Contents

Introduction

One-to-one NAT (aka Static NAT) is a way to make systems behind a firewall and configured with private IP addresses appear to have public IP addresses.

Setup

Begin by assigning one of the static addresses to the WAN port using the Web interface and then use these scripts to add the rest.

Everything in square brackets needs to be replaced by your values. Examples are at the bottom.

Startup

Set up new public static IP on dd-wrt WAN interface. This must be done for each public static IP and should be saved to the Startup script using the Save Startup button on the Administration -> Commands page. If you do not know how to calculate your broadcast address, then enter your IP and subnet mask into this [calculator].

```
WANIF=`get_wanface`
ifconfig $WANIF:1 [PUBLIC_IP1] netmask [NETMASK] broadcast [BROADCAST]
ifconfig $WANIF:2 [PUBLIC_IP2] netmask [NETMASK] broadcast [BROADCAST]
```

```
ifconfig $WANIF:3 [PUBLIC_IP3] netmask [NETMASK] broadcast [BROADCAST]
```

Firewall

Here are some examples of firewall rules to NAT the external IP's to your internal IP's. Put them in the command box and use the Save Firewall button on the Administration -> Commands page to save them to your firewall script.

SNAT/DNAT

Route all packets for the new public IP, to a certain local IP.

```
iptables -t nat -I PREROUTING -d [PUBLIC_IP] -j DNAT --to-destination [LAN_IP]
```

Route packets on a port on the new public IP, to a different port of a local IP. Note that you can skip [LAN_Port] if it matches [Destination_Port].

```
iptables -t nat -I PREROUTING -d [PUBLIC_IP] -p tcp --dport [Destination_Port] -j DNAT --to-desti
```

Masquerade returned packets from the local ip to the public IP

```
iptables -t nat -I POSTROUTING -s [LAN_IP] -j SNAT --to-source [PUBLIC_IP]
```

PORT FORWARD

Forward port X to above local IP

```
iptables -I FORWARD -d [LAN_IP] -p tcp --dport [Destination_Port] -j ACCEPT
```

You could also replace above rule(s) with the following:

```
iptables -I FORWARD -d [LAN_IP] -j ACCEPT
```

Which instead of forwarding just a single port, will let through all tcp/udp connections on all ports to this public ip-->lan ip.

In other words, forwarding all connections would be no firewalling for that IP address.

Copy/Paste Examples

Startup Script

```
# Save Startup
WANIF=`get_wanface`
ifconfig $WANIF:1 173.X.X.250 netmask [NETMASK] broadcast [BROADCAST]
ifconfig $WANIF:2 173.X.X.251 netmask [NETMASK] broadcast [BROADCAST]
ifconfig $WANIF:3 173.X.X.252 netmask [NETMASK] broadcast [BROADCAST]
```

Firewall Script

```
# Save Firewall

# WAN .250 -> LAN .15
iptables -t nat -I PREROUTING -d 173.X.X.250 -j DNAT --to 192.168.0.15
iptables -t nat -I POSTROUTING -s 192.168.0.15 -j SNAT --to 173.X.X.250
iptables -I FORWARD -d 192.168.0.15 -p tcp --dport 21 -j ACCEPT
iptables -I FORWARD -d 192.168.0.15 -p tcp --dport 80 -j ACCEPT
iptables -I FORWARD -d 192.168.0.15 -p tcp --dport 5900 -j ACCEPT

# WAN .251 -> LAN .20
iptables -t nat -I PREROUTING -d 173.X.X.251 -j DNAT --to 192.168.0.20
iptables -t nat -I POSTROUTING -s 192.168.0.20 -j SNAT --to 173.X.X.251
iptables -I FORWARD -d 192.168.0.20 -p tcp --dport 21 -j ACCEPT
iptables -I FORWARD -d 192.168.0.20 -p tcp --dport 80 -j ACCEPT
iptables -I FORWARD -d 192.168.0.20 -p tcp --dport 5900 -j ACCEPT
```

Resources

- http://www.shorewall.net/NAT.htm
- http://www.dd-wrt.com/phpBB2/viewtopic.php?t=24555
- http://www.dd-wrt.com/phpBB2/viewtopic.php?p=400472#400472