

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](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[情况/环境](#)

[问题](#)

[解决方案](#)

[相关信息](#)

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。

The image shows a Wireshark packet capture window. The main pane displays a list of network packets. Packet 6 is highlighted with a red box and contains an unauthorized HTTP request. The details pane below shows the structure of this request, with the 'WWW-Authenticate' header highlighted in red. The hex and ASCII panes at the bottom show the raw data of the packet.

No.	Time	Source	Destination	Protocol	Info
1	0.000000	10.10.1.70	92.123.154.59	TCP	53091 > http [SYN] Seq=0 Win=65536 Len=0 MSS=1460 SACK_PERM=1 TSV=346473880 TSEQ=0 WSEQ=0
2	0.000412	92.123.154.59	10.10.1.70	TCP	http > 53091 [SYN, ACK] Seq=0 Ack=1 Win=5776 Len=0 MSS=1380 SACK_PERM=1 TSV=346473880
3	0.000810	10.10.1.70	92.123.154.59	TCP	53091 > http [ACK] Seq=1 Ack=1 Win=5840 Len=0 TSV=346473881 TSEQ=346473880
4	0.0008702	10.10.1.70	92.123.154.59	HTTP	GET /PT/112/35AA20A338A2CEE485829C1156C94561B03A1A016BCFFA4965213B25AA186411050485093
5	0.0008805	92.123.154.59	10.10.1.70	TCP	http > 53091 [ACK] Seq=1 Ack=112 Win=6848 Len=0 TSV=346473881 TSEQ=346473881
6	0.037052	10.10.1.70	92.123.154.59	HTTP	HTTP/1.1 401 Unauthorized
7	0.037297	10.10.1.70	92.123.154.59	TCP	53091 > http [ACK] Seq=233 Ack=112 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSV=346473890 TSEQ=346473890
8	0.037327	10.10.1.70	92.123.154.59	TCP	53091 > http [FIN, ACK] Seq=232 Ack=147 Win=6912 Len=0 TSV=346473890 TSEQ=346473890
9	0.045215	10.10.1.70	92.123.154.80	TCP	33920 > http [SYN] Seq=0 Win=65536 Len=0 MSS=1460 SACK_PERM=1 TSV=346473892 TSEQ=0 WSEQ=0
10	0.045780	92.123.154.80	10.10.1.70	TCP	http > 33920 [SYN, ACK] Seq=0 Ack=1 Win=5776 Len=0 MSS=1380 SACK_PERM=1 TSV=346473892
11	0.045856	92.123.154.59	10.10.1.70	TCP	http > 53091 [FIN, ACK] Seq=147 Ack=253 Win=6848 Len=0 TSV=346473892 TSEQ=346473892
12	0.045948	10.10.1.70	92.123.154.80	TCP	33920 > http [ACK] Seq=1 Ack=1 Win=5840 Len=0 TSV=346473892 TSEQ=346473892
13	0.045994	10.10.1.70	92.123.154.59	TCP	53091 > http [ACK] Seq=233 Ack=148 Win=6912 Len=0 TSV=346473892 TSEQ=346473892
14	0.046131	10.10.1.70	92.123.154.80	HTTP	GET /PT/112/35AA20A338A2CEE485829C1156C94561B03A1A016BCFFA4965213B25AA186411050485093
15	0.046253	92.123.154.80	10.10.1.70	TCP	http > 33920 [ACK] Seq=1 Ack=279 Win=6848 Len=0 TSV=346473892 TSEQ=346473892

```

=> [Expert Info (Unset/sequence): HTTP/1.1 401 Unauthorized/v\n]
[Message: HTTP/1.1 401 Unauthorized/v\n]
[Severity Level: chat]
[Group: sequence]
Request Version: HTTP/1.1
Response Code: 401
WWW-Authenticate: Basic realm="HTTP Authentication"
Connection: close/v\n
Proxy-Support: Session-Based-Authentication
/v\n
0000  d0 d0 f0 52 ae dc d0 d0 f0 52 b1 32 08 00 41 00  ...R...R.2..E.
0010  00 c6 d0 76 40 80 40 06 67 b5 7c 7b 9a 3b 0a 0a  ...v9..g.\.i..
0020  01 46 80 50 cf 63 18 da 15 ac 10 b4 6a 4a 80 18  .F.P.c...3..
0030  06 b9 f7 88 00 80 02 01 08 0a 14 a6 c3 32 14 a6  .....
0040  c5 99 4f 54 54 50 2f 31 2a 31 30 34 30 31 70 51  ..HTTP/1.1 401 U
0050  6e 61 75 74 68 6f 72 69 7a 65 64 0d 0a 87 3f 98  neathorize: 401
0060  41 75 74 68 6f 74 65 63 61 74 65 63 61 74 65 63  ..authenticatio:
0070  41 75 69 63 70 72 65 61 6c 6d 3d 23 48 14 14 10  ..sic realm="HTT
0080  30 41 73 74 68 6f 74 65 63 61 74 65 63 61 74 65  ..Authenticatio
0090  30 41 43 6f 69 69 65 65 74 69 6f 6f 6a 3a 20 63 6c  ..connection: cl
00a0  6f 73 65 68 0a 50 72 6f 78 79 3d 33 73 70 70 6f  ..ose..Pro xy-Suppo
00b0  72 74 3a 20 53 65 73 73 60 6f 6e 2d 42 61 73 65  ..rt: Sess ion-basa
00c0  6a 2d 41 75 74 68 65 6e 74 69 63 61 74 69 6f 6e  ..d-Authen tificati
00d0  0d 0a 0d 0a  ....

```

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](#)