# 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：      1. CISCO ASA5505内网DHCP服务器的IP范围是：     范围是10.1.3.2-10.1.3.33   1. SSL VPN用户地址池的名称和地址范围是：     名称是ssluser,范围是10.10.10.1-10.10.10.10   1. 创建的SSL VPN用户名是：   创建的用户名是 vpnuser1 和 vpnuser2   1. 所配置的防火墙测试方案及结果是：                1. 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：    PC3抓到的包：    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   1. 步骤9完成后，记录和分析外网Web方式访问过程。       PC2的数据包：    服务器的数据包:    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   1. 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）。       PC1的exp网卡：    PC1的虚拟网卡：    服务器的数据包：    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。 | | | | | | | | | | |
| 本组四人主要工作： | | 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，负责进阶自设计部分的分析和撰写 | | | | | | | | | |
| 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。 | | | | | | | | | |
| 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。 | | | | | | | | | |
| 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。 | | | | | | | | | |
| 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。 | | | | | | | | | |
| 实验中问题及解决方法，经验总结 | | 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。 | | | | | | | | | |
| 师生互动交流 | | 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。 | | | | | | | | | |
| 验收教师 | | 张利平 | | | | | 本实验成绩 | | | |  |