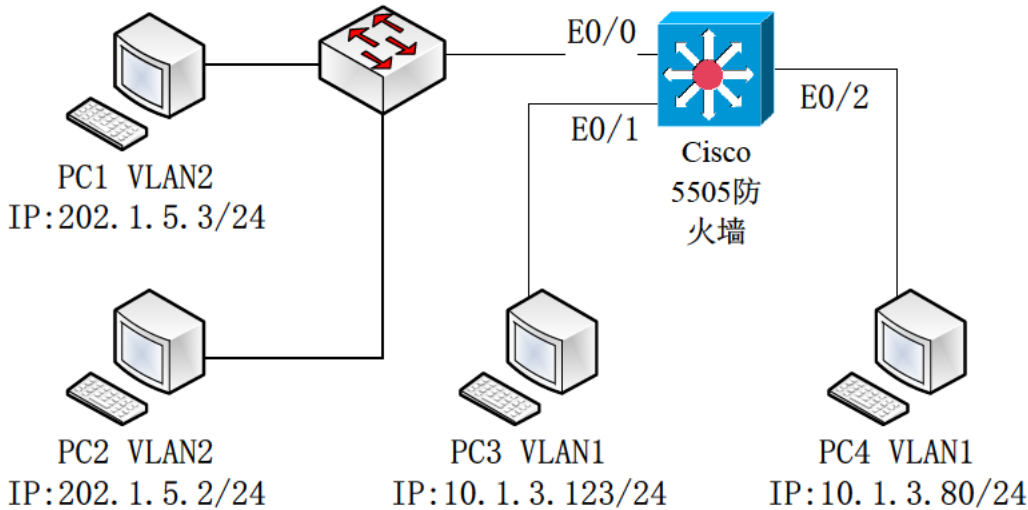


# 计算机网络专题实验现场检查单 7

实验名称：防火墙与 SSLVPN 实验

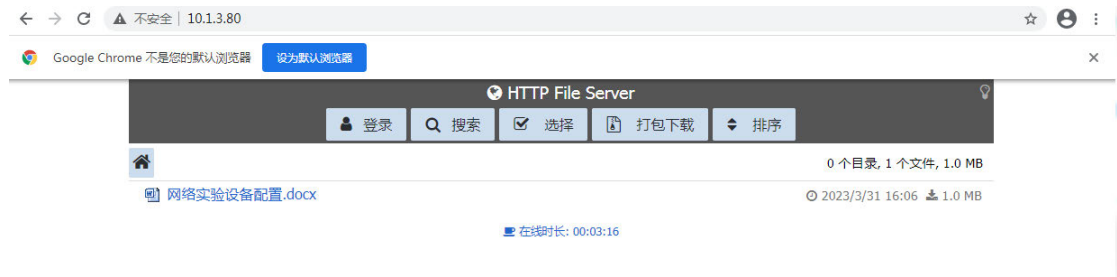
时间： 2023 年 4 月 5 日 早 ☐ 午 ☒ 晚 ☐

组号	■	实验位	■	控制器地址	■
姓名	■	■	■	郭松坚	■
实验组网图	<p>【可以手画拍照。拓扑图中，请标明设备编号、端口号、vlan 号、IP 地址、掩码等】</p>  <p>PC1 VLAN2 IP:202. 1. 5. 3/24</p> <p>PC2 VLAN2 IP:202. 1. 5. 2/24</p> <p>PC3 VLAN1 IP:10. 1. 3. 123/24</p> <p>PC4 VLAN1 IP:10. 1. 3. 80/24</p> <p>Cisco 5505 防火墙</p>				
实验结果	<p>1. 本组 CISCO ASA5505 中 Vlan 的划分、命名及端口分配方案是： VLAN 划分：CISCO ASA5505 防火墙的 VLAN 被划分为 VLAN1 与 VLAN2； 命名：PC1（IP 地址：202.1.5.3/24）与 PC2（IP 地址：202.1.5.2/24）位于 VLAN2， PC3（IP 地址：10.1.3.123/24）与 PC4（IP 地址：10.1.3.80/24）位于 VLAN1； 端口分配方案：CISCO ASA5505 防火墙的 E0/0 端口连接交换机，交换机与 PC1、PC2 相连；E0/1 端口连接 PC3；E0/2 端口连接 PC4。</p> <p>2. CISCO ASA5505 内网 DHCP 服务器的 IP 范围是： 10.1.3.2-10.1.3.33</p> <p>3. SSL VPN 用户地址池的名称和地址范围是： 地址池的名称：ssluser 地址范围：10.10.10.1-10.10.10.10</p> <p>4. 创建的 SSL VPN 用户名是： vpnuser1 和 vpnuser2</p>				

