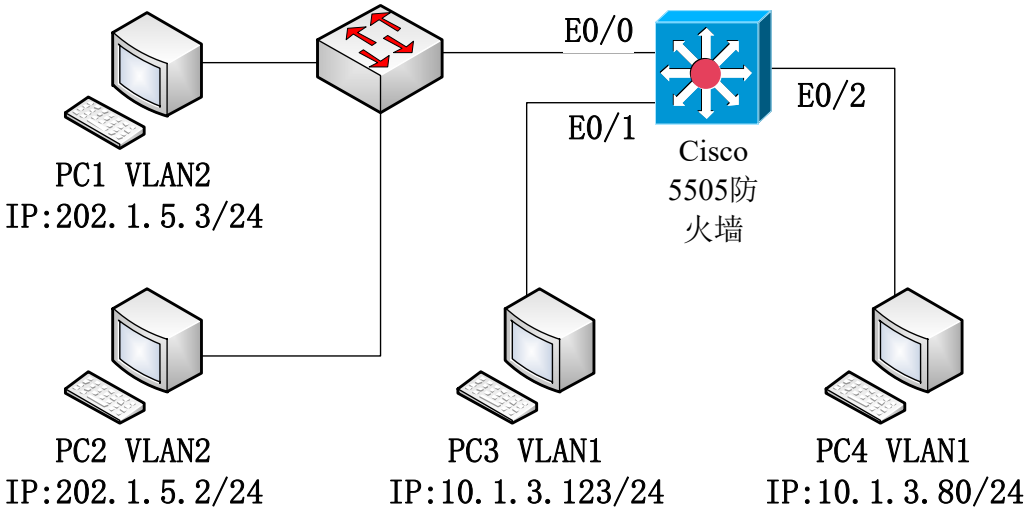
计算机网络专题实验现场检查单 7

实验名称：**防火墙与 SSLVPN 实验**　　时间：　2024 年 4 月 27 日　早☑　午☐　晚☐

组号		实验位	1	控制器地址	192.168.1.10
姓名				任天驰	

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：

Vlan 的划分：0 号端口（连接交换机）划分为 VLAN2。其余端口（连接 PC3、PC4）划分为 VLAN1。

命名：命名 vlan 1 为 inside。命名 vlan 2 为 outside。

端口分配：交换机接入防火墙的 0 口。PC3 接入防火墙的 1 口。PC4 接入防火墙的 2 口。

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

2. CISCO ASA5505 内网 DHCP 服务器的 IP 范围是：

IP 范围是：10.1.3.2-10.1.3.3

```
ciscoasa(config)# 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
```

3. SSL VPN 用户地址池的名称和地址范围是：

名称：ssluser

地址范围：10.10.10.1~10.10.10.10

```
ciscoasa(config)# ip local pool ssluser 10.10.10.1-10.10.10.10
ciscoasa(config)# access-list go-vpn permit ip 10.1.3.0 255.255.255.0 10.10.10$
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
```

4. 创建的 SSL VPN 用户名是：

vpnuser1 和 vpnuser2

```
ciscoasa(config)# username vpnuser1 password vpnuser1
ciscoasa(config)#  username vpnuser1 attributes
ciscoasa(config-username)# vpn-group-policy mypolicy
ciscoasa(config-username)# exit
ciscoasa(config)#  tunnel-group mytg type webvpn
ciscoasa(config)# tunnel-group mytg general-attributes
ciscoasa(config-tunnel-general)#
ciscoasa(config-tunnel-general)# address-pool ssluser
ciscoasa(config-tunnel-general)# exit
ciscoasa(config)# tunnel-group mytg webvpn-attributes
ciscoasa(config-tunnel-webvpn)# group-alias vpntest enable
ciscoasa(config-tunnel-webvpn)# exit
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# tunnel-group-list enable
ciscoasa(config-webvpn)# exit
ciscoasa(config)# write
Building configuration...
Cryptochecksum: 9877bd60 f1f8051f 575dc505 d5bbbec1

2804 bytes copied in 1.640 secs (2804 bytes/sec)
[OK]
```

5. 所配置的防火墙测试方案及结果是：

配置：

1、划分 VLAN 和接口：创建两个 VLAN，分别为外部（VLAN 2）和内部（VLAN 1），分配 IP 地址。将接口 e0/0 分配给 VLAN 2（外部），其他接口分配给 VLAN 1（内部）。

2、为 VLAN 分配接口并开启：配置接口 e0/0、e0/1、e0/2 分别分配给 VLAN 2 和 VLAN 1。

测试内网：

1、启用 HTTP 服务及内网 DHCP 服务器：开启 HTTP 服务和内网 DHCP 服务器，配置 IP 地址池以及内部 DHCP。

2、结果：内网之间数据传输的源地址和目的地址就是两个 pc 的 ip 地址，互相之间可直接通信，不加密。

测试外网 Web 模式：

1、在外网口上启动 WEBVPN，并同时启动 SSL VPN 功能：配置 WEBVPN 服务并在外网口上启用。启用 SSL VPN 并指定 SSL VPN Client 软件包。

2、创建 SSL VPN 用户 IP 地址池：创建 SSL VPN 用户的 IP 地址池，并配置存取控制列表以定义访问权限。配置 NAT，以确保内部访问不经过 NAT 翻译。

3、WEB VPN 隧道组与策略组的配置：创建 SSL VPN 组策略并配置内部组策略特性。配置 SSL VPN 隧道组，并为其启用 SSL VPN。

4、创建 SSL VPN 用户并赋予访问策略：创建 SSL VPN 用户并分配组策略。配置 SSL VPN 隧道组，并为其启用别名以简化 SSL VPN 用户访问。

5、外网 Web 模式访问内部 Web 资源：通过浏览器访问 WEB VPN，在弹出的对话框中输入用户名和密码登录。测试访问内部资源，进行数据包分析和网络连通性测试。

