NAT basics

Yuriy Andamasov - 2018-10-13 - 0 Comments - in Basics

Network Address Translation is a method of remapping one IP address space into another by modifying network address information in the IP header of packets while they are in transit across a traffic routing device.

There are two types of NAT: *source* and *destination* NAT (SNAT and DNAT respectively). The names can be slightly confusing, as they refer to the field of the raw IP Packet that they're changing; SNAT modifies the Source IP Address field, and DNAT modifies the Destination IP Address.

Source NAT

One of the most common use cases of Source NAT is the translation of IP addresses of many internal hosts into one or several public IP address(es).

To setup SNAT, we need to know:

- The internal IP addresses we want to translate
- The outgoing interface to perform the translation on
- The external IP address(es) to translate to

In this example, we need to provide internet access from our ISP on the interface `eth1`to the private subnet `192.168.1.0/24`.
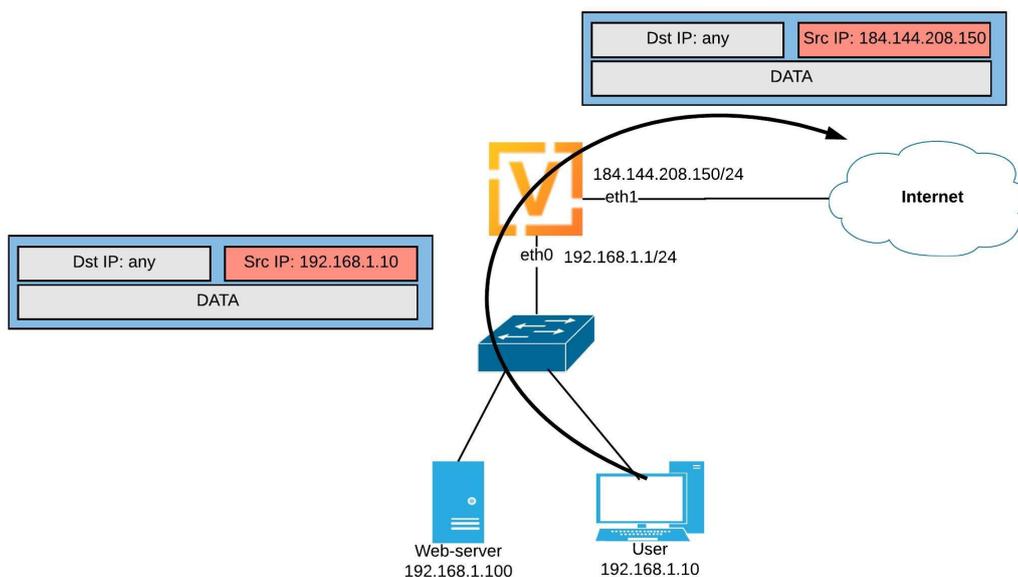
In this example, we use **masquerade** as the translation address instead of an IP address.

The **masquerade** target is effectively an alias to say "use whatever IP address is on the outgoing interface", rather than a statically configured IP address.

```
set nat source rule 10 outbound-interface 'eth1'
set nat source rule 10 source address '192.168.1.0/24'
set nat source rule 10 translation address 'masquerade'
```

To verify that translation occurs and view current translations, we can run `show nat source translations`:

```
vyos@vyos:~$ show nat source translations
Pre-NAT              Post-NAT            Prot  Timeout
192.168.1.5          184.144.208.150     tcp   431994
192.168.1.9          184.144.208.150     tcp   0
192.168.1.10         184.144.208.150     tcp   431947
192.168.1.10         184.144.208.150     tcp   58
```
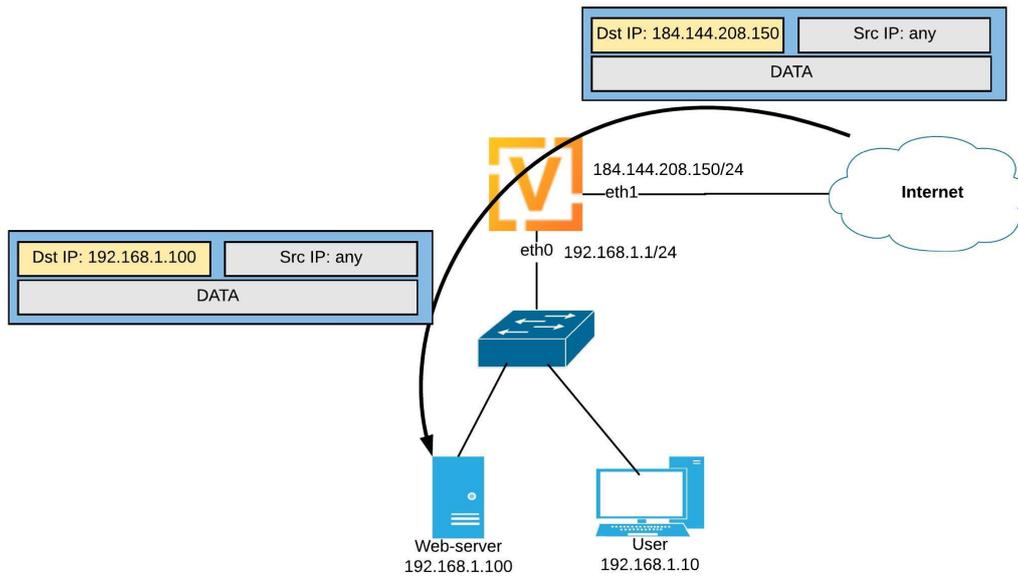
Destination NAT

DNAT is typically referred to as a **Port Forward**. When using VyOS as a NAT router, a common configuration task is to redirect incoming traffic to a system behind the VyOS router.

To setup a DNAT rule we need to gather:

- The interface traffic will be coming in on
- The protocol and port we wish to forward
- The IP address of the internal system we wish to forward traffic to

In our example, we will be forwarding web server traffic to an internal web server on `192.168.1.100`.

HTTP traffic makes use of the TCP protocol on port 80.

```
set nat destination rule 10 description 'Port Forward: HTTP to
192.168.1.100'
set nat destination rule 10 destination port '80'
set nat destination rule 10 inbound-interface 'eth1'
set nat destination rule 10 protocol 'tcp'
set nat destination rule 10 translation address '192.168.1.100'
```

More complex examples will be provided in future articles.