Networking

Network Address Translation

What NAT is

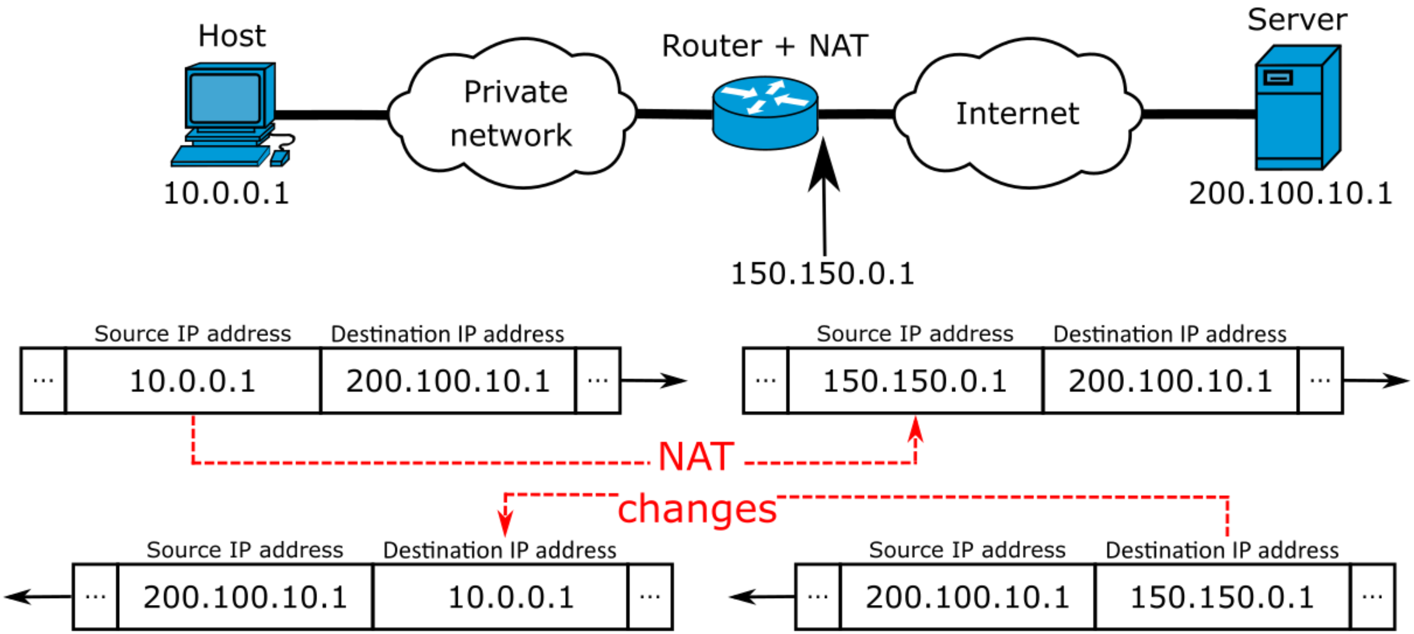
Network address translation (**NAT**) is a method of mapping an IP address space into another by modifying network address information in the IP header of packets while they are in transit across a traffic routing device.

Wikipedia ©

Network Address Translation is a method by which IP addresses are mapped from one realm to another, in an attempt to provide transparent routing to hosts.

