CSC−SSM URL Filter Fails with Cut−through Proxy Authentication Configured on In−line ASA

TAC **Document ID: 115729**

Contributed by Anu Chacko and Magnus Mortensen, Cisco TAC Engineers.
Jan 24, 2013

Contents

Introduction

This document describes the problem when the URL filter fails on the Content Security and Control Security Services Module (CSC−SSM) when cut−through proxy authentication is configured on the Adaptive Security Appliance (ASA) or a device between the CSC−SSM's management port and the Internet.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

This document is not restricted to specific software and hardware versions.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Conditions/Environment

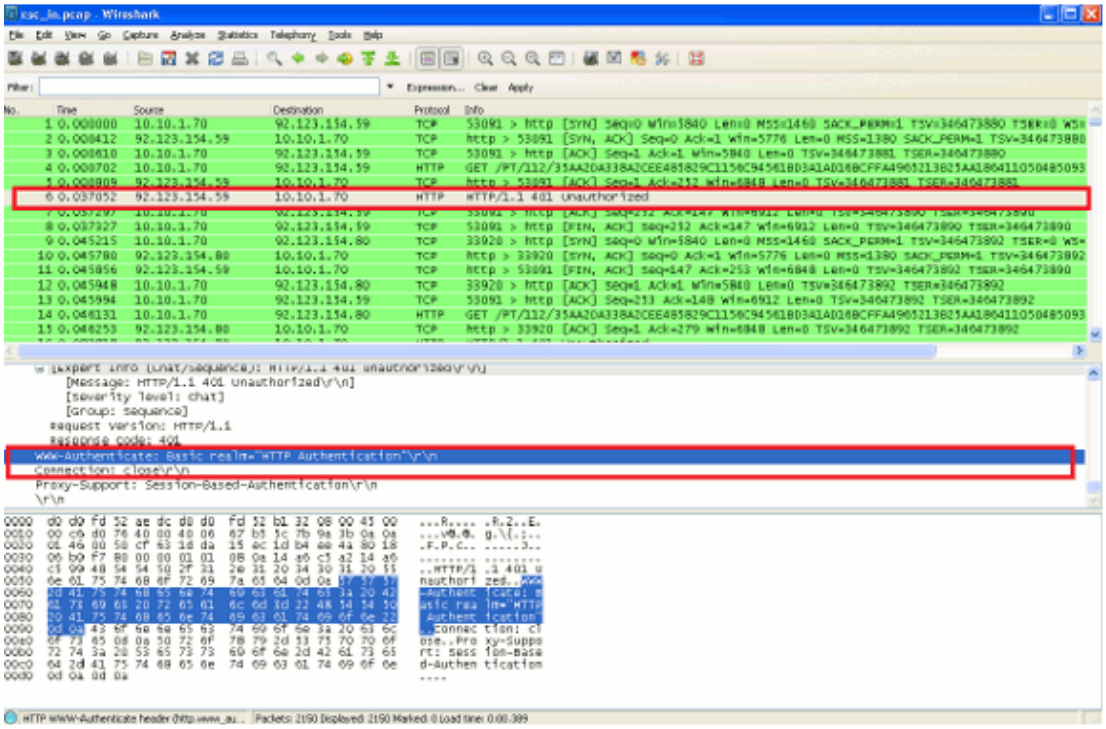
Authentication, authorization, and accounting (AAA) cut−through proxy authentication is configured on an ASA that is in the path between the CSC Module's Management port and the Internet.

Problem

The websites are not URL−filtered through the CSC−SSM and the CSC−SSM HTTP. The logs show messages similar to these:

```
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=
```

The problem is easily identified after packet captures are collected to and from the CSC−SSM's management port on the ASA inside interface. In the example below, the inside network IP address is 10.10.1.0/24 and the CSC module's IP address is 10.10.1.70. The IP address 92.123.154.59 is the IP address of one of the Trend Micro Classification servers.



When the CSC module looks to determine the category that a certain URL falls into, the CSC module must ask the Trend Micro Classification servers for information about that specific URL. The CSC−SSM sources this connection from its own management IP address and it uses TCP/80 for communication. In the screen display above, the 3−way handshake completes successfully between the Trend Micro Classification server and the CSC−SSM. The CSC−SSM now sends a GET request to the server and it receives an "HTTP/1.1 401 Unauthorized" message generated by the ASA (or other in−line network device) that does cut−through proxy.

On this example ASA, AAA cut−through proxy authentication is configured with these commands:

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

These commands require the ASA to prompt all users on the inside (due to "tcp any any" in the authentication ACL) for authentication to go to any website. The CSC−SSM's management IP address is 10.10.1.70, which belongs to the same subnet as that of the inside network is now subject to this policy. As a result, the ASA considers the CSC−SSM to be just another host in the inside network and challenges it for a username and password. Unfortunately, the CSC−SSM is not designed to provide authentication when it tries to reach the

Trend Micro Classification servers for classification of URLs. Since the CSC−SSM fails authentication, the ASA sends an "HTTP/1.1 401 Unauthorized" message to the module. The connection closes and the URL in question is not successfully classified by the CSC Module.

Solution(s)

Use this solution to solve the problem.

Enter these commands to exempt the CSC−SSM's management IP address from authentication:

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

The CSC−SSM's management port needs to have completely unimpeded access to the Internet. It should not go through any filters or security checks that might prevent access to the Internet. Also, it should not have to authenticate, in any way, to obtain access to the Internet.

Related Information

- **Technical Support & Documentation − Cisco Systems**

Updated: Jan 24, 2013 Document ID: 115729