Beginner's Guide to OPNsense®

Build Your Own Open Source Firewall

zenarmor

Published by

zenarmor

10080 N. Wolfe Rd. Ste SW3-200 Cupertino, CA 95014

+1 (650) 288 4488

hi@zenarmor.com

www.zenarmor.com

Disclaimer:

OPNsense® is an open-source firewall and routing platform, registered trademark by Decisio Group B.V.

Foreword

Welcome to the world of OPNsense, where the strength of your network's security meets the flexibility of open-source innovation. If you are taking your first steps into this vibrant community, you have chosen an exciting time to embark on your journey.

At Zenarmor, we believe that security should be accessible, manageable, and, most importantly, effective. Our mission has always been about empowering users, from seasoned IT professionals to those just starting. That's why we have paired our next-generation firewall capabilities with OPNsense's powerful platform to create a solution that's not just more secure, but also smarter and more responsive to the evolving landscape of cyber threats.

This guide is an invitation to you—whether you're a hobbyist looking to secure your home network or an IT professional tasked with guarding critical infrastructure. Here, we demystify the process of building your OPNsense firewall, ensuring that you have the knowledge and confidence to construct a robust defense for your digital realm.

But it's more than just about building walls; it's about opening doors—doors to understanding, to capability, and to trust. With Zenarmor's NGFW features enhancing OPNsense such as deep packet inspection, real-time threat prevention, and detailed network control you are not just setting up a firewall; you are architecting a bastion for your digital life, with visibility and control that were once the domain of only the largest enterprises.

At Zenarmor, we deeply believe in the power of community and collaborative knowledge-sharing. This eBook is our contribution to a thriving cybersecurity community, where we stand together in securing our digital spaces. As we continue to innovate, we hope this guide serves not only as a valuable resource but also as a testament to our collective growth and strength in the ever-evolving world of cybersecurity.

Enjoy the read, apply the knowledge, and may your endeavors in cybersecurity be as rewarding as they are secure.

Warm regards,

Murat Balaban

CEO, Zenarmor

Table of Contents

Getting Started with OPNsense: A Beginner's Guide

The OPNsense story began in 2014, when it split off from pfSense® and m0n0wall. Its official debut was in January 2015, and since then, it's been on a fast-paced evolution while preserving the best of both m0n0wall and pfSense.

OPNsense started out as a simple fork of pfSense, but it has since blossomed into a robust alternative to pfSense as a standalone firewall. Today, OPNsense stands as one of the most potent open-source firewalls and routing platforms you can get your hands on.

OPNsense is different because it has features that are on an equal level with or better than those found in expensive commercial firewalls. Not only does it work, but it does so in the open and honest way that open source is known for. A strong dedication to security and excellent code quality is at the heart of this development.

OPNsense doesn't leave you hanging when it comes to security. It delivers weekly security updates in small, timely increments to address emerging threats swiftly. Plus, it follows a fixed release cycle, dropping two major releases each year. This predictability empowers businesses to plan their upgrades proactively.

For every major release, OPNsense makes a roadmap that guides work and spells out clear goals. This careful approach makes sure that OPNsense stays a strong, reliable, and always-evolving firewall solution.

We can now take a closer look at OPNsense after briefly talking about how it originated and how it has grown. Because it would be too hard to cover everything under each heading, we will refer to your previous sense articles when we need to. There, you will be able to find a lot of information.

This article will talk about a number of things, such as:

- What is OPNsense?
- Why is the OPNsense firewall essential for network security?
- What are the basic system requirements for OPNsense?
- What steps are involved in the initial setup of OPNsense?

- What are the key elements of the OPNsense user interface?
- What are firewall rules, and why are they important?
- What is network and port forwarding work in OPNsense?
- What security features does OPNsense offer to protect a network?
- What is a VPN, and why might beginners want to set up one with OPNsense?
- What are the best plugins every OPNsense user should have?

What is OPNsense and its History?

OPNsense is an open-source, FreeBSD-based firewall and routing software developed by Deciso, a Dutch business that manufactures hardware and sells support packages for OPNsense. OPNsense is a branch of pfSense, which was forked from the FreeBSD-based m0n0wall. OPNsense went live in January of 2015.

The history of OPNsense started with the release of m0n0wall, an ambitious project that aimed to create firewall software based on FreeBSD. The main selling points of m0n0wall were compatibility with embedded PCs and older hardware and an easy-to-use web interface powered by PHP. It was a solid start, focusing on Layer 3 and Layer 4 firewalling.

However, some network and security administrators were craving more features. They wanted things like web proxying, intrusion detection, and prevention systems. Commercial firewalls were offering these features as part of a Unified Threat Management (UTM) solution.

So, in 2004, a new project was born: a fork of m0n0wall. This new kid on the block was named pfSense. As the name suggests, it utilized Packet Filter (PF) instead of IPfilter, which was its predecessor's packet filter. pfSense gained a dedicated community and constantly improved over time. Even those who had been loyal to Linux-based firewalls started making the switch to this FreeBSD-based firewall.

Both m0n0wall and pfSense coexisted for several years until 2015, when m0n0wall was discontinued. The signs of discontent were there: license changes and the project's direction left part of the pfSense community unhappy.

In 2014, a group of determined developers decided to take matters into their own hands. They forked from both pfSense and m0n0wall, giving birth to OPNsense in January 2015.

While it inherited a lot of code from its predecessors, OPNsense had a grand vision to change how things were done.

OPNsense quickly emerged as a worthy pfSense alternative, and its reputation got a significant boost when Manuel Kasper, the founder of m0n0wall, recommended his community migrate to OPNsense. It marked the beginning of one of the most exciting open-source firewall projects.

Why is the OPNsense firewall essential for network security?

Due to the abundance of valuable data, hackers have historically targeted businesses and government institutions. Nevertheless, as the boundaries between our physical and digital realms blur and remote work becomes the new normal, home networks have emerged as enticing prospects for cybercriminals.

A prominent menace to home networks is malware. An exemplary case is the Mirai botnet, a malicious software that capitalizes on vulnerable IoT devices to create 'zombies' or botnets. These botnets can then be wielded to launch colossal DDoS attacks, leading to substantial disruptions in internet services.

Another challenging adversary is ransomware, wherein hackers encrypt files and demand a ransom for their decryption. The infamous WannaCry attack in 2017 left numerous home computer users grappling with a dilemma: pay an exorbitant ransom or bid farewell to their cherished files.

In addition to malware and ransomware, phishing scams ensnare unsuspecting users into revealing personal information, while Wi-Fi hacking entails attackers gaining access to your network by exploiting weak Wi-Fi passwords. All these risks underscore the critical need for a robust home network security system.

Your quest to enhance cybersecurity may start with other open-source or paid firewall solutions. However, you might encounter issues as it can introduce instability into your network.

Being a powerful open-source firewall and routing platform, OPNsense provides ways to combat these threats and improve home network security. OPNsense can detect and block unwanted behavior by evaluating incoming and outgoing communications, defending against malware and lowering IoT-related risks. Intrusion Detection and Prevention Systems (IDPS) can detect malware patterns and behaviors, providing an additional layer of protection. OPNsense prevents access to known harmful websites in order to combat ransomware. Frequent data backups help to lessen the impact of ransomware. OPNsense stops phishing websites with features like DNS filtering, and email filtering helps detect and quarantine phishing communications. Enhancing Wi-Fi security using strong passwords and, if available, WPA3 support offers an extra degree of protection. The VPN capabilities of OPNsense provide safe remote access, while regular software upgrades keep the system secure. A complete security policy must include user education and community support. You may efficiently protect your home network against various cyber attacks by leveraging these solutions and OPNsense's characteristics, resulting in a secure digital environment in this age of distant work and growing security problems.

What are the basic system requirements for OPNsense?

Having highlighted the significance of OPNsense in bolstering network security, it's time to shift our focus to understanding the fundamental system requirements necessary to begin your journey with this robust open-source firewall. OPNsense is packed with features, including a stateful firewall, an intrusion detection system (IDS), and web content filtering. OPNsense can be deployed on a variety of hardware platforms, from physical servers to virtual machines.

Here are the fundamental system requirements for OPNsense:

- *Processor*: 1 GHz dual-core CPU
- *Memory*: 4 GB RAM
- *Storage*: 40 GB SSD or HDD (more storage may be required for additional features or packages.)
- *Network interface*: 1 or more network interfaces

In addition to these basic requirements, there are a few other things to keep in mind when choosing hardware for OPNsense:

- Use a 64-bit CPU.
- Use an SSD for the OPNsense installation drive. This will improve performance and startup times.
- Use a dedicated network interface for the OPNsense WAN port. This will help to isolate OPNsense from the rest of your network and improve security.
- Consider using a more powerful CPU and more memory if you plan on using a lot of features or packages.

What steps are involved in the initial setup of OPNsense?

Because the installation of OPNsense cannot be adequately described using a single heading, we will provide an overview of the installation process and then redirect you to additional resources that provide detailed instructions.

Here is a step-by-step guide to the initial setup of OPNsense: Prerequisites for OPNsense Installation:

- A computer with an internet connection
- A USB drive to install OPNsense from
- A physical server or virtual machine to install OPNsense on

Basic steps to follow for installing OPNsense are given below:

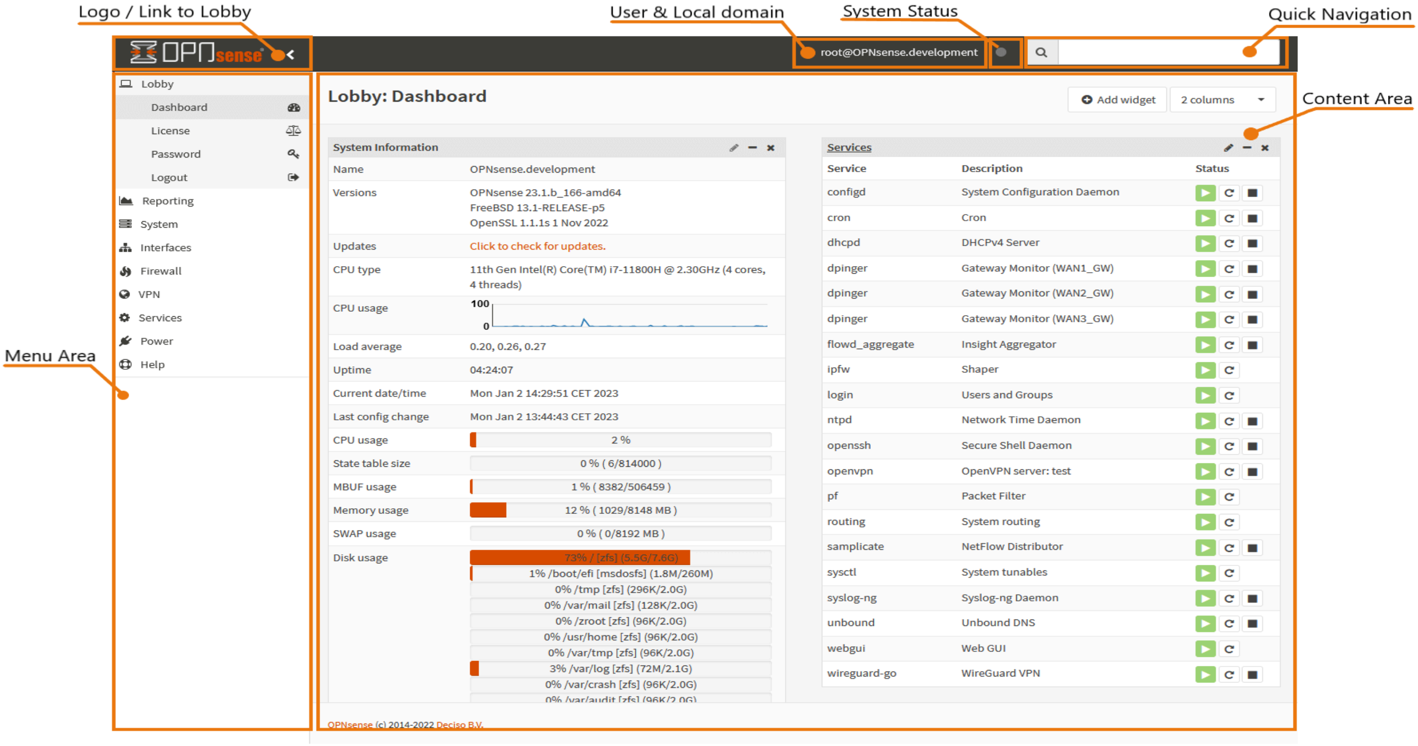
1. Download the OPNsense ISO image from the official website.
2. Create a bootable USB drive using the ISO image.
3. Boot the server or virtual machine from the bootable USB drive.
4. Select the "**Install**" option and follow the on-screen instructions.
5. Once the installation is complete, reboot the server or virtual machine.
6. Open a web browser and navigate to the OPNsense web interface at `https://opnsense_ip_address:443`.
7. Log in to the web interface using the OPNsense default password and username:
    - Username: **root**
    - Password: **opnsense**

8. Change the default password immediately.
9. Configure the basic OPNsense settings, such as the hostname, time zone, and network interfaces.
10. Create firewall rules to allow and deny traffic to and from your network.
11. Enable the IDS to detect and block malicious traffic.
12. Configure web content filtering to block access to unwanted websites.
13. Monitor your OPNsense logs for suspicious activity.

What are the key elements of the OPNsense user interface?

The OPNsense user interface is designed to be easy to use and navigate, even for users with no prior experience. The main elements of the OPNsense user interface are:

- ***Menubar***: The menubar at the top of the screen provides access to all of the OPNsense features.
- ***Main content area***: The main content area in the center of the screen displays the current page or view.
- ***Quick Navigation***: When you configure and manage your network security, quick navigation will assist you in finding OPNsense's web interface parts.



Lobby: Dashboard

System Information

Name	OPNsense.development
Versions	OPNsense 23.1.b_166-amd64 FreeBSD 13.1-RELEASE-p5 OpenSSL 1.1.1s 1 Nov 2022
Updates	Click to check for updates.
CPU type	11th Gen Intel(R) Core(TM) i7-11800H @ 2.30GHz (4 cores, 4 threads)
CPU usage	100 0
Load average	0.20, 0.26, 0.27
Uptime	04:24:07
Current date/time	Mon Jan 2 14:29:51 CET 2023
Last config change	Mon Jan 2 13:44:43 CET 2023
CPU usage	2 %
State table size	0 % (6/814000)
MBUF usage	1 % (8382/506459)
Memory usage	12 % (1029/8148 MB)
SWAP usage	0 % (0/8192 MB)
Disk usage	73% / [zfs] (5.5G/7.6G) 1% /boot/efi [msdosfs] (1.8M/260M) 0% /tmp [zfs] (296K/2.0G) 0% /var/mail [zfs] (128K/2.0G) 0% /zroot [zfs] (96K/2.0G) 0% /usr/home [zfs] (96K/2.0G) 0% /var/tmp [zfs] (96K/2.0G) 3% /var/log [zfs] (72M/2.1G) 0% /var/crash [zfs] (96K/2.0G) 0% /var/audit [zfs] (96K/2.0G)

Services

Service	Description	Status
configd	System Configuration Daemon	▶ ↻ ■
cron	Cron	▶ ↻ ■
dhcpd	DHCPv4 Server	▶ ↻ ■
dpinger	Gateway Monitor (WAN1_GW)	▶ ↻ ■
dpinger	Gateway Monitor (WAN2_GW)	▶ ↻ ■
dpinger	Gateway Monitor (WAN3_GW)	▶ ↻ ■
flowd_aggregate	Insight Aggregator	▶ ↻ ■
ipfw	Shaper	▶ ↻
login	Users and Groups	▶ ↻
ntpd	Network Time Daemon	▶ ↻ ■
openssh	Secure Shell Daemon	▶ ↻ ■
openvpn	OpenVPN server: test	▶ ↻ ■
pf	Packet Filter	▶ ↻
routing	System routing	▶ ↻
samplicate	NetFlow Distributor	▶ ↻ ■
sysctl	System tunables	▶ ↻
syslog-ng	Syslog-ng Daemon	▶ ↻ ■
unbound	Unbound DNS	▶ ↻ ■
webgui	Web GUI	▶ ↻
wireguard-go	WireGuard VPN	▶ ↻ ■

OPNsense (c) 2014-2022 Deciso B.V.

Figure 1. *OPNsense User Interface*

The OPNsense user interface is highly customizable. Users can change the layout of the screen, the colors of the interface, and even the default language.

Here are some of the critical elements of the OPNsense user interfaces in the menu bar.

- ***Lobby***: The OPNsense Lobby menu is a special menu that provides access to a few basic features, such as the dashboard, license, password, and logout. It is designed to be a quick and easy way to access these features without having to navigate through the main menu system.
- ***Dashboard***: This menu provides a high-level overview of the system status, including information about CPU usage, memory usage, and network traffic.
- ***Reporting***: This menu provides access to tools for generating reports about the OPNsense system and network, such as firewall reports and traffic reports.
- ***System***: This menu provides access to settings for the OPNsense system, such as the hostname, time zone, and networking.
- ***Interfaces***: The Interfaces menu in OPNsense provides access to settings for the network interfaces on your system. You can use this menu to configure the IP addresses, routing, and other settings for your network interfaces.
- ***Firewall***: This menu provides access to settings for the OPNsense firewall, such as rules, NAT, and port forwarding.
- ***VPN***: This menu provides access to settings for the OPNsense VPN server, such as protocols, users, and certificates.
- ***Services***: This menu provides access to settings for various OPNsense services, such as the DHCP server, DNS server, and web server.
- ***Power***: The Power menu in OPNsense provides access to options for shutting down or restarting your system. You can also use this menu to schedule a shutdown or restart.
- ***Help***: This menu provides access to the OPNsense documentation and community forum.

What are Firewall Rules, and Why are They Important?

Your firewall rules serve as guards, keeping out intruders and preventing damage to your network. You must fully understand the significance of these rules to provide adequate network security:

- **The Gatekeepers of Network Security**: Imagine your network as a majestic castle, and the firewall rules as the vigilant gatekeepers stationed at the castle's gates. Their role is to determine who can enter and who must be turned away.
- **Guidelines for Network Traffic**: Firewall rules provide clear guidelines for network traffic. They specify what's allowed and what's blocked, ensuring that only the right connections are permitted. This helps maintain the integrity of your network.
- **Defense Against Unwanted Guests**: As a means of keeping unwelcome visitors out of your network, firewall rules serve an important purpose.Creating rules to stop unauthorized access will stop bad people from taking advantage of security holes or getting in without permission.
- **Thwarting Various Threats**: Firewall rules are your first line of defense against a variety of cyber threats. They can thwart denial-of-service attacks, port scanning attempts, and intrusion attacks. With the right rules in place, you can significantly reduce your network's vulnerability.
- **Managing Ports and Protocols**: Firewall rules offer control over the use of specific ports and protocols. For example, you can block known malware-associated ports or limit access to critical services. This level of control enhances your network's security posture.
- **Filtering Traffic for Safety**: You can filter traffic based on certain factors, such as content, with these rules. Firewall rules help you get rid of possible threats by blocking dangerous websites or applying limits to certain programs.
- **Guard Against Denial-of-Service Attacks**: Denial-of-service (DoS) attacks aim to flood your network with traffic, rendering it unavailable. Firewall rules can be configured to detect and mitigate these attacks by limiting incoming traffic rates or blocking suspicious sources.
- **Visibility and Control**: You can see what is going on in the network thanks to firewall rules, which let you keep an eye on things and figure out what is going on. This

information is beneficial for finding strange things and handling possible security problems.

- **Compliance and Regulations**: Many industries have regulatory requirements for network security. Firewall rules help you align with these standards, such as PCI DSS or HIPAA, by safeguarding sensitive data and demonstrating compliance.

Firewall rules protect your network by enforcing rules and letting only authorized traffic into your digital world. When you carefully write and follow these rules, you strengthen your defenses and are ready to protect your network from all the threats that live in the digital world.

What is Network and Port Forwarding in OPNsense?

Network forwarding allows you to direct traffic from your computer's Internet connection to another device, such as a server, when someone visits your website. Port forwarding is a type of network forwarding that allows you to redirect traffic from a specific port on one network interface to a specific port on another network interface. For example, if you have a home network with a router and a gaming console, you can configure port forwarding on the router to send traffic on port 80 (which is the port that web servers typically use) to the gaming console. This will allow you to play online games that require port 80 to be open. Network forwarding is the process of routing traffic from one network interface to another.

There are many situations where users might need to configure network and port forwarding. Here are a few examples:

- To host a website or web application
- To run a gaming server
- To use peer-to-peer software
- To access remote devices, such as security cameras or NAS devices
- To use VoIP software, such as Skype or Discord

It is important to follow some best practices when configuring your network and port forwarding to protect your network from potential security risks, including the following:

- Only forward ports that you need to forward
- Use strong passwords for all of your devices.

- Keep your software up to date.
- Use a firewall to filter traffic on your network.

What security features does OPNsense offer to protect a network?

Keeping your network secure is more crucial than ever in today's interconnected world. You can protect your network from threats and vulnerabilities with OPNsense. It is one of the best multipurpose open-source firewall and routing platforms. OPNsense security features are as follows:

- **Stateful Firewall**: When it comes to protecting your network from unwanted visitors, OPNsense's stateful firewall is your first and best line of defense. It thoroughly examines all incoming and outgoing data and discards any packets that do not conform to its rules. Firewall rules can be set up quickly and easily, even by those with no prior experience, thanks to the intuitive web interface.
- **IDPS (Intrusion Detection and Prevention System)**: OPNsense's Intrusion Detection and Prevention System (IDPS) is a watchful protector that keeps an eye out for attacks like port scans and DOS attacks in network traffic. This advanced system can detect potential threats and take proactive measures to protect your network, for example, blocking traffic or sending alerts to administrators.
- **VPN (Virtual Private Networking)**: There are several VPN protocols that OPNsense supports, such as IPsec, OpenVPN, and WireGuard. This lets you set up safe tunnels between your devices and the OPNsense firewall. This feature lets you access network resources from afar, keeping your data safe from being hacked or intercepted. Configuration wizards simplify the setup of VPN connections, making it easy to get started.
- **Web Content Filtering**: OPNsense equips you with powerful web content filtering capabilities, enabling you to block access to malicious and unwanted websites. This feature acts as a shield against malware, phishing attacks, and various online threats. Configuring web content filtering rules is straightforward through the user-friendly web interface. Zenarmor, the most popular OPNsense plugin, uses artificial intelligence (AI)-powered threat intelligence systems to protect users from malicious content on the web.

- **2FA (Two-Factor Authentication)**: To make security even stronger, OPNsense supports 2FA, which adds another level of security to user accounts. With 2FA, users must enter both their password and a code from their phone to log in. This robust authentication mechanism thwarts unauthorized access, even if passwords are compromised.

OPNsense's popularity stems from the fact that it is designed with the user in mind. With its user-friendly web-based interface, extensive documentation, and community support, users can rest assured that their networks are well protected. With these safeguards in place, you can feel safe knowing your network is protected from today's vulnerabilities and threats.

What is a VPN, and why might beginners want to set up one with OPNsense?

VPN is an abbreviation for Virtual Private Network. While you use the internet, a VPN operates in the background, keeping you safe and preserving your privacy. It's like having a digital bodyguard on call at all times, whether you're at home, at work, or using public Wi-Fi.

When you use a VPN, all of your data is encrypted from the moment it leaves your device. Your data is sent through a secure intermediate step known as a VPN server. This server can conceal your personal information. It may pretend that you are checking in from somewhere else in the world, allowing you to access geo-restricted services.

OPNsense beginners might want to set up a VPN with OPNsense for several compelling reasons. First and foremost, VPNs enhance security by adding an extra layer of protection to your internet connection. Let's delve into the additional reasons why beginners might opt to set up a VPN with OPNsense:

- VPNs offer an extra layer of protection to your internet connection, making it more difficult for cybercriminals to access the information stored on your device.
- Beginners can use a VPN to encrypt their internet traffic when connecting to public Wi-Fi networks. It secures users by protecting sensitive data from potential surveillance by malicious actors on the same network.

- By hiding your IP address and location, a VPN can help you retain your privacy by making it more difficult for marketers and other third parties to monitor your online behavior.
- A VPN can facilitate the circumvention of content restrictions imposed by geographical boundaries. Users can access websites or streaming services that are inaccessible because their internet service provider may have blocked them by using a VPN.
- Some ISPs (Internet Service Providers) throttle or restrict Internet traffic. VPNs can protect beginner users from bandwidth limitations by ISPs.
- Some internet service providers restrict or slow down certain kinds of online activity. If you're just starting online, a VPN might help you avoid having your connection slowed down by your ISP.
- Setting up a VPN using OPNsense may be an excellent learning experience for newbies interested in networking, security, and system administration.

Configuring a VPN on OPNsense is easy thanks to the use of plugins like OpenVPN, WireGuard, and IPsec. These protocols provide not just strong encryption but also extra safety measures.

OPNsense makes VPN configuration easy for newcomers by providing thorough documentation and tutorials.

What are the best plugins every OPNsense user should have?

OPNsense offers a wide array of plugins, each designed to enhance the functionality and capabilities of this open-source firewall and routing platform. These plugins cater to various needs, from network security and monitoring to VPN solutions and content filtering.

While the selection of OPNsense plugins depends on specific requirements, certain plugins stand out for their versatility and utility. Whether you're looking to bolster network security, improve performance, or enhance usability, these are the essential OPNsense plugins that every user should consider integrating into their system.

Here's a list of some noteworthy OPNsense plugins that can elevate your network management experience:

1. Zenarmor
2. WireGuard
3. NGINX
4. Rspamd
5. FreeRADIUS
6. OpenVPN
7. Snort
8. Suricata
9. Tailscale
10. HAProxy

1. Zenarmor

The advanced OPNsense firewall plugin Zenarmor NGFW, created by Zenarmor, offers cutting-edge next-generation features. This all-software instant firewall can be seamlessly deployed virtually anywhere. Zenarmor is currently compatible with OPNsense, FreeBSD, pfSense software, and Ubuntu Linux.

Key features of Zenarmor include:

- **Application control**: Zenarmor NGFW allows you to control which applications are allowed to access the internet and which resources they can access. This can help to prevent malware and unauthorized access to sensitive data.
- **Network analytics**: Zenarmor provides real-time network traffic analysis and reporting. This can help you identify and investigate suspicious activity.
- **TLS inspection**: Zenarmor can inspect encrypted TLS traffic for malware and other threats. This is important because many malware attacks now use TLS encryption to evade detection.
- **Web filtering**: Zenarmor can be used to block access to malicious and inappropriate websites.
- **User filtering**: Zenarmor can be used to filter traffic based on user, group, or device.
- **Policy-based filtering**: Zenarmor can be used to create and enforce policies based on a variety of factors, such as application, user, group, or device.

- **Reporting**: Zenarmor provides a variety of reports that can help you monitor and analyze your network traffic.

Zenarmor conveniently utilizes the OPNsense package system for hassle-free updates. You can install it through the OPNsense web interface or via SSH or local system access through the command line interface. Once installed, you'll find the Zenarmor menu in the OPNsense web interface's left sidebar.

2. WireGuard

WireGuard is a VPN (Virtual Private Network) protocol known for its simplicity and speed, harnessing modern cryptographic techniques. This versatile protocol can be configured in two main modes: as a Road Warrior WireGuard setup for remote clients or as a Site-to-Site setup, facilitating the secure connection of two networks. Unlike its counterparts, IPsec and OpenVPN, WireGuard stands out for its commitment to delivering a faster and less complex VPN solution. It is renowned for its ease of configuration, especially on the OPNsense platform, making it an attractive choice for users ranging from individuals at home to small office and business environments.

Some of the Key Features of WireGuard are given below:

- Road Warrior setup for remote clients or Site-to-Site setup for network connections.
- Simple configuration and setup on OPNsense
- Utilizes modern cryptography and network code for encryption.
- Aims for speed, simplicity, and efficiency compared to IPsec and OpenVPN.

The most notable benefits of the WireGuard plugin in Opnsense can be listed as:

- Fast and secure VPN connections with modern cryptography.
- Easy configuration and setup on OPNsense.
- Designed to be faster, simpler, and more efficient than IPsec and OpenVPN.

Here are some use cases for WireGurad VPN:

- Providing fast and secure VPN connections for remote employees.
- Connecting two networks securely.
- Enhancing network security for home, small office, and business users

3. NGINX

NGINX is a versatile plugin for OPNsense that extends its capabilities in local website hosting, load balancing, reverse proxy, and web application firewall (WAF) functionalities. Some of the key features and use cases of NGINX are given below:

- **Local Website Hosting**: NGINX enables the hosting of websites directly from OPNsense, though caution is advised due to security considerations. Suitable for technically savvy home users seeking power savings and control
- **Load Balancing**: NGINX can distribute incoming traffic across a group of servers, with default upstream verification for added reliability.
- **Reverse Proxy**: NGINX serves as a straightforward reverse proxy solution, incorporating web application firewall and SSL capabilities. It facilitates proxying requests to pre-configured upstream servers.
- **Web Application Firewall (WAF)**: NGINX can function as a WAF through the NAXSI module, enhancing security.

NGINX brings additional functionality to OPNsense, offering users local website hosting, load balancing, reverse proxy, and WAF capabilities. However, it's important to note that certain features may require advanced expertise, making them better suited for experienced users. Installation and configuration guidance for NGINX on OPNsense can be found in the official OPNsense documentation.

4. Rspamd

Rspamd is an advanced spam filtering and email scanning system that can be integrated with OPNsense, a popular open-source firewall and routing platform. When implemented as a plugin in OPNsense, Rspamd provides powerful email security features.

Key Features and Uses of Rspamd are as follows:

- **Spam Filtering**: Rspamd specializes in robust spam detection and filtering, helping to keep unwanted and potentially harmful emails out of your inbox.
- **Malware Scanning**: It can scan emails for malware and malicious attachments, providing an additional layer of protection against cyber threats.
- **Custom Policies**: Users can configure custom filtering policies and rules to tailor the email security settings to their specific needs.

- **Greylisting**: Rspamd supports greylisting, a technique that helps reduce spam by temporarily rejecting emails from unknown senders. Rspamd complements OPNsense by bolstering email security. It's particularly useful for organizations and individuals looking to protect their email systems from spam, phishing attempts, and malware.

5. FreeRADIUS

FreeRADIUS is an open-source, high-performance Remote Authentication Dial-In User Service (RADIUS) server that can be integrated seamlessly with OPNsense. This integration enhances network authentication and security.

