

# Сбои фильтра URL SSM CSC со сквозной проверкой подлинности прокси-сервера, настроенной на встроенном ASA

## Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Условные обозначения](#)

[Условия/Среда](#)

[Проблема](#)

[Решение \(решения\)](#)

[Дополнительные сведения](#)

## **Введение**

Этот документ описывает проблему, когда фильтр URL отказывает на Модуле Сервисов безопасности Безопасности содержания и Контроля (SSM CSC), когда сквозная проверка подлинности прокси-сервера настроена на Устройстве адаптивной защиты (ASA) или устройстве между портом управления SSM CSC и Интернетом.

## **Предварительные условия**

### **Требования**

Для этого документа отсутствуют особые требования.

### **Используемые компоненты**

Настоящий документ не имеет жесткой привязки к каким-либо конкретным версиям программного обеспечения и оборудования.

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

### **Условные обозначения**

[Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.](#)

## Условия/Среда

Сквозная проверка подлинности прокси-сервера аутентификации, авторизации и учета (AAA) настроена на ASA, который находится в пути между Портом управления Модуля CSC и Интернетом.

## Проблема

Веб-сайты не проникаются URL SSM CSC и HTTP SSM CSC. Журналы показывают сообщения, подобные им:

```
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=
```

Проблема легко определена после того, как захваты пакета собраны к и от порта управления SSM CSC на Внутреннем интерфейсе ASA. В примере ниже, IP-адрес внутренней сети является 10.10.1.0/24, и IP-адрес модуля CSC 10.10.1.70. IP-адресом 92.123.154.59 является IP-адрес одного из серверов Классификации Trend Micro.

The screenshot shows a Wireshark capture of network traffic. The packet list pane highlights a packet with the following details:

No.	Time	Source	Destination	Protocol	Info
6	0.057052	92.123.154.59	10.10.1.70	HTTP	HTTP/1.1 401 Unauthorized

The packet bytes pane shows the raw data of the HTTP response:

```
0000 00 d0 fd 52 ae dc d0 d0 fd 52 b1 32 08 00 43 00 ...R....R.Z..E.  
0010 00 c9 d0 78 40 80 40 08 67 bf 3c 7b 9a 3b 0a 0a ...v0.0. g.\.1...  
0020 01 46 80 58 cf 63 18 0a 15 ec 1d b4 ee 4a 80 18 ..F.P.C....3...  
0030 06 b0 f7 80 00 80 01 01 08 0a 14 a5 c5 a2 14 a5 .....  
0040 c1 99 48 54 94 50 2f 31 2e 31 20 34 30 31 20 51 ..HTTP/1.1 401 u  
0050 6e 01 75 74 68 6f 72 65 7a 65 64 0d 0a 17 17 51 nautho rized...  
0060 00 41 75 74 68 65 6a 74 69 65 61 74 65 34 20 42 -Authenticat: s  
0070 0a 73 69 65 20 72 65 61 6c 6d 10 22 48 34 34 36 asic rea in= HTTP  
0080 10 41 75 74 68 65 6e 74 69 63 61 74 69 6f 6e 23 -Authenticat: s  
0090 03 03 42 5f 68 65 65 63 74 69 6f 69 3a 20 63 5c ..Connct ion: c  
00a0 0f 73 65 68 68 30 75 6f 78 79 61 33 75 70 70 6f as..Pro xy-Suppo  
00b0 72 74 3a 28 53 65 73 73 60 6f 6e 2d 42 61 73 65 rt: sess ion-Basa  
00c0 64 2d 41 75 74 68 65 6e 74 69 63 61 74 69 6f 6e d-Authen tication  
00d0 0d 0a 0d 0a .....
```

Когда модуль CSC надеется определить категорию, в которую падает определенный URL, модуль CSC должен спросить серверы для получения информации Классификации Trend Micro о том определенном URL. SSM CSC получает это соединение от своего собственного

управления IP-адресами, и это использует TCP/80 для связи. В изображении на экране выше, трехстороннее квитирование завершает успешно между сервером Классификации Trend Micro и SSM CSC. SSM CSC теперь отправляет запрос GET к серверу, и это получает "HTTP/1.1 401 Неавторизованное" сообщение, генерируемое ASA (или другое встроенное сетевое устройство), который делает сквозной прокси.

На ASA данного примера AAA сквозная проверка подлинности прокси-сервера настроена с этими командами:

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

Эти команды требуют, чтобы ASA побудил всех пользователей на внутренней части (из-за "tcp любой любой" в опознавательном ACL) для аутентификации переходить к любому веб-сайту. Управление IP-адресами SSM CSC 10.10.1.70, который принадлежит той же подсети, поскольку та из внутренней сети теперь подвергается этой политике. В результате ASA полагает, что SSM CSC просто другой хост во внутренней сети, и бросает вызов ему для имени пользователя и пароля. К сожалению, SSM CSC не разработан для обеспечения аутентификации, когда это пытается достигнуть серверов Классификации Trend Micro для классификации URL. Так как SSM CSC отказывает аутентификацию, ASA передает "HTTP/1.1 401 Неавторизованное" сообщение к модулю. Завершения соединения и рассматриваемый URL успешно не классифицированы Модулем CSC.

## [Решение \(решения\)](#)

Используйте следующее решение проблемы.

Введите эти команды для освобождения управления IP-адресами SSM CSC от аутентификации:

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

Порт управления SSM CSC должен иметь абсолютно беспрепятственный доступ к Интернету. Это не должно проходить фильтры или проверки безопасности, которые могли бы предотвратить доступ к Интернету. Кроме того, этому не придется аутентифицироваться, ни в каком случае, для получения доступа к Интернету.

## [Дополнительные сведения](#)

- [Cisco Systems – техническая поддержка и документация](#)