。 残念ながら、CSC-SSM は URL の分類の Trend Micro 分類サーバに達することを試みるとき認証を提供するように設計されていません。 CSC-SSM が認証失敗するので、ASA はモジュールへの "HTTP/1.1 401 不正 な」メッセージを送信 します。 接続は閉じ、疑わしい URL は CSC モジュールによって正常に分類されません。

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。

認証からの CSC-SSM の管理IPアドレスを免除するこれらのコマンドを入力して下さい:

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

CSC-SSM のマネージメントポートはインターネットに完全に妨げられていないアクセスがある必要があります。 それはインターネットにアクセスを防ぐかもしれない保安検査かフィルターを通過するべきではありません。 また、それは、インターネットにアクセスを得るどうにか認証しなければならないべきではありません。

関連情報

- テクニカルサポートとドキュメント - Cisco Systems