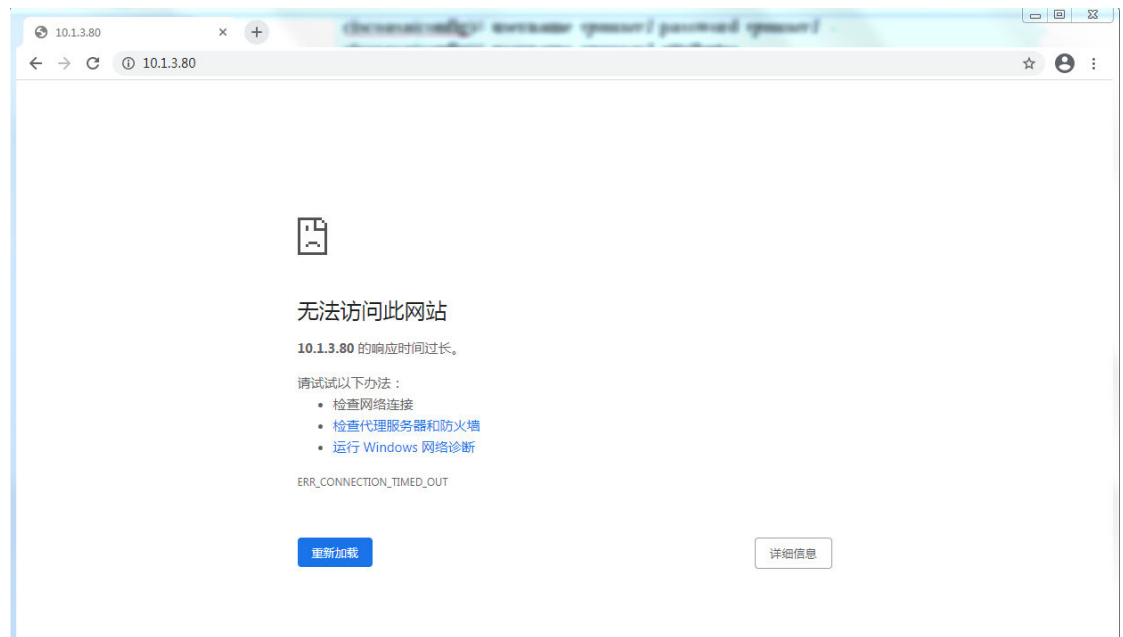
5. 所配置的防火墙测试方案及结果是：

1) 步骤 8:

本机 PC4 及内部 PC3 均能正常访问 Web 服务：



外部 PC2 无法访问 Web 服务：



2) 步骤 9:

①在 VPN 软件环境下，分别以客户端模式和 Web 模式访问内部 Web 资源服务器，并运行 ping 测试网络连通性（比如在 PC1 ping PC4）。

客户端模式和 Web 模式均能访问内部 Web 资源服务器，执行 PC1 ping PC4 的结果如下：

```
C:\Users\Administrator>ping 10.1.3.80

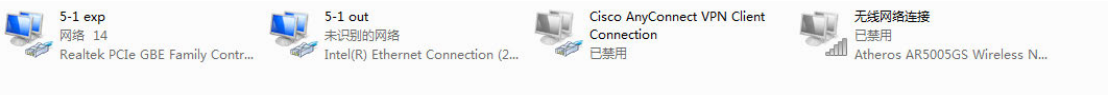
正在 Ping 10.1.3.80 具有 32 字节的数据:
来自 10.1.3.80 的回复: 字节=32 时间=1ms TTL=128
来自 10.1.3.80 的回复: 字节=32 时间=1ms TTL=128
来自 10.1.3.80 的回复: 字节=32 时间=1ms TTL=128
来自 10.1.3.80 的回复: 字节=32 时间=1ms TTL=128

10.1.3.80 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
    往返行程的估计时间(以毫秒为单位):
        最短 = 1ms, 最长 = 1ms, 平均 = 1ms
```

