ASDM无法正常登陆ASA

目录

硬件平台

ASA 5500 系列

软件版本

所有版本

问题描述

用户有一台新上线的ASA 5585 防火墙,发现在日常使用维护中，少部分用户可以正常的使用ASDM登陆ASA进行配置和管理，大部分用户的电脑不能够正常的登陆ASDM。 有问题的用户在IE浏览器,敲入ASA的地址以后没有任何反应，页面呈现空白页。

问题分析思路

1. 确认防火墙上的相关配置是否无误。
2. 能够访问ASDM 和不能够访问ASDM的电脑是否是同一网段,设备是否有区别。
3. 在用户的笔记本上抓包分析，能够访问ASDM和不能访问ASDM分析不同点。
4. 查看ASA上相关的log 信息。

故障排除步骤

1. 确实配置

   show run http
   检查交换机上关于http 配置，是否在正确的接口上调用了命令，是否允许相应的网络访问.

```
ciscoasa(config)# show run http
http server enable
http 10.1.0.0 255.255.0.0 outside
http 0.0.0.0 0.0.0.0 inside
```

   用户的inside 接口确实是放行了所有的地址来访问ASA.

   show run asdm
   检查ASDM 调用asdm image 的情况。

```
ciscoasa(config)# show run asdm
asdm image disk0:/asdm-711-52.bin
```

```
no asdm history enable
```

show asp table socket

查看对应的接口是否在监听443端口

```
ciscoasa(config)# show asp table socket
Protocol  Socket    Local Address               Foreign Address         State
TCP       0000f1bf  10.75.61.192:23             0.0.0.0:*               LISTEN
SSL       0001d87f  10.14.48.54:443             0.0.0.0:*               LISTEN
SSL       0001e97f  10.193.11.4:443             0.0.0.0:*               LISTEN ciscoasa(config)#
```

从配置上分析配置都是正确的配置，而且相应的接口也在监听TCP对应的443端口。

2. 询问用户能够访问ASDM 和不同够访问ASDM 的主机是否在同一个网段？

网管ASA的PC都是同一交换机上同一VLAN的主机。

从网络路径上分析,所有PC经过的路径都是相同的，排错网络差异的问题。

3. 抓包分析。

有问题的数据包

```
 66 50277 > https [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
 58 https > 50277 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1380
 54 50277 > https [ACK] Seq=1 Ack=1 Win=64860 Len=0
158 Client Hello
 54 https > 50277 [ACK] Seq=1 Ack=105 Win=32664 Len=0
 54 [TCP Window Update] https > 50277 [ACK] Seq=1 Ack=105 Win=32768 Len=0
 61 Alert (Level: Fatal, Description: Handshake Failure)
 54 https > 50277 [RST] Seq=8 Win=32768 Len=0
```

有问题的数据包

```
 62 bfd-control > https [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1
 58 https > bfd-control [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1380
 54 bfd-control > https [ACK] Seq=1 Ack=1 Win=65535 Len=0
124 Client Hello
 54 https > bfd-control [ACK] Seq=1 Ack=71 Win=32698 Len=0
 54 [TCP Window Update] https > bfd-control [ACK] Seq=1 Ack=71 Win=32768 Len=0
574 Server Hello, Certificate, Server Hello Done
244 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
 54 https > bfd-control [ACK] Seq=521 Ack=261 Win=32578 Len=0
 54 [TCP Window Update] https > bfd-control [ACK] Seq=521 Ack=261 Win=32768 Len=0
105 Change Cipher Spec, Encrypted Handshake Message
```

对比两个样本的数据包发现，有问题的PC在于ASA在SSL 建立的过程中失败了。

SSL Handshake Failure (40)

4. 在ASA上打开log功能，记录在用户登录ASDM过程中的SSL建立过程的log。

```
ciscoasa(config)# show run logging
logging enable
logging class ssl buffered debugging
ciscoasa(config)#
```

