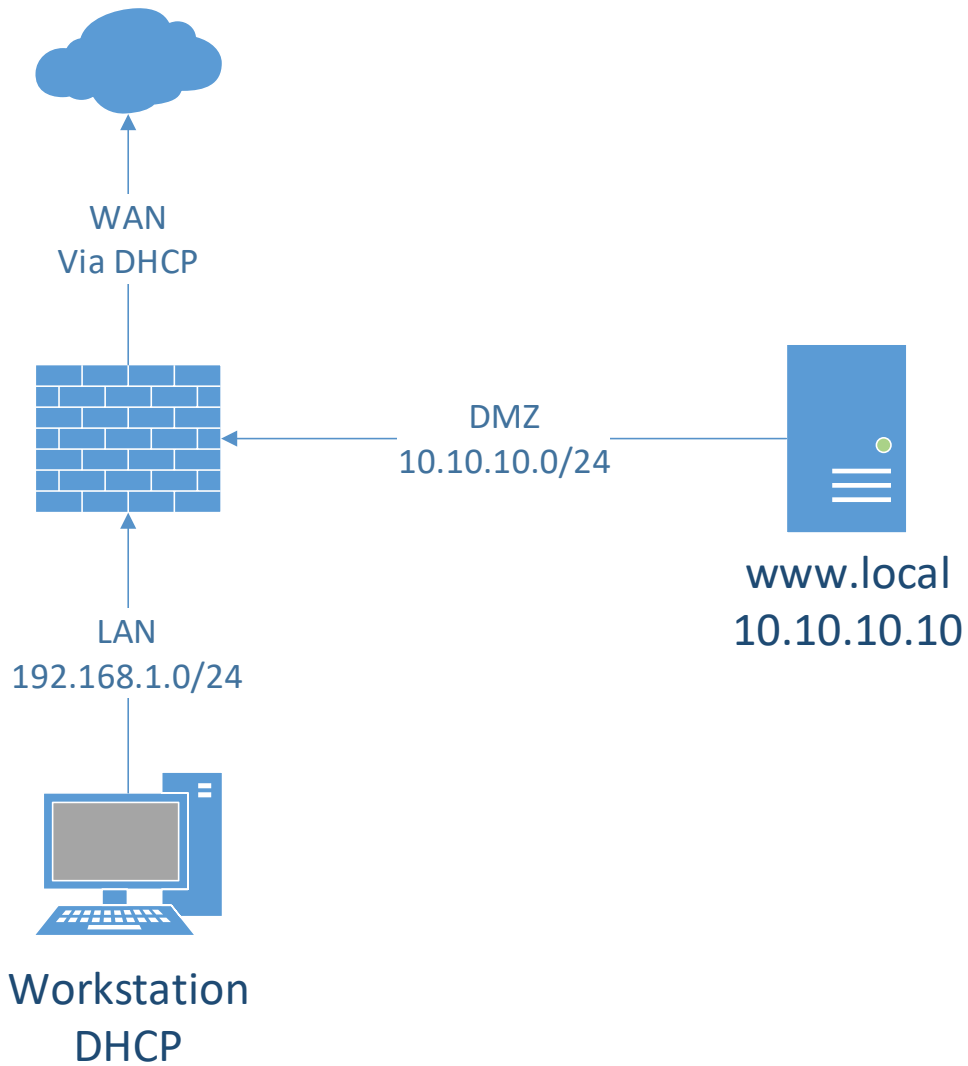


## Lab1 – Firewall basics

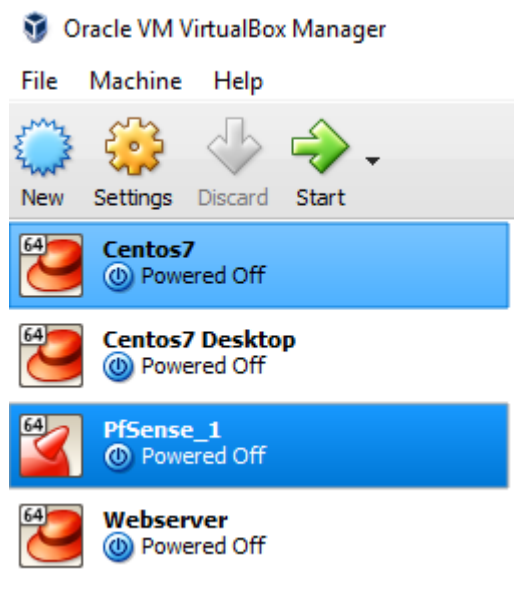
Document your commands or take screenshots. Answer questions in english or finnish.

