FCN 局域网互联方案

boywhp@126.com

需求：通过互联网和 FCN 将两个不同网段的局域网连接起来，使得两个局域网中的机器可以相互访问，实验拓扑如下。

局域网 1：网段 172.16.20.1/24 网关 172.16.20.1，其中 Linux elk Server **172.16.20.197**。
局域网 2：网段 192.168.177.1/24 网关 192.168.177.1，其中 Linux 树莓派 3 **192.168.177.99**

计划通过两台 Linux Server 和 FCN 实现两个局域网相互透明访问。

首先在两台机器上各自运行 FCN 服务端。

方案 1：在 Linux elk Server **172.16.20.197** 机器上配置代理网关，正常上网流量重定向到网关 172.16.20.1，指定网段（192.168.177.1/24）的数据通过 FCN 重定向到 Linux 树莓派 3，实现局域网 2 的访问。

步骤：

1. Linux elk Server 172.16.20.197 命令行启动 FCN

./fcn --uid FCN_xxxx --svr HOME_PI3 —psk PASS

连接成功后，ifconfig 应该能够看到 fcn_tun 虚拟网卡，并且能够 ping 通 192.168.1.1

2. 配置代理网关 iptables 转发规则

;开启 iptables ipv4 数据转发
echo 1 > /proc/sys/net/ipv4/ip_forward

;设置默认转发规则 ACCEPT
iptables -P FORWARD ACCEPT

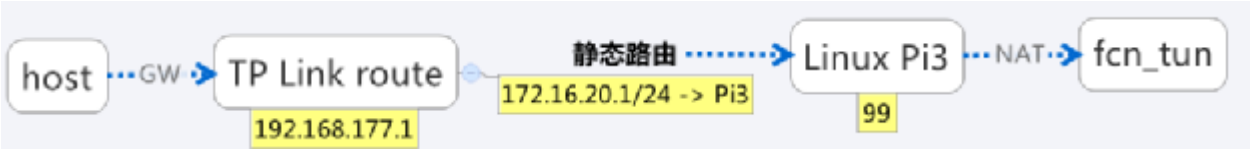
;目标局域网段的数据路由发出前执行源 IP NAT 变换
iptables -t nat -A POSTROUTING -d 192.168.177.1/24 -j MASQUERADE

；设置转发链路时 TCP/MTU 自动适配[FCN MTU 默认 1400]
iptables -A FORWARD -p tcp --tcp-flags SYN,RST SYN -j TCPMSS —clamp-mss-to-pmtu

3. 将局域网预访问目标网段的机器网关设置为 Linux elk Server 172.16.20.197

方案优缺点: 该方案不需要对网络设备作任何设置改动即可实现代理连接远程局域网, 缺点需要修改主机网关配置。

方案 2：在局域网 2 Tplink 路由器上设置静态路由指向 Linux 树莓派 3 **192.168.177.99**，然后通过 Pi 3 上 FCN 虚拟网卡转发数据。



步骤：

1. 登录 TpLink route 添加一条静态路由，指向 Pi 3

本页设置路由器的静态路由信息。

ID	目的IP地址	子网掩码	网关	状态	配置
1	172.16.20.1	255.255.255.0	192.168.177.99	生效	编辑 删除

2. Linux 树莓派 3 192.168.177.99 命令行启动 FCN

./fcn --uid FCN_xxxx —svr elk_server —psk PASS

连接成功后，ifconfig 应该能够看到 fcn_tun 虚拟网卡，并且能够 ping 通 172.16.20.1

3. 配置 Pi 3 iptables 转发规则

;开启 iptables ipv4 数据转发
echo 1 > /proc/sys/net/ipv4/ip_forward

;设置默认转发规则 ACCEPT
iptables -P FORWARD ACCEPT

;目标局域网段的数据路由发出前执行源 IP NAT 变换
iptables -t nat -A POSTROUTING -d 172.16.20.1/24 -j MASQUERADE

；设置转发链路时 TCP/MTU 自动适配[FCN MTU 默认 1400]
iptables -A FORWARD -p tcp --tcp-flags SYN,RST SYN -j TCPMSS —clamp-mss-to-pmtu

方案优缺点: 该方案无需改动局域网主机配置即可实现连接远程局域网, 缺点需要修改路由器静态路由。