6、结果：两台主机都是在跟自己的网关对话，外网间加密，内网间不加密。

测试外网客户端模式：

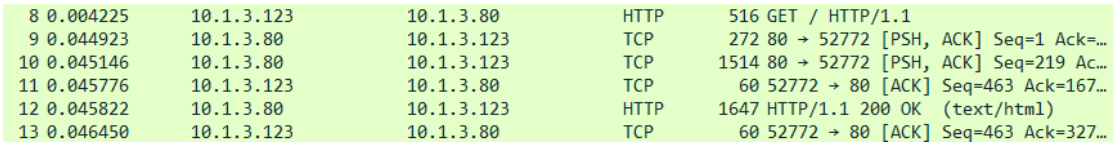
1、外网客户端模式访问内部 Web 资源：安装 AnyConnect 客户端并登录 VPN。测试访问内部资源，进行数据包分析和网络连通性测试。

2、结果：外网 pc 的物理网卡上抓到的是 pc 跟自己的网关加密通信，外网 pc 的虚拟网卡上抓到的是它使用 SSL VPN 用户地址池中的某个地址跟内网 pc 不加密通信，内网 pc 上抓到的是 pc 跟内网上的另一个设备直接不加密通信。

6. 步骤 8 完成后，记录和分析内网方式访问过程。

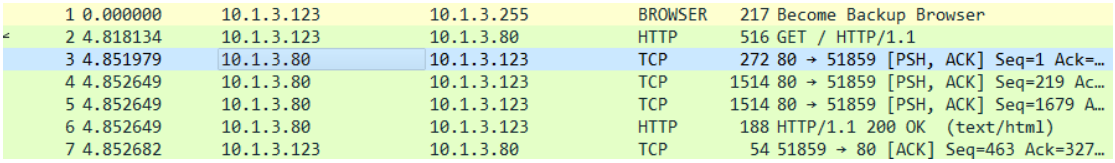
在 PC3 访问服务器下载资源。

下图是服务器抓包图



8	0.004225	10.1.3.123	10.1.3.80	HTTP	516 GET / HTTP/1.1
9	0.044923	10.1.3.80	10.1.3.123	TCP	272 80 → 52772 [PSH, ACK] Seq=1 Ack=…
10	0.045146	10.1.3.80	10.1.3.123	TCP	1514 80 → 52772 [PSH, ACK] Seq=219 Ac…
11	0.045776	10.1.3.123	10.1.3.80	TCP	60 52772 → 80 [ACK] Seq=463 Ack=167…
12	0.045822	10.1.3.80	10.1.3.123	HTTP	1647 HTTP/1.1 200 OK (text/html)
13	0.046450	10.1.3.123	10.1.3.80	TCP	60 52772 → 80 [ACK] Seq=463 Ack=327…

下图是 PC3 抓包图



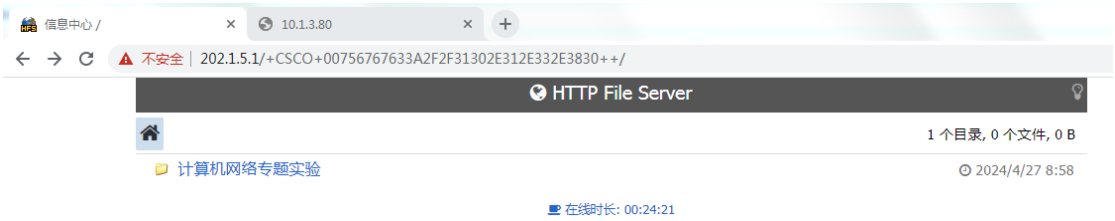
1	0.000000	10.1.3.123	10.1.3.255	BROWSER	217 Become Backup Browser
2	4.818134	10.1.3.123	10.1.3.80	HTTP	516 GET / HTTP/1.1
3	4.851979	10.1.3.80	10.1.3.123	TCP	272 80 → 51859 [PSH, ACK] Seq=1 Ack=…
4	4.852649	10.1.3.80	10.1.3.123	TCP	1514 80 → 51859 [PSH, ACK] Seq=219 Ac…
5	4.852649	10.1.3.80	10.1.3.123	TCP	1514 80 → 51859 [PSH, ACK] Seq=1679 A…
6	4.852649	10.1.3.80	10.1.3.123	HTTP	188 HTTP/1.1 200 OK (text/html)
7	4.852682	10.1.3.123	10.1.3.80	TCP	54 51859 → 80 [ACK] Seq=463 Ack=327…

二者之间一一对应，可以将访问过程概括为下表

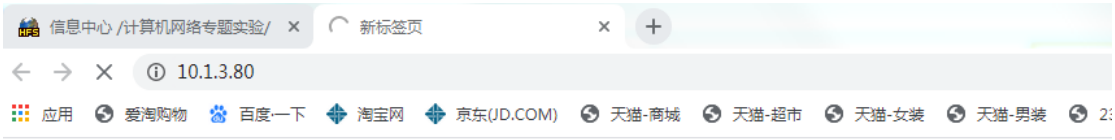
抓包位置	源地址	目的地址	主要协议	是否加密
PC3	10.1.3.123	10.1.3.80	TCP	否
服务器	10.1.3.80	10.1.3.123	TCP	否

7. 步骤 9 完成后，记录和分析外网 Web 方式访问过程。

在 PC2 浏览器中输入 https://202.1.5.1 访问 WEB VPN，登录 vpnuser2。可以访问 Web 资源，如下页图所示



打开一个新网页，在地址栏输入内部服务器地址，发现无法访问内网资源如下图所示



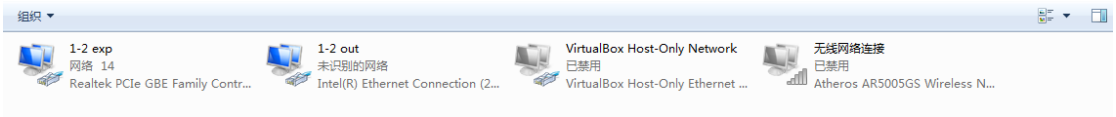
如下图，ping 内网 10.1.3.80，发现无法 ping 通

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

正在 Ping 10.1.3.80 具有 32 字节的数据:
请求超时。
请求超时。
请求超时。
请求超时。

10.1.3.80 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 0, 丢失 = 4 (100% 丢失),
```

检查本地网卡，发现没有虚拟网卡



查看 PC2 路由表，发现没有与 10.x.x.x 有关的路由记录