Some of the key features and use cases of FreeRADIUS are given below:

- **User Authentication**: FreeRADIUS is primarily used for authenticating users who connect to a network or services like VPNs, Wi-Fi, and more. It ensures that only authorized users gain access.
- **Accounting**: It tracks usage data, providing detailed accounting and auditing capabilities, which are crucial for billing and compliance.
- **Multi-Protocol Support**: FreeRADIUS supports a variety of authentication protocols, including EAP (Extensible Authentication Protocol), PAP (Password Authentication Protocol), and more.
- **LDAP Integration**: Integration with Lightweight Directory Access Protocol (LDAP) and Active Directory for centralized user management is possible, simplifying administration.

FreeRADIUS enhances OPNsense by providing robust user authentication and accounting capabilities. It's particularly valuable for organizations that require secure user access control to their networks and services. FreeRADIUS is essential for businesses, educational institutions, and organizations of all sizes that need to manage user access and authentication effectively. It's indispensable for secure network access, VPN connections, and Wi-Fi access control.

6. OpenVPN

OpenVPN is a VPN solution that may be easily integrated with the open-source firewall and routing software OPNsense. Collectively, they constitute a safe and flexible method of establishing distant connections. Some of the key features and use cases of OpenVPN are given below:

- **Remote Access**: OpenVPN facilitates secure remote access to a network, enabling users to connect to their organization's resources or home network from virtually anywhere.
- **Site-to-Site VPN**: It supports Site-to-Site VPN connections, allowing different networks (e.g., branch offices) to communicate securely over the internet as if they were on the same local network.
- **Strong Encryption**: OpenVPN employs robust encryption protocols to protect data transmission, ensuring the confidentiality and integrity of information.
- **User Authentication**: Users can be required to authenticate themselves before accessing the network, enhancing security.
- **Multi-Platform Support**: OpenVPN is compatible with various operating systems and devices, making it versatile for both personal and enterprise use.

OpenVPN is a fantastic addition to OPNsense since it allows for safe remote connectivity. It guarantees the greatest levels of security while allowing users to access network resources, collaborate, and work remotely.

OpenVPN on OPNsense is invaluable for businesses, organizations, and individuals who require secure remote access to their networks. It's suitable for remote employees, remote branch offices, or anyone seeking a secure and versatile VPN solution.

7. Snort

As an Intrusion Prevention System (IPS), Snort can be added to OPNsense as a plugin. Its main function is to quickly find and stop security threats through deep packet inspection. Some of the key features and use cases of Snort are given below

- **IPS Capabilities**: Snort operates as a robust IPS system, capable of identifying and thwarting security threats effectively.

- **Alerts**: Users can access alerts generated by the IDS/IPS system in the "Alerts" tab. This provides crucial details about detected events or threats, aiding in rapid response.
- **Custom Configurations**: OPNsense supports personalized Snort configurations using a specific file format. Users can add custom options by creating a template file.
- **Rulesets**: Snort allows users to choose from a variety of intrusion detection rules (referred to as rulesets) tailored to monitor or block specific network traffic types. These rulesets can be automatically updated to maintain relevance. Some rulesets are freely available, while others require a subscription.

Snort significantly enhances OPNsense's capabilities by delivering a comprehensive IPS system that identifies and prevents security threats.

Snort is great in many situations. For example, it improves the network security of home users, small businesses, and businesses by monitoring and blocking network traffic well, letting you make your own configurations, and giving you a lot of ruleset options.

8. Suricata

Suricata is a free and open-source network intrusion detection system (IDS) and intrusion prevention system (IPS). It is a high-performance and scalable solution that can be used to detect and block a wide range of malicious network traffic, including malware, exploits, and denial-of-service attacks.

Suricata is available as a plugin for OPNsense, which makes it easy to set up and manage. To install the Suricata plugin, simply go to the System > Plugins page in the OPNsense web interface and search for "Suricata". Once installed, you can enable and configure Suricata from the Firewall > IDS/IPS page.

Suricata can be used in a variety of ways to protect your OPNsense firewall. For example, you can use Suricata to:

- Detect and block malicious traffic before it reaches your network
- Monitor your network for suspicious activity
- Identify and track known attackers
- Generate reports on security incidents

Suricata is a powerful tool that can help to improve the security of your OPNsense firewall. However, it is important to note that it can be resource-intensive, so it is important to make sure that your hardware is powerful enough to run it effectively.

Here are some of the key features of Suricata:

- High performance and scalability
- Wide range of detection capabilities, including malware, exploits, and denial-of-service attacks
- Flexible configuration options
- Support for a variety of rule sets
- Integration with other security tools, such as firewalls and SIEM systems

9. Tailscale

Tailscale is a secure, zero-trust, and modern VPN solution that can be seamlessly integrated with OPNsense. This integration enhances network security, accessibility, and management. Some of the key features and use cases of Tailscale are given below:

- **Mesh VPN connectivity**: Tailscale allows OPNsense to connect to other Tailscale-enabled devices using a mesh VPN topology. This means that devices can communicate with each other directly without the need for a central server. This can improve performance and reliability, and it also makes it easier to set up and manage VPNs.
- **Easy to use**: Tailscale is designed to be easy to use, even for people with no prior experience with VPNs. Once the Tailscale plugin is installed and configured on your OPNsense firewall, you can simply install the Tailscale client on your devices and connect them to your Tailscale network.
- **Secure**: Tailscale uses WireGuard, a fast and secure VPN protocol. It also uses end-to-end encryption to protect your data in transit.
- **Scalable**: Tailscale can scale to support a large number of devices. It is a good choice for organizations of all sizes, from small businesses to large enterprises.

The Tailscale plugin can enhance the capabilities of OPNsense in the following ways:

- **Provide easy-to-use VPN connectivity**: Tailscale makes it easy to set up and manage VPNs for remote workers, site-to-site VPNs, and other use cases.

- **Improve performance and reliability**: Tailscale's mesh VPN topology can improve performance and reliability for VPN connections.
- **Increase flexibility**: Tailscale can be used to create a variety of VPN configurations, such as remote access VPNs, site-to-site VPNs, and mesh VPNs.

10. HAProxy

HAProxy is a high-performance, open-source load balancer and reverse proxy solution that can be seamlessly integrated with OPNsense. This integration enhances web traffic management, distribution, and security. Some of the key features and use cases of HAProxy are given below

- **Load balancing**: HAProxy can be used to distribute traffic across multiple servers. This can improve performance and reliability, and it can also help reduce the load on individual servers.
- **Reverse proxying**: HAProxy can be used as a reverse proxy to direct traffic to specific servers based on the request. This can be used to improve security and performance, and it can also be used to implement complex web applications.
- **Content caching**: HAProxy can be used to cache content, which can improve performance and reduce bandwidth usage.
- **SSL termination**: HAProxy can be used to terminate SSL connections, which can improve performance and security.
- **Health checking**: HAProxy can be used to monitor the health of servers and automatically switch traffic to healthy servers.
- **Session persistence**: HAProxy can be used to keep users connected to the same server for the duration of their session. This can improve performance and reliability.

HAProxy enhances OPNsense by providing advanced web traffic management capabilities. It ensures that web services remain available, scalable, and secure, making it suitable for organizations of all sizes.

OPNsense Firewall Installation

`OPNsense` is a FreeBSD-based open source firewall distribution. OPNsense, a fork of Pfsense, was released in 2015. In addition to the Firewall, there are DHCP servers, DNS servers, VPNs, and other services available. Especially Zenarmor `os-sensei` plugin which provides application control and web filtering features is very useful for the administrators to protect their networks against cyberattacks. It can be installed on a physical server as well as a virtual machine.

`Proxmox VE` is an excellent open-source enterprise virtualization platform built on `Debian` Linux.

You can easily manage VMs and containers, highly available clusters, and integrated disaster recovery tools using the integrated web-based user interface. `PVE` has a significant advantage over other virtualization solutions in terms of simplicity. Even inexperienced users can set it up and install it in minutes. Most importantly, because it runs on Debian, all Linux experience is required.

OPNsense runs well in a KVM-based VM running on a Proxmox VE server. In this OPNsense installation on the Proxmox VE tutorial, we will explain why you should install OPNsense and walk you through a basic installation of `OPNsense 21.1` to get you started by following the next steps given below:

1. Checking hardware requirements of OPNsense firewall
2. Downloading OPNsense image
3. Uploading OPNsense ISO File to Proxmox VE
4. Creating a Virtual Machine on Proxmox VE
5. Setting Network Configuration of the OPNsense Virtual Machine on Proxmox VE
    i. Creating Linux Bridge
    ii. Adding Network Devices to OPNsense VM on Proxmox
6. Installing OPNsense
    i. Network Device Assignments for OPNsense Firewall
    ii. IP Address Settings for OPNsense Firewall
    iii. Updating OPNsense Firewall on CLI
    iv. Accessing the OPNsense Web GUI
    v. Initial Configuration of the OPNsense Firewall
    vi. Disable Network Hardware Off-loading on OPNsense Firewall

Why You Should Install OPNsense

By installing the OPNsense firewall to protect your network, you will get the following benefits of the OPNsense.

- OPNsense has significant advantages over competitors, such as forward caching proxy, traffic shaping, intrusion detection, and simple OpenVPN client setup.
- The emphasis on security in OPNsense results in unique features such as the ability to use LibreSSL instead of OpenSSL (selectable in the GUI) and a custom version based on HardenedBSD.
- OPNsense's robust and dependable update mechanism enables it to provide critical security updates on time.

For more information about the OPNsense features, please refer to the Best Open Source Firewalls article.

1. OPNsense Hardware Requirements

Before installing the OPNsense firewall, you should verify the hardware requirements for the installation. You can review the requirements located on the official website. OPNsense is available for `x86-64 (amd64)` bit microprocessor architectures. Although OPNsense supports a wide range of devices from embedded systems to rack-mounted servers, the hardware must be capable of running `64-bit` operating systems.

Minimum hardware requirements of OPNsense

At the time of the writing, minimum requirements are given as below. If you install OPNsense on a device with these specifications, you can not use features that require disk writes, e.g. a caching proxy (cache) or intrusion detection and prevention.

Type	Description
Processor	1 GHz dual-core CPU
RAM	2 GB
Install method	Serial console or video (VGA)
Install target	SD or CF card with a minimum of 4 GB, use nano images for installation.

Table 1: *Minimum hardware requirements*

Reasonable hardware requirements of OPNsense

If you install OPNsense on a device with these specifications, you can use every standard feature of the OPNsense. However, you may encounter some problems with high loads or lots of users.

Type	Description
Processor	1 GHz dual-core CPU
RAM	4 GB
Install method	Serial console or video (VGA)
Install target	40 GB SSD, a minimum of 2 GB memory is needed for the installer to run.

Table 2: *Reasonable hardware requirements*

Recommended hardware requirements of OPNsense

If you install OPNsense on a device with these specifications, you can use every standard feature of the OPNsense without any problem.

Type	Description
Processor	1.5 GHz multi-core CPU
RAM	8 GB
Install method	Serial console or video (VGA)
Install target	120 GB SSD

Table 3: *Recommended hardware requirements*

Virtual environment requirements

To install the OPNsense on a virtual environment such as Proxmox VE or Virtual Box, minimum hardware requirements are given below:

Type	Description
Processor	1 or more virtual cores
RAM	The minimum required RAM is 2 GB
Install method	ISO
Install target	Minimum recommended virtual disk size of 8GB

Table 4: *Minimum hardware requirements for virtual environment*

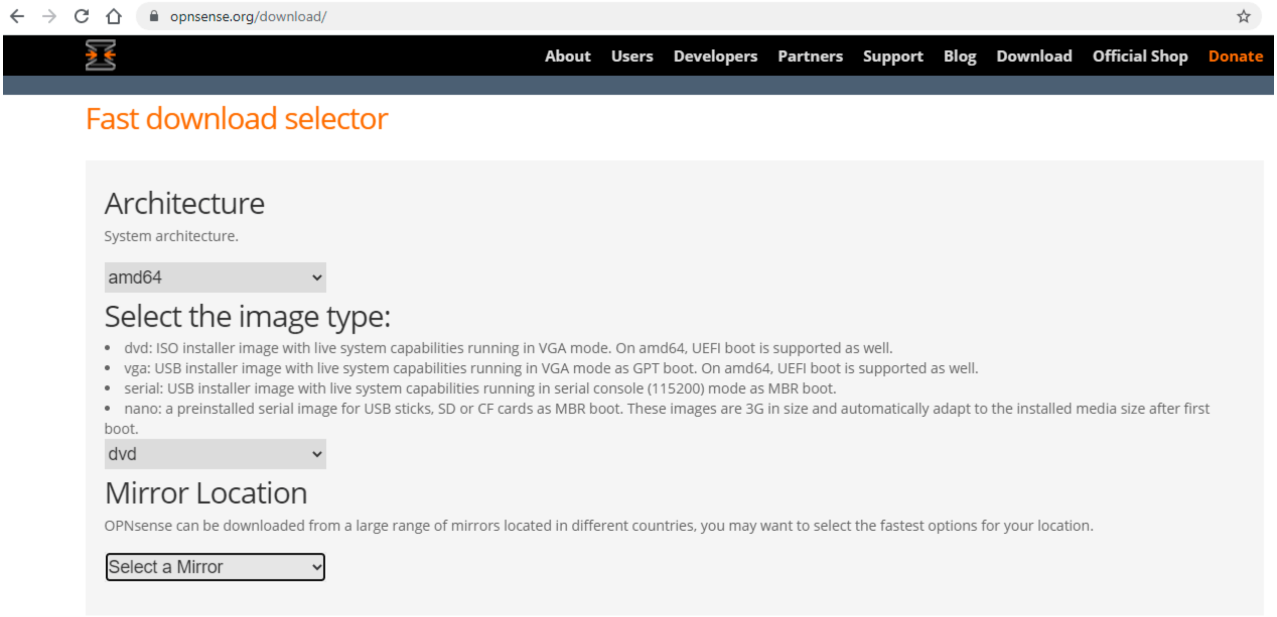
⚠️ **CAUTION**

Beware that some features have a massive impact on hardware dimensioning. For example, Captive Portal features is a CPU-intensive feature and Squid is heavily reliant on CPU load and disk-cache writes.

Now that you've checked if your system is compatible with OPNsense, let's get started with the OPNsense setup guide.

2. Downloading OPNsense image

Now, you can go to the official OPNsense Download page. Installing OPNsense on a virtual machine can be done by using the DVD ISO image. So, download the DVD `ISO` image from the OPNsense mirror site which is closest to you.



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.

Select a Mirror

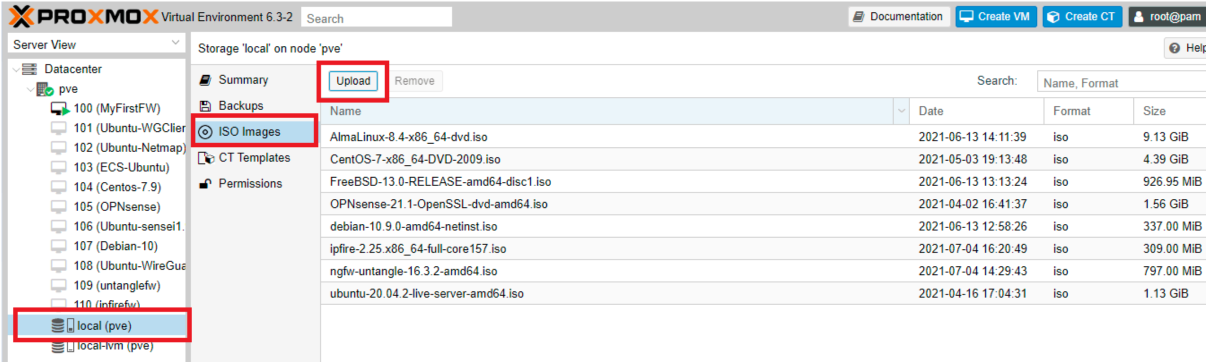
Figure 1. *Downloading OPNsense DVD ISO file*

After downloading the `bzip` compressed ISO file `(OPNsense-21.1-OpenSSL-DVD-amd64.iso.iso.bz2)`, uncompress it to your local disk.

3. Upload OPNsense ISO File to Proxmox VE

To start the installation of the OPNsense on the Proxmox environment, you must upload the OPNsense ISO image from your local disk to the Proxmox node. You can easily upload the ISO file to your Proxmox VE system by following the next instructions.

1. Connect your Proxmox VE Web interface(such as `https://192.168.0.100:8006`) using your favorite browser and log in as root.
2. Navigate to `Datacenter` -> `pve/node` -> `local disk (pve)` -> `ISO Images`

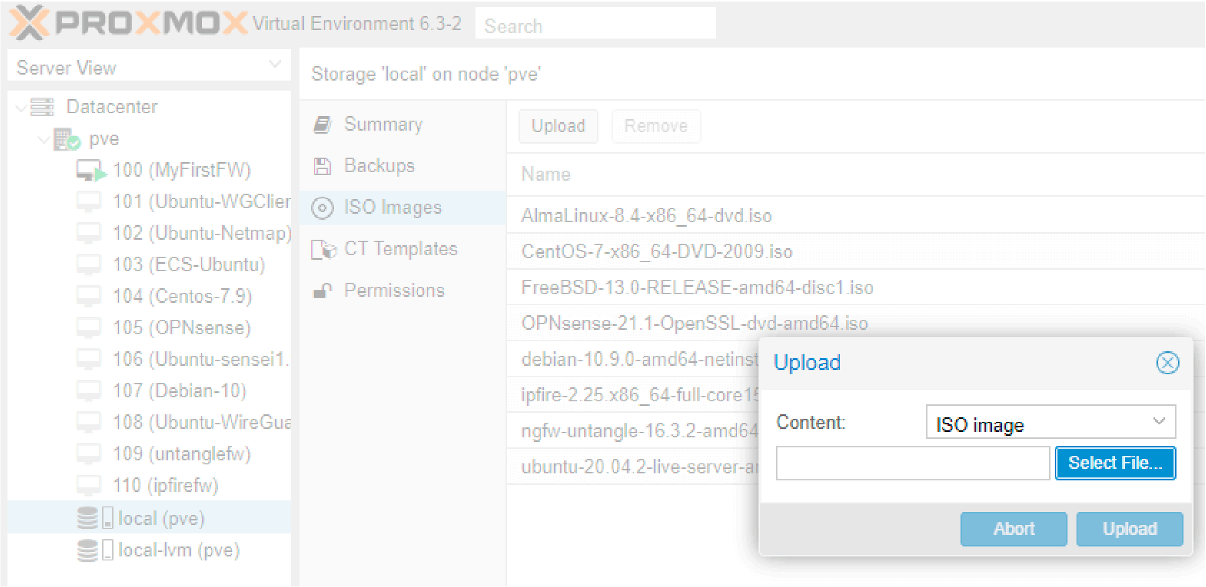


Name	Date	Format	Size
AlmaLinux-8.4-x86_64-dvd.iso	2021-06-13 14:11:39	iso	9.13 GiB
CentOS-7-x86_64-DVD-2009.iso	2021-05-03 19:13:48	iso	4.39 GiB
FreeBSD-13.0-RELEASE-amd64-disc1.iso	2021-06-13 13:13:24	iso	926.95 MiB
OPNsense-21.1-OpenSSL-dvd-amd64.iso	2021-04-02 16:41:37	iso	1.56 GiB
debian-10.9.0-amd64-netinst.iso	2021-06-13 12:58:26	iso	337.00 MiB
ipfire-2.25.x86_64-full-core157.iso	2021-07-04 16:20:49	iso	309.00 MiB
ngfw-untangle-16.3.2-amd64.iso	2021-07-04 14:29:43	iso	797.00 MiB
ubuntu-20.04.2-live-server-amd64.iso	2021-04-16 17:04:31	iso	1.13 GiB

Figure 2. *Uploading OPNsense ISO image to Proxmox VE node*

3. Click the `Upload` button.

4. Select the OPNsense ISO image from your local disk to upload.



Name
AlmaLinux-8.4-x86_64-dvd.iso
CentOS-7-x86_64-DVD-2009.iso
FreeBSD-13.0-RELEASE-amd64-disc1.iso
OPNsense-21.1-OpenSSL-dvd-amd64.iso
debian-10.9.0-amd64-netinst
ipfire-2.25.x86_64-full-core15
ngfw-untangle-16.3.2-amd64
ubuntu-20.04.2-live-server-a

Content: ISO image

Figure 3. *Selecting OPNsense ISO image from local disk to upload Proxmox VE*

5. Click the `Upload` button.

💡 **TIP**

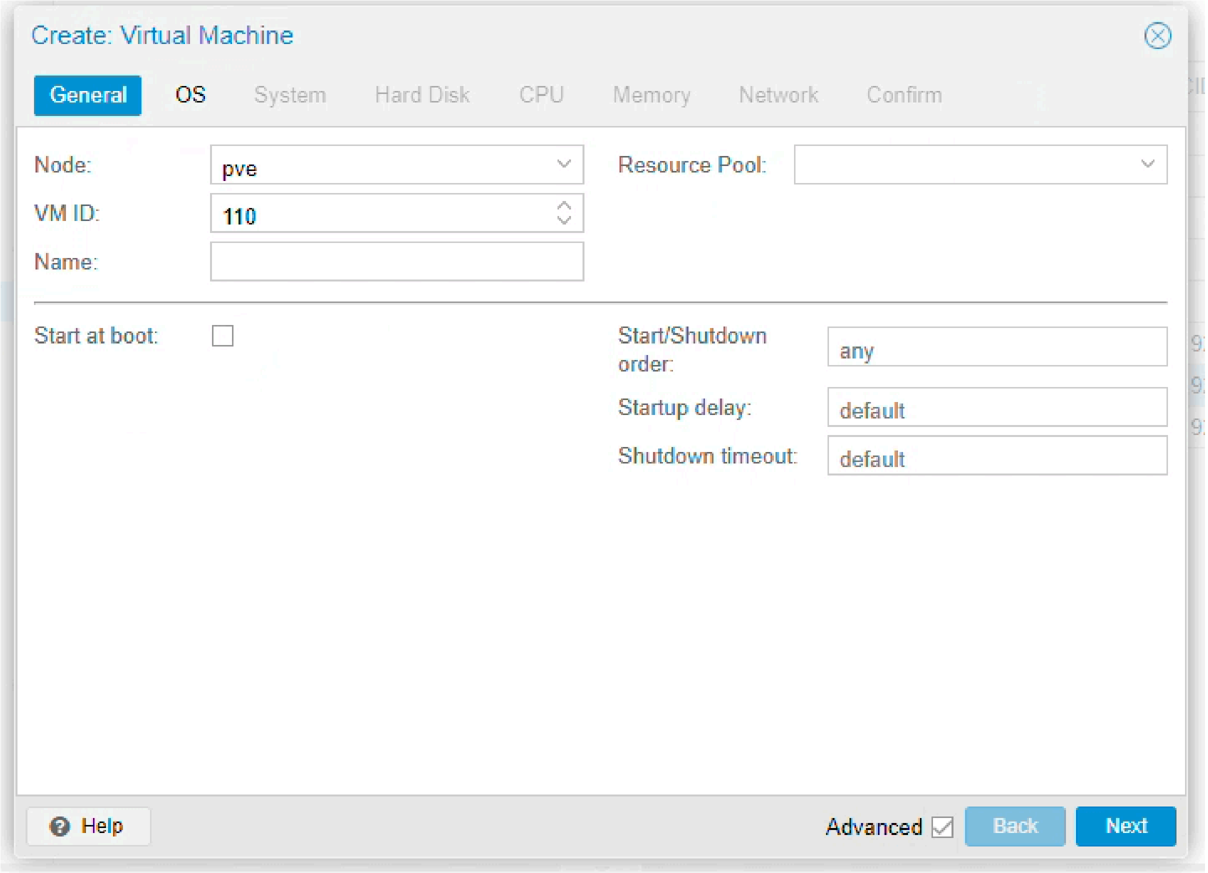
You can also copy the OPNsense ISO image to your Proxmox environment by using an SCP/SFTP client application. You should upload the ISO file into the `/var/lib/vz/template/iso` directory on the Proxmox VE server.

4. Creating a Virtual Machine on Proxmox VE

After uploading the OPNsense ISO image to the Proxmox VE, we will create a Virtual Machine for our OPNsense firewall. To create a virtual machine on Proxmox, you should follow the next steps given below.

1. Click on the blue `Create VM` button in the upper right-hand corner of the Proxmox VE web UI.

2. Enter a name for your virtual machine, such as `OPNsensefw`. Then, click `Next`



Create: Virtual Machine

Node: pve

Resource Pool:

VM ID: 110

Name:

Start at boot: □

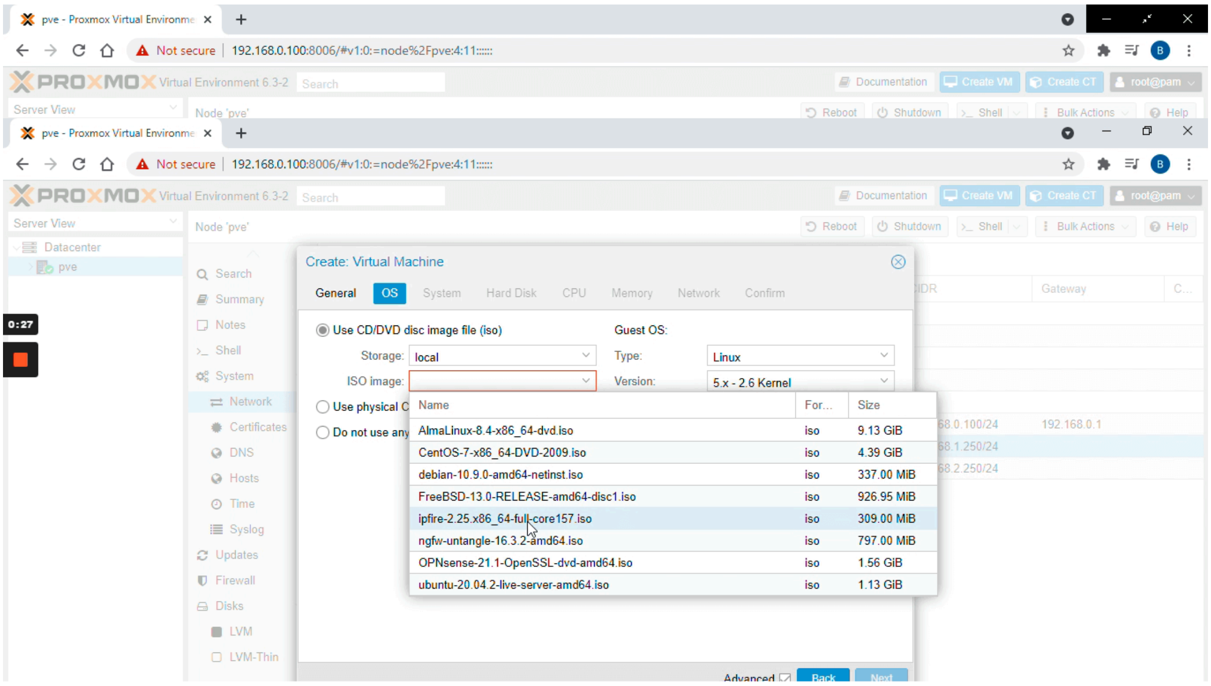
Start/Shutdown order: any

Startup delay: default

Shutdown timeout: default

Figure 4. *Naming the OPNsense VM on Proxmox*

3. Select the OPNsense ISO image under the `OS` tab, and then click `Next.`



Create: Virtual Machine

● Use CD/DVD disc image file (iso)

Storage: local

ISO image:

○ Use physical C

○ Do not use any

Guest OS:

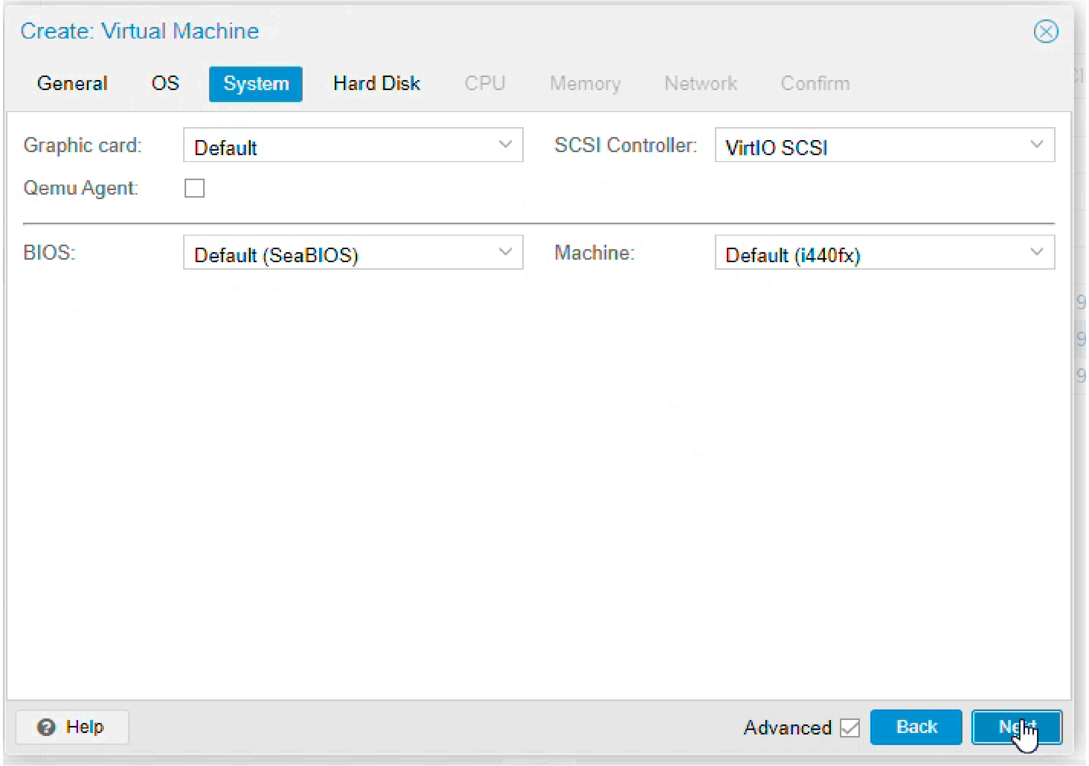
Type: Linux

Version: 5.x - 2.6 Kernel

Name	For...	Size
AlmaLinux-8.4-x86_64-dvd.iso	iso	9.13 GiB
CentOS-7-x86_64-DVD-2009.iso	iso	4.39 GiB
debian-10.9.0-amd64-netinst.iso	iso	337.00 MiB
FreeBSD-13.0-RELEASE-amd64-disc1.iso	iso	926.95 MiB
ipfire-2.25.x86_64-full-core157.iso	iso	309.00 MiB
ngfw-untangle-16.3.2-amd64.iso	iso	797.00 MiB
OPNsense-21.1-OpenSSL-dvd-amd64.iso	iso	1.56 GiB
ubuntu-20.04.2-live-server-amd64.iso	iso	1.13 GiB

Figure 5. *Selecting OPNsense ISO to install on Proxmox VE as an OS*

4. You may accept the default settings on the `System` tab by clicking `Next`.



Graphic card: Default

SCSI Controller: VirtIO SCSI

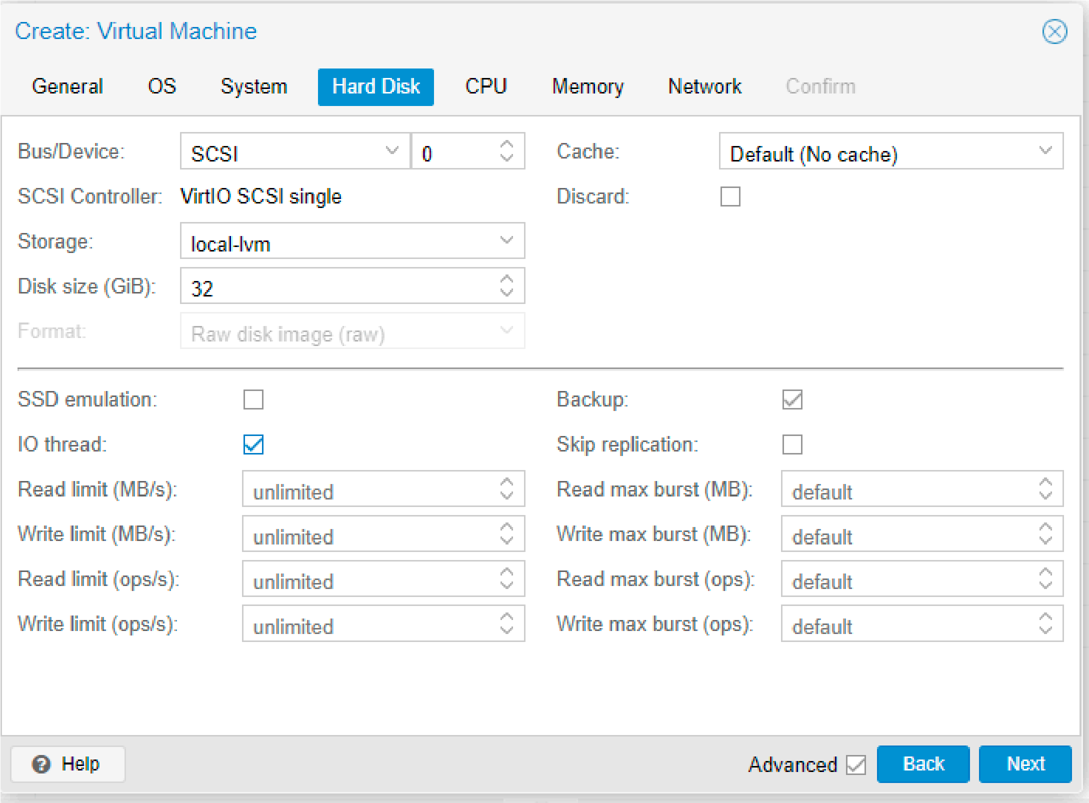
Qemu Agent: □

BIOS: Default (SeaBIOS)

Machine: Default (i440fx)

Figure 6. *System settings of the OPNsense VM on Proxmox*

5. Set the `Hard Disk` size as you wish. We recommend enabling the `IO thread` which should improve IO performance by giving the disk its Datacenter worker thread.



