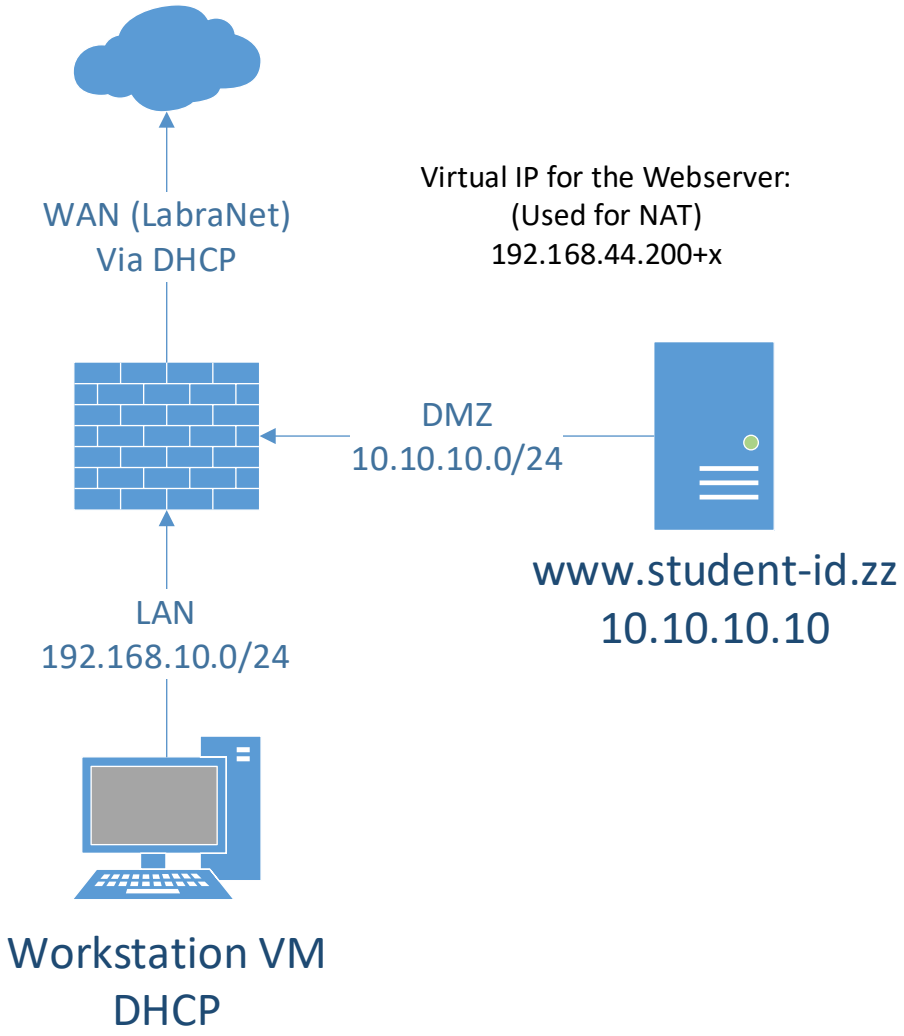
Lab8 – Firewall basics

You can use this lab manual for your personal documentation. Use screenshots for your own documentation, there will be questions later on that may point to this lab manual. Take care to check if you need to collect some information from the lab for the answers.

\ at the end of the line is used to mark that the command needs to be on one line. Replace **student-id** with your own student-id and **x** or **y** as your VMs correct IP in the labs.

NOTE! The subsequent labs will have more complex topology. The Firewall will have two internal networks (intnet) with names LAN and DMZ, the third network is bridged.

This lab is a bit complex to do at home, but not impossible. You need to change the WAN Virtual IP to match your home network settings.



- **Install the Topology**

Retrieve the pre-installed VM images (TTKS_Appliance.ova) for all lab virtual machines from \\ghost.labranet.jamk.fi\virtuaalikoneet\TTKS\. Import them to virtualbox and be sure to set “Reinitialize the MAC address…” tickbox in the import wizard.

