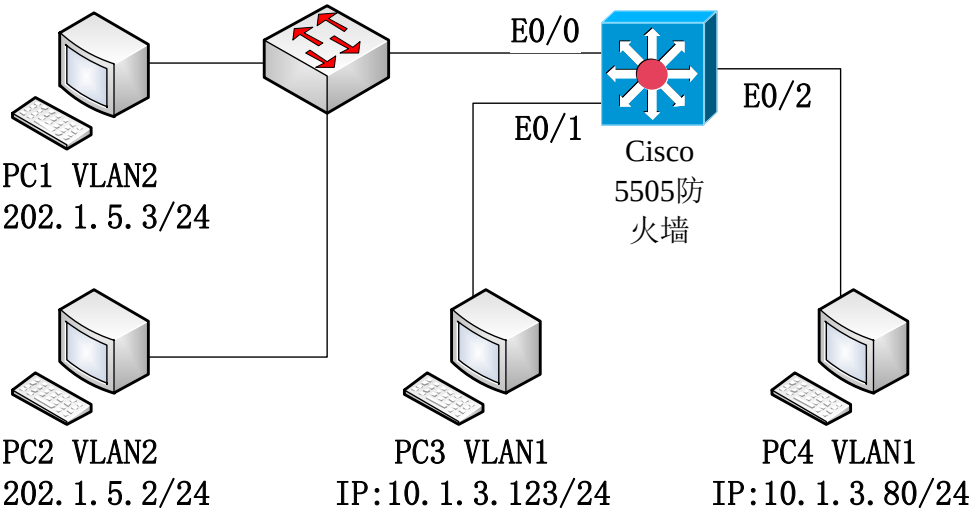
计算机网络专题实验现场检查单 7

实验名称：**防火墙与 SSLVPN 实验**　　时间：　2024 年 4 月 28 日　早☑ 午☐ 晚☐

组号	7-1	**实验位**	实验 1 组	**控制器地址**	192.168.1.10
姓名	白佳兴	廖立彬	侯凯耀	余小康	谭兆基

实验组网图

【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】



实验结果

1. 本组 CISCO ASA5505 中 Vlan 的划分、命名及端口分配方案是：

```
ciscoasa(config-if)# show ip
System IP Addresses:
Interface                  Name                IP address      Subnet mask
Method
Vlan1                      inside              202.1.3.1       255.255.255.0
manual
Vlan2                      outside             202.1.5.1       255.255.255.0
manual
Current IP Addresses:
Interface                  Name                IP address      Subnet mask
Method
Vlan1                      inside              202.1.3.1       255.255.255.0
manual
Vlan2                      outside             202.1.5.1       255.255.255.0
manual
```

2. CISCO ASA5505 内网 DHCP 服务器的 IP 范围是：

```
ciscoasa(config)# interface vlan 1
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)#ip address 10.1.3.1 255.255.255.0
ciscoasa(config-if)#
ciscoasa(config-if)# dhcpd address 10.1.3.2-10.1.3.33 inside
ciscoasa(config)# dhcpd enable inside
ciscoasa(config)# show dhcpd state
Context  Configured as DHCP Server
Interface outside, Not Configured for DHCP
Interface inside, Configured for DHCP SERVER
```

范围是 10.1.3.2-10.1.3.33

3. SSL VPN 用户地址池的名称和地址范围是：

```
ciscoasa(config-webvpn)# ip local pool ssluser 10.10.10.1-10.10.10.10
ciscoasa(config)#
```

