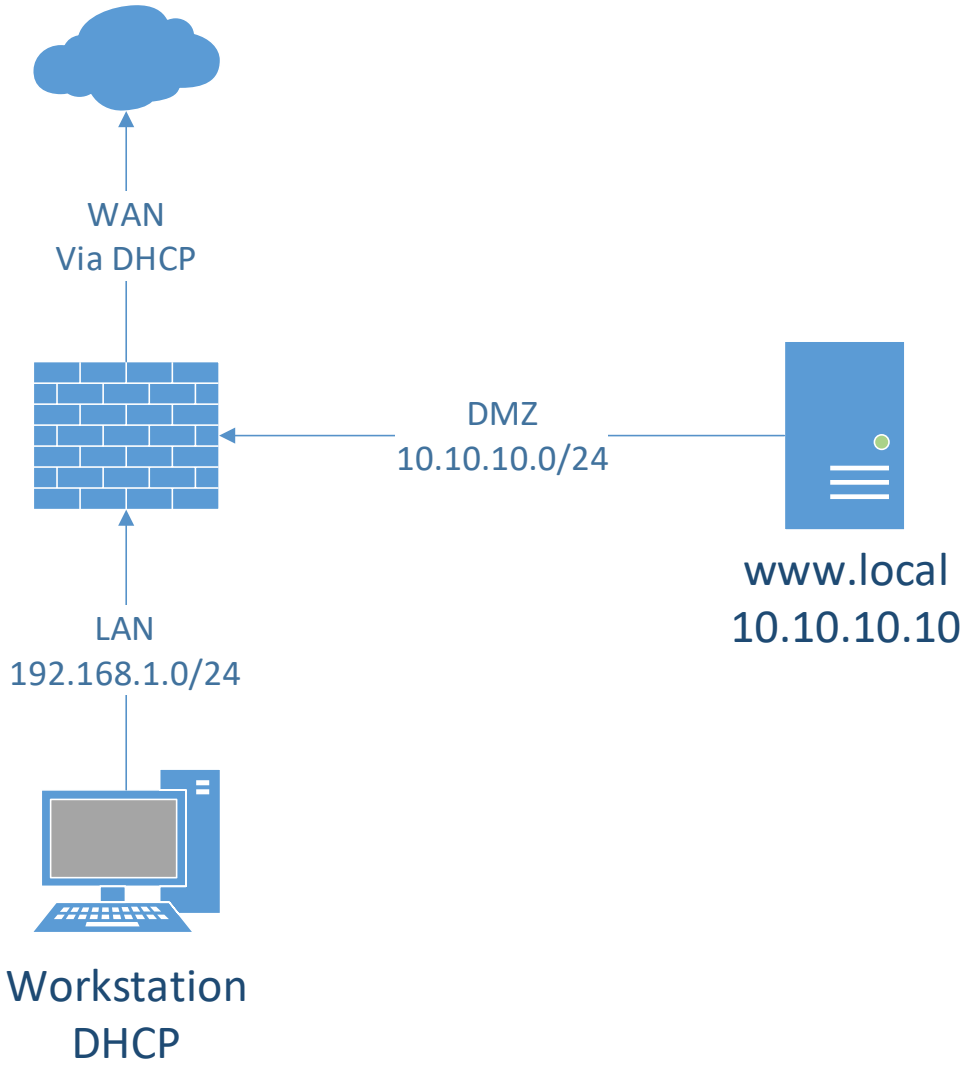
Lab1 – Firewall basics

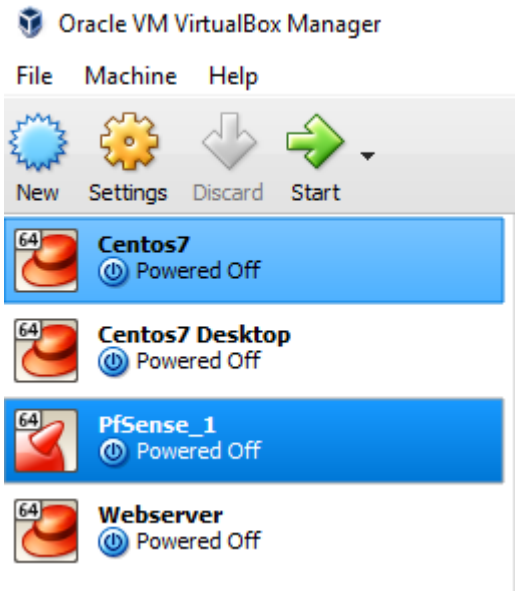
Document your commands or take screenshots. Answer questions in english or finnish.

