1. # 大作业要点大纲

虚拟机与软件安装

1. Linux，2台，一台做防火墙，一台是hostB
2. Windows（可选）
3. vsftpd（hostB）
4. apache2（hostB）

vsftpd配置

开启pasv
开放1024-65535端口

网络配置

- 网段配置
  在虚拟网络编辑器中添加自定义网络，设置网段为`192.168.33.0`，关闭DHCP服务（Linux主机有IP要求，需要设置静态IP）。并且确保虚拟网络编辑器中存在1个NAT类型的网段。
- 网卡配置
  配置完网段后，关闭虚拟机，在编辑虚拟机设置界面添加网卡。新的网卡选择自定义添加的网段（33网段对应的vmnet）。
- IP配置
  由于关闭了DHCP，所以需要手动配置静态IP，hostB静态IP设置为`192.168.33.11`，hostB网关为防火墙IP。防火墙的IP设置为`192.168.33.254`作为网关，33网段内的IP，防火墙该网卡不设置网关，并且防火墙的另一张网卡模式设置为NAT，不需要手动配置IP。
  如遇到设置完成后防火墙不能上网的情况，请重启网络服务。具体表现为防火墙双网卡ping外部地址显示`from 192.168.33.254 host unreachable`

Attention

虚拟机挂起或者宿主机重启后需要重启一下宿主机的vmnet8（默认的NAT网段）获取宿主机地址，确保网络通畅

- VMnet8(NAT)
  宿主机IP：`192.168.x.x 255.255.255.0`
  防火墙IP：`192.168.x.x 255.255.255.0`
  确保宿主机和防火墙外部网卡都获得IP，并且IP地址在同一个网段内
- VMnet0(Custom)
  防火墙IP(静态IP的内网网关):`192.168.33.254 255.255.255.0`
  内网IP(静态IP)：`192.168.33.x 255.255.255.0`
- 无法确定问题在哪儿可以使用wireshark在宿主机，防火墙两个网卡，hostB上监听报文排查问题所在位置

防火墙配置

在防火墙主机配置iptables。
注意：

1. ubuntu系统一般默认禁止转发，可以用`sysctl net.ipv4.ip_forward=1`开启转发

2. 命令较多可以写一个bash，清除现有iptables策略的命令是`iptables -F`和`iptables -t nat -F`
3. `sudo iptables -t nat -L`查看当前iptables的策略

测试检查点

1. 网段配置，防火墙双网卡配置，hostB网卡配置
2. 内网可以上网ping外网，并且用wireshark抓包防火墙外网卡，源地址已经转换为防火墙外网地址，宿主机ping不通内网IP
3. 宿主机ftp测试需要浏览器和flashfxp均可访问
4. 宿主机web可以访问防火墙外网地址获得内网主机上的Apache服务