②查看本地网卡配置，参考路由表信息，分析外部 PC 如何通过 VPN 安全访问 10.1.3.x 上的资源。

(1) Web 模式：

PC1 本地网卡配置如下：通过 Web 模式连接 VPN 时，PC 是通过原先使用的网卡进行连接的，因此在网卡配置里虚拟网卡显示已禁用。



PC1 本地路由信息如下：

```
C:\Users\Administrator>netstat -r
=====
接口列表
16...f0 bf 97 e5 60 ae .....Realtek PCIe GBE Family Controller #2
13...48 4d 7e a8 1d e1 .....Intel(R) Ethernet Connection (2) I219-LM
1.....Software Loopback Interface 1
17...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #2
15...00 00 00 00 00 00 00 e0 Microsoft 6to4 Adapter
18...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #3
19...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #4
=====

IPv4 路由表
=====
活动路由:
网络目标      网络掩码      网关      接口      跃点数
0.0.0.0      0.0.0.0      0.0.0.0      202.1.5.1      202.1.5.3      276
127.0.0.0      255.0.0.0      255.0.0.0      在链路上      127.0.0.1      306
127.0.0.1      255.255.255.255      255.255.255.255      在链路上      127.0.0.1      306
127.255.255.255      255.255.255.255      255.255.255.255      在链路上      127.0.0.1      306
192.168.0.0      255.255.0.0      192.168.0.1      192.168.0.51      276
192.168.0.0      255.255.255.0      在链路上      192.168.0.51      276
192.168.0.51      255.255.255.255      在链路上      192.168.0.51      276
192.168.0.255      255.255.255.255      在链路上      192.168.0.51      276
202.1.5.0      255.255.255.0      在链路上      202.1.5.3      276
202.1.5.3      255.255.255.255      在链路上      202.1.5.3      276
202.1.5.255      255.255.255.255      在链路上      202.1.5.3      276
224.0.0.0      240.0.0.0      在链路上      127.0.0.1      306
224.0.0.0      240.0.0.0      在链路上      202.1.5.3      276
224.0.0.0      240.0.0.0      在链路上      192.168.0.51      276
255.255.255.255      255.255.255.255      在链路上      127.0.0.1      306
255.255.255.255      255.255.255.255      在链路上      202.1.5.3      276
255.255.255.255      255.255.255.255      在链路上      192.168.0.51      276
=====
永久路由:
网络地址      网络掩码      网关地址      跃点数
192.168.0.0      255.255.0.0      192.168.0.1      默认
0.0.0.0      0.0.0.0      202.1.5.1      默认
=====
```

Web 模式里，PC 和防火墙进行认证后，PC 向内网发送数据时只需要向防火墙发送数据包即可，防火墙会根据数据包内的 SSL 加密信息 转发给内网的 PC。

(2)客户端模式：

PC1 本地网卡配置如下：通过客户端连接 VPN 时，会产生一个虚拟网卡，即下图中的 Cisco AnyConnect VPN Client Connection，通过该网卡获得一个内网的 VPN 用户地址，即网卡内的 IP 地址 10.10.10.2。



PC1 本地路由信息如下:

```
C:\Users\Administrator>netstat -r
=====
接口列表
21...00 05 9a 3c 7a 00 .....Cisco AnyConnect VPN Virtual Miniport Adapter for
Windows x64
16...f0 bf 97 e5 60 ae .....Realtek PCIe GBE Family Controller #2
13...48 4d 7e a8 1d e1 .....Intel(R) Ethernet Connection (2) I219-LM
1.....Software Loopback Interface 1
20...00 00 00 00 00 00 e0 Microsoft ISATAP Adapter
17...00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #2
15...00 00 00 00 00 00 e0 Microsoft 6to4 Adapter
18...00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #3
19...00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #4
=====

IPv4 路由表
=====
活动路由:
网络目标      网络掩码      网关      接口      跃点数
0.0.0.0        0.0.0.0        202.1.5.1    202.1.5.3    276
0.0.0.0        0.0.0.0        10.0.0.1     10.10.10.2    2
10.0.0.0        255.0.0.0      在链路上    10.10.10.2    257
10.10.10.2     255.255.255.255 在链路上    10.10.10.2    257
10.255.255.255 255.255.255.255 在链路上    10.10.10.2    257
127.0.0.0      255.0.0.0      在链路上    127.0.0.1     306
127.0.0.1      255.255.255.255 在链路上    127.0.0.1     306
127.255.255.255 255.255.255.255 在链路上    127.0.0.1     306
202.1.5.1      255.255.255.255 202.1.5.1    202.1.5.3     21
224.0.0.0      240.0.0.0      在链路上    127.0.0.1     306
224.0.0.0      240.0.0.0      在链路上    202.1.5.3     276
224.0.0.0      240.0.0.0      在链路上    192.168.0.51   276
224.0.0.0      240.0.0.0      在链路上    10.10.10.2     257
255.255.255.255 255.255.255.255 在链路上    127.0.0.1     306
255.255.255.255 255.255.255.255 在链路上    202.1.5.3     276
255.255.255.255 255.255.255.255 在链路上    192.168.0.51   276
255.255.255.255 255.255.255.255 在链路上    10.10.10.2     257
=====
永久路由:
网络地址      网络掩码  网关地址  跃点数
192.168.0.0    255.255.0.0 192.168.0.1 默认
0.0.0.0        0.0.0.0    202.1.5.1 默认
0.0.0.0        0.0.0.0    10.0.0.1 1
=====
```

