7 实验七 防火墙与 SSLVPN 实验

7.1 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。

7.2 SSL VPN 基础

7.2.1 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。

7.2.2 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，我们将仅使用无客户端 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。

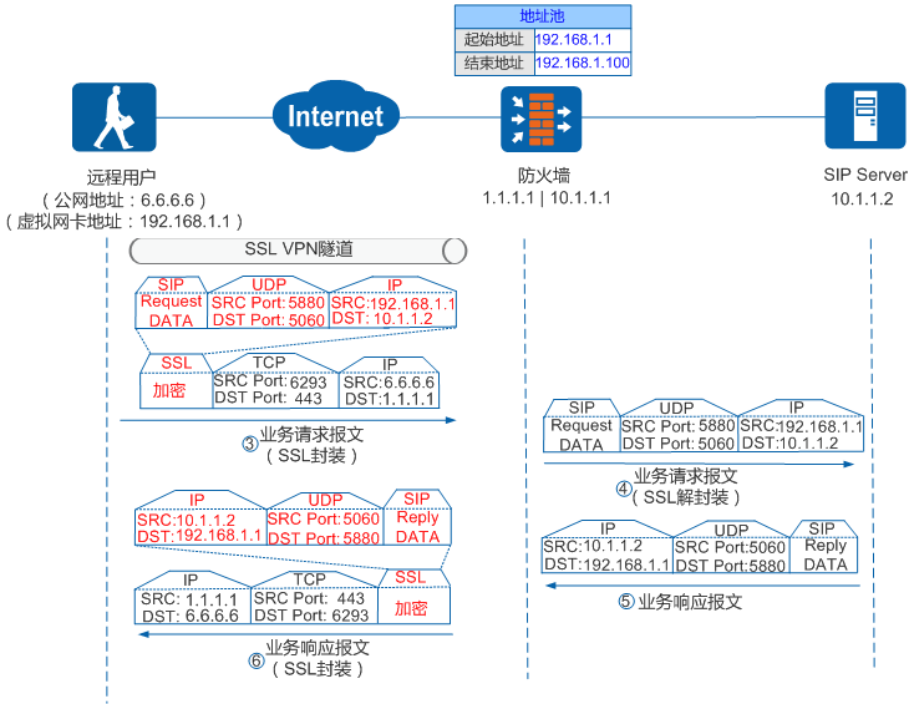

图 7-1 SSL VPN 的工作原理图

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。

7.3 实验规划及拓扑结构

7.3.1 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。

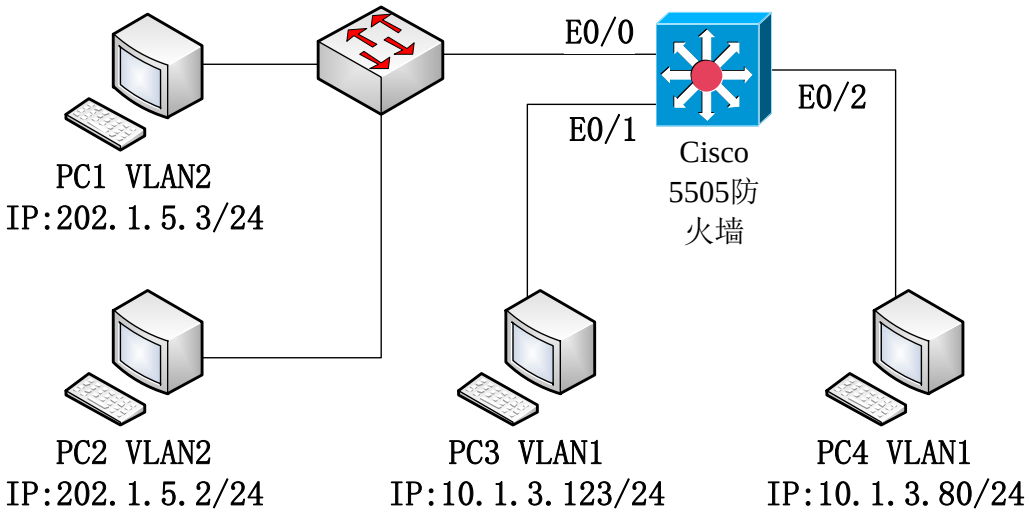

图 7-2 SSL VPN 组网图

7.3.2 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。

7.4 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
```

防火墙：

```
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）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。在本机和另外一台内部 PC 上用浏览器测试。

步骤 9：在外网 PC1 和 PC2 用 SSLVPN 接入并下载内部 Web 资源。

1）在浏览器中输入 https://202.1.5.1 访问 WEB VPN，在随后弹出的对话框中输入用户名和密码单击登陆。两个 PC 的用户名不能取同一个。

2）系统会弹出要求安装 SSL VPN CLIENT 程序，单击“YES”，系统自动安装并连接 SSLVPN，在 SSLVPN 连通之后在任务栏的右下角会出现一个小锁，你可以双击打开查看其状态。

3）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）。

4）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。

注：如果 VPN 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
```

步骤 10：捕获报文并分析

分别在内网和外网请求 Web 资源服务器（PC4，10.1.3.80）上的同一个资源并捕获报文，分析两种报文的差别。解释外部 PC 通过 VPN 访问内网的安全性。

7.5 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（可自己架设服务器），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。

7.6 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**