# 实验七 防火墙与SSLVPN实验

## 实验方案及目的

SSL VPN是以SSL/TLS协议为安全基础的VPN远程接入技术，移动办公人员（在SSL VPN中被称为远程用户）使用SSL VPN可以安全、方便的接入企业内网，访问企业内网资源，提高工作效率。在SSLVPN解决方案中，远程用户通过SSLVPN客户端程序，在不可靠的公共网建立一条加密的SSL数据通道，直接连接到了企业内网中，这对远程/全球办公室的建立非常必要。本实验的目的是利用CISCO ASA5505防火墙设备的SSL VPN技术构建一个虚拟专用网VPN解决企业内部资源的安全访问问题。

## SSL VPN基础

### 功能特点

SSL VPN 提供增强的远程安全接入功能。 IPSec VPN 通过在两站点间创建隧道提供直接（非代理方式）接入，实现对整个网络的透明访问。SSL VPN的特点主要有：① SSL VPN 提供安全、可代理连接，只有经认证的用户才能对资源进行访问；②SSL VPN 能对加密隧道进行细分，从而使得终端用户能够同时接入 Internet 和访问内部企业网资源，也就是说它具备可控功能；③SSL VPN 还能细化接入控制功能，易于将不同访问权限赋予不同用户，实现伸缩性访问。④SSL VPN 基本上不受接入位置限制，可以从众多 Internet 接入设备、任何远程位置访问网络资源。

### 技术特点

SSL VPN 通信基于标准 TCP/UDP 协议传输，因而能遍历所有 NAT 设备、基于代理的防火墙和状态检测防火墙。这使得用户能够从任何地方接入，无论是处于其他公司网络中基于代理的防火墙之后，或是宽带连接中。

SSL VPN 不需要复杂的客户端支撑，广泛支持SSL的浏览器就可以使Internet上的远程机计算机如同在自己企业内部LAN 中一样。

Cisco ASA防火墙提供了两种SSL VPN模式：无客户端WebVPN和AnyConnect VPN。无客户端WEBVPN模式中，用户的计算机不需要安装VPN客户端，只需打开Web浏览器，输入ASA防火墙的IP地址，通过了身份认证，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。

使用客户端Anyconnect的 VPN可以提供完全的网络访问。远程用户将使用anyconnect客户端连接到ASA防火墙，并将从VPN池接收IP地址，从而允许完全访问网络。

在本实验中，我们将使用无客户端WebVPN来安装anyconnect VPN客户端。远程用户将打开Web浏览器，输入ASA的IP地址，然后它将自动下载anyconnect VPN客户端并建立连接。

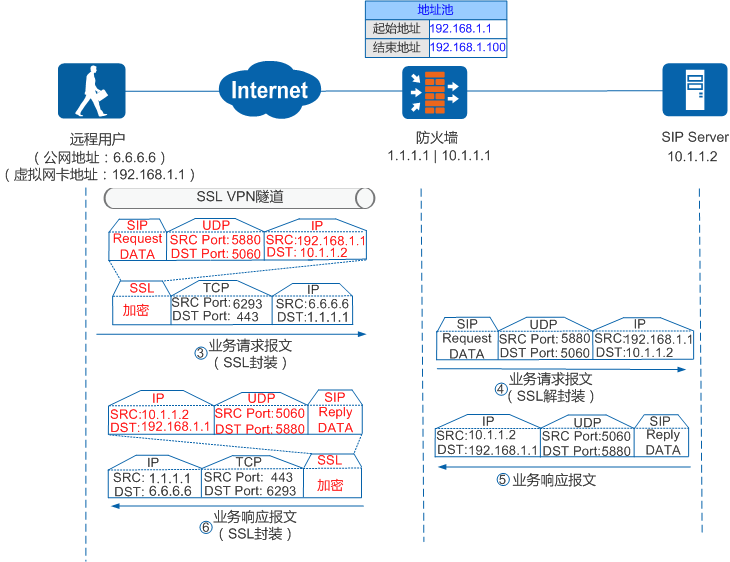


图7-1 SSL VPN的工作原理图

图7-1给出了一个典型的SSLVPN的工作原理图，远程用户与内部网络的SIP服务器的通信，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。