名称是 ssluser,范围是 10.10.10.1-10.10.10.10

4. 创建的 SSL VPN 用户名是：

创建的用户名是 vpnuser1 和 vpnuser2

5. 所配置的防火墙测试方案及结果是：

```
ciscoasa(config)# show nat

NAT policies on Interface inside:
  match ip inside 10.1.3.0 255.255.255.0 outside 10.10.10.0 255.255.255.0
    NAT exempt
    translate_hits = 0, untranslate_hits = 0
  match ip inside 10.1.3.0 255.255.255.0 inside 10.10.10.0 255.255.255.0
    NAT exempt
    translate_hits = 0, untranslate_hits = 0
  match ip inside 10.1.3.0 255.255.255.0 _internal_loopback 10.10.10.0 255.255.2
55.0
    NAT exempt
    translate_hits = 0, untranslate_hits = 0
```

```
ciscoasa(config-webvpn)# show webvpn  svc
1. disk0:/anyconnect-win-2.0.0343-k9.pkg 1
  CISCO STC win2k+
  2,0,0343
  Mon 04/23/2007  4:16:34.63

1 SSL VPN Client(s) installed
```

```
ciscoasa(config-if)# show interface vlan 2
Interface Vlan2 "outside", is down, line protocol is down
  Hardware is EtherSVI, BW 100 Mbps, DLY 100 usec
        MAC address 0021.55fa.f43f, MTU 1500
        IP address 202.1.5.1, subnet mask 255.255.255.0
  Traffic Statistics for "outside":
        0 packets input, 0 bytes
        0 packets output, 0 bytes
        0 packets dropped
      1 minute input rate 0 pkts/sec,  0 bytes/sec
      1 minute output rate 0 pkts/sec,  0 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  0 bytes/sec
      5 minute output rate 0 pkts/sec,  0 bytes/sec
      5 minute drop rate, 0 pkts/sec
```

```
ciscoasa(config)# show dhcpd state
Context  Configured as DHCP Server
Interface outside, Not Configured for DHCP
Interface inside, Configured for DHCP SERVER
```

```
ciscoasa(config)# show access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
            alert-interval 300
access-list go-vpn; 1 elements
access-list go-vpn line 1 extended permit ip 10.1.3.0 255.255.255.0 10.10.10.0 2
55.255.255.0 (hitcnt=0) 0xcf3c45b3
```

```
ciscoasa(config-if)# show switch vlan
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    inside                           down      Et0/1, Et0/2, Et0/3, Et0/4
                                                Et0/5, Et0/6, Et0/7
2    outside                          down      Et0/0
```

6. 步骤 8 完成后，记录和分析内网方式访问过程。

服务器抓到的包：

Time	No.	Source	Destination	Protocol	Len	Info
0.001609	7	10.1.3.123	10.1.3.80	HTTP	481	GET / HTTP/1.1
0.034597	8	10.1.3.80	10.1.3.123	TCP	330	80 → 51841 [PSH, ACK] Seq=1 Ac
0.034803	9	10.1.3.80	10.1.3.123	TCP	15…	80 → 51841 [PSH, ACK] Seq=277
0.035499	10	10.1.3.123	10.1.3.80	TCP	60	51841 → 80 [ACK] Seq=428 Ack=1
0.035530	11	10.1.3.80	10.1.3.123	HTTP	16…	HTTP/1.1 200 OK (text/html)
0.036139	12	10.1.3.123	10.1.3.80	TCP	60	51841 → 80 [ACK] Seq=428 Ack=3
0.053903	13	10.1.3.123	10.1.3.80	HTTP	424	GET /?mode=section&id=style.cs
0.053928	14	10.1.3.123	10.1.3.80	TCP	66	51843 → 80 [SYN] Seq=0 Win=819
0.053983	15	10.1.3.80	10.1.3.123	TCP	66	80 → 51843 [SYN, ACK] Seq=0 Ac
0.054595	16	10.1.3.123	10.1.3.80	HTTP	395	GET /?mode=jquery HTTP/1.1
0.054595	17	10.1.3.123	10.1.3.80	TCP	60	51843 → 80 [ACK] Seq=1 Ack=1 W
0.054595	18	10.1.3.123	10.1.3.80	HTTP	406	GET /?mode=section&id=lib.js H
0.062048	19	10.1.3.80	10.1.3.123	TCP	242	80 → 51841 [PSH, ACK] Seq=3380
0.069502	20	10.1.3.80	10.1.3.123	TCP	246	80 → 51842 [PSH, ACK] Seq=1 Ac
0.075313	21	10.1.3.80	10.1.3.123	TCP	15…	80 → 51841 [PSH, ACK] Seq=3568
0.075340	22	10.1.3.80	10.1.3.123	TCP	15…	80 → 51841 [PSH, ACK] Seq=5028
0.075359	23	10.1.3.80	10.1.3.123	TCP	15…	80 → 51841 [PSH, ACK] Seq=6488
0.075375	24	10.1.3.80	10.1.3.123	TCP	15…	80 → 51841 [PSH, ACK] Seq=7948
0.075876	25	10.1.3.123	10.1.3.80	TCP	60	51841 → 80 [ACK] Seq=798 Ack=5
0.075908	26	10.1.3.80	10.1.3.123	TCP	29…	80 → 51841 [PSH, ACK] Seq=9408