客户端连接 VPN 时, 会产生一个虚拟网卡, 通过该网卡获得一个内网的 VPN 用户地址。此时, 可以认为外网 PC 与内网 PC 在同一个虚拟局域网内, 因此, 路由表里有该局域网网关地址 10.0.0.1。

6. 分析步骤 10 完成捕获的报文, 分析几种访问模式的差别。

(1) 内网:

PC3 访问 PC4:

PC3 抓包

No.	Time	Source	Destination	Protocol	Length	Info
10	1.521433	10.1.3.123	10.1.3.80	TCP	54	54486 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
11	1.522024	10.1.3.123	10.1.3.80	HTTP	543	GET / HTTP/1.1
12	1.555678	10.1.3.80	10.1.3.123	TCP	272	80 → 54486 [PSH, ACK] Seq=1 Ack=490 Win=65536 Len=218 [TCP segment ...
13	1.556376	10.1.3.80	10.1.3.123	TCP	1514	80 → 54486 [PSH, ACK] Seq=219 Ack=490 Win=65536 Len=1460 [TCP segme...
14	1.556419	10.1.3.123	10.1.3.80	TCP	54	54486 → 80 [ACK] Seq=490 Ack=1679 Win=65536 Len=0
15	1.557688	10.1.3.80	10.1.3.123	TCP	1514	80 → 54486 [ACK] Seq=1679 Ack=490 Win=65536 Len=1460 [TCP segment o...
16	1.557688	10.1.3.80	10.1.3.123	HTTP	205	HTTP/1.1 200 OK (text/html)



## PC4 抓包

No.	Time	Source	Destination	Protocol	Length	Info
10	1.521515	10.1.3.123	10.1.3.80	TCP	60	54486 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
11	1.522238	10.1.3.123	10.1.3.80	HTTP	543	GET / HTTP/1.1
12	1.555169	10.1.3.80	10.1.3.123	TCP	272	80 → 54486 [PSH, ACK] Seq=1 Ack=490 Win=65536 Len=218 [TCP segment ...
13	1.555397	10.1.3.80	10.1.3.123	TCP	1514	80 → 54486 [PSH, ACK] Seq=219 Ack=490 Win=65536 Len=1460 [TCP segme...
14	1.556523	10.1.3.123	10.1.3.80	TCP	60	54486 → 80 [ACK] Seq=490 Ack=1679 Win=65536 Len=0
15	1.556569	10.1.3.80	10.1.3.123	HTTP	1665	HTTP/1.1 200 OK (text/html)

通过内网访问，两台 PC 可以没有阻碍地连通，且通过 TCP 明文传输。

### (2) 外网：

①PC1 通过 Web 方式访问 PC4：

## PC1 抓包

38	3.789628	202.1.5.1	202.1.5.3	TLSv1	299	Application Data
39	3.789628	202.1.5.1	202.1.5.3	TLSv1	107	Application Data
40	3.789628	202.1.5.1	202.1.5.3	TLSv1	91	Application Data
41	3.789698	202.1.5.3	202.1.5.1	TCP	54	49595 → 443 [ACK] Seq=1685 Ack=671 Win=63892 Len=0
42	3.806733	202.1.5.1	202.1.5.3	TLSv1	331	Application Data
43	3.807402	202.1.5.1	202.1.5.3	TLSv1	1467	Application Data
44	3.807402	202.1.5.1	202.1.5.3	TLSv1	91	Application Data
45	3.807439	202.1.5.3	202.1.5.1	TCP	54	49593 → 443 [ACK] Seq=1003 Ack=1728 Win=64860 Len=0
46	3.821180	202.1.5.3	202.1.5.1	TLSv1	880	Application Data, Application Data
47	3.821821	202.1.5.1	202.1.5.3	TCP	60	443 → 49593 [ACK] Seq=1728 Ack=1829 Win=8192 Len=0
48	3.822319	202.1.5.3	202.1.5.1	TLSv1	864	Application Data, Application Data
49	3.822982	202.1.5.3	202.1.5.1	TLSv1	864	Application Data, Application Data
50	3.823196	202.1.5.3	202.1.5.1	TLSv1	864	Application Data, Application Data

```
> Frame 42: 331 bytes on wire (2648 bits), 331 bytes captured (2648 bits) on interface \Device\NPF_{C
> Ethernet II, Src: Cisco_e5:54:e3 (00:21:55:e5:54:e3), Dst: Sony_e5:60:ae (f0:bf:97:e5:60:ae)
> Internet Protocol Version 4, Src: 202.1.5.1, Dst: 202.1.5.3
> Transmission Control Protocol, Src Port: 443, Dst Port: 49593, Seq: 1, Ack: 1003, Len: 277
< Transport Layer Security
  < TLSv1 Record Layer: Application Data Protocol: Hypertext Transfer Protocol
    Content Type: Application Data (23)
    Version: TLS 1.0 (0x0301)
    Length: 272
    Encrypted Application Data: aa7b7254c130ebfe02deae27df7be20cce7fb5f27c7a51e1a6e158f32c3e90e432
    [Application Data Protocol: Hypertext Transfer Protocol]
```