## 实验规划及拓扑结构

### 需要的设备及环境

CISCO ASA5505防火墙设备1台；4台计算机PC1到PC4 分别承担不同角色和作用。

图7-2给出了在CISCO ASA5505防火墙上进行SSLVPN配置的组网图。图中的参数只作为参考，鼓励各小组灵活自定义IP等参数。



图7-2 SSL VPN组网图

### 实验的主要工作

1）检查CISCO ASA5505防火墙设备状态，查看该设备上有关的软件系统。SSL VPN的支持软件为anyconnect-win-2.2开头的文件；

2）按照实验设计图连接有关设备；为CISCO ASA5505划分vlan和接口，vlan1是其缺省值，包含了所有的8个以太网接口；激活有设备连接的接口；

3）为CISCO ASA5505配置dhcp服务，该服务可以为内部网络和外部网络分配IP 地址；

4）配置SSL VPN参数；

5）配置WEB VPN隧道组与组策略；

6）在组策略中启用SSL VPN；

7）创建SSL VPN用户，并将策略赋予用户；

8）在外部客户端启动SSL VPN，浏览内部PC上的Web资源，同时捕获有关报文；

9）在内部客户端浏览另一个内部PC上的Web资源，同时捕获有关报文；

10）对捕获有关报文进行对比分析。

## 实验主要步骤

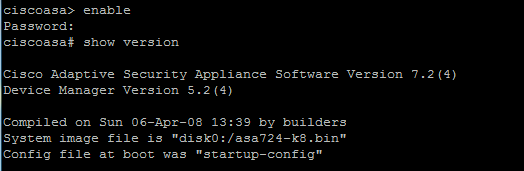
实验前需将防火墙和交换机恢复出厂设置，参考命令如下：

交换机：

|  |
| --- |
| Switch> enable !进入特权用户模式  Switch# set default !启动初始化  Are you sure? [Y/N] = y ！确认初始化，显示初始化信息  Switch# write ！写入初始化信息到启动文件  Switch# reload ！重新启动交换机 |

先查看防火墙版本号，参考命令：

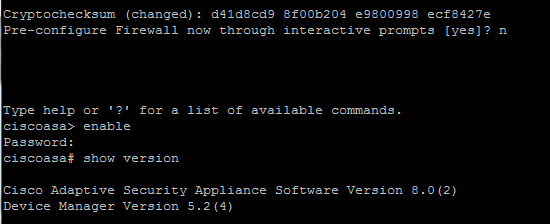
|  |
| --- |
| ciscoasa> enable  Password: !直接敲回车  ciscoasa#show version |



如果为Version 8.0，可以直接进行“恢复出厂设置”操作；如果为Version 7.2，则需要先升级，参考命令：

|  |
| --- |
| ciscoasa> enable  ciscoasa#config t  ciscoasa(config)#no boot system disk0:/asa702-k8.bin  ciscoasa(config)#boot system disk0:/asa802-k8.bin  ciscoasa(config)#exit  ciscoasa#reload |

升级重启完毕后，提示“Pre-configure Firewall now through interactive prompts [yes]?”时输入“N”，登录设备，查看版本号，版本号为Version 8.0表式升级成功。



防火墙恢复出厂设置：

|  |
| --- |
| ciscoasa> enable !进入特权模式，回应*Password:* 时按回车。  ciscoasa#write erase !清除当前设备全部配置，恢复到出厂状态。  Erase configuration in flash memory? [confirm] Y  ciscoasa#reload !重新启动设备。  Proceed with reload? [confirm] Y  Pre-configure Firewall now through interactive prompts [yes]? N !注意不要选错 |