PC3 抓到的包：

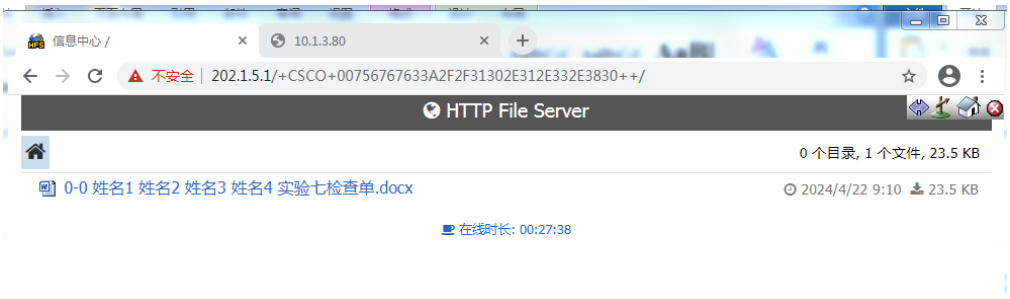
Time	No	Source	Destination	Protocol	Len	Info
0.000000	1	10.1.3.123	10.1.3.80	TCP	66	51841 → 80 [SYN] Seq=0 Win=819
0.000327	2	10.1.3.123	10.1.3.80	TCP	66	51842 → 80 [SYN] Seq=0 Win=819
0.000673	3	10.1.3.80	10.1.3.123	TCP	66	80 → 51841 [SYN, ACK] Seq=0 Ac
0.000673	4	10.1.3.80	10.1.3.123	TCP	66	80 → 51842 [SYN, ACK] Seq=0 Ac
0.000746	5	10.1.3.123	10.1.3.80	TCP	54	51841 → 80 [ACK] Seq=1 Ack=1 W
0.000762	6	10.1.3.123	10.1.3.80	TCP	54	51842 → 80 [ACK] Seq=1 Ack=1 W
0.001756	7	10.1.3.123	10.1.3.80	HTTP	481	GET / HTTP/1.1
0.035017	8	10.1.3.80	10.1.3.123	TCP	330	80 → 51841 [PSH, ACK] Seq=1 Ac
0.035679	9	10.1.3.80	10.1.3.123	TCP	15…	80 → 51841 [PSH, ACK] Seq=277
0.035723	10	10.1.3.123	10.1.3.80	TCP	54	51841 → 80 [ACK] Seq=428 Ack=1
0.036354	11	10.1.3.80	10.1.3.123	TCP	15…	80 → 51841 [ACK] Seq=1737 Ack=
0.036354	12	10.1.3.80	10.1.3.123	HTTP	237	HTTP/1.1 200 OK (text/html)
0.036381	13	10.1.3.123	10.1.3.80	TCP	54	51841 → 80 [ACK] Seq=428 Ack=3
0.053826	14	10.1.3.123	10.1.3.80	HTTP	424	GET /?mode=section&id=style.cs
0.054099	15	10.1.3.123	10.1.3.80	TCP	66	51843 → 80 [SYN] Seq=0 Win=819
0.054482	16	10.1.3.80	10.1.3.123	TCP	66	80 → 51843 [SYN, ACK] Seq=0 Ac
0.054488	17	10.1.3.123	10.1.3.80	HTTP	395	GET /?mode=jquery HTTP/1.1
0.054523	18	10.1.3.123	10.1.3.80	TCP	54	51843 → 80 [ACK] Seq=1 Ack=1 W
0.054693	19	10.1.3.123	10.1.3.80	HTTP	406	GET /?mode=section&id=lib.js H

可以发现 10.1.3.123(PC3)向 10.1.3.80(PC4)请求数据，同时二者通信内容没有进行加密，直接通过 TCP 协议和 HTTP 协议进行通信。这是因为二者同在防火墙内部的同一个 VLAN，相互通信可以直接转发，不需要进行加密

7. 步骤 9 完成后，记录和分析外网 Web 方式访问过程。

```
C:\Users\Administrator>route print
===========================================================================
接口列表
 13...48 4d 7e a8 1d ce ......Intel(R) Ethernet Connection (2) I219-LM
 11...00 e0 4c 70 61 48 ......Realtek PCIe GBE Family Controller
  1...........................Software Loopback Interface 1
 16...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter
 15...00 00 00 00 00 00 00 e0 Microsoft 6to4 Adapter
 17...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #3
===========================================================================

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       202.1.5.2    276
        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
      192.168.0.0      255.255.0.0     192.168.0.1     192.168.0.12    276
      192.168.0.0    255.255.255.0         在链路上      192.168.0.12    276
     192.168.0.12  255.255.255.255         在链路上      192.168.0.12    276
    192.168.0.255  255.255.255.255         在链路上      192.168.0.12    276
        202.1.5.0    255.255.255.0         在链路上         202.1.5.2    276
        202.1.5.2  255.255.255.255         在链路上         202.1.5.2    276
      202.1.5.255  255.255.255.255         在链路上         202.1.5.2    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         202.1.5.2    276
        224.0.0.0        240.0.0.0         在链路上      192.168.0.12    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         202.1.5.2    276
  255.255.255.255  255.255.255.255         在链路上      192.168.0.12    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
===========================================================================
```