The labs use the following topology (Workstation will be Centos7 Desktop):

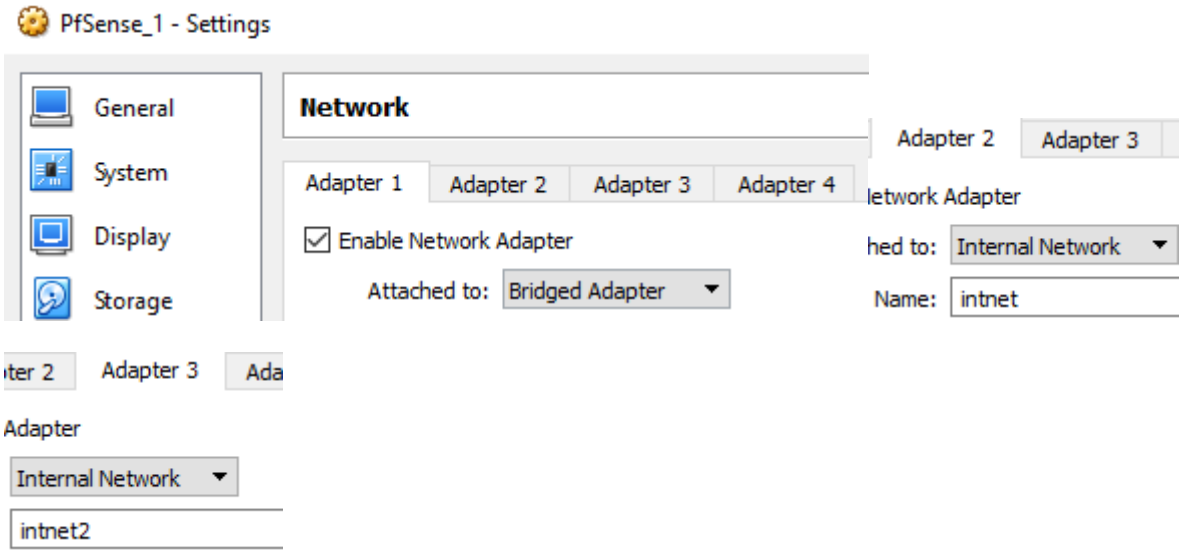


- ## Install PfSense (1p)

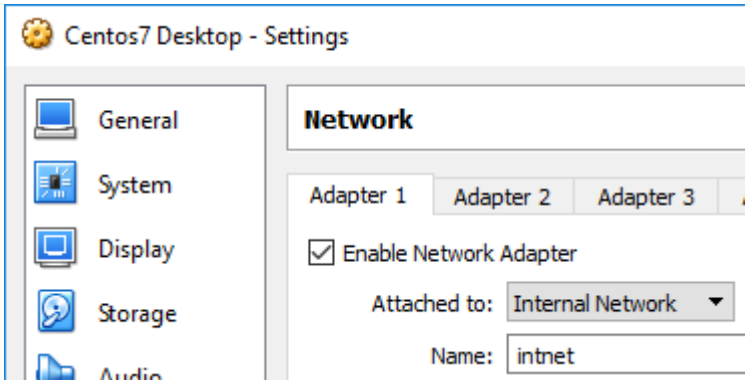
Retrieve the pre-installed VM images for PfSense, Centos7 Workstation and the Webserver from \\ghost.labranet.jamk.fi\ (PATH TBA). Import them to virtualbox and be sure to set “Reinitialize the MAC address…” tickbox in the import wizard. Set VM interfaces as following:



