

计算机网络安全实验

华中科技大学

实验3 TLSVPN 说明



基于隧道的SSLVPN

- ▣ 采用跟IPSecVPN类似的技术，需要安装客户端软件，以及虚拟网卡
- ▣ 到内网服务器的IP报文（虚拟IP → 内网服务器）会被客户端软件进行SSL协议封装（真实IP → SSLVPN网关地址），到对端的SSLVPN网关设备再解密解封装，还原为原始IP报文，交给内网服务器
- ▣ 能支持基于TCP、UDP、ICMP协议的各种应用
- ▣ 因工作在套接字层，无IPSecVPN的NAT穿越问题
- ▣ **缺点：**平台兼容性不够好
- ▣ **开源代码：**OpenVPN

基于隧道的SSLVPN

1:外网访问SSLVPN服务器,
发送数据报到10.0.0.1,80

原始报文:
S:172.16.1.3:2045
D:10.0.0.1: 80

1

S:202.114.1.3:1035
D: 138.76.29.7:443

1.登录SSLVPN, SSL协商



公网IP: 202.114.1.3

分配虚拟IP: 172.16.1.3

还原报文:

S: 10.0.0.1: 80
D:172.16.1.3:2045

S: 138.76.29.7,443
D: 202.114.1.3,1035

4:SSLVPN加密封装

2:SSLVPN解密、解封装后,
得到原始报文

2

S:172.16.1.3:2045
D:10.0.0.1:80

10.0.0.4

10.0.0.1

10.0.0.2

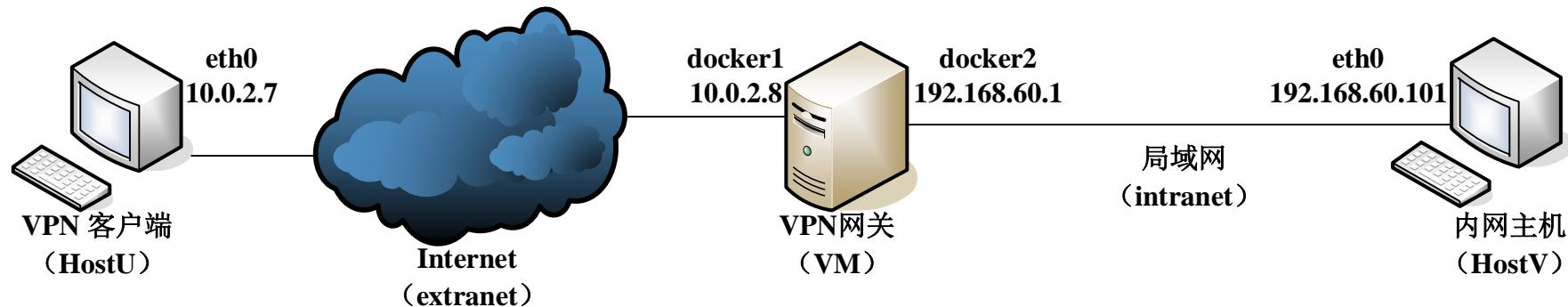
10.0.0.3

S: 10.0.0.1, 80
D: 172.16.1.3, 2045

3:内部服务器返回响应报文



1、实验环境



- ⌚ 可以使用提供的linux虚拟机环境ubuntu-seed
 - 例程代码可直接使用
- ⌚ 可以自行选用linux环境
 - 例程代码需自行适配
- ⌚ 若有能力，也可选择其他OS环境
 - 例程代码仅供参考

2、实验指导

 实验介绍PPT

 实验指导手册

 实验讲解视频

 SSL编程简介PPT

3、实验任务

⌚ 学习例程代码，掌握隧道通信和SSL编程的基本方法

- vpn-2024-1.zip
 - ◆ 基于UDP协议的TUN虚接口隧道通信示例
- tls-2024-1.zip
 - ◆ TLS编程基本流程示例

⌚ 设计开发TLSVPN的客户端和服务端

- 整合例程代码，实现基于TLS协议的TUN虚接口隧道通信
 - ◆ **建议将vpn-2024-1.zip中的隧道功能向tls-2024-1.zip移植**
- 使用openssl生成个人专有的服务器证书
- 设计实现自己的认证登录协议
- 设计实现支持多客户端并发登录的服务端工作机制

4、实验考核

验收

- 按检查单项目完成验收
- 截止时间：2026年1月11日

报告提交

- 按模板要求撰写实验报告
- 报告和源码按要求提交至相关平台
- 截止时间：2026年1月23日