步骤1：为CISCO ASA5505划分vlan和接口

|  |
| --- |
| ciscoasa# config t ！进入配置模式  ciscoasa(config)# show switch vlan ！查看系统目前配置  ciscoasa(config)# interface vlan 2 ！创建vlan 2，进入接口配置模式ciscoasa(config-if)#  ciscoasa(config-if)# nameif outside ！命名vlan 2为outside，安全级别缺省为0  ciscoasa(config-if)# ip address 202.1.5.1 255.255.255.0 ！为vlan 2设置ip  ciscoasa(config-if)# q  ciscoasa(config)# interface vlan 1 ！进入vlan 1  ciscoasa(config-if)# nameif inside ！命名vlan 1为 inside，安全级别缺省为100  ciscoasa(config-if)# ip address 10.1.3.1 255.255.255.0  ciscoasa(config-if)#show ip |

步骤2：为Vlan分配接口并开启

|  |
| --- |
| ciscoasa(config)# interface e0/0 ！进入设备0号端口  ciscoasa(config-if)# switchport access vlan 2 ！0端口分到vlan 2，其余在vlan 1  ciscoasa(config-if)# no shutdown ！开启 0号端口  ciscoasa(config-if)# show interface vlan 2 ！查看vlan 2的全部配置参数 |

同理开启vlan 1的 e0/1和e0/2端口 ，观察其配置参数和状态

|  |
| --- |
| ciscoasa(config)# show switch vlan ！查看vlan的端口分配情况 |

步骤3：启用HTTP服务及内网DHCP服务器

|  |
| --- |
| ciscoasa(config)# http server enable ! 开启http server  ciscoasa(config)# http 10.1.3.0 255.255.255.0 inside ！配置 DHCP Server  ciscoasa(config)# dhcpd address 10.1.3.2-10.1.3.33 inside !内部用户地址池  ciscoasa(config)# dhcpd enable inside ！启动内部DHCP  ciscoasa(config)# show dhcpd state ！查看dhcpd状态 |

步骤4：在外网口上启动WEBVPN，并同时启动SSL VPN功能

接下来启动SSL VPN ，并指定SSL VPN Client 的软件包文件名，注：如果发生错误，可能名字不对，请从防火墙上用dir查看具体软件包名字。

|  |
| --- |
| ciscoasa(config)# webvpn ！配置WebVPN 服务  ciscoasa(config-webvpn)# enable outside ！在外网口上启动WEBVPN  ciscoasa(config-webvpn)# svc image disk0:/anyconnect-win-2.0.0343-k9.pkg  ciscoasa(config-webvpn)# svc enable  ciscoasa(config)# show webvpn svc ！查看webvpn服务状态 |

步骤5：创建SSL VPN用户IP地址池ssluser

|  |
| --- |
| 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 10.10.10.0 255.255.255.0 !定义存取控制列表go-vpn  ciscoasa(config)# show access-list  ciscoasa(config)# nat (inside) 0 access-list go-vpn !对inside访问不做NAT翻译  ciscoasa(config)# show nat |

步骤6：WEB VPN隧道组与策略组的配置

创建名为mypolicy的组策略，并为其配置内部组策略特性：设置隧道协议类型webvpn，并在组策略中启用SSL VPN

|  |
| --- |
| ciscoasa(config)# group-policy *mypolicy* internal  ciscoasa(config)# group-policy *mypolicy* attributes  ciscoasa(config-group-policy)# vpn-tunnel-protocol webvpn  ciscoasa(config-group-policy)# webvpn  ciscoasa(config-group-webvpn)# svc enable  ciscoasa(config-group-webvpn)# exit  ciscoasa(config-group-policy)# exit  ciscoasa(config)# |

步骤7：创建SSL VPN用户vpnuser1和vpnuser2，赋予访问策略

大概步骤是：先创建用户及密码，再把组策略赋予用户，然后定义webvpn类型的隧道组***mytg***，并使用地址池***ssluser***。最后进入隧道组***mytg***的 webvpn- attributes 命令模式，为隧道组起别名***vpntest***，简化SSLVPN用户访问。

|  |
| --- |
| 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)#  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 |