```
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
===========================================================================
```

PC2 抓包如下图所示

5	0.160791	202.1.5.2	202.1.5.1	TLSv1	896 Application Data, Application Da…
6	0.161128	202.1.5.1	202.1.5.2	TCP	60 443 → 53166 [ACK] Seq=1 Ack=843 …
7	0.168847	202.1.5.1	202.1.5.2	TLSv1	299 Application Data
8	0.168847	202.1.5.1	202.1.5.2	TLSv1	107 Application Data
9	0.168922	202.1.5.2	202.1.5.1	TCP	54 53166 → 443 [ACK] Seq=843 Ack=29…
10	0.169756	202.1.5.1	202.1.5.2	TLSv1	91 Application Data
11	0.186000	202.1.5.2	202.1.5.1	TLSv1	1056 Application Data, Application Da…
12	0.186329	202.1.5.1	202.1.5.2	TCP	60 443 → 53166 [ACK] Seq=336 Ack=18…
13	0.186714	202.1.5.1	202.1.5.2	TCP	60 [TCP Window Update] 443 → 53166 …
14	0.223841	202.1.5.1	202.1.5.2	TLSv1	267 Application Data

服务器抓包如下图所示

1	0.000000	10.1.3.1	10.1.3.80	TCP	74 1063 → 80 [SYN] Seq=0 Win=8192 L…
2	0.000102	10.1.3.80	10.1.3.1	TCP	70 80 → 1063 [SYN, ACK] Seq=0 Ack=1…
3	0.000516	10.1.3.1	10.1.3.80	TCP	66 1063 → 80 [ACK] Seq=1 Ack=1 Win=…
4	0.000906	10.1.3.1	10.1.3.80	HTTP	623 GET / HTTP/1.1
5	0.035240	10.1.3.80	10.1.3.1	TCP	238 80 → 1063 [PSH, ACK] Seq=1 Ack=5…
6	0.035473	10.1.3.80	10.1.3.1	TCP	1434 80 → 1063 [ACK] Seq=173 Ack=558 …
7	0.035473	10.1.3.80	10.1.3.1	TCP	158 80 → 1063 [PSH, ACK] Seq=1541 Ac…
8	0.035622	10.1.3.1	10.1.3.80	TCP	66 1063 → 80 [ACK] Seq=558 Ack=173 …

服务器发送数据给 PC2 过程中报文的信息总结如下表

抓包位置	源地址	目的地址	主要协议	是否加密
PC2	202.1.5.1	202.1.5.2	TLS	是
服务器	10.1.3.80	10.1.3.1	TCP	否

访问过程：服务器将数据包通过 TCP 发给网关 10.1.3.1（防火墙），之后防火墙将数据加密，通过 TLS 在公网传输，至 202.1.5.1（PC2 网关）。最后 202.1.5.1 把相应的数据包发给 PC2。这个过程中内，内网传输部分（服务器到防火墙）没有加密，公网传输部分使用了 TLS 加密。

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）。

在 PC1 下载安装 AnyConnect 客户端并登录 vpnuser1。可以发现已经出现了虚拟网卡。

```
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::2496:57b3:3346:d464%20(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 . . . . . . . . . . . : 335545754
   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
```

打开一个新网页，在地址栏输入内部服务器地址，发现可以访问，运行 ping 测试网络连通性如下图

```
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
```

查看 PC1 路由表，可以发现出现了 10.0.0.0 和 10.10.10.1 这样的记录