使用 logging class 命令可以使ASA只存储特定类别的log。

```
ciscoasa(config)# show logging
Syslog logging: enabled

%ASA-6-725001: Starting SSL handshake with client inside:192.188.1.235/49972 for TLSv1
session.
%ASA-7-725010: Device supports the following 1 cipher(s).
%ASA-7-725011: Cipher[1] : DES-CBC-SHA
%ASA-7-725008: SSL client inside:192.188.1.235/49972 proposes the following 8 cipher(s).
%ASA-7-725011: Cipher[1] : AES128-SHA
```

```
%ASA-7-725011: Cipher[2] : AES256-SHA
%ASA-7-725011: Cipher[3] : RC4-SHA
%ASA-7-725011: Cipher[4] : DES-CBC3-SHA
%ASA-7-725011: Cipher[5] : DHE-DSS-AES128-SHA
%ASA-7-725011: Cipher[6] : DHE-DSS-AES256-SHA
%ASA-7-725011: Cipher[7] : EDH-DSS-DES-CBC3-SHA
%ASA-7-725011: Cipher[8] : RC4-MD5
%ASA-7-725014: SSL lib error. Function: SSL3_GET_CLIENT_HELLO Reason: no shared cipher
```

可以看到当前ASA 就支持一种加密算法DES-CBC-SHA, 而这仅有的一种加密方式又不在浏览器支持的范围内，所有PC无法与ASA完成SSL的握手连接。

5. 查看当前ASA SSL的配置，并添加加密方式。

```
ciscoasa(config)# show run all ssl
ssl server-version any
ssl client-version any
ssl encryption des-sha1
ssl certificate-authentication fca-timeout 2
```

发现只有1种加密方式，这时候我们尝试去添加更多的加密算法。 通过show version 检查ASA是不是有3DES-AES 加密的license. 如果没有需要申请相应的license。

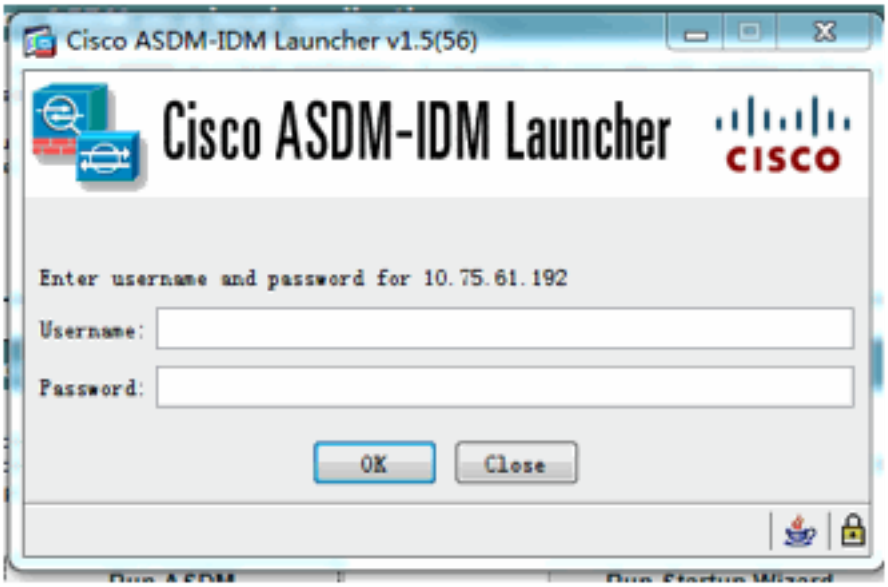
```
ciscoasa(config)# show version

VPN-DES                           : Enabled        perpetual
VPN-3DES-AES                      : Enabled        perpetual
```

我们给ASA添加其他的加密算法。

```
ciscoasa(config)# ssl encryption 3des-sha1 des-sha1 aes128-sha1 aes256-sha1
```

6. 用户可以成功的登陆ASDM



经验总结

1. 要分析ASDM登陆ASA的整个过程。
   先是https网页登陆进入，然后是允许java 程序。
2. 在日常的troubleshooting 中一定要注意观察设备的系统日志。
   有时候日志能够帮我们快速准确的定位问题。