PC2 的数据包：

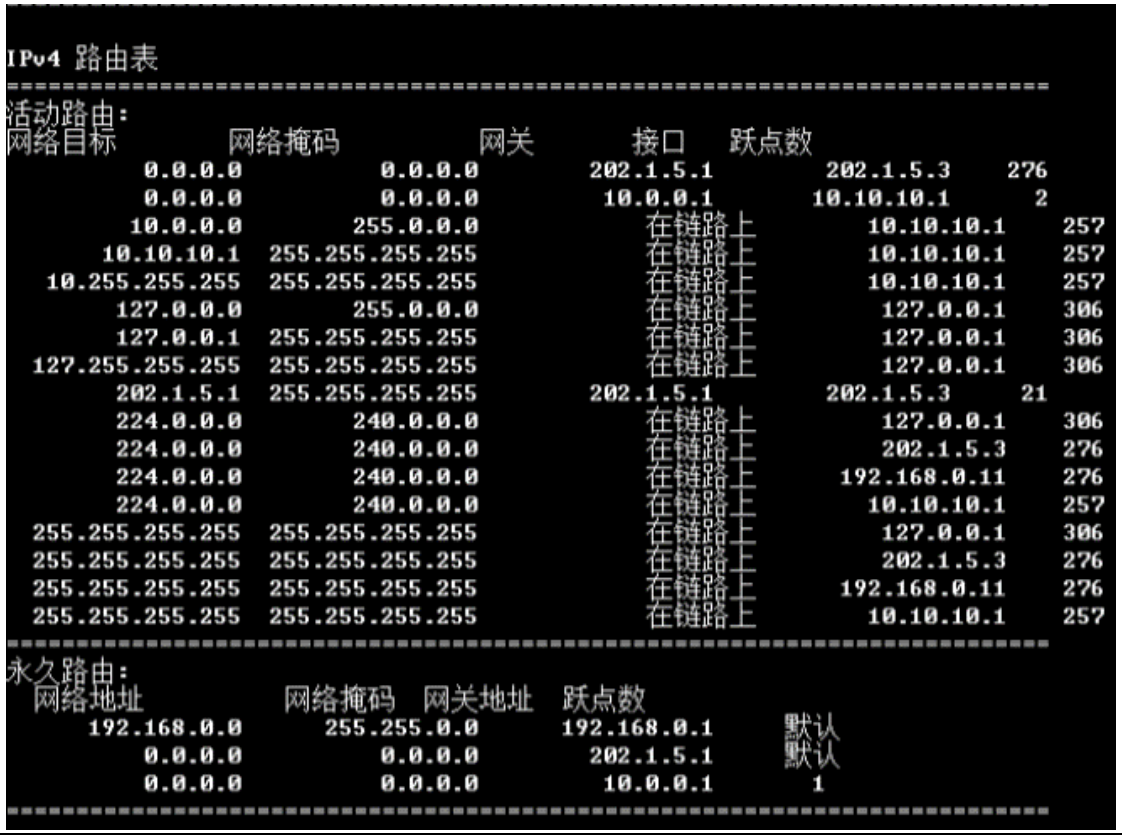
No	Source	Destination	Protocol	Len	Info
1	202.1.5.3	202.1.5.255	BROWSER	243	Host Announcement 1-PC1,
2	202.1.5.2	202.1.5.1	TLSv1	816	Application Data, Applica
3	202.1.5.1	202.1.5.2	TCP	60	443 → 52290 [ACK] Seq=1 A
4	202.1.5.2	202.1.5.1	TLSv1	992	Application Data, Applica
5	202.1.5.2	202.1.5.1	TCP	54	52297 → 443 [FIN, ACK] Se
6	202.1.5.1	202.1.5.2	TLSv1	299	Application Data
7	202.1.5.1	202.1.5.2	TCP	60	443 → 52297 [ACK] Seq=1 A
8	202.1.5.1	202.1.5.2	TCP	60	443 → 52297 [ACK] Seq=1 A
9	202.1.5.1	202.1.5.2	TLSv1	107	Application Data
10	202.1.5.2	202.1.5.1	TCP	54	52290 → 443 [ACK] Seq=763
11	202.1.5.1	202.1.5.2	TLSv1	91	Application Data
12	202.1.5.2	202.1.5.1	TLSv1	816	Application Data, Applica
13	202.1.5.2	202.1.5.1	TLSv1	992	Application Data, Applica
14	202.1.5.1	202.1.5.2	TCP	60	443 → 52290 [ACK] Seq=336
15	202.1.5.1	202.1.5.2	TCP	60	[TCP Window Update] 443 →
16	202.1.5.1	202.1.5.2	TCP	60	443 → 52294 [ACK] Seq=1 A
17	202.1.5.1	202.1.5.2	TLSv1	331	Application Data

