CSC-SSM URL過濾器失敗，在串聯ASA上配置了直通代理身份驗證

目錄

簡介

本文描述當在自適應安全裝置(ASA)或CSC-SSM的管理埠與網際網路之間的裝置上配置直通代理身份驗證時，內容安全和控制安全服務模組(CSC-SSM)上的URL過濾器失敗的問題。

必要條件

需求

本文件沒有特定需求。

採用元件

本文件所述內容不限於特定軟體和硬體版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

條件/環境

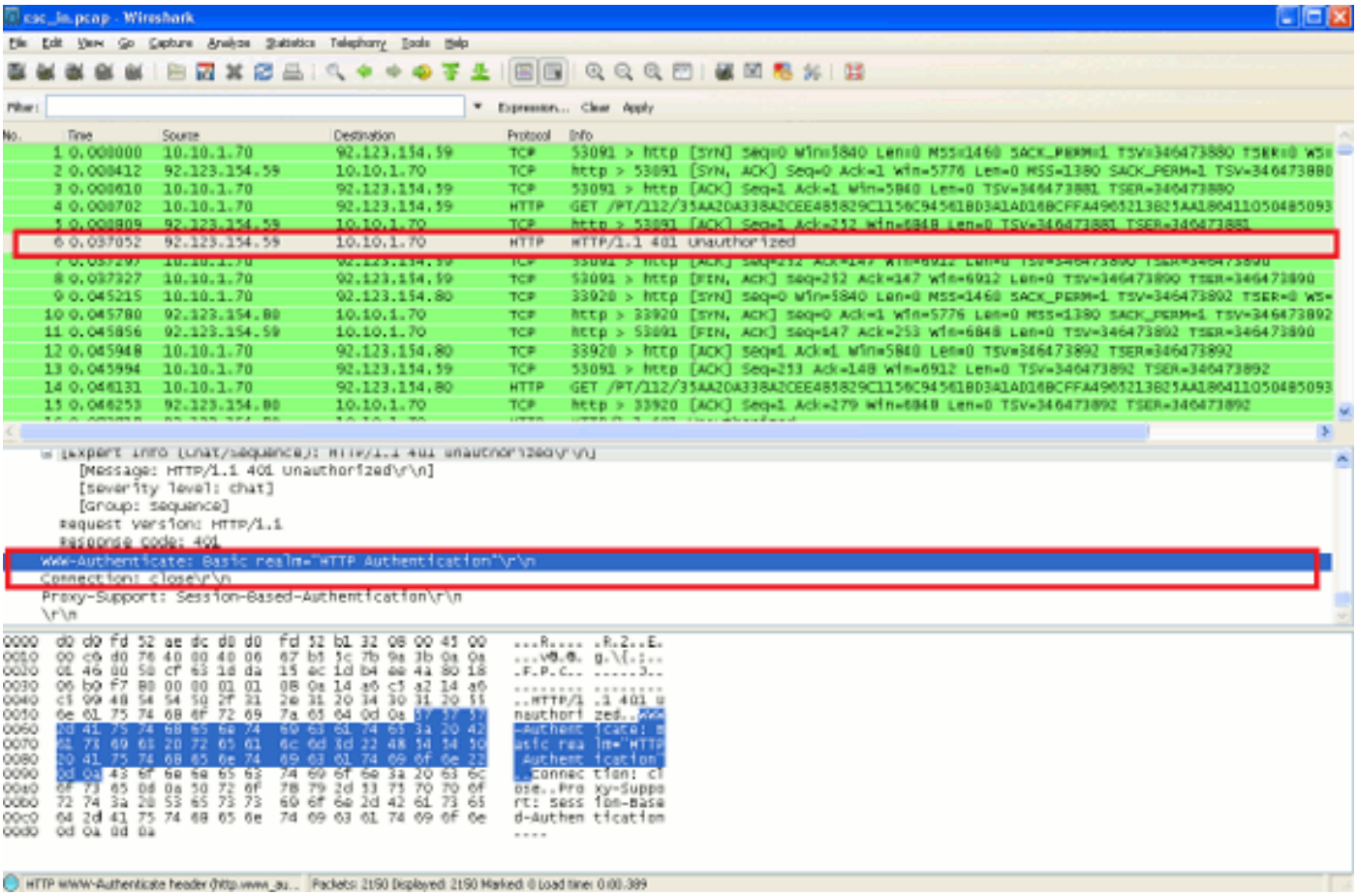
驗證、授權和記帳(AAA)直通代理驗證是在CSC模組的管理埠和網際網路之間的路徑中的ASA上配置的。

問題

網站不會通過CSC-SSM和CSC-SSM HTTP進行URL過濾。日誌顯示類似以下內容的消息：

```
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=
```

從ASA內部介面上的CSC-SSM管理埠收集資料包捕獲後，可以輕鬆發現問題。在下面的示例中，內部網路IP地址為10.10.1.0/24,CSC模組的IP地址為10.10.1.70。IP地址92.123.154.59是趨勢科技分類伺服器之一的IP地址。



當CSC模組查詢確定某個URL所屬的類別時，CSC模組必須詢問趨勢科技分類伺服器有關該特定URL的資訊。CSC-SSM從自己的管理IP地址獲取此連線，並使用TCP/80進行通訊。在上面的螢幕顯示中，趨勢科技分類伺服器和CSC-SSM之間的三次握手成功完成。CSC-SSM現在向伺服器傳送GET請求，並接收由執行直通Proxy的ASA（或其他線上網路裝置）生成的「HTTP/1.1 401未授權」消息。

在此示例中，使用以下命令配置AAA直通代理身份驗證：

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

這些命令要求ASA提示內部的所有使用者（由於身份驗證ACL中的「tcp any any」）進行身份驗證，使其進入任何網站。CSC-SSM的管理IP地址為10.10.1.70，它屬於與內部網路屬於同一子網，現

在受此策略約束。因此，ASA認為CSC-SSM只是內部網路中的另一台主機，並質詢其使用者名稱和密碼。很遺憾，CSC-SSM在嘗試訪問趨勢科技分類伺服器以分類URL時不能提供身份驗證。由於CSC-SSM身份驗證失敗，ASA向模組傳送「HTTP/1.1 401 Unauthorized」消息。連線會關閉，而且有問題的URL未被CSC模組成功分類。

解決方案

使用此解決方案可解決此問題。

輸入以下命令可免除CSC-SSM的管理IP地址進行身份驗證：

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

CSC-SSM的管理埠需要完全暢通無阻地訪問Internet。它不應通過任何可能阻止訪問Internet的過濾器或安全檢查。此外，它不應以任何方式通過身份驗證來獲取網際網路訪問許可權。

相關資訊

- 技術支援與文件 - Cisco Systems