CSC-SSM URL过滤失效与在轴向ASA配置的直通代理验证

目录

简介

本文描述问题，当URL过滤在内容安全和控制安全服务模块时(CSC-SSM)失效，当直通代理验证在可适应安全工具(ASA)时或在CSC-SSM的管理端口和互联网之间的一个设备配置。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

情况/环境

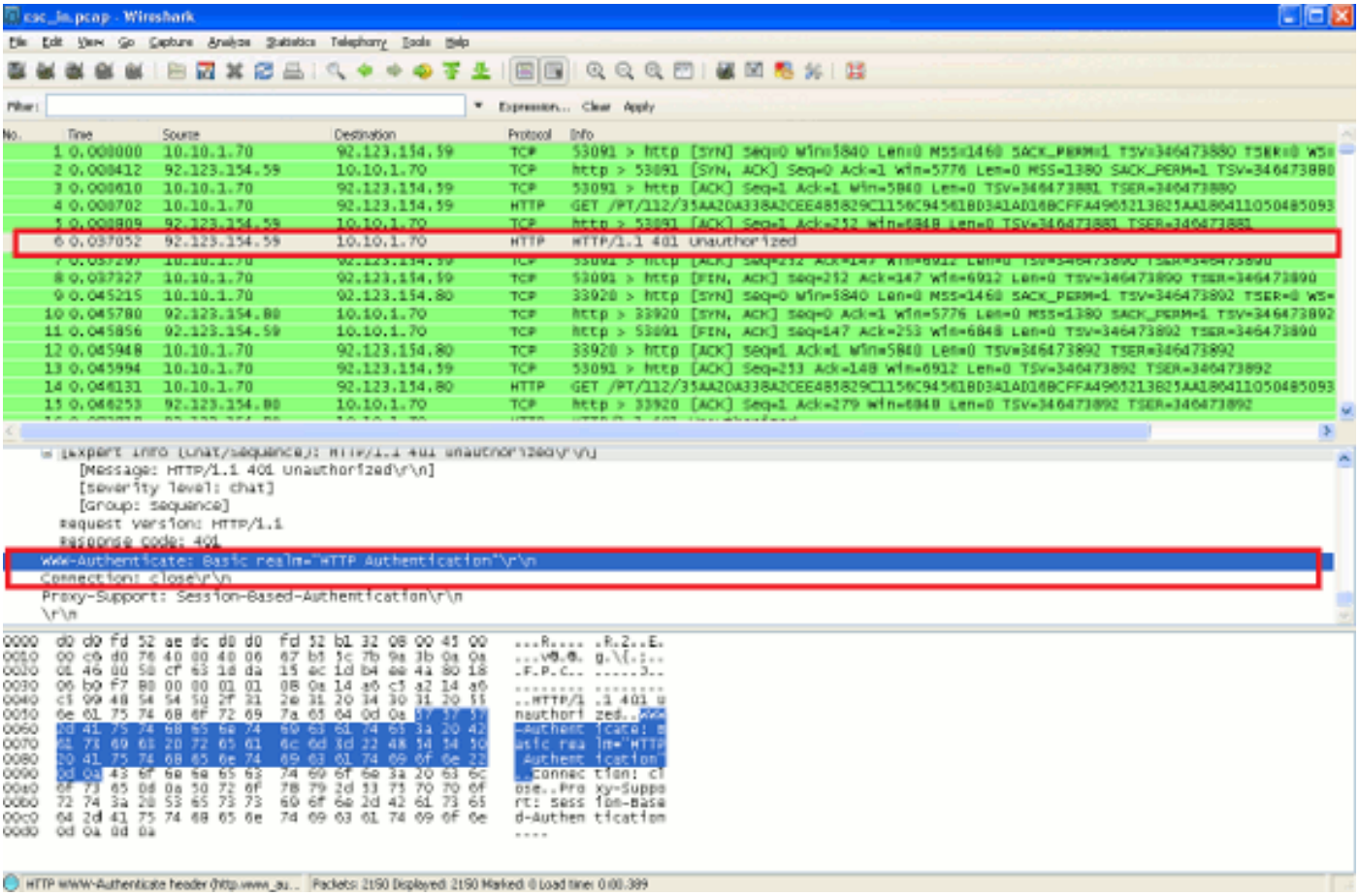
验证、授权和统计(AAA)在CSC模块的管理端口和互联网之间的路径的直通代理验证在ASA配置。

问题

网站通过CSC-SSM和CSC-SSM HTTP不是URL已过滤。日志表示消息类似于这些：

```
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=
```

在数据包捕获到/从ASA内部接口的后， CSC-SSM的管理端口收集问题容易地识别。在下面的示例中的，网络内部IP地址是10.10.1.0/24，并且CSC模块的IP地址是10.10.1.70。IP地址92.123.154.59是IP地址的其中一个Trend Micro分类服务器。



当CSC模块查找确定类别时某URL下跌到，关于该特定URL的信息， CSC模块必须要求Trend Micro分类服务器。CSC-SSM从其自己的管理IP地址来源此连接，并且使用TCP/80通信。在以上的屏幕显示，三通的握手成功地完成在Trend Micro分类服务器和CSC-SSM之间。CSC-SSM当前发送GET请求到服务器，并且收到执行直通代理ASA (或其他轴向网络设备)生成的"HTTP/1.1 401未授权的”消息。

在此示例ASA， AAA直通代理验证用这些命令配置：

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

这些命令要求ASA提示里面的所有用户(由于“tcp任何中的任一”在验证ACL)验证的能去所有网站。CSC-SSM的管理IP地址是10.10.1.70，属于相同子网和那网络内部当前受此策略支配。结果，ASA认为CSC-SSM在网络内部的另一台主机并且为用户名和密码向它挑战。不幸地，当设法到达URL的分类的时， Trend Micro分类服务器CSC-SSM没有设计提供验证。因为CSC-SSM发生故障验证， ASA传送对模块的"HTTP/1.1 401未授权的”信息。连接关闭，并且有问题的URL没有由

CSC模块顺利地分类。

解决方案

使用此解决方法解决问题。

输入这些命令豁免从验证的CSC-SSM的管理IP地址：

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

CSC-SSM的管理端口需要得以进入完全对互联网的畅通无阻的。它不应该通过也许防止对互联网的访问的任何过滤器或安全性检查。并且，它不应该必须在任何情况下，获取对互联网的访问验证。

相关信息

- 技术支持和文档 - Cisco Systems