服务器的数据包:

No	Source	Destination	Protocol	Len	Info
7	RealtekSem…	Broadcast	ARP	42	Who has 10.1.3.1? Tell 10.1.3.80
8	Cisco_fa:f…	RealtekSemic…	ARP	60	10.1.3.1 is at 00:21:55:fa:f4:3f
9	10.1.3.80	10.1.3.1	TCP	70	80 → 1029 [SYN, ACK] Seq=0 Ack=1
10	10.1.3.1	10.1.3.80	TCP	66	1029 → 80 [ACK] Seq=1 Ack=1 Win=
11	10.1.3.1	10.1.3.80	HTTP	586	GET / HTTP/1.1
12	10.1.3.80	10.1.3.1	TCP	296	80 → 1029 [PSH, ACK] Seq=1 Ack=5
13	10.1.3.80	10.1.3.1	TCP	14…	80 → 1029 [ACK] Seq=231 Ack=521
14	10.1.3.80	10.1.3.1	TCP	158	80 → 1029 [PSH, ACK] Seq=1599 Ac
15	10.1.3.1	10.1.3.80	TCP	66	1029 → 80 [ACK] Seq=521 Ack=231
16	10.1.3.80	10.1.3.1	TCP	14…	80 → 1029 [ACK] Seq=1691 Ack=521
17	10.1.3.80	10.1.3.1	TCP	204	80 → 1029 [PSH, ACK] Seq=3059 Ac
18	10.1.3.1	10.1.3.80	TCP	66	1029 → 80 [ACK] Seq=521 Ack=1599
19	10.1.3.1	10.1.3.80	TCP	66	1029 → 80 [ACK] Seq=521 Ack=1691
20	10.1.3.1	10.1.3.80	TCP	66	1029 → 80 [ACK] Seq=521 Ack=3059
21	10.1.3.1	10.1.3.80	TCP	66	1029 → 80 [ACK] Seq=521 Ack=3197
22	10.1.3.80	10.1.3.1	TCP	14…	80 → 1029 [ACK] Seq=3197 Ack=521
23	10.1.3.80	10.1.3.1	TCP	14…	80 → 1029 [PSH, ACK] Seq=4565 Ac
24	10.1.3.80	10.1.3.1	TCP	14…	80 → 1029 [PSH, ACK] Seq=5933 Ac
25	10.1.3.80	10.1.3.1	HTTP	218	HTTP/1.1 200 OK (text/html)

可以看到 PC2 能够访问服务器的内部资源，但是和服务器无法 ping 通。Web 模式里，PC 和防火墙进行认证后，PC 向内网发送数据时无需知道内网 PC 的地址，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。PC2 和服务器进行数据通信是通过各自的网关（即 202.1.5.1 和 10.1.3.1）进行通信

8. 步骤 10 完成后，记录和分析外网客户端方式访问过程（exp 网卡和虚拟网卡数据包）。



```
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     10.10.10.1      2
         10.0.0.0        255.0.0.0         在链路上       10.10.10.1    257
     10.10.10.1  255.255.255.255         在链路上       10.10.10.1    257
 10.255.255.255  255.255.255.255         在链路上       10.10.10.1    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      192.168.0.11    276
        224.0.0.0        240.0.0.0         在链路上       10.10.10.1    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      192.168.0.11    276
  255.255.255.255  255.255.255.255         在链路上       10.10.10.1    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
===========================================================================
```

```
以太网适配器 本地连接 2:

   连接特定的 DNS 后缀 . . . . . :
   描述. . . . . . . . . . . . . . : Cisco AnyConnect VPN Virtual Miniport Ada
pter for Windows x64
   物理地址. . . . . . . . . . . . : 00-05-9A-3C-7A-00
   DHCP 已启用 . . . . . . . . . . : 否
   自动配置已启用. . . . . . . . . : 是
   本地链接 IPv6 地址. . . . . . . . : fe80::1cfe:f26e:a9c2:56cb%35(首选)
   IPv4 地址 . . . . . . . . . . . . : 10.10.10.1(首选)
   子网掩码 . . . . . . . . . . . . : 255.0.0.0
   默认网关. . . . . . . . . . . . . : 10.0.0.1
   DHCPv6 IAID . . . . . . . . . . . : 587203994
   DHCPv6 客户端 DUID  . . . . . . . : 00-01-00-01-24-A7-91-D3-00-E0-4C-70-70-59

   DNS 服务器  . . . . . . . . . . . : fec0:0:0:ffff::1%1
                                       fec0:0:0:ffff::2%1
                                       fec0:0:0:ffff::3%1
   TCPIP 上的 NetBIOS  . . . . . . . : 已启用

以太网适配器 1-1 exp:

   连接特定的 DNS 后缀 . . . . . :
   描述. . . . . . . . . . . . . . : Realtek PCIe GBE Family Controller
   物理地址. . . . . . . . . . . . : 00-E0-4C-68-DD-02
   DHCP 已启用 . . . . . . . . . . : 否
   自动配置已启用. . . . . . . . . : 是
   本地链接 IPv6 地址. . . . . . . . : fe80::a5d6:e374:aa99:d59e%14(首选)
   IPv4 地址 . . . . . . . . . . . . : 202.1.5.3(首选)
   子网掩码 . . . . . . . . . . . . : 255.255.255.0
   默认网关. . . . . . . . . . . . . : 202.1.5.1
   DHCPv6 IAID . . . . . . . . . . . : 436265036
   DHCPv6 客户端 DUID  . . . . . . . : 00-01-00-01-24-A7-91-D3-00-E0-4C-70-70-59

   DNS 服务器  . . . . . . . . . . . : fec0:0:0:ffff::1%1
                                       fec0:0:0:ffff::2%1
                                       fec0:0:0:ffff::3%1
```

