Windows7 无法打开ASA SSL VPN 首页

目录

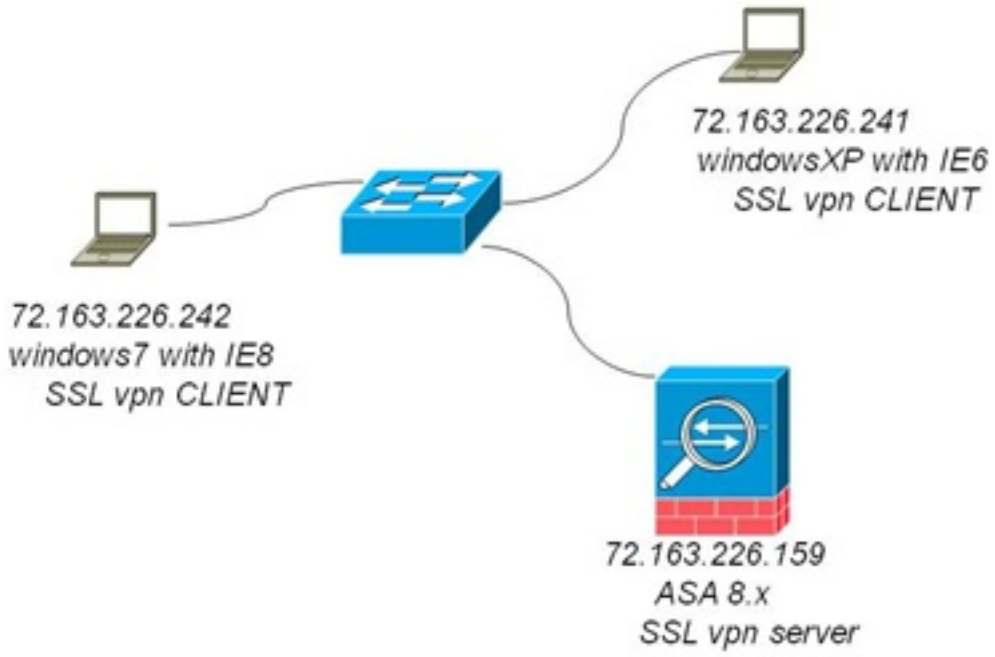
背景

随着windows 7 操作系统的普及，伴随着新功能出现的同时，一些与其它厂商的兼容性问题也就出现了，下面我们就来讲述一个Cisco ASA 防火墙SSL VPN 与 windows7 的兼容性实际案例。

硬件及软件要求

SSLVPN 客户端： Windows XP SP2 with IE6 ,Windows7 with IE8
SSL VPN 服务器端： ASA5500 8.x with 3DES license

网络拓扑



问题描述

客户反映Windows7 无法打开ASA SSL VPN 登陆页面 ，如图4.1 。 但WindowsXP 一切正常，如图4.2。

图4.1.