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

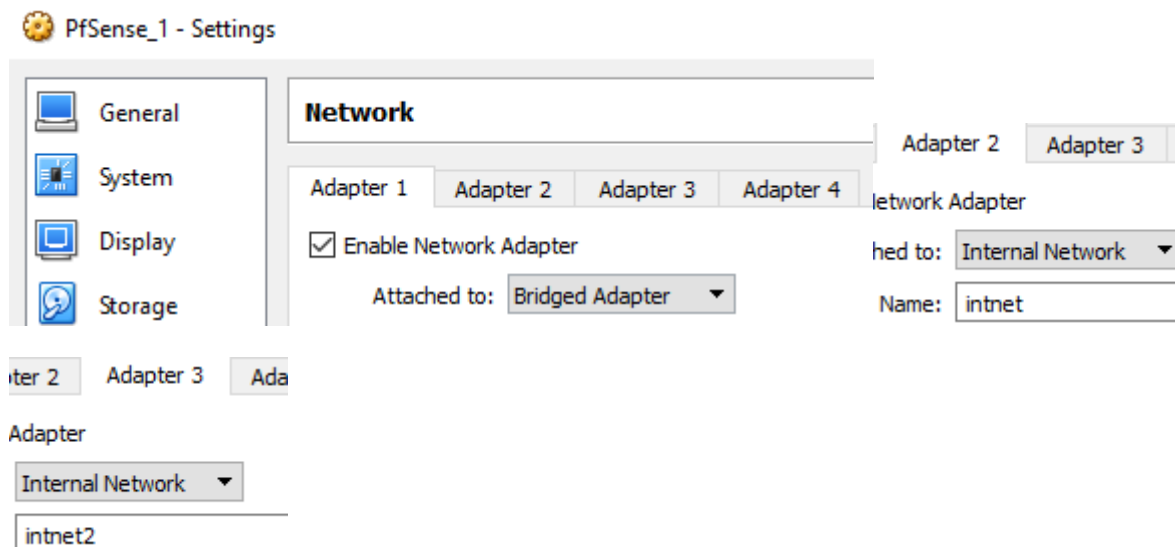


- **Install PfSense (1p)**

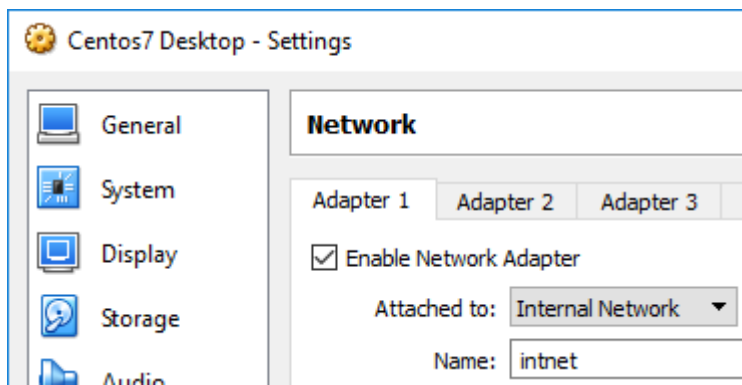
Retrieve the pre-installed VM images for PfSense, Centos7 Workstation and the Webserver from [\\ghost.labranet.jamk.fi](http://ghost.labranet.jamk.fi) (PATH TBA). Import them to virtualbox and be sure to set "Reinitialize the MAC address..." tickbox in the import wizard. Set VM interfaces as following:



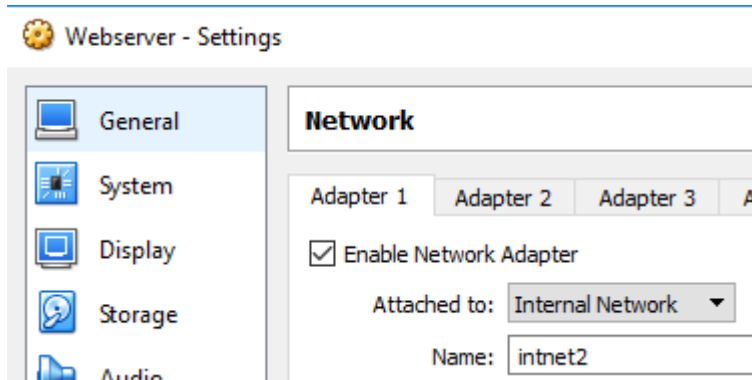
Pfsense: NIC1 Bridged, NIC2 Internal network (Name: intnet), NIC3 Internal network (intnet2)