Bus/Device: SCSI 0

Cache: Default (No cache)

SCSI Controller: VirtIO SCSI single

Discard: □

Storage: local-lvm

Disk size (GiB): 32

Format: Raw disk image (raw)

SSD emulation: □

Backup: ☑

IO thread: ☑

Skip replication: □

Read limit (MB/s): unlimited

Read max burst (MB): default

Write limit (MB/s): unlimited

Write max burst (MB): default

Read limit (ops/s): unlimited

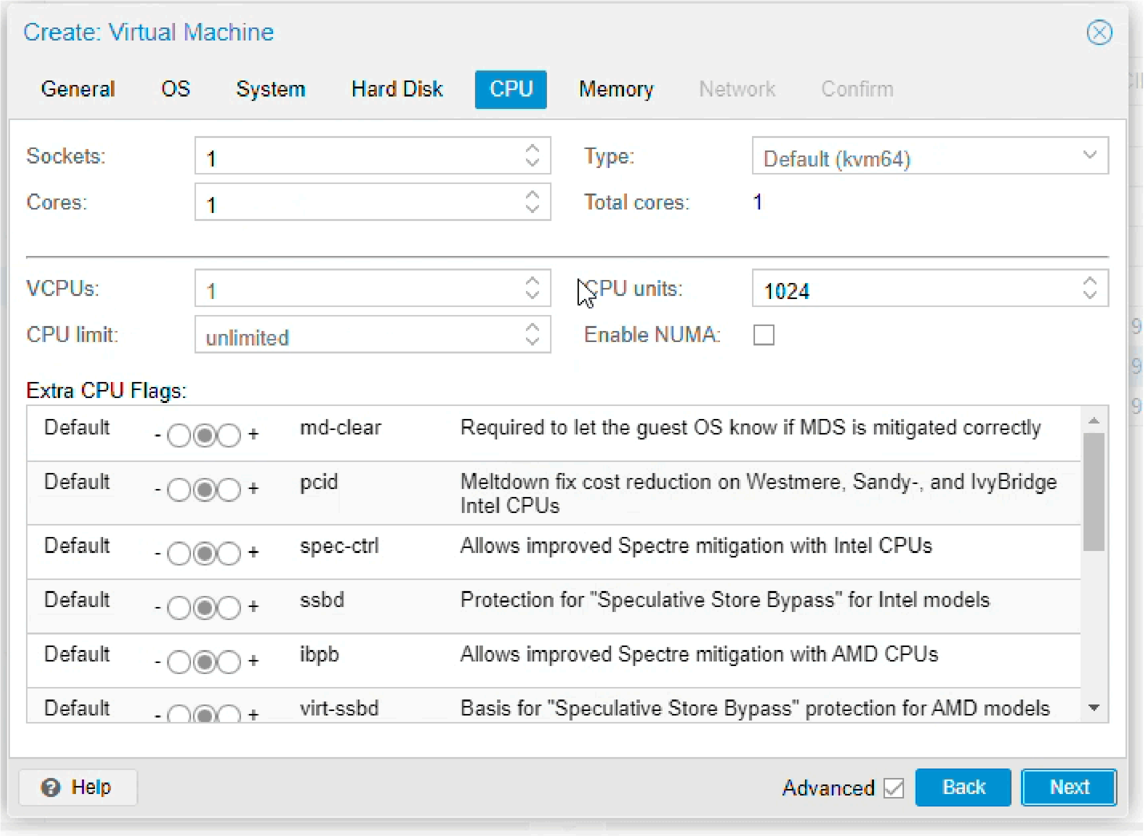
Read max burst (ops): default

Write limit (ops/s): unlimited

Write max burst (ops): default

Figure 7. *Setting Hard disk size as 32 GB for OPNsense on Proxmox VE*

6. Set the CPU configuration as you wish.



Sockets: 1

Cores: 1

Type: Default (kvm64)

Total cores: 1

VCPUs: 1

CPU units: 1024

CPU limit: unlimited

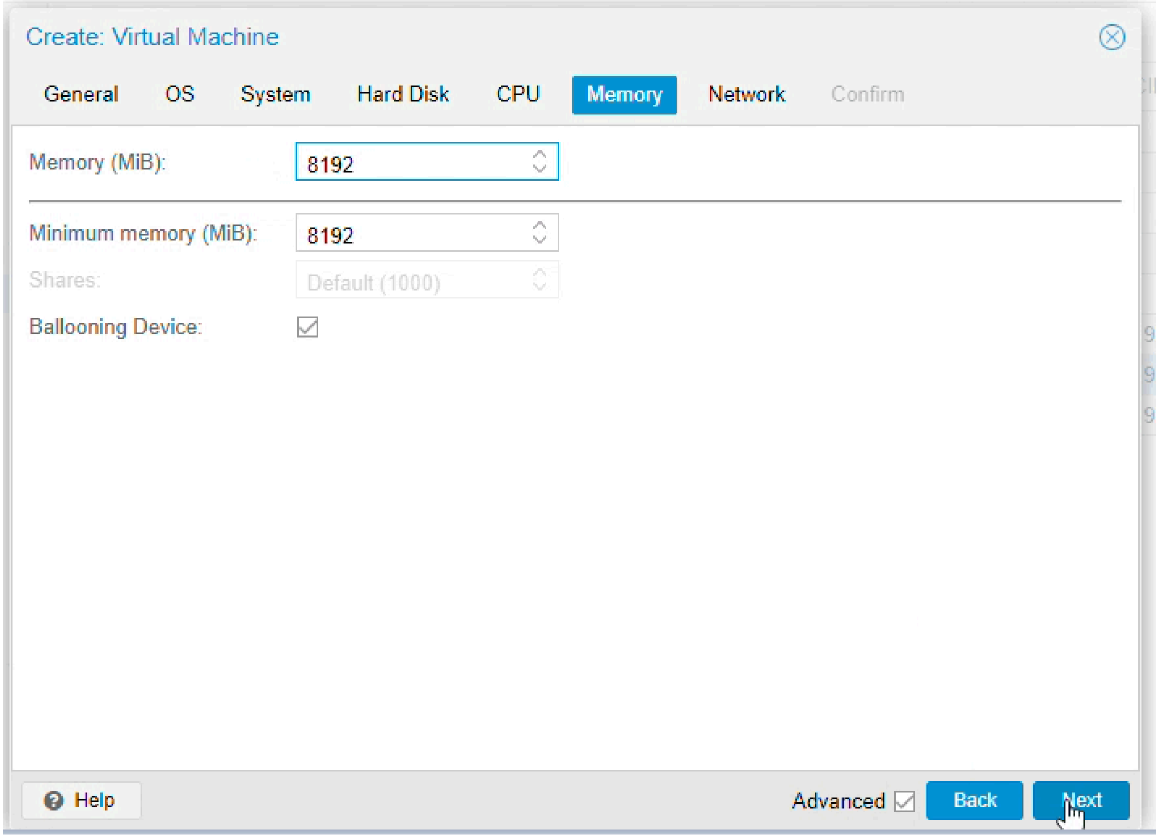
Enable NUMA: □

Extra CPU Flags:

Default	- ○●○ +	md-clear	Required to let the guest OS know if MDS is mitigated correctly
Default	- ○●○ +	pcid	Meltdown fix cost reduction on Westmere, Sandy-, and IvyBridge Intel CPUs
Default	- ○●○ +	spec-ctrl	Allows improved Spectre mitigation with Intel CPUs
Default	- ○●○ +	ssbd	Protection for "Speculative Store Bypass" for Intel models
Default	- ○●○ +	ibpb	Allows improved Spectre mitigation with AMD CPUs
Default	- ○●○ +	virt-ssbd	Basis for "Speculative Store Bypass" protection for AMD models

Figure 8. *CPU settings for OPNsense firewall on Proxmox VE*

7. Set the `Memory` size as you wish.



Memory (MiB): 8192

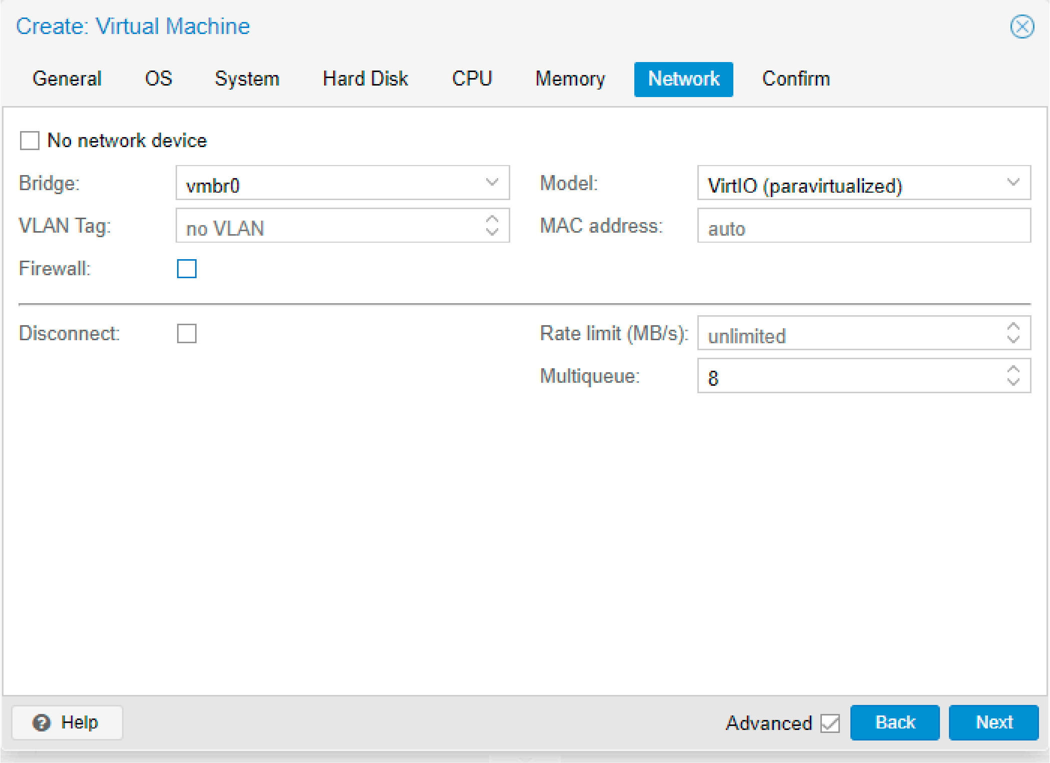
Minimum memory (MiB): 8192

Shares: Default (1000)

Ballooning Device: ☑

Figure 9. *Setting Memory size 8 GB for OPNsense firewall on Proxmox*

8. Set `Multiqueue to 8` which will allow the BSD kernel to negotiate the optimal value with Proxmox VE in the Network configuration. We will cover this configuration for our topology deeply later.



☐ No network device

Bridge: vmbr0

Model: VirtIO (paravirtualized)

VLAN Tag: no VLAN

MAC address: auto

Firewall: ☐

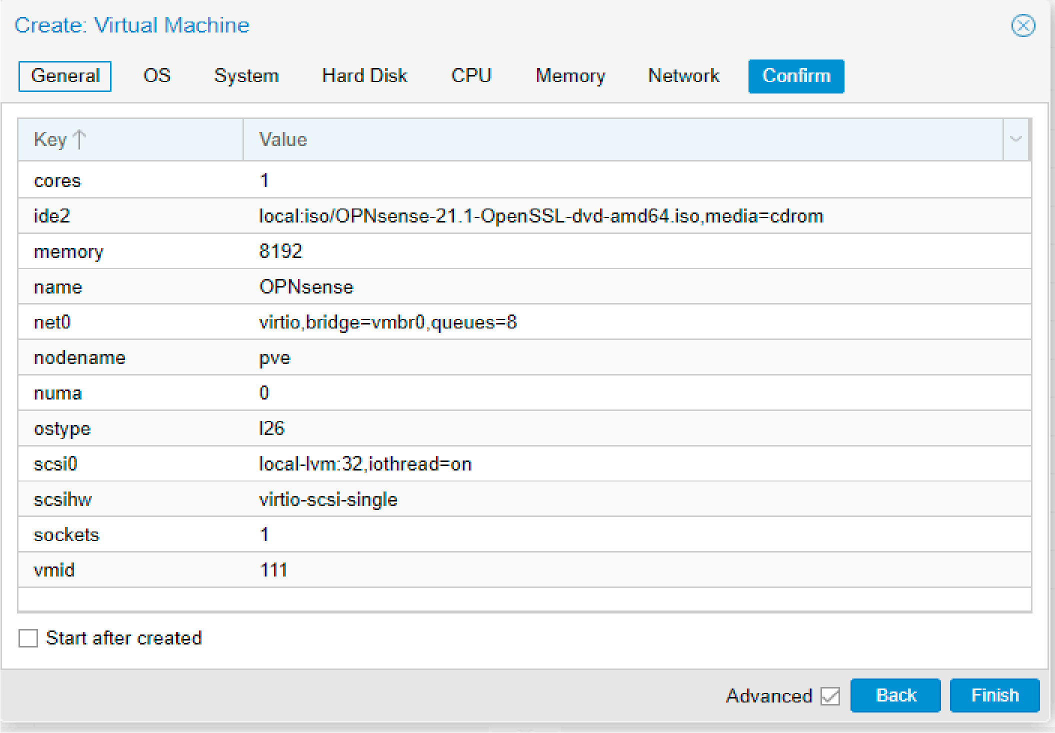
Disconnect: ☐

Rate limit (MB/s): unlimited

Multiqueue: 8

Figure 10. *Network configuration of OPNsense VM on Proxmox VE*

9. Confirm the OPNsense virtual machine configuration by clicking on the `Finish` button.



Key ↑	Value
cores	1
ide2	local:iso/OPNsense-21.1-OpenSSL-dvd-amd64.iso,media=cdrom
memory	8192
name	OPNsense
net0	virtio,bridge=vmbr0,queues=8
nodename	pve
numa	0
ostype	l26
scsi0	local-lvm:32,iothread=on
scsihw	virtio-scsi-single
sockets	1
vmid	111

☐ Start after created

Figure 11. *Confirming the OPNsense virtual machine configuration*

5. Setting Network Configuration of the OPNsense Virtual Machine on Proxmox VE

In this tutorial, we will configure two physical NICs for our OPNsense firewall. These NICs will be used and configured for the following purposes

- **WAN Connection**: Internet connection/Untrusted zone.
- **LAN Connection**: Clients and servers are placed in this trusted zone.

You may complete network configuration of the OPNsense Virtual Machine on Proxmox VE by following the next 2 steps:

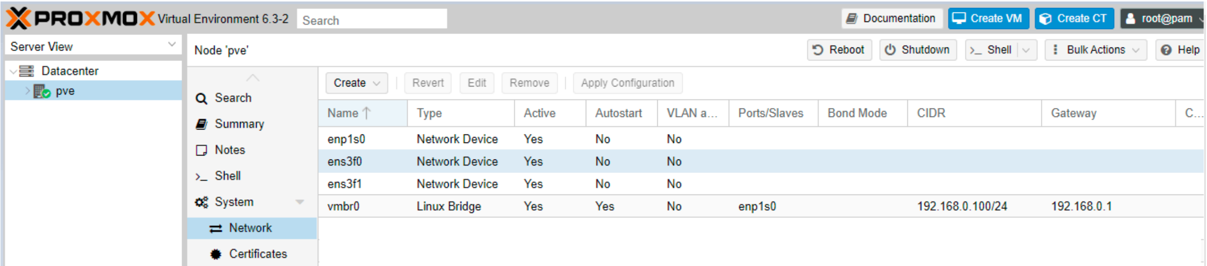
1. Creating Linux Bridge
2. Adding Network Devices to OPNsense VM on Proxmox

5.1. Creating Linux Bridge

To be able to define 2 network interfaces for the OPNsense virtual machine, firstly we must create Linux bridge devices on the Proxmox device.

To create a `Network Bridge` follow the next steps.

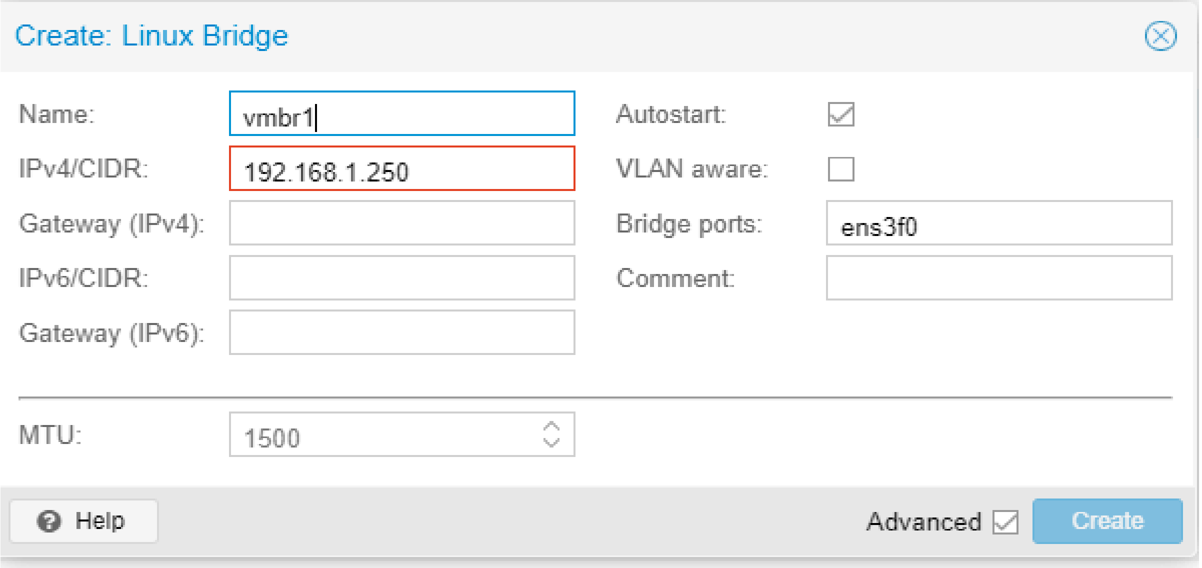
1. Navigate to `Data center` -> `pve` -> `Network`.



Name	Type	Active	Autostart	VLAN a...	Ports/Slaves	Bond Mode	CIDR	Gateway	C...
enp1s0	Network Device	Yes	No	No					
ens3f0	Network Device	Yes	No	No					
ens3f1	Network Device	Yes	No	No					
vmbr0	Linux Bridge	Yes	Yes	No	enp1s0		192.168.0.100/24	192.168.0.1	

Figure 12. *Viewing the network devices of the Proxmox VE*

2. Click on the `Create` button. This will pop up the `Linux Bridge` configuration window.
3. You may leave the name as default such as `vmbr1`. Enter `IPv4/CIDR` address and `Bridge ports` (Network devices name seen on Network configuration window, such as ens3f0). Then, click on the `Create` button.

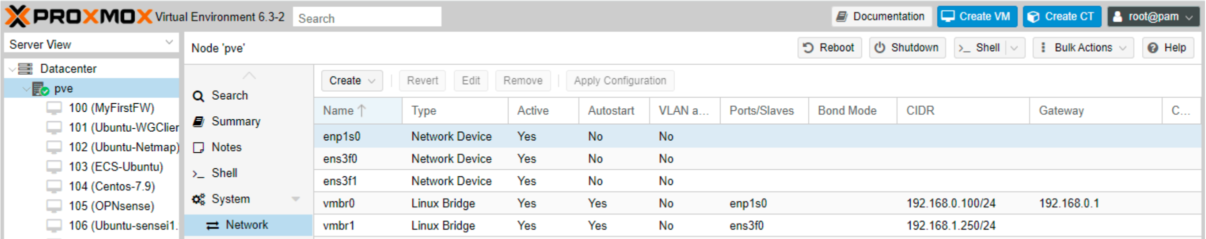


Name:	vmbr1	Autostart:	☑
IPv4/CIDR:	192.168.1.250	VLAN aware:	□
Gateway (IPv4):		Bridge ports:	ens3f0
IPv6/CIDR:		Comment:	
Gateway (IPv6):			
MTU:	1500	Advanced	☑

Figure 13. *Creating a Linux bridge on the Proxmox VE*

4. Click on the `Apply Configuration` button or `Reboot` the Proxmox device to start to use new Linux bridges.

Now, you have two Linux Bridges as seen in the Figure below.



Name	Type	Active	Autostart	VLAN a...	Ports/Slaves	Bond Mode	CIDR	Gateway	C...
enp1s0	Network Device	Yes	No	No					
ens3f0	Network Device	Yes	No	No					
ens3f1	Network Device	Yes	No	No					
vmbr0	Linux Bridge	Yes	Yes	No	enp1s0		192.168.0.100/24	192.168.0.1	
vmbr1	Linux Bridge	Yes	Yes	No	ens3f0		192.168.1.250/24		

Figure 14. *Viewing the network devices of the Proxmox VE*

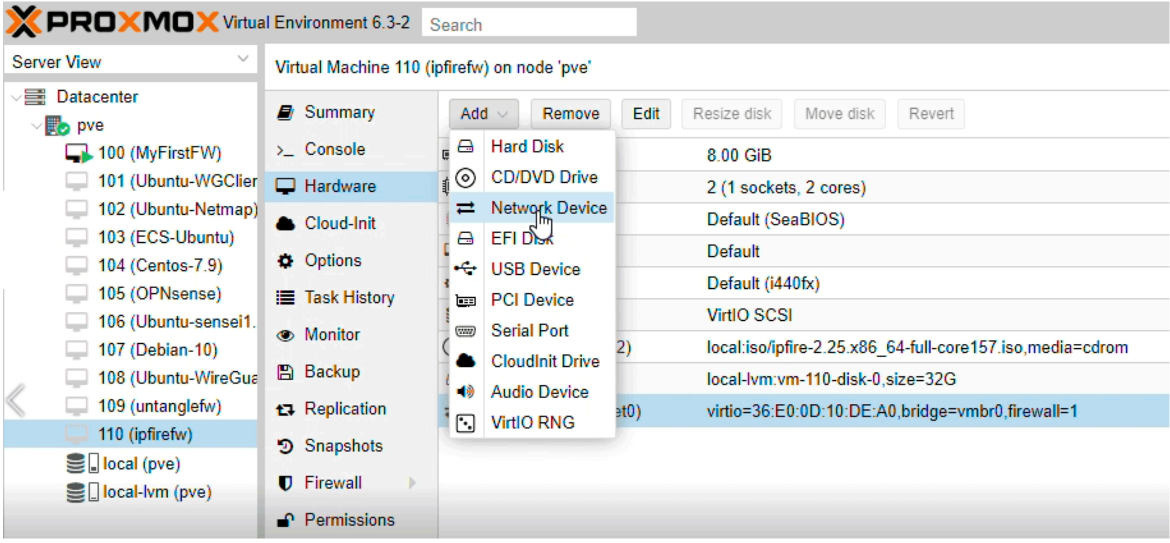
5.2. Adding Network Devices to OPNsense VM on Proxmox

It is time to add a network device that will be used for LAN connections.

To add a new network interface to the OPNsense virtual machine on Proxmox you can follow these steps.

1. Navigate to the `Data center` -> `pve` -> `OPNsensefw VM` -> `Hardware` -> `Add`.

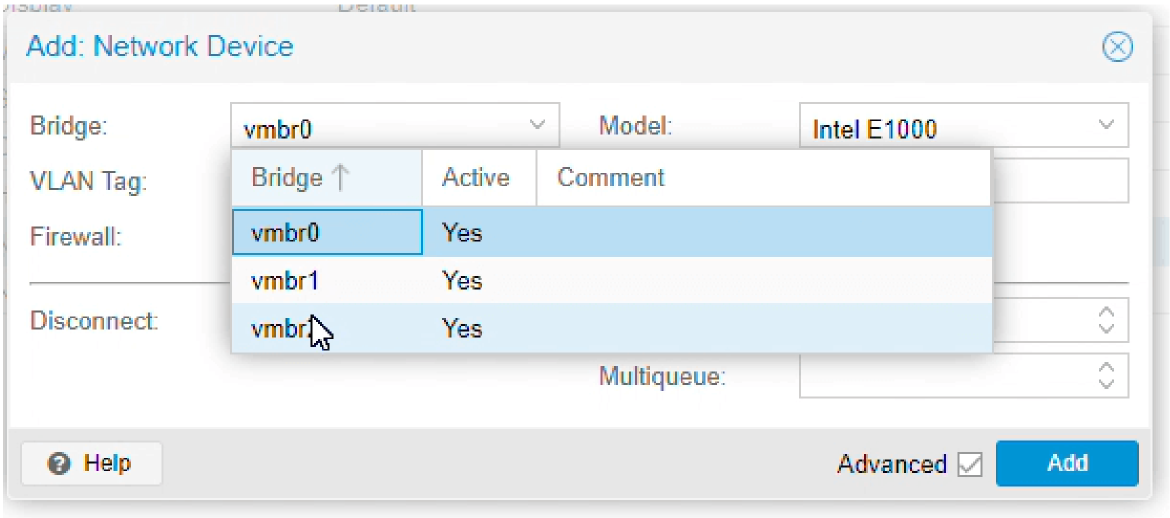
2. Click on `Network Device`.