## PC4 抓包

No.	Time	Source	Destination	Protocol	Length	Info
10	4.255049	10.1.3.1	10.1.3.80	TCP	66	1059 → 80 [ACK] Seq=1 Ack=1 Win=8192 Len=0 TSval=4373573 TSecr=9460...
11	4.255049	10.1.3.1	10.1.3.80	HTTP	586	GET / HTTP/1.1
12	4.288097	10.1.3.80	10.1.3.1	TCP	297	80 → 1059 [PSH, ACK] Seq=1 Ack=521 Win=64296 Len=231 TSval=946057 T...
13	4.288330	10.1.3.80	10.1.3.1	TCP	1526	80 → 1059 [PSH, ACK] Seq=232 Ack=521 Win=64296 Len=1460 TSval=94605...
14	4.288812	10.1.3.1	10.1.3.80	TCP	66	1059 → 80 [ACK] Seq=521 Ack=232 Win=8192 Len=0 TSval=4373606 TSecr=...
15	4.288859	10.1.3.80	10.1.3.1	TCP	1434	80 → 1059 [ACK] Seq=1692 Ack=521 Win=64296 Len=1368 TSval=946057 TS...
16	4.288859	10.1.3.80	10.1.3.1	TCP	205	80 → 1059 [PSH, ACK] Seq=3060 Ack=521 Win=64296 Len=139 TSval=94605...
17	4.290179	10.1.3.1	10.1.3.80	TCP	66	1059 → 80 [ACK] Seq=521 Ack=1600 Win=8192 Len=0 TSval=4373607 TSecr=...
18	4.290179	10.1.3.1	10.1.3.80	TCP	66	1059 → 80 [ACK] Seq=521 Ack=1692 Win=8192 Len=0 TSval=4373607 TSecr=...
19	4.290226	10.1.3.80	10.1.3.1	TCP	2802	80 → 1059 [PSH, ACK] Seq=3199 Ack=521 Win=64296 Len=2736 TSval=9460...
20	4.293072	10.1.3.1	10.1.3.80	TCP	66	1059 → 80 [ACK] Seq=521 Ack=3060 Win=8192 Len=0 TSval=4373611 TSecr=...
21	4.293072	10.1.3.1	10.1.3.80	TCP	66	1059 → 80 [ACK] Seq=521 Ack=3199 Win=8192 Len=0 TSval=4373611 TSecr=...
22	4.293072	10.1.3.1	10.1.3.80	TCP	66	1059 → 80 [ACK] Seq=521 Ack=4567 Win=8192 Len=0 TSval=4373611 TSecr=...
23	4.293072	10.1.3.1	10.1.3.80	TCP	66	1059 → 80 [ACK] Seq=521 Ack=5935 Win=8192 Len=0 TSval=4373611 TSecr=...
24	4.293147	10.1.3.80	10.1.3.1	HTTP	1478	HTTP/1.1 200 OK (text/html)

通过 Web 方式连接 VPN 时，在外网 PC 上只能看见本机与防火墙之间的报文，且报文协议为 TLS 1.0，说明报文是通过密文传输，且需要经由防火墙转发处理后才能在内网 PC 与外网 PC 之间传输；在内网 PC 上看到的数据包，则都是通过明文 TCP 传输，且收发双方是防火墙（10.1.3.1）与 PC4（10.1.3.80），这也说明了内网 PC 在与外网 PC 传输数据包时需要由防火墙进行转发处理。

②PC1 通过客户端方式访问 PC4:

PC1 虚拟网卡抓包

No.	Time	Source	Destination	Protocol	Length	Info
7	10.167477	10.10.10.2	10.1.3.80	TCP	66	49567 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1366 WS=256 SACK_PERM
8	10.167886	10.10.10.2	10.1.3.80	TCP	66	49568 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1366 WS=256 SACK_PERM
9	10.169612	10.1.3.80	10.10.10.2	TCP	66	80 → 49568 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1380 WS=256 SA...
10	10.169684	10.10.10.2	10.1.3.80	TCP	54	49568 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
11	10.171424	10.10.10.2	10.1.3.80	HTTP	517	GET / HTTP/1.1
12	10.202682	10.1.3.80	10.10.10.2	TCP	272	80 → 49568 [PSH, ACK] Seq=1 Ack=464 Win=65536 Len=218 [TCP segment ...
13	10.203319	10.1.3.80	10.10.10.2	TCP	1420	80 → 49568 [ACK] Seq=219 Ack=464 Win=65536 Len=1366 [TCP segment of...
14	10.203339	10.10.10.2	10.1.3.80	TCP	54	49568 → 80 [ACK] Seq=464 Ack=1585 Win=65536 Len=0
15	10.203376	10.1.3.80	10.10.10.2	TCP	148	80 → 49568 [PSH, ACK] Seq=1585 Ack=464 Win=65536 Len=94 [TCP segmen...
16	10.204535	10.1.3.80	10.10.10.2	TCP	1420	80 → 49568 [ACK] Seq=1679 Ack=464 Win=65536 Len=1366 [TCP segment o...
17	10.204552	10.10.10.2	10.1.3.80	TCP	54	49568 → 80 [ACK] Seq=464 Ack=3045 Win=65536 Len=0
18	10.204580	10.1.3.80	10.10.10.2	HTTP	302	HTTP/1.1 200 OK (text/html)

PC1 物理网卡抓包

No.	Time	Source	Destination	Protocol	Length	Info
28	2.547557	202.1.5.3	202.1.5.1	TCP	54	49601 → 443 [ACK] Seq=1 Ack=1 Win=64860 Len=0
29	2.548152	202.1.5.3	202.1.5.1	TLSv1	571	Client Hello
30	2.548904	202.1.5.1	202.1.5.3	TCP	60	443 → 49601 [ACK] Seq=1 Ack=518 Win=8192 Len=0
31	2.549642	202.1.5.1	202.1.5.3	TLSv1	576	Server Hello, Certificate, Server Hello Done
32	2.550253	202.1.5.3	202.1.5.1	TLSv1	252	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
33	2.551010	202.1.5.1	202.1.5.3	TCP	60	443 → 49601 [ACK] Seq=523 Ack=716 Win=7994 Len=0
34	2.551734	202.1.5.1	202.1.5.3	TCP	60	[TCP Window Update] 443 → 49601 [ACK] Seq=523 Ack=716 Win=8192 Len=0
35	2.553415	202.1.5.1	202.1.5.3	TLSv1	113	Change Cipher Spec, Encrypted Handshake Message
36	2.554227	202.1.5.3	202.1.5.1	TLSv1	1088	Application Data, Application Data

PC4 抓包

No.	Time	Source	Destination	Protocol	Length	Info
7	0.703427	10.10.10.2	10.1.3.80	TCP	60	49568 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
8	0.705275	10.10.10.2	10.1.3.80	HTTP	517	GET / HTTP/1.1
9	0.735709	10.1.3.80	10.10.10.2	TCP	272	80 → 49568 [PSH, ACK] Seq=1 Ack=464 Win=65536 Len=218 [TCP segment ...
10	0.735940	10.1.3.80	10.10.10.2	TCP	1514	80 → 49568 [PSH, ACK] Seq=219 Ack=464 Win=65536 Len=1460 [TCP segme...
11	0.737017	10.10.10.2	10.1.3.80	TCP	60	49568 → 80 [ACK] Seq=464 Ack=1585 Win=65536 Len=0
12	0.737062	10.1.3.80	10.10.10.2	HTTP	1668	HTTP/1.1 200 OK (text/html)

通过客户端连接 VPN 时，客户端会被分配一个 IP 地址，即上图中的 10.10.10.2，客户端使用这个 IP 地址与内网主机进行直接通信，在客户端的虚拟网卡及内网主机上，数据包都是通过 TCP 明文传输而不经防火墙。但实际上，客户端是使用物理网卡进行数据包的传输，并使用 TLS 协议进行加密后由防火墙进行转发。

访问模式的区别：

- (a) 位于内网的两台主机可以直接进行通信，并以明文传输报文；
- (b) 位于外网的主机访问内网主机时，在 Web 模式下，身份认证后即可通过防火墙进行内部网络的 Web 访问，但没有完整的网络访问；在客户端模式下，外网主机将从 VPN 池接收 IP 地址，从而允许完全访问网络。

此外，外网主机与内网主机的通信，完全被封装在一个 SSL 隧道中传输，内容是加密的，所以在公网中也是安全的。

7. 进阶自设计

分别在校园网和外网（通过校园 VPN 服务 <http://vpn.xjtu.edu.cn/>）访问校内资源，通过抓包分析对比三种模式（内网访问、外网 WebVPN 访问和外网 SSLVPN 访问）的访问过程及相关参数。