步骤8：在内部PC4（[10.1.3.80](https://192.168.5.1)）上创建测试用Web资源服务

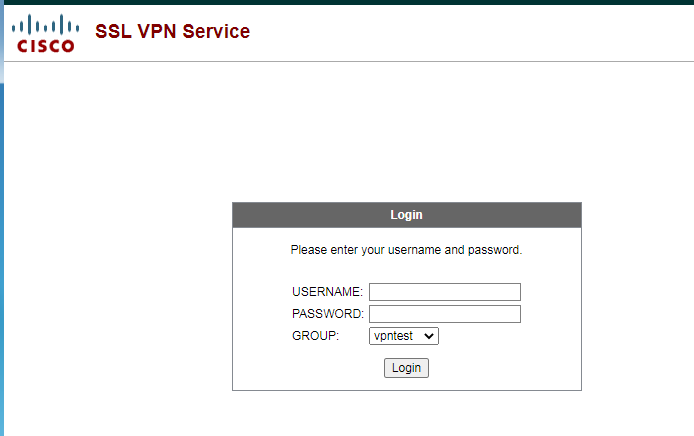
启动HFS（http file server)，添加共享文件资源，设置内部IP（exp接口的地址）和端口（80），构建一个可以供外部VPN用户访问的Web服务。

**内网访问：**

在PC3访问服务器下载资源，PC3和服务器同时抓包，观察访问过程（源地址、目的地址，是否加密等）。

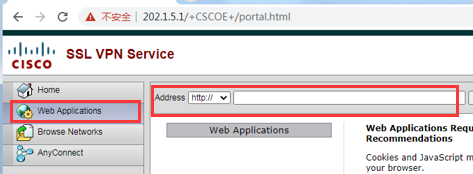
步骤9：**外网Web模式**访问内部Web资源。

在PC2浏览器中输入<https://202.1.5.1>访问WEB VPN（如果提示网站不安全，点击高级->继续访问），在随后弹出的对话框中输入用户名*vpnuser2*和密码单击登陆。



在PC2和服务器打开抓包软件抓包。

在“Web Applications”页面的“Address”栏输入内网服务器地址，看能否访问内部资源。

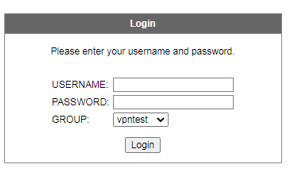


打开一个新网页，在地址栏输入内部服务器地址，看能否访问内部资源。

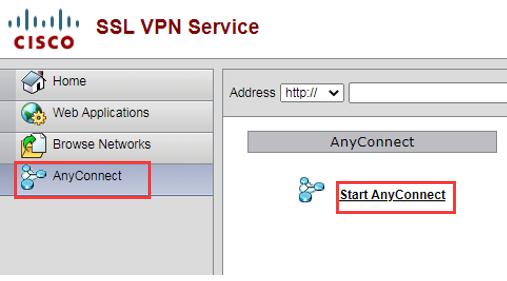
运行ping测试网络连通性，查看本地网卡是否有虚拟网卡，查看PC2路由表，结合数据包分析PC2的访问过程。

