端口转发

打开转发开关

要让iptables的端口转发生效，首先需要打开转发开关

方法一：临时打开，重启后失效

```
sudo su
echo 1 >/proc/sys/net/ipv4/ip_forward
```

方法二：永久打开，重启依然有效
编辑/etc/sysctl.conf文件，将net.ipv4.ip_forward=1前面的#注释去掉，保存文件

```
vim /etc/sysctl.conf
```

然后执行 `sudo sysctl -p` 使其生效

```
sudo sysctl -p
sysctl --system
```

`sysctl net.ipv4.ip_forward` 查看是否生效

```
sysctl net.ipv4.ip_forward
```

典型使用场景举例

> 场景一：目标机的22端口外网没有打开，通过本地端口转发实现通过其他端口访问ssh的22端口

本机端A端口转发到本机的B端口

案例：10.10.40.40机器的22端口未对外开放，但开放了3000~4000之间的端口，因此通过3078端口转发到22实现ssh登录

其中 `enp2s0` 为你的网卡名称

```
sudo iptables -t nat -A PREROUTING -p tcp -i enp2s0 -d 10.10.40.40 --dport 3078 -j DNAT --to 10.10.4
```

> 场景二：将内网的22端口映射到外网的一个端口，实现SSH直接登录，不用跳转

案例：`10.10.66.12` 为外网机，`10.10.40.40` 为内网机，如果不做映射，需要先登录到66.12，再登录到40.40，做如下映射之后，可直接通过外网机的 `3079` 登录到内网机

```
sudo iptables -t nat -I PREROUTING -p tcp -d 10.10.40.40 --dport 3079 -j DNAT --to-destination 10.10.
sudo iptables -t nat -I POSTROUTING -p tcp --dport 22 -d 10.10.66.12 -j SNAT --to-source 10.10.40.40
```

> 场景三：在外网直接访问内网的MySQL数据库

案例：很多时候数据库在内网机，外网不能直接访问，但做运维的时候可能需要通过图形界面工具直接连上去。做端口映射就可以解决这个问题。例如：将外网机 `10.10.40.40` 的3001端口转发到内网机 `10.10.66.12` 的MySQL的 `3306` 端口

```
sudo iptables -t nat -I PREROUTING -p tcp -d 10.10.40.40 --dport 3001 -j DNAT --to-destination 10.10.
sudo iptables -t nat -I POSTROUTING -p tcp --dport 3306 -d 10.10.66.12 -j SNAT --to-source 10.10.40.4
```

显示nat规则列表：`iptables -t nat -L -n --line-numbers`

删除指定规则：`iptables -t nat -D PREROUTING 1`

iptables规则永久生效

首先安装iptables-persistent工具

```
sudo apt install iptables-persistent
```

每当设置了新的iptables规则后，使用如下命令保存规则即可，规则会根据ipv4和ipv6分别保存在了/etc/iptables/rules.v4和/etc/iptables/rules.v6文件中。

```
netfilter-persistent  save
```

由于 iptables-persistent 在安装时已经把它作为一个服务设置为开机启动了，它在开机后会自动加载已经保存的规则，所以也就达到了永久保存的目的。

路由网关

使用场景：服务器群组里，只有机器A连接了外网，其他机器和机器A在同一局域网内，可将机器A作为网关，使其他机器也能访问外网

例如：

将局域网内的 `10.10.200.203` 作为网关

操作前也需要**打开转发开关**

将输出数据包的源IP更改为网关的IP。不用担心，因为iptables会自动将回复的数据包的目标IP更改为原始源IP。

```
iptables -t nat -A POSTROUTING ! -d 10.10.0.0/16 -o enp2s0 -j SNAT --to-source 10.10.200.203
```

客户端配置

在局域网内的其他Windows、Mac或linux上配置:

IP地址： 手动

网关： 10.10.200.203

Linux Linux 网关 iptables NAT 端口转发