8.00 GiB
2 (1 sockets, 2 cores)
Default (SeaBIOS)
Default
Default (i440fx)
VirtIO SCSI
local:iso/ipfire-2.25.x86_64-full-core157.iso,media=cdrom
local-lvm:vm-110-disk-0,size=32G
virtio=36:E0:0D:10:DE:A0,bridge=vmbr0,firewall=1

Figure 15. *Adding NIC to OPNsense VM on Proxmox VE*

3. Select the `Linux Bridge` such as vmbr1.

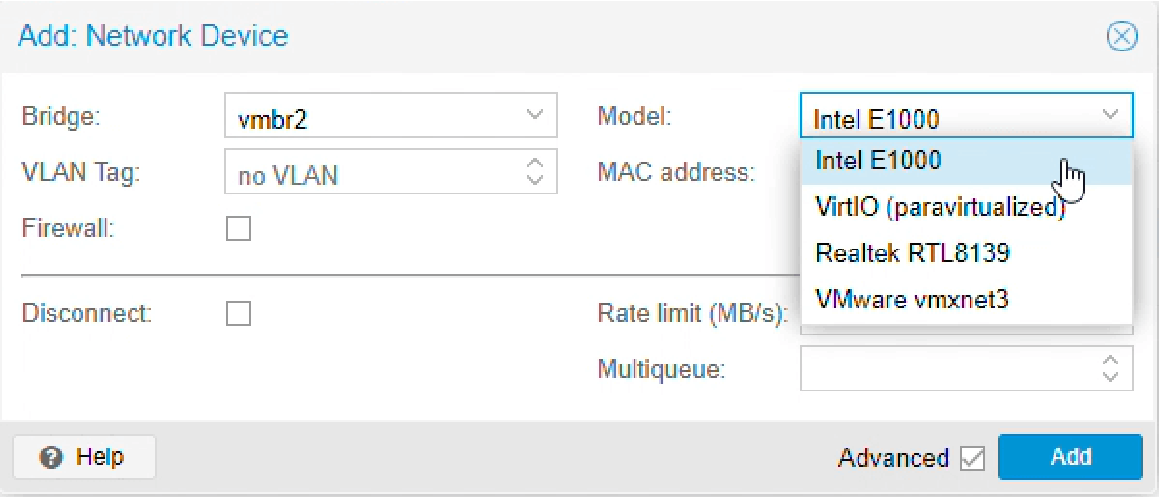


Bridge: vmbr0
Model: Intel E1000
VLAN Tag:
Firewall:
Disconnect:
Multiqueue:
Advanced ☑

Bridge ↑	Active	Comment
vmbr0	Yes	
vmbr1	Yes	
vmbr2	Yes	

Figure 16. *Selecting Linux bridge for a NIC*

4. Select `Model` as `VirtIO(paravirtualized)`.

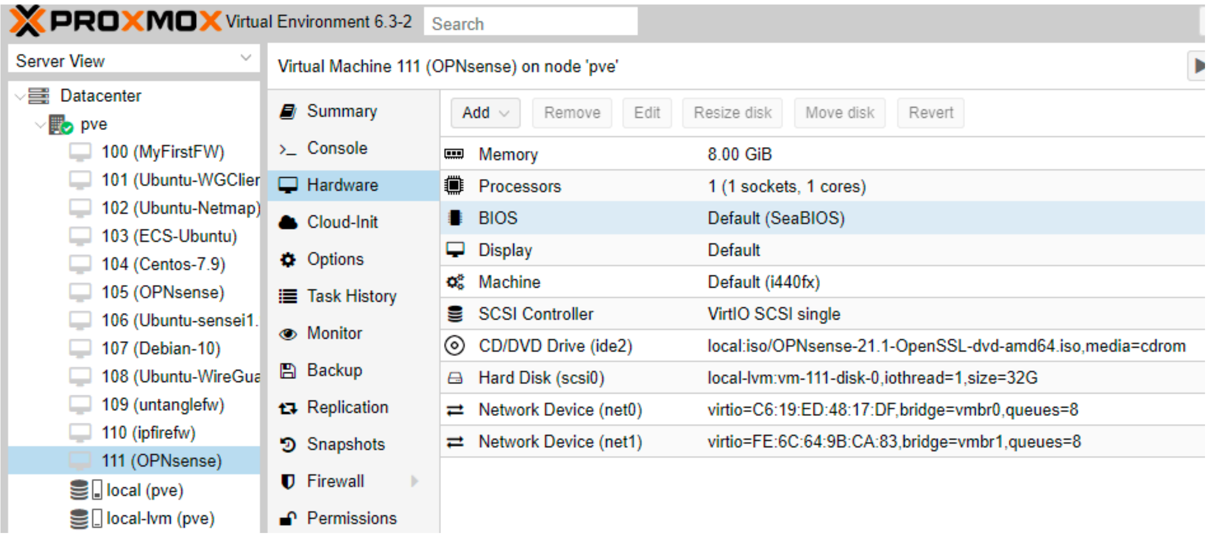


Bridge: vmbr2
VLAN Tag: no VLAN
Firewall: □
Disconnect: □
Model: Intel E1000
MAC address:
Rate limit (MB/s):
Multiqueue:
Advanced ☑

Figure 17. *Setting model for a network device of OPNsense VM on Proxmox VE*

5. Uncheck `Firewall` option.
6. Set `Multiqueue to 8.`
7. Click the `Add` button

After finishing the network configuration of the OPNsense virtual machine on Proxmox, you should see the Hardware configuration for the OPNsense VM similar to the following figure.



Virtual Machine 111 (OPNsense) on node 'pve'

Memory	8.00 GiB
Processors	1 (1 sockets, 1 cores)
BIOS	Default (SeaBIOS)
Display	Default
Machine	Default (i440fx)
SCSI Controller	VirtIO SCSI single
CD/DVD Drive (ide2)	local:iso/OPNsense-21.1-OpenSSL-dvd-amd64.iso,media=cdrom
Hard Disk (scsi0)	local-lvm:vm-111-disk-0,iothread=1,size=32G
Network Device (net0)	virtio=C6:19:ED:48:17:DF,bridge=vmbr0,queues=8
Network Device (net1)	virtio=FE:6C:64:9B:CA:83,bridge=vmbr1,queues=8

Figure 18. *Hardware configuration of the OPNsense VM on Proxmox VE*

Now, your OPNsense firewall has 2 different physical interfaces ready to connect to different networks, Internet and LAN respectively.

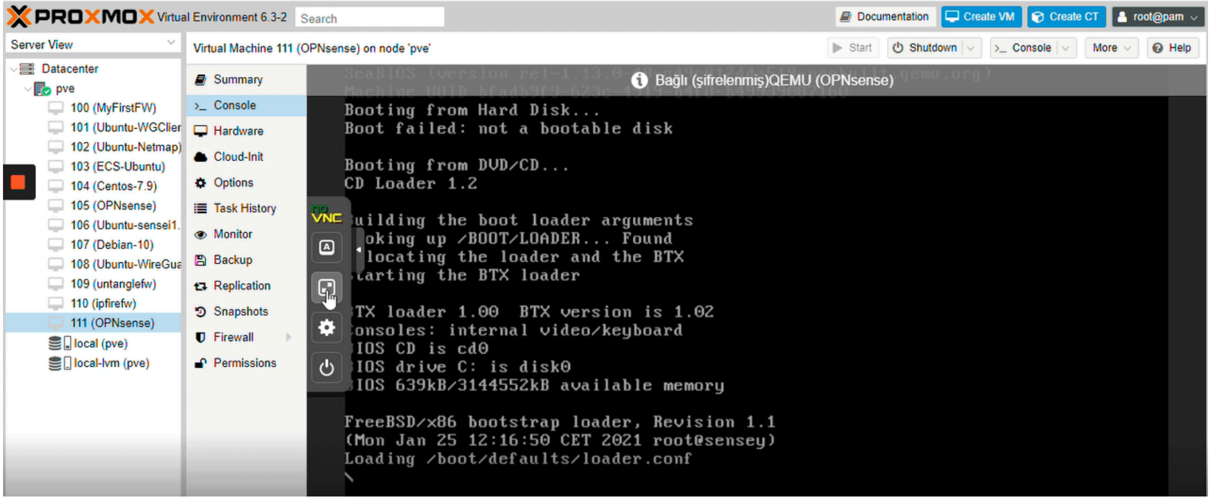
> 💡 **TIP**
>
> It is recommended that you should note the MAC address of the network devices used by OPNsense VM. You will need them to complete the network settings of the firewall after installing the OPNsense software.

6. Installing OPNsense

To start the installation of the OPNsense on your Proxmox environment, first, you should start the OPNsense virtual machine. To start the machine,

1. Click on the `OPNsensefw` virtual machine on the node list.
2. Click on the `Start` button.

To continue the installation of the OPNsense, you should connect the virtual machine from the Proxmox console by clicking on the `Console`.

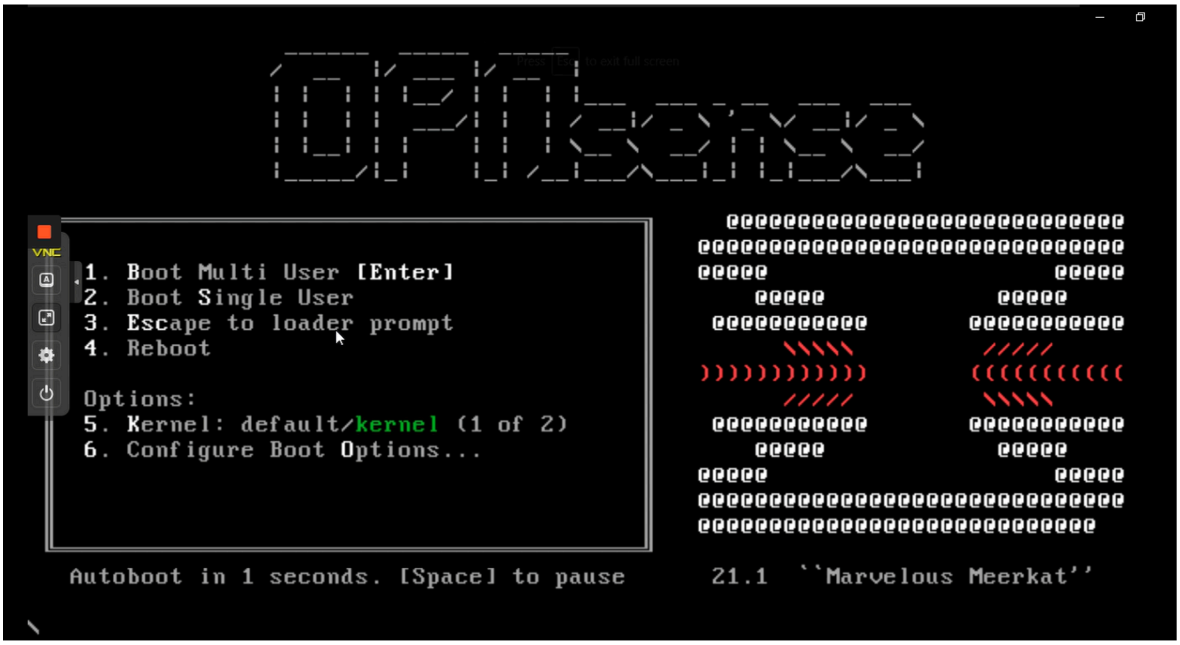


```
Booting from Hard Disk...
Boot failed: not a bootable disk

Booting from DVD/CD...
CD Loader 1.2

uilding the boot loader arguments
oking up /BOOT/LOADER... Found
locating the loader and the BTX
tarting the BTX loader

TX loader 1.00  BTX version is 1.02
onsoles: internal video/keyboard
IOS CD is cd0
IOS drive C: is disk0
IOS 639kB/3144552kB available memory

FreeBSD/x86 bootstrap loader, Revision 1.1
(Mon Jan 25 12:16:50 CET 2021 root@sensey)
Loading /boot/defaults/loader.conf
\
```

Figure 19. *Connecting OPNsense VM console on Proxmox VE*

And then, you may follow the steps listed below.

1. While the system is booting do not press any key and wait for the login prompt.

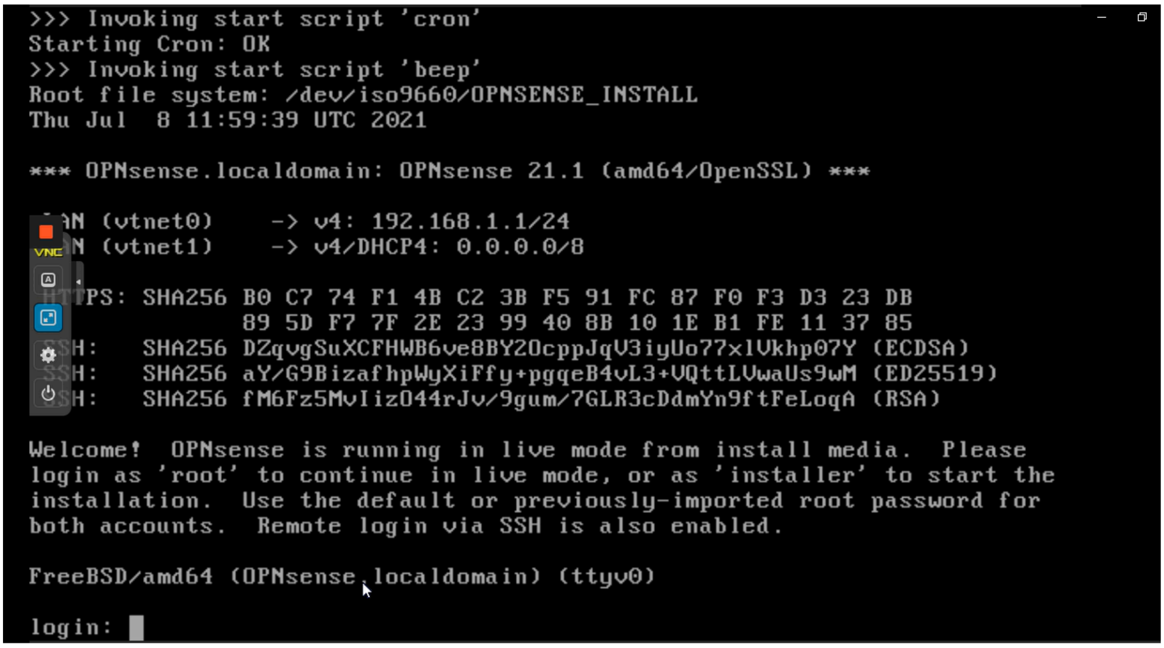


```
1. Boot Multi User [Enter]
2. Boot Single User
3. Escape to loader prompt
4. Reboot

Options:
5. Kernel: default/kernel (1 of 2)
6. Configure Boot Options...

Autoboot in 1 seconds. [Space] to pause      21.1  ``Marvelous Meerkat''
```

Figure 20. *OPNsense boot menu*

2. **Login**: Login as `installer` and the default password is `opnsense`. This will start the installation process.

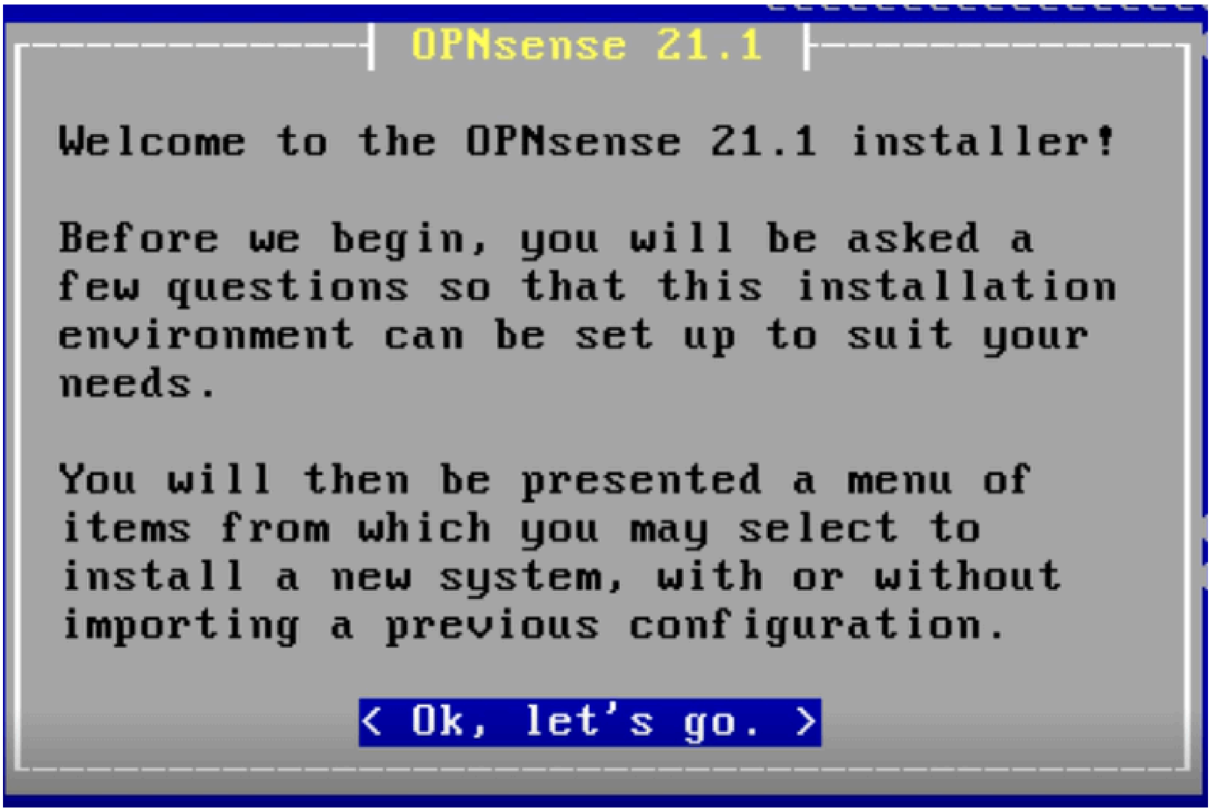
> 📣 **INFO**
>
> On OPNsense, default installer password is opnsense.



```
>>> Invoking start script 'cron'
Starting Cron: OK
>>> Invoking start script 'beep'
Root file system: /dev/iso9660/OPNSENSE_INSTALL
Thu Jul  8 11:59:39 UTC 2021

*** OPNsense.localdomain: OPNsense 21.1 (amd64/OpenSSL) ***

LAN (vtnet0)     -> v4: 192.168.1.1/24
WAN (vtnet1)     -> v4/DHCP4: 0.0.0.0/8

HTTPS: SHA256 B0 C7 74 F1 4B C2 3B F5 91 FC 87 F0 F3 D3 23 DB
              89 5D F7 7F 2E 23 99 40 8B 10 1E B1 FE 11 37 85
SSH:   SHA256 DZqvgSuXCFHWB6ve8BY2OcppJqV3iyUo77xlVkhp07Y (ECDSA)
SSH:   SHA256 aY/G9BizafhpWyXiFfy+pgqeB4vL3+VQttLVwaUs9wM (ED25519)
SSH:   SHA256 fM6Fz5MvIiz044rJv/9gum/7GLR3cDdmYn9ftFeLoqA (RSA)

Welcome!  OPNsense is running in live mode from install media.  Please
login as 'root' to continue in live mode, or as 'installer' to start the
installation.  Use the default or previously-imported root password for
both accounts.  Remote login via SSH is also enabled.

FreeBSD/amd64 (OPNsense.localdomain) (ttyv0)

login:
```

Figure 21. *OPNsense installation login prompt*

3. **Confirmation**: To confirm the installation press `Ok, let's go.`



OPNsense 21.1

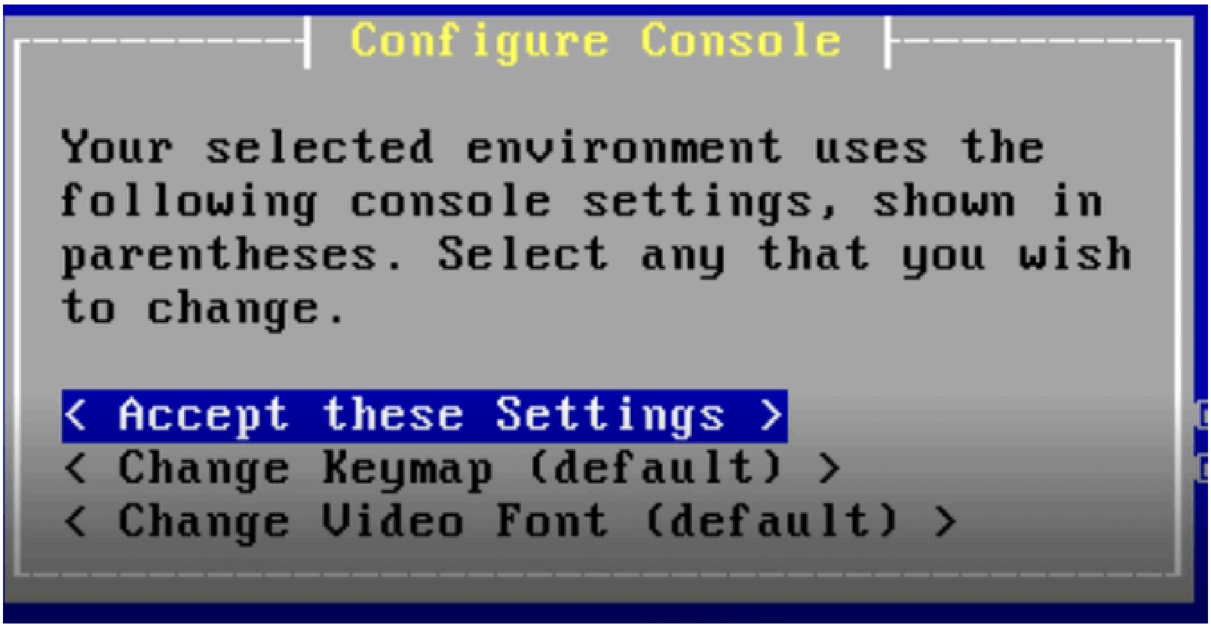
Welcome to the OPNsense 21.1 installer!

Before we begin, you will be asked a few questions so that this installation environment can be set up to suit your needs.

You will then be presented a menu of items from which you may select to install a new system, with or without importing a previous configuration.

Figure 22. *Confirming the OPNsense installation*

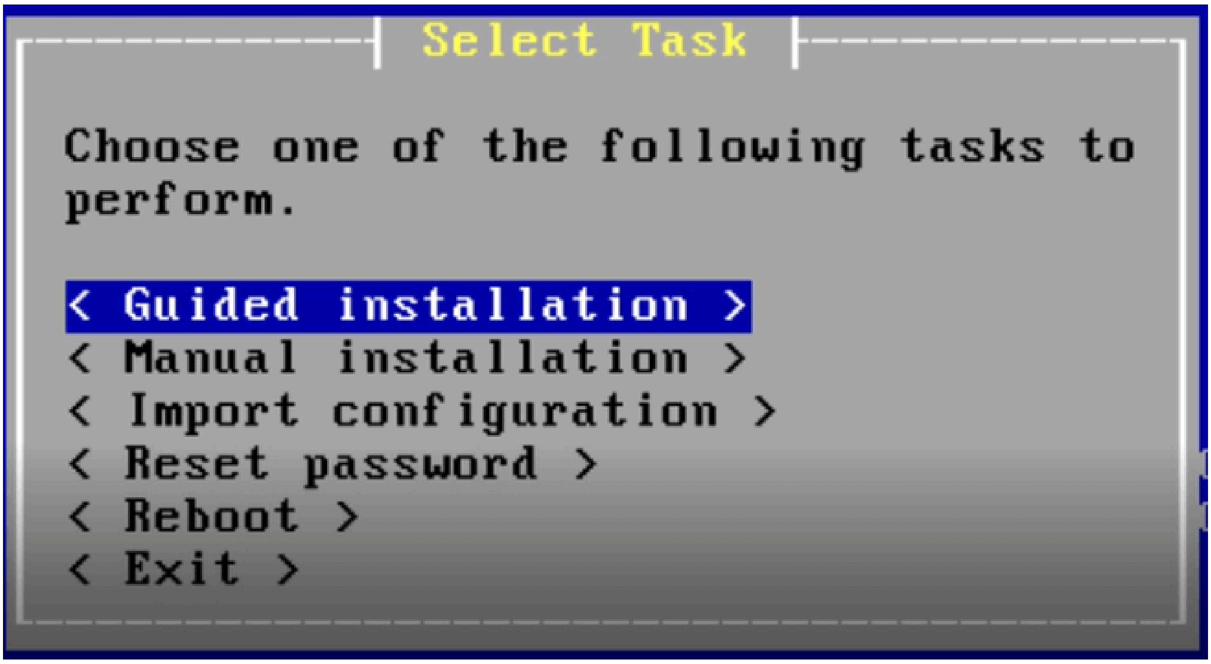
4. **Console configuration**: Click on the `Accept these settings` for the console. The installer likely will detect the proper keymap by default. Or you may change `Keymap` and `Video Font` as you wish.



```
Configure Console

Your selected environment uses the
following console settings, shown in
parentheses. Select any that you wish
to change.

< Accept these Settings >
< Change Keymap (default) >
< Change Video Font (default) >
```

Figure 23. *Configuring console*

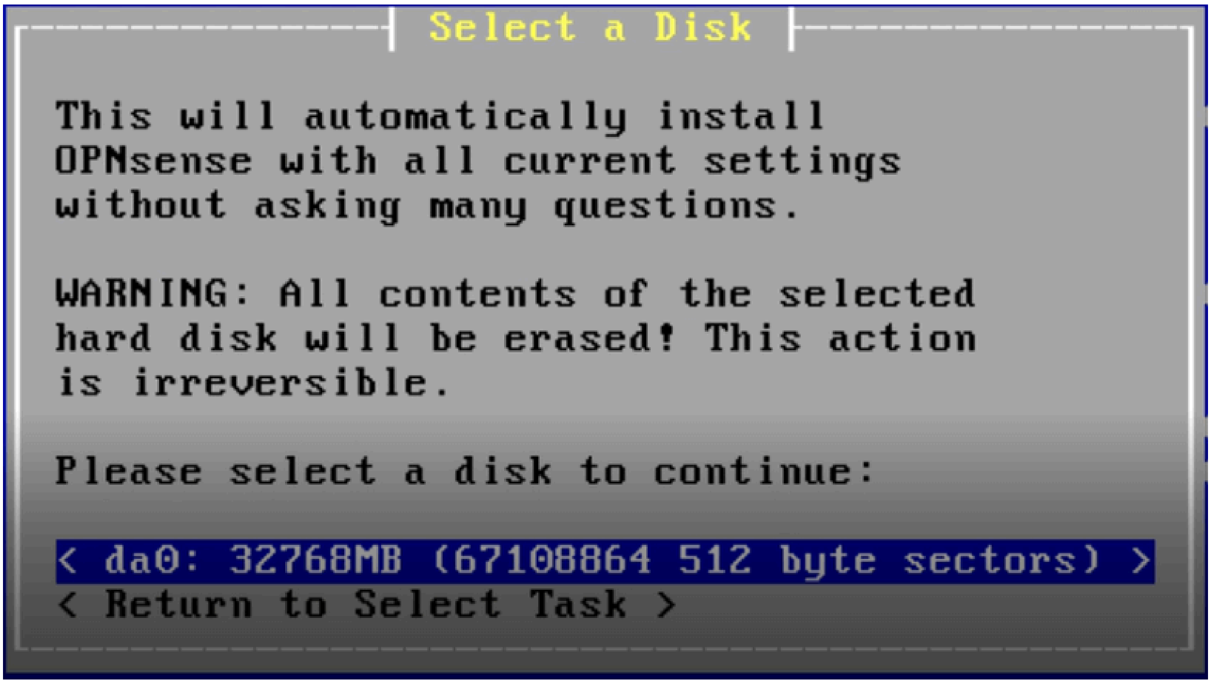
5. **Select Task**: Click on the `Guided Installation`. If you wish to do advanced partitioning or import a configuration from another OpnSense firewall, you can accomplish these settings at this step.



```
Select Task

Choose one of the following tasks to
perform.

< Guided installation >
< Manual installation >
< Import configuration >
< Reset password >
< Reboot >
< Exit >
```

Figure 24. *Selecting Guided installation*

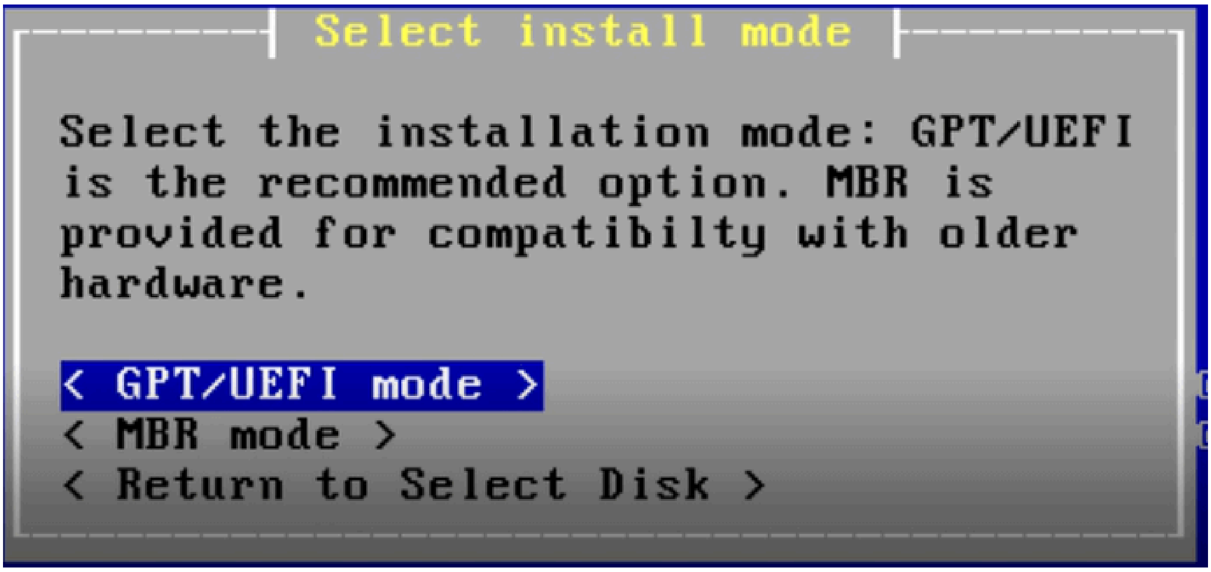
6. **Select a Disk**: Select the hard disk on which OPNsense will be installed. Be careful that all files on this disk will be deleted.



```
Select a Disk

This will automatically install
OPNsense with all current settings
without asking many questions.

WARNING: All contents of the selected
hard disk will be erased! This action
is irreversible.

Please select a disk to continue:

< da0: 32768MB (67108864 512 byte sectors) >
< Return to Select Task >
```

Figure 25. *Selecting disk to install OPNsense*

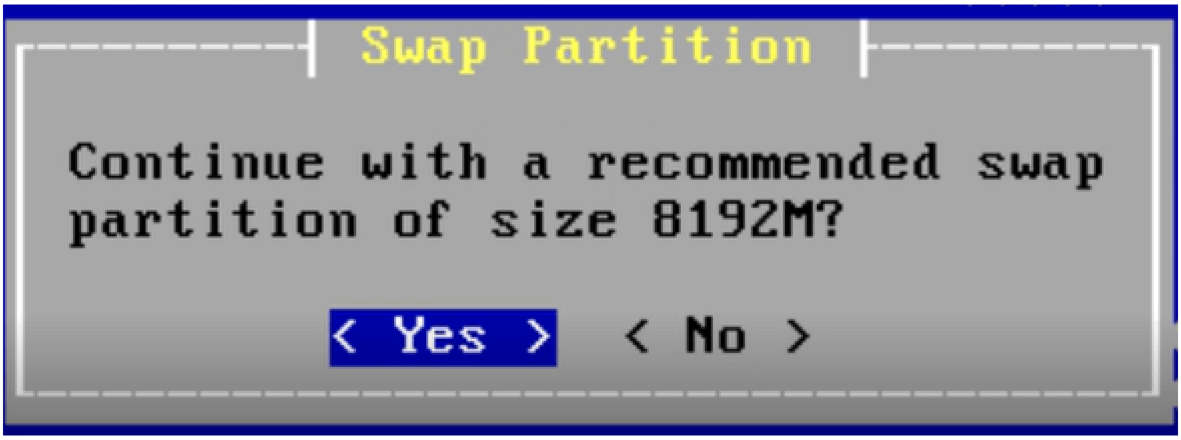
7. **Selecting Install Mode**: Select `GBT/UEFI` as an installation mode. Most modern-day systems support GPT/EFI but if you are using an older computer, MBR may be the only option supported. You may check within the BIOS settings of your system to see if it supports EFI/GPT.



```
Select install mode

Select the installation mode: GPT/UEFI
is the recommended option. MBR is
provided for compatibilty with older
hardware.

< GPT/UEFI mode >
< MBR mode >
< Return to Select Disk >
```

Figure 26. *Selecting installation mode for OPNsense installation on Proxmox VE*

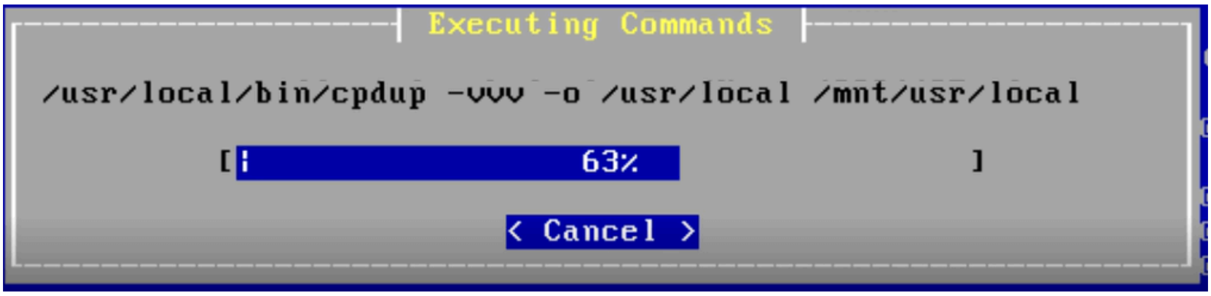
8. **Swap Size:** Accept the recommended partition swap size by pressing `Yes`.



