Secure Network using OPNSense®

Appendix B, Final Degree Assessment - 2020/21

Version 1.0.0 - 19/05/2021

Purpose

The purpose of this tutorial is to learn how to secure a network. A firewall's job is to filter packets, based on a set of rules it has. In its most basic form, it intercepts the traffic that goes through it, and allow or block traffic based on rules. In the tutorial, the OPNSense® firewall solution is used. It is an environment with multiple features/services that can be used to secure a network. The tutorial will guide you through most of the features that exist in the OPNSense® firewall solution.

During the period you are working on this tutorial, it is expected that you explore and experiment with the features that exist in this environment. Try to add features that are not present in this tutorial or explorer other similar environments.

OPNSense®

OPNSense®[1] is a firewall solution created by Deciso[2]. It is free to use, and it is an open-source firewall, that has features that can do the same as commercial-grade equipment. It originates from a fork from pFsense and m0n0wall in 2014. The firewall is based on HardenedBSD. Some examples of features will be firewall rules, VPN, NAT, and proxy.

If you later want to develop features, submit or find answers to issues, or support them in any other way, it can be done using their Github pages.

OPNsense Github page: https://github.com/opnsense

[1] https://opnsense.org/
[2] https://www.deciso.com/

VMware

VMWare will be used as our hypervisor for this tutorial. During the tutorial, you will be creating some virtual machines. Such as:

1. A virtual machine with OPNSense® as your firewall.
2. As your client, you will be using a virtual machine Ubuntu desktop machine. It is possible to use your host machine, but it is not recommended.
3. And at last one virtual Ubuntu server machine.

How to use

This tutorial is made modular. Each of the chapters can be used standalone as a module. It is possible to do the tutorial from the first to the last page or choose one or multiple of the different modules. If the modular approach is used, then the 2 chapter needs to be done first since it is the initial configuration of the firewall.

Questions

In this tutorial, all questions are numbered from one (1) and upward. The questions in each module are related to the topic the module contained. There are mainly two different types of questions, the first type is questions that are used to check if you have understood the topic. The second type is questions that are used to enhance your understanding of the topic and to research on your own.

In appendix A, all the questions are listed with their answer. This will make it easy if you are stuck on one or multiple questions. Not all questions will have answers since some of them are to encourage you to explore some topics.

It is highly recommended that you do as many as possible of the questions that are in each of the modules you are working on.

Learning objectives

The learning objectives depend on how the tutorial is used. But if all modules are done, you should have learned:

- To be able to use OPNSense® as a firewall.
- Configure the different features that the firewall has. The main features are:
  - Create firewall rules.
  - How to limit bandwidth.
  - How VPN works.
  - How a proxy can be used.
  - Set up an IDS (Intrusion Detection System).
  - Configure a VPN server and client.
- Use this knowledge to create a secure network.

> Writing notes during this tutorial to make it easier for you to remember what you are doing and quickly look up what you have done. This is discussed in section 1.

Additional sources

> Stubbig 2019 has a book named "Practical OPNsense". The book goes through most of the features that OPNSense® has, but the degree of detail varies during the different features. The book is directed at enterprise environment, where multiple OPNSense® firewalls are used. The book can be bought at regular bookshops or online.

> Another great source for information about the OPNsense firewall is their online documentation, found at `https://docs.opnsense.org/intro.html`

Legend

The legends will inform you about key details in the tutorial. Please follow them. Be careful when the warning legends are present, orange or red colored.

⚙ You will need to do the following configuration

💡 You may find this useful to answer the question, to get passed the current task, or just generally

☁ You will need to download something from somewhere http://somewhere.com

? You should answer this question

☢ This will take a lot of time, but you will find it useful in addition to your study

📖 This is additional reading that will support you

⊞ These instructions apply to Microsoft Windows

 These instructions apply to Apple MacOS

🐧 These instructions apply to a Linux System

🐙 Grab this project or resource from the following https://github.com/rhofset

⚠ **This is a POTENTIALLY RISKY task.**

✓ You can do this to know you are correct

❗ Do NOT do this.

Those legends are here to guide you through the tutorial.

In the tutorial, you will see something like this when you are configuring the different features: `System -> Access -> Users`. When you see something like this, it means that you go to the System menu, then to the submenu Access, and at last another sub submenu Users or a tab called Users.

Contents

Legend IV

1 Notes 1

2 Preparation 2
- 2.1 Ubuntu Desktop . . . 2
- 2.2 Ubuntu Server . . . 2
- 2.3 OPNSense® . . . 3
- 2.4 Create a virtual network in VMware . . . 3
- 2.5 The first configuration of the firewall . . . 4

3 General administration 8
- 3.1 User and Groups . . . 8
- 3.2 Login using SSH without password . . . 9
- 3.3 Password reset . . . 10
- 3.4 Get help . . . 11
- 3.5 Update, upgrade, and plugins . . . 11
- 3.6 Backup / restore of configuration . . . 11
- 3.7 Enable / disable individual rules . . . 12
- 3.8 Alias . . . 12
- 3.9 Troubleshooting . . . 13
  - 3.9.1 Ping . . . 13
  - 3.9.2 Disable all packet filtering . . . 14

4 Firewall 15
- 4.1 Firewall rules . . . 15
- 4.2 Creating first rule . . . 16
  - 4.2.1 Logging . . . 17
- 4.3 Second firewall rule . . . 17
- 4.4 Thrughput and best practice . . . 18
  - 4.4.1 Rulesets best prasctice . . . 19
- 4.5 Time-based rules . . . 19
- 4.6 Anti-spoofing . . . 19
- 4.7 Geoblocking . . . 19
- 4.8 Throubleshooting rules . . . 20

5 Network Address Translation 21
- 5.1 Outbound . . . 21
- 5.2 Port Forwarding . . . 22
- 5.3 One-to-one NAT . . . 24
- 5.4 NPTv6 . . . 24

6 Management network 25

7 Bandwidth 26
- 7.1 Queue . . . 27
- 7.2 Status . . . 27

8 VPN 28
- 8.1 OpenVPN wizard . . . 28

8.2 Client setup . . . 30
8.2.1 Export user certificate and configuration . . . 30
8.2.2 Firewall rule for VPN clients . . . 31
8.2.3 Configure the client . . . 32

9 Web proxy **33**
9.1 Enable proxy service on the firewall . . . 33
9.2 Browser settings . . . 34
9.3 URL filtering with proxy . . . 34
9.4 Category filtering . . . 35
9.5 Proxy logs . . . 37
9.6 SSL inspection . . . 37
9.6.1 Create Certificate Authority . . . 38
9.6.2 Firewall configuration . . . 38
9.6.3 Client configuration . . . 38
9.6.4 Test . . . 39

10 Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) **40**
10.1 Enable IDS . . . 40
10.2 Setup IDS rule . . . 40
10.3 Setup the IPS . . . 41
10.4 Disabling/removing rules . . . 42

11 Domain Name System (DNS) **44**

12 Dynamic Host Configuration Protocol (DHCP) **46**
12.1 DHCP . . . 46

13 Routing **47**

14 Reporting **48**
14.1 NetFlow and Insight . . . 48

Resources **50**

A Questions and Answers **51**

References **54**

CHANGELOG

- v1.0.0 - Initial Release - 19/05/2021 Runar Hofset

1 Notes

It is recommended that you make notes during the tutorial. This will improve what you remember after the tutorial, and it can be used as an encyclopedia later in your studies or career. When you are making notes, you are forcing your brain to think about what you are writing, and therefore you will improve your learning outcomes. How to make notes is up to you, but some tips can be:

- Make notes about what **you** think is important.
- Make notes about how you configured features/services.
- Make notes about settings you are using that could be important later. For example, IP addresses, passwords.
- Make notes about thoughts that you get during the tutorial.
- Always use the same format on your notes.

If you have trouble making notes during the tutorial, create a note with keywords and rewrite it to something you understand when you have finished with the task.

The notes can be done using pen and paper or using electronic aids such as a computer or an electronic pad. Some examples of computer tools that can help you with this are, for example, Endnote[3], Obsidian[4], Joplin[5], or OneNote[6].

⚠ If you decide to use some of the tools listed for your notes, you are on your own. This tutorial will not provide guidance for them. If you get problems with them, check the vendor's page or use google to see if other persons have had the same problem.

? 1. How do you think making notes during the tutorial will benefit you?

[3] https://endnote.com/
[4] https://obsidian.md/
[5] https://joplinapp.org/
[6] https://www.microsoft.com/nb-no/microsoft-365/onenote/digital-note-taking-app

2 Preparation

Before you start with the tutorial, it is important that the lab environment is configured. This section will guide you through the configuration. In this section, you will learn to install and configure the basics of:

- Configure the OPNSense® firewall using the VMware hypervisor.
- Create a virtual network in VMware.
- Install an extra network interface on the hypervisor that runs the OPNSense® firewall.

> There could be newer versions of the operating systems than being used in this tutorial. If another version is downloaded and used, it will in most cases, not impact the tutorial. If problems are encountered, change to the version used in this tutorial

Prerequisites

Make sure that you have installed VMWare before you start on this task. As a Noroff student, you can log in and download VMWare from www.onthehub.com. You should have received a link with information about this earlier. How to install VMWare is not included in this tutorial. VMWare has a tutorial that can be used: https://kb.vmware.com/s/article/2053973

> **If you want to use a different client or virtual hypervisors, you are on your own!**

There is expected that you know how to create and deploy a virtual server, so the creation of the Ubuntu machines is not covered in this tutorial. The OPNSense® firewall has some additional configurations that need to be done, so the installation and configuration are detailed.

2.1 Ubuntu Desktop

> The latest version of Ubuntu Desktop can be found at: https://ubuntu.com/download/desktop.

The version that is used in this tutorial is `Ubuntu 20.04.2.0 LTS`

If you need any help during the process of installing the Ubuntu Desktop, find a tutorial online that you can use. For example; https://linuxhint.com/install_ubuntu_vmware_workstation/. Or you could ask one of your fellow students or ask on Teams.

2.2 Ubuntu Server

> The latest version of Ubuntu Server can be found at: https://ubuntu.com/download/server.

The version that is used in this tutorial is `Ubuntu Server 20.04.2 LTS`

If you need any help during the process of installing the Ubuntu Server, find a tutorial online that you can use. For example; https://blog.eldernode.com/install-ubuntu-20-04-lts-server-on-vmware/. Or you could ask one of your fellow students or ask on Teams.

2.3 OPNSense®

Download OPNSense® from https://opnsense.org/download/. Chose amd64 architecture, dvd as the image type. The chosen location to download from does not matter, but normally a location that is close to your location is the fastest one when downloading.

Start with downloading the file and follow the configuration below:

1. Go to https://opnsense.org/download/ and chose the different options. The download page should look something like figure 1 now. The checksum (hash) will be different than in the figure.
2. Before clicking on Download button, make sure to make a note with the SHA256 hash.
3. The file you are downloading has a name similar to this: `OPNsense-20.7-OpenSSL-dvd-amd64.iso.bz2`.
4. Check if your file has the same SHA256 hash as the one provided to you on the download page. Depending on what OS you are using, there are multiple methods to find the SHA256 hash of the file. Examples for Linux and Windows below:
   - Linux: `sha256sum <Your OPNsense iso file>`
   - Windows: `certutil -hashfile <Your OPNsense iso file> SHA256`
5. When the download is finished, extract the iso file from the compressed archive. You should now have a `.iso` file.

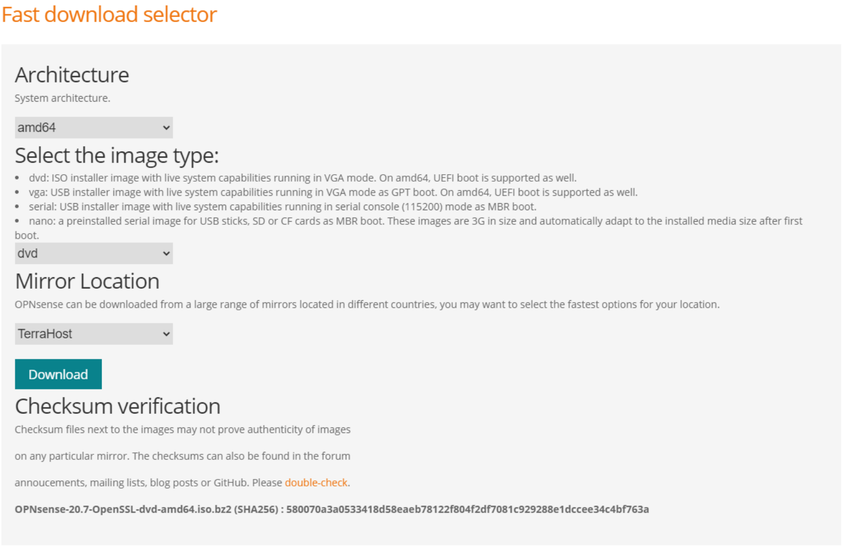
Using hashes to verify the authenticity of the file is important. Also, do this for the Ubunto iso files you downloaded.

Do not extract the .iso file. If it is extracted, it will not work properly.

2. What is a hash?
3. Did your hash values match?

2.4 Create a virtual network in VMware

Now you can start to configure a virtual network in VMWare. This is important since all the clients we are creating must be in the same network.


Fast download selector

Architecture

System architecture.

amd64

Select the image type:

- dvd: ISO installer image with live system capabilities running in VGA mode. On amd64, UEFI boot is supported as well.
- vga: USB installer image with live system capabilities running in VGA mode as GPT boot. On amd64, UEFI boot is supported as well.
- serial: USB installer image with live system capabilities running in serial console (115200) mode as MBR boot.
- nano: a preinstalled serial image for USB sticks, SD or CF cards as MBR boot. These images are 3G in size and automatically adapt to the installed media size after first boot.

dvd

Mirror Location

OPNsense can be downloaded from a large range of mirrors located in different countries, you may want to select the fastest options for your location.

TerraHost

Checksum verification

Checksum files next to the images may not prove authenticity of images

on any particular mirror. The checksums can also be found in the forum

annoucements, mailing lists, blog posts or GitHub. Please double-check.

OPNsense-20.7-OpenSSL-dvd-amd64.iso.bz2 (SHA256) : 580070a3a0533418d58eaeb78122f804f2df7081c929288e1dccee34c4bf763a

Figure 1: An example of the download page for OPNSense®

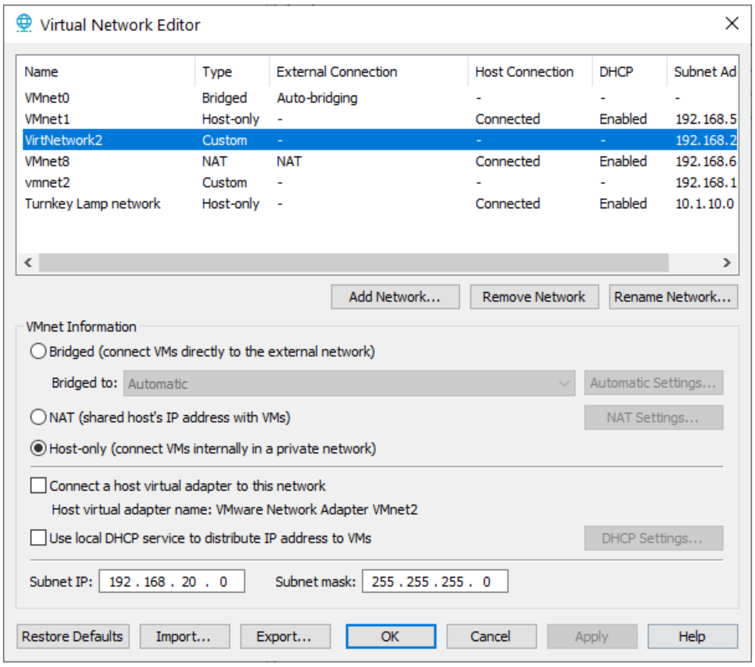
1. In VMWare go to `Edit` and click on `Virtual Network Editor`.
2. Click on `Add Network`. Name it **VirtNetwork2**.
3. Make sure it is a `Host-Only` network.
4. Deselect this two options if they are selected:
   - `Connect a host virtual adapter to this network`.
   - `Use local DHCP service to distribute IP address to VMs`.
5. Set the IP you want and the subnet mask of 255.255.255.0 (CIDR \24). This is the subnet we are using as our LAN network later. It does not matter what you are using as IP here, but in this tutorial we are using 192.168.20.0. If you use a different IP, write it down in your notes.
6. The result should look something like figure 2 now.
7. Click `OK` to save.

Remember to add the two Ubuntu clients to the virtual network you have created here.

4. Why do you create a virtual network?

2.5 The first configuration of the firewall

The next step is to create your virtual machine. During the creation, you need to add another network interface to the firewall. This network interface will be your WAN interface later on:



Virtual Network Editor

Name	Type	External Connection	Host Connection	DHCP	Subnet Ad
VMnet0	Bridged	Auto-bridging	-	-	-
VMnet1	Host-only	-	Connected	Enabled	192.168.5
VirtNetwork2	Custom	-	-	-	192.168.2
VMnet8	NAT	NAT	Connected	Enabled	192.168.6
vmnet2	Custom	-	-	-	192.168.1
Turnkey Lamp network	Host-only	-	Connected	Enabled	10.1.10.0

VMnet Information

○ Bridged (connect VMs directly to the external network)

Bridged to: Automatic

○ NAT (shared host's IP address with VMs)

● Host-only (connect VMs internally in a private network)

□ Connect a host virtual adapter to this network

Host virtual adapter name: VMware Network Adapter VMnet2

□ Use local DHCP service to distribute IP address to VMs

Subnet IP: 192 . 168 . 20 . 0 Subnet mask: 255 . 255 . 255 . 0

Figure 2: VMWare virtual network configuration

1. Start VMWare.
2. Go to File and click on New Virtual machine.
3. Choose Typical and click Next.
4. Chose Installer disk image-file (iso) and point to the .iso file you downloaded earlier. Click Next.
5. Set a name for the virtual machine and chose where you want to store it. Recommend that you are using an SSD or faster storage for it. Click Next.
6. The default values for storage capacity are OK for this tutorial. Click Next.
7. Click on Customize Hardware, and do this:
8. (a) Set memory to 1024 MB.
   (b) Processors to 1.
   (c) Set network adapter to your custom virtual network created earlier.
   (d) Click on the Add button and add a new Network Adapter. Set this adapter to bridged. This will be your WAN connection later in this tutorial.
9. Click Close, and Finish.

You are now ready to start your virtual firewall for the first time. Start your virtual machine with OPNSense®.

1. If the boot process was without errors, you should have heard a sound.
2. Check that your `em0` is LAN and `em1` is WAN. At this moment, do not panic if your LAN IP is not correct, it will be fixed later.
3. Use the username `installer` and the password `opnsense` to start the installing process.
4. Accept all default values in the setup wizard. Leve root password blank, then it will be the password we provided when we logged in as installer.
5. When asked for a reboot, do it.
6. When the reboot is done, you will see that the LAN IP is 192.168.1.1. This is always the default IP for OPNSense®.
7. Now we are leaving the OPNSense® virtual machine running, do not turn it off.
8. Start your Ubuntu Desktop and navigate to 192.168.1.1 using a browser. Like figure 3.
9. Use the username and password you got, to log in. (the username: root and the password: opnsense)
10. The setup wizard will start automatically.

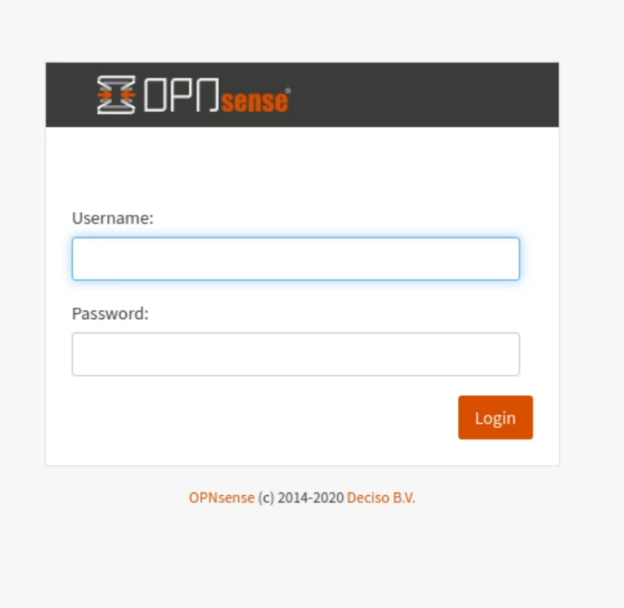


Figure 3: OPNSense® login screen

Configuration using the wizard:

1. Click Next when the wizard starts.
2. Insert Primary and Secondary DNS servers. You can use the IPs for google's DNS. (8.8.8.8 and 8.8.4.4). Click Next. Read more about DNS in chapter 11.
3. Set your timezone. Most likely to Europe/Oslo. Click Next.
4. Remove the checkmark at RFC1918 Networks. Click Next.
5. Change the LAN IP to 192.168.20.1. (This will be your IP to OPNSense® from your virtual network (LAN)). Click Next.
6. Let the password be empty. (You then keep the password you created earlier). Click Next.
7. Click Reload.
8. Go to 192.168.20.1, login, and you are welcomed with the dashboard of OPNSense®.

If you have problems connecting to your OPNSense® firewall via the browser after the reload, check your clients IP settings

5. What does the em in the network card stand for?
6. Why did you remove the checkmark for RFC1918 Networks?
7. Can you ping your firewall from your client?

3 General administration

In this chapter, there is mostly reading. There are some questions that can be useful to answer. This chapter contains information about:

- Adding a user.
- Adding a user to a group.
- Connecting using SSH without a password.
- How to reset your password.
- How to get a short description of what options does.
- How to update/upgrade your firewall.
- How to create a backup or restore a configuration.
- Enable/disable individual rules.
- Create an alias.
- Use the `PING` command from the firewall interface.
- Disable all packet filtering.

Use it as an encyclopedia if you get stuck on some of the topics in this chapter.

3.1 User and Groups

You can add users, and users can be added to a group. A normal security strategy is that a user only has access to their level of usage. Therefore you should not use a root account if you do not need to have root access to what you are doing. With that said, you will need a root account to perform the configurations that we are going to do in this tutorial.

If you need to create users, follow the configuration below:

1. Go to `System -> Access -> Users`.
2. Click `Add` to create a new user.
3. Set `Username` and `Password` for the user.
4. Set the `Full name` and `Email` for the user.
5. Set the `Expiration date` for the user. If this field is `blank`, the user will never expire. This should be avoided. When date is set, it uses the format: `mm/dd/yyyy`.
6. Configure `Group Memberships`. If groups do not exist, go to the next configuration below.
7. Click the checkbox `Certification` if a user certificate should be created.
8. If any authentication method other than username and a password is going to be used, insert the keys that should be used or create an internal certificate. (`OTP seed`, `Authorized keys` (section 3.2) or `IPsec Pre-Shared Key`)

If you need to create groups, follow the configuration below:

1. Go to `System -> Access -> Groups`.
2. Click `Add` to create a new group.
3. Give the new group a name and a description.
4. Move user(s) to the group in the `Group memberships` part of the configuration.

3.2 Login using SSH without password

OPNSense® comes with an OpenSSH server as default after you have set it up. The first step is to create a key pair for your client. When creating a key pair it is important to choose the correct key size. NIST (National Institute of Standards and Technology) is recommending at least 2048 bit as a minimum (Barker and Dang 2015).

Follow the instructions below depending on what operating system you are using as your client:

1. Check if the SSH client is installed using the command `ssh`. If it is successful, you will get a message with the different options you can use. If you do not have it installed, install it using the command `sudo apt install openssh-client`.
2. `ssh-keygen -t rsa -b 4096` to create the key-pair. When prompt, input your password and where you want to save it.
3. Go to the common step below.

1. Check if you have the SSH client on your system using the command `ssh`. If it is successful you will get a message with the different options you can use. If you do not have it installed, install it via the add/remove windows functions or use the Windows Store.
2. `ssh-keygen -b 4096` to create the key-pair. When prompt, input your password and where you want to save it.
3. Go to the common step below the Linux step.

The next step is to get your public key to the OPNSense® firewall.

Common step:

1. Go to your OPNSense® web GUI and `System -> Access -> Users`.
2. Click on the edit button (a pencil on the right side of the user name) and add your public key in the `Authorized keys`. Make sure your public key is on one line.
3. Test from your client if you can log in using passwordless SSH.

If you get problems adding the ssh key, make sure the key is on one line.

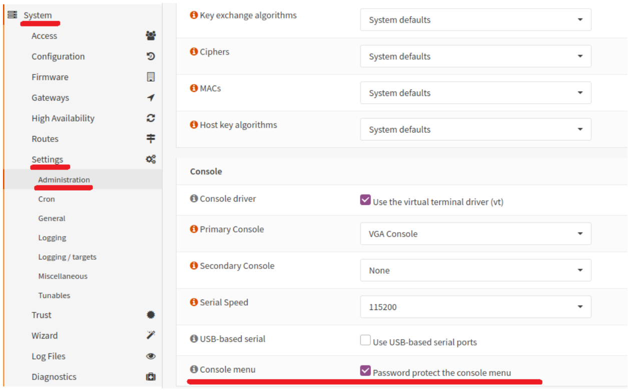
?

8. What is key-size?
9. What is the difference between a private key and a public key?

3.3 Password reset

There are three different methods that can be used depending on if the `Password protect the console menu` is set in `System -> Settings -> Administration` in the web GUI (Graphical User Interface) (figure 4) or if you have access to the web GUI at all.

- Method one can be used when you have access to the web GUI.
- Method two is only going to work if the `Password protect the console menu` checkbox is not checked and you do not have access to the web GUI.
- Method three is only going to work if the `Password protect the console menu` checkbox is checked.



Key exchange algorithms: System defaults
Ciphers: System defaults
MACs: System defaults
Host key algorithms: System defaults

Console

Console driver: ☑ Use the virtual terminal driver (vt)
Primary Console: VGA Console
Secondary Console: None
Serial Speed: 115200
USB-based serial: ☐ Use USB-based serial ports
Console menu: ☑ Password protect the console menu

Figure 4: OPNSense® Password protect the console menu checkbox

Method 1:

Using the web GUI, go to `Lobby -> Password`, enter your new password, retype (confirm) it and click on `Save` to confirm, and set the new password.

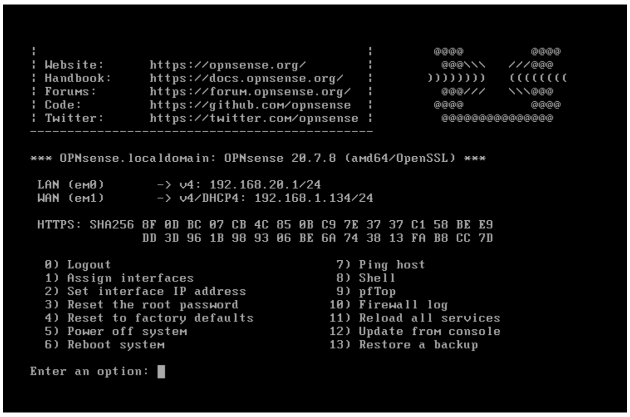
Method 2:

!

Method two is only going to work if the checkbox `Password protect the console menu` is not checked and you do not have access to web GUI. If you do not know, if the `Password protect the console menu` is checked, go to method 3.3 instead.

Start your OPNSense® firewall and wait for it to start completely. Then login[7] using the CLI. After you have logged in, you should see a screen similar to figure 5. Choose option 3, and change your password.

[7] root:opnsense (Username and password if you did not change it)



```
 |                                              |        @@@@          @@@@
 | Website:      https://opnsense.org/          |         @@@\\\     ///@@@
 | Handbook:     https://docs.opnsense.org/     |       ))))))))   ((((((((
 | Forums:       https://forum.opnsense.org/    |         @@@///     \\\@@@
 | Code:         https://github.com/opnsense    |        @@@@          @@@@
 | Twitter:      https://twitter.com/opnsense   |         @@@@@@@@@@@@@@@@
 ----------------------------------------------

*** OPNsense.localdomain: OPNsense 20.7.8 (amd64/OpenSSL) ***

 LAN (em0)       -> v4: 192.168.20.1/24
 WAN (em1)       -> v4/DHCP4: 192.168.1.134/24

 HTTPS: SHA256 8F 0D BC 07 CB 4C 85 0B C9 7E 37 37 C1 58 BE E9
               DD 3D 96 1B 98 93 06 BE 6A 74 38 13 FA B8 CC 7D

  0) Logout                              7) Ping host
  1) Assign interfaces                   8) Shell
  2) Set interface IP address            9) pfTop
  3) Reset the root password            10) Firewall log
  4) Reset to factory defaults          11) Reload all services
  5) Power off system                   12) Update from console
  6) Reboot system                      13) Restore a backup

Enter an option: █
```

Figure 5: OPNSense® login screen CLI

Method 3:

1. Reboot and when the boot menu is displayed after the reboot, choose the `Boot Single User` option.
2. You are now presented with a CLI with the question: `Enter full pathname of shell or RETURN for /bin/sh`. Hit the ENTER key to get the default shell.
3. Mount the disk using the command `mount -o rw /`
4. Write this file path in your shell: `/usr/local/opnsense/scripts/shell/password.php`. This will ask if you want to continue and answer with the command `y`.
5. Type your new password twice when asked for it.
6. Reboot
7. Log in as normal using your new password. The new password will work in CLI, SSH and, via the web portal.

10. What does the `Password protect the console menu` checkbox in `System -> Settings -> Administration` in the web GUI do?

3.4 Get help

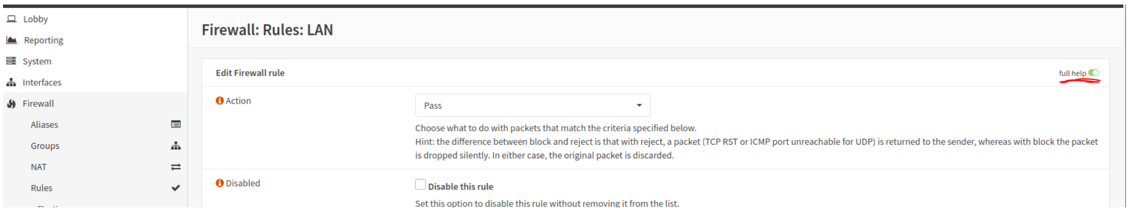
Many of the variables/options that can be set during your work with OPNSense® have a short description that can help you to understand better what it does. If it exists, there will be an icon in the right top corner, below the search bar, that can be clicked. It is activated when it has a green colour. This can be seen in figure 6.

3.5 Update, upgrade, and plugins

In `System --> Firmware` it is possible to update and upgrade the different packages, plugins, and the firmware itself. This is also the place where new plugins are installed from.

3.6 Backup / restore of configuration

Backup and restore is done in the menu: `System --> Configuration --> Backups`. To download the backup configuration file, click on the `Download configuration` button and save it to your disk. And when



Firewall: Rules: LAN

Edit Firewall rule

Action: Pass

Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled: □ Disable this rule

Set this option to disable this rule without removing it from the list.

Figure 6: OPNSense® Help

restoring the configuration, click on the `Restore configuration` button and choose the configuration file you want to use.

When downloading a configuration file, there is a checkbox option to protect it from unauthorized usage. And the same exist for restoring an encrypted configuration file.

> Please, make backups of your configuration before you are starting with another topic in this tutorial. It will make it is easy to restore to an earlier point that you know is working.

3.7 Enable / disable individual rules

Most rules have a checkbox that can be used to enable the rule (see figure 7). If it has a checkmark, it is enabled.

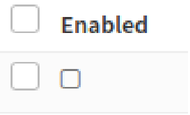


Figure 7: Enable / disable rules

3.8 Alias

An alias is used for items that are bundled together using one name. An alias can, for example, contain off hosts, networks, or ports (for the full list, see table 1). The main reason for the usage of aliases is to make, for example, the list of firewall rules easier to read. If the aliases are used, one rule can be used for something that affects multiple hosts. To create an alias:

1. Go to `Firewall --> Aliases`.
2. Click the `+` button on the right side of the screen.
3. Give the alias a name in the `Name` field.
4. Chose the type you want to use.
5. And the `Content` field is where you type in, for example, the IP, hostname, or port.
6. Give the alias a description in the `Description` field.

> The character `!` can be used to exclude items from an alias.

Type:	Description:
Hosts	IP or FQDN (Fully Qualified Domain Name).
Networks	A network range with CIDR added at the end.
Ports	Port number or port range (divided with a :).
MAC addresses	Partial or full mac address.
URL (IPs)	one or multiple IPs.
URL Tables (IPs)	one or multiple IPs.
GeoIP	Country or region.
Network group	A combination of different types.
External (advanced)	Alias that is managed externally.

Table 1: Full list of what an alias can consist of

3.9 Troubleshooting

In this section, there are some troubleshooting tips and tricks that you can use if you get problems. In the `Interfaces --> Diagnostics` menu, there are multiple tools that can be used to find an error during troubleshooting. In the following bullet point list, there is a short overview of the different tools and what they can be used for.

- ARP table - The ARP table (Address Resolution Protocol) is a table over all known network IP's and MAC (Media Access Control) addresses that are connected to the firewall.
- DNS lookup - Can resolve IPs or hostnames to a domain.
- NDP table - The NDP (Neighbor Discovery Protocol) table shows addresses that are learned for IPv6.
- Netstat - Shows status information about interfaces, protocol, sockets, netisr, memory, and bpf.
  - Interfaces - Contains information about each interface. This could be both physical or virtual interfaces. Metrics shown is number of packets, bytes sent/recived.
  - Protocol - Contains statistical information for multiple protocols. Examples of statistics it show is number of tcp listening connections, sent packets, duplicate packets, etc, etc.
  - Sockets - Combines the `netstat`[8] with `sockstat`[9] in FreeBSD and produce statistics about processes that are listening.
  - Netisr - Show statistics from the kernel network dispatch service, known as `netisr(9)`[10].
  - Memory - Shows information from the memory management routines (`mbuf(9)`[11]).
  - Bpf - Shows statistics from `bpf(4)`[12].
- Packet Capture - See section 3.9.2
- Ping - See section 3.9.1
- Port Probe - Can be used to test if a port is open.
- Trace Route - Can be used to follow a route. Lists all the IPs in the route.

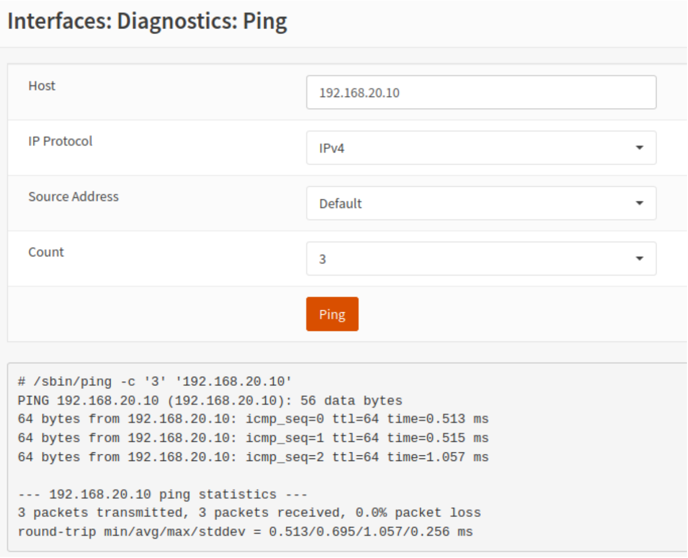
3.9.1 Ping

The `ping` command is very useful when you are trying to find errors in your network setup. To use the ping command, follow the instructions below:

[8] https://www.freebsd.org/cgi/man.cgi?query=netstat&sektion=1
[9] https://www.freebsd.org/cgi/man.cgi?query=sockstat&sektion=1&format=html
[10] https://www.freebsd.org/cgi/man.cgi?format=html&query=netisr(9)
[11] https://www.freebsd.org/cgi/man.cgi?query=mbuf&sektion=9&format=html
[12] https://www.freebsd.org/cgi/man.cgi?bpf(4)

1. Go to `Interface --> Diagnostics --> Ping`.
2. Set `Host` to the address (or IP) you want to ping.
3. Set `Source Address` to the interface that should be used.
4. Set `Count` to how many ping requests you want to send.

11. Try to ping your client. Do you get something similar to figure 8?


Interfaces: Diagnostics: Ping

Host: 192.168.20.10

IP Protocol: IPv4

Source Address: Default

Count: 3

```
# /sbin/ping -c '3' '192.168.20.10'
PING 192.168.20.10 (192.168.20.10): 56 data bytes
64 bytes from 192.168.20.10: icmp_seq=0 ttl=64 time=0.513 ms
64 bytes from 192.168.20.10: icmp_seq=1 ttl=64 time=0.515 ms
64 bytes from 192.168.20.10: icmp_seq=2 ttl=64 time=1.057 ms

--- 192.168.20.10 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.513/0.695/1.057/0.256 ms
```

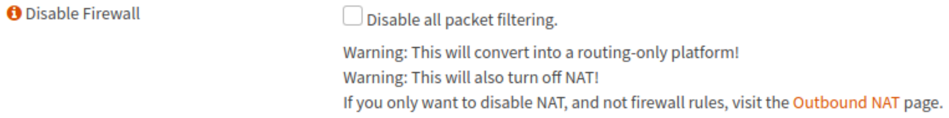
Figure 8: `ping` command

3.9.2 Disable all packet filtering

Another feature that could help you during troubleshooting is to disable packet filtering temporarily.

This will allow everything through your firewall. Be careful if you choose to do this in a production environment! Remember to enablethis feature when you are done with troubleshooting.

1. Go to `Firewall --> Settings --> Advanced`.
2. Scroll down and find `Disable Firewall`, figure 9.
3. Click the checkmark and the `Save` button at the bottom.



ℹ Disable Firewall

□ Disable all packet filtering.

Warning: This will convert into a routing-only platform!
Warning: This will also turn off NAT!
If you only want to disable NAT, and not firewall rules, visit the Outbound NAT page.

Figure 9: Disable Firewall

4 Firewall

There are different types of firewall, depending on what their job is. In this tutorial, you will be exposed to a firewall that is placed in a network. The firewall's job is to filter packets that are travelling through it and decide what should be done with the packets. More on that in the next section.

In this tutorial, you will be working with the OPNSense® firewall. It is an open-source firewall solution that is developed by Deciso. A firewall can have other functions in a network than just filtering packets. Such jobs could be as a proxy server or a VPN server. The OPNSense® firewall that you are going to work with within this tutorial, contains a lot of different features. For an overview of the features, go to https://www.deciso.com/short-introduction-opnsense/.

In this section, you will learn to:

- Configure firewall rules.
- Logging of firewall rules.
- Best practice to achieve good throughput
- Create rules based on a time schedule.
- Geoblocking.
- And some tips and tricks regarding troubleshooting

4.1 Firewall rules

To go to the firewall rules, click on the `Firewall --> Rules` and then on the network interface you want the rules to apply (figure 10). In this case, rules can be applied to four different interfaces:

- Floating - Rules that apply for all interfaces, and will be matched before any of the other interfaces, if the `Quick` checkbox is checked. Also, the only interface that allows `outbound` rules.
- LAN - Your internal pointing interface.
- Loopback - A interface that is used to communicate with the host (itself).
- WAN - Your external pointing interface.

When OPNSense® is processing rules, it is using the first rule it gets a match in. This is called the "first match principle". The rules are checked from the top of the list to the bottom. The basic rule for firewall ruleset is that the rule is acting one interface and filtering packets in the inbound direction. If you want to match in the outgoing direction or on multiple interfaces, floating rules need to be used.

OPNSense® is a stateful firewall. This means that the firewall is remembering information about the outgoing packets and are automatically allowing the response from those packets back into the client that sent it.

When creating rules in OPNSense® three different types of actions can be done:

- Pass - Allow the request.
- Block - Deny the request, but silently discards the request. Mostly used when you want the network to not know that the request has been denied, such as traffic from the internet.
- Reject - Deny the request, also discards the request, but lets the sender know it is discarded. Mostly used on requests from the internal network.

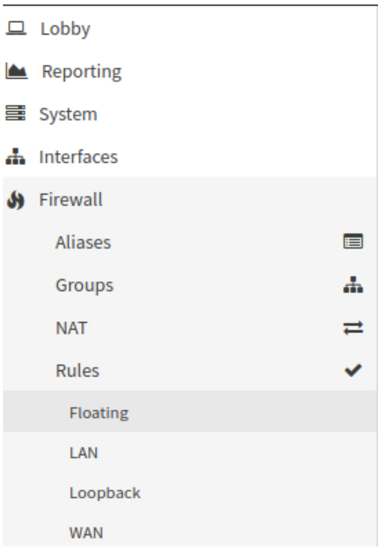


Figure 10: OPNSense® Firewall

12. Why do you think the action `Reject` is mostly used on so-called friendly networks?

4.2 Creating first rule

You are now set to create the first rule in the firewall. Follow the instructions below.

1. First step is to start your Ubuntu Server that was created earlier in section 2.2.
2. Make sure that the network in VMWare is set correct for the Ubuntu Server. Set to the virtual network that was created earlier.
3. Use the Ubuntu Desktop and try to `PING` the Ubuntu Server. Continue if you can ping it.
4. Ping any website that are online. If this works, continue.
5. Goto `Firewall --> Rules --> LAN` and click on `Add`.
6. Change the following settings:
   (a) `Action` to `Block`
   (b) `TCP/IP Version` to `IPv4`
   (c) `Direction` to `In`
   (d) `Source` to `Single host or Network` and the IP below to the IP address that your Ubuntu Server has, and the correct CIDR (Classless Inter-Domain Routing).
   (e) Click the box next to `Log` to log the rule.
   (f) In the `Descripion` box, write what this rule is. For example, "Block ¡IP¿ from internet access."
   (g) Click `Save` at the bottom and apply the rule when asked.

13. Try now to `PING` the same website as you did in bullet point 4. What is happening?
14. How can you disable the rule that was created?
15. Are you able to ping any website from the Ubuntu Server when the rule is disabled?

To stop the `PING` command, use the keyboard keys `CTRL-C` to stop it, or use the option `-c 3` to ping the server 3 times.

Play around with the different settings and try to understand how the rules are created.

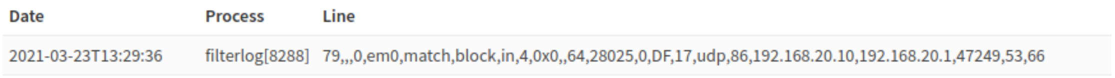
4.2.1 Logging

Each of the rules can be logged. To log a rule, click on the `Log packets that are handled by this rule` to add the rule to the logs. The best practice is to use logging only on critical rules, such as anti-spoofing or critical segments of the network, like a DMZ. Turn logging on and off after what the user needs. For example, logging is great for troubleshooting.

Be aware that the logs can fill up fast when this is applied and the rule is handling a lot of traffic.

There are three different ways to see the information from the logs. The first one is `Live view`. This is showing the user a live view of the log entries. When a new entry is made, it will appear at the top, and the one at the bottom will go to the next page in the log. This happens in real-time. The second view is the `Overview`. This is a more graphical presentation of what is going on in the logs. The last view is the `Plain view`. This is more like a command line like view.

An example can be seen in figure 11. First is the Data, then the process that wrote the entry. Under the `Line` column, there is a lot of information. Some of them are which interface is used (em0), the reason for the log entry (match), what the rule did (block), the direction of communication (in) and the protocol and IP source and destination.



Date	Process	Line
2021-03-23T13:29:36	filterlog[8288]	79,,,0,em0,match,block,in,4,0x0,,64,28025,0,DF,17,udp,86,192.168.20.10,192.168.20.1,47249,53,66

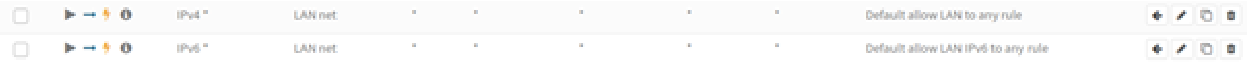
Figure 11: OPNSense® Firewall log; Plain view

16. Do you see any evidence in the log when the first rule that was created earlier is active?

4.3 Second firewall rule

For this second rule, the goal is to block all LAN traffic and allow connection to the Ubuntu Server using the 8080 port. First, we are disabling the two default rules that allow all LAN traffic.

1. Go to `Firewall --> Rules --> LAN`.
2. Click on the green right arrow for both default allow LAN to any rules (IPv4 and IPv6). When this is done, the rules should look like figure 12, the arrows greyed out.
3. Click on `Add` to add a rule.
4. Change the following settings:
   (a) `Action` to `Pass`
   (b) `TCP/IP Version` to `IPv4`
   (c) `Direction` to `In`
   (d) `Source` to `Single host or Network` and the IP below to the IP address that your Ubuntu Server has, and the correct CIDR (Classless Inter-Domain Routing).
   (e) Click the box next to `Log` to log the rule.
   (f) In the `Descripion` box, write what this rule is. For example, "Allow <IP>to use port 8080."
   (g) `Source port range` to `other` and from port `8080` to port `8080`.
   (h) `Destination` to `Any`
   (i) `Destination port range` to `any`.
   (j) Make a checkmark in the checkbox beside `Log`.
   (k) Click `Save` at the bottom and apply the rule when asked.



□	IPv4 *	LAN net	*	*	*	*	*	Default allow LAN to any rule
□	IPv6 *	LAN net	*	*	*	*	*	Default allow LAN IPv6 to any rule

Figure 12: Default allow LAN rules disabled

17. How can you test if this is working?
18. Play around and try to create other rules.

Remember to enable the two default allow rules before continuing with the tutorial

If you have problems when testing the rule that was created, try to restart the service used for testing purposes on the Ubuntu Server after each time the rule is enabled/disabled.

4.4 Thrughput and best practice

Some basic rules to keep the ruleset as close to best practice as possible (Stubbig 2019) regarding throughput.

- Keep it simple - Do not make it complicated. Complicated rules are only working until the next time you change something.
- Documentation - Document rules. Each rules has an `description` field.
- Aliases - Merge everything that has the same rules into groups.
- Use source network - If the rule allows traffic, choose the source network. If the rule is denying traffic, choose any as the source.

- IPv4 and IPv6 - It is possible to use one rule for both. Remember to add both the IPv4 and IPv6 address to aliases if it is used.
- Use inbound rules - It is possible to use inbound and outbound rules, but the best practice is to use inbound rules. An outbound rule can be created using the floating rule.
- Audit - Audit regularly. Goto `Firewall --> Diagnostics --> pfInfo` to see statistics about each rule. Assess if rules that are not used, should be removed.

4.4.1 Rulesets best prasctice

To make the rulesets as effective as possible, use this as a guideline for how to implement a strategy of which rules should be first in the hierarchy (which rule is matched first):

1. Anti-spoofing rules - block bogus addresses. See section 4.6.
2. Special rules - Rules that are specific for IP's, and ports.
3. General rules - Rules that are for networks and/or ports.
4. Cleanup rules - A rule to clean up events that should not be in a log.
5. Final-deny-any-log - Block everything that is left and log anything that hit this rule.

4.5 Time-based rules

In `Firewall --> Settings --> Schedule` there can be configured schedules that are based on time and day. Those schedules can be added to any firewall rule. This can be smart, for example, if a company is blocking specific pages during periods of the day to minimize the load on the outgoing network.

19. Where in the rule editor page can you add the time-based rule?
20. Try to create a schedule and add it to a rule that blocks access to `www.nrk.no` inside the normal working hours (08.00 - 16.00).

4.6 Anti-spoofing

As standard, the OPNSense® firewall can detect a spoofed IP from network adapters. It creates a hidden rule that detects and blocks incoming traffic, where the source IP belongs to some of the other adapters.

If the firewall has multiple networks to an adapter, a rule needs to be created to block spoofed IP's. First, create an alias with all of the networks that are behind the adapter. Then create a rule that blocks all traffic from the alias that was created, but inverted. This will deny all incoming traffic on that alias that does not originate from the alias.

4.7 Geoblocking

The geo blocking feature in OPNSense® is using the MaxMind GeoIP database. So the first step is to create an account for it:

1. Go to `https://www.maxmind.com/en/geolite2/signup` and sign up.
2. Log in on your account and find the `My License Key` link and generate the license key.
3. To create a link, replace `My_License_key` with the license key you generated in the previous step in `https://download.maxmind.com/app/geoip_download?edition_id=GeoLite2-Country-CSV&license_key=My_License_key&suffix=zip`.
4. Goto `Firewall --> Aliases` and choose the `GeoIP Settings` tab.
5. In the `Url` insert the link you created in step 3, and click `Apply` to finish.

Now the connection to MaxMind GeoIP database is finished. The next step is to greate an alias that is using it.

1. Go to `Firewall --> Aliases`. Click the `+` sign to add a new alias.
2. Set the `Name` to the something that describes what it does. For example, `block <countryname>`
3. Set `Type` to `GeoIP`
4. Choose the country you want to block.
5. Set the `Description` to something that describes what it do. In this case to the same as the `Name` could be great.
6. Click `Save` to exit and save the alias.

The alias is made and the last step is to create a rule in the firewall that is blocking that alias.

21. Can you create a firewall rule that uses the alias you created to block one country?
22. How can you test if the previous create rule is working?

Remember that the order of the rules matter. If you, for example, want to access one website from the country that you are blocking, the allow rule needs to be before the block rule.

4.8 Throubleshooting rules

If a rule is not behaving as expected, the steps below can help you to figure out what is happening:

1. Check the logic of your rules. Check if it is using the correct interface, ports, IP, protocols, and so on.
2. Are the rules in the correct order? Rules are processed from the top to the bottom.
3. Floating rules are processed before other firewall rules. Check if some of them are hindering your new rule.
4. Does NAT (Native Translation Protocol) modify packets?
5. Is the routing done correctly?
6. Check the logs to check what is going on.

23. Is it possible to do a packet capture with OPNSense®?

5 Network Address Translation

NAT (Network Address Translation) can be explained as a part of the firewall that modifies packets so it reaches a specific address in a local network. This is the method that is used when you only have one IP on your WAN interface and all of the local IPs can communicate via that IP to the rest of the world. Most often, NAT is also changing the port numbers.

Learning objectives for this module:

- How NAT is implemented.
- Port forwarding.
- NAT and IPv6.

In OPNSense® there are four different settings/types of NAT that can be changed. Going through some of them in the next chapters. Use the menu; `Firewall --> NAT` to access the different types. The different types that OPNSense® offers is, outbound, port forwarding, one-to-one, and NPTv6. The two last ones are not explained in this tutorial.

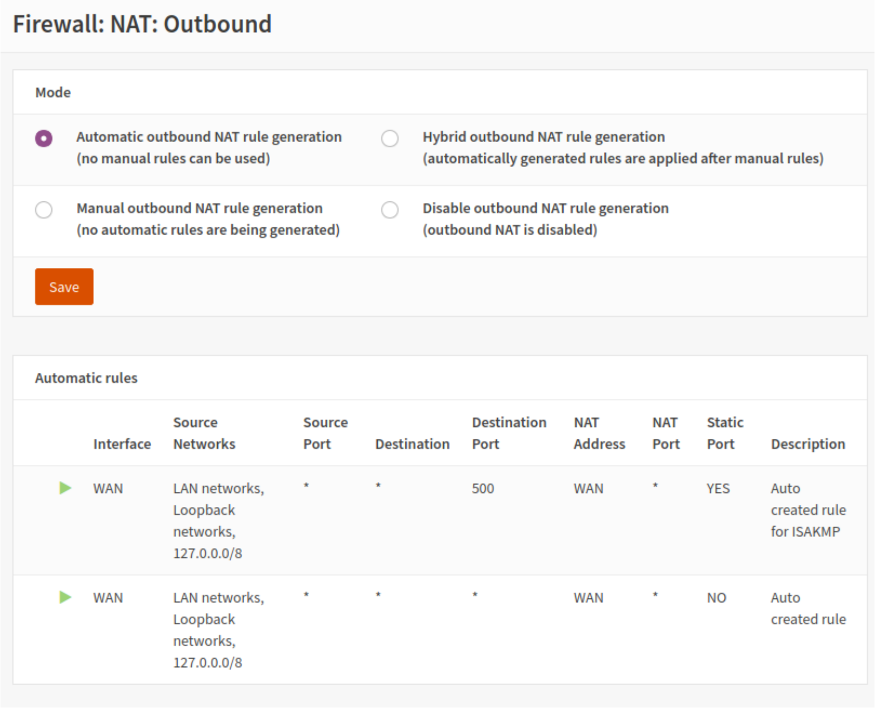
Before starting on any of the configurations below, create snapshots of your OPNSense® firewall or create a backup of your configuration, so it is easy to restore it if errors are made.

5.1 Outbound

This is the most simple implementation of NAT, and it can be used in an automatic, manually or hybrid configuration. We are going to look at the manual mode here.

Manually configuration is needed when the ISP (Internet Service Provider) is providing a pool of IPs that can be used on the WAN side.

In meny `Firewall --> NAT --> Outbound` the outbound NAT can be configured. The standard configuration can be seen in figure 13.



Firewall: NAT: Outbound

Mode

● Automatic outbound NAT rule generation (no manual rules can be used)

○ Hybrid outbound NAT rule generation (automatically generated rules are applied after manual rules)

○ Manual outbound NAT rule generation (no automatic rules are being generated)

○ Disable outbound NAT rule generation (outbound NAT is disabled)

Automatic rules

	Interface	Source Networks	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description
▶	WAN	LAN networks, Loopback networks, 127.0.0.0/8	*	*	500	WAN	*	YES	Auto created rule for ISAKMP
▶	WAN	LAN networks, Loopback networks, 127.0.0.0/8	*	*	*	WAN	*	NO	Auto created rule

Figure 13: NAT Simple outbound NAT

To change from the automatic to manual follow the steps below:

1. Click the box besides `Manual outbound NAT rule generation.`
2. Click on `save`.
3. Create a new rule and set the configuration to:
   (a) `Interface` to the WAN interface you are using.
   (b) `TSP/IP Version` to `IPv4`.
   (c) `Protocol` to `any`.
   (d) `Source invert` no check mark in the box.
   (e) `Source address` to `192.168.20.0/24`.
   (f) `Source port` to `any`.
   (g) `Destination invert` no check mark in the box.
   (h) `Destination address` to `any`.
   (i) `Destination port` to `any`.
   (j) `Translation / target` to `Interface address`.

24. What is outbound NAT?
25. Is it working?

The following step is not required since our network does not have multiple WAN addresses.

If there is a pool of WAN addresses, either physical network adapters or virtual addresses, there are three changes that are needed in the configuration over. The first one is to change the `Translation / target` to the physical network adapters or virtual addresses. The second change is to choose how the firewall should choose which WAN IP is going to be used. This is done in the `Pool Option`. There are four different methods to choose from:

- Random - Random select an IP in the pool.
- Round Robin - This is the default option. Loops through the IPs in the pool.
- Source hash - Hashes the source address to ensure that the translation is correct.
- Bitmask - Keeps the last portion identical (`10.0.0.10 --> X.X.X.10`).

If your setup is using aliases, only Round Robin can be used.

The last one is to create a firewall rule that is passing through the traffic.

5.2 Port Forwarding

The port Forward NAT method is used when you want to expose an internal service to the world. This could be a web server, email server or in a home network for example your Xbox console. In this tutorial, we are forwarding a simple python web server on port 8080 on the Ubuntu server. This web server will be accessible from your client machine when you are done with the configuration.

To set it up, follow the guide below:

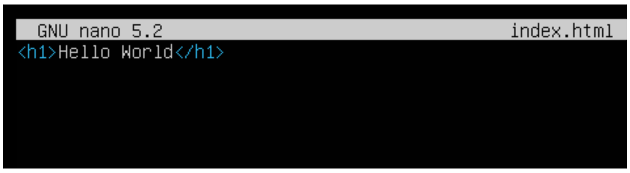
1. Go to `Firewall --> NAT --> Port forward`
2. Click on `add`.
3. Configure:
   (a) Set `Interface` to WAN.
   (b) Set `TSP/IP Version` to `IPv4`.
   (c) Set `Protocol` to `TCP`.
   (d) `Destination invert` no check mark in the box.
   (e) Set `Destination` to `WAN address`.
   (f) `Destination port range` to `other` and choose `8080` in both of the `from` and `to` boxes.
   (g) Set `Redirect target IP` to `192.168.20.12` (Check if this is your Ubuntu Server IP).
   (h) Set `Redirect target port` to `8080`.
   (i) Make a checkmark in the `Log` checkbox.
   (j) Click `Save` and `Apply Changes`.

Creating and accessing a simple web server

Now the port forwarding is done, let's create a simple web server using Python. Python 3 should be preinstalled, if not use the command `sudo apt install python3` on the Ubuntu server to install it.

Configure the web server and creating the `index.html` file:

1. In your home directory, on the Ubuntu server, create a new folder called `www`. Use the command: `mkdir www` to make it.
2. Go to the directory using the command: `cd www`.
3. Create a `index.html` file that returns a hello world when someone is acceesing it. This can be done using multiple methods: Below are two methods:
   - Use this command: `echo "<h1>Hello World</h1>" > index.html`, or
   - Use your favorite editor and insert the command `<h1>Hello World</h1>` on line one. (`nano and vim are installed on the Ubuntu server`) When `index.html` is opened in nano it should look like figure 14.



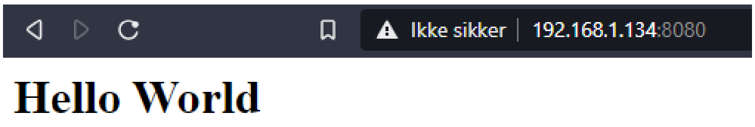
```
  GNU nano 5.2                                    index.html
<h1>Hello World</h1>
```

Figure 14: index.html opened in nano

The next step is to create the Python 3 web server on port 8080. This is done using the command:

```
python3 -m http.server 8080
```

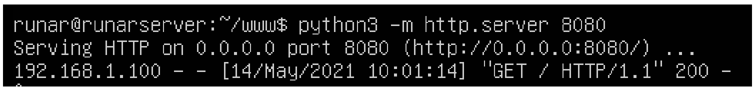
Now, try to access the webserver from your host machine. Open a browser and use the WAN address on your firewall and port 8080. You should get something like figure 15, but using your WAN IP address.



Hello World

Figure 15: Accessing the simple web server from the host machine

If you go to the Ubuntu Server you will see that the console output from the python webserver gives you an HTTP status code of 200 like figure 16.



```
runar@runarserver:~/www$ python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
192.168.1.100 - - [14/May/2021 10:01:14] "GET / HTTP/1.1" 200 -
```

Figure 16: Simple Python 3 server

26. What does port forward do?
27. What can be done to improve the security when port forwarding is used?

The two sections below are only for information and for the student to explore.

5.3 One-to-one NAT

To set up a One-to-one NAT rule requires a three-step process. First, create a virtual IP (or use a physical network adapter), then create the NAT rule, and at last, create a firewall rule that can pass the traffic through.

5.4 NPTv6

IPv6 does not need to use NAT, since the address range is so large. But for load balancing, it can be smart to use NAT on IPv6.

6 Management network

The management interface is the website you access during the configuration. Since this is using an IP that is in the same range as the other devices, this is called `in-band` management. This should be avoided since a high load on the network can make it hard to manage the firewall. A solution for this is to create an own management network. When this is done it is called `out-of-band` management.

In this section, you will learn:

- Create another network interface.
- Use the new interface as a management interface.

Before starting on any of the configurations below, create a snapshot or a backup of the configuration of your OPNSense® firewall, so it is easy to restore if errors are made.
It is **recommended** that you restore to your backup configuration after you have done this task to make it easier later in the tutorial.

When an own management interface is set, it is hardening our network infrastructure. Since it is not possible to access the management page of the firewall anymore outside of the interface that is set, versus the previous one that could be accessed via the local network.

1. Create a new virtual interface (see section 2.3 if unsure) on the firewall.
2. Goto `System --> Settings --> Administration` and change the option called `Listen interface` to the new interface you created.
3. Modify the Ubuntu Desktop network interface to connect to the new network interface on the firewall.

When you are changing to the new managing interface, you will not be able to access the firewall as you did earlier. You will need to change your IP to match the newly created interface network.

The two next paragraphs are not necessary to do, it is just a high-level example of what could be done.

This can also be done using aliases. Create two aliases, the first one with the IPs that should have access to the management interface and the alias with the ports that are required. Use those aliases to create the firewall rules that give the IP, with those ports access to the management interface and another rule that is blocking everything else and log it.

If there are multiple IP's in the alias that is using the management interface, there must be created routing rules in `System --> Routes --> Configure`, so they can talk to each other.

You should also block all traffic from the other interfaces to the management interface. To do this, use a floating rule.

28. Why would you put the management of the firewall and other network devices on a separate network?

7 Bandwidth

In OPNSense®, bandwidth limitation is called shaper and can be found in the menu `Firewall --> Shaper`. There are many reasons for implementing a bandwidth limitation solution. It could be to prioritize certain network traffic or optimize the bandwidth that is used. Some other vendors could call this for **QoS**, Quality of Service.

In this section, you will learn:

- Create a bandwidth limitation rule.
- The difference between using a pipe and a queue.

To create a bandwidth limitation, you first need to create a pipe and then assign that pipe to an interface using the rule configuration. The first step is to create a pipe:

1. Goto `Firewall --> Shaper --> Pipe`. A pipe defines the speed you set.
2. Change `Bandwidth` to the amount you want. For this to work in this tutorial, it needs to be lower than the speed you get from your ISP. For example, 10.
3. Change `Bandwidth Metric` to the correct designation. For example, `Mbit/s`.
4. And give it a `Description` that describes what this pape does. For example, "10mbps".
5. Click on `Save` and `Apply`.

Now, you have created a pipe that can be used in a rule to limit bandwidth. The next step is to create the rule:

1. Goto `Firewall --> Shaper --> Rule`. This defines where the pipe should apply.
2. Set the `Sequence` to `1`.
3. Set `Interface` to WAN.
4. Set `Proto` to `ip`.
5. Set `Source` and `Destination` to `All`.
6. And set `Target` to the pipe you created earlier (10mbps).
7. Click on `Save` and `apply` to create and start the rule.

29. Test the configuration you have made using a site that can do a speed test. Do you get the same result as in figure 17?
30. How can you use this rule against on IP instead of all on the interface?
31. There is also one more configuration that can be done, `queues`. What does it do?
32. Why would you prioritize some traffic over other traffic?

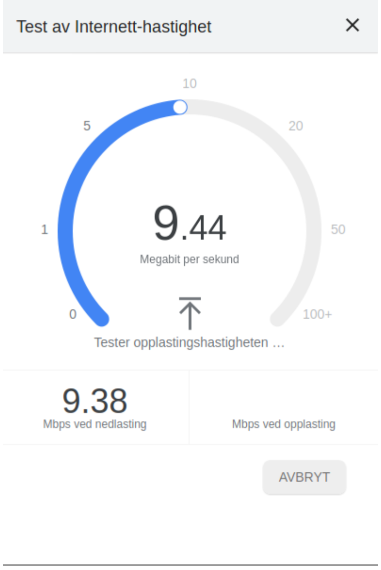
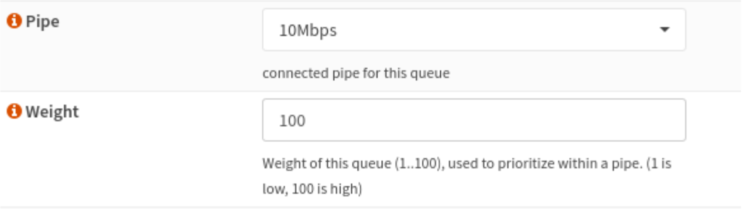


Figure 17: Google speedtest

7.1 Queue

Using the `Queue` options implement the WF2Q+ (Worst-case Fair Weighted Fair Queueing) policy. The queue is associating a **weight** and a pipe to a flow. The difference between a pipe and a queue is that a pipe is a hard limit, while a queue is used to share the bandwidth in a pipe, based on the ”weight” that is used. There can be multiple queues in a pipe.

The configuration of a queue is almost the same as when you created a pipe. The only difference is that you need to choose a pipe the queue is going to use and the weight (1 - 100) the queue has (see figure 18). The lower weight, the more prioritized it is.



Pipe	10Mbps connected pipe for this queue
Weight	100 Weight of this queue (1..100), used to prioritize within a pipe. (1 is low, 100 is high)

Figure 18: Queue configuration differences from pipe configuration

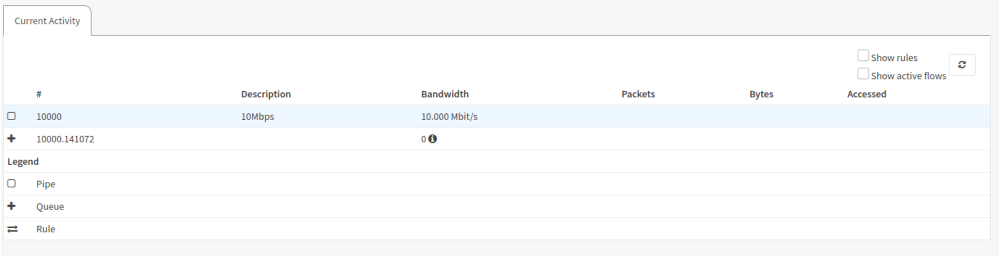
?

33. How can you test if the queue is working?

7.2 Status

The `Status` will show you which bandwidth limitation that is implemented on the firewall at all time. Only rules, pipes, and queues that are `Enabled` will be shown on the status page. An example with the rule created in the first task in this section can be seen in 19.

Only pipes, queues, and rules that are `enabled` will be displayed on the status page.



	#	Description	Bandwidth	Packets	Bytes	Accessed
☐	10000	10Mbps	10.000 Mbit/s			
+	10000.141072		0 ℹ			

Legend	
☐	Pipe
+	Queue
⇄	Rule

Figure 19: Shaper status

8 VPN

OPNSense® has two different VPN solutions built-in. It is IPsec and OpenVPN. There is also possible to use L2TP (Legacy), PPTP (Legacy), OpenConnect, Stunnel, Tinc, WireGuard, and ZeroTier via installing plugins. This tutorial will use OpenVPN.

Two different connection methods could be used when using VPN. Site to site and client-server tunnel. Site to site is used to connect two or more different sites. For example, a business that has multiple divisions that need to connect back to a headquarter. A client-server tunnel is when someone is connecting to the business network remotely. In this tutorial, the client-server tunnel method is explored.

In this section, you will learn:

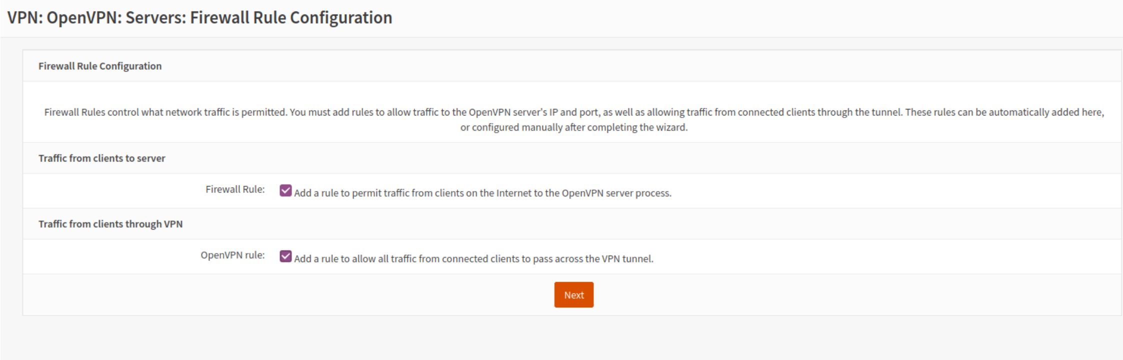
- How to configure OpenVPN using a client-server tunnel.
- Create a CA (Certificate Authority).
- Create a new user.

8.1 OpenVPN wizard

In this task, you are using the VPN wizard to configure the server-side of the VPN service. The wizard will guide you through the steps:

1. Create a certificate authority.
2. Create a certificate.
3. Configure the VPN server.
4. Create Firewall rules.

1. Goto `VPN --> OpenVPN --> Servers`.
2. Click on the button `Use a wizard to setup a new server`.
3. Choose `Local User Access`.
4. Click on `Add New CA`.
5. Configure the following fields:
   (a) Set `Descriptive name` to `opensense_vpn`.
   (b) Set `Country Code` to `NO`.
   (c) Set `State or Province` to `Agder`.
   (d) Set `City` to `Kristiansand`.
   (e) Set `Organization` to `Noroff`.
   (f) Set `Email` to the email you use.
6. The next step in the wizard is to create the certificate. Click on `Add new CA`.
7. Configure the following fields:
   (a) Set `Descriptive name` to `opensense_cert`.
   (b) The other field here should be prefilled from the previous fields you changed.
   (c) Click `Create new Certificate`.
8. The next step in the wizard is to setup the OpenVPN server. Change only the following fields:
   (a) Set `IPv4 Tunnel Network` to `192.168.50.0/24`. - A new network that the clients are using when they are connecting using the VPN.
   (b) Set `IPv4 Local Network` to `192.168.20.0/24`. - Our original local network.
   (c) Set `DNS server 1` to `8.8.8.8`. - Google DNS server.
   (d) Set `DNS server 2` to `8.8.4.4`. - Google DNS server.
   (e) Click on `Next`.
9. The next step in the wizard is to configure the firewall rules (figure 20). Here you will see two options. The first one is to accept traffic from the newly created network to the internet, and the second one is to accept client traffic to the VPN tunnel.
10. Check both of them and click the `Next` button.
11. Click the `Finish` button to quit the wizard.



VPN: OpenVPN: Servers: Firewall Rule Configuration

Firewall Rule Configuration

Firewall Rules control what network traffic is permitted. You must add rules to allow traffic to the OpenVPN server's IP and port, as well as allowing traffic from connected clients through the tunnel. These rules can be automatically added here, or configured manually after completing the wizard.

Traffic from clients to server

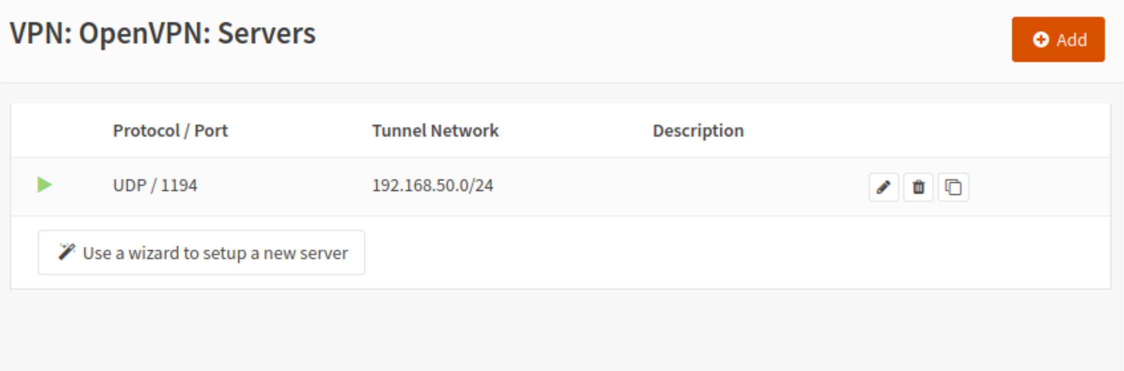
Firewall Rule: ☑ Add a rule to permit traffic from clients on the Internet to the OpenVPN server process.

Traffic from clients through VPN

OpenVPN rule: ☑ Add a rule to allow all traffic from connected clients to pass across the VPN tunnel.

Figure 20: Adding firewall rules during VPN configuration

When you are finished with the wizard, the first page after will show you if the VPN service is running (figure 21). It could also be checked on the `Dashboard` page.



VPN: OpenVPN: Servers

	Protocol / Port	Tunnel Network	Description
▶	UDP / 1194	192.168.50.0/24	

Figure 21: VPN is running

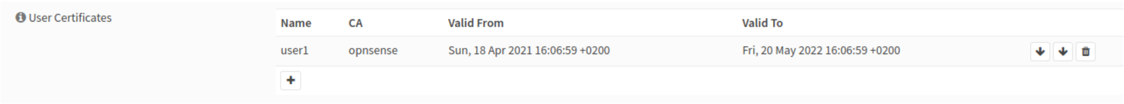
8.2 Client setup

The next step is to create a user with a certificate and get the user to access the VPN network we have created. If you do not have a user, create the user with the guide in 3.1. When the user is created, remember to check the box that says `Certification` and when prompted later for certificate method to use, choose `Create internal Certificate`.

If you have a user and want to add a certificate to the user:

1. Goto `System --> Access --> Users`.
2. Locate the user you want to create a certificate for and click on the pencil on the right side of the username.
3. Click on the plus sign beside `User Certificate` to add a certificate to an existing user.
4. Choose `Create internal Certificate`.
5. Click `Save`

If you go back to the user you either created or modified, there is now a certificate attached to the user (figure 22).



User Certificates

Name	CA	Valid From	Valid To
user1	opnsense	Sun, 18 Apr 2021 16:06:59 +0200	Fri, 20 May 2022 16:06:59 +0200

Figure 22: Certificate added to user

8.2.1 Export user certificate and configuration

To test that the OpenVPN is working correctly, we have two options. We could use the Ubuntu client we are using and connect it to the VPN, this is one simple solution, but not exactly what we want for this solution, since it is not connecting **remotely**. The second solution is to use our host machine. The following configuration will guide you through the process.

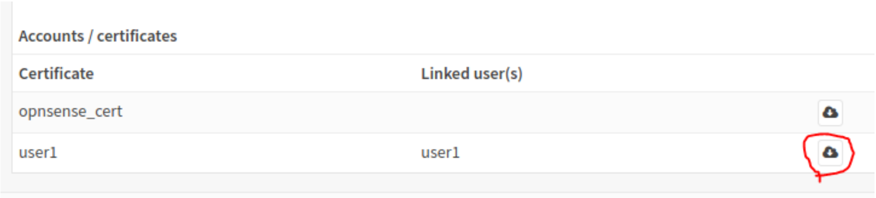
First you need to give the host machine access to the firewalls web interface:

1. Goto `Firewall --> Rules --> Wan`.
2. Create a new rule using the `Add` button.
3. Change this in the configuration:
   (a) Set `Protocol` to `TCP`.
   (b) Set `Destination` to `This firewall`.
   (c) Set `Destination port range` to `HTTPS` (on both to and from).
   (d) Set `Description` to `Access to web interface`.
   (e) Optional, make a checkmark in the `Log` box. - If `Log` has a checkmark, all packets that are using this rule will be logged. It is recommended since you want to have accounting on who is accessing the web interface.
4. Click `Save` and `Apply changes`.

34. Find the OPNSense® WAN IP address and try to access it from your host. Does it work?

The next step is to export the certificate and configuration.

1. On your host machine, goto `https://<YOUR-FIREWALL-WAN-IP-ADRESS>` and login.
2. Goto `VPN --> OpenVPN --> Client Export`.
3. Change this in the configuration:
   (a) Set `Hostname` to the WAN IP address your firewall has.
   (b) Remove any passwords that are in the configuration.
   (c) Remove the checkmark in the `Validate Server Subject` box.
   (d) At the bottom, there is a cloud symbol to the right of the user you want to download the configuration for (see figure 23).
   (e) Download and extract the files on your host.



Accounts / certificates

Certificate	Linked user(s)	
opnsense_cert		☁
user1	user1	☁

Figure 23: Download certificate for a user

8.2.2 Firewall rule for VPN clients

We need to configure a firewall rule to give VPN clients access to the WAN interface on the firewall. This is the last step on the server-side for the configuration of the OpenVPN server.

1. Goto `Firewall --> Rules --> Wan`.
2. Create a new rule using the `Add` button.
3. Change this in the configuration:
   (a) Set `Protocol` to `UDP`.
   (b) Set `Destination` to `This firewall`.
   (c) Set `Destination port range` to `OpenVPN` (on both to and from).
   (d) Set a checkmark beside `Log` to log packets and events.
   (e) Set `Description` to `Client access to OpenVPN`.
4. Click `Save` and `Apply changes`.

8.2.3 Configure the client

Start with downloading the OpenVPN client to your host machine. Other options work also, but you are on your own if you decide to do that.

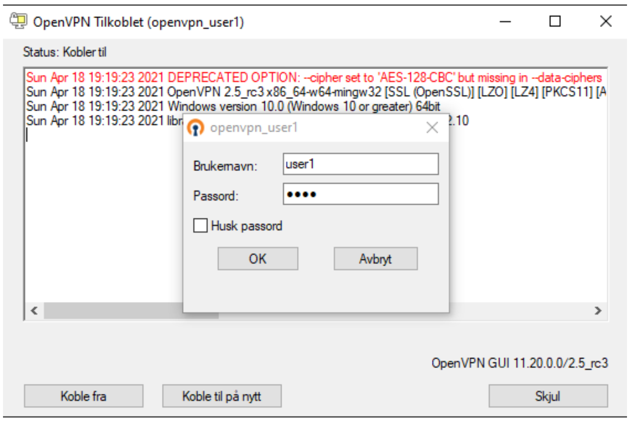
OpenVPN can be downloaded from here, regardless of what OS you have: https://openvpn.net/vpn-client/

1. Install the VPN client.
2. Depending on if you are using a GUI or CLI choose your correct step below.
   - GUI: Import the `.ovnp` file to the VPN client if you are using a GUI version (Goto step 3).
   - CLI: If you are using a CLI version, you can use this command `sudo openvpn <YOUR OPENVPN FILE HERE>` to connect to the VPN service.
3. When the file is imported, try to connect and you will be prompt for username and password (figure 24).

If you have a problem connecting with the GUI version, make sure that all of the files you downloaded is in the correct folder. Check the OpenVPN settings to see where the files are moved when they are imported.

Goto `VPN --> OpenVPN --> Connection Status` to see if the client (your host machine) connected to the VPN network we created (figure 25).

35. Did you manage to connect to the firewall?
36. What is the minimum recommended key size for RSA encryption?



OpenVPN Tilkoblet (openvpn_user1)

Status: Kobler til

```
Sun Apr 18 19:19:23 2021 DEPRECATED OPTION: --cipher set to 'AES-128-CBC' but missing in --data-ciphers
Sun Apr 18 19:19:23 2021 OpenVPN 2.5_rc3 x86_64-w64-mingw32 [SSL (OpenSSL)] [LZO] [LZ4] [PKCS11] [A
Sun Apr 18 19:19:23 2021 Windows version 10.0 (Windows 10 or greater) 64bit
Sun Apr 18 19:19:23 2021 libr                                              2.10
```

openvpn_user1

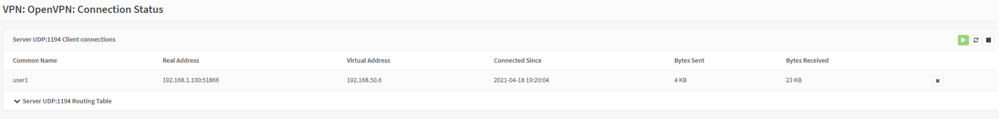
Brukernavn: user1

Passord: ●●●●

□ Husk passord

OpenVPN GUI 11.20.0.0/2.5_rc3

Figure 24: OpenVPN asks for username and password



VPN: OpenVPN: Connection Status

Server UDP:1194 Client connections

Common Name	Real Address	Virtual Address	Connected Since	Bytes Sent	Bytes Received
user1	192.168.1.100:51866	192.168.50.6	2021-04-18 19:20:04	4 KB	23 KB

Figure 25: OpenVPN status on the firewall

9 Web proxy

A web proxy can be used to:

- Antivirus - Sending the traffic through a central unit that is checking for viruses.
- Authentication - Everyone that wants to access the internet needs to provide some sort of login for access.
- Accounting - Have a record of who is accessing which site. Depending on the situation, this could be a GDPR breach!!
- Filter - Filter websites based on IP, website, web domain, or category.

Learning objectives for this module is:

- Configure a web proxy.
- Filter using URLs.
- Filter using category.
- Proxy logs.
- SSL inspection

> When using the proxy service in OPNSense®, there are some limits that are important to remember. There are not possible to apply proxy rules for only one specific client. If a rule is implemented, it will affect every client. This can make it difficult to use the firewall in a complex environment.
> Make a backup of your configuration before continuing with the tasks below.

9.1 Enable proxy service on the firewall

The first step is to enable the proxy service on the firewall:

1. Goto `Services --> Web-proxy --> Administration`
2. Choose `General Proxy settings`
3. Click in the `Enable` box and apply the changes.

9.2 Browser settings

To enable the browser to send data via the proxy, you need to make some change in the browser settings. In this task, the Firefox browser in our Ubuntu client is configured to use the proxy.

1. Goto your browser settings in the browser you want to use.
2. Search for proxy settings. This needs to be on a machine that is connected to the same network as the OPNSense® firewall.
3. Change the following settings (for Firefox browser):
   (a) Change to manual configuration.
   (b) Change `HTTP Proxy` to `192.168.20.1` and the port to `3128`.
   (c) Click the box that says `Also use this proxy for FTP and HTTPS`.
   (d) Add the IP range (`192.168.20.0/24`) to `No proxy for`.
4. Click in the `Enable` box and apply the changes.

If you use another browser than the Firefox browser in the Ubuntu client, you are on your own.

9.3 URL filtering with proxy

There are two different methods that can be used to filter websites. The first one is a blacklist and the second one is to whitelist. A blacklist will allow everything except what is on the blacklist. A whitelist will block everything and only allow what is in the whitelist. Blacklist is the default configuration of OPNSense® and is the method used in this tutorial.

1. Goto `Services --> Web-proxy --> Administration`
2. Choose `Access control list`. This can be found in the drop down meny besides `Forward Proxy`. See figure 26.
3. In the `Blacklist` insert a domain you want to block. In this case use `nrk.no`.
4. Click `Apply` and reload the proxy service (top right corner).

37. What are regular expressions?
38. What is the difference between using `nrk.no` and `https://www.nrk.no` when filtering?
39. How can you use a whitelist instead of a blacklist?

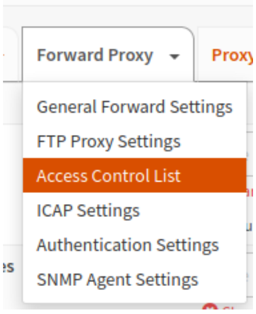


Figure 26: Access control list

9.4 Category filtering

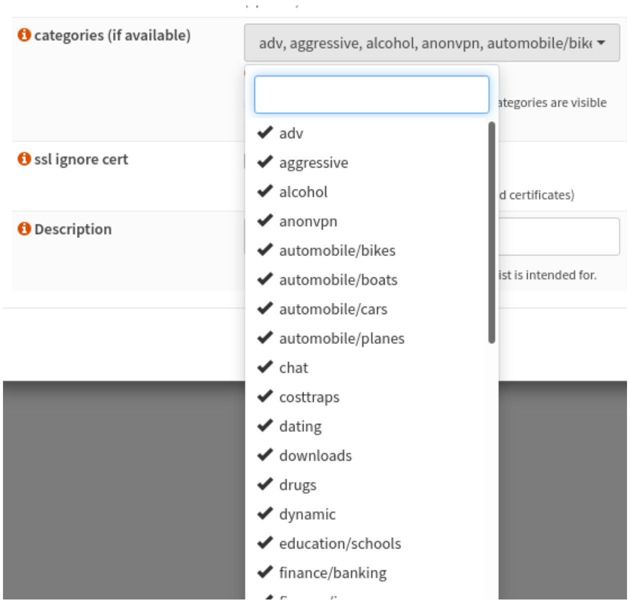
Using a category list is an easy method to block a lot of URLs fast and easy. There are multiple services that provide such lists. One of them is Shalla, which is used in our example.

1. Goto `Services --> Web-proxy --> Administration`
2. Choose `Remote Access Control List`.
3. Click on the + sign to add a new filter.
4. Configure the following:
   - (a) Make sure `Enabled` is checked.
   - (b) Set `Filename` to Shalla.
   - (c) Set `URL` to https://www.shallalist.de/Downloads/shallalist.tar.gz.
   - (d) And the `Description` to `Shalla`.
   - (e) Click save.
5. Click `Download ACLs & Apply`

The Shallalist that is downloaded contains over 70 different categories. To see them, click on the edit pencil sign and remove or add categories (figure 27).

No proxy bypass

First create two (2) firewall rules that block access without using proxy. Change the `Destinaiton port range` between `HTTP` and `HTTPS` for each of the rules created. The following configuration is only for `HTTP`:



categories (if available): adv, aggressive, alcohol, anonvpn, automobile/bik

ategories are visible

- ✓ adv
- ✓ aggressive
- ✓ alcohol
- ✓ anonvpn
- ✓ automobile/bikes
- ✓ automobile/boats
- ✓ automobile/cars
- ✓ automobile/planes
- ✓ chat
- ✓ costtraps
- ✓ dating
- ✓ downloads
- ✓ drugs
- ✓ dynamic
- ✓ education/schools
- ✓ finance/banking

ssl ignore cert

d certificates)

Description

ist is intended for.

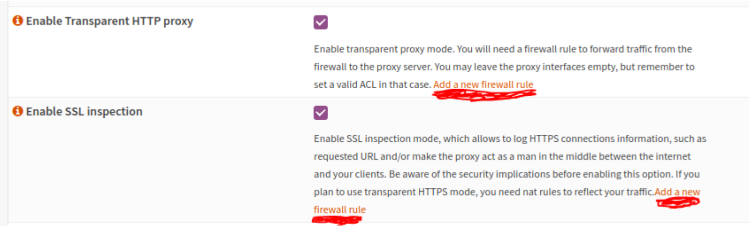
Figure 27: Category blacklist

1. Go to `Firewall --> Rules --> LAN`.
2. Change:
   (a) Set `Action` to `Block`.
   (b) Set `Interface` to `LAN`.
   (c) Set `Protocol` to `TCP/UDP`.
   (d) Set `Source` to `LAN`.
   (e) Set `Destination port range` to `HTTP`. Remember to change this to `HTTPS` for rule number two.
   (f) Make a checkmark in the `Log` checkbox.
   (g) Set `Category` to `Block Proxy Bypass`.
   (h) Set `Descripion` to `Block http bypass`. Change this to `Block https bypass` for rule number two.
   (i) Click `Save`.
3. Go to `Services --> Web-proxy --> Administration`
4. Choose `Forward Proxy`.
5. Make a checkmark in the `Enable Transparent HTTP Proxy` check box.

Use the clone besides the pencil in the rule overview to clone the first rule and make the changes and save the new rule.

Forward WAN traffic to proxy

1. Go to `Service --> Web Proxy`.
2. Click the arrow beside `Forward Proxy` and choose `General Forward Settings`.
3. Make a checkmark in the `Enable Transparent HTTP proxy` checkbox.
4. Make a checkmark in the `Enable SSL inspection` checkbox.
5. Click apply.
6. Click on `Add a new firewall rule` in the help text for both `Enable Transparent HTTP Proxy` and `Enable SSL inspection`. If you do not see the help test, see 3.4. Accept the values and create the rule. Those rule will no be seen in the port forward section in NAT.



Enable Transparent HTTP proxy ☑

Enable transparent proxy mode. You will need a firewall rule to forward traffic from the firewall to the proxy server. You may leave the proxy interfaces empty, but remember to set a valid ACL in that case. Add a new firewall rule

Enable SSL inspection ☑

Enable SSL inspection mode, which allows to log HTTPS connections information, such as requested URL and/or make the proxy act as a man in the middle between the internet and your clients. Be aware of the security implications before enabling this option. If you plan to use transparent HTTPS mode, you need nat rules to reflect your traffic.Add a new firewall rule

Figure 28: Creating NAT rules

40. Use some time and see if you can find another list that can be used.
41. How can you test if the Shallalist is working? Just explain it, do not try to do it.
42. How can you configure OPNSense® to automatically update the rule list?

9.5 Proxy logs

For the proxy service there are three different logs that can be seen in the `Services --> web proxy`. `Cache log`,`Access log`, and `Store log`.

43. Explorer the three logs and explain what they log.

Learn more about Squid[13] on their homepage.

9.6 SSL inspection

The firewall can act as a man in the middle and inspect packets that are encrypted. This is done using a proxy. When the firewall receives the packet, it decrypts it and inspects it. When the inspection is finished it encrypts the packet again. To make this work, the first step is to create a certificate that can be used to encrypt the traffic between the client and the firewall. This means that there are two connections per request. The first one between the client and the firewall, and the second one is between the firewall and the webserver.

[13] http://www.squid-cache.org/

9.6.1 Create Certificate Authority

The CA (Certificate Authority) needs to be either a self-signed root certificate or a certificate from an existing root CA. We are creating a self-signed one.

1. Goto `System --> Trust --> Authorities`.
2. Choose `Remote Access Control List`.
3. Click on `Add`.
4. Change the following:
   - (a) Set `Descriptive name` to `ssl_inspect.lab`.
   - (b) Set `Method` to `Create and internal Certificate Authority`.
   - (c) Set `Lifetime` to `3650`.
   - (d) Set `Country Code` to Norway.
   - (e) Set `State or Province` to `Agder`.
   - (f) Set `City` to `Kristiansand`.
   - (g) Set `Organization` to `Noroff`.
   - (h) Set `Email Address` to your Noroff student mail address.
   - (i) Set `Common Name` to `ssl_inspect_ca`.
5. Click `Save`.

When the certificate is created, the next step is to export it. Click on the `Export CA cert` button. Save it on the client. This file will be used later when you configure your client.

9.6.2 Firewall configuration

Follow the configuration below to configure the firewall.

1. Goto `Services --> Web-proxy --> Administration`.
2. Goto `Forward Proxy`.
3. Click the checkbox named `Enable SSL inspection`.
4. Select to use the certificate we created in the previous configuration (9.6.1) in the `CA to use` dropdown menu.
5. Click `Apply` to finish the server configuration.

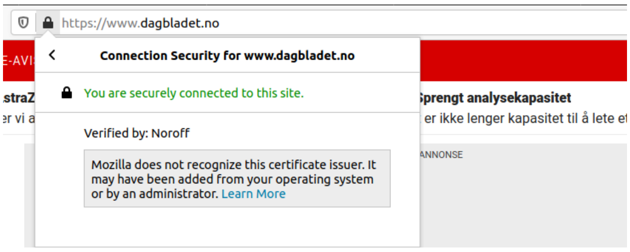
9.6.3 Client configuration

The client configuration is done in Firefox on the Ubuntu client.

1. Start Firefox and goto the `preferences` settings.
2. Goto the `Privacy & Security` tab.
3. Click on `View Certificates`.
4. Import the certificate created earlier (9.6.1).
5. In the next window, click in the box beside `Trust this CA to identify websites`.

9.6.4 Test

Goto any website that is using HTTPS and checks who is verifying the connection. In this test example, www.dagbladet.no is used (figure 29). The connection, in this case, is verified by Noroff. This is in line with the information we used when configuring the CA earlier (9.6.1).



https://www.dagbladet.no

Connection Security for www.dagbladet.no

You are securely connected to this site.

Verified by: Noroff

Mozilla does not recognize this certificate issuer. It may have been added from your operating system or by an administrator. Learn More

Figure 29: CA test on www.dagbladet.no.

10 Intrusion Detection System (IDS) and Intrusion Prevention System (IPS)

IDS and IPS are services on the OPNSense® firewall. To perform the operation, the firewall uses Suricata[14]. Suricata is an open-source signature-based IDS and IPS solution. Suricata is signature-based, which means that it matches the content in packets against a list or database with signatures of known strings/patterns that are suspicious.

The difference between an IDS and an IPS is that the IDS (Intrusion Detection System) is a service that is used to **detect** anomalies in the network. And the IPS (Intrusion Prevention System) is a service that is used to **block or halt** anomalies in the network.

In this section, you will learn to:

- Configure an IDS.
- Create IDS rules.
- Testing if EICAR is detected.
- Add IPS capabilities to the IDS.
- Understand what the differences between IDS and IPS are.

10.1 Enable IDS

> Before continuing with this task, it is recommended to add more RAM to your OPNSense® firewall. Depending on how much memory you have on your host machine, it is recommended to increase the memory to at least 2GB. To do this, you need to shut down the firewall and edit the memory setting in VMware for the firewall client.

It is fairly easy to enable the IDS in the firewall. Follow the following steps to activate IDS:

> 1. Goto `Services --> Intrusion Detection --> Administration`.
> 2. Click the checkbox besides `Enabled` to enable the IDS.
> 3. Click `Apply`.

If everything went well, you will now see that three icons appear in the right top corner of the `Administration` page (icons like the ones in figure 30), and there will be an entry in the log that tells you that **Suricata** is running. The log can be found in `Services --> Intrusion Detection --> Log File`. Another method to check if the service is running is to go to `Lobby --> Dashboard` and check if the **Suricata** service is running.

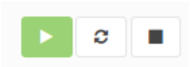


Figure 30: Top right corner of `Administration` page of Intrusion Detection

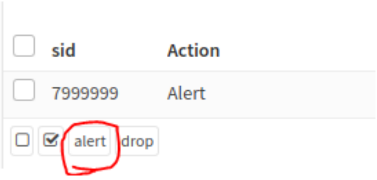
Now that the IDS is enabled, the next step is to configure the IDS.

10.2 Setup IDS rule

To create a rule, we need to download a ruleset and activate it:

[14] https://suricata-ids.org/

1. Goto `Services --> Intrusion Detection --> Administration --> Download`.
2. Scroll down to the rule called `OPNsense-App-detect/test`.
3. Mark the checkbox beside the rule and click on the `Enable selected` in the top of the menu. Now there will be an chackmark on the right side of the rule (in the `Enabled` coloumn).
4. Click the `Download & Update Rules`.
5. Goto `Services --> Intrusion Detection --> Administration --> Rules` and you will see that there is one rule there (rule 7999999).
6. Mark the rule and click on the alert box below. See figure 31.
7. Reload the IDS using the reload button. The middle button in the top right corner, as seen in figure 30.



□	sid	Action
□	7999999	Alert

□ ☑ alert drop

Figure 31: `Alert` box below IDS rules

Testing

The `OPNsense-App-detect/test` rule is a rule that is used to test if the IDS is properly configured. It is testing against the EICAR (European Institute for Computer Anti-Virus Research) standard.

1. Goto `Services --> Intrusion Detection --> Administration --> Alerts`.
2. This is now empty, since we have not tested against anything.
3. Goto `http://www.csm-testcenter.org/cgi-bin/eicar.txt` to test if the IDS is working.

If you get problems during testing of the EICAR rule, check if you have any other services that could prevent your firewall to access the EICAR string, such as a proxy service. Make sure the EICAR test link is using **http** and not **https**.

44. Try to test the IDS using a EICAR rule that has a **https** (`https://secure.eicar.org/eicar.com.txt`)? Why do you think it is not working?

10.3 Setup the IPS

To reconfigure the IDS to an IPS there are two settings that needs to be changed:

1. Goto `Services --> Intrusion Detection --> Administration`.
2. Make a checkmark in the checkbox besides `IPS mode` and click on the `Apply` button.
3. Goto `Services --> Intrusion Detection --> Administration --> Rules`.
4. Mark the the 7999999 rule that was created earlier and hit the `drop` button (right of the alert button in figure 31).
5. Click the `Apply` button and reload the IDS.

Testing

The `OPNsense-App-detect/test` rule is a rule that is used to test if the IDS is properly configured. It is testing against the EICAR (European Institute for Computer Anti-Virus Research) standard.

1. Goto `Services --> Intrusion Detection --> Administration --> Alerts`.
2. Remove all alerts using the `Delete Alert Logs` button on the right side of the date dropdown menu.
3. Goto http://www.csm-testcenter.org/cgi-bin/eicar.txt to test if the IPS is working.

You should now have one entry in the log, and it should say `Blocked` in the action column.

If you get problems when testing this, delete cookies and reload the page you are checking and make sure that the rules are enabled.

45. Try to add the OPNsense social media ruleset and go to one of the well known social media sites. What happens in the log?

All of the OPNsense rules can be found in this GitHub repository: https://github.com/opnsense/rules

10.4 Disabling/removing rules

There are two different methods that can be used to remove/disabling rules for the IDS/IPS in the firewall. The first one is to disable the rules individually and the second one is to use the reverse method used when adding a ruleset to remove the ruleset.

- Disable individually rules:
  1. Goto `Services --> Intrusion Detection --> Administration --> Rules`.
  2. Remove the checkmark in the `Enabled` coloumn behind the rule(s) you want to disable.
  3. Click `Apply` and reload the service to finish.
  4. You will now see that the rule you disabled, is in a lighter grey colour.
- Disable and remove ruleset:
  1. Goto `Services --> Intrusion Detection --> Administration --> Download`.
  2. Mark the ruleset you want to disable and click on the `Disable Selected` button.
  3. Click `Apply` and reload the service to finish.

11 Domain Name System (DNS)

> This chapter is a reading task. It is not required to do the configurations, since the configuration was done during the initial setup of the firewall. If you choose to use the OpenDNS service, make a backup of your configuration before starting.

Learning objectives for this module are:

- How to setup/configure DNS on the OPNSense® firewall.
- Setup/configure the OpenDNS service.

DNS is a service that resolves IP addresses to a human-readable website. For example the Norwegian newspaper `www.vg.no` has the IP addresses `195.88.54.16 - 19`. A total of four (4) different IP's. A DNS can resolve both IPv4 and IPv6. If a client cannot get access to a DNS server, it will not be able to access the internet, since it does not know which IP a website is pointing to.

> `https://whois.domaintools.com/` can be used to lookup IP's.

As default, OPNSense® have the `Unbound DNS` service enabled. It can be found in `Services --> Unbound DNS`. The `Unbound DNS` service will do validating, caching, and recursive DNS queries.

- Recursive - If the IP cannot be resolved locally (in cache), it asks one of the root authorities to look it up.
- Validate - Validates the result from a root DNS server. Uses most often DNSSEC.
- Cache - A local copy that stores lookup done earlier.

This means that you can use an external DNS or the firewalls IP as DNS when you are configuring a client on your tutorial network. During the preparation phase of this tutorial, there was a wizard (see section 2.5) where you inserted the google DNS servers IP addresses. This is the IP's the firewall is relaying DNS request to.

Some well know addresses for DNS is:

- 8.8.8.8 - google.com
- 8.8.4.4 - google.com

Other DNS services on the firewall:

DNSmasque DNS

This was the prefered solution for DNS in the firewall before version 17.7[15]. Legacy is the reason it exists as a service in the firewall.

OpenDNS

OpenDNS is a service provided by OpenDNS[16]. They deliver DNS services that you need to pay for or for the basic packs there are free options. Depending on which services you choose, they will try to give you protection from phishing.

To try their "Family Shield" plan, which is free and super easy to set up, just change the DNS servers you are using to: `208.67.222.123`.

[15] `https://docs.opnsense.org/manual/dnsmasq.html`

[16] `https://www.opendns.com/`

If you sign up for their service, use the `Service --> Open DNS` to configure it.

1. Check the checkbox besides `Enable` to enable OpenDNS.
2. Set your `Username` and `Password` to the username and password used on the OpenDNS website.
3. Set `Network` to the network you configured/created on the OpenDNS website dashboard[17].
4. Change the DNS server the firewall is using in `System --> Settings --> General`.

If you choose to sign up for this service and is removing it later, remember to check that you are using the correct DNS servers after you disable the service. (`System --> Settings --> General`)

46. What does DNS do?

12 Dynamic Host Configuration Protocol (DHCP)

> This chapter is a reading task. It is not required to do the configurations, since the configuration was done during the initial setup of the firewall. If you choose to change the DHCP service, make a backup of your configuration before starting.

12.1 DHCP

The configuration we have made in this tutorial is very common, a firewall with some clients behind it. DHCP is a service that gives each device (client) that are connected to the network an IP address. Since the IPv4 address range is limited, DHCP is used to ”expand” the numbers of available IP on the local network. RFC1918 (Geert Jan de and Yakov 1996) describes which IP addresses can be used in a local network.

Learning objectives for this module are:

- How to setup/configure DHCP on the OPNSense® firewall.

The settings for DHCP can be found at `Services --> DHCPv4` for IPv4 and `Services --> DHCPv6` for IPv6. For IPv6 you are dependent that your ISP provides an IPv6 prefix that the firewall can use to distribute IPv6 addresses to the clients.

An explanation of the different menu options for DHCP. The two first entries are unique for IPv4:

- `Interface name` - Each interface is listed and it is possible to enable/disable DHCP on the interface, change the IP range for DHCP and which DNS server it should use.
- `Log File` - The log file for the IPv4 DHCP server.
- `Relay` - If the DHCP server is somewhere else than the firewall. Need to disable the DHCP server for this to work.
- `Leases` - See the different clients that use the DHCP.

> 47. Can you explain what DHCP is?

13 Routing

This chapter is a reading task. It is not required to do the configuration since it requires more infrastructure (another network).

Learning objectives for this module are:

- How to setup/configure routing

The firewall has a routing table that contains all known routes. With routes, in this case, means routes between interfaces on the firewall and other networks locally. OPNSense® creates automatically routes between interfaces that are present on the firewall.

Goto `System --> Routes --> Status` to see the routes that exists.

If you have other networks locally, that the firewall needs to deliver packets to, you need to create a route to it. If not, the firewall does not know about the other network. To create a route there must be a gateway present at the other network, and an entry in the routing table needs to be created. Follow the configuration below to add a route:

1. Make sure that there is a gateway on the network that is added to the routing table.
2. Goto `System --> Routes --> Configuration`.
3. Configure the `Network Address` (destination network), `Gateway` (gateway to use), and set a `Description`.

OPNSense® can only create static routes.

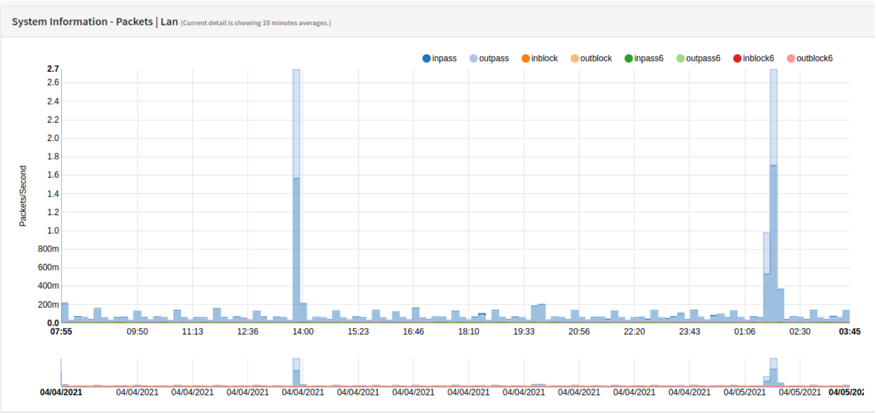
Some features in OPNSense® create routes automatically. Such as VPN.

48. How could you check if routing is working?

14 Reporting

Besides logs that the different features and services have, three different reporting tools can be found in the reporting tab on the managing page for the firewall. The reporting tab in OPNSense® contains a total of five different tabs. Those are:

- Health - Gives you information about the firewall, such as the amount of traffic that is going through each of the interfaces. It is also possible to get information about the system, like how much of the RAM or CPU is used, how many states are known by the firewall, and CPU temperature if the hardware supports it (Not supported in our case, since we are using a virtual hypervisor). The information displayed here is not "live". You need to update the page to get updated information. An example can be seen in figure 32. The data that is collected is called RRD (Round Robin Data). The displayed data can be exported to a `.csv` using the `Show Tables` function on the top right side of the screen.
- Insight - This is the local collector for the NetFlow information, and it displays it in pie charts.
- NetFlow - Create packages that contain information about the different data streams. The package contains:
  - IP (source and destination).
  - Port (source and destination).
  - Amount of bytes and packages for the stream.
  - Time of the stream.
  - Ingress and egress interface[18].
  - Information about QoS.
  - Autonomous system (BGP).
  - TCP flags.
  - Which protocol is used.
- Settings - Enable and disable RRD, reset and repair NetFlow data and flush collected reports.
- Traffic - Divided into two tabs. The first one is graphs that give you a real-time graph over the amount of traffic that is going through the interfaces. The second one is the overview of the different IPs your network is communicating with.



System Information - Packets | Lan (Current detail is showing 10 minutes averages.)

Figure 32: Reporting - Healt

14.1 NetFlow and Insight

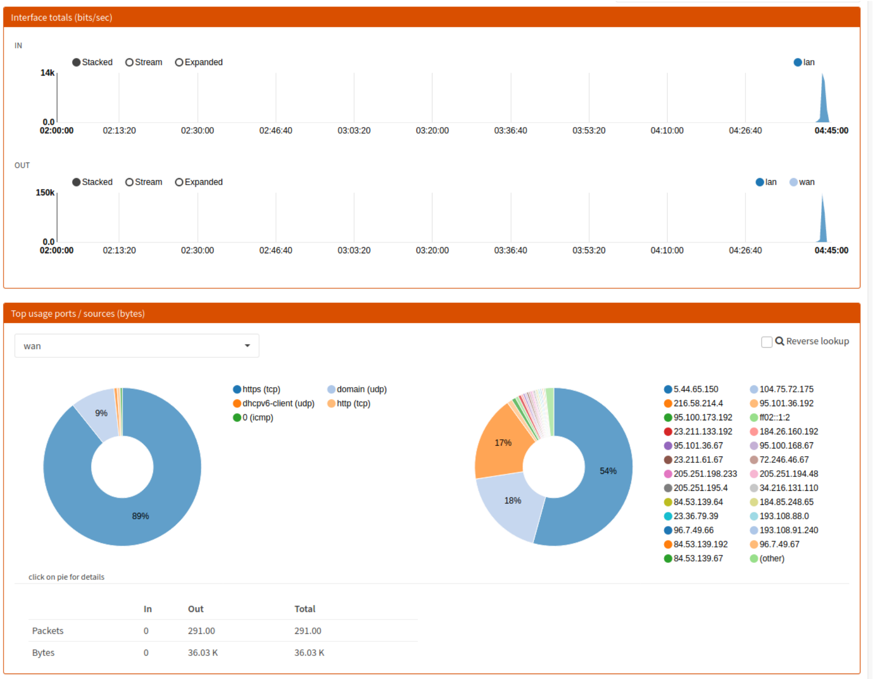
NetFlow was created by Cisco and implemented in their equipment. There are different standards, but version 9[19] is the newest one. Created by Darren Kerr and Barry Bruins in 1996 (Cisco Systems Division Internet Technologies 2005).

[18] Ingress = traffic to or from the firewall. Egress = traffic passing through the firewall
[19] https://www.ietf.org/rfc/rfc3954.txt

In the setup of NetFlow, version 9 is the default setting. OPNSense® supports v5 and v9. The difference is: Version 5 = IPv4, version 9 = IPv4 and IPv6.

It is possible to set up NetFlow to work internally or externally. In this case, we are setting it up to work internally. Follow the configuration below to start the collection of data:

1. Goto `Reporting --> NetFlow`.
2. Set:
   (a) `Listening interface` to `LAN and WAN`.
   (b) `WAN interface` to `WAN`.
   (c) Make a checkmark in `Capture local`.
   (d) `Destination` to `127.0.0.1`.
3. If you do not get any warnings, goto some web sites and create some traffic.
4. Goto `Reporting --> Insight` and see if you get something similar to figure 33.



	In	Out	Total
Packets	0	291.00	291.00
Bytes	0	36.03 K	36.03 K

Figure 33: Reporting - Insight

49. When is it useful to use an external NetFlow collector?

Detailed information from NetFlow can be exported, so it can be used else were. The exported data is in `.csv` form. Four different collections can be exported (Source address, source total, destination port, and interface totals.).

?

50. Play around with the export function and see if you can find some opensource tool and import the data too.

A Questions and Answers

This section will guide you or give answers to the questions asked during the tutorial. First, the question is repeated, and after - or : there will be an answer. The questions are numbered the same as the ones in the text earlier.

1. How do you think making notes during the tutorial will benefit you? - No answer given. Personal statement from the student. The student gives a short statement of why taking notes is beneficial (or not) when doing a tutorial.
2. What is a hash? - A hash is a value that is calculated from the file. It is used to verify data authenticity. If a hash is calculated on a file, it will never change unless the file is changed.
3. Did your hash values match?: - If the values do not match, check if you did it correctly.
   - In Windows: Start and CMD or PowerShell prompt and use the command: `certutil -hashfile <NAME OF YOUR FILE> SHA256`
   - In Ubuntu: Start your terminal and use the following command: `sha256sum <NAME OF YOUR FILE>`
4. Why do you create a virtual network? - If this were a physical lab, you would have used switches, cables, and other network devices to create a physical network, to make the clients talk to each other. When it is done virtualized, you need the same, but the virtual network is emulating those physical devices in your network. Another reason is that you are now segregating the network from your original host network.
5. What does the `em` in the network card stand for? - em references to the manufacturer of the network adapter. em = intel and for example bge = Broadcom.
6. Why did you remove the checkmark for RFC1918 Networks? - Since the IP's you are using are private IP's you need to remove the checkmark. If you do not remove it, IP's that are private cannot be used. https://tools.ietf.org/html/rfc1918.
7. Can you ping your firewall from your client? - Use the ping command. `ping 192.168.20.1`. On Linux, use `CTRL + C` to stop the ping command or use the (-c 3) to limit the amount of ping sent to three (3).
8. What is key-size? - Key-size is the length of bits that are used by the algorithm when generating cryptographic keys.
9. What is the difference between a private key and a public key? - Private key is your key and must be kept secret. The public key is the key that can be shared and given to for example a server that you want to login to.
10. What does the `Password protect the console menu` checkbox in `System -> Settings -> Administration` in the web GUI do? - It makes it impossible to change the password, without having physical access to the firewall.
11. Try to ping your client. Do you get something similar to figure 8? - Answered in the section. See figure 8.
12. Why do you think the action `Reject` is mostly used on so-called friendly networks? - To save time for the client that is trying to connect, it is important that the client knows that the request is blocked. This can save time for troubleshooting.
13. Try now to `PING` the same website as you did in bullet point 4. What is happening? - If it is done correctly, you are not able to ping any websites.
14. How can you disable the rule that was created? - By clicking on the red cross in the overview of the firewall rules.
15. Are you able to ping any website from the Ubuntu Server when the rule is disabled? - Yes.
16. Do you see any evidence in the log when the rule that was created earlier is active? - It should be possible to see something like figure 34 in the log.
17. How can you test if this is working? - See 5.2

18. Play around and try to create other rules. - The student can try to allow FTP or Telnet and test if it is working.
19. Where in the rule editor page can you add the time-based rule? - When the time-based rules are created, it is possible to choose it under the `Schedule` options almost at the bottom of the rule edit page.
20. Try to create a schedule and add it to a rule that blocks access to `www.nrk.no` inside the normal working hours (08.00 - 16.00). -
21. Can you create a firewall rule that uses the alias you created to block one country? -
22. How can you test if the previous create rule is working? -
23. Is it possible to do a packet capture with OPNSense®? - Yes it is possible. Goto `Interfaces --> Diagnostics --> Live View --> Packet Capture`.
24. What is outbound NAT? - Easy explained; it translates the internal IP in packets to the WAN IP on outgoing packets, and reverse on incoming packets.
25. Is it working? - Try to browse the internet.
26. What does port forward do? - Expose a service that is run on an internal IP address to a port on the WAN side of your network.
27. What can be done to improve the security when port forwarding is used? - Set up firewall rules, use HTTPS instead of HTTP and general hardening for the service and the server.
28. Why would you put the management of the firewall and other network devices on a separate network? - When it is on its own network, it will not slow down or fail during periods with high load on the firewall.
29. Test the configuration you have made, using a site that can do speed tests. Do you get the same result as in figure 17? - Answer is given in the question.
30. How can you use this rule against on IP instead of all on the interface? - Change the Source and Destination in the `Firewall --> Shaper --> Rule` to the IP you want to limit.
31. There is also one more configuration that can be done, `queues`. What does it do? - It can be used to creates flow (one or multiple) in a pipe. It can prioritize which flow in a pipe is getting access to the bandwidth first or need to wait. Can also choose how the bandwidth in the pipe is divided by source or destination. Mainly pipes are used to hard limits and queues to give hosts a different share of the flow in a pipe.
32. Why would you prioritize some traffic over other traffic? - A good example could be the IP telephone. You would prioritize the IP telephone over for example a user that is streaming something or downloading something. This will be useful especially if there are a lot of users or the ISP cannot deliver a fast line.
33. How can you test if the queue is working? - Create a pipe. Then create 2 queues. It is important that they are weighted differently. Then create one rule for each of the queues that were created. When the rules are created, use different protocols. For example FTP, HTTP or something else. To test this, start something that creates traffic for the protocol that has the highest weight first, and see what happens when you starts to create traffic on the other protocol. A good idea is to use for example HTTP/HTTPS on the rule with the high weight (easy to start a download to saturate the pipe.).
34. Find the OPNSense® WAN IP address and try to access it from your host. Does it work? - Find the WAN IP address on the `Lobby --> Dashboard` page on your firewall, and insert https:// before the WAN IP when trying from the host machine.
35. Did you manage to connect to the firewall? - If you managed to connect, you will see it in the `VPN --> OpenVPN --> Connection Status` page.
36. What is the minimum recommended key size for RSA encryption? - NIST (National Institute of Standards and Technology) recommends at least 2048 bits (Barker and Dang 2015). This recommendation can be different in other organisations and will be higher when years go by.
37. What are regular expressions? - Regular expressions are used to match patterns in a string.

38. What is the difference between using `nrk.no` and `https://www.nrk.no` when filtering? - The difference is that it filters on the exact string that is used. So `nrk.no` will be found everywhere in the URL, versus `https://www.nrk.no` will be only found first in a URL.

39. How can you use a whitelist instead of a blacklist? - Insert a `.` in the blacklist and start using the whitelist.

40. Use some time and see if you can find another list that can be used. - Explore the lists.

41. How can you test if the Shallalist is working? Just explain it, do not try to do it. - WARNING: A solution can be to go to a page that is in the block list. THIS IS NOT RECOMMENDED!!

42. How can you configure OPNSense® to automatically update the rule list? - Use the `Schedule with Cron` button to create a scheduling task.

43. Explorer the three logs and explain what they log. - This is a logfile from Squid. `Cache log` is the cache.log file. It stores information about configuration, warnings and errors. `Access log` is the access.log file. It is used to store client requests. And the `Store log` is the store.log file. It stores the decisions made by Squid to store and remove objects from the cache.

44. Try to test the IDS using a EICAR rule that has a **https** (`https://secure.eicar.org/eicar.com.txt`)? Why do you think it is not working? - The IDS cannot see data that is in an encrypted packet, since the encryption/decryption is happening on each endpoint. If the firewall should inspect encrypted packets a proxy need to be configured.

45. Try to add the OPNsense social media ruleset and go to one of the well known social media sites. What happens in the log? - If you goto `https://facebook.com` you will get multiple alerts in your log.

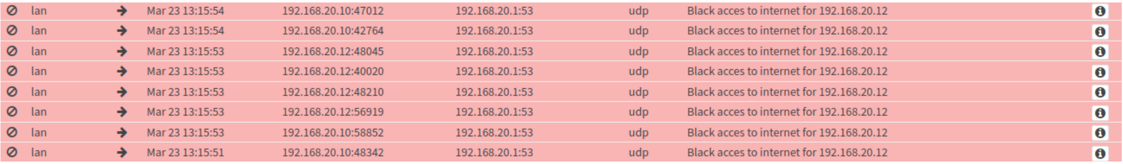
46. What does DNS do? - DNS makes it easier to navigate the internet. Instead of remembering each individual IP address, you can remember a name. DNS translate Ips to human readble names.

47. Can you explain what DHCP is? - DHCP is a service that gives Ips to each device that is connected.

48. How could you check if routing is working? - Using the ping command, see 3.9.1 and disable packet filtering, see 3.9.2.

49. When is it useful to use an external NetFlow collector? - When there are multiple sources of data, that is merged. For example, a company that has multiple firewalls and maybe servers that can send NetFlow data.

50. Play around with the export function and see if you can find some opensource tool and import the data too. - A cool open-source tool is https://github.com/robcowart/elastiflow.



```
⊘ lan   →  Mar 23 13:15:54  192.168.20.10:47012  192.168.20.1:53  udp  Black acces to internet for 192.168.20.12
⊘ lan   →  Mar 23 13:15:54  192.168.20.10:42764  192.168.20.1:53  udp  Black acces to internet for 192.168.20.12
⊘ lan   →  Mar 23 13:15:53  192.168.20.12:48045  192.168.20.1:53  udp  Black acces to internet for 192.168.20.12
⊘ lan   →  Mar 23 13:15:53  192.168.20.12:40020  192.168.20.1:53  udp  Black acces to internet for 192.168.20.12
⊘ lan   →  Mar 23 13:15:53  192.168.20.12:48210  192.168.20.1:53  udp  Black acces to internet for 192.168.20.12
⊘ lan   →  Mar 23 13:15:53  192.168.20.12:56919  192.168.20.1:53  udp  Black acces to internet for 192.168.20.12
⊘ lan   →  Mar 23 13:15:53  192.168.20.10:58852  192.168.20.1:53  udp  Black acces to internet for 192.168.20.12
⊘ lan   →  Mar 23 13:15:51  192.168.20.10:48342  192.168.20.1:53  udp  Black acces to internet for 192.168.20.12
```

Figure 34: OPNSense® logging of rule that blocks all internett access

References

Barker, Elaine and Quynh Dang (2015). 'NIST SP 800-57 Part 3 Rev. 1, Recommendation for Key Management, Part 3: Application-Specific Key Management Guidance'. In: DOI: 10.6028/NIST.SP.800-57pt3r1. URL: http://dx.doi.org/10.6028/NIST.SP.800-57pt3r1.

Cisco Systems Division Internet Technologies (2005). 'Cisco Ios Netflow and Security Internet Technologies Division February 2005'. In: February.

Geert Jan de, Groth and Rekhter Yakov (1996). *RFC 1918 - Address Allocation for Private Internets*. URL: https://tools.ietf.org/html/rfc1918 (visited on 23/02/2021).

Stubbig, Markus (2019). *Practical OPNsense - Enterprise firewall build on open source*. BoD - Books on Demand, Norderstedt. ISBN: 978-3-73863-201-9.