NOTE: The VM interfaces should be correct but please verify:

- Pfsense: NIC1 Bridged, NIC2 Internal network (Name: LAN), NIC3 Internal network (DMZ)
- Webserver: NIC1 Internal network (DMZ)
- Workstation: NIC1 Internal network (LAN)

Next, boot up PfSense and check that the interfaces are in correct order::

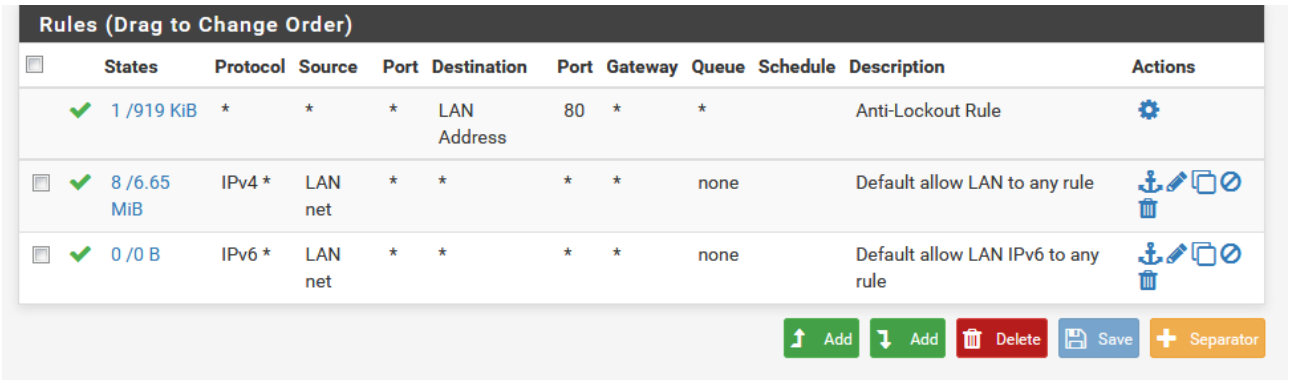
- WAN -> vtnet0
- LAN -> vtnet1
- OPT1 -> vtnet2 (We will rename this interface later)

If the interfaces are incorrect or not shown in the console, set them via *1) Assign Interfaces*

Boot up the Workstation VM (should not need credentials) 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. Check that the workstation has internet access.
When you get IP address, try accessing 192.168.10.1 with a browser in the Workstation VM. The default username/password are **admin/pfsense**

- **Firewall rules**

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.



-default rules

Automatic Rules:

	Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description
✔	WAN	127.0.0.0/8 ::1/128 192.168.10.0/24	*	*	500	WAN address	*	✔	Auto created rule for ISAKMP
✔	WAN	127.0.0.0/8 ::1/128 192.168.10.0/24	*	*	*	WAN address	*	⇄	Auto created rule

Disable the default Allow any rule. Add three rules to LAN that allow UDP/53, TCP/80 and TCP/443 to any. You can use the correct protocols from the drop-down list also. Also create a rule that allows ICMP (ping). Check the tickbox for traffic logging and give an appropriate name for the rules. Apply settings and test that Internet browsing still works from the Workstation VM. Find out where the traffic is logged.

✔	9 /23 KiB	IPv4 UDP	*	*	*	53 (DNS)	*	none	DNS	
✔	0 /29 KiB	IPv4 TCP	*	*	*	80 (HTTP)	*	none	HTTP	
✔	5 /1.70 MiB	IPv4 TCP	*	*	*	443 (HTTPS)	*	none	HTTPS	
✔	0 /0 B	IPv4 ICMP any	*	*	*	*	*	none	ICMP	

