

“计算机网络安全”实验报告

——VPN实验

|  |  |
| --- | --- |
| **院 系：** | 网络空间安全学院 |
| **专业班级：** | 网安2104班 |
| **姓 名：** | 邬雪菲 |
| **学 号：** | U202112131 |
| **日 期：** | 2024年5月12日 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **评分项** | **实验报告评分**  **（50%）** | **检查单分数**  **（50%）** | **综合得分** | **教师签名** |
| **得分** |  |  |  |  |

实验报告评分表

|  |  |  |  |
| --- | --- | --- | --- |
| **评分项目** | **分值** | **评分标准** | **得分** |
| 实验原理 | 10 | 10-8：原理理解准确，说明清晰完整  7-5：原理理解基本准确，说明较为清楚  4-0：说明过于简单 |  |
| VPN系统设计 | 25 | 25-19：系统架构和模块划分合理，详细设计说明翔实准确  18-11：系统架构和模块划分基本合理，详细设计说明较为准确  10-0：系统架构和模块划分不恰当，详细设计说明过于简单 |  |
| VPN实现细节 | 25 | 25-19：回答准确清晰，实现方法技术优良，与设计及代码一致  18-11：回答较准确清晰，实现方法一般，与设计及代码有偏差  10-0：文字表达混乱，实现方法过于简单 |  |
| 测试结果与分析 | 20 | 20-15：功能测试覆盖完备，测试结果理想，分析说明合理可信  14-9：功能测试覆盖基本完备，测试结果基本达标，分析说明较少  8-0：功能测试覆盖不够，测试未达到任务要求，缺乏分析说明 |  |
| 体会与建议 | 10 | 10-8：心得体会真实，意见中肯、建议合理可行，体现个人思考  7-5：心得体会较为真实，意见建议较为具体  4-0：过于简单敷衍 |  |
| 格式规范 | 10 | 图、表的说明，行间距、缩进、目录等不规范相应扣分 |  |
| **总 分** | | |  |

目 录

[1 实验原理 1](#_Toc103367188)

[2 VPN系统设计 1](#_Toc103367189)

[2.1 概要设计 1](#_Toc103367190)

[2.2 详细设计 1](#_Toc103367191)

[3 VPN实现细节 1](#_Toc103367192)

[4 测试结果与分析 2](#_Toc103367193)

[5 体会与建议 2](#_Toc103367194)

[5.1 心得体会 2](#_Toc103367195)

[5.2 意见建议 3](#_Toc103367196)

# 实验原理

（根据个人对实验要求和指导书的理解，说明个人完成本次实验的技术原理，包括但不限于网络拓扑、通信机制、加密原理、认证机制等）

TLS/SSL VPN是一种基于安全套接层（SSL）或其后继者传输层安全（TLS）协议的虚拟私人网络（VPN）技术。它允许远程用户通过加密的通道安全地访问企业内部网络资源。与传统的IPSec VPN相比，SSL VPN的优势在于它主要通过标准的Web浏览器进行连接，不需要安装专门的客户端软件，这使得SSL VPN在易用性和可访问性方面具有优势。

SSL VPN的工作原理主要基于HTTPS（HTTP Secure），即在HTTP协议上应用SSL/TLS协议来提供数据传输的安全性。当用户通过浏览器尝试连接到SSL VPN服务器时，服务器会提供一个SSL VPN门户，用户在此门户上进行认证。一旦认证成功，用户的浏览器与SSL VPN服务器之间就会建立起一个加密的SSL/TLS隧道，所有通过这个隧道的数据都会被加密，从而保护数据传输的安全性。

在SSL VPN的实现中，TUN/TAP设备扮演了重要的角色。TUN/TAP是Linux内核中的虚拟网络设备，它们允许用户空间程序与内核网络协议栈进行数据包的接收和传输。TUN设备工作在网络层（第三层），主要处理IP数据包，而TAP设备工作在链路层（第二层），可以处理以太网数据帧。通过这些虚拟设备，SSL VPN可以创建一个虚拟的网络接口，使得远程用户就像是直接连接到了企业内部网络一样。

# VPN系统设计

## 概要设计

（说明系统架构、模块划分、工作机制等）

VPN系统的通信结构如下图所示：

## 详细设计

（详细说明各模块的数据结构、重要算法、主要函数流程图、关键代码等）

# VPN实现细节

（根据个人设计实现情况，回答下列问题）

## 问题1

回答实验指导手册4.2第6步提出的问题：在HostU上，telnet到HostV。在保持telnet连接存活的同时，断开VPN隧道。然后我们在telnet窗口中输入内容，并报告观察到的内容。然后我们重新连接VPN隧道。需要注意的是，重新连接VPN隧道，需要将vpnserver和vpnclient都退出后再重复操作，请思考原因是什么。正确重连后，telnet连接会发生什么？会被断开还是继续？请描述并解释你的观察结果。

## 问题2

请介绍你的VPN的登录协议，即在SSL连接建立之后、隧道通信传输之前，SSLVPN客户端与服务器交互了哪些报文？每个报文的格式是怎样的？每个报文的作用是什么？报文内容取值是如何定义的？报文交互的顺序是怎样的？

## 问题3

你的VPN服务器支持多客户端采用的什么技术？VPN服务器收到保护子网主机的应答报文时，如何判断应发送给哪个VPN客户端的隧道？

# 测试结果与分析

（按照指导书的任务要求进行功能测试，介绍测试结果，分析功能完成情况）

# 体会与建议

## 心得体会

## 意见建议