Continue with a recommended swap partition of size 8192M?

Figure 27. *Setting swap partition size*

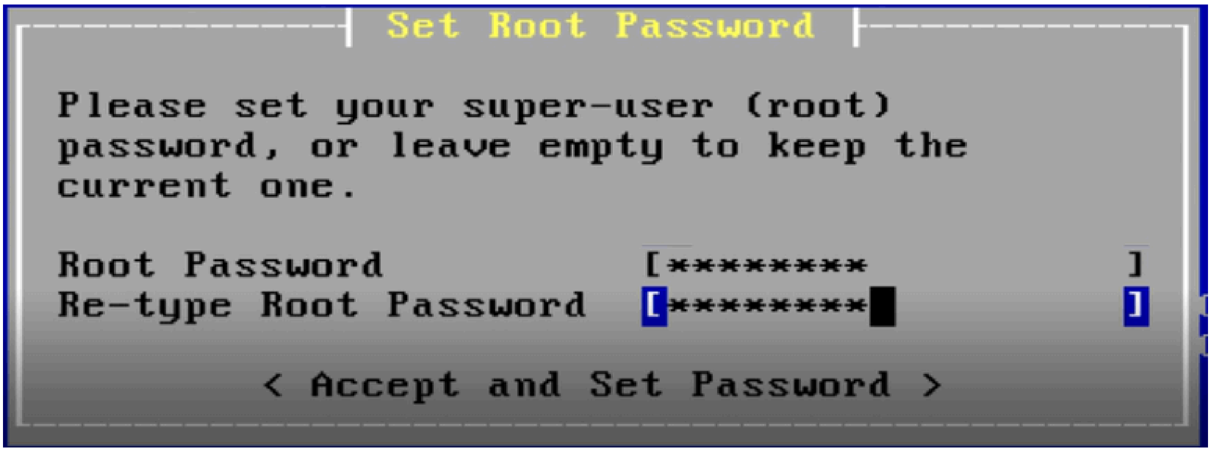
9. **Package Installation:** Packages are installed in your system for up to ten minutes.



```
/usr/local/bin/cpdup -vvv -o /usr/local /mnt/usr/local
```

Figure 28. *Installing OPNsense packages*

10. **Setting root password:** You may set your root password or left as default which is `opnsense` for now.



Please set your super-user (root) password, or leave empty to keep the current one.

Root Password [*********]

Re-type Root Password [*********]

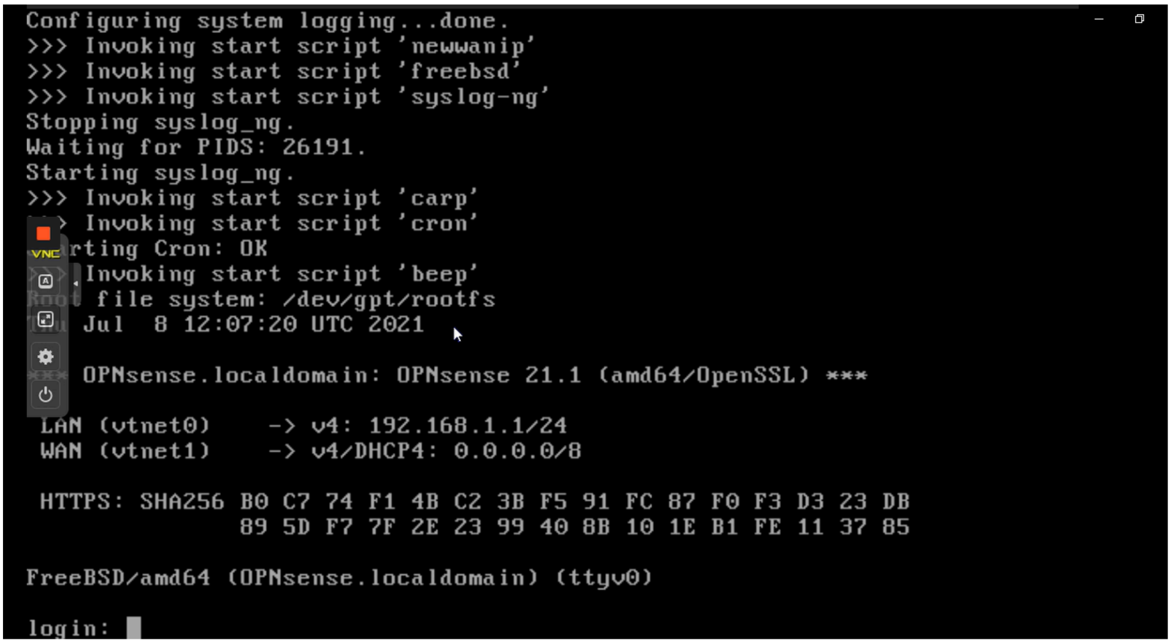
Figure 29. *Setting root password*

11. **Reboot:** By pressing the `Reboot`, you should reboot your system.

12. **Unmount ISO image:** Exit from the console and return to the Proxmox GUI.

- Navigate to the `OPNsensefw` VM node -> `Hardware` -> `CD/DVD Drive`.
- Click on the `Remove`.
- Confirm removing the CD/DVD Drive by clicking on `Yes`.

13. Return to the Console of the OPNsense firewall in Proxmox VE. After the OPNsense reboot is completed, you will see the login prompt.



```
Configuring system logging...done.
>>> Invoking start script 'newwanip'
>>> Invoking start script 'freebsd'
>>> Invoking start script 'syslog-ng'
Stopping syslog_ng.
Waiting for PIDS: 26191.
Starting syslog_ng.
>>> Invoking start script 'carp'
>>> Invoking start script 'cron'
Starting Cron: OK
>>> Invoking start script 'beep'
Root file system: /dev/gpt/rootfs
Thu Jul  8 12:07:20 UTC 2021

*** OPNsense.localdomain: OPNsense 21.1 (amd64/OpenSSL) ***

 LAN (vtnet0)     -> v4: 192.168.1.1/24
 WAN (vtnet1)     -> v4/DHCP4: 0.0.0.0/8

 HTTPS: SHA256 B0 C7 74 F1 4B C2 3B F5 91 FC 87 F0 F3 D3 23 DB
               89 5D F7 7F 2E 23 99 40 8B 10 1E B1 FE 11 37 85

FreeBSD/amd64 (OPNsense.localdomain) (ttyv0)

login:
```

Figure 30. *OPNsense CLI login prompt*

```
Welcome to the OPNsense 21.1 installer!

Before we begin, you will be asked a
few questions so that this installation
environment can be set up to suit your
needs.

You will then be    ed a menu of
items from which you may select to
install a new system, with or without
importing a previous configuration.

              < Ok, let's go. >
```

Now, you can complete the installation of the OPNsense on your Proxmox environment by following the next 6 main steps:

1. Network Device Assignments for OPNsense Firewall
2. IP Address Settings for OPNsense Firewall
3. Updating OPNsense Firewall on CLI

4. Accessing the OPNsense Web GUI
5. Initial Configuration of the OPNsense Firewall
6. Disable Network Hardware Off-loading on OPNsense Firewall

6.1. Network Device Assignments for OPNsense Firewall

By default, the system will be configured with 2 interfaces LAN & WAN. The first network port found will be configured as LAN and the second will be WAN. However, OPNsense may not assign the network interface cards to the proper networks correctly. Then, you must assign the network devices to the proper networks manually.

For example, in our installation, OPNsense assigned the `vtnet0` device to the LAN, and `vtnet1` device to the WAN. But, the correct configuration is vice versa. While the `vtnet0` device should be assigned to the WAN, `vtnet1` device should be assigned to the LAN. Let's correct the network device configuration for our OPNsense.

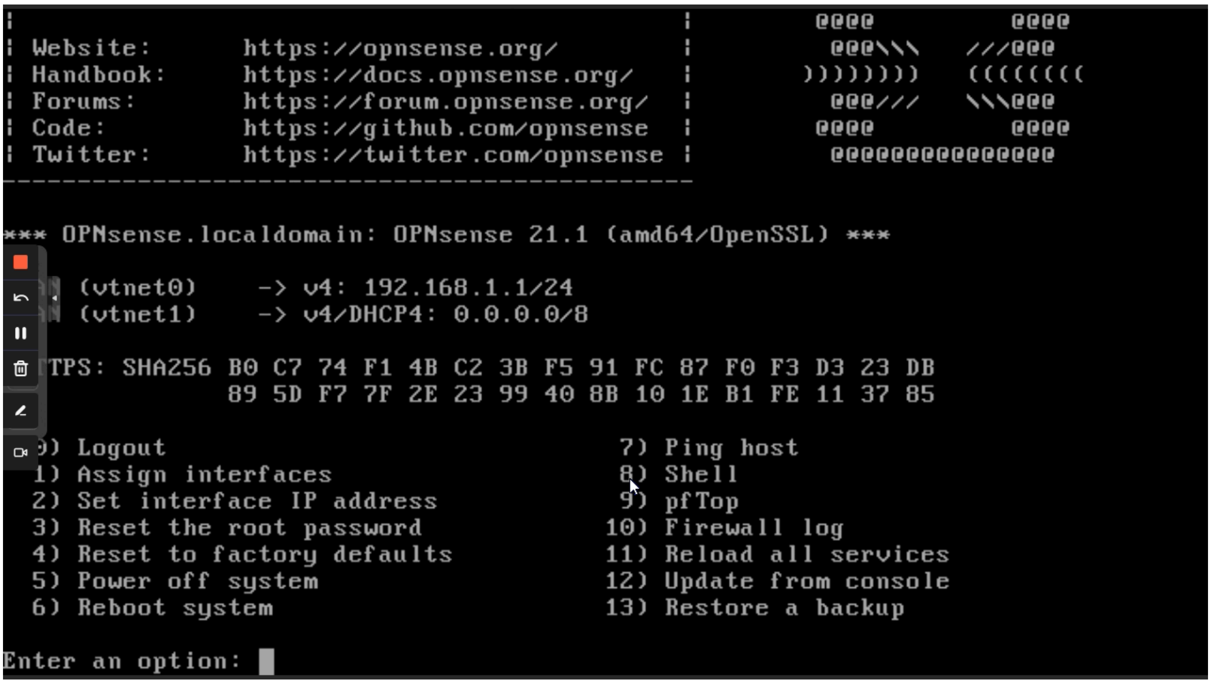
⚠️ **CAUTION**

Default DHCP configuration of the networks interfaces on OPNsense firewall are as follows:

- The WAN interface works as a DHCP client and expects to be assigned an IP address.
- The LAN interface works as a DHCP server, has a static IP of 192.168.1.1/24, and offers IP addresses in the range of 192.168.1.100-200.

For network device assignments on your OPNsense firewall, you may follow the next steps given below:

1. **Log in as root**. Then, the Options menu will be displayed on the screen.

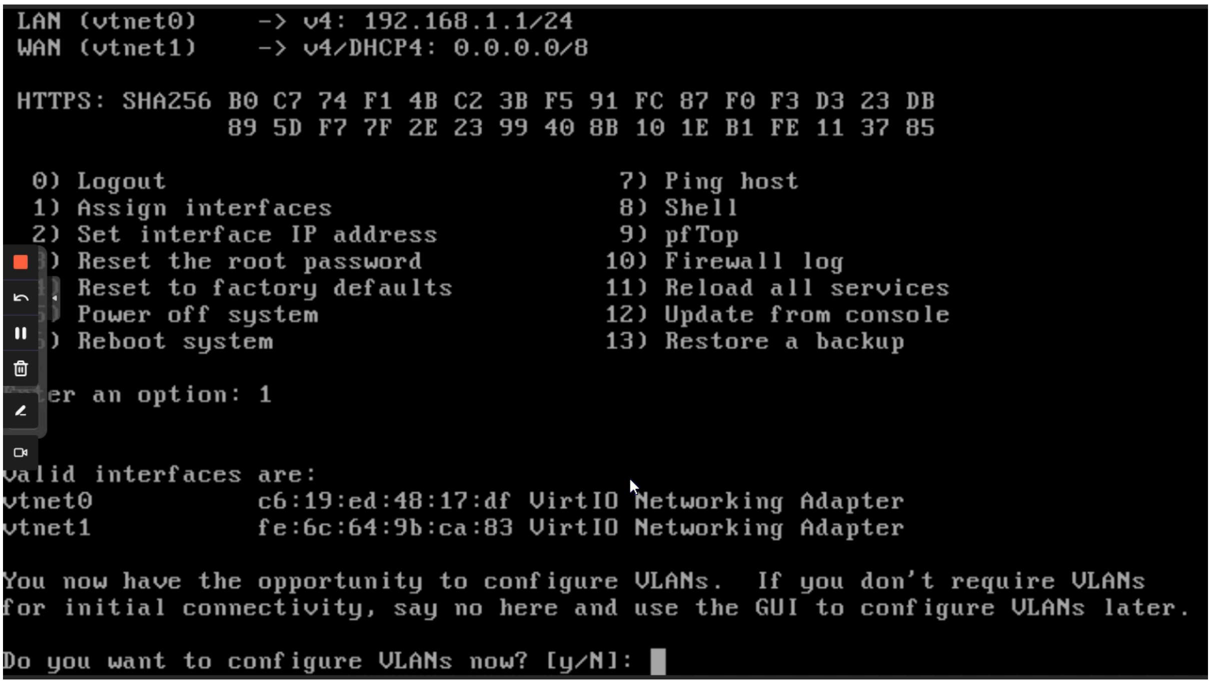


```
|                                                        |        @@@@         @@@@
| Website:      https://opnsense.org/                    |         @@@\\\   ///@@@
| Handbook:     https://docs.opnsense.org/               |       ))))))))   ((((((((
| Forums:       https://forum.opnsense.org/ 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

*** OPNsense.localdomain: OPNsense 21.1 (amd64/OpenSSL) ***

    (vtnet0)     -> v4: 192.168.1.1/24
    (vtnet1)     -> v4/DHCP4: 0.0.0.0/8

   TPS: SHA256 B0 C7 74 F1 4B C2 3B F5 91 FC 87 F0 F3 D3 23 DB
               89 5D F7 7F 2E 23 99 40 8B 10 1E B1 FE 11 37 85

   ) 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 31. *Options menu on OPNsense CLI*

2. Press 1 to Assign interfaces.

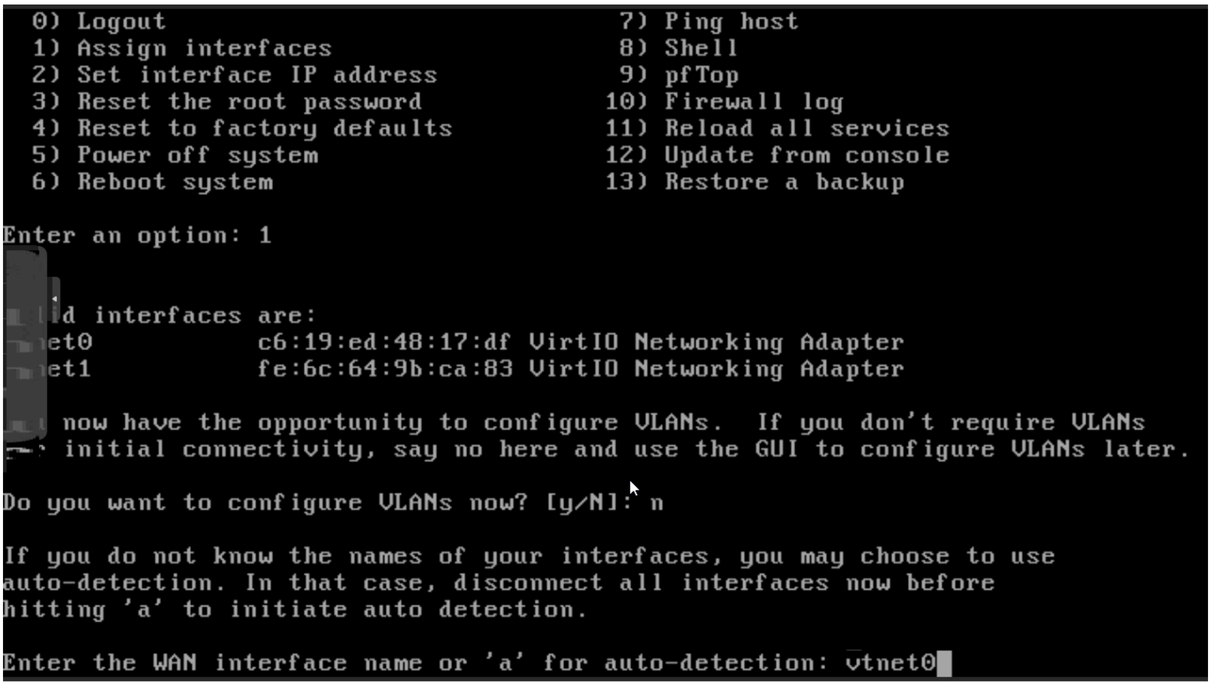
3. **VLAN configuration**: Wizard will ask for the VLAN configuration. You may also configure VLAN settings on OPNsense GUI later. Since we will not configure any VLAN now, Press n to continue.



```
 LAN (vtnet0)     -> v4: 192.168.1.1/24
 WAN (vtnet1)     -> v4/DHCP4: 0.0.0.0/8

 HTTPS: SHA256 B0 C7 74 F1 4B C2 3B F5 91 FC 87 F0 F3 D3 23 DB
               89 5D F7 7F 2E 23 99 40 8B 10 1E B1 FE 11 37 85

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

   er an option: 1


Valid interfaces are:
vtnet0           c6:19:ed:48:17:df VirtIO Networking Adapter
vtnet1           fe:6c:64:9b:ca:83 VirtIO Networking Adapter

You now have the opportunity to configure VLANs.  If you don't require VLANs
for initial connectivity, say no here and use the GUI to configure VLANs later.

Do you want to configure VLANs now? [y/N]: █
```

Figure 32. *VLAN configuration for network interfaces of OPNsense on CLI*

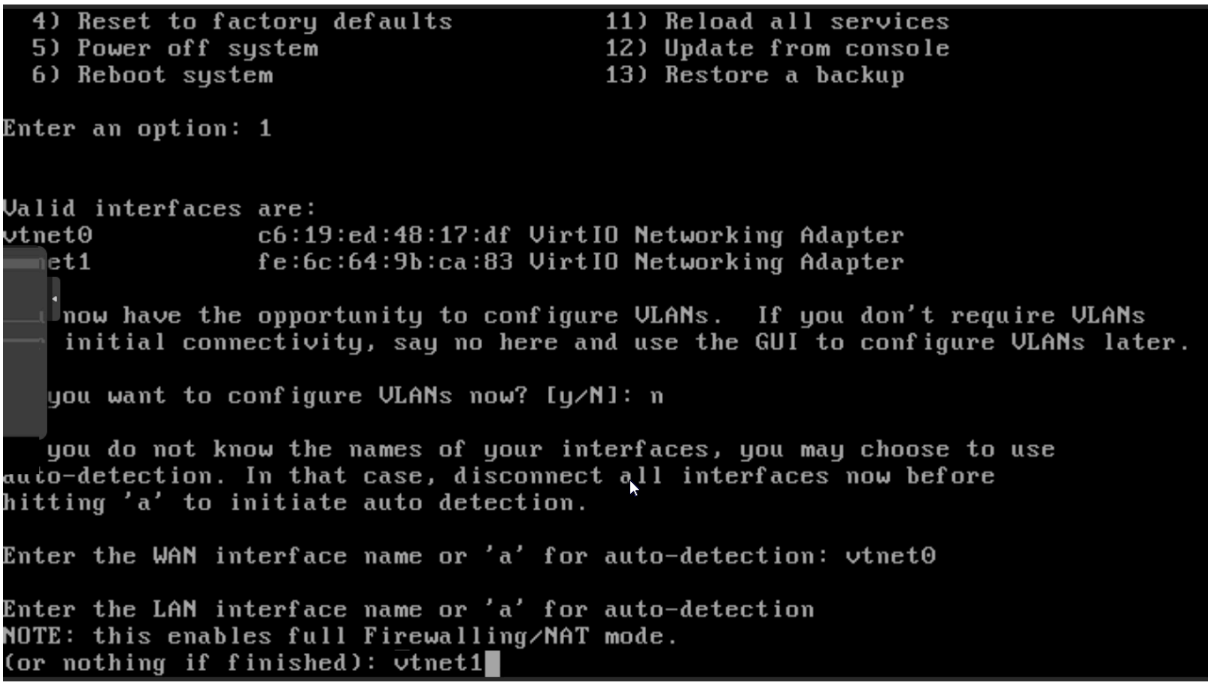
4. **Setting WAN interface**: Wizard will ask for the WAN interface name. Enter the name of the WAN interface and then press enter. For example, in our OPNsense system, the WAN interface name is `vtnet0`.



```
  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: 1


   d interfaces are:
   et0          c6:19:ed:48:17:df VirtIO Networking Adapter
   et1          fe:6c:64:9b:ca:83 VirtIO Networking Adapter

    now have the opportunity to configure VLANs.  If you don't require VLANs
    initial connectivity, say no here and use the GUI to configure VLANs later.

Do you want to configure VLANs now? [y/N]: n

If you do not know the names of your interfaces, you may choose to use
auto-detection. In that case, disconnect all interfaces now before
hitting 'a' to initiate auto detection.

Enter the WAN interface name or 'a' for auto-detection: vtnet0
```

Figure 33. WAN interface assignment on OPNsense CLI

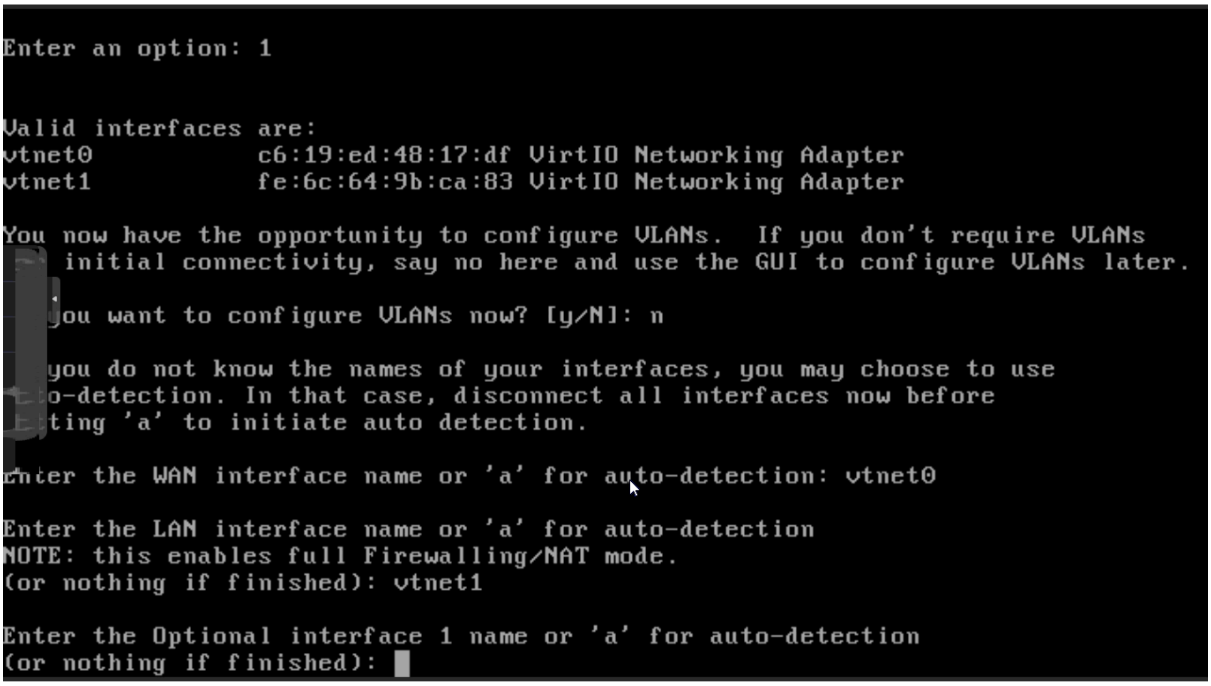
5. **Setting LAN interface**: Wizard will ask for the LAN interface name. Enter the name of the LAN interface and then press enter. For example, in our OPNsense system, the nterface name is `vtnet1`.



```
  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: 1


Valid interfaces are:
vtnet0          c6:19:ed:48:17:df VirtIO Networking Adapter
   et1          fe:6c:64:9b:ca:83 VirtIO Networking Adapter

    now have the opportunity to configure VLANs.  If you don't require VLANs
    initial connectivity, say no here and use the GUI to configure VLANs later.

   you want to configure VLANs now? [y/N]: n

   you do not know the names of your interfaces, you may choose to use
auto-detection. In that case, disconnect all interfaces now before
hitting 'a' to initiate auto detection.

Enter the WAN interface name or 'a' for auto-detection: vtnet0

Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(or nothing if finished): vtnet1
```

Figure 34. LAN interface assignment on OPNsense CLI

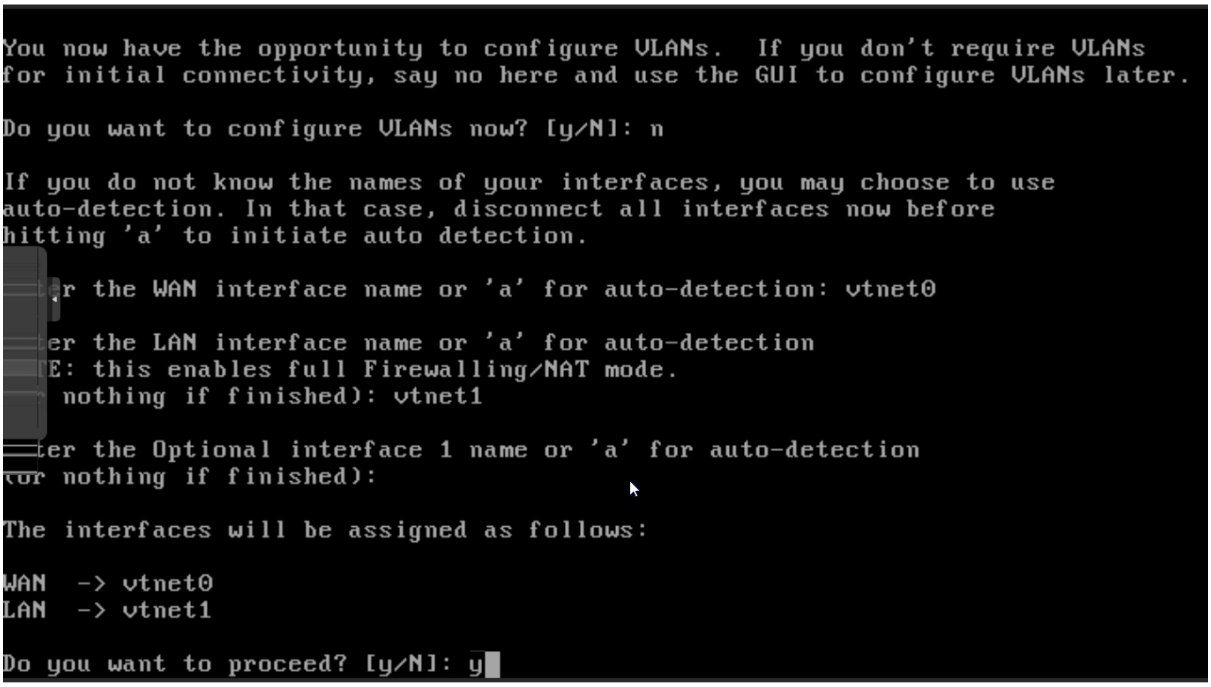
6. **Setting Optional interface**: Since we do not have any other network interface press `enter` to continue.



```
Enter an option: 1

Valid interfaces are:
vtnet0          c6:19:ed:48:17:df VirtIO Networking Adapter
vtnet1          fe:6c:64:9b:ca:83 VirtIO Networking Adapter

You now have the opportunity to configure VLANs.  If you don't require VLANs
for initial connectivity, say no here and use the GUI to configure VLANs later.

Do you want to configure VLANs now? [y/N]: n

If you do not know the names of your interfaces, you may choose to use
auto-detection. In that case, disconnect all interfaces now before
hitting 'a' to initiate auto detection.

Enter the WAN interface name or 'a' for auto-detection: vtnet0

Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(or nothing if finished): vtnet1

Enter the Optional interface 1 name or 'a' for auto-detection
(or nothing if finished):
```

Figure 35. *Optional interface assignment on OPNsense CLI*

7. **Confirmation:** Network interface assignments will be listed. Press `y` to proceed.



```
You now have the opportunity to configure VLANs.  If you don't require VLANs
for initial connectivity, say no here and use the GUI to configure VLANs later.

Do you want to configure VLANs now? [y/N]: n

If you do not know the names of your interfaces, you may choose to use
auto-detection. In that case, disconnect all interfaces now before
hitting 'a' to initiate auto detection.