```
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       10.0.0.1      10.10.10.1      2
          0.0.0.0          0.0.0.0     202.1.5.1      202.1.5.3    276
         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
===========================================================================
```

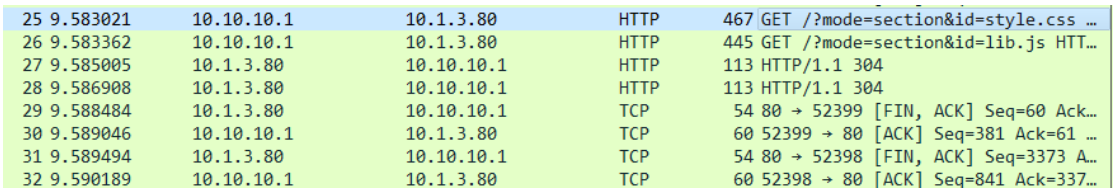
PC1 物理网卡抓包如下图所示

1699	19.154687	202.1.5.1	202.1.5.3	DTLS 1…	1511	Application Data
1700	19.154687	202.1.5.1	202.1.5.3	DTLS 1…	231	Application Data
1701	19.154687	202.1.5.1	202.1.5.3	DTLS 1…	1511	Application Data
1702	19.154687	202.1.5.1	202.1.5.3	DTLS 1…	231	Application Data
1703	19.154819	202.1.5.3	202.1.5.1	DTLS 1…	135	Application Data
1704	19.154869	202.1.5.3	202.1.5.1	DTLS 1…	135	Application Data

PC1 虚拟网卡抓包如下图所示

52	7.930200	10.10.10.1	10.1.3.80	HTTP	467 GET /?mode=section&id=style.css …
53	7.930362	10.10.10.1	10.1.3.80	HTTP	434 GET /?mode=jquery HTTP/1.1
54	7.930433	10.1.3.80	10.10.10.1	TCP	66 80 → 52400 [SYN, ACK] Seq=0 Ack=…
55	7.930461	10.10.10.1	10.1.3.80	TCP	54 52400 → 80 [ACK] Seq=1 Ack=1 Win…
56	7.930631	10.10.10.1	10.1.3.80	HTTP	445 GET /?mode=section&id=lib.js HTT…
57	7.933175	10.1.3.80	10.10.10.1	HTTP	113 HTTP/1.1 304
58	7.935057	10.1.3.80	10.10.10.1	HTTP	113 HTTP/1.1 304
59	7.936607	10.1.3.80	10.10.10.1	TCP	54 80 → 52399 [FIN, ACK] Seq=60 Ack…
60	7.936650	10.10.10.1	10.1.3.80	TCP	54 52399 → 80 [ACK] Seq=381 Ack=61 …

服务器抓包如下图所示



25	9.583021	10.10.10.1	10.1.3.80	HTTP	467 GET /?mode=section&id=style.css …
26	9.583362	10.10.10.1	10.1.3.80	HTTP	445 GET /?mode=section&id=lib.js HTT…
27	9.585005	10.1.3.80	10.10.10.1	HTTP	113 HTTP/1.1 304
28	9.586908	10.1.3.80	10.10.10.1	HTTP	113 HTTP/1.1 304
29	9.588484	10.1.3.80	10.10.10.1	TCP	54 80 → 52399 [FIN, ACK] Seq=60 Ack…
30	9.589046	10.10.10.1	10.1.3.80	TCP	60 52399 → 80 [ACK] Seq=381 Ack=61 …
31	9.589494	10.1.3.80	10.10.10.1	TCP	54 80 → 52398 [FIN, ACK] Seq=3373 A…
32	9.590189	10.10.10.1	10.1.3.80	TCP	60 52398 → 80 [ACK] Seq=841 Ack=337…

其中，PC1 虚拟网卡和服务器中抓的包一一对应。但两个包的帧头以及以太网协议部分不同。这是显然的，因为即使 PC1 虚拟网卡和服务器间的通信可以看作在一个局域网内通信，但终究需要经过公网隧道，而虚拟网卡封装的信息并不是真实的。在物理网卡中的包反映了实际，数据包必须经由网关（202.1.5.1）转发。

服务器发送数据给 PC1 过程中报文的信息总结如下表

抓包位置	源地址	目的地址	主要协议	是否加密
PC1 物理网卡	202.1.5.1	202.1.5.3	DTLS	是
PC1 虚拟网卡	10.1.3.80	10.10.10.1	TCP	否
服务器	10.1.3.80	10.10.10.1	TCP	否

访问过程：服务器向 10.10.10.1（MAC：Cisco_fa:f4:3f (00:21:55:fa:f4:3f)，实际上是防火墙，该 IP 属于防火墙创建的用户池）发送未加密的 TCP 包，防火墙将数据通过 DTLS（基于 UCP 的加密通信协议）加密发送到 202.1.5.1（PC1 网关），最后发给 PC1 实现通信。

在 PC1 的物理网卡收到加密数据包后，这些数据包通过网络适配器被传输到 PC1 的操作系统内核。操作系统的网络协议栈识别出这些数据包是发送到 PC1 的虚拟网卡的。虚拟网卡被认为是操作系统的一部分，因此操作系统会将接收到的数据包传递给虚拟网卡。虚拟网卡收到加密数据包后，会调用 VPN 客户端软件中的解密模块，解密数据包内容。解密后的 TCP 数据包被虚拟网卡传递给操作系统的网络协议栈。操作系统会根据目标 IP 地址（10.10.10.1）和端口号等信息来确定如何处理这些数据包。

总的来说，虚拟网卡在 PC1 上扮演了一个接收和解密加密数据的角色，它能够从物理网卡上获取加密数据，并使用 VPN 客户端软件提供的解密功能将数据解密后传递给操作系统进行处理。

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。

内网访问：

在内网访问模式下，用户直接连接到内部网络，无需通过 VPN（Virtual Private Network，虚拟专用网络）进行连接。用户可以直接访问内部资源，因为他们已经位于内部网络中。

外网 Web 模式：

在外网 Web 模式下，用户通过 Web 浏览器访问内部资源，通常通过 SSL/TLS 加密。用户需要通过登录页面进行身份验证，网络管理员可以通过防火墙和代理服务器来控制对内部资源的访问，并对用户进行身份验证和授权。这种模式访问受限，只能通过 Web 界面访问部分内部资源，不适用于所有应用程序或服务。

外网客户端模式：

在外网客户端模式下，用户需要需要安装额外的 VPN 客户端软件，并通过 VPN 客户端软件提供的身份验证机制进行身份验证。该软件会为用户的计算机创建一个虚拟网络接口，通过该接口发送的数据会被加密并通过 VPN 隧道传输到远程网络。外网客户端模式不仅适用于通过 Web 界面访问的情况，还可以用于任何需要安全访问内部资源的场景。用户可以通过本地应用程序直接访问内部服务器、共享文件等，而无需限制于 Web 界面。VPN 客户端通常提供了更多的功能和配置选项，如拆分隧道、路由控制、网络隔离等。这使得外网客户端模式在网络配置和安全性方面具有更高的灵活性和功能性。

外部 PC 通过 VPN 访问内网提供了一种安全的远程访问方式，通过加密通信、身份验证、访问控制、网络隔离和防火墙穿越等多重安全措施，有效保护了内部资源的安全性和隐私性，防止未经授权的访问和数据泄露。下面介绍这些特征：

加密通信： VPN 通过在公共网络上创建加密的隧道，将外部 PC 和内网之间的通信加密传输。这意味着即使数据在公共网络上被截获，黑客也无法读取其中的内容，因为数据是经过加密的。

