NAT-PT - Installation

Home | Installation (PDF) | Documentation (PDF) | Download

NAT-PT is very easy to set up and in a default scenario should require a minimum amount of configuration. There are four simple steps you must follow:

Step 1 - Install NAT-PT

Simply go to the download and choose and RPM package for your distribution and architecture, and install it with

```
rpm -ivh naptd-version-system-arch.rpm
```

If you cannot find an RPM package suitable for your system, please write me an email detailing your distribution and architecture and I will create a installation package for you. You can also compile from source, simply get the source code, change the directory to where you downloaded it, and issue the following commands:

```
su
tar -zxf naptd-0.1.tar.bz2
cd naptd-0.1
./configure
make
make install
```

Step 2 - Configure NAT-PT

After installing the RPM run

```
naptd-confmaker
```

To get NAT-PT configured simply follow the questions asked and press enter to select the default options if you aren't sure how to answer. Only the very last part of the configuration will require your input. You must specify to NAT-PT which interfaces it will consider "inside" (IPv6) and which will be considered "outside" (IPv4). Please be aware that it is possible to use one interface for both functions. NAT-PT will work just fine on a computer with only one network interface!

Step 3 - Setup iptables and ip6tables

NAT-PT needs **both** iptables and ip6tables installed and running on your system. Most systems come with iptables pre-installed, but many do not have ip6tables. Simply go to http://rpmfind.net and obtain an ip6tables RPM package for your system and architecture. In order for NAT-PT to work correctly, ip6tables must be configured to drop all outbound ICMP "Destination Unreachable" packets to prevent your system from sending "Route Unreachable" messages. This can be done with the following commands (assuming default ip6tables configuration).

```
ip6tables -A OUTPUT -p icmpv6 --icmpv6-type 1 -j DROP
```

If your router is configured to perform IPv6 forwarding you must drop all packets going to the NAT-PT prefix (default: 2000:ffff::). The following rule will do:

```
ip6tables -A FORWARD -d 2000:ffff:: -j DROP
```

The second important thing is the configuration of iptables. If you intend to use the outbound IPv4 addresses as part of your translation pool, you must DROP all packets that are not part of NEW, ESTABLISHED, or RELATED connections. This should be part of a healthy firewall policy anyway. A set of rules as the one below will work perfectly.

```
iptables -A INPUT -i lo -j ACCEPT
iptables -A INPUT -m state --state ESTABLISHED -j ACCEPT
iptables -A INPUT -m state --state NEW -p tcp -m tcp --dport 22 -j ACCEPT
iptables -A INPUT -j DROP
```

Please make sure that both iptables and ip6tables both start during boot time. On most Linux systems this can be accomplished with the following commands. Don't worry if you get an error message similar to "ln: `/etc/rc3.d/S08iptables': File exists", this simply means that iptables was already setup to start up at boot time.

```
ln -s /etc/init.d/iptables /etc/rc3.d/S08iptables
ln -s /etc/init.d/iptables /etc/rc5.d/S08iptables
ln -s /etc/init.d/ip6tables /etc/rc3.d/S08ip6tables
ln -s /etc/init.d/ip6tables /etc/rc5.d/S08ip6tables
```

The technical reasons that make all the above necessary are explained in the documentation.

Step 4 - Setup the default router and DNS server for your hosts

All your internal hosts must have somehow obtain IP address as well as the address of their default router and DNS server. You can do this by using radvd or DHCPv6, but describing how to setup these daemons is beyond the scope of this document.

If you are running an IPv6 network which has a IPv6 connection to the rest of the IPv6 cloud you should use **totd** as a proxy DNS server. If your network has no connectivity to the rest of the IPv6 cloud, you can use NAT-PT's built in DNS translator.

If you choose to use the built in DNS translator, running 'naptd-confmaker' will help you determine the address of the DNS server to use. If you ever need to do it by yourself, simply take the translation prefix that you entered while configuring NAT-PT (by default 2000:ffff::) and add the IPv4 address of the DNS server you are currently using to the end of the prefix, to obtain the DNS server address. You can also use the form below:

Prefix:	2000:ffff::
IPv4 DNS server:	
IPv6 DNS server:	