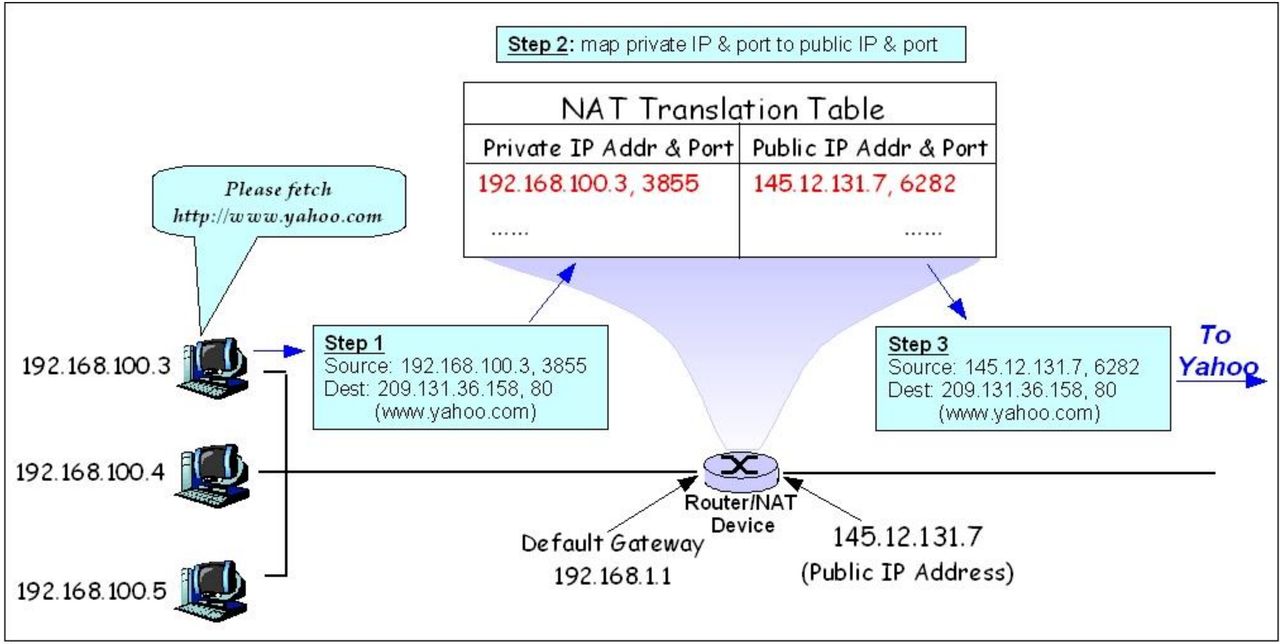
IETF RFC 2663

How NAT works in basis



Wikipedia ©

How NAT works ont-to-many



Step 2: map private IP & port to public IP & port

NAT Translation Table

Private IP Addr & Port	Public IP Addr & Port
192.168.100.3, 3855	145.12.131.7, 6282
......	......

Step 1
Source: 192.168.100.3, 3855
Dest: 209.131.36.158, 80
(www.yahoo.com)

Step 3
Source: 145.12.131.7, 6282
Dest: 209.131.36.158, 80
(www.yahoo.com)

Please fetch http://www.yahoo.com
192.168.100.3
192.168.100.4
192.168.100.5
Router/NAT Device
Default Gateway 192.168.1.1
145.12.131.7 (Public IP Address)
To Yahoo

Wikipedia ©

Type of NAT

Type of NAT will have different names and different technologies by vendors, it described in

RFC as:

- Traditional NAT (or) Outbound NAT
- Basic NAT
- Network Address Port Translation (NAPT)
- Bi-directional NAT (or) Two-Way NAT
- Twice NAT
- Multihomed NAT

Wikipedia as:

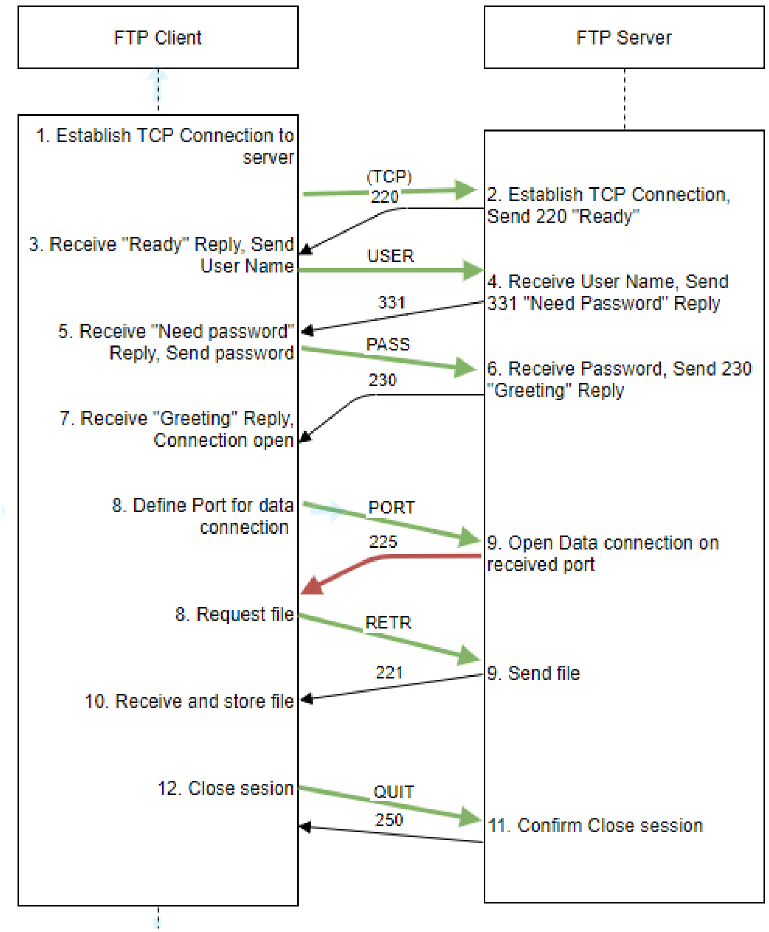
- DNAT
- SNAT
- Dynamic network address translation
- NAT hairpinning

