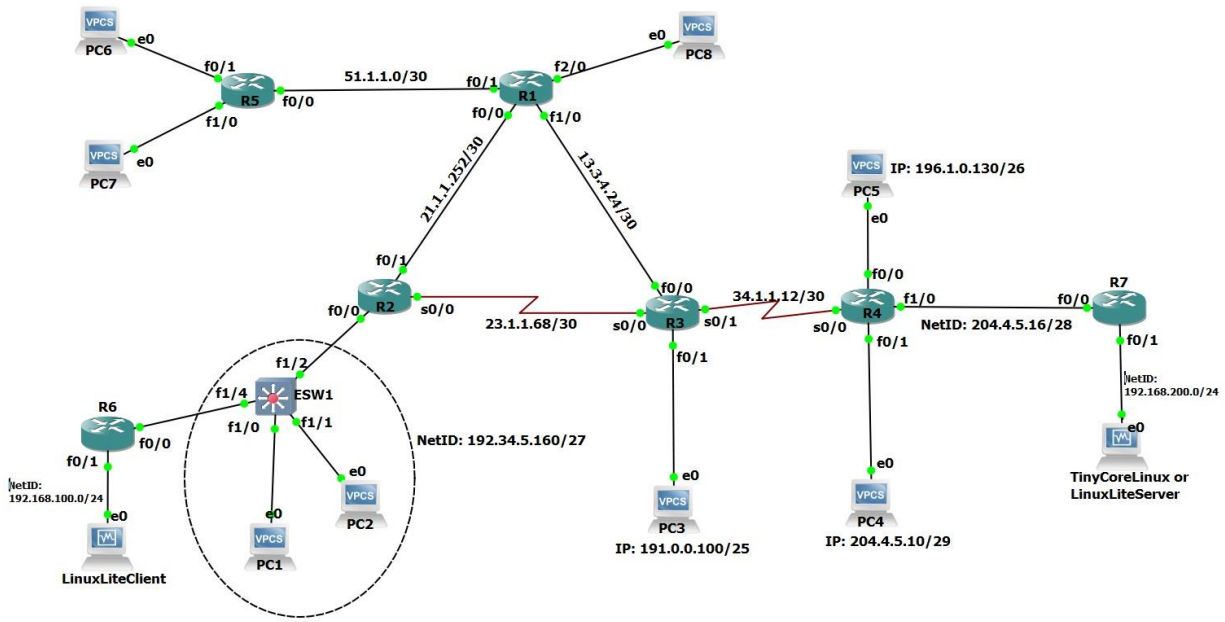
Netlab 6: NATs in GNS3

Purpose: In this Lab exercise, you will experiment with Network Address Translation (NAT) and Firewalls

Procedure

We are using the topology from the previous lab. We need to do a few modifications to it. Use the depicted topology below to implement the changes. In this case, routers R6 and R7 are going to operate as NAT/Firewall devices. **Important Note:** These two routers must be C7200s, NOT the C3725s.



Notes:

1.- Login credentials for the VMs are: username: tc and pass: netlab2020

2.- If you are using TinyCoreLinux VM, you need to update the password for the user ***tc***. In a CLI window apply the command: sudo passwd tc (enter the password **netlab2020**) . If you are using the LinuxLiteServer VM, you don't need to do do this step.

NAT Setup

Recall that a NAT device isolates a private network from the Internet. It also helps to leverage on public IP to connect multiple hosts in a private network. That said, we need to setup R6 and R7 with public and private IP addresses and activate NAT feature to avoid the router to continue functioning as "a router". Also, we need a DHCP server setup in each NAT. Apply the following settings in global config. (Note: If you get error messages when creating the NAT, you might need to increment the RAM size of the routers to 256Mb or 512Mb).

R6 Config: *interface f0/0*
description "Untrusted Network"
ip address 192.34.5.162 255.255.255.224 ← Important: exclude this IP in R1 DHCP server *ip nat outside*

interface f0/1 description "Trusted Network" ip address 192.168.100.1 255.255.255.0
ip nat inside

ip dhcp excluded-address 192.168.100.1 ← DHCP settings
ip dhcp pool INSIDE network 192.168.100.0 255.255.255.0 default-router 192.168.100.1

ip route 0.0.0.0 0.0.0.0 192.34.5.161 ← This is the default route for the untrusted network

access-list 1 permit 192.168.100.0 0.0.0.255 ← This statement identifies the private network to use the NAT

ip nat inside source list 1 interface FastEthernet0/0 overload ← This activates the translation from inside out using the indicated interface

R7 Config: *interface f0/0*
ip address 204.4.5.18 255.255.255.240
ip nat outside

interface f0/1

ip address 192.168.200.1 255.255.255.0
ip nat inside
ip dhcp excluded-address 192.168.200.1 ← DHCP settings
ip dhcp pool INSIDE network 192.168.200.0
255.255.255.0 default-router 192.168.200.1

ip route 0.0.0.0 0.0.0.0 204.4.5.17 ← This is the default route for the untrusted network

access-list 1 permit 192.168.200.0 0.0.0.255 ← This statement identifies the private network to use the NAT

ip nat inside source list 1 interface FastEthernet0/0 overload ← This activates the translation from inside out using the indicated interface

At this point, you should be able to ping any host in the topology from either Linux VM; but the Linux VMs cannot ping each other because the are behind the new created NATs. This also means you cannot reach the webserver, ftp, or ssh into the LinuxServer VM. Start two Wireshark captures, one in the link between R4 and R7 and the second between R7 and the LinuxServer VM. Apply the ICMP filter on both. Answer the following Question.

1.- When pinging any from LinuxServer VM to any of the VPCs, what difference(s) do you see between the two captures?

The source address and the destination address is different.

2.- What is the private IP addresses of both Linux VMs (Client and Server)?

Client- 192.168.100.2, Server- 192.168.200.2

3.- Continue both packet captures but modify the filter from *icmp* to *tcp*. Try to ftp or ssh into the LinuxServer from the LinuxClient using the private IP address. ***Explain*** what your captures are showing:

Nothing.

It is evident that the LinuxServer is isolated from the public network because the applications are no longer reachable. Let's fix that with a **static port translation**. This is the syntax of the command to apply in R7: (remember to be in Global Configuration to apply the command)

ip nat inside source static tcp [private IP of the server] [application port] [public IP of the NAT] [translated application port]

Replace the indicated parameters with the proper values. You need one static rule per application. Enable access the webserver using port 8080 instead of the well-known port 80. Also, enable access to the FTP and SSH services running in the server using the well-known ports.

4.- Open the web browser in the LinuxClient and try to contact the Web Server using the public IP as the URL and do not forget you are using port 8080.

a) ***Explain*** what your captures are showing:

A communication between R4-R7 using the public address and the communication between R7 and server address.

b) Can you see the content of the page in the packet capture?

No

5.- Now, try to FTP the LinuxServer from the LinuxClient VM.

a) ***Explain*** what are the differences in your captures:

A communication between R4-R7 using the public address and the communication between R7 and server address.

b) For the FTP packet capture, are you able to see the username in plain-text?

Yes.

6.- NAT provides some level of security; but can something else be done to improve the security even more?

NAT transfers packets of data from public to private addresses, it also prevents anything else from accessing the private device, but the request comes out as plain text. Something has to be done to protect that.

Save you configuration and upload your portable project to OneDrive. Post your Lab paper with answers on Beachboard.