

iptables

iptables arguments

-t = table, -X = del chain, -i = interface

Deleting a line:

```
iptables -L --line-numbers  
iptables -D (CHAIN) (LINE NUMBER)
```

Nating:

example for FTP NAT:

```
iptables -t nat -A PREROUTING -p tcp --dport 21 -j DNAT --to-destination 192.168.1.100:21  
iptables -t nat -A PREROUTING -p tcp --dport 49152:65534 -j DNAT --to-destination 192.168.1.100:49152-65534
```

to check a nat rule:

```
iptables -t nat -nvL
```

masquerade traffic from an IP to another host

Enable ip forwarding

```
echo "1" > /proc/sys/net/ipv4/ip_forward
```

Then, we will add a rule telling to forward the traffic on port 1111 to ip 2.2.2.2 on port 1111:

```
iptables -t nat -A PREROUTING -p tcp --dport 1111 -j DNAT --to-destination 2.2.2.2:1111
```

and finally, we ask IPtables to masquerade:

```
iptables -t nat -A POSTROUTING -j MASQUERADE
```

Optionally, you could only redirect the traffic from a specific source/network with, for a host only:

```
iptables -t nat -A PREROUTING -s 192.168.1.1 -p tcp --dport 1111 -j DNAT --to-destination 2.2.2.2:1111
```

or for a whole network

```
iptables -t nat -A PREROUTING -s 192.168.1.0/24 -p tcp --dport 1111 -j DNAT --to-destination 2.2.2.2:1111
```

that's it, now the traffic to port 1111 will be redirected to IP 2.2.2.2 .

If you go on host 2.2.2.2, you should see a lot of traffic coming from the host doing the redirection.

Revision #4

Created 3 July 2017 21:51:06 by Dave

Updated 16 December 2017 08:41:55 by Dave