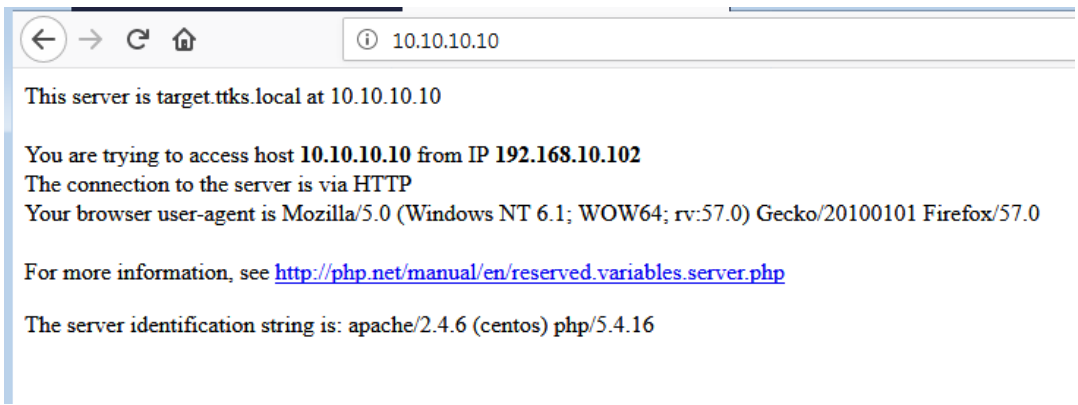
- kuvassa luodut säännöt palomuurille, liikenteen logitiedot löytyy status/system logs tabista

- **DMZ**

Modify the OPT1 interface. Set the name as DMZ and static 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. (Hint: You can copy the rules from the LAN rules with the button next to edit by changing the interface on the new rule)

Modify your webserver VM (www.student-id.zz) from LAB1 so it is connected to Internal network (DMZ) also and change the IP address to 10.10.10.10/24 and gateway and DNS to 10.10.10.1.

Test that you can access the Webserver from the Workstation VM (using the IP 10.10.10.10).

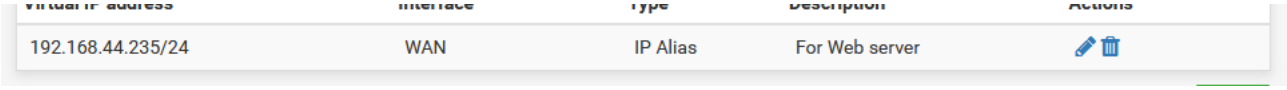


- sivulle pääsee

- **WWW NAT**

For other to gain access to your web server again from the classroom (which simulates the Internet here), you must create a NAT rule. In this lab we will use a Virtual IP from the classroom IP address block. Check the topology for the correct IP address. 235

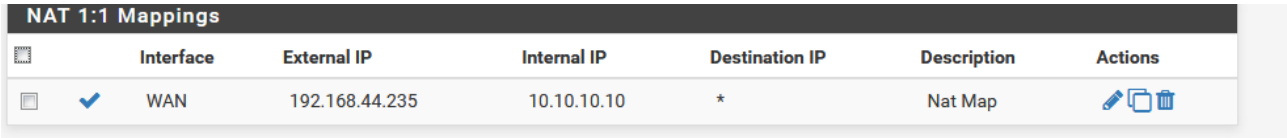
At Firewall -> Virtual IPs, add a new VIP with type IP Alias, interface WAN and the correct address from the topology picture. Set description as "For Web server". Remember to Apply changes



Virtual IP address	Interface	Type	Description	Actions
192.168.44.235/24	WAN	IP Alias	For Web server	

- Virutaalinen ip

Next, create a 1:1 NAT Mapping (Firewall - NAT - 1:1). External subnet IP is the virtual IP address with netmask /32, Internal IP is the webserver address (10.10.10.10) and Destination is Any. You can add a description also.