①内网访问：

44	2.451047	192.168.1.109	202.117.18.202	TCP	54	52310 → 80 [ACK] Seq=1545 Ack=5341 Win=484 Len=0
45	2.451217	202.117.18.202	192.168.1.109	HTTP	74	HTTP/1.1 200 (text/html)
46	2.535857	192.168.1.109	202.117.18.202	HTTP	628	GET /openplatform/js/login/login.js?t=1680684814584 HTTP/1.1
47	2.546966	202.117.18.202	192.168.1.109	TCP	1514	80 → 52310 [ACK] Seq=5361 Ack=2119 Win=1024 Len=1460 [TCP segment of a reassembled PDU]
48	2.547278	202.117.18.202	192.168.1.109	TCP	1514	80 → 52310 [ACK] Seq=6821 Ack=2119 Win=1024 Len=1460 [TCP segment of a reassembled PDU]
49	2.547294	192.168.1.109	202.117.18.202	TCP	54	52310 → 80 [ACK] Seq=2119 Ack=8281 Win=479 Len=0
50	2.547658	202.117.18.202	192.168.1.109	TCP	1514	80 → 52310 [ACK] Seq=8281 Ack=2119 Win=1024 Len=1460 [TCP segment of a reassembled PDU]
51	2.547982	202.117.18.202	192.168.1.109	TCP	1514	80 → 52310 [ACK] Seq=9741 Ack=2119 Win=1024 Len=1460 [TCP segment of a reassembled PDU]

内网访问时使用未加密的 HTTP 协议进行通信。192.168.1.109 是本地主机地址，

202.117.18.202 是校内资源地址，两者直接进行通信。

②外网 WebVPN 访问：

23 2.115730	192.168.43.62	117.32.153.183	TLSv1.2	805 Application Data
24 2.116066	192.168.43.62	117.32.153.183	TLSv1.2	802 Application Data
25 2.215628	117.32.153.183	192.168.43.62	TLSv1.2	873 Application Data
26 2.271530	117.32.153.183	192.168.43.62	TCP	1414 443 → 50040 [ACK] Seq=1 Ack=752 Win=110 Len=1360 [TCP segment of a reassembled PDU]
27 2.276406	117.32.153.183	192.168.43.62	TCP	1414 443 → 50040 [ACK] Seq=1361 Ack=752 Win=110 Len=1360 [TCP segment of a reassembled PDU]
28 2.276426	192.168.43.62	117.32.153.183	TCP	54 50040 → 443 [ACK] Seq=752 Ack=2721 Win=69 Len=0
29 2.277066	117.32.153.183	192.168.43.62	TCP	1414 443 → 50040 [ACK] Seq=2721 Ack=752 Win=110 Len=1360 [TCP segment of a reassembled PDU]

外网 WebVPN 访问时使用加密的 TLS 协议进行通信。192.168.43.62 是本地主机地址，117.32.153.183 (webvpn.xjtu.edu.cn) 是 WebVPN 服务的地址。外网主机在访问校内资源时需要经过 117.32.153.183 进行数据包的转发。