Workstation: NIC1 Internal network (intnet)



Linux webserver: NIC1 Internal network (intnet2)

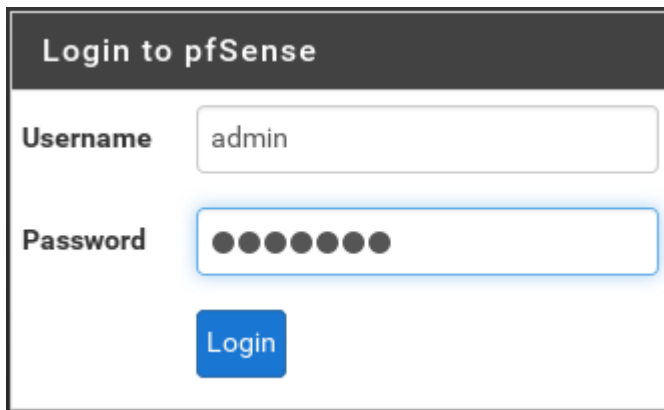


Next, boot up PfSense and assign interfaces if asked. If the system asks about setting up VLANs, answer no. Set the interfaces in the order displayed (usually vtnet0 vtnet1 vtnet2). vtnet0 will be the WAN, vtnet1 will be LAN and vtnet2 will be OPT1. We will rename this interface later.

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**

A screenshot of the pfSense login interface. It features a dark header bar with the text "Login to pfSense". Below the header, there are two input fields: "Username" with the text "admin" and "Password" with seven black dots. A blue "Login" button is positioned below the password field. The entire form is enclosed in a thin black border.

Login to pfSense

Username admin

Password ●●●●●●●

Login

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

Name of the firewall host, without domain part

Domain

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

### DNS Server Settings

DNS Server 1

DNS Server 2



## 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.

Firewall / NAT / Outbound

Port Forward

1:1

Outbound

NPt

General Logging Options

Mode

Automatic  
outbound NAT rule  
generation.  
(IPsec passthrough  
included)

|                          |                                     |             |        |         |   |   |   |   |      |                                    |  |  |  |  |
|--------------------------|-------------------------------------|-------------|--------|---------|---|---|---|---|------|------------------------------------|--|--|--|--|
| <input type="checkbox"/> | <input checked="" type="checkbox"/> | 2/22.19 MiB | IPv4 * | LAN net | * | * | * | * | none | Default allow LAN to any rule      |  |  |  |  |
| <input type="checkbox"/> | <input checked="" type="checkbox"/> | 0/0 B       | IPv6 * | LAN net | * | * | * | * | none | Default allow LAN IPv6 to any rule |  |  |  |  |

Delete the default Allow any rule.

| Rules (Drag to Change Order)  |  |            |           |      |             |             |           |       |          |                   |  |
|---|--|------------|-----------|------|-------------|-------------|-----------|-------|----------|-------------------|--|
|   | States                                       | Protocol   | Source    | Port | Destination | Port        | Gateway   | Queue | Schedule | Description       | Actions                                      |
| <div><div><div></div><div></div><div></div></div><div><div></div><div></div><div></div></div></div> | ✓  | 1/2.57 MiB | *         | *    | *           | LAN Address | 80        | *     | *        | Anti-Lockout Rule | <div><div></div><div></div><div></div></div> |
| <div><div><div></div><div></div><div></div></div><div><div></div><div></div><div></div></div></div> | <div><div></div><div></div><div></div></div> | 0/0 B      | IPv4 TCP  | *    | *           | *           | 80 (HTTP) | *     | none     |                   | <div><div></div><div></div><div></div></div> |
| <div><div><div></div><div></div><div></div></div><div><div></div><div></div><div></div></div></div> | <div><div></div><div></div><div></div></div> | 0/0 B      | IPv4 UDP  | *    | *           | *           | 53 (DNS)  | *     | none     |                   | <div><div></div><div></div><div></div></div> |
| <div><div><div></div><div></div><div></div></div><div><div></div><div></div><div></div></div></div> | <div><div></div><div></div><div></div></div> | 0/336 B    | IPv4 ICMP | *    | *           | *           | *         | *     | none     |                   | <div><div></div><div></div><div></div></div> |