PC1 的 exp 网卡：

No	Source	Destination	Protocol	Len	Info
1	202.1.5.3	202.1.5.1	TCP	54	51752 → 443 [FIN, ACK] Seq=1 A
2	202.1.5.3	202.1.5.1	DTLS 1.0 (OpenSSL pre 0.9.8f)	151	Application Data
3	202.1.5.1	202.1.5.3	TCP	60	443 → 51752 [ACK] Seq=1 Ack=2
4	202.1.5.1	202.1.5.3	TCP	60	443 → 51752 [FIN, PSH, ACK] Se
5	202.1.5.3	202.1.5.1	TCP	54	51752 → 443 [ACK] Seq=2 Ack=2
6	202.1.5.3	202.1.5.1	DTLS 1.0 (OpenSSL pre 0.9.8f)	151	Application Data
7	202.1.5.1	202.1.5.3	DTLS 1.0 (OpenSSL pre 0.9.8f)	151	Application Data
8	202.1.5.3	202.1.5.1	DTLS 1.0 (OpenSSL pre 0.9.8f)	135	Application Data
9	202.1.5.1	202.1.5.3	DTLS 1.0 (OpenSSL pre 0.9.8f)	151	Application Data
10	202.1.5.3	202.1.5.1	DTLS 1.0 (OpenSSL pre 0.9.8f)	135	Application Data
11	202.1.5.3	202.1.5.1	DTLS 1.0 (OpenSSL pre 0.9.8f)	567	Application Data
12	202.1.5.1	202.1.5.3	DTLS 1.0 (OpenSSL pre 0.9.8f)	423	Application Data
13	202.1.5.1	202.1.5.3	DTLS 1.0 (OpenSSL pre 0.9.8f)	15…	Application Data
14	202.1.5.1	202.1.5.3	DTLS 1.0 (OpenSSL pre 0.9.8f)	231	Application Data
15	202.1.5.3	202.1.5.1	DTLS 1.0 (OpenSSL pre 0.9.8f)	135	Application Data
16	202.1.5.1	202.1.5.3	DTLS 1.0 (OpenSSL pre 0.9.8f)	15…	Application Data
17	202.1.5.1	202.1.5.3	DTLS 1.0 (OpenSSL pre 0.9.8f)	423	Application Data
18	202.1.5.3	202.1.5.1	DTLS 1.0 (OpenSSL pre 0.9.8f)	135	Application Data
19	202.1.5.3	202.1.5.1	DTLS 1.0 (OpenSSL pre 0.9.8f)	503	Application Data
20	202.1.5.3	202.1.5.1	DTLS 1.0 (OpenSSL pre 0.9.8f)	151	Application Data
21	202.1.5.3	202.1.5.1	DTLS 1.0 (OpenSSL pre 0.9.8f)	487	Application Data
22	202.1.5.1	202.1.5.3	DTLS 1.0 (OpenSSL pre 0.9.8f)	151	Application Data
23	202.1.5.3	202.1.5.1	DTLS 1.0 (OpenSSL pre 0.9.8f)	135	Application Data
24	202.1.5.3	202.1.5.1	DTLS 1.0 (OpenSSL pre 0.9.8f)	487	Application Data
25	202.1.5.1	202.1.5.3	DTLS 1.0 (OpenSSL pre 0.9.8f)	327	Application Data