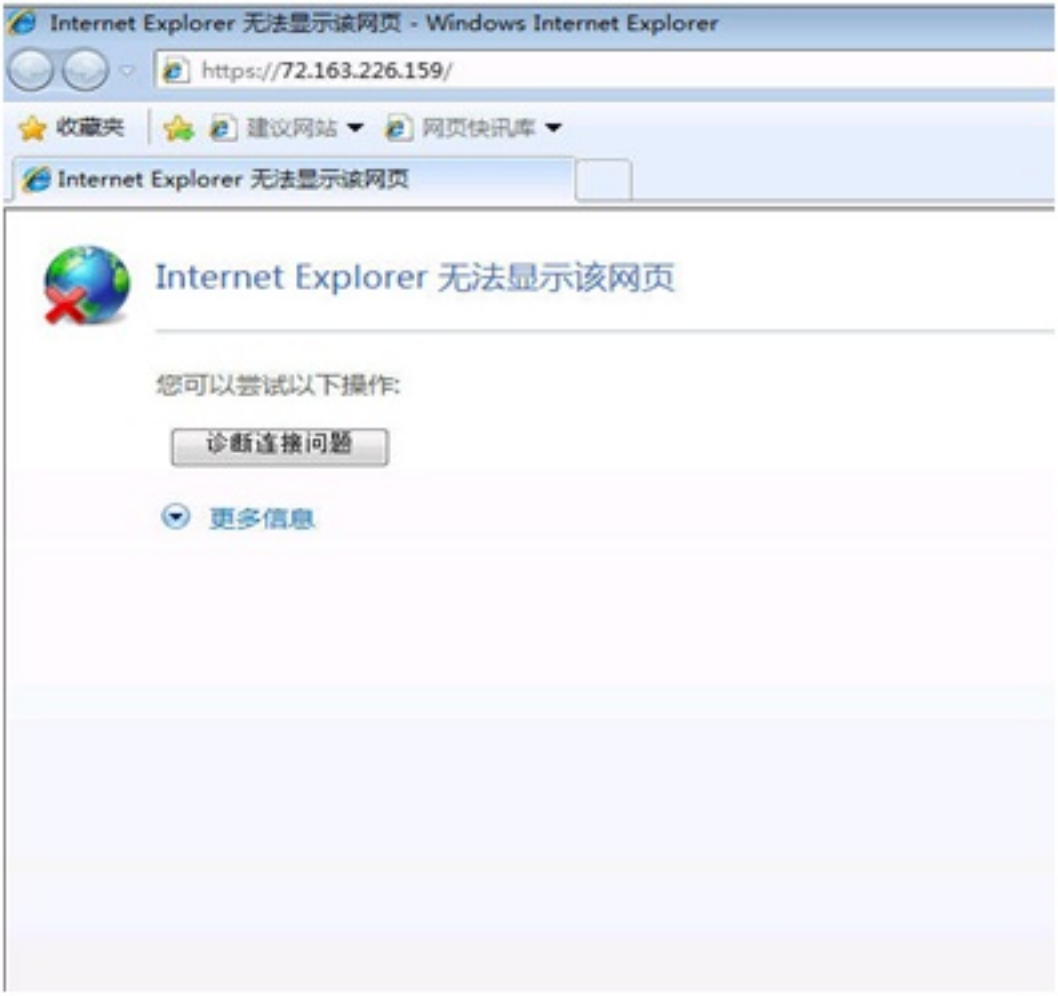
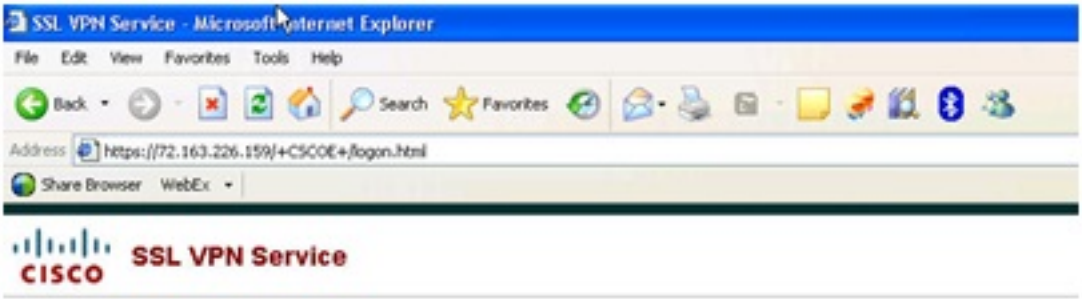


图4.2.



故障处理

出现此类问题时，我建议用户首先收集log 文件来找到蛛丝马迹，这也是我们处理问题解决问题的很好的敲门砖。

ciscoasa(config)#logging buffered debugging “ 将日志级别调成debugging 级别。”
ciscoasa(config)#logging buffer-size 1048576 “将日志buffer 容量扩大，已缓存更多的信息。”
ciscoasa(config)#logging on

此时让客户重新尝试用windows7 登陆ASA SSL VPN 首页，通过日志我们可以看到如下信息，请注意我将关键信息用粗体字标出

```
ciscoasa(config)#show log
%ASA-6-302013: Built inbound TCP connection 3 for outside:72.163.226.242/59371 (
72.163.226.242/59371) to identity:72.163.226.159/443 (72.163.226.159/443)
%ASA-6-725001: Starting SSL handshake with client outside:72.163.226.242/58911 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 outside:72.163.226.242/58911 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
%ASA-6-302014: Teardown TCP connection 77 for outside:72.163.226.242/58911
to identity:72.163.226.159/443 duration 0:00:00 bytes 7 TCP Reset-I
```

同过以上信息我们可以注意到SSL 的加密算法的协商在ASA与Windows7 之间出现了不匹配。

下面我们需要通过show ssl 命令来确定ASA SSL 加密算法情况。通过下面的输出信息我们看到，只有DES-SHA1 加密算法被开启，而其它加密算法均已关闭。我将关键字用粗体字标出。

```
ciscoasa# show ssl
Accept connections using SSLv2, SSLv3 or TLSv1 and negotiate to SSLv3 or TLSv1
Start connections using SSLv3 and negotiate to SSLv3 or TLSv1
Enabled cipher order: des-sha1
Disabled ciphers: 3des-sha1 rc4-md5 rc4-sha1 aes128-sha1 aes256-sha1 null-sha1
--omitted--
```