Enter the WAN interface name or 'a' for auto-detection: vtnet0

Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(or nothing if finished): vtnet1

Enter the Optional interface 1 name or 'a' for auto-detection
(or nothing if finished):

The interfaces will be assigned as follows:

WAN  -> vtnet0
LAN  -> vtnet1

Do you want to proceed? [y/N]: y
```

Figure 36. *Confirming the network interface assignments on OPNsense CLI*

All of the network interfaces on your OPNsense firewall are assigned to the proper networks.

6.2. IP Address Settings for OPNsense Firewall

After assigning the network interfaces to the corresponding networks (WAN and LAN), you should configure the IP address for the network interfaces of your OPNsense firewall.

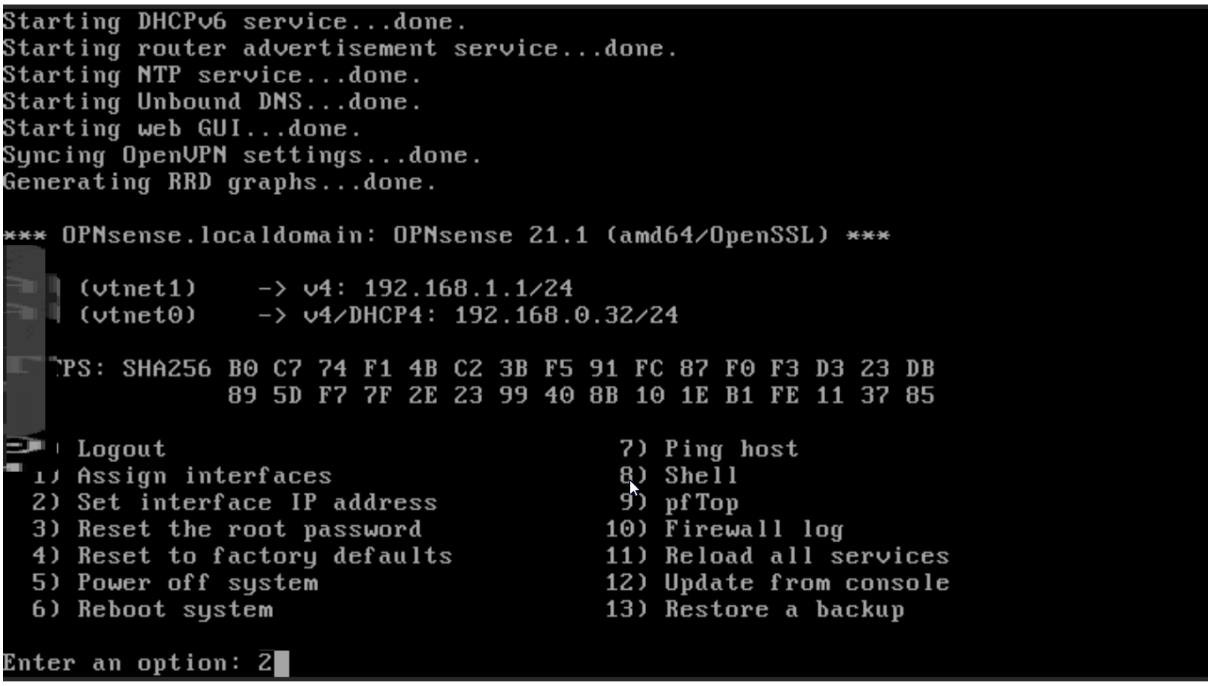
In our OPNsense firewall, we will configure the WAN and LAN interfaces as given below.

Network	Interface name	IP assignment method	IP address
WAN	vtnet0	Automatic via DHCP server	-
LAN	vtnet1	static	10.10.10.1/24

We will enable a DHCP server for LAN on our OPNsense firewall. The DHCP server assigns the IP address in range 10.10.10.11-200/24 for our clients in LAN.

For IP address settings of the OPNsense firewall you can follow the next steps:

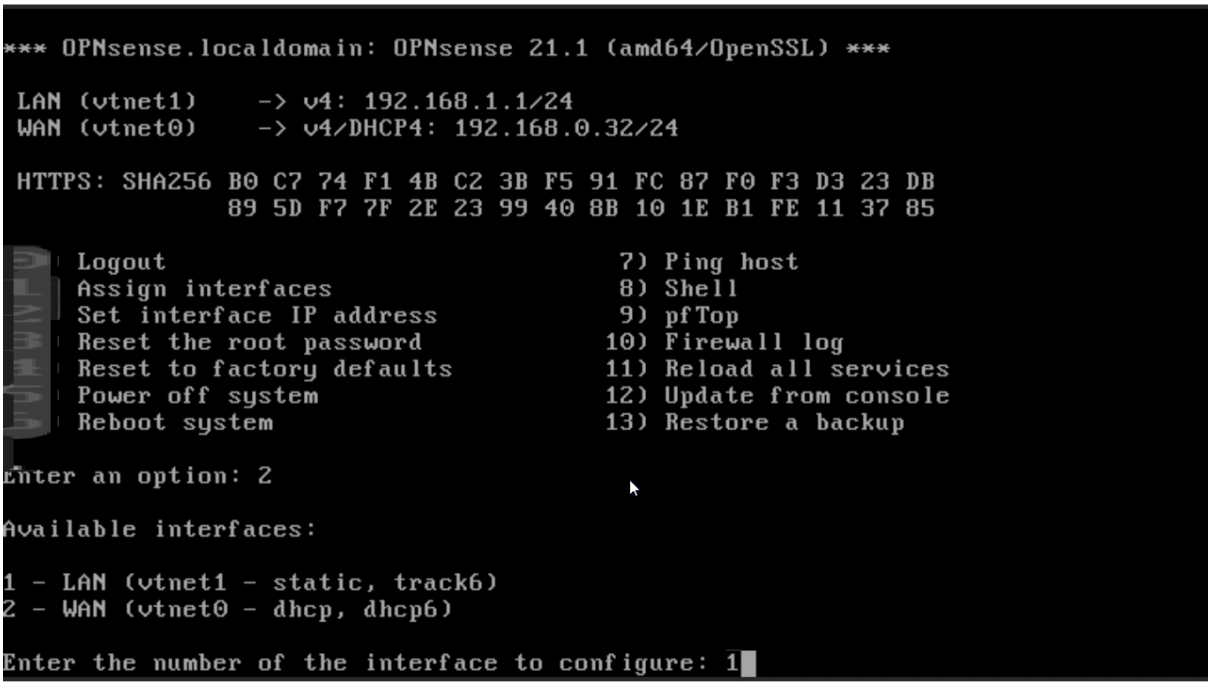
1. Select 2 in the OPNsense options menu to Set `interface IP address.`



```
Starting DHCPv6 service...done.
Starting router advertisement service...done.
Starting NTP service...done.
Starting Unbound DNS...done.
Starting web GUI...done.
Syncing OpenVPN settings...done.
Generating RRD graphs...done.

*** OPNsense.localdomain: OPNsense 21.1 (amd64/OpenSSL) ***

     (vtnet1)    -> v4: 192.168.1.1/24
     (vtnet0)    -> v4/DHCP4: 192.168.0.32/24

    PS: SHA256 B0 C7 74 F1 4B C2 3B F5 91 FC 87 F0 F3 D3 23 DB
               89 5D F7 7F 2E 23 99 40 8B 10 1E B1 FE 11 37 85

     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: 2
```

Figure 37. *Setting IP address for network interface of OPNsense on CLI*

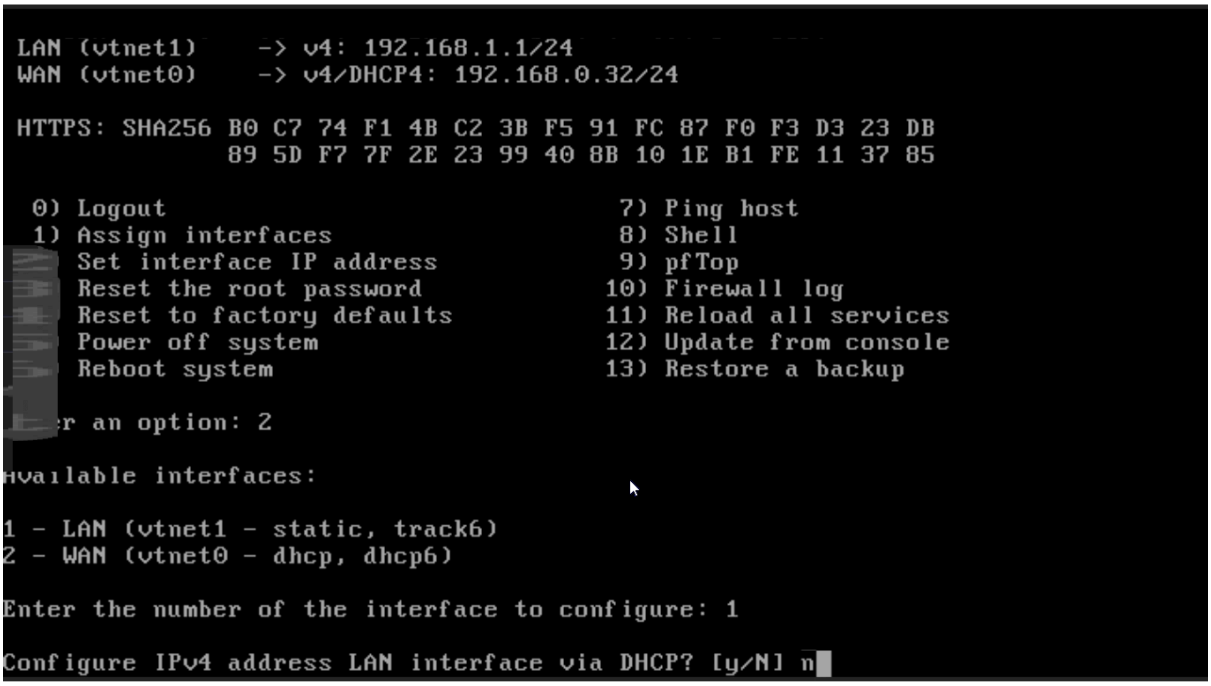
2. Selecting interface to configure: Available interfaces will be displayed. Press 1 to configure the LAN interface.



```
*** OPNsense.localdomain: OPNsense 21.1 (amd64/OpenSSL) ***

 LAN (vtnet1)     -> v4: 192.168.1.1/24
 WAN (vtnet0)     -> v4/DHCP4: 192.168.0.32/24

 HTTPS: SHA256 B0 C7 74 F1 4B C2 3B F5 91 FC 87 F0 F3 D3 23 DB
               89 5D F7 7F 2E 23 99 40 8B 10 1E B1 FE 11 37 85

  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: 2

Available interfaces:

1 - LAN (vtnet1 - static, track6)
2 - WAN (vtnet0 - dhcp, dhcp6)

Enter the number of the interface to configure: 1
```

Figure 38. *Selecting LAN interface to configure on OPNsense CLI*

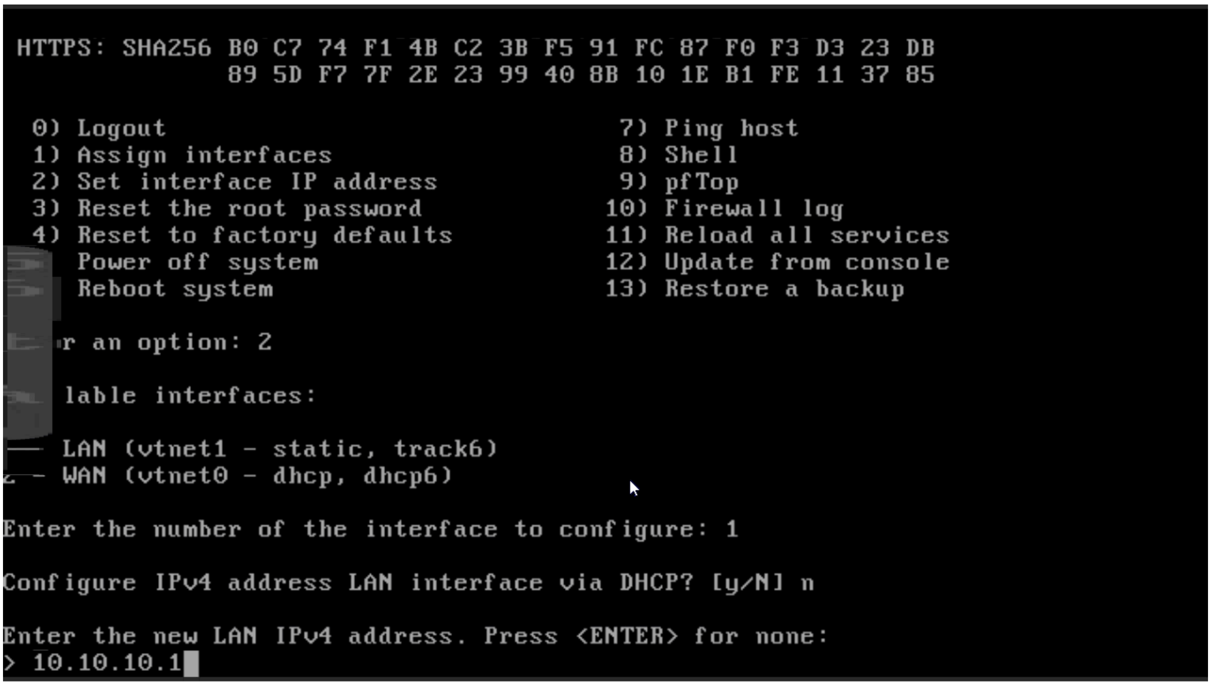
3. IP assignment method. Wizard will ask to configure the IPv4 via the DHCP server. Since we will assign a static IP address manually Press n.



```
 LAN (vtnet1)     -> v4: 192.168.1.1/24
 WAN (vtnet0)     -> v4/DHCP4: 192.168.0.32/24

 HTTPS: SHA256 B0 C7 74 F1 4B C2 3B F5 91 FC 87 F0 F3 D3 23 DB
               89 5D F7 7F 2E 23 99 40 8B 10 1E B1 FE 11 37 85

  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: 2

Available interfaces:

1 - LAN (vtnet1 - static, track6)
2 - WAN (vtnet0 - dhcp, dhcp6)

Enter the number of the interface to configure: 1

Configure IPv4 address LAN interface via DHCP? [y/N] n
```

Figure 39. *Selecting IP assignment for LAN interface on OPNsense CLI*

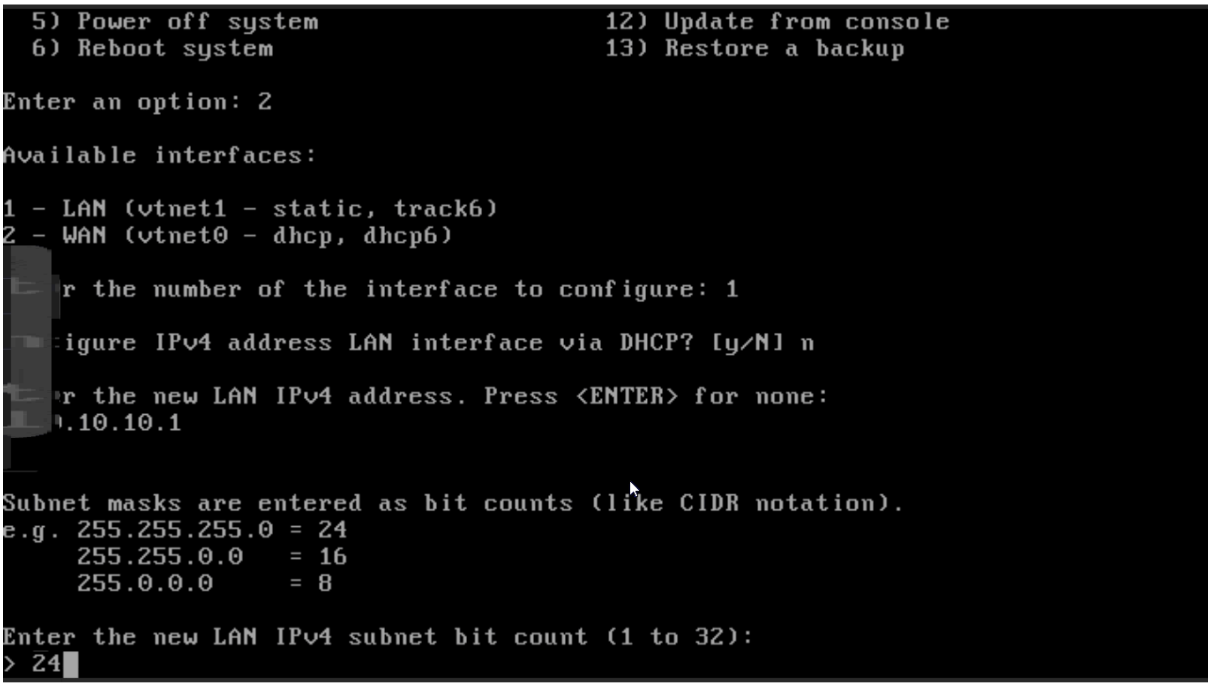
4. **Setting IP address**: Enter the IPv4 address for the LAN interface. For example, 10.10.10.1.



```
HTTPS: SHA256 B0 C7 74 F1 4B C2 3B F5 91 FC 87 F0 F3 D3 23 DB
              89 5D F7 7F 2E 23 99 40 8B 10 1E B1 FE 11 37 85

  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
     Power off system                   12) Update from console
     Reboot system                      13) Restore a backup

    r an option: 2

    lable interfaces:

 ── LAN (vtnet1 - static, track6)
 - WAN (vtnet0 - dhcp, dhcp6)

Enter the number of the interface to configure: 1

Configure IPv4 address LAN interface via DHCP? [y/N] n

Enter the new LAN IPv4 address. Press <ENTER> for none:
> 10.10.10.1
```

Figure 40. Setting IP address for LAN interface on OPNsense CLI

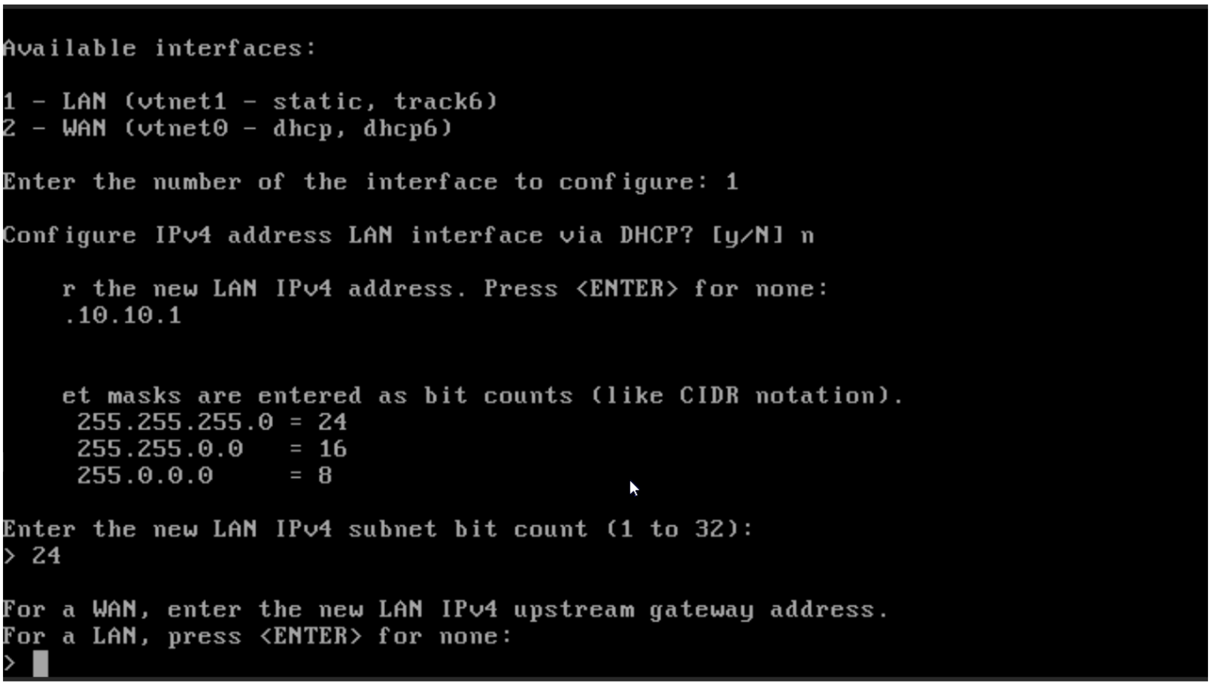
5. **Setting subnet mask**: Enter the subnet mask for the LAN interface. For example, 24.



```
  5) Power off system                   12) Update from console
  6) Reboot system                      13) Restore a backup

Enter an option: 2

Available interfaces:

1 - LAN (vtnet1 - static, track6)
2 - WAN (vtnet0 - dhcp, dhcp6)

    r the number of the interface to configure: 1

    igure IPv4 address LAN interface via DHCP? [y/N] n

    r the new LAN IPv4 address. Press <ENTER> for none:
    .10.10.1


Subnet masks are entered as bit counts (like CIDR notation).
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new LAN IPv4 subnet bit count (1 to 32):
> 24
```

Figure 41. Setting subnet mask for LAN interface on OPNsense CLI

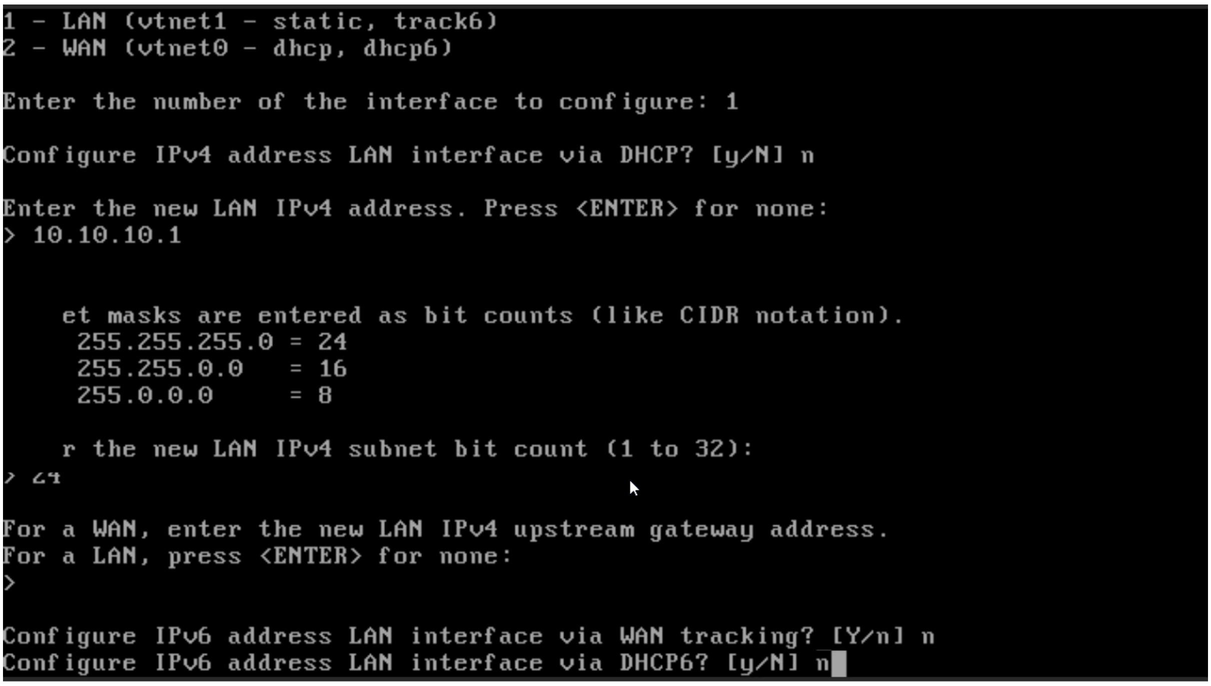
6. **Setting gateway**: Press `enter.`



```
Available interfaces:

1 - LAN (vtnet1 - static, track6)
2 - WAN (vtnet0 - dhcp, dhcp6)

Enter the number of the interface to configure: 1

Configure IPv4 address LAN interface via DHCP? [y/N] n

    r the new LAN IPv4 address. Press <ENTER> for none:
    .10.10.1


    et masks are entered as bit counts (like CIDR notation).
     255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new LAN IPv4 subnet bit count (1 to 32):
> 24

For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
> 
```

Figure 42. *Setting gateway for LAN interface on OPNsense CLI*

7. **Setting IPv6 via WAN tracking**: You may press `n.`
8. **Setting IPv6 via DHCPv6**: You may press `n.`

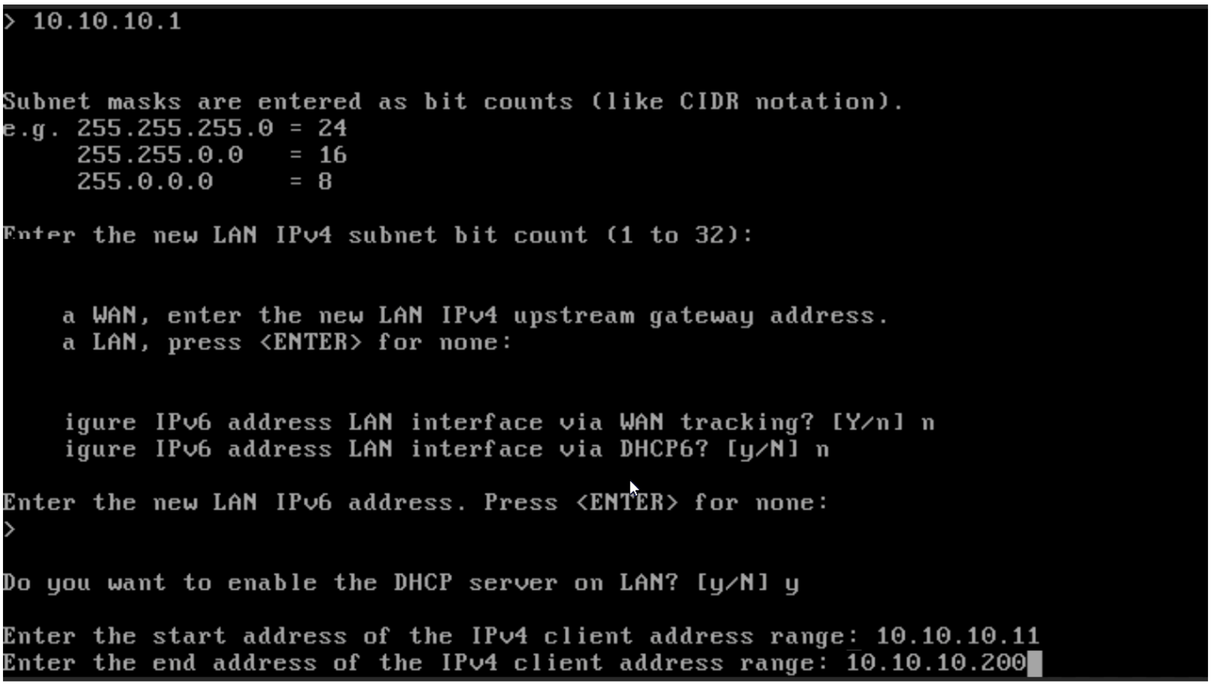


```
1 - LAN (vtnet1 - static, track6)
2 - WAN (vtnet0 - dhcp, dhcp6)

Enter the number of the interface to configure: 1

Configure IPv4 address LAN interface via DHCP? [y/N] n

Enter the new LAN IPv4 address. Press <ENTER> for none:
> 10.10.10.1


    et masks are entered as bit counts (like CIDR notation).
     255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

    r the new LAN IPv4 subnet bit count (1 to 32):
> 24

For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Configure IPv6 address LAN interface via WAN tracking? [Y/n] n
Configure IPv6 address LAN interface via DHCP6? [y/N] n
```

Figure 43. IPv6 settings of LAN interface on OPNsense CLI

9. **Setting IPv6**: You may press `enter.`
10. **Enable DHCP server**: To enable DHCP server on your LAN, press `y.`
11. **Setting start address of the IPv4 client address range**: Enter the start address of the IPv4 client address range such as 10.10.10.11.

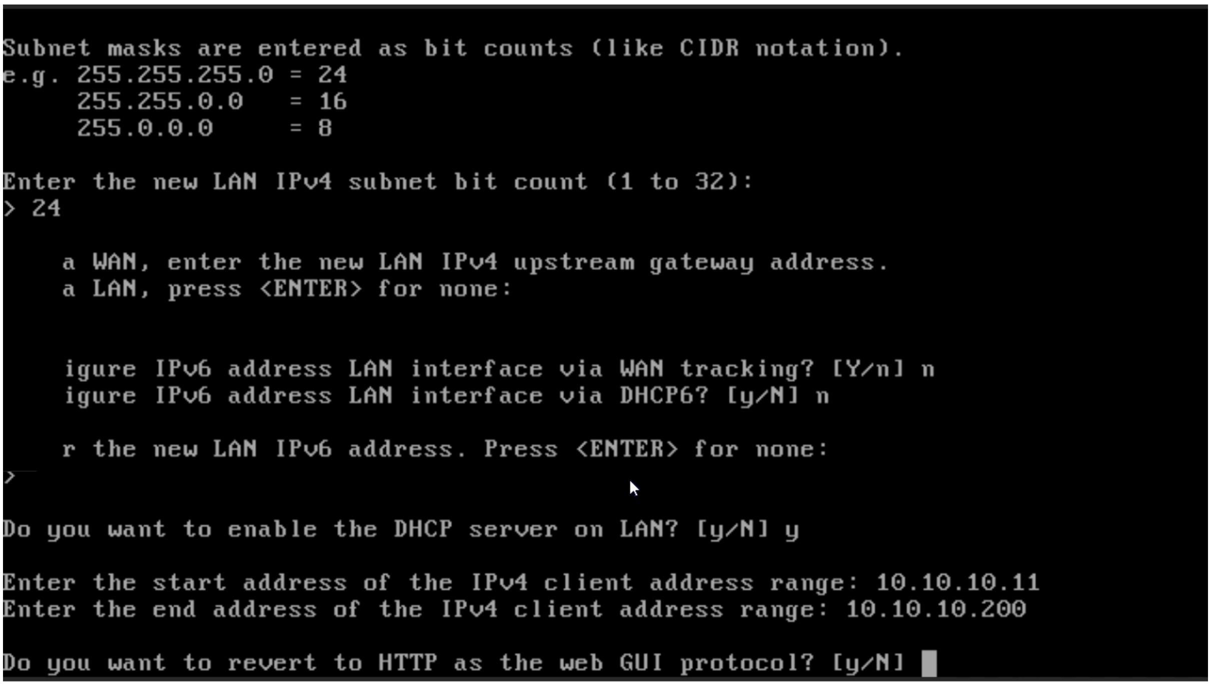
12. **Setting end address of the IPv4 client address range**: Enter the end address of the IPv4 client address range such as 10.10.10.200.



```
> 10.10.10.1

Subnet masks are entered as bit counts (like CIDR notation).
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new LAN IPv4 subnet bit count (1 to 32):


    a WAN, enter the new LAN IPv4 upstream gateway address.
    a LAN, press <ENTER> for none:


    igure IPv6 address LAN interface via WAN tracking? [Y/n] n
    igure IPv6 address LAN interface via DHCP6? [y/N] n

Enter the new LAN IPv6 address. Press <ENTER> for none:
>

Do you want to enable the DHCP server on LAN? [y/N] y

Enter the start address of the IPv4 client address range: 10.10.10.11
Enter the end address of the IPv4 client address range: 10.10.10.200
```

Figure 44. *Configuring DHCP server on LAN interface of OPNsense*

13. **Enabling HTTP**: pressing n you may access the OPNsense GUI via HTTPS protocol which is secure. If you wish to use the web interface with HTTP you may press y.