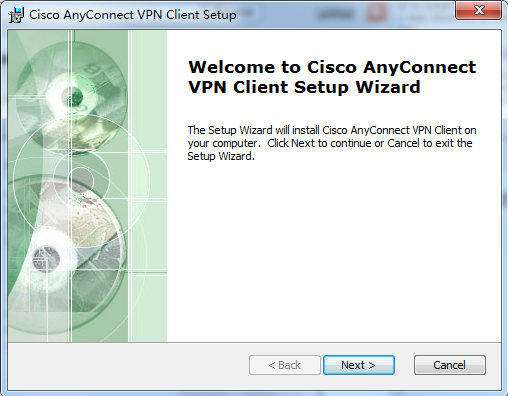
步骤10：**外网客户端模式**访问内部Web资源。

在PC1浏览器中输入<https://202.1.5.1>访问WEB VPN，在随后弹出的对话框中输入用户名*vpnuser1*和密码单击登陆。

在Web页面下载安装AnyConnect客户端。



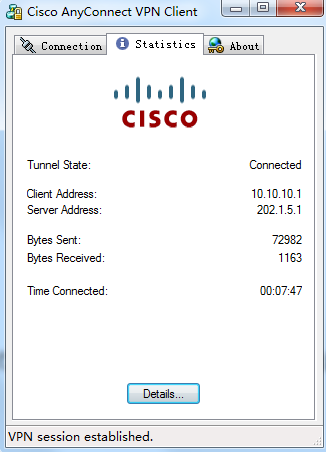
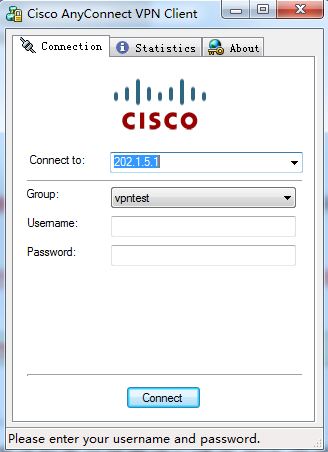
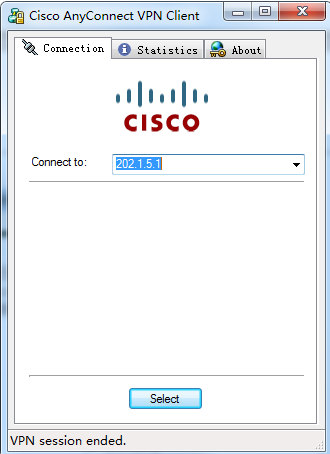


安装完成后，双击任务栏右下角的锁型图标，输入防火墙地址、用户名*vpnuser1*和密码登录。

注：如果用户重新登陆时提示登陆失败，需要在防火墙中注销已登陆的VPN用户，参考命令：

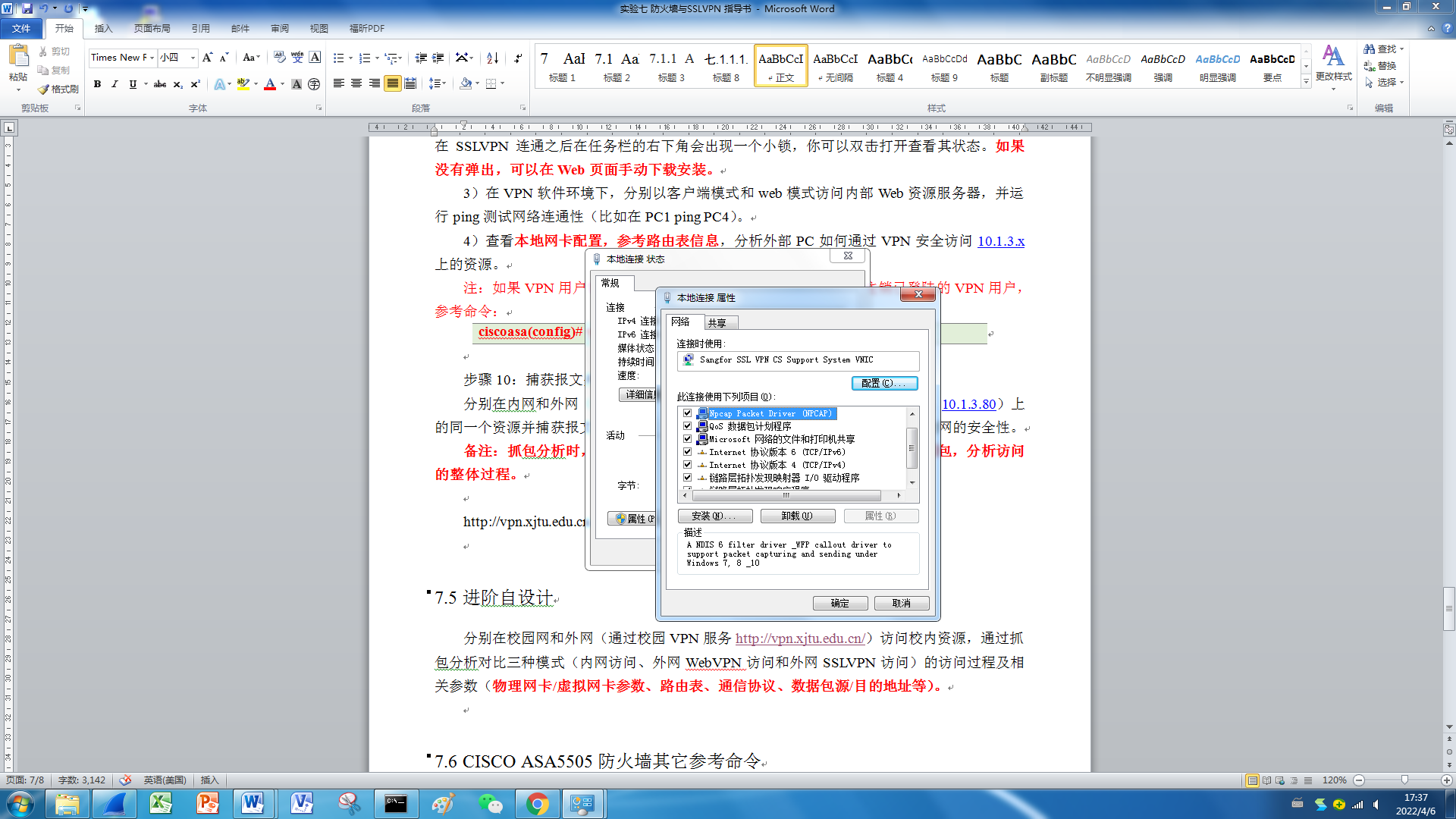
|  |
| --- |
| ciscoasa(config)# vpn-sessiondb logoff all |