身份验证： 外部 PC 在连接到 VPN 时通常需要进行身份验证，以确保只有经过授权的用户可以访问内网资源。这可以通过用户名和密码、证书或其他多因素身份验证方法来实现。

访问控制： VPN 服务器通常会实施访问控制策略，以确保只有经过授权的用户可以访问特定的内部资源。这可以根据用户身份、角色、设备健康状态等因素进行限制。

网络隔离： VPN 连接可以将外部 PC 隔离在内部网络之外，并且通常只允许访问特定的内部资源。这可以减少攻击面，防止外部 PC 对内部网络造成潜在的安全风险。

防火墙穿越： VPN 连接通常能够穿越防火墙，建立安全的连接。这意味着外部 PC 可以从任何位置连接到内部网络，即使在受限制的网络环境中也可以访问内部资源。

进阶自设计

内网访问

ip.addr==202.117.1.13

No.	Time	Source	Destination	Protocol	Lengtl	Info
2027	10.378364	192.168.1.105	202.117.1.13	TCP	66	62261 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
2029	10.380186	202.117.1.13	192.168.1.105	TCP	66	443 → 62261 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1440 SACK_PERM WS=12
2030	10.380275	192.168.1.105	202.117.1.13	TCP	54	62261 → 443 [ACK] Seq=1 Ack=1 Win=132352 Len=0
2031	10.380626	192.168.1.105	202.117.1.13	TCP	1494	62261 → 443 [ACK] Seq=1 Ack=1 Win=132352 Len=1440 [TCP segment of a reassembl
2032	10.380626	192.168.1.105	202.117.1.13	TLSv1.2	371	Client Hello (SNI=www.xjtu.edu.cn)
2033	10.381432	192.168.1.105	202.117.1.13	TCP	66	62263 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
2034	10.382007	202.117.1.13	192.168.1.105	TCP	54	443 → 62261 [ACK] Seq=1 Ack=1758 Win=18176 Len=0
2035	10.382422	202.117.1.13	192.168.1.105	TLSv1.2	1494	Server Hello
2036	10.382874	202.117.1.13	192.168.1.105	TCP	1494	443 → 62261 [ACK] Seq=1441 Ack=1758 Win=18176 Len=1440 [TCP segment of a rea
2037	10.382874	202.117.1.13	192.168.1.105	TCP	1270	443 → 62261 [PSH, ACK] Seq=2881 Ack=1758 Win=18176 Len=1216 [TCP segment of
2038	10.382874	202.117.1.13	192.168.1.105	TCP	66	443 → 62263 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1440 SACK_PERM WS=12
2039	10.383047	192.168.1.105	202.117.1.13	TCP	54	62261 → 443 [ACK] Seq=1758 Ack=4097 Win=132352 Len=0
2040	10.383195	192.168.1.105	202.117.1.13	TCP	54	62263 → 443 [ACK] Seq=1 Ack=1 Win=132352 Len=0
2041	10.383551	192.168.1.105	202.117.1.13	TCP	1494	62263 → 443 [ACK] Seq=1 Ack=1 Win=132352 Len=1440 [TCP segment of a reassembl

对于 www.xjtu.edu.cn(地址 202.117.1.13),与本地 PC 进行直接 TCP 和 TLS 连接，表明其在加密通信，传递数据

ip.addr==192.168.1.105

.	Time	Source	Destination	Protocol	Lengtl	Info
5	3.931862	192.168.1.105	103.28.8.25	TCP	54	62217 → 80 [ACK] Seq=1 Ack=1 Win=132352 Len=0
6	3.948007	192.168.1.105	103.28.8.25	HTTP	657	POST /scan HTTP/1.1 (application/x-www-form-urlencoded)
7	3.972375	103.28.8.25	192.168.1.105	TCP	54	80 → 62217 [ACK] Seq=1 Ack=604 Win=64128 Len=0
8	3.972375	103.28.8.25	192.168.1.105	HTTP	322	HTTP/1.1 200 OK
9	3.972375	103.28.8.25	192.168.1.105	TCP	54	80 → 62217 [FIN, ACK] Seq=269 Ack=604 Win=64128 Len=0
10	3.972473	192.168.1.105	103.28.8.25	TCP	54	62217 → 80 [ACK] Seq=604 Ack=270 Win=132096 Len=0
11	3.972544	192.168.1.105	103.28.8.25	TCP	54	62217 → 80 [FIN, ACK] Seq=604 Ack=270 Win=132096 Len=0
12	3.993794	103.28.8.25	192.168.1.105	TCP	54	80 → 62217 [ACK] Seq=270 Ack=605 Win=64128 Len=0
13	4.239356	192.168.1.105	61.134.1.4	DNS	72	Standard query 0xc262 A www.bing.com
14	4.241673	192.168.1.105	103.28.8.250	TCP	66	62218 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_
15	4.246391	61.134.1.4	192.168.1.105	DNS	222	Standard query response 0xc262 A www.bing.com CNAME wwwprod.
16	4.264965	103.28.8.250	192.168.1.105	TCP	62	80 → 62218 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1440 W
17	4.265050	192.168.1.105	103.28.8.250	TCP	54	62218 → 80 [ACK] Seq=1 Ack=1 Win=132352 Len=0
18	4.265175	192.168.1.105	103.28.8.250	HTTP	633	POST /wdinfo.php HTTP/1.1
19	4.269725	192.168.1.105	180.163.252.156	TCP	66	62219 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_
20	4.284943	103.28.8.250	192.168.1.105	TCP	54	80 → 62218 [ACK] Seq=1 Ack=580 Win=64128 Len=0