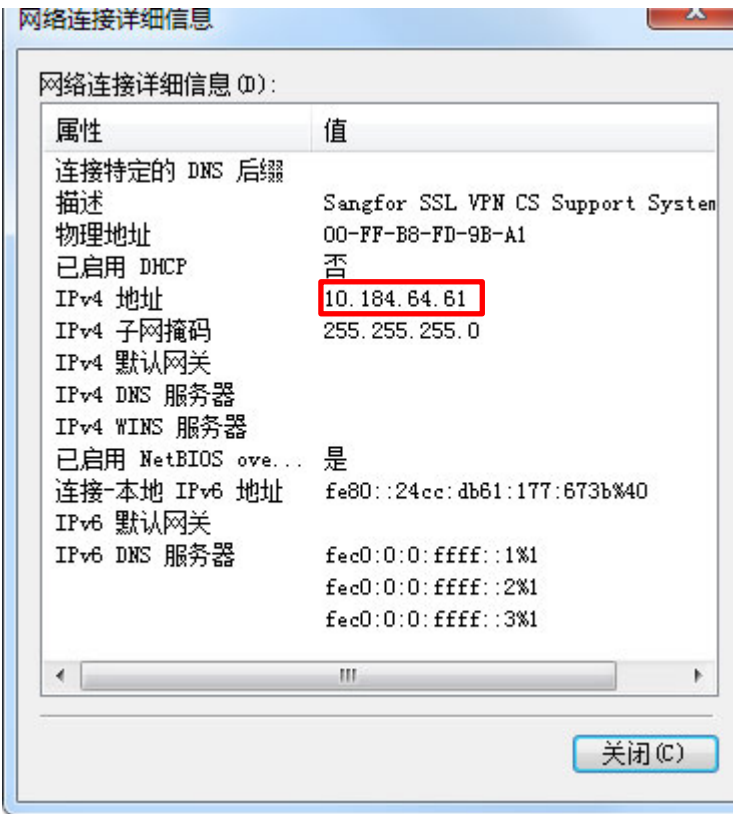
③外网 SSLVPN 访问：

虚拟网卡抓包如下：

125 6.043211	202.117.13.146	10.184.64.61	HTTP	751 HTTP/1.1 200 (application/javascript)
126 6.044461	202.117.13.146	10.184.64.61	TCP	1414 80 → 51841 [ACK] Seq=1 Ack=493 Win=30336 Len=1360 [TCP segment of a reassembled PDU]
127 6.044575	202.117.13.146	10.184.64.61	TCP	132 80 → 51841 [PSH, ACK] Seq=1361 Ack=493 Win=30336 Len=78 [TCP segment of a reassembled PDU]
128 6.044600	10.184.64.61	202.117.13.146	TCP	54 51841 → 80 [ACK] Seq=493 Ack=1439 Win=17664 Len=0
129 6.044620	202.117.13.146	10.184.64.61	HTTP	457 HTTP/1.1 200 (application/javascript)
130 6.063217	202.117.13.146	10.184.64.61	TCP	1414 80 → 51837 [ACK] Seq=27553 Ack=921 Win=31360 Len=1360 [TCP segment of a reassembled PDU]
131 6.066855	202.117.13.146	10.184.64.61	TCP	1414 80 → 51837 [ACK] Seq=28913 Ack=921 Win=31360 Len=1360 [TCP segment of a reassembled PDU]
132 6.066912	10.184.64.61	202.117.13.146	TCP	54 51837 → 80 [ACK] Seq=921 Ack=30273 Win=17664 Len=0

外网 SSLVPN 访问时使用未加密的 HTTP 协议进行通信。10.184.64.61 是本地主机分配到的 IP 地址，用于直接访问校内资源 (202.117.13.146)。

虚拟网卡：



路由表（截取部分）：



	<div>199.74.248.13 255.255.255.255 10.184.64.64 10.184.64.61 286 202.103.20.55 255.255.255.255 10.184.64.64 10.184.64.61 286 202.114.51.71 255.255.255.255 10.184.64.64 10.184.64.61 286 202.117.0.0 255.255.192.0 10.184.64.64 10.184.64.61 286 202.117.160.0 255.255.240.0 10.184.64.64 10.184.64.61 286 202.117.200.0 255.255.248.0 10.184.64.64 10.184.64.61 286 202.117.208.0 255.255.240.0 10.184.64.64 10.184.64.61 286 202.134.99.132 255.255.255.255 10.184.64.64 10.184.64.61 286 202.200.224.0 255.255.240.0 10.184.64.64 10.184.64.61 286 203.69.105.155 255.255.255.255 10.184.64.64 10.184.64.61 286 203.81.18.55 255.255.255.255 10.184.64.64 10.184.64.61 286 203.163.124.46 255.255.255.255 10.184.64.64 10.184.64.61 286 203.208.41.0 255.255.255.0 10.184.64.64 10.184.64.61 286 203.208.42.0 255.255.254.0 10.184.64.64 10.184.64.61 286 203.208.44.0 255.255.252.0 10.184.64.64 10.184.64.61 286 203.208.48.0 255.255.254.0 10.184.64.64 10.184.64.61 286 203.208.50.0 255.255.255.192 10.184.64.64 10.184.64.61 286 203.208.50.64 255.255.255.240 10.184.64.64 10.184.64.61 286 203.208.50.80 255.255.255.248 10.184.64.64 10.184.64.61 286 203.208.50.88 255.255.255.254 10.184.64.64 10.184.64.61 286 203.208.50.90 255.255.255.255 10.184.64.64 10.184.64.61 286 204.93.150.152 255.255.255.255 10.184.64.64 10.184.64.61 286</div>				
	可以看到，本地主机的路由表中增添了可以访问的校内资源的路由。				
本组四人主要工作：	■■■■■，主要负责 PC1 的控制，配置防火墙，完成部分实验报告的撰写。				
	■■■■■，主要负责 PC2 的控制，完成部分实验报告的撰写。				
	■■■■■，主要负责 PC3 的控制，配置交换机，完成部分实验报告的撰写。				
	■■■■■，主要负责 PC4 的控制，完成部分实验报告的撰写。				
实验中问题及解决方法，经验总结	外网 PC 登录 VPN 客户端失败，分析发现是由于 Web 模式访问时使用的账号未退出，导致客户端与 Web 模式使用了同一账号而引发冲突。解决方案是在防火墙中注销已登陆的 VPN 用户。				
师生互动交流	防火墙创建 SSL VPN 用户 IP 地址池时显示配置已存在，在张老师的帮助下，我们了解到是由于之前的配置未完全清除导致的，在清除完之前的配置后，成功创建了用户 IP 地址池。				
验收教师	张利平	本实验成绩			