# Lab 5: Firewalls & VPN

IT&C 366 – Due Mar 6, 2025 at 8:00 a.m.

## Background

Watch these two videos as an introduction to this lab:

- Introduction to Firewalls
- VPN Types Options and Protocols Explained

Within the learning outcomes of this course, you are expected to install and configure various security technologies such as a firewall and VPN. These are tried and true solutions that contribute to a strong security posture at the personal, home, and enterprise level. Firewalls are traditionally thought of as a keystone in cyber defense. Although it is just one piece of the puzzle, when leveraged correctly, it is a powerful first line of defense. As we progress through the course, we expect that you will all go above and beyond in exploring these technologies and their capabilities.

This lab will introduce you to a firewall known as OPNsense. You will also integrate an OpenVPN server within the firewall to observe how those two technologies might work together. This is the first lab in a series that will dive into Network Security and Security Applications, a critical part of securing enterprise infrastructure.

## Outcomes

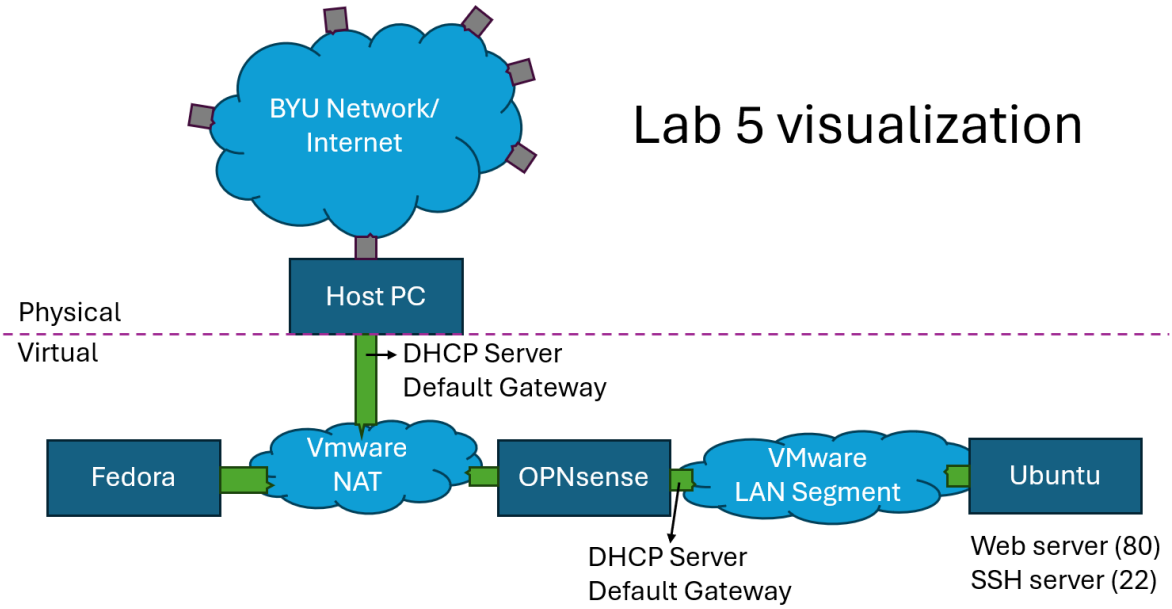
Students will be able to:

- Install and configure an advanced firewall.
- Interpret, test, and write firewall rules.
- Install and configure a VPN connection.
- Understand how VPNs and Firewalls are applied in Enterprise environments.

Class learning objectives: Secure Network Environments, Organizational Implications

## Setup

To truly get a feel for firewalls, we need a controlled environment with (at least) two networks, with a firewall device bridging them that we can play with. To accomplish this, we will use 3 Virtual Machines: Fedora as a desktop on one virtual network (treated as the “WAN”), Ubuntu as a server on a different virtual network (treated as the “LAN), and OPNsense as a firewall bordering both virtual networks. The graphic below shows how they will be laid out:

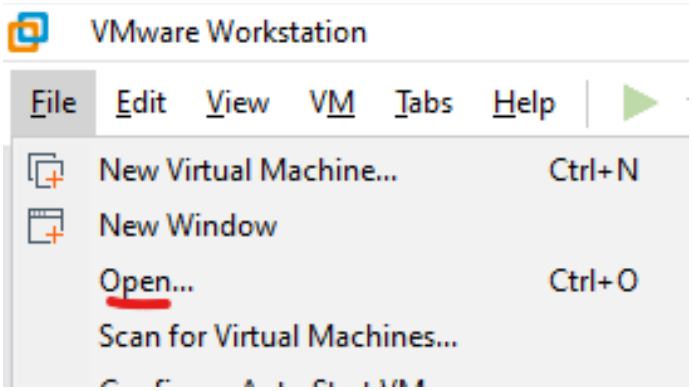



With this setup, the Fedora desktop cannot directly communicate with the Ubuntu server, and vice versa. Instead, we will configure the firewall allow the traffic we want through according to certain rules.

Specifically, we will use the following techniques:

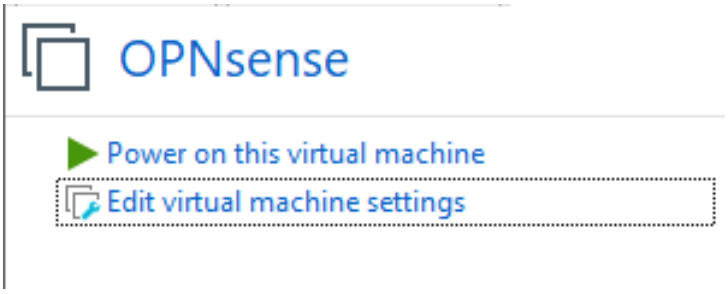
1. Port forwarding, so firewall acts as a middleman forwarding traffic from the WAN to actual servers within its LAN.
2. VPN, so authenticated devices can join the LAN virtually and interact with servers there directly.

Download the three VM files from Learning Suite, then import them to VMware Workstation.

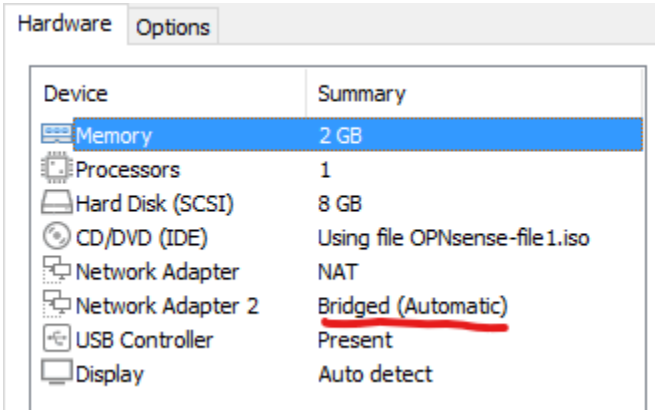



*Use the Open… option rather than New Virtual Machine…*

**IMPORTANT**: fix the network interfaces of each VM after importing them. By default, VMware will assign the “Bridged” option to the OPNsense and the Ubuntu machines, but they should have a LAN segment instead. The ones with NAT should stay the same.

