现代移动通信与物联网综合系统实验

—— LTE 防火墙方案

在进行 LTE 环境防火墙实验时，我们只需要对防火墙虚拟机进行配置即可。根据场景要求，核心网网关将指定防火墙虚拟机作为网关，因此，在正式实验之前，我们需要启用防火墙虚拟机的两张网卡，其中，网卡 1 配置为 NAT 模式，且高级配置修改为混杂模式，网卡 2 配置为桥接模式，且界面名称为主机的有线网卡。虚拟机启动后，输入 *dhclient eth1* 为 eth1 分配 IP 地址，再手动为 eth2 配置 IP，假设为 20.70.20.164，即 *ifconfig eth2 20.70.20.164 netmask 255.255.255.0*。假设手机的虚拟地址为 172.16.1n.xxx，由于其不在 20.70.20.0/24 网段，需要对防火墙的路由表进行修改。其中，当从手机发出数据包访问公网时，数据报的目标地址可与路由表中的 destination 对应，进而从网卡 1 发送出去，故不做修改；当公网发送响应数据包到手机时，路由表将指示从网卡 1 转发该包，显然错误，故添加表项，使数据包从网卡 2 转发到核心网网关，具体指令为 *route add -net 172.16.0.0 netmask 255.255.0.0 gw 20.70.20.2*。最后，我们需要开启虚拟机 IPV4 层面的 IP 数据包转发功能，即 *sysctl -w net.ipv4.ip_forward=1*，再配置 iptables，即 *iptables -t nat -I POSTROUTING -s 172.16.0.0/16 -o eth1 -j MASQUERADE*，使手机发送的数据包在被丢弃之前转发给网卡 eth1，由其发送到公网。

综上，我们的 LTE 防火墙配置方案为：

ifconfig：

dhclient eth1

ifconfig eth2 20.70.20.164 netmask 255.255.255.0

route：

route add -net 172.16.0.0 netmask 255.255.0.0 gw 20.70.20.2

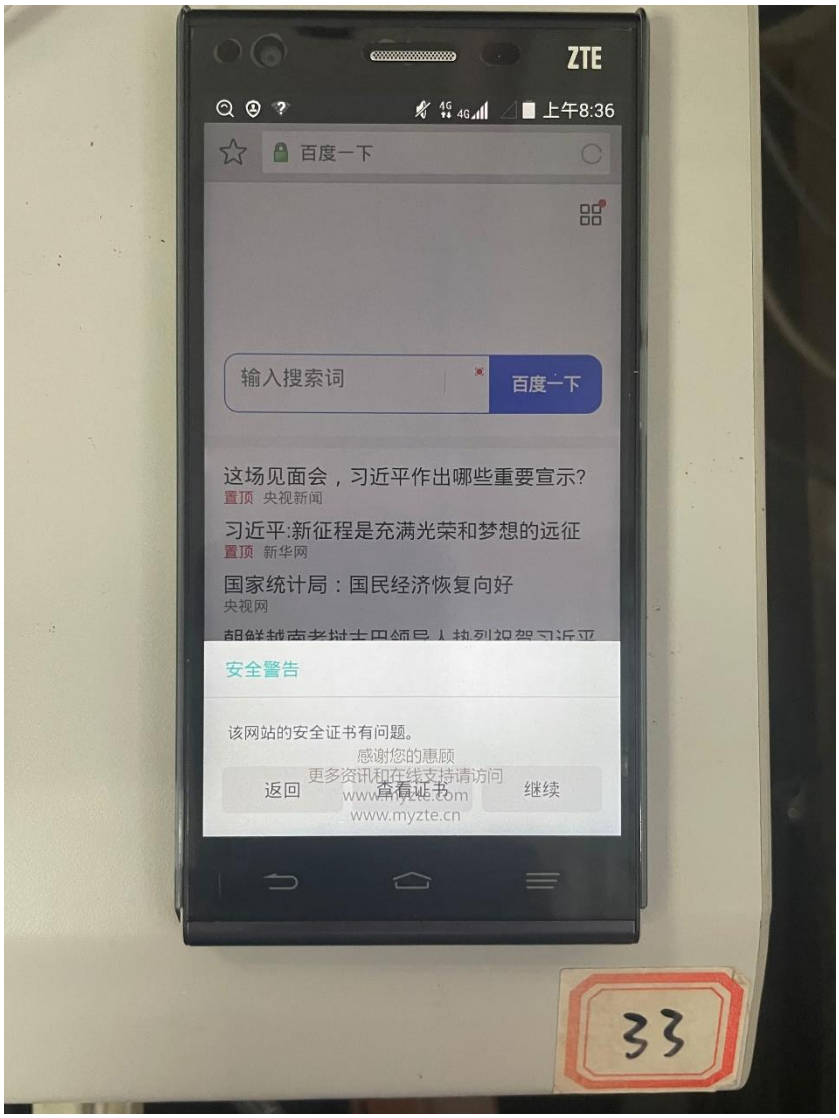
IPv4 转发：

sysctl -w net.ipv4.ip_forward=1

iptables：

iptables -t nat -I POSTROUTING -s 172.16.0.0/16 -o eth1 -j MASQUERADE

最终在手机上访问百度，测试成功截图如下：


ZTE
上午8:36
百度一下
输入搜索词
百度一下
这场见面会，习近平作出哪些重要宣示?
置顶 央视新闻
习近平:新征程是充满光荣和梦想的远征
置顶 新华网
国家统计局：国民经济恢复向好
央视网
安全警告
该网站的安全证书有问题。
返回
查看证书
继续
33