到此时我们似乎已经有点眉目了，还记得吗？客户还曾经反映过WindowsXP 是没有任何问题的，那么我们让客户在用WindowsXP 登陆以下SSL VPN首页。我们再次收集一下日志。我将重点用粗体字标出。

```
ciscoasa#show log
%ASA-6-725001: Starting SSL handshake with client outside:72.163.226.170/4301 fo
r 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 outside:72.163.226.170/4301 proposes the following 8 c
ipher(s).
%ASA-7-725011: Cipher[1] : RC4-MD5
%ASA-7-725011: Cipher[2] : RC4-SHA
%ASA-7-725011: Cipher[3] : DES-CBC3-SHA
%ASA-7-725011: Cipher[4] : DES-CBC-SHA
%ASA-7-725011: Cipher[5] : EXP-RC4-MD5
%ASA-7-725011: Cipher[6] : EXP-RC2-CBC-MD5
%ASA-7-725011: Cipher[7] : EDH-DSS-DES-CBC3-SHA
%ASA-7-725011: Cipher[8] : EDH-DSS-DES-CBC-SHA
%ASA-7-725012: Device chooses cipher : DES-CBC-SHA for the SSL session with clie
nt outside:72.163.226.170/4301
%ASA-6-725002: Device completed SSL handshake with client outside:72.163.226.170
/4300
```

目前问题根源已经明确，在协商SSL 加密算法的过程中， ASA SSL加密组只接受DES 加密， 承载了IE8 的Windows7 关闭了DES SSL加密。而承载IE6 的WindowsXP 是打开SSL DES加密的。

到目前为止我们知道了问题的根源，那么我们就开始解决它:

我们要知道SSL 加密组在ASA上是可定制的，具体命令是 ssl encryption

```
ciscoasa#show log
%ASA-6-725001: Starting SSL handshake with client outside:72.163.226.170/4301 fo
r 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 outside:72.163.226.170/4301 proposes the following 8 c
ipher(s).
%ASA-7-725011: Cipher[1] : RC4-MD5
%ASA-7-725011: Cipher[2] : RC4-SHA
%ASA-7-725011: Cipher[3] : DES-CBC3-SHA
%ASA-7-725011: Cipher[4] : DES-CBC-SHA
%ASA-7-725011: Cipher[5] : EXP-RC4-MD5
%ASA-7-725011: Cipher[6] : EXP-RC2-CBC-MD5
%ASA-7-725011: Cipher[7] : EDH-DSS-DES-CBC3-SHA
%ASA-7-725011: Cipher[8] : EDH-DSS-DES-CBC-SHA
%ASA-7-725012: Device chooses cipher : DES-CBC-SHA for the SSL session with clie
nt outside:72.163.226.170/4301
%ASA-6-725002: Device completed SSL handshake with client outside:72.163.226.170
/4300
```

既然有这个命令那么我们就看看客户到底定制了哪个SSL加密组：

```
ciscoasa(config)# show run ssl
ssl encryption des-sha1
```

果然如此，客户手工制定了SSL加密组在ASA ，Ok 我们就制定一组IE8 支持的加密组吧

```
ciscoasa(config)# ssl encryption aes128-sha1
ciscoasa(config)# show ssl
Accept connections using SSLv2, SSLv3 or TLSv1 and negotiate to SSLv3 or TLSv1
Start connections using SSLv3 and negotiate to SSLv3 or TLSv1
```

```
Enabled cipher order: aes128-sha1
Disabled ciphers: 3des-sha1 des-sha1 rc4-md5 rc4-sha1 aes256-sha1 null-sha1
--omitted--
```

再让客户用Windows7 /IE8 尝试登陆一次ASA SSL VPN首页 。 成功登陆，问题解决。 让我们看看日志的体现：

```
%ASA-6-725001: Starting SSL handshake with client outside:72.163.226.242/61132 f
or TLSv1 session.
%ASA-7-725010: Device supports the following 1 cipher(s).
%ASA-7-725011: Cipher[1] : AES128-SHA
%ASA-7-725008: SSL client outside:72.163.226.242/61132 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-7-725012: Device chooses cipher : AES128-SHA for the SSL session with clien
t outside:72.163.226.242/61132
%ASA-6-725002: Device completed SSL handshake with client outside:72.163.226.242
/61132
```

在这里我要提一下ASA上SSL encryption 这条命令，默认情况下不需要刻意指定加密组，加密组会ASA 会去尝试匹配任何一个它支持的加密组，这是很多朋友没有注意的问题

关于此命令的更详细信息请参见以下连接：

http://www.cisco.com/en/US/docs/security/asa/asa80/command/reference/s8.html#wp1406272

结论

在承载了IE8 的Windows7中SSL加密组对于DES是关闭的，而在承载IE6 的WindowsXP中此SSL加密标准是开启的，而客户在ASA上人为限定了SSL 加密组只接受DES协商，这才导致了此次故障的发生。将ASA SSL 加密组设置为IE8 支持的SSL加密标准将可以解决此问题。