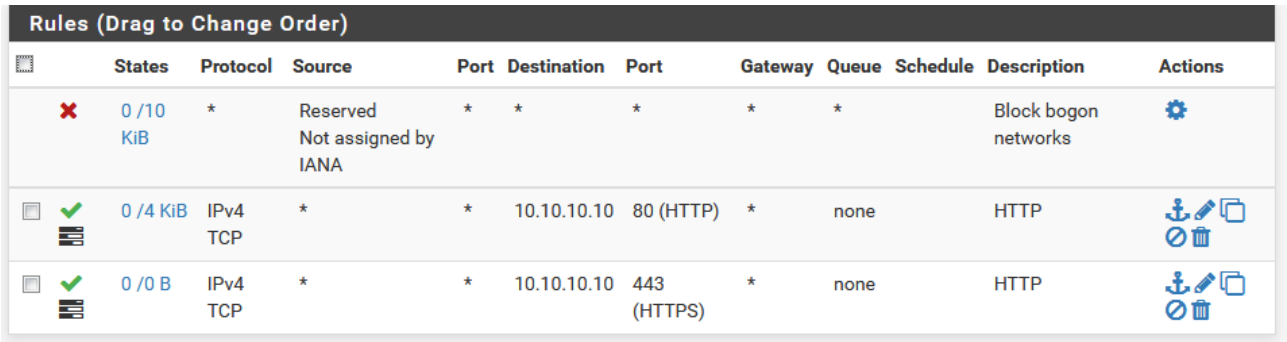


NAT 1:1 Mappings

	Interface	External IP	Internal IP	Destination IP	Description	Actions
✔	WAN	192.168.44.235	10.10.10.10	*	Nat Map	

- 1:1 reititys virtuaalisesta ipstä web serveriin.

Finally, add a firewall rule in WAN, allowing HTTP and HTTPS traffic to the webserver. Use 10.10.10.10 as the destination. You need two separate firewall rules. Set the "Log packets…" checkbox also.



Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✖	0 /10 KiB	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	
✔	0 /4 KiB	IPv4 TCP	*	*	10.10.10.10	80 (HTTP)	*	none		HTTP	
✔	0 /0 B	IPv4 TCP	*	*	10.10.10.10	443 (HTTPS)	*	none		HTTP	

- palomuurisäännöt http ja https

At WAN interface, disable the option called “Block private networks…”. This is because in classroom, our “WAN” connection uses private addressing (192.168.x.0 depending on the classroom).

After applying the changes, your webserver should respond from the Classroom Workstation (not the VM) using the Virtual IP. Update the correct IP to your DNS name in https://zz.labranet.jamk.fi/

Take a screenshot of the firewall logs showing your access to the Webserver from the Windows side.

✔	Mar 5 15:32:30	WAN	HTTP (1583414795)	192.168.44.35:34793	10.10.10.10:80 TCP:S

- logitieto, josta näkyy https liikenne web serverille

- ## Extra work for the fastest

- Figure out how to do IP blocklisting for JAMK public IP blocks. Go to PfSense management, Firewall – Aliases. Create an IP alias with the name “Blocklist” and choose type as Network(s). Add at least following IP blocks: 195.148.26.0/24 – description: Labranet; 195.148.128.0/24 – Public services 1; 195.148.129.0/24 – Public services 2. Save and Apply. Then create a firewall rule on LAN. Set Action as Block, Protocol: any and destination: alias Blocklist. Note! This Rule must be at the top of the list (it’s okay if it is below the anti-lockout rule). Apply changes and try to use JAMK services (www.jamk.fi, student.labranet.jamk.fi, etc.). If you find a service that still works, find out its IP block/address and add it to the alias. Lastly, change the Action on the rule to Reject. Try accessing the pages now and see how this changes the response.

- Figure out how to simplify firewall rules by using Floating rules. Basically you can create common rules for LAN/DMZ for HTTP, HTTPS and DNS

- Overwrite the DNS name www.student-id.zz using the webservers IP in the DNS Forwarder. This way the names work correctly from inside. (This is usually called split DNS)’

- Make a manual outgoing NAT rule so that public IP is 192.168.44.50+x