连通之后，可以双击任务栏图标打开查看其状态和参数。

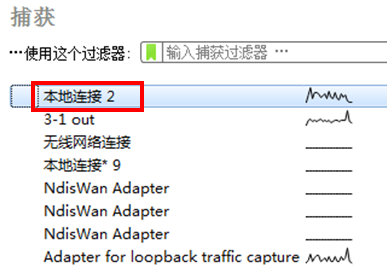


客户端登录成功后，在PC1和服务器打开抓包软件抓包。

**备注：抓包分析时，需在PC机（exp网卡、虚拟网卡）和服务器端同时抓包，如果Wireshark不识别虚拟网卡，在虚拟网卡的“属性”🡪“网络”选项卡，勾选“Npcap Packet Driver （NPCAP）”。**



在命令行用ipconfig /all命令查看虚拟网名，在Wireshark选择对应的网卡抓包分析。



打开一个新网页，在地址栏输入内部服务器地址，看能否访问，运行ping测试网络连通性。

查看本地网卡中新出现的虚拟网卡参数，查看PC1路由表，分析虚拟网卡的作用，结合数据包分析PC1的访问过程。

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。

## 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（**物理网卡/虚拟网卡参数、路由表、通信协议、数据包源/目的地址等）。**

## CISCO ASA5505防火墙其它参考命令

|  |  |  |
| --- | --- | --- |
| 序号 | 命令 | 含义 |
| 1 | Ciscoasa>enable | 进入特权模式#，提示Password时安回车健 |
| 2 | ciscoasa#dir | 查看文件系统 |
| 3 | ciscoasa#config t | 进入配置模式ciscoasa(config)# |
| 4 | ciscoasa#？ | 查看当前模式下的可用命令或参数 |
| 5 | ciscoasa#show IP | 查看当前配置的IP |
| 6 | ciscoasa#show switche vlan | 查看VLan配置 |
| 7 | ciscoasa#show webvpn svc | 查看SSLVPN提供给客户端的可用文件 |
| 8 | ciscoasa(config)#q | 退出当前命令模式 |
| 9 | ciscoasa# show run | 查看系统目前配置 |
| 10 | ciscoasa# show route | 查看路由表 |
| 11 | ciscoasa# no 命令 | 取消命令的原有结果 |
| 12 | ciscoasa#write erase | 清除当前设备全部配置，恢复到出厂状态。Erase configuration in flash memory? [confirm] Y |
| 13 | ciscoasa#reload | 重新启动设备。Proceed with reload? [confirm] **Y**  Pre-configure Firewall now through interactive prompts [yes]? **N** |