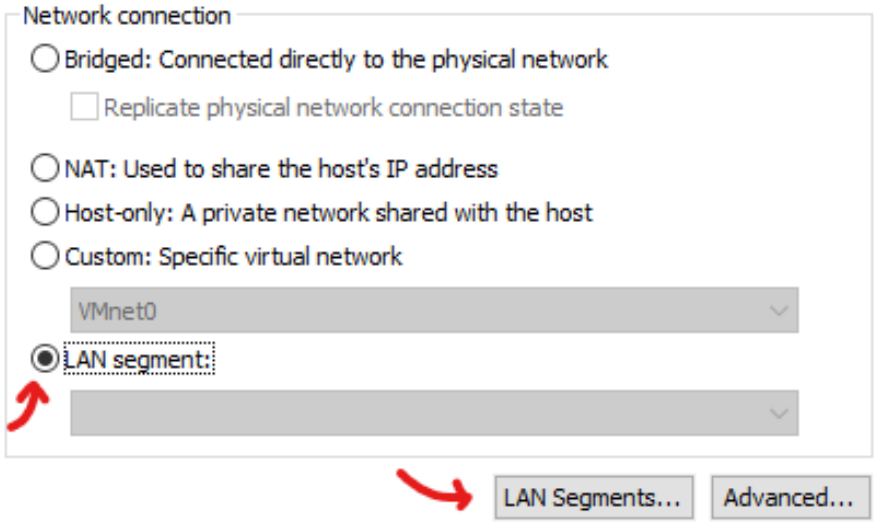



*Edit the VM*

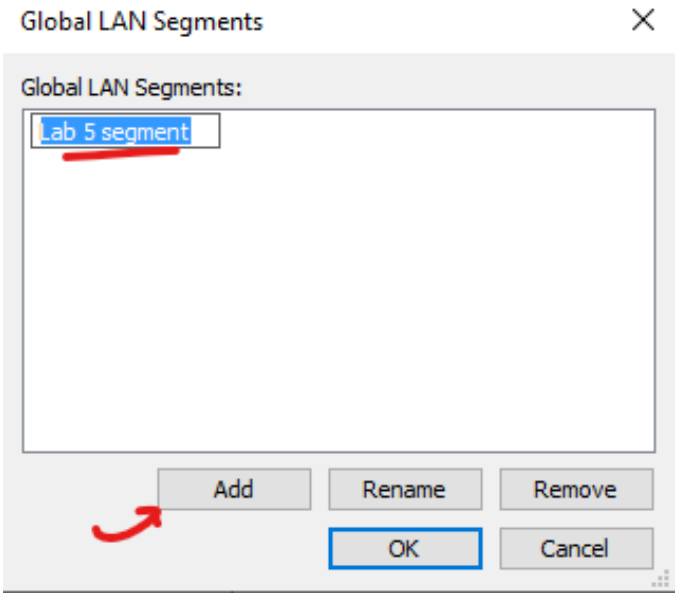



*If you see Bridged, this is needs to be changed!*

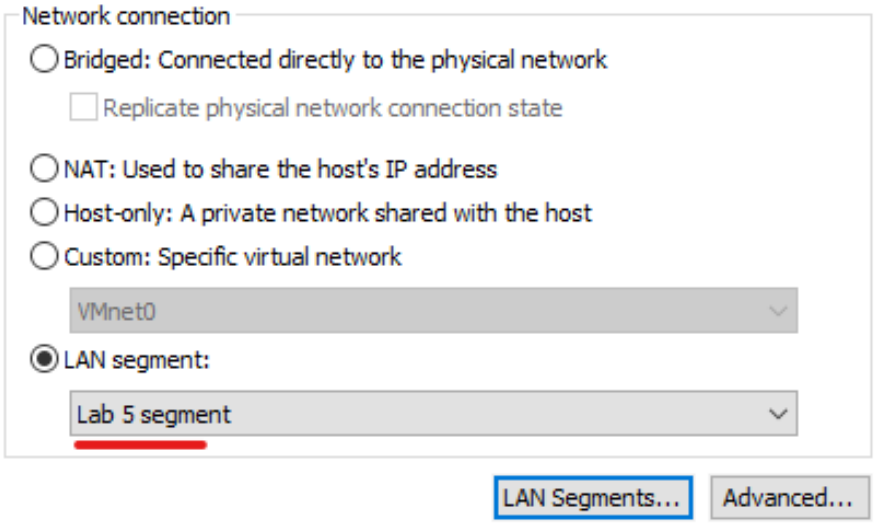
1. Select the Bridged network adapter.
2. Select “LAN segment” from the network connection options.



3. Create a new LAN segment (if you haven't yet) by clicking "LAN Segments…"

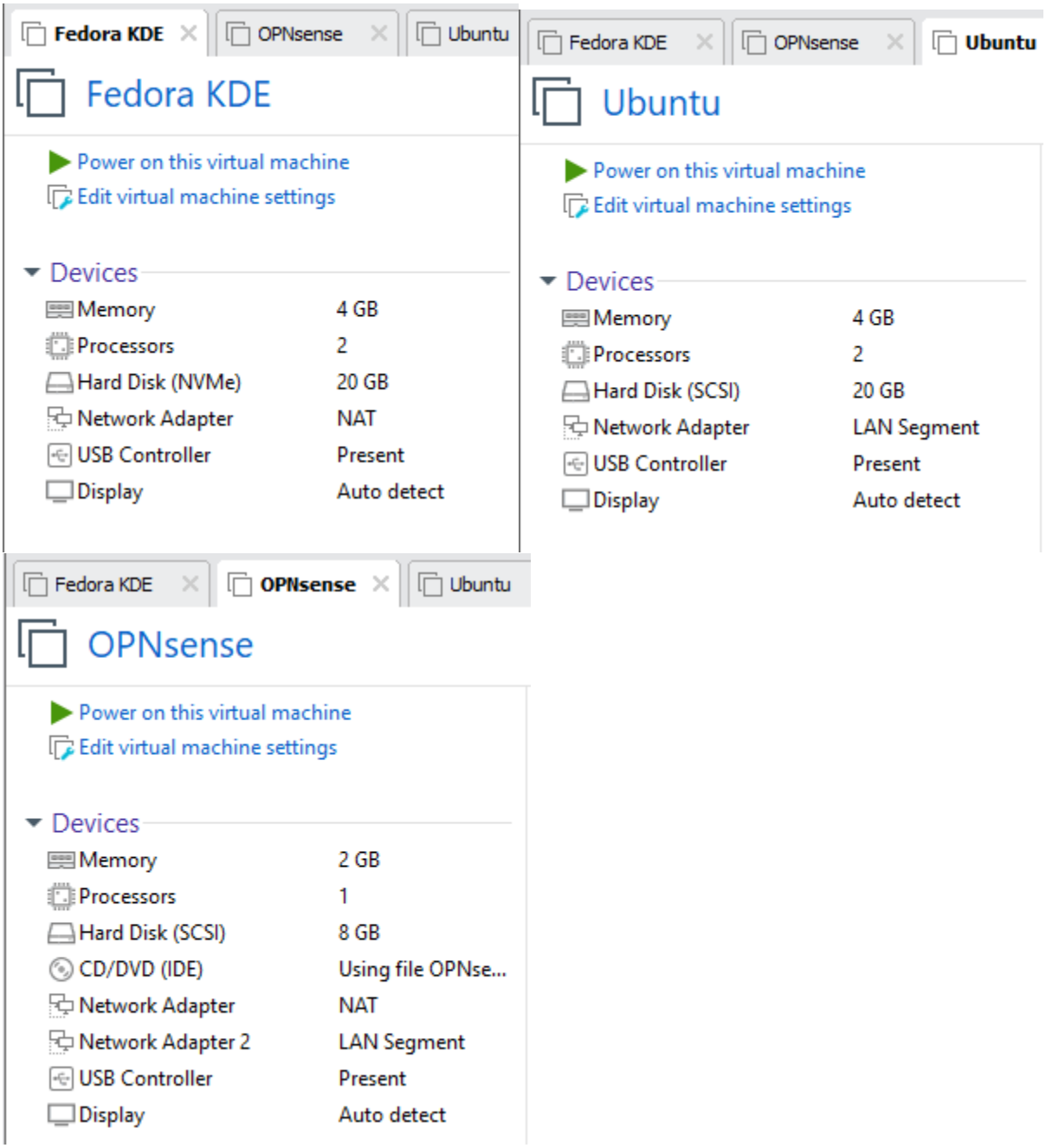



4. Give it a sensible name.
5. Now you can select this LAN segment from the drop-down menu.




6. Make sure to use the same LAN segment for the OPNsense and Ubuntu machines.

Once your VMs match what's shown below, you should be ready to power them on!




If you are asked, select "I copied it" when powering the VM on. This will simply randomize the MAC address to avoid collisions, but it shouldn't really be an issue.

We've set up automatic login, but here's the login credentials if you need them:

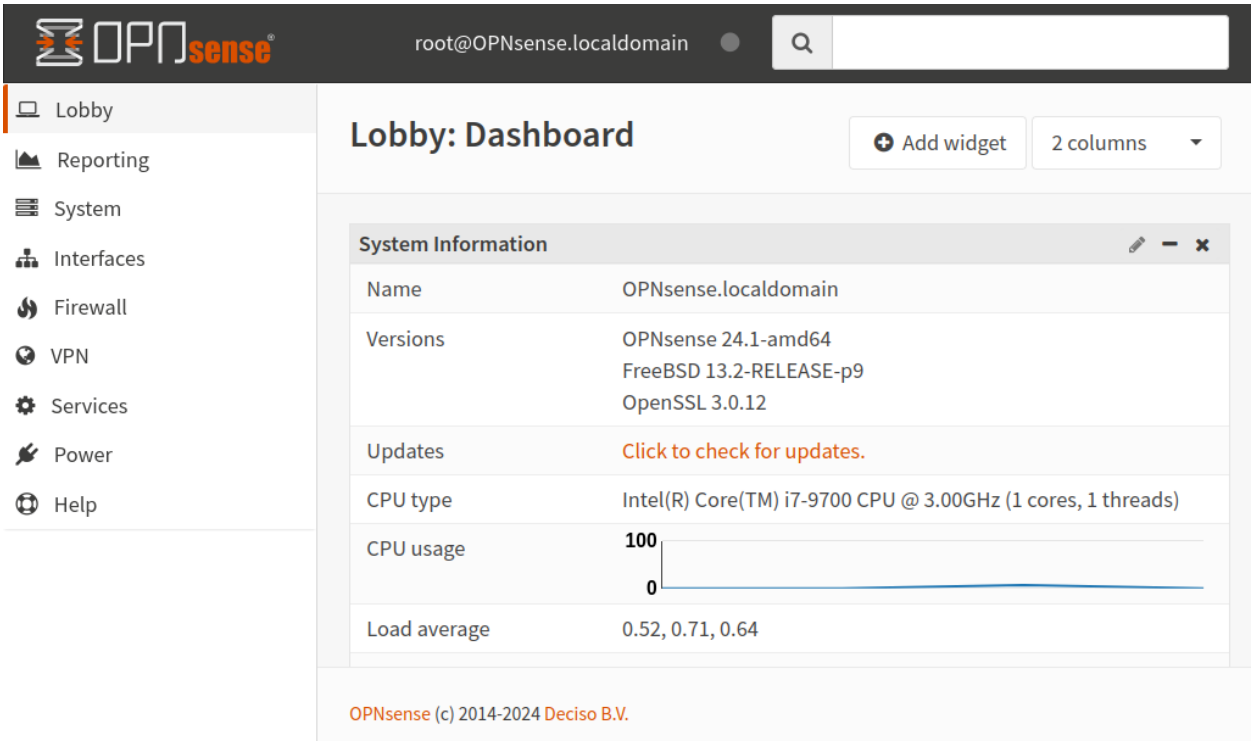
- Fedora: fedora/fedora
- Ubuntu: user/Ubuntu

## Activity

For each step, you will configure the firewall using its web interface. For security, OPNsense only makes this accessible from within the LAN, which in our case means just the Ubuntu machine.

1. In the Ubuntu machine, open Firefox.
2. Navigate to the OPNsense LAN address, which should be bookmarked as 192.168.1.1
3. Log in with the default credentials.
    - Username: root
    - Password: opnsense

Welcome to the firewall!




## Step 1: Change the root password

It is critical to change the default passwords of any network boundary devices. Find where to do that in OPNsense and set it to something you will remember.

In your submission, note where this setting is found.

Although not necessary for this lab, be sure to do the same for your home router too.

## Step 2: Familiarize yourself with firewall rules

You will find a prepopulated collection of firewall rules in the Firewall > Rules > WAN section. Look over them and try to understand the syntax of the rule and what type of traffic it applies to. Understanding these rules will prove helpful in the upcoming sections.

## Step 3: Create firewall rules

For security, pretty much all incoming traffic from the WAN is blocked by default, including ICMP packets. If you try pinging the firewall's WAN address from the Fedora desktop, you'll see nothing happens, even though they are on the same network.

For this step, you will add a rule to allow pings.

1. Try pinging the OPNsense firewall from the Fedora desktop.
2. We know both machines are online, but the pings are failing. This is because the firewall is dropping them.
3. If you're curious, look for the logs in the firewall showing the packets being dropped.

Now it's time to actually make the firewall rules.

1. On the menu on the left, navigate to Firewall > Rules > WAN.
2. Click the + button to add a new rule.
3. Here you'll see fields to configure all the options a firewall rule could need, like we discussed in class. You can click the info button for more info on each option.
4. After familiarizing yourself, fill in the rule to allow pings from your Fedora machine on the WAN.
    a. Hint: this means allowing ICMP echo requests.
    b. Hint: if your feeling stuck, someone described their solution in this forum post.
    c. Note: For the 'source', please do not use 'any'. Specify the IP address of the Fedora machine. While using 'any' will work, it's bad practice to allow more than you know you need.
5. Once you finish your rule, save it and apply the new configuration.
6. Test your rule by pinging the firewall from the Fedora machine. If it works, congrats! Take a screenshot for your submission. If it doesn't work, what existing rule might be causing the problem? How might you fix that without deleting any rules?

## Step 4: Configure port forwarding

Port forwarding is one way to make LAN resources accessible on the WAN. Luckily, OPNsense makes has an easy wizard to configure this. We will forward port 80 to the Ubuntu machine, so Fedora can access its web server via the firewall.

Try accessing the HTTP site from Fedora machine to confirm it doesn't work.

1. On the menu on the left, navigate to Firewall > NAT > Port Forwarding.
2. Click the + button to add a new port forward.
3. Here you will see fields almost like the firewall rule menu from before. That's because the desired behavior is mostly the same as a firewall rule, just with an added step of redirecting the packet to some other host.
4. Add a rule to forward HTTP requests from the Fedora machine over to the Ubuntu machine.
    a. The source address is the Fedora machine IP address. But as we've learned, the source port is usually random, so you can put 'any' for that.
    b. The destination is the OPNsense WAN address, for TCP port 80.
    c. It should redirect this to the Ubuntu machine's IP address, whatever that is.

5. When you finish, save it then apply the new configuration.
6. You'll see an indicator on your new entry showing it's linked to a rule. If you go back to the WAN firewall rules, you'll see a rule was automatically created for you. Handy!
7. Test this by navigating to the firewall in Firefox on the Fedora machine. If you see the Ubuntu web server, congrats! Take a screenshot for your submission.

## Step 5: Create more port forwarding

The Ubuntu machine is hosting another secret website on port 25565. Go through the same process of port forwarding as before, just using port 25565 instead of 80.

However, after doing this, you will notice the Fedora machine's requests to port 25565 (which will look like http://<ip-address>:25565 in the web browser) are still being rejected! This is because of that sneaky firewall rule that rejects this traffic.

Look through the firewall rules and find the problematic rule. Don't delete it; instead, change the order of the rules to prioritize the "Allow" rule generated in the port forwarding process. (Remember, rules are evaluated from top to bottom in the list.)

Once that's done, navigating to the website should work. Good work! Take a screenshot for your submission.

## Step 6: Using logs to help identify problems

Logs can be very helpful in addressing problems. OPNsense has a live view of traffic that we will use in this section to help us create the necessary port forward and rule adjustments to allow for DNS traffic from our Fedora machine to the Ubuntu machine.

On the Fedora machine run the following comand:

- nslookup nameserver.lab5.test <WAN-ip-address>

On the Ubuntu machine navigate to Firewall > Logs Files > Live View. You will see a series of red lines indicating blocked traffic. You can click on the 'i' icon on the right side of the line to pull up additional information. Using this information, create a port forwarding rule that allows this traffic to reach the Ubuntu machine. You may have to adjust the order of existing firewall rules under the WAN section.

When you've done this correctly submit screenshots of the output of the command for the following hostnames: nameserver.lab5.test and firewall.lab5.test.

On the Fedora machine run the following command:

- dig @<firewall-ip-address> lab5.test AXTR

Use the live view of the logs to identify this traffic. How is it different? Create the necessary port forward rule to allow this traffic to reach the Ubuntu machine. You may have to adjust the order of existing firewall rules under the WAN section.

When you've done this correctly submit a screenshot of the output of the command.

## Step 7: Configure VPN

Virtual Private Networks are another tool to make LAN resources available on the WAN. Luckily OPNsense has an easy setup wizard for this too. We will host an OpenVPN server to let Fedora securely join the LAN and access Ubuntu's SSH server.

These instructions are modified from the official OPNsense example for an OpenVPN SSL Road Warrior VPN. Road Warrior basically means client-based tunnel instead of site to site.

This section is more of a walkthrough because the process is somewhat complex. Take note of the things we leave default to appreciate how else you might configure a VPN, and consider skimming the OPNsense or OpenVPN documentation for more information.

1. Create an internal Certificate Authority.
    a. Navigate to System > Trust > Authorities.
    b. Click the + button to add a new one.
    c. Give it a sensible descriptive name, like "Lab 5 CA for VPN".
    d. For the Method, select "Create an internal Certificate Authority" from the dropdown.
    e. For our purposes, the cryptography settings can be left default, although you ought to change the country code to US.
    f. Make the common name "lab5-ca".
    g. Click *Save* to finish.
2. Create a Server Certificate using that CA.
    a. Navigate to System > Trust > Certificates.
    b. Click the + button to add a new one.
    c. For the Method, select "Create an internal Certificate".
    d. Give it a descriptive name, like "OpenVPN Server Cert".
    e. For the Certificate Authority, select the CA we just made.
    f. For the Type, select "Server".
    g. Leave the cryptography settings default again, although you may as well change the country code to US.
    h. Make the common name the FQDN (fully qualified domain name) of this OPNsense machine (by default it will be OPNsense.localdomain).
    i. Click *Save* to finish.
3. Create an internal user and certificate to be used for authentication.
    a. Navigate to System > Access > Users.
    b. Click the + button to add a new one.
    c. Name the user "fedorakde".
    d. Check the box to randomly generate a password, as we won't use password-based operations.
    e. For Certificate, select "Click to create a user certificate".
    f. Click *Save* to enter the certificate creation window.
    g. Select "Create an internal certificate".
    h. Here the defaults are all good, so just click *Save* again to finish.
4. Create static keys for authentication.
    a. Navigate to VPN > OpenVPN > Instances > Static Keys.

    b. Create a new one, and name it “Lab 5 static keys”
    c. Select “auth” for the mode.
    d. Click the gear button to generate the keys.
    e. Click *Save* to finish.
5. Create the actual OpenVPN server.
    a. Navigate to VPN > OpenVPN > Instances.
    b. Click + to make a new one.
    c. Give it a description “Lab 5 VPN Server”
    d. For the Port number, select 1194 (the default OpenVPN port).
    e. For Server (IPv4), give it 192.168.11.0/24
    f. For Certificate, select the server certificate we made earlier.
    g. Finally, for Local Network, enter the network ID for your LAN with the Ubuntu machine (likely 192.168.1.0/24)
    h. Click *Save* to finish.
6. Unfortunately, this process does not automatically make firewall rules, so let’s do that now.
    a. Navigate to Firewall > Rules > WAN.
    b. Add a new rule that allows UDP on port 1194 for the WAN interface.
    c. Now navigate to Firewall > Rules > OpenVPN.
    d. To keep things simple, allow all traffic by creating a rule with all the default values.
    e. Make sure to apply the changes.
7. Finally, export the client configuration.
    a. Navigate to VPN > OpenVPN > Client Export.
    b. Set the Export Type to “File Only” (to get a nice ovpn file instead of zip)
    c. Set the Hostname to the WAN address of your OPNsense machine.
    d. Scroll down and download the export for fedorakde.
8. Import the VPN profile on your Fedora desktop.
    a. Copy the contents of your client export to a file on your Fedora machine; save it with the .ovpn extension.
    b. In the network configuration, add a new connection.
    c. Choose the option to import a VPN connection from a file (at the bottom of the list)
    d. Select the file you just made.
9. Now you should be able to select this VPN connection. If it works, congrats! Test that you can reach the Ubuntu machine’s IP address.
10. Take a screenshot of the Fedora machine directly SSH’d into the Ubuntu machine.

To wrap up, take a screenshot of the final WAN firewall rules page.

## Submission

By completing the lab, you will gather the following information to submit in Learning Suite.

- Where is the setting to change the root password?
- Screenshot showing Fedora successfully pinging the firewall.
- Screenshot showing Fedora accessing the Ubuntu web server via the OPNsense WAN address (thanks to port forwarding).
- Screenshot showing Fedora accessing the secret webpage on 25565

- Screenshot of output from nslookup commands
- Screenshot of output from dig command
- Screenshot showing Fedora SSH'd directly to the Ubuntu's IP address (thanks to the VPN).
- Screenshot showing your port forwarding configuration.
- Screenshot showing your OpenVPN configuration.
- Screenshot showing the final firewall rules.