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

|                          |                                     |       |          |   |   |   |           |   |      |  |  |  |  |  |  |
|--------------------------|-------------------------------------|-------|----------|---|---|---|-----------|---|------|--|--|--|--|--|--|
| <input type="checkbox"/> | <input checked="" type="checkbox"/> | 0/0 B | IPv4 TCP | * | * | * | 80 (HTTP) | * | none |  |  |  |  |  |  |
| <input type="checkbox"/> | <input checked="" type="checkbox"/> | 0/0 B | IPv4 UDP | * | * | * | 53 (DNS)  | * | none |  |  |  |  |  |  |

Also create a rule that allows ICMP (ping).

|                          |                                     |         |           |   |   |   |   |   |      |  |  |  |  |  |  |
|--------------------------|-------------------------------------|---------|-----------|---|---|---|---|---|------|--|--|--|--|--|--|
| <input type="checkbox"/> | <input checked="" type="checkbox"/> | 0/336 B | IPv4 ICMP | * | * | * | * | * | none |  |  |  |  |  |  |
|--------------------------|-------------------------------------|---------|-----------|---|---|---|---|---|------|--|--|--|--|--|--|

Check the tickbox for traffic logging.

Extra Options

Log

☒ Log packets that are handled by this rule

Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the [Status: System Logs: Settings](#) page).

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

Status / System Logs / Firewall / Normal View

System

Firewall

DHCP

Captive Portal Auth

IPsec

PPP

VPN

Normal View

Dynamic View

Summary View

✓

Jan 12 11:04:43

LAN

📄

192.168.1.101

📄

8.8.8.8

ICMP

• DMZ (1p)

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

Interfaces / OPT1

General Configuration

Enable

☒ Enable interface

Description

DMZ

Enter a description (name) for th

IPv4 Configuration Type

Static IPv4

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

Static IPv4 Configuration

IPv4 Address

10.10.10.1

/

24

IPv4 Upstream gateway

None

+

Add a new gateway

If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button. On local area network interfaces the upstream gateway should be "none". Gateways can be managed by [clicking here](#).

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 |
| <input type="checkbox"/>     | 0/0 B  | IPv4 IGMP | *      | *    | *           | *         | *       | none  |          |             |         |
| <input type="checkbox"/>     | 0/0 B  | IPv4 TCP  | *      | *    | *           | 80 (HTTP) | *       | none  |          |             |         |
| <input type="checkbox"/>     | 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 |
|--|-----------|----------|----------------|--------------|---------------|-------------|--------|-----------|-------------|---------|
| <div><div><div></div><div>✓</div><div>🔒</div></div></div> <div>WAN</div> <div>TCP</div> <div>*</div> <div>*</div> <div>*</div> <div>80 (HTTP)</div> <div>10.10.10.10</div> <div>80 (HTTP)</div> <div></div> <div><div><div></div><div>🔧</div><div>📄</div><div>🗑️</div></div></div> |           |          |                |              |               |             |        |           |             |         |

→

|                          |     |     |   |   |             |           |             |           |  |  |
|--------------------------|-----|-----|---|---|-------------|-----------|-------------|-----------|--|--|
| <input type="checkbox"/> | 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      ->
```



**Reserved Networks**

**Block private networks and loopback addresses** ☐ Blocks traffic from IP addresses that are reserved for private networks per RFC 1918 (10/8, 172.16/12, 192.168/16) and unique local addresses per RFC 4193 (fc00::/7) as well as loopback addresses (127/8). This option should generally be turned on, unless this network interface resides in such a private address space, too.



### • 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.

**Destination** ☐ Invert match. WAN address Type Address/mask

**Destination port range** Other 2222 Other 2222

From port Custom To port Custom

Specify the port or port range for the destination of the packet for this mapping. The 'to' field may be left empty if only mapping a single port.

**Redirect target IP** 10.10.10.10

Enter the internal IP address of the server on which to map the ports.  
e.g.: 192.168.1.12

☐ ☒ ☐ WAN TCP \* \* WAN address 2222 10.10.10.10 22 (SSH)

**PuTTY Configuration**

Category:

- Session
  - Logging
- Terminal
  - Keyboard
  - Bell
  - Features
- Window
  - Appearance
  - Behaviour

Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address) Port

192.168.39.134 2222

Connection type:

☐ Raw ☐ Adb ☐ Telnet ☐ Rlogin

☒ SSH ☐ Serial ☐ Cygterm

```
root@K1521:~
login as: root
root@192.168.39.134's password:
Last login: Thu Jan 12 13:34:24 2017
[root@K1521 ~]#
```