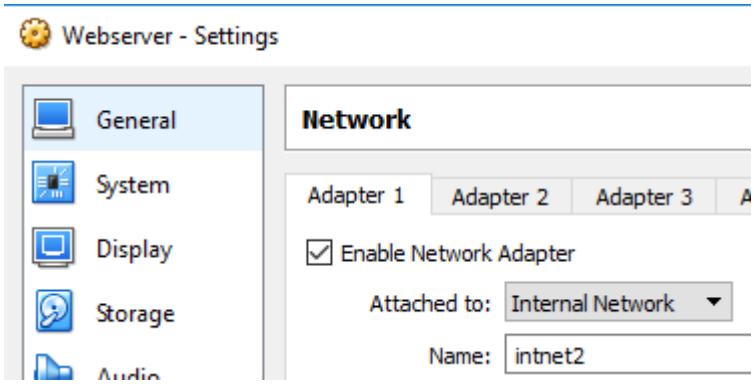
Pfsense: NIC1 Bridged, NIC2 Internal network (Name: intnet), NIC3 Internal network (intnet2)



Workstation: NIC1 Internal network (intnet)



Linux webserver: NIC1 Internal network (intnet2)

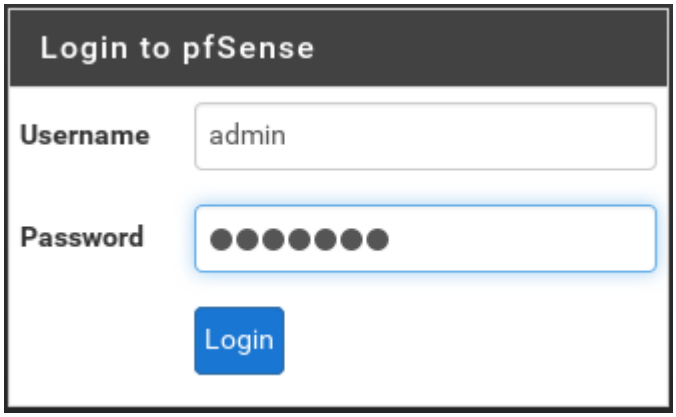


Next, boot up PfSense and assign interfaces if asked. If the system asks about setting up VLANs, answer no. Set the interfaces in the order displayed (usually vtnet0 vtnet1 vtnet2). vtnet0 will be the WAN, vtnet1 will be LAN and vtnet2 will be OPT1. We will rename this interface later.