PC1 的虚拟网卡：

No	Source	Destination	Protoc	Len	Info
1	Cisco_3c:7…	Broadcast	ARP	42	Who has 10.1.3.80? Tell 10.10.10.1
2	CIMSYS_33:…	Cisco_3c:7a:…	ARP	42	10.1.3.80 is at 00:11:22:33:44:55
3	10.10.10.1	10.1.3.80	TCP	66	51788 → 80 [SYN] Seq=0 Win=8192 Len=0
4	10.10.10.1	10.1.3.80	TCP	66	51789 → 80 [SYN] Seq=0 Win=8192 Len=0
5	10.1.3.80	10.10.10.1	TCP	66	80 → 51788 [SYN, ACK] Seq=0 Ack=1 Win=
6	10.10.10.1	10.1.3.80	TCP	54	51788 → 80 [ACK] Seq=1 Ack=1 Win=65536
7	10.1.3.80	10.10.10.1	TCP	66	80 → 51789 [SYN, ACK] Seq=0 Ack=1 Win=
8	10.10.10.1	10.1.3.80	TCP	54	51789 → 80 [ACK] Seq=1 Ack=1 Win=65536
9	10.10.10.1	10.1.3.80	HTTP	481	GET / HTTP/1.1
10	10.1.3.80	10.10.10.1	TCP	330	80 → 51788 [PSH, ACK] Seq=1 Ack=428 Wi
11	10.1.3.80	10.10.10.1	TCP	14…	80 → 51788 [ACK] Seq=277 Ack=428 Win=6
12	10.10.10.1	10.1.3.80	TCP	54	51788 → 80 [ACK] Seq=428 Ack=1643 Win=
13	10.1.3.80	10.10.10.1	TCP	148	80 → 51788 [PSH, ACK] Seq=1643 Ack=428
14	10.1.3.80	10.10.10.1	TCP	14…	80 → 51788 [ACK] Seq=1737 Ack=428 Win=
15	10.10.10.1	10.1.3.80	TCP	54	51788 → 80 [ACK] Seq=428 Ack=3103 Win=
16	10.1.3.80	10.10.10.1	HTTP	330	HTTP/1.1 200 OK (text/html)
17	10.10.10.1	10.1.3.80	HTTP	424	GET /?mode=section&id=style.css HTTP/1
18	10.10.10.1	10.1.3.80	TCP	66	51790 → 80 [SYN] Seq=0 Win=8192 Len=0
19	10.10.10.1	10.1.3.80	HTTP	395	GET /?mode=jquery HTTP/1.1
20	10.1.3.80	10.10.10.1	TCP	66	80 → 51790 [SYN, ACK] Seq=0 Ack=1 Win=
21	10.10.10.1	10.1.3.80	TCP	54	51790 → 80 [ACK] Seq=1 Ack=1 Win=65536
22	10.10.10.1	10.1.3.80	HTTP	406	GET /?mode=section&id=lib.js HTTP/1.1
23	10.1.3.80	10.10.10.1	TCP	242	80 → 51788 [PSH, ACK] Seq=3379 Ack=798
24	10.1.3.80	10.10.10.1	TCP	246	80 → 51789 [PSH, ACK] Seq=1 Ack=342 Wi
25	10.1.3.80	10.10.10.1	TCP	14…	80 → 51788 [ACK] Seq=3567 Ack=798 Win=
26	10.10.10.1	10.1.3.80	TCP	54	51788 → 80 [ACK] Seq=798 Ack=4933 Win=