```
Subnet masks are entered as bit counts (like CIDR notation).
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new LAN IPv4 subnet bit count (1 to 32):
> 24

    a WAN, enter the new LAN IPv4 upstream gateway address.
    a LAN, press <ENTER> for none:


    igure IPv6 address LAN interface via WAN tracking? [Y/n] n
    igure IPv6 address LAN interface via DHCP6? [y/N] n

    r the new LAN IPv6 address. Press <ENTER> for none:
>

Do you want to enable the DHCP server on LAN? [y/N] y

Enter the start address of the IPv4 client address range: 10.10.10.11
Enter the end address of the IPv4 client address range: 10.10.10.200

Do you want to revert to HTTP as the web GUI protocol? [y/N]
```

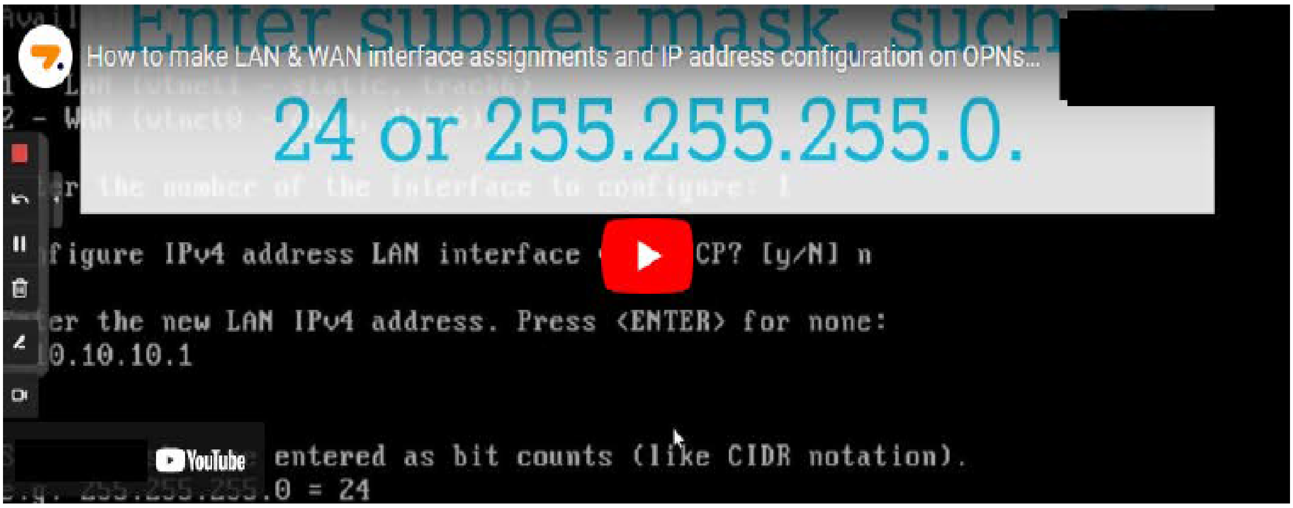
Figure 45. *HTTP setting for the OPNsense web GUI*

14. Restore web GUI defaults. Press n. By pressing y you can access the OPNsense GUI with default user and password.

📝**NOTE**

Default OPNsense user: root

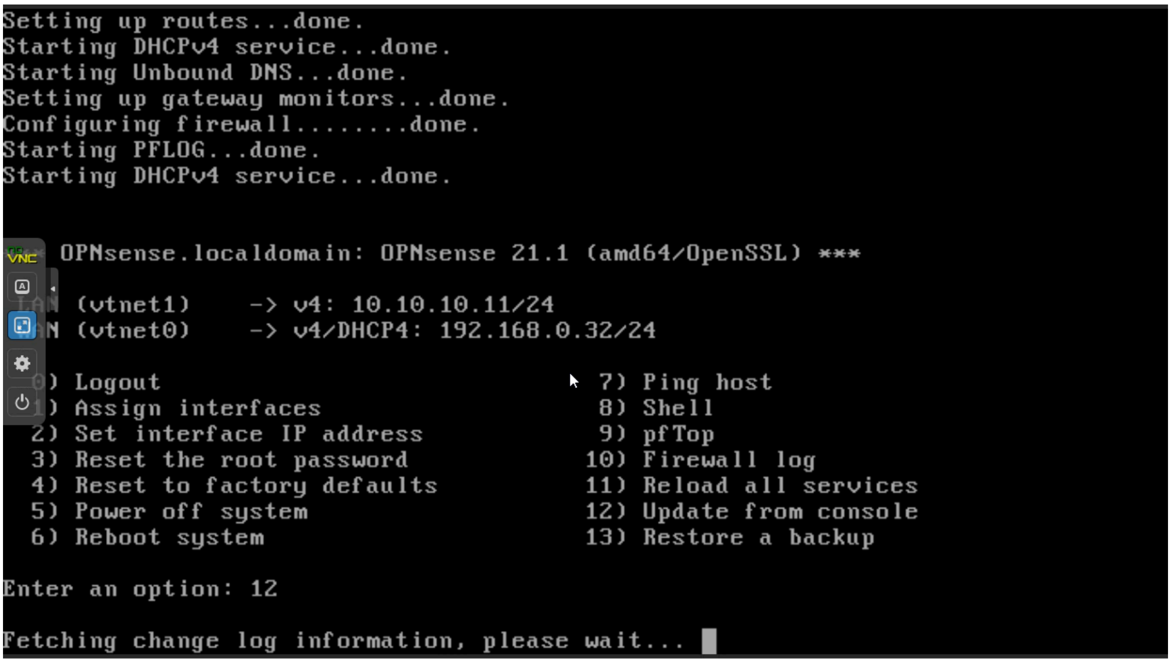
Default OPNsense password: opnsense


How to make LAN & WAN interface assignments and IP address configuration on OPNs...
Enter subnet mask, such
24 or 255.255.255.0.
YouTube

```
1 - LAN (vtnet1 - static, track6)
2 - WAN (vtnet0 - dhcp, dhcp6)

r the number of the interface to configure: 1

figure IPv4 address LAN interface    CP? [y/N] n

er the new LAN IPv4 address. Press <ENTER> for none:
0.10.10.1

                  entered as bit counts (like CIDR notation).
.g. 255.255.255.0 = 24
```

6.3. Updating OPNsense Firewall on CLI

After completing the OPNsense firewall installation on Proxmox VE, you should update your firewall. You can easily update the OPNsense system by selecting `12) Update from console` in the options menu on CLI.



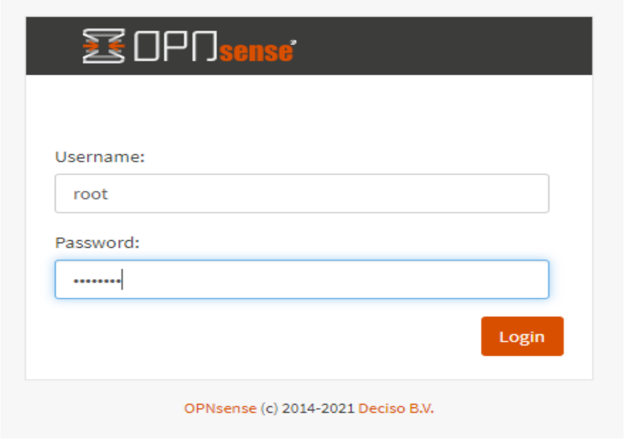
```
Setting up routes...done.
Starting DHCPv4 service...done.
Starting Unbound DNS...done.
Setting up gateway monitors...done.
Configuring firewall........done.
Starting PFLOG...done.
Starting DHCPv4 service...done.


    OPNsense.localdomain: OPNsense 21.1 (amd64/OpenSSL) ***

 LAN (vtnet1)     -> v4: 10.10.10.11/24
 WAN (vtnet0)     -> v4/DHCP4: 192.168.0.32/24

  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: 12

Fetching change log information, please wait...
```

Figure 46. *Updating OPNsense firewall from the console*

> ⚠️ **CAUTION**
>
> Beware that some critical updates require your system to reboot.

6.4. Accessing the OPNsense Web GUI

Congratulations! You have successfully completed the installation of the OPNsense firewall. You can access the web GUI of your OPNsense firewall from a client in LAN using a browser. `https://10.10.10.1` or `http://10.10.10.1`.



Username:

root

Password:

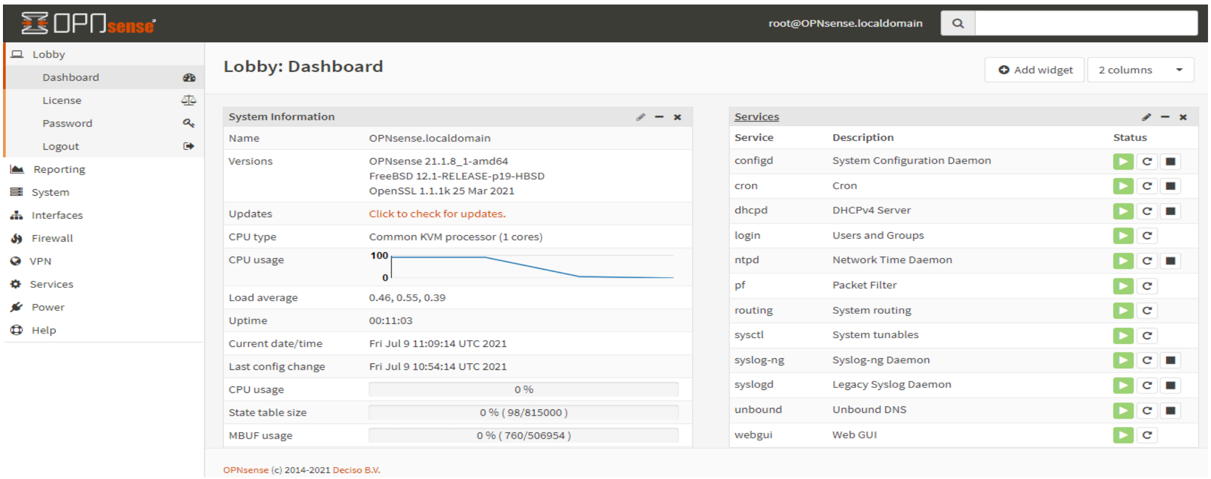
••••••••

OPNsense (c) 2014-2021 Deciso B.V.

Figure 47. *Login OPNsense GUI*

> 💡 **TIP**
>
> For security reasons ssh is disabled by default and the console access is password protected on the OPNsense firewall.

When you log in OPNsense GUI, the Dashboard page will be displayed.



Lobby: Dashboard

System Information	
Name	OPNsense.localdomain
Versions	OPNsense 21.1.8_1-amd64 FreeBSD 12.1-RELEASE-p19-HBSD OpenSSL 1.1.1k 25 Mar 2021
Updates	Click to check for updates.
CPU type	Common KVM processor (1 cores)
CPU usage	
Load average	0.46, 0.55, 0.39
Uptime	00:11:03
Current date/time	Fri Jul 9 11:09:14 UTC 2021
Last config change	Fri Jul 9 10:54:14 UTC 2021
CPU usage	0 %
State table size	0 % (98/815000)
MBUF usage	0 % (760/506954)

Services

Service	Description	Status
configd	System Configuration Daemon	▶ C ■
cron	Cron	▶ C ■
dhcpd	DHCPv4 Server	▶ C ■
login	Users and Groups	▶ C
ntpd	Network Time Daemon	▶ C ■
pf	Packet Filter	▶ C
routing	System routing	▶ C
sysctl	System tunables	▶ C
syslog-ng	Syslog-ng Daemon	▶ C ■
syslogd	Legacy Syslog Daemon	▶ C ■
unbound	Unbound DNS	▶ C ■
webgui	Web GUI	▶ C

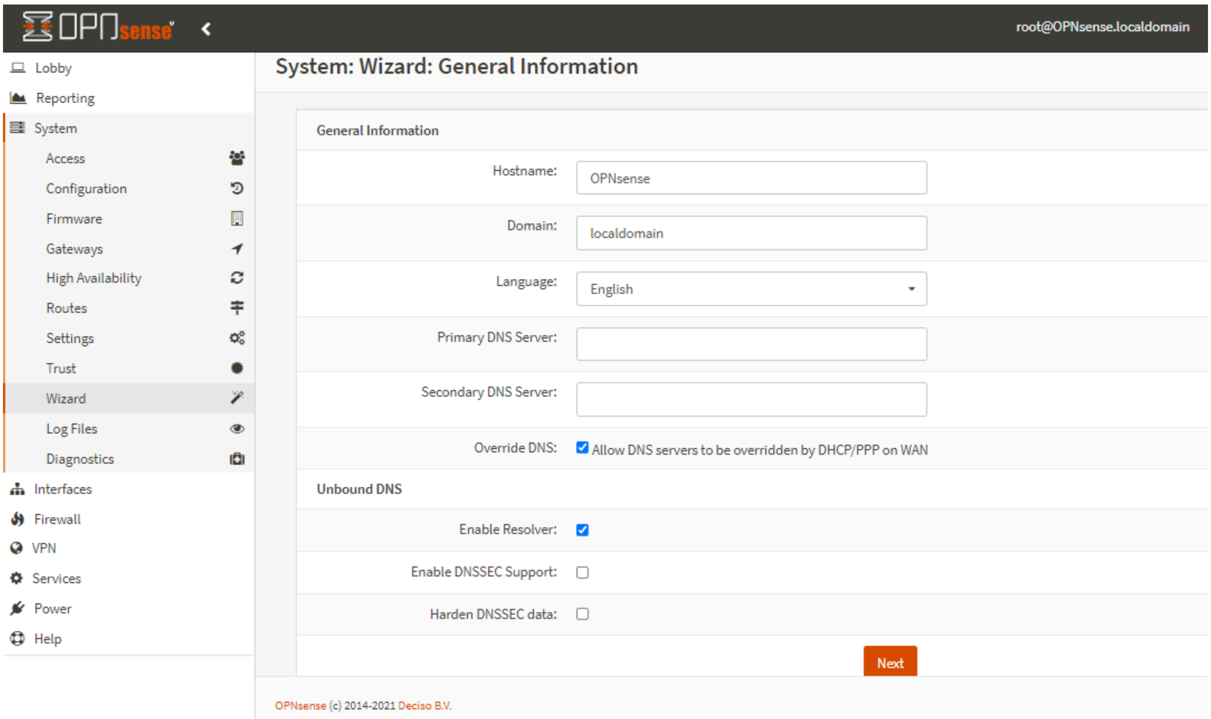
OPNsense (c) 2014-2021 Deciso B.V.

Figure 48. *OPNsense dashboard*

6.5. Initial Configuration of the OPNsense Firewall

To complete the initial configuration of your OPNsense firewall, you can follow the given steps below:

1. Navigate to the `System -> Wizard` on OPNsense Web GUI.
2. This wizard will guide you through the initial system configuration. Click the `Next` button.
3. You may set your hostname and domain name for your device. You may leave the `Override DNS` option selected. This will enable the OpnSense firewall to obtain DNS information from the ISP over the WAN interface. Then, click the `Next` button.



System: Wizard: General Information

General Information

Hostname: OPNsense

Domain: localdomain

Language: English

Primary DNS Server:

Secondary DNS Server:

Override DNS: ☑ Allow DNS servers to be overridden by DHCP/PPP on WAN

Unbound DNS

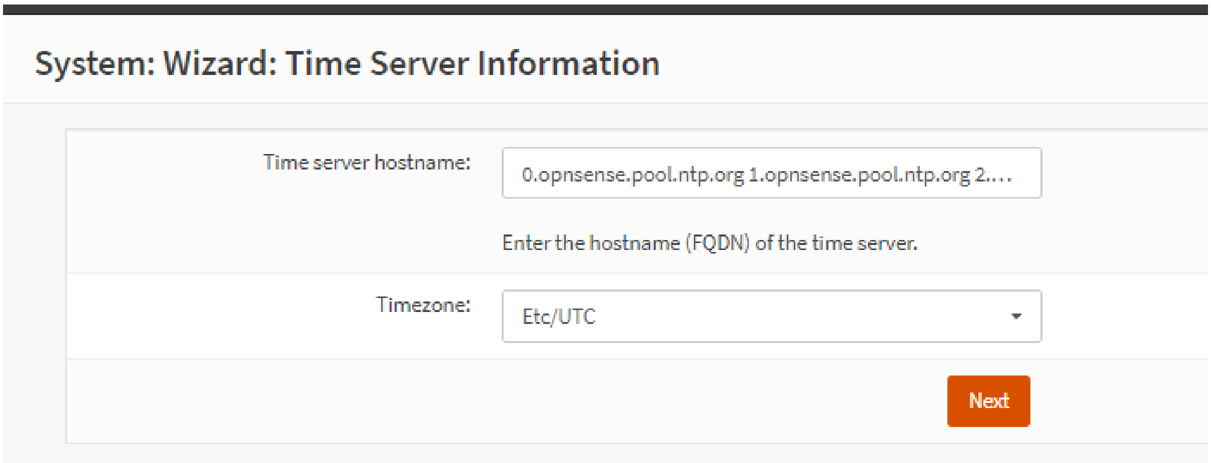
Enable Resolver: ☑

Enable DNSSEC Support: □

Harden DNSSEC data: □

Figure 49. *Initial configuration of OPNsense*

4. Set `NTP server and timezone` for your OPNsense firewall. If you do not have your own NTP systems, OpnSense will provide a default set of NTP server pools. Then, click the `Next` button.



System: Wizard: Time Server Information

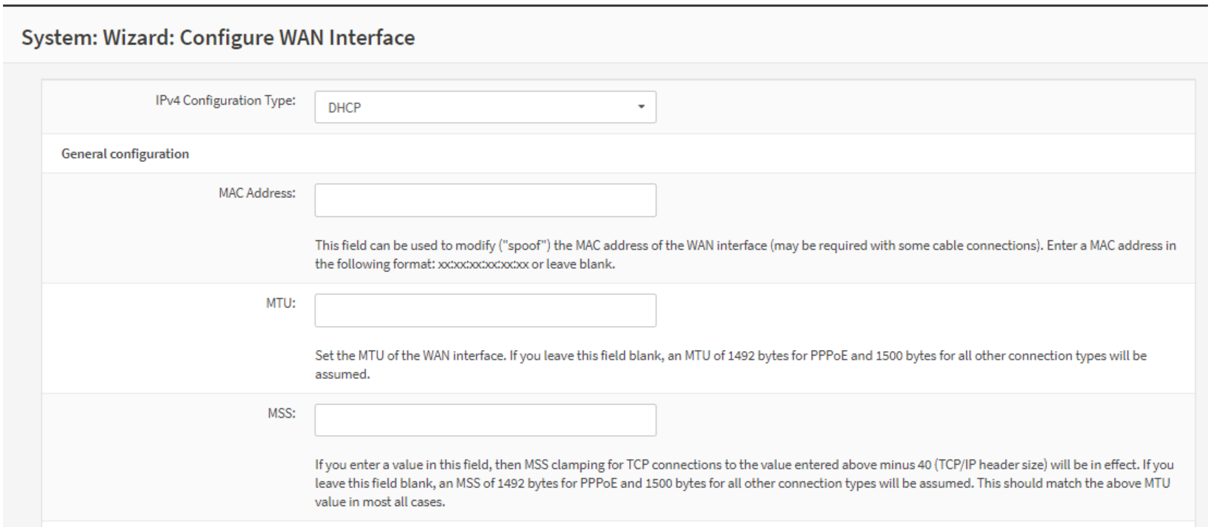
Time server hostname: 0.opnsense.pool.ntp.org 1.opnsense.pool.ntp.org 2....

Enter the hostname (FQDN) of the time server.

Timezone: Etc/UTC

Figure 50. *Setting NTP server and Timezone on OPNsense GUI*

5. You may change the WAN interface configurations or leave them as default. You should leave `RFC1918` Networks settings as checked for security reasons.



System: Wizard: Configure WAN Interface

IPv4 Configuration Type: DHCP

General configuration

MAC Address:

This field can be used to modify ("spoof") the MAC address of the WAN interface (may be required with some cable connections). Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank.

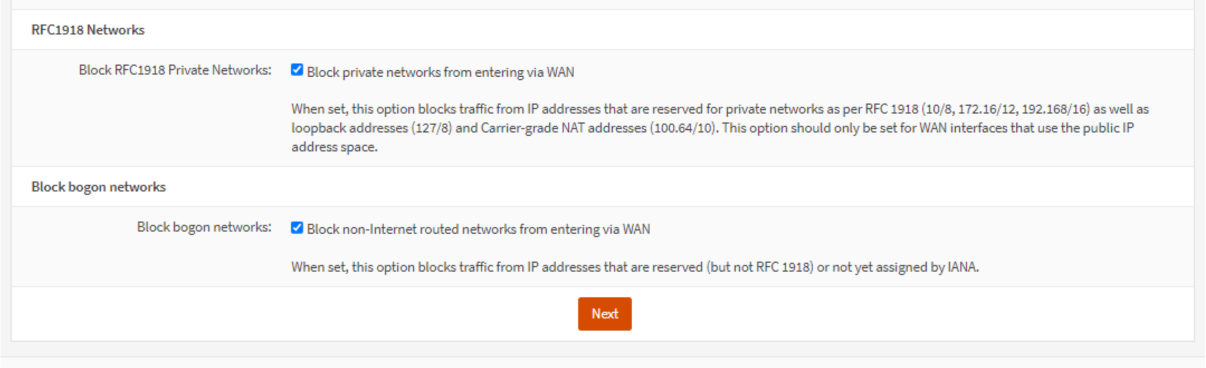
MTU:

Set the MTU of the WAN interface. If you leave this field blank, an MTU of 1492 bytes for PPPoE and 1500 bytes for all other connection types will be assumed.

MSS:

If you enter a value in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect. If you leave this field blank, an MSS of 1492 bytes for PPPoE and 1500 bytes for all other connection types will be assumed. This should match the above MTU value in most all cases.

Figure 51. *WAN interface configuration on OPNsense GUI*



RFC1918 Networks

Block RFC1918 Private Networks: ☑ Block private networks from entering via WAN

When set, this option blocks traffic from IP addresses that are reserved for private networks as per RFC 1918 (10/8, 172.16/12, 192.168/16) as well as loopback addresses (127/8) and Carrier-grade NAT addresses (100.64/10). This option should only be set for WAN interfaces that use the public IP address space.

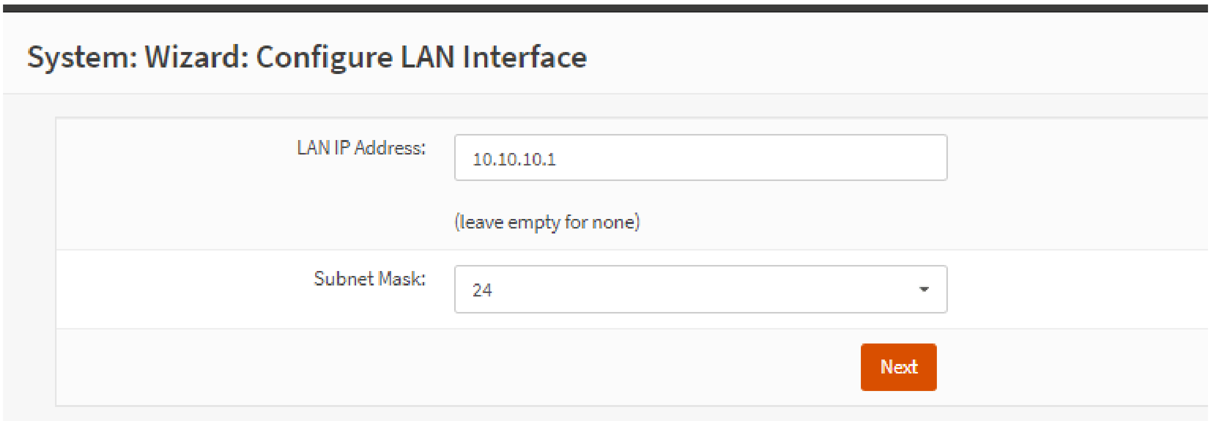
Block bogon networks

Block bogon networks: ☑ Block non-Internet routed networks from entering via WAN

When set, this option blocks traffic from IP addresses that are reserved (but not RFC 1918) or not yet assigned by IANA.

Figure 52. *RFC1918 Networks settings for WAN interface on OPNsense GUI*

6. You may change the LAN interface configurations or leave it as default.



System: Wizard: Configure LAN Interface

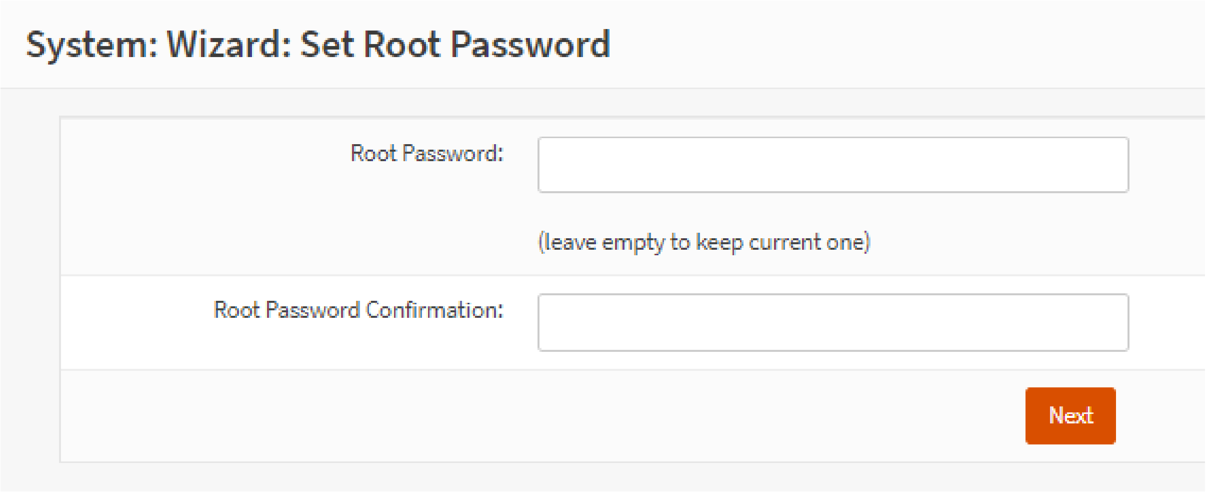
LAN IP Address: 10.10.10.1

(leave empty for none)

Subnet Mask: 24

Figure 53. *LAN interface configuration on OPNsense GUI*

7. You may change the `root` password or leave it as before.



System: Wizard: Set Root Password

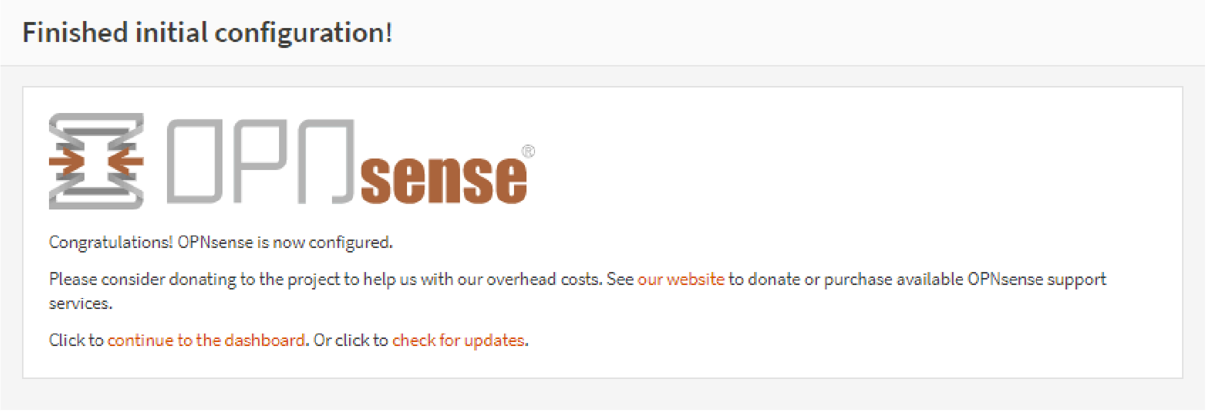
Root Password:

(leave empty to keep current one)

Root Password Confirmation:

Figure 54. *Setting root password on OPNsense GUI*

8. Click `Reload` to apply the changes.
9. When everything is completed successfully, OpnSense will welcome the user. You can get back to the main dashboard, by clicking `Dashboard` in the upper left corner of the web browser window.



Finished initial configuration!

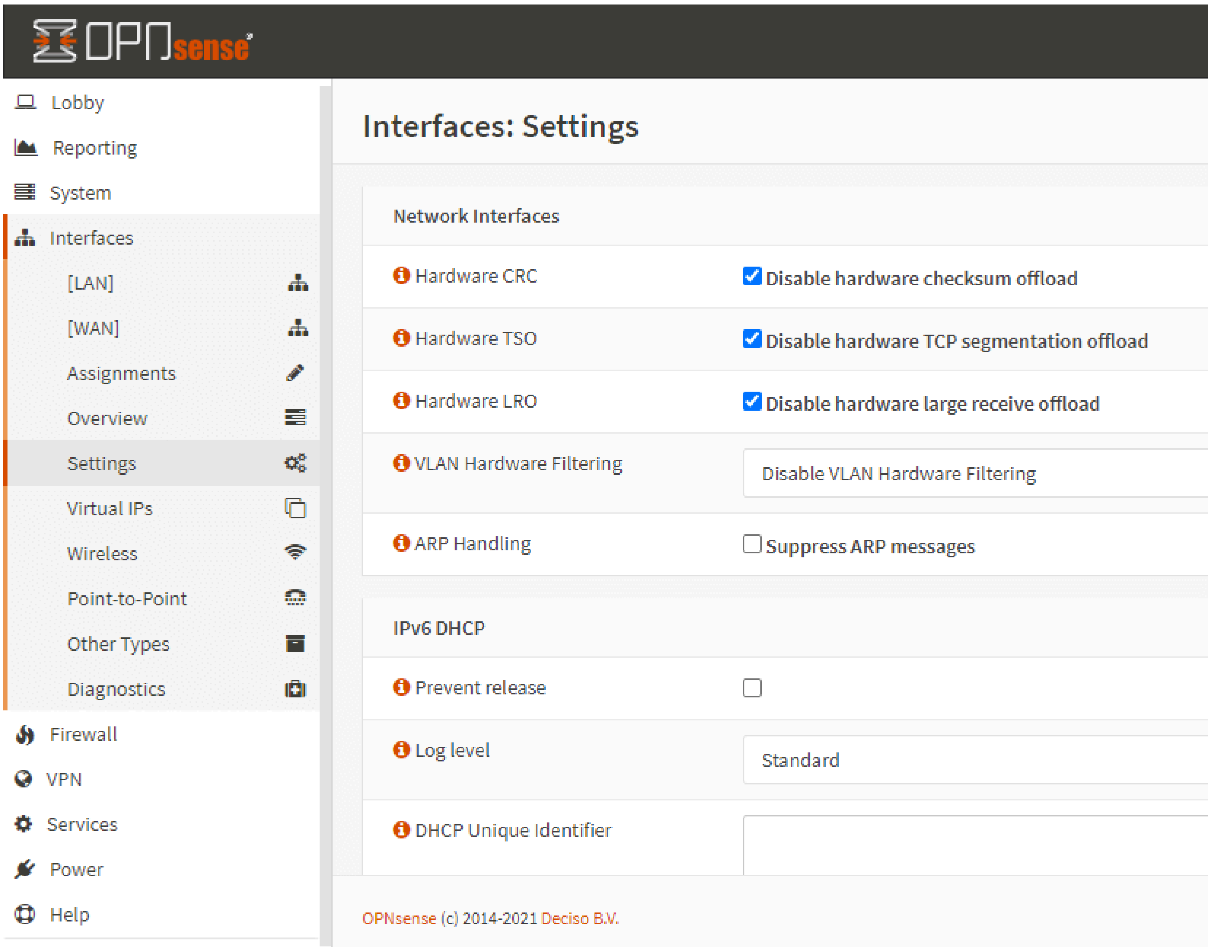
Congratulations! OPNsense is now configured.

Please consider donating to the project to help us with our overhead costs. See our website to donate or purchase available OPNsense support services.

Click to continue to the dashboard. Or click to check for updates.

Figure 55. *Finished initial configuration of OPNsense firewall*

6.6. Disable Network Hardware Off-loading on OPNsense Firewall



Interfaces: Settings

Network Interfaces

Hardware CRC	☑ Disable hardware checksum offload
Hardware TSO	☑ Disable hardware TCP segmentation offload
Hardware LRO	☑ Disable hardware large receive offload
VLAN Hardware Filtering	Disable VLAN Hardware Filtering
ARP Handling	□ Suppress ARP messages

IPv6 DHCP

Prevent release	□
Log level	Standard
DHCP Unique Identifier	

OPNsense (c) 2014-2021 Deciso B.V.

Figure 56. *Disabling hardware offloading on OPNsense GUI*

After finishing the installation of the OPNsense, you should ensure that hardware offload features are disabled on the network interfaces. Because VirtIO interfaces have problems with NAT. To disable the hardware offloading on the network interface,

- Navigate to `Interfaces -> Settings` on OPNsense GUI.
- Set `Hardware CRC`, `Hardware TSO`, and `Hardware LRO` to Disable.
- Click `Save`.
- `Reboot` the firewall.

How to Install OPNsense from USB

OPNsense is an open-source firewall distribution based on FreeBSD. There are also DHCP servers, DNS servers, VPNs, and other services available in addition to the firewall. OPNsense has a number of advantages over competitors, including forward caching proxy, traffic shaping, intrusion detection, and a simple OpenVPN client setup. The Zenarmor plugin, in particular, which provides application control and web filtering features, is extremely useful for administrators in protecting their networks from cyberattacks. OPNsense's dependable update mechanism allows it to deliver critical security updates on time.

For more information about the OPNsense features, please refer to the Best Open Source Firewalls article written by Zenarmor.

💡**BEST PRACTICE**

Zenarmor NGFW Plug-in for OPNsense is one of the most popular OPNsense plug-ins and allows you to easily upgrade your firewall to a Next Generation Firewall in seconds. NG Firewalls empower you to combat modern-day cyber attacks that are becoming more sophisticated every day.

Some of the capabilities are layer-7 application/user aware blocking, granular filtering policies, commercial-grade web filtering utilizing cloud-delivered AI-based Threat Intelligence, parental controls, and the industry's best network analytics and reporting.

Zenarmor Free Edition is available at no cost for all OPNsense users.

In this OPNsense installation guide, we will cover how to install OPNsense from a USB stick by describing the following topics.

- What are the System Requirements for OPNSense Setup?
- Where to Download OPNSense?
- How to Install OPNSense Files?
- Step 1: Selecting Hardware
- Step 2: Downloading OPNSense ISO
- Step 3: Writing OPNsense Image to Installation Media
- Step 4: Installing OPNSense from USB to Target Device
- Step 5: Completing OPNSense Initial Configuration

What are the System Requirements for OPNSense Setup?

You should check the hardware requirements for the installation before installing the OPNsense firewall. Up-to-date requirements can be found on the official website.

OPNsense supports a variety of devices ranging from embedded systems to rack-mounted servers. But, the hardware must be capable of running 64-bit operating systems. Since only x86-64 (amd64)bit microprocessor architectures are supported by OPNsense.

Full installs can run on solid-state disks (SSD), hard disk drives (HDD), or SD memory cards.

The option to install an embedded OPNsense image has been supported since version 15.1.10 (04 May 2015).

Embedded images (nano) only keep logging and cache data in memory, whereas full image versions keep the data on the local drive. By enabling RAM disks, a full version can mimic the behavior of an embedded version, which is especially useful for SD memory card installations.

OPNsense is built on `HardenedBSD 11.2-RELEASE`. The OPNsense kernel includes all HardenedBSD drivers, and hardware compatibility is the same.

The hardware requirements of the OPNsense may be constrained for its functionality. There are minimum, reasonable, and recommended system requirements for the full functionality of OPNsense. At the time of the writing, the hardware requirements of the OPNsense are given as below.

1. Minimum System Requirements

If you install OPNsense on a device that meets these requirements, you will be unable to use features that require disks writes, such as a caching proxy (cache) or intrusion detection and prevention.

Type	Description
Processor	1 GHz dual-core CPU
RAM	2 GB
Install method	Serial console or video (VGA)
Install target	SD or CF card with a minimum of 4 GB, use nano images for installation.

Table 1: *Minimum system requirements*

2. Reasonable System Requirements

If you install OPNsense on a device that meets these requirements, you will be able to use all of the standard features of the OPNsense. However, if you have a large number of users or a high load, you may run into some issues.

Type	Description
Processor	1 GHz dual-core CPU
RAM	4 GB
Install method	Serial console or video (VGA)
Install target	40 GB SSD, a minimum of 2 GB memory is needed for the installer to run.

Table 2: *Reasonable system requirements*

3. Recommended System Requirements

If you install OPNsense on a device that meets these requirements, you will be able to use all of the OPNsense's standard features without issue.

Type	Description
Processor	1.5 GHz multi-core CPU
RAM	8 GB
Install method	Serial console or video (VGA)
Install target	120 GB SSD

Table 3: *Recommended system requirements*

Where to Download OPNSense?

Depending on your hardware and use case different installation files are provided to download and install OPNsense:

- `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.

Sample file listing

- OPNsense-21.7.1-OpenSSL-cdrom-amd64.iso.bz2
- OPNsense-21.7.1-OpenSSL-nano-amd64.img.bz2
- OPNsense-21.7.1-OpenSSL-serial-amd64.img.bz2
- OPNsense-21.7.1-OpenSSL-vga-amd64.img.bz2

The USB-memstick installer is the simplest way to install OPNsense. If your target platform has a serial interface, download the serial image. If not, you should select `vga` for the image type. You may choose any mirror for your liking.

How to Install OPNSense Files?

You may easily install the OPNsense firewall by following the 5 steps given below.

Step 1: Selecting Hardware

While the majority of features have no effect on hardware dimensioning, a few do. The candidates are as follows:

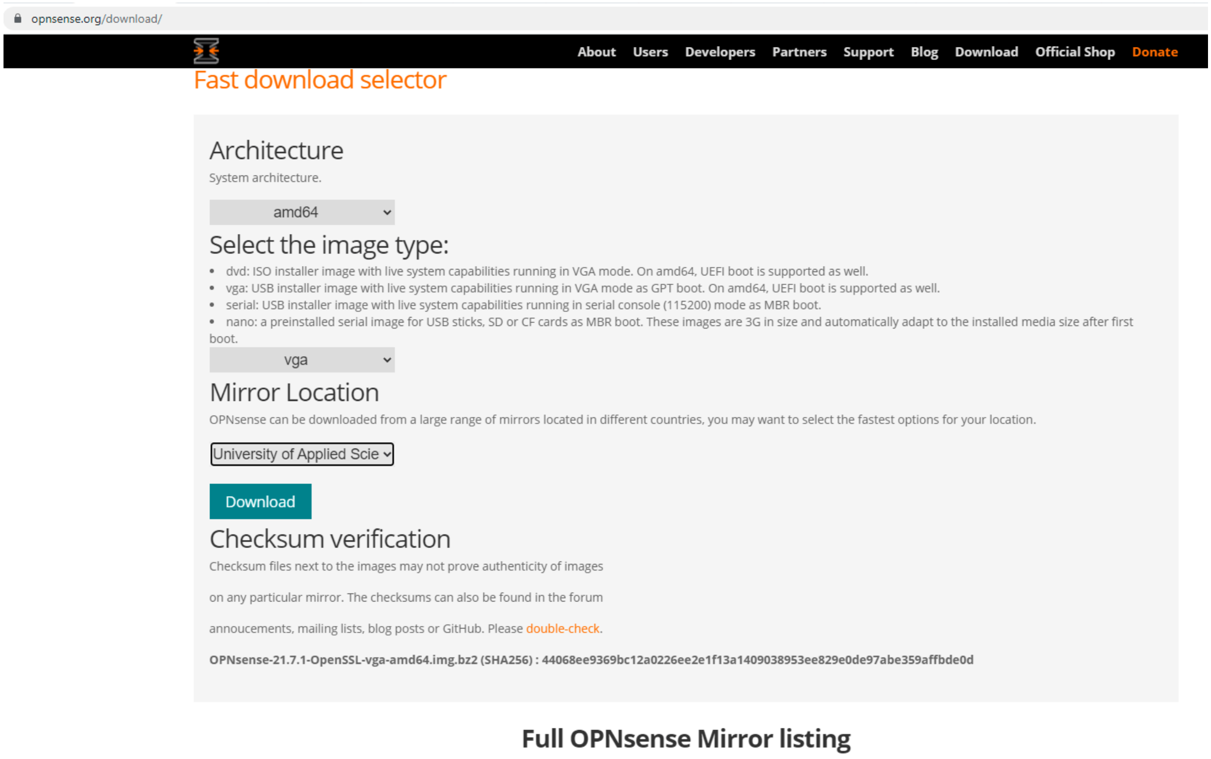
- Squid: A caching web proxy that is used for web-content control, and so on. These packages are heavily reliant on CPU load and disk-cache writes.
- Captive Portal: Settings with hundreds of concurrently served captive portal users will necessitate high CPU power
- State transition tables: Each state table entry requires approximately 1 kB (kilobytes) of RAM. A typical state table with 1000 entries will take up about 10 MB (megabytes) of RAM. OPNsense usage settings with hundreds of thousands of connections will necessitate additional memory.

You should select the hardware according to the system requirements given above.

Step 2: Downloading OPNSense ISO

You may download the OPNsense installation file from the official OPNsense download page. You may select system architecture according to your system's CPU architecture, and also specify image type and mirror location as well. `OPNsense ISO` Download steps are given below.

- Select `vga` image type for USB installation
- Select the fastest mirror for your location
- Click `Download` button.



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.

vga

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.

University of Applied Scie

Download

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-21.7.1-OpenSSL-vga-amd64.img.bz2 (SHA256) : 44068ee9369bc12a0226ee2e1f13a1409038953ee829e0de97abe359affbde0d

Full OPNsense Mirror listing

Figure 1. *Downloading OPNsense vga ISO file*

Step 3: Writing OPNsense Image to Installation Media

After downloading the OPNsense image, you need to unpack it first by running the following command..