Boot up the Workstation VM and check that it gets IP address from the PfSense VM. If not, check your network settings and the ordering of interfaces in the PfSense VM.

```
[root@localhost ~]# ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.101  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::a00:27ff:feb3:b7f  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:b3:0b:7f  txqueuelen 1000  (Ethernet)
        RX packets 20  bytes 2551 (2.4 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 92  bytes 10377 (10.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

When you get IP address, try accessing 192.168.1.1 with a browser in the Workstation VM. The default username/password are **admin/pfsense**



First configure the system to use LabraNet DNS servers (192.168.40.21 and .22). Go to Services -> DNS Resolver and turn it off. Then go to DNS Forwarder and turn it on.

System / General Setup

System

Hostname pfSense

Name of the firewall host, without domain part

Domain localdomain

Do not use 'local' as a domain name. It will cause local hosts run hosts not running mDNS.

DNS Server Settings

DNS Server 1 192.168.40.21

DNS Server 2 192.168.40.22

pfSense COMMUNITY EDITION

Services / DNS Resolver / General Settings

General Settings | Advanced Settings | Access Lists

General DNS Resolver Options

Enable ☐ Enable DNS resolver

Save

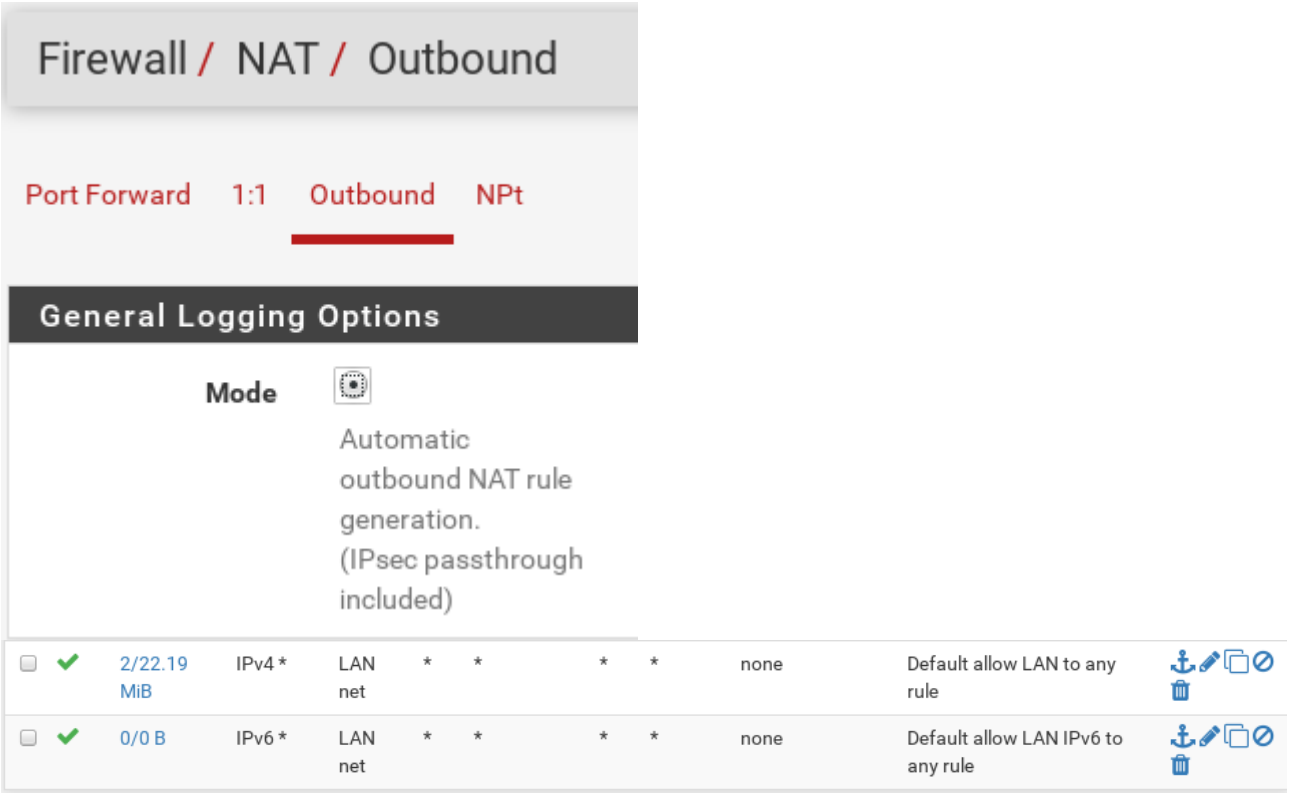