服务器的数据包：

No	Source	Destination	Protocol	Len	Info
1	fe80::c442…	ff02::1:2	DHCPv6	147	Solicit XID: 0x022e82 CID: 0001000124a
2	10.10.10.1	10.1.3.80	TCP	66	51788 → 80 [SYN] Seq=0 Win=8192 Len=0
3	RealtekSem…	Broadcast	ARP	42	Who has 10.1.3.1? Tell 10.1.3.80
4	Cisco_fa:f…	RealtekSemic…	ARP	60	10.1.3.1 is at 00:21:55:fa:f4:3f
5	10.10.10.1	10.1.3.80	TCP	66	51789 → 80 [SYN] Seq=0 Win=8192 Len=0
6	10.1.3.80	10.10.10.1	TCP	66	80 → 51788 [SYN, ACK] Seq=0 Ack=1 Win=
7	10.1.3.80	10.10.10.1	TCP	66	80 → 51789 [SYN, ACK] Seq=0 Ack=1 Win=
8	10.10.10.1	10.1.3.80	TCP	60	51788 → 80 [ACK] Seq=1 Ack=1 Win=65536
9	10.10.10.1	10.1.3.80	TCP	60	51789 → 80 [ACK] Seq=1 Ack=1 Win=65536
10	10.10.10.1	10.1.3.80	HTTP	481	GET / HTTP/1.1
11	10.1.3.80	10.10.10.1	TCP	330	80 → 51788 [PSH, ACK] Seq=1 Ack=428 Wi
12	10.1.3.80	10.10.10.1	TCP	15…	80 → 51788 [PSH, ACK] Seq=277 Ack=428
13	10.10.10.1	10.1.3.80	TCP	60	51788 → 80 [ACK] Seq=428 Ack=1643 Win=
14	10.1.3.80	10.10.10.1	HTTP	16…	HTTP/1.1 200 OK (text/html)
15	10.10.10.1	10.1.3.80	TCP	60	51788 → 80 [ACK] Seq=428 Ack=3103 Win=
16	10.10.10.1	10.1.3.80	HTTP	424	GET /?mode=section&id=style.css HTTP/1
17	10.10.10.1	10.1.3.80	TCP	66	51790 → 80 [SYN] Seq=0 Win=8192 Len=0
18	10.1.3.80	10.10.10.1	TCP	66	80 → 51790 [SYN, ACK] Seq=0 Ack=1 Win=
19	10.10.10.1	10.1.3.80	HTTP	395	GET /?mode=jquery HTTP/1.1
20	10.10.10.1	10.1.3.80	TCP	60	51790 → 80 [ACK] Seq=1 Ack=1 Win=65536
21	10.10.10.1	10.1.3.80	HTTP	406	GET /?mode=section&id=lib.js HTTP/1.1
22	10.1.3.80	10.10.10.1	TCP	242	80 → 51788 [PSH, ACK] Seq=3379 Ack=798
23	10.1.3.80	10.10.10.1	TCP	246	80 → 51789 [PSH, ACK] Seq=1 Ack=342 Wi

<table>
<tr><td></td><td colspan="3">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，该地址就取自之前 SSLVPN 定义的地址池 ssluser，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，路由表有该局域网网关地址。虚拟网卡和内网 PC 的通过在物理上要经过物理网卡 exp,但是物理网卡 exp 不在防火墙内，所以 exp 捕获的数据包都是经过加密的数据包，数据包报文协议为 DTLS 1.0(OpenSSL pre 0.9.8f)，说明该报文需要经由防火墙处理后转发给内网 PC，即报文先由外网 PC 发送给防火墙，再由防火墙转发给内部服务器；

分析几种模式访问内部资源（内网访问、外网 web 模式、外网客户端模式）的差别，解释外部 PC 通过 VPN 访问内网的安全性。</td></tr>
<tr><td rowspan="5">本组四人主要工作：</td><td colspan="3">白佳兴：按实验指导进行操作，负责 PC2 和交换机 S1 的控制，连接设备，配置交换机、路由器的设置，负责实验的验收演示，负责实验报告的大部分撰写和统筹，负责进阶自设计部</td></tr>
<tr><td colspan="3">廖立彬：按实验指导进行操作，负责 PC1 的控制，连接设备，配置交换机、路由器的设置，负责实验的验收演示，负责实验报告的一部分撰写。</td></tr>
<tr><td colspan="3">侯凯耀：按实验指导进行操作，负责 PC3 和防火墙的控制，连接设备，配置交换机、路由器的设置，负责实验的验收演示，负责实验报告的一部分撰写。</td></tr>
<tr><td colspan="3">余小康：按实验指导进行操作，负责 PC4 和服务器的控制，连接设备，配置交换机、路由器的设置，负责实验的验收演示，负责实验报告的一部分撰写。</td></tr>
<tr><td colspan="3">谭兆基：按实验指导进行操作，帮助各组员进行实时沟通，连接设备，配置交换机、路由器的设置，负责实验的验收演示，负责实验报告的一部分撰写。</td></tr>
<tr><td>实验中问题及解决方法，经验总结</td><td colspan="3">外网 PC 登录 VPN 客户端的过程中出现无法登录的情况，分析原因应该是多个主机使用同一用户而产生了冲突，解决方案是在防火墙端注销已登陆的 VPN 用户，然后再重新登陆即可解决问题。</td></tr>
<tr><td>师生互动交流</td><td colspan="3">在验收过程中，老师主要提出的一个问题是通过 web 方式连接和客户端方式连接的区别在哪，当时我们不是很理解，老师带着我们从原理图来分析，二者最本质的区别在于客户端方式连接会生成一个虚拟网卡而 web 方式连接不生成虚拟网卡。因此，抓包结果显示，web 方式连接是主机和防火墙直接的报文的发送和接收，而客户端方式连接是两台主机间报文的发送和接受。</td></tr>
<tr><td>验收教师</td><td>张利平</td><td>本实验成绩</td><td></td></tr>
</table>