21	4.285950	103.28.8.250	192.168.1.105	HTTP	480	HTTP/1.1 200 OK

对于本地 PC（192.168.1.105），在内网中不依靠网关转发数据和 DNS 查询，而是直接进行 TCP 连接和 HTTP 访问

外网 WEBVPN 访问

ip.addr==192.168.139.149

No.	Time	Source	Destination	Protocol	Length	Info
37	2.617267	192.168.139.111	192.168.139.149	DNS	78	Standard query 0x2147 A galaxy.safe.360.cn
38	2.644642	192.168.139.149	192.168.139.111	DNS	331	Standard query response 0x2147 A galaxy.safe.360.cn A 180.163.246.68 A 3
144	11.649912	192.168.139.111	192.168.139.149	DNS	94	Standard query 0x83b7 A edge-consumer-static.azureedge.net
145	11.650145	192.168.139.111	192.168.139.149	DNS	94	Standard query 0x318c HTTPS edge-consumer-static.azureedge.net
146	11.691564	192.168.139.149	192.168.139.111	DNS	347	Standard query response 0x83b7 A edge-consumer-static.azureedge.net CNAME
147	11.691564	192.168.139.149	192.168.139.111	DNS	293	Standard query response 0x318c HTTPS edge-consumer-static.azureedge.net C
326	23.830073	192.168.139.111	192.168.139.149	DNS	70	Standard query 0x2324 A s.f.360.cn
327	23.864822	192.168.139.111	192.168.139.149	DNS	70	Standard query 0x2324 A s.f.360.cn
328	23.874116	192.168.139.149	192.168.139.111	DNS	299	Standard query response 0x2324 A s.f.360.cn CNAME s.f.qh-lb.com A 111.7.6
329	23.874116	192.168.139.149	192.168.139.111	DNS	129	Standard query response 0x2324 A s.f.360.cn CNAME s.f.qh-lb.com A 111.7.6
644	41.877824	192.168.139.111	192.168.139.149	DNS	76	Standard query 0x4043 A go.microsoft.com
645	41.878128	192.168.139.111	192.168.139.149	DNS	76	Standard query 0x4e6f HTTPS go.microsoft.com
646	41.893923	192.168.139.111	192.168.139.149	DNS	78	Standard query 0xaece A edge.microsoft.com
647	41.894158	192.168.139.111	192.168.139.149	DNS	78	Standard query 0xd1f0 HTTPS edge.microsoft.com

本地 IP 地址为 192.168.139.149，以上为本地 PC 与本地网关（192.168.139.111）发送 DNS 解析的过程

3190	126.2731…	192.168.139.111	192.168.139.149	DNS	78	Standard query 0xa3ae A webvpn.xjtu.edu.cn
3191	126.2734…	192.168.139.111	192.168.139.149	DNS	78	Standard query 0x6ac9 HTTPS webvpn.xjtu.edu.cn
3192	126.2979…	192.168.139.149	192.168.139.111	DNS	222	Standard query response 0xa3ae A webvpn.xjtu.edu.cn A 117.32.15
3193	126.3022…	192.168.139.149	192.168.139.111	DNS	127	Standard query response 0x6ac9 HTTPS webvpn.xjtu.edu.cn SOA dec
3194	126.3027…	192.168.139.111	117.32.153.183	TCP	66	61402 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PE
3195	126.3297…	117.32.153.183	192.168.139.111	TCP	66	443 → 61402 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1360 SAC
3196	126.3298…	192.168.139.111	117.32.153.183	TCP	54	61402 → 443 [ACK] Seq=1 Ack=1 Win=66560 Len=0
3197	126.3301…	192.168.139.111	117.32.153.183	TCP	1414	61402 → 443 [ACK] Seq=1 Ack=1 Win=66560 Len=1360 [TCP segment c
3198	126.3301…	192.168.139.111	117.32.153.183	TLSv1.2	454	Client Hello (SNI=webvpn.xjtu.edu.cn)

本地网关 192.168.139.111 与 webvpn.xjtu.edu.cn(地址 117.32.156.183)建立 TCP 与 TLS 连接，为加密连接

ip.addr==117.32.153.183

No.	Time	Source	Destination	Protocol	Length	Info
3194	126.3027…	192.168.139.111	117.32.153.183	TCP	66	61402 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
3195	126.3297…	117.32.153.183	192.168.139.111	TCP	66	443 → 61402 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1360 SACK_PERM WS=512
3196	126.3298…	192.168.139.111	117.32.153.183	TCP	54	61402 → 443 [ACK] Seq=1 Ack=1 Win=66560 Len=0
3197	126.3301…	192.168.139.111	117.32.153.183	TCP	1414	61402 → 443 [ACK] Seq=1 Ack=1 Win=66560 Len=1360 [TCP segment of a reassembled PDU]
3198	126.3301…	192.168.139.111	117.32.153.183	TLSv1.2	454	Client Hello (SNI=webvpn.xjtu.edu.cn)
3205	126.3695…	117.32.153.183	192.168.139.111	TCP	54	443 → 61402 [ACK] Seq=1 Ack=1361 Win=17920 Len=0
3206	126.3695…	117.32.153.183	192.168.139.111	TCP	54	443 → 61402 [ACK] Seq=1 Ack=1761 Win=20480 Len=0
3207	126.3695…	117.32.153.183	192.168.139.111	TLSv1.2	1414	Server Hello
3208	126.3695…	117.32.153.183	192.168.139.111	TCP	1414	443 → 61402 [ACK] Seq=1361 Ack=1761 Win=20480 Len=1360 [TCP segment of a reassembled PDU]
3209	126.3695…	117.32.153.183	192.168.139.111	TCP	1414	443 → 61402 [ACK] Seq=2721 Ack=1761 Win=20480 Len=1360 [TCP segment of a reassembled PDU]
3210	126.3695…	117.32.153.183	192.168.139.111	TCP	70	443 → 61402 [PSH, ACK] Seq=4081 Ack=1761 Win=20480 Len=16 [TCP segment of a reassembled P
3211	126.3695…	117.32.153.183	192.168.139.111	TLSv1.2	448	Certificate, Server Key Exchange, Server Hello Done
3212	126.3696…	192.168.139.111	117.32.153.183	TCP	54	61402 → 443 [ACK] Seq=1761 Ack=4491 Win=66560 Len=0
3213	126.3739…	192.168.139.111	117.32.153.183	TCP	66	61404 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
3215	126.3806…	192.168.139.111	117.32.153.183	TLSv1.2	147	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
3216	126.3808…	192.168.139.111	117.32.153.183	TLSv1.2	909	Application Data

对于 webvpn.xjtu.edu.cn(地址 117.32.156.183)，则只有 TCP 与 TLS 连接的报文，与本地 PC 的网关 192.168.139.111 进行通信，仍为加密连接

1201	117.6762…	192.168.139.111	112.65.69.207	HTTP	288	GET /xtrk/acntr.gif?mid=9ae13bf2a4d6e4e727b
1211	117.7144…	112.65.69.207	192.168.139.111	HTTP	79	HTTP/1.1 100 Continue
1212	117.7146…	192.168.139.111	112.65.69.207	HTTP	1236	POST /main/v2/winpp/acheck?m2=737c160cfaff8
1225	117.7442…	192.168.139.111	111.7.68.178	HTTP	681	POST /wdinfo.php HTTP/1.1
1227	117.7454…	112.65.69.207	192.168.139.111	HTTP	214	HTTP/1.1 200 OK (GIF89a)
1231	117.7499…	192.168.139.111	112.65.69.207	HTTP	288	GET /xtrk/acntr.gif?mid=9ae13bf2a4d6e4e727b
1235	117.7996…	111.7.68.178	192.168.139.111	HTTP	480	HTTP/1.1 200 OK
1247	117.8118…	112.65.69.207	192.168.139.111	HTTP	214	HTTP/1.1 200 OK (GIF89a)
1287	117.8532…	112.65.69.207	192.168.139.111	HTTP/J…	902	HTTP/1.1 200 OK , JSON (application/json)
2836	124.3834…	192.168.139.111	111.7.68.178	HTTP	665	POST /wdinfo.php HTTP/1.1
2896	124.5565…	111.7.68.178	192.168.139.111	HTTP	488	HTTP/1.1 200 OK
3224	126.4077…	192.168.139.111	111.7.68.178	HTTP	697	POST /wdinfo.php HTTP/1.1
3250	126.4634…	111.7.68.178	192.168.139.111	HTTP	440	HTTP/1.1 200 OK
3300	127.4366…	192.168.139.111	111.7.68.178	HTTP	729	POST /wdinfo.php HTTP/1.1
3308	127.4993…	111.7.68.178	192.168.139.111	HTTP	440	HTTP/1.1 200 OK

以上为 http 请求，全部由网关 192.168.139.111 即本地网关负责通信

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	192.168.139.149	192.168.139.111	55
127.0.0.0	255.0.0.0	在链路上	127.0.0.1	331
127.0.0.1	255.255.255.255	在链路上	127.0.0.1	331
127.255.255.255	255.255.255.255	在链路上	127.0.0.1	331
172.19.64.0	255.255.240.0	在链路上	172.19.64.1	271
172.19.64.1	255.255.255.255	在链路上	172.19.64.1	271
172.19.79.255	255.255.255.255	在链路上	172.19.64.1	271
192.168.119.0	255.255.255.0	在链路上	192.168.119.1	291
192.168.119.1	255.255.255.255	在链路上	192.168.119.1	291
192.168.119.255	255.255.255.255	在链路上	192.168.119.1	291
192.168.137.0	255.255.255.0	在链路上	192.168.137.1	291
192.168.137.1	255.255.255.255	在链路上	192.168.137.1	291
192.168.137.255	255.255.255.255	在链路上	192.168.137.1	291
192.168.139.0	255.255.255.0	在链路上	192.168.139.111	311
192.168.139.111	255.255.255.255	在链路上	192.168.139.111	311
192.168.139.255	255.255.255.255	在链路上	192.168.139.111	311
224.0.0.0	240.0.0.0	在链路上	127.0.0.1	331
224.0.0.0	240.0.0.0	在链路上	192.168.139.111	311
224.0.0.0	240.0.0.0	在链路上	192.168.119.1	291
224.0.0.0	240.0.0.0	在链路上	192.168.137.1	291
224.0.0.0	240.0.0.0	在链路上	172.19.64.1	271

打开路由表，同样没有到 VPN 服务器的路由，同时也没有虚拟网卡

外网 SSLVPN 访问