Services / DNS Forwarder

General DNS Forwarder Options

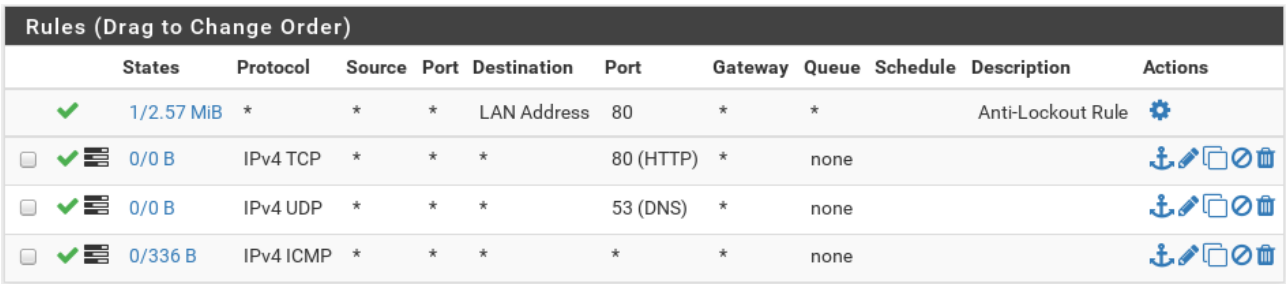
Enable ☑ Enable DNS forwarder

- **Firewall rules (1p)**

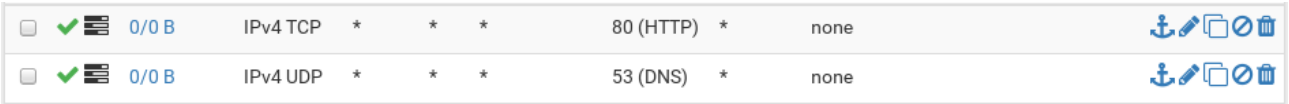
By default, the LAN subnet has Allow any rule attached to it. The default installation also has automatic outgoing NAT. Confirm and screenshot these rules in the Firewall-tab.



Delete the default Allow any rule.

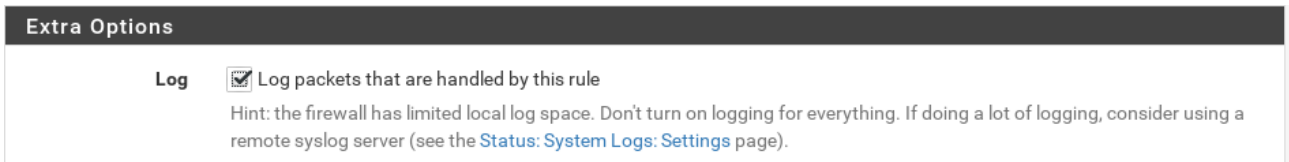


Add two rules to LAN that allow UDP/53 and TCP/80 to any.

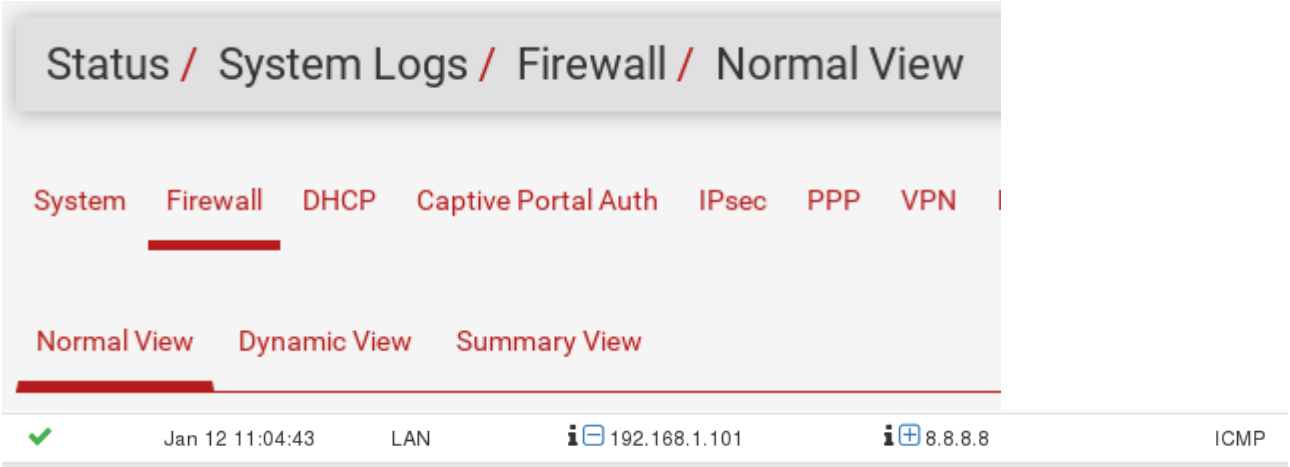


Also create a rule that allows ICMP (ping).

Check the tickbox for traffic logging.

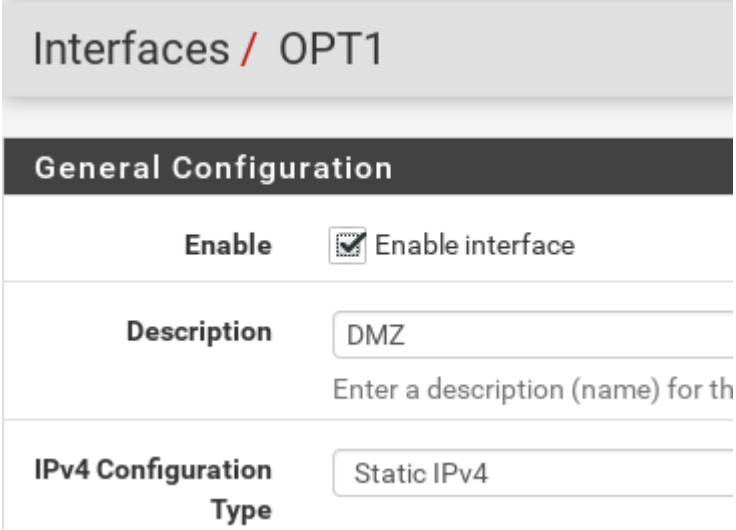


Apply settings and test that Internet browsing still works from the Windows 7 VM. Find out where the traffic is logged and screenshot.

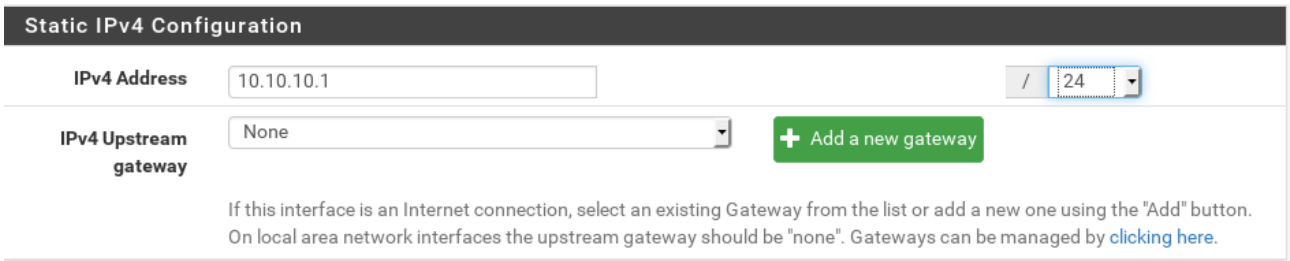


- **DMZ (1p)**

Modify the OPT1 interface. Set the name as DMZ and IP address as 10.10.10.1/24.



Remember to apply changes. Configure the same firewall rules for the DMZ as you did for the LAN.



Boot the Linux Webserver VM and login (root/root66). Check if it can ping its new gateway or if you can access it from the Workstation VM.

Floating WAN LAN DMZ

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	0/0 B	IPv4 IGMP	*	*	*	*	*	none			
	0/0 B	IPv4 TCP	*	*	*	80 (HTTP)	*	none			
	0/0 B	IPv4 UDP	*	*	*	53 (DNS)	*	none			