Several vendors have his own classification.

Must know for success use NAT

- Session flow vs. Packet flow
- NAT Limitations

Use case with FTP:


FTP Client
FTP Server
1. Establish TCP Connection to server
(TCP)
220
2. Establish TCP Connection, Send 220 "Ready"
3. Receive "Ready" Reply, Send User Name
USER
4. Receive User Name, Send 331 "Need Password" Reply
331
5. Receive "Need password" Reply, Send password
PASS
6. Receive Password, Send 230 "Greeting" Reply
230
7. Receive "Greeting" Reply, Connection open
8. Define Port for data connection
PORT
225
9. Open Data connection on received port
8. Request file
RETR
9. Send file
221
10. Receive and store file
12. Close sesion
QUIT
250
11. Confirm Close session

Config NAT on iptables

At sample :
Eth0 – LAN 192.168.0.0/24
Eth1 – WAN 10.188.106.33/32

Allow to forwarding:

```
$ iptables -A FORWARD -i eth0 -o eth1 -s 192.168.0.0/24 -j ACCEPT
$ iptables -A FORWARD -i eth1 -o eth0 -d 192.168.0.0/24 -j ACCEPT
$ iptables -P FORWARD DROP
```

Do the NAT (addresses is sample):

```
$ iptables -A POSTROUTING -s 192.168.0.0/24 -o eth1 -j SNAT —to-source 10.188.106.33
```

Do the PAT for RDP server (address is sample):

```
$ iptables -A PREROUTING -i eth1 -p tcp -m tcp —dport 3389 -j DNAT —to-destination 192.168.0.2
```

Do the transparent proxy redirection (address and ports as sample)

```
$ iptables -A PREROUTING -d! 192.168.0.0/24 -i eth0 -p tcp -m multiport —dports 80,443 -j REDIRECT —to-ports 3128 .
```

Self study

GOAL:

Publish by NAT internal SSH server on you own virtual environment

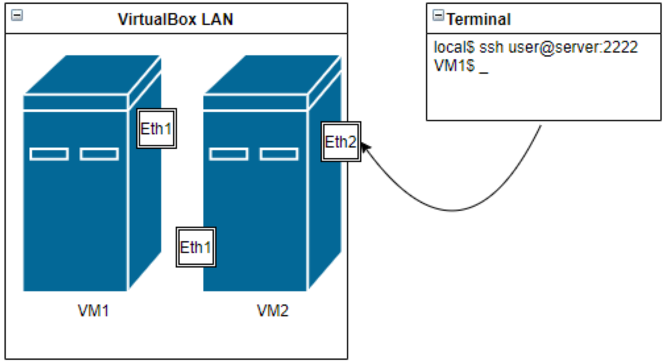
What to do:

- install and switch to iptables package on Server VM
- Configure environment
- Config iptables rules and OS for forward traffic and service NAT from first internal server to second adapter on second server at port 2222
- Do logon from your host PC by SSH on VM in internal Virtual network trough created NAT rule.

Environment:
2 Virtual machines (VM) with one and tow ethernet adapters on first and second VM. First adapter of VM's in same network and Second adapter from second VM in to bridged network for end testing purposes, as external egress. Suggest use VirtualBox and CentOS 7 images, used after SSH self study point.

How to check:
do login the
$ ssh user@server:2222

Where *user* is your user on fist VM , and *server* is address (in bridged network) on second adapter on second VM.



```
local$ ssh user@server:2222
VM1$ _
```

THANK YOU