



三、设备说明

- 1、“墙外”服务器, CentOS Linux release 7.9.2009 (64 位系统)
- 2、“墙内”服务器, 树莓派 4B , 安装 Ubuntu 20.04.1 LTS (64 位系统)

四、需要安装的软件

- 1、“墙外服务器”:

标准软件 - dnsmasq、unbound

开发软件 - tun_nat.c、udp-proxy.c

- 2、“墙内服务器”:

标准软件 - dnsmasq、hostap、create_ap

开发软件 - tun_nat.c、udp-proxy.c

五、难点说明

- 1、需要安装 tuntap 虚拟网卡设备 (tun0), 用于网络数据转发。
- 2、需要使用 iptables (mangle 标记) + ip rule (规则路由) 来设置网络通路。
- 3、需要自己开发程序, 用于实现“udp 隧道”、dns 请求 (加密) 转发。

六、软件安装

- 1、标准软件的安装，请参考官方文档，这里不进行说明。

七、“墙内”服务器配置

- 1、网卡信息截图：

```
ubuntu@ubuntu:~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.31.72 netmask 255.255.255.0 broadcast 192.168.31.255
    inet6 [REDACTED] prefixlen 64 scopeid 0x20<link>
    ether [REDACTED] txqueuelen 1000 (Ethernet)
    RX packets 46066 bytes 24372067 (24.3 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 16516 bytes 1253815 (1.2 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 4761 bytes 531244 (531.2 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4761 bytes 531244 (531.2 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

tun0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST> mtu 1500
    inet 172.20.100.1 netmask 255.255.255.0 destination 172.20.100.1
    inet6 fe80::d90d:770e:50d0:dc38 prefixlen 64 scopeid 0x20<link>
    unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00 txqueuelen 500 (UNSPEC)
    RX packets 125 bytes 10172 (10.1 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 218 bytes 16368 (16.3 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

wlan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.0.1 netmask 255.255.255.0 broadcast 10.0.0.255
    inet6 [REDACTED] prefixlen 64 scopeid 0x20<link>
    ether [REDACTED] txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 61 bytes 8236 (8.2 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

ubuntu@ubuntu:~$
```

- 2、iptables 配置

◆ Mangle 表

```
-A PREROUTING -s 10.0.0.0/24 ! -d 10.0.0.0/24 -j MARK --set-xmark 0x2/0xffffffff
-A OUTPUT -s 10.0.0.0/24 ! -d 10.0.0.0/24 -j MARK --set-xmark 0x2/0xffffffff
```

◆ Nat 表

```
-A PREROUTING -s 10.0.0.0/24 -d 10.0.0.1/32 -p tcp -m tcp --dport 53 -j REDIRECT --to-ports 5353
-A PREROUTING -s 10.0.0.0/24 -d 10.0.0.1/32 -p udp -m udp --dport 53 -j REDIRECT --to-ports 60000
-A POSTROUTING -s 10.0.0.0/24 ! -o wlan0 -j MASQUERADE
```

◆ Filter 表

```
-A INPUT -p udp -m udp --dport 67 -j ACCEPT
-A INPUT -p udp -m udp --dport 5353 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 5353 -j ACCEPT
-A INPUT -p udp -m udp --dport 60000 -j ACCEPT
-A FORWARD -d 10.0.0.0/24 -i eth0 -j ACCEPT
-A FORWARD -s 10.0.0.0/24 -i wlan0 -j ACCEPT
```

3、规则路由设置情况

```
root@ubuntu:~# ip rule
0:      from all lookup local
32765:  from all fwmark 0x2 lookup 100
32766:  from all lookup main
32767:  from all lookup default
root@ubuntu:~# ip route show table 100
default via 172.20.100.1 dev tun0
root@ubuntu:~#
```

4、进程启动参数

```
/root/bin/tun_nat -i tun0 -c X.X.X.X -p 55559 -d
./udpproxy 10.0.0.1 60000 127.0.0.1 60000
./uredir 127.0.0.1 60000 X.X.X.X 60000
```

八、“墙外”服务器配置

1、网卡信息截图：

```
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.0.15 netmask 255.255.252.0 broadcast 10.0.3.255
    inet6 [REDACTED] prefixlen 64 scopeid 0x20<link>
    ether [REDACTED] txqueuelen 1000 (Ethernet)
    RX packets 15687 bytes 3881711 (3.7 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 15661 bytes 3737332 (3.5 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 30439 bytes 4358294 (4.1 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 30439 bytes 4358294 (4.1 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

tun0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST> mtu 1500
    inet 172.20.100.254 netmask 255.255.255.0 destination 172.20.100.254
    inet6 [REDACTED] prefixlen 64 scopeid 0x20<link>
    unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00 txqueuelen 500 (UNSPEC)
    RX packets 43 bytes 3539 (3.4 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 36 bytes 2892 (2.8 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

2、iptables 配置

◆ Mangle 表

```
-A PREROUTING -s 172.20.100.0/24 ! -d 172.20.100.0/24 -j MARK --set-xmark 0x2/0xffffffff
-A INPUT -s 172.20.100.0/24 ! -d 172.20.100.0/24 -j MARK --set-xmark 0x2/0xffffffff
-A OUTPUT -s 172.20.100.0/24 ! -d 172.20.100.0/24 -j MARK --set-xmark 0x2/0xffffffff
```

◆ Nat 表

```
-A POSTROUTING -o eth0 -j MASQUERADE
-A POSTROUTING -s 172.20.100.0/24 ! -o tun0 -j MASQUERADE
```

◆ Filter 表

```
-A FORWARD -s 10.0.0.0/24 -i tun0 -j ACCEPT
-A FORWARD -i tun0 -o eth0 -j ACCEPT
-A FORWARD -i tun0 -j ACCEPT
-A IN_public_allow -p udp -m udp --dport 55559 -m conntrack --ctstate NEW,UNTRACKED -j ACCEPT
-A IN_public_allow -p udp -m udp --dport 60000 -m conntrack --ctstate NEW,UNTRACKED -j ACCEPT
```

5、规则路由设置情况

```
[root@VM-0-15-centos ~]# ip rule
0:      from all lookup local
32765:  from all fwmark 0x2 lookup 100
32766:  from all lookup main
32767:  from all lookup default
[root@VM-0-15-centos ~]# ip route show table 100
default via 10.0.0.15 dev eth0
[root@VM-0-15-centos ~]#
```

6、进程启动参数

```
/root/bin/tun_nat -i tun0 -s
/root/bin/udpproxy 0.0.0.0 60000 127.0.0.1 53
```

九、其他说明

- 1、本文档仅用于学习研究目的，如果用于其他用途本文作者不承担任何责任。
- 2、部分代码来自互联网，版权由原作者所有。
- 3、欢迎访问 <https://github.com/wanpf>