```
CentOS Linux 7 (Core)
Kernel 3.10.0-229.el7.x86_64 on an x86_64

K1521 login: root
Password:
Last login: Thu Jan 12 13:24:52 on tty1
[root@K1521 ~]# ping 10.10.10.1
PING 10.10.10.1 (10.10.10.1) 56(84) bytes of data.
64 bytes from 10.10.10.1: icmp_seq=1 ttl=64 time=0.860 ms
```

- **WWW NAT (1p)**

In this lab we configure a port forward -based NAT. Incoming connection to port 80 from the WAN will be forwarded to the webserver.

Create a Port Forward NAT rule at Firewall - NAT. Select Destination port as 80. Destination NAT address is the webserver address. To port is also 80. By default a firewall rule to allow this traffic will be created for you also. Apply changes.

Port Forward 1:1 Outbound NPt

Rules

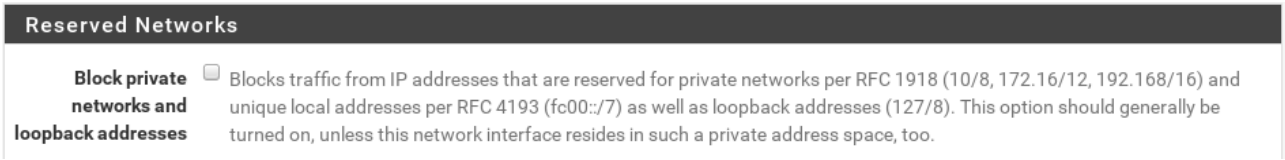
	Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
	WAN	TCP	*	*	*	80 (HTTP)	10.10.10.10	80 (HTTP)		

→

	WAN	TCP	*	*	WAN address	80 (HTTP)	10.10.10.10	80 (HTTP)		

Find out your firewalls public (WAN) address. It will be on the same subnet as the classroom PCs. With your Classroom PC, try to access the WAN address with your browser. This should forward the traffic to your webserver. You can also ask your neighboring students to test your address.

```
WAN (wan)       -> vtnet0     -> v4/DHCP4: 192.168.39.134/24
LAN (lan)       -> vtnet1     -> v4: 192.168.1.1/24
OPT1 (opt1)     -> vtnet2     ->
```



- **SSH NAT (1p)**

Create another port forward rule for SSH traffic. Set destination port as 2222 and To port as 22. This will move the SSH port from the default to something that is harder to guess. Test again with your classroom PC using PuTTY.