# Setting `iptables` - `Port` forwarding from one interface to another.

iptables is a user-space application program that allows a system administrator to configure the tables provided by the Linux kernel firewall (implemented as different Netfilter modules) and the chains and rules it stores. Different kernel modules and programs are currently used for different protocols; iptables applies to IPv4, ip6tables to IPv6, arptables to ARP, and ebtables to Ethernet frames.

Current scenario.

1. We have 2 Networks `192.168.0.0/24` which is a private network. `172.14.14.0/24` which is the Edge node network, which can communicate to the Active Directory.
2. We have Edge node, which have 2 Interfaces. `eth0` for `172.14.14.0/24` network which can communicate to Active Directory, Another is `eth1` for `192.168.0.0/24` which communicates with all the internal nodes.
3. Now, when the internal nodes which reside on the `192.168.0.0/24` network wants to authenticate from `AD` then it has to communicate to `EDGE` node which will port forward these request to the AD.

NOTE: There is no bridge between `172.14.14.237` and `192.168.0.10` interfaces.

`iptables` configuration used on `EDGE`.

```
iptables -t nat -A PREROUTING -p tcp -m tcp --dport 88 -j DNAT --to-destination 172.14.14.174:88
iptables -t nat -A PREROUTING -p udp -m udp --dport 88 -j DNAT --to-destination 172.14.14.174:88
iptables -t nat -A POSTROUTING -d 172.14.14.174/32 -p tcp -m tcp --dport 88 -j SNAT \
                                                                --to-source 172.14.14.237
iptables -t nat -A POSTROUTING -d 172.14.14.174/32 -p udp -m udp --dport 88 -j SNAT \
                                                                --to-source 172.14.14.237
iptables -t nat -A POSTROUTING -d 172.14.14.237/32 -p tcp -m tcp --dport 88 -j SNAT \
                                                                --to-source 192.168.0.10
iptables -t nat -A POSTROUTING -d 172.14.14.237/32 -p udp -m udp --dport 88 -j SNAT \
                                                                --to-source 192.168.0.10
```

Here is little more explanation about the `iptables` config used.

```
iptables -t nat -A PREROUTING -p tcp -m tcp --dport <port_to_forward> -j DNAT \
                                        --to-destination <active_directory_ip>:<port_to_forward>

iptables -t nat -A PREROUTING -p udp -m udp --dport <port_to_forward> -j DNAT \
                                        --to-destination <active_directory_ip>:<port_to_forward>

iptables -t nat -A POSTROUTING -d <active_directory_ip>/32 -p tcp -m tcp \
                                        --dport <port_to_forward> -j SNAT --to-source <eth0_ip>

iptables -t nat -A POSTROUTING -d <active_directory_ip>/32 -p udp -m udp \
                                        --dport <port_to_forward> -j SNAT --to-source <eth0_ip>

iptables -t nat -A POSTROUTING -d <eth0_ip>/32 -p tcp -m tcp \
```

```
                                        --dport <port_to_forward> -j SNAT --to-source <eth1_ip>

iptables -t nat -A POSTROUTING -d <eth0_ip>/32 -p udp -m udp \
                                        --dport <port_to_forward> -j SNAT --to-source <eth1_ip>
```

Check updated configuration.

```
[root@server-edge ~]# service iptables status
Table: nat
Chain PREROUTING (policy ACCEPT)
num  target     prot opt source               destination
1    DNAT       tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:88 to:172.14.14.174:88
2    DNAT       udp  --  0.0.0.0/0            0.0.0.0/0           udp dpt:88 to:172.14.14.174:88

Chain POSTROUTING (policy ACCEPT)
num  target     prot opt source               destination
1    SNAT       tcp  --  0.0.0.0/0            172.14.14.174       tcp dpt:88 to:172.14.14.237
2    SNAT       udp  --  0.0.0.0/0            172.14.14.174       udp dpt:88 to:172.14.14.237
3    SNAT       tcp  --  0.0.0.0/0            172.14.14.237       tcp dpt:88 to:192.168.0.10
4    SNAT       udp  --  0.0.0.0/0            172.14.14.237       udp dpt:88 to:192.168.0.10

Chain OUTPUT (policy ACCEPT)
num  target     prot opt source               destination
```

Trying to `telnet` to port 88 from slave node. Here we connect to `192.168.0.10` which forward the port to `172.14.14.237`, which inturn forward to `172.14.14.174`.

```
[root@waepprrkhd001 ~]# telnet 192.168.0.10 88
Trying 192.168.0.10...
Connected to 192.168.0.10.
Escape character is '^]'.
```