```
以太网适配器 以太网 2:

   连接特定的 DNS 后缀 . . . . . :
   描述. . . . . . . . . . . . . . : Sangfor SSL VPN CS Support System VNIC
   物理地址. . . . . . . . . . . . : 00-FF-FC-AC-81-1B
   DHCP 已启用 . . . . . . . . . . : 否
   自动配置已启用. . . . . . . . . : 是
   本地链接 IPv6 地址. . . . . . . : fe80::31ba:e02b:754:b9b7%35(首选)
   IPv4 地址 . . . . . . . . . . . : 10.184.65.8(首选)
   子网掩码 . . . . . . . . . . . . : 255.255.255.0
   默认网关. . . . . . . . . . . . :
   DHCPv6 IAID . . . . . . . . . . : 587268092
   DHCPv6 客户端 DUID . . . . . . . : 00-01-00-01-2A-4A-EB-5C-58-11-22-83-EB-A7
   DNS 服务器 . . . . . . . . . . . : 127.0.0.1
   TCPIP 上的 NetBIOS . . . . . . . : 已启用

无线局域网适配器 WLAN:

   连接特定的 DNS 后缀 . . . . . :
   描述. . . . . . . . . . . . . . : MediaTek Wi-Fi 6 MT7921 Wireless LAN Card
   物理地址. . . . . . . . . . . . : 78-65-18-2F-9D-1B
   DHCP 已启用 . . . . . . . . . . : 是
   自动配置已启用. . . . . . . . . : 是
   本地链接 IPv6 地址. . . . . . . : fe80::23e5:b682:4985:e85b%15(首选)
   IPv4 地址 . . . . . . . . . . . : 192.168.31.240(首选)
   子网掩码 . . . . . . . . . . . . : 255.255.255.0
   获得租约的时间 . . . . . . . . . : 2024年5月5日 20:37:35
   租约过期的时间 . . . . . . . . . : 2024年5月6日 8:37:37
   默认网关. . . . . . . . . . . . : 192.168.31.1
   DHCP 服务器 . . . . . . . . . . : 192.168.31.1
   DHCPv6 IAID . . . . . . . . . . : 162827421
   DHCPv6 客户端 DUID . . . . . . . : 00-01-00-01-2A-4A-EB-5C-58-11-22-83-EB-A7
   DNS 服务器 . . . . . . . . . . . : 127.0.0.1
                                       192.168.31.1
   TCPIP 上的 NetBIOS . . . . . . . : 已启用
```

如图，WLAN 网卡配置的本机 IP 为 192.168.31.240，SSLVPN 虚拟网卡的本机 IP 为 10.184.65.8

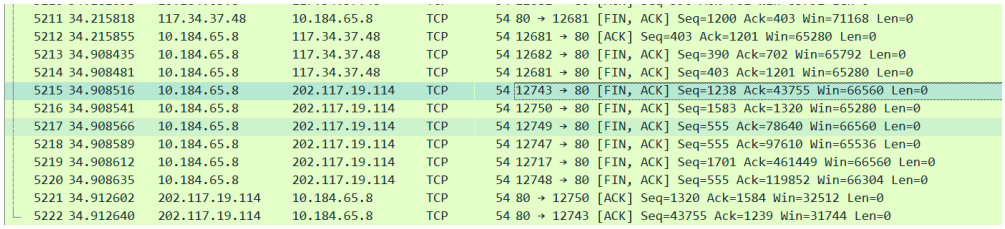
使用 SSLVPN 时我们首先检查网卡，发现多了一个虚拟以太网适配器，从其描述可以看出是 sslvpn：

在配置好后我们浏览数个 www.xjtu.edu.cn 的网页，使用 wireshark 抓包：

在 WLAN 网卡中，大部分流量是通过 TCP 协议由 WLAN 网卡的本机地址 192.168.31.240 发送至 61.185.212.158：

8283	40.475087	61.185.212.158	192.168.31.240	TLSv1…	1494	Application Data
8284	40.475178	192.168.31.240	61.185.212.158	TLSv1…	119	Application Data
8285	40.475320	61.185.212.158	192.168.31.240	TLSv1…	1464	Application Data
8286	40.475334	192.168.31.240	61.185.212.158	TCP	54	5164 → 443 [ACK] Seq=1 Ack=4492685 Win=32768 Len=0
8287	40.475558	61.185.212.158	192.168.31.240	TLSv1…	1494	Application Data
8288	40.475656	192.168.31.240	61.185.212.158	TLSv1…	119	Application Data
8289	40.475798	61.185.212.158	192.168.31.240	TLSv1…	1494	Application Data
8290	40.475819	192.168.31.240	61.185.212.158	TCP	54	5164 → 443 [ACK] Seq=1 Ack=4495565 Win=32768 Len=0
8291	40.476019	61.185.212.158	192.168.31.240	TLSv1…	1449	Application Data
8292	40.476120	192.168.31.240	61.185.212.158	TLSv1…	119	Application Data
8293	40.484532	192.168.31.240	61.185.212.158	TLSv1…	119	Application Data
8294	40.485170	61.185.212.158	192.168.31.240	TCP	60	443 → 5163 [ACK] Seq=1 Ack=178215 Win=1526 Len=0
8295	40.485170	61.185.212.158	192.168.31.240	TCP	60	443 → 5163 [ACK] Seq=1 Ack=178605 Win=1526 Len=0
8296	40.485314	61.185.212.158	192.168.31.240	TLSv1…	1479	Application Data
8297	40.485345	192.168.31.240	61.185.212.158	TCP	54	5164 → 443 [ACK] Seq=1 Ack=4498385 Win=32768 Len=0

在虚拟网卡中，可以看到其为由 HTTP 协议从虚拟网卡的 IP10.184.65.8 发送至 202.117.19.114：



5211	34.215818	117.34.37.48	10.184.65.8	TCP	54 80 → 12681 [FIN, ACK] Seq=1200 Ack=403 Win=71168 Len=0
5212	34.215855	10.184.65.8	117.34.37.48	TCP	54 12681 → 80 [ACK] Seq=403 Ack=1201 Win=65280 Len=0
5213	34.908435	10.184.65.8	117.34.37.48	TCP	54 12682 → 80 [FIN, ACK] Seq=390 Ack=702 Win=65792 Len=0
5214	34.908481	10.184.65.8	117.34.37.48	TCP	54 12681 → 80 [FIN, ACK] Seq=403 Ack=1201 Win=65280 Len=0
5215	34.908516	10.184.65.8	202.117.19.114	TCP	54 12743 → 80 [FIN, ACK] Seq=1238 Ack=43755 Win=66560 Len=0
5216	34.908541	10.184.65.8	202.117.19.114	TCP	54 12750 → 80 [FIN, ACK] Seq=1583 Ack=1320 Win=65280 Len=0
5217	34.908566	10.184.65.8	202.117.19.114	TCP	54 12749 → 80 [FIN, ACK] Seq=555 Ack=78640 Win=66560 Len=0
5218	34.908589	10.184.65.8	202.117.19.114	TCP	54 12747 → 80 [FIN, ACK] Seq=555 Ack=97610 Win=65536 Len=0
5219	34.908612	10.184.65.8	202.117.19.114	TCP	54 12717 → 80 [FIN, ACK] Seq=1701 Ack=461449 Win=66560 Len=0
5220	34.908635	10.184.65.8	202.117.19.114	TCP	54 12748 → 80 [FIN, ACK] Seq=555 Ack=119852 Win=66304 Len=0
5221	34.912602	202.117.19.114	10.184.65.8	TCP	54 80 → 12750 [ACK] Seq=1320 Ack=1584 Win=32512 Len=0
5222	34.912640	202.117.19.114	10.184.65.8	TCP	54 80 → 12743 [ACK] Seq=43755 Ack=1239 Win=31744 Len=0

可以推测，实际上 SSLVPN 是与远端代理服务器建立安全连接后，通过虚拟网卡模拟将请求发送至代理服务器，再由其转发回来，在虚拟网卡视角是从分配的新 IP 直接发送请求接收回复。

本组四人主要工作：	
实验中问题及解决方法，经验总结	本次实验我们主要使用了内网访问、webvpn 和 sslvpn，主要对比了三者的功能和一些特性： （1）内网访问认为安全，因此直接通过 TCP 连接 （2）WebVPN 通过 Web 浏览器访问特定界面，在公网中通过 TLS 加密，适用于简单的 Web 应用访问。 （3）SSL VPN 可以使用 Web 浏览器或专用客户端，支持更广泛的应用和协议访问。SSL VPN 采用 SSL/TLS 协议建立安全通道并提供更高的安全性。 在配置网络过程中曾出现了 ping 同 vlan 下个别设备失败但其他成功的情况，经过检查发现是出错设备的网卡 ipv4 协议配置问题，在修正后恢复正常。 实验过程中我们更加清晰地认识了内网访问、webvpn 和 sslvpn 的工作原理，且在实验过程中能更熟练地配置网络设备（路由器，交换机等），更清晰地认识了网络结构。
师生互动交流	老师给我们讲解了内网访问、WebVPN 访问以及 SSL VPN 访问的细节。在我们 vlan 无法连通时，老师给我们分析了原因并指导我们改正。

验收教师		本实验成绩	