```
bunzip2 OPNsense-21.7.1-OpenSSL-vga-amd64.img.bz2
```

Then, you may write the image to a USB flash drive (>= 1GB), either with `dd` under FreeBSD or under Windows with `physdiskwrite (or Rufus).`

Writing an OPNsense image to a USB is explained in detail below for various platforms.

1. FreeBSD

To write the OPNsense image to a USB drive on FreeBSD system, run the following command.

```
dd if=OPNsense-##.#.##-[Type]-[Architecture].[img|iso] of=/dev/daX bs=16k
```

📝 **NOTE**

Where `X` = the device number of your USB flash drive (check `dmesg`)

For example,

```
dd if=OPNsense-21.7.1-OpenSSL-vga-amd64.img of=/dev/da1 bs=16k
```

2. Linux

To write the OPNsense image to a USB drive on a Linux system, run the following command.

```
dd if=OPNsense-##.#.##-[Type]-[Architecture].[img|iso] of=/dev/sdX bs=16k
```

📝 **NOTE**

Where X = the IDE device name of your USB flash drive (check with `hdparm -i /dev/sdX`)

(ignore the warning about trailing garbage, it's because of the digital signature)

For example,

```
dd if=OPNsense-21.7.1-OpenSSL-vga-amd64.img of=/dev/da1 bs=16k
```

3. OpenBSD

To write the OPNsense image to a USB drive on an OpenBSD system, run the following command.

```
dd if=OPNsense-##.#.##-[Type]-[Architecture].[img|iso] of=/dev/rsd6c bs=16k
```

📝**NOTE**

The device must be the ENTIRE device (in Windows/DOS language: the 'C' partition), and a raw I/O device (the 'r' in front of the device "sd6"), not a block mode device.

For example,

```
dd if=OPNsense-21.7.1-OpenSSL-vga-amd64.img of=/dev/rsd6c bs=16k
```

4. Mac OS X

To write the OPNsense image to a USB drive on a Mac OS X system, run the following command.

```
sudo dd if=OPNsense-##.#.##-[Type]-[Architecture].[img|iso] of=/dev/rdiskX bs=64k
```

📝**NOTE**

Where `r` = raw device, and where `X` = the disk device number of your CF card (check Disk Utility) (ignore the warning about trailing garbage, it's because of the digital signature)

For example,

```
sudo dd if=OPNsense-21.7.1-OpenSSL-vga-amd64.img of=/dev/rdiskX bs=64k
```

5. Windows

To write the OPNsense image to a USB drive on a Windows system, run the following command.

```
physdiskwrite -u OPNsense-##.#.##-[Type]-[Architecture].[img|iso].img
```

For example,

```
physdiskwrite -u OPNsense-21.7.1-OpenSSL-vga-amd64.img
```

📝**NOTE**

A simple alternative for writing images under Windows is Rufus a tool to create bootable USB sticks with a nice GUI.

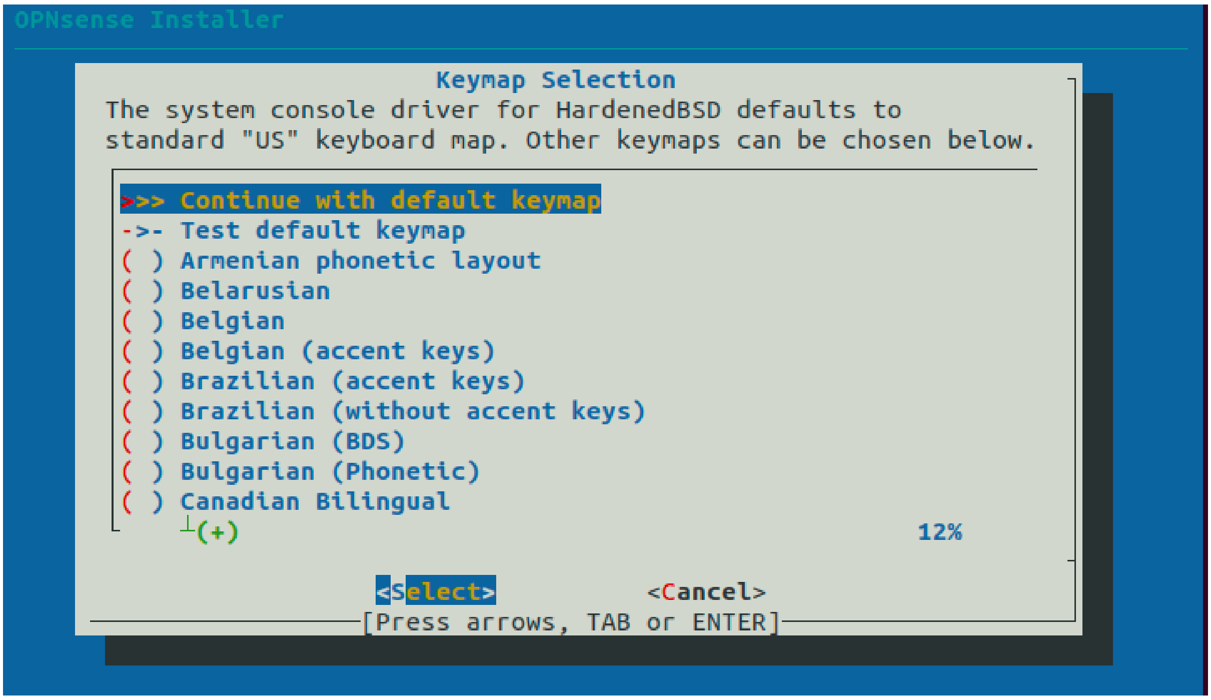
Step 4: Installing OPNSense from USB to Target Device

After configuring your system to boot from a USB device, place the USB stick into the one of USB slots and boot your system. The default behavior is to start the Live environment. Therefore, to start the installation login with user `installer` and password `opnsense.`

- Default OPNsense username: **installer**
- Default OPNsense installer password: **opnsense**

You can connect either on the local console or via SSH.

1. Keymap selection: Select the keymap as you wish. The default configuration is a US keyboard map. You may continue with default settings.

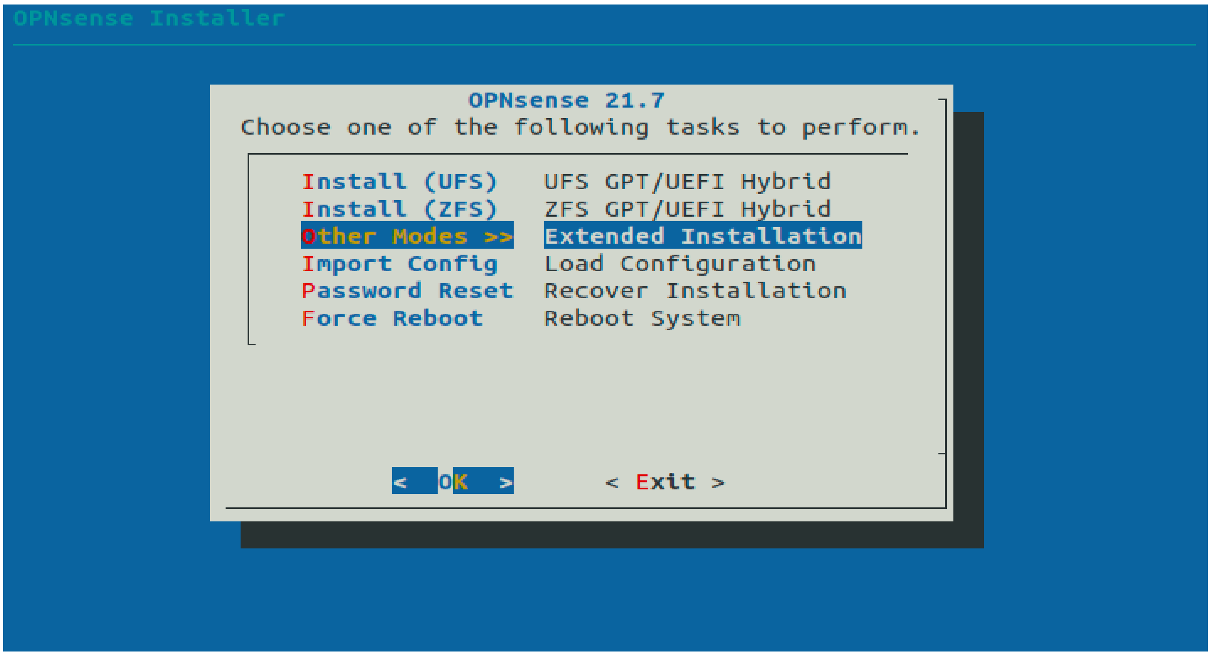


```
OPNsense Installer

                          Keymap Selection
   The system console driver for HardenedBSD defaults to
   standard "US" keyboard map. Other keymaps can be chosen below.

    >>> Continue with default keymap
    ->- Test default keymap
    ( ) Armenian phonetic layout
    ( ) Belarusian
    ( ) Belgian
    ( ) Belgian (accent keys)
    ( ) Brazilian (accent keys)
    ( ) Brazilian (without accent keys)
    ( ) Bulgarian (BDS)
    ( ) Bulgarian (Phonetic)
    ( ) Canadian Bilingual
        (+)                                              12%

                     <Select>           <Cancel>
                     [Press arrows, TAB or ENTER]
```

Figure 2. *Keymap Selection*

2. Installation Selection. The native ZFS installation is officially supported by the installer with the release of OPNsense 21.7. You may select one of the following installation tasks.

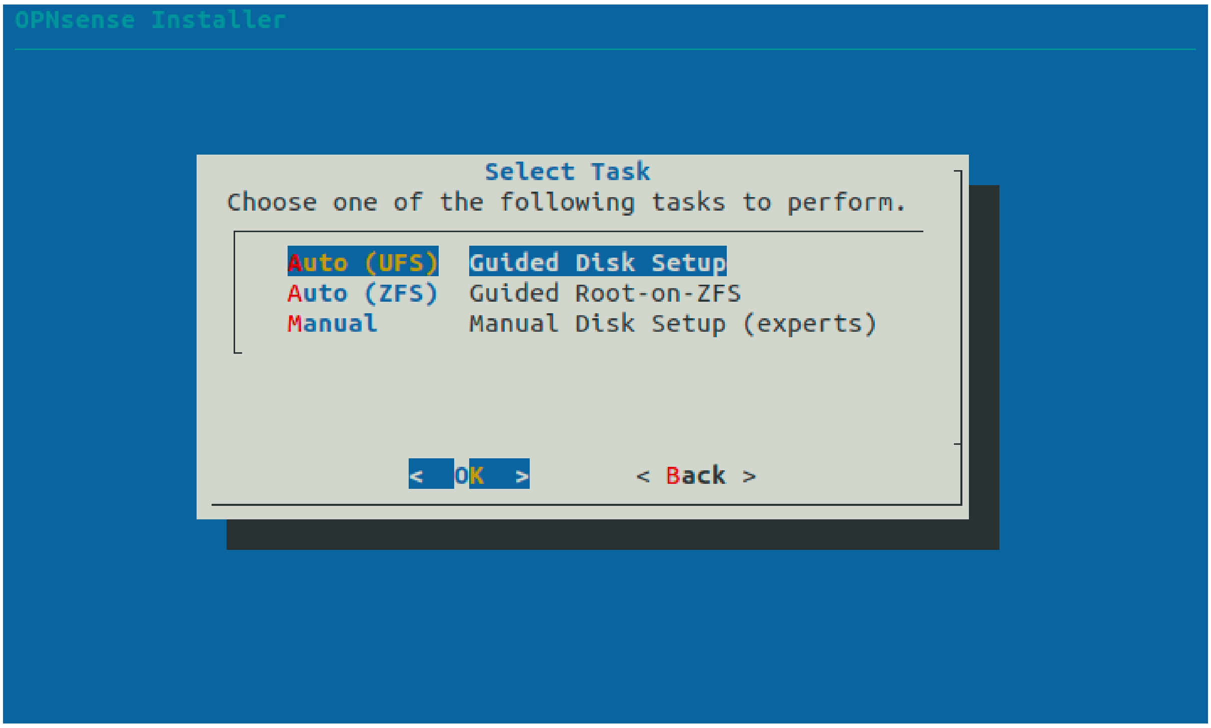
- UFS
- ZFS
- Other Modes (Extended Installation)



```
OPNsense Installer

                   OPNsense 21.7
   Choose one of the following tasks to perform.

       Install (UFS)     UFS GPT/UEFI Hybrid
       Install (ZFS)     ZFS GPT/UEFI Hybrid
       Other Modes >>    Extended Installation
       Import Config     Load Configuration
       Password Reset    Recover Installation
       Force Reboot      Reboot System

              <  OK  >         < Exit >
```

Figure 3 . *Installation Selection*

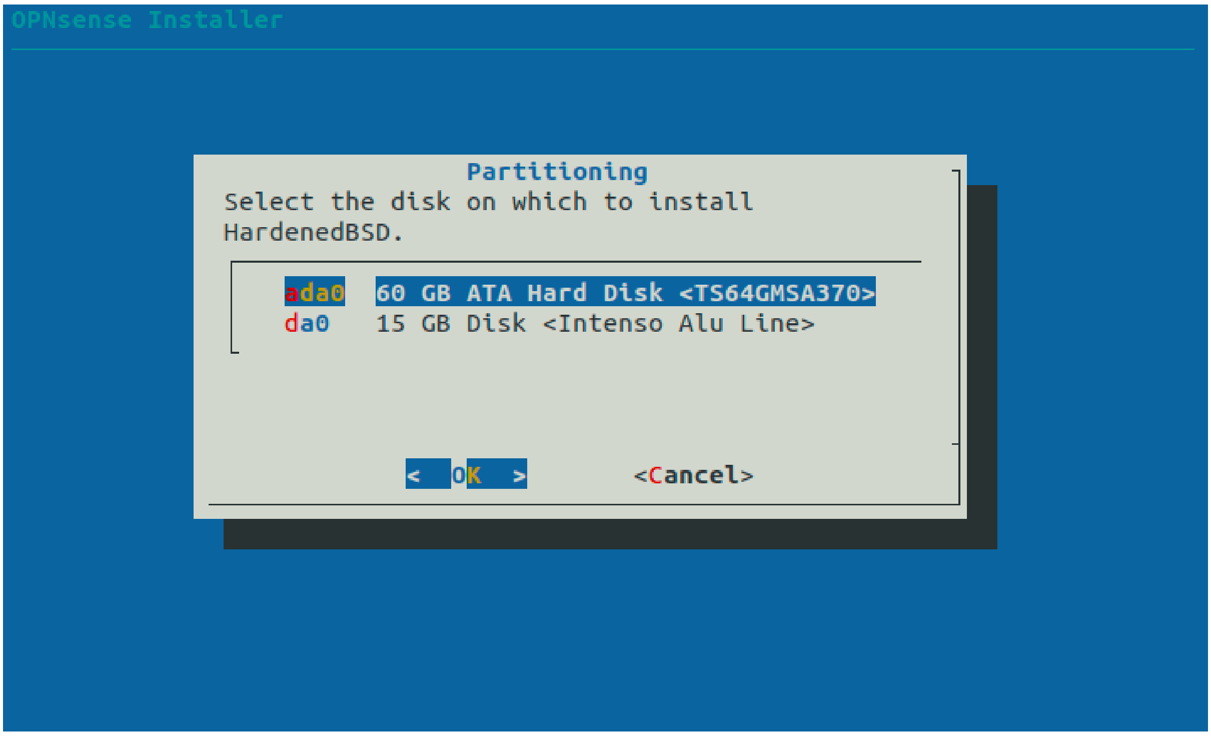
3. Task Selection: You may select one of the Guided Disk Setup, such as UFS and ZFS or Manual Disk Setup.



```
OPNsense Installer

                    Select Task
 Choose one of the following tasks to perform.

     Auto (UFS)   Guided Disk Setup
     Auto (ZFS)   Guided Root-on-ZFS
     Manual       Manual Disk Setup (experts)

           <  OK  >         < Back >
```

Figure 4 . *Selecting Disk Setup*

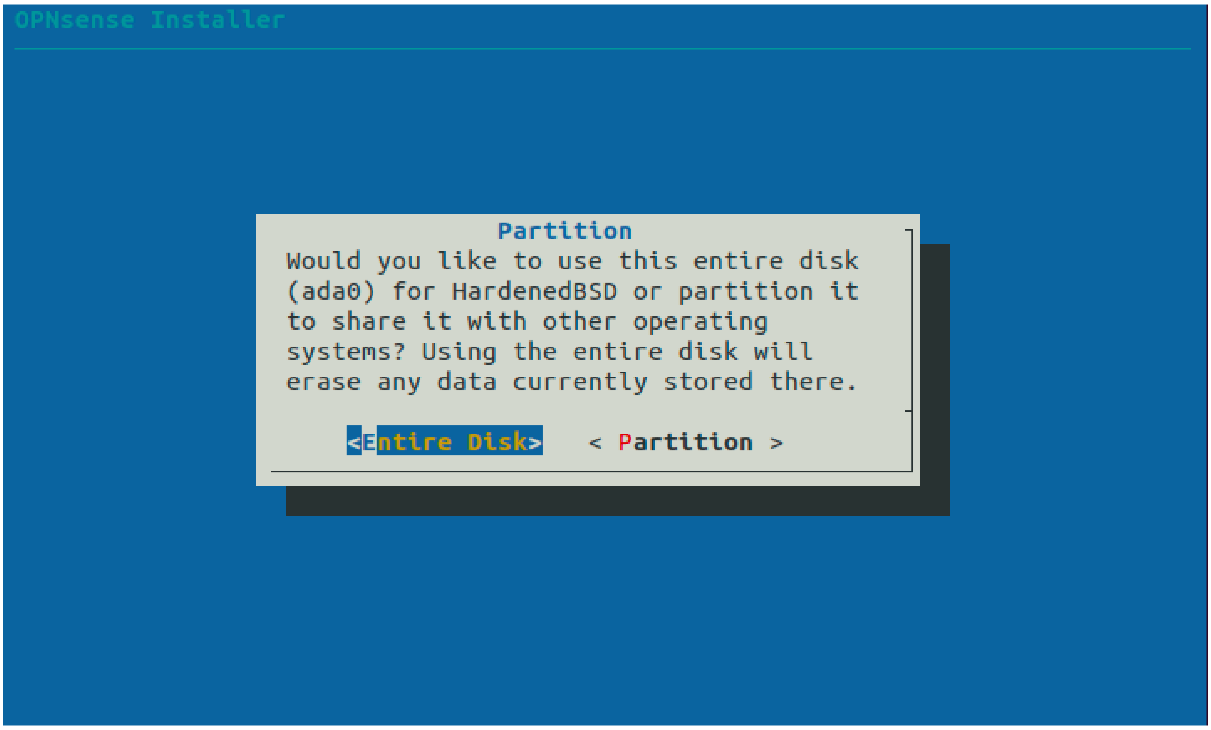
4. Select Disk: Select the disk on which you want to install the OPNsense.



```
OPNsense Installer

                 Partitioning
 Select the disk on which to install
 HardenedBSD.

     ada0   60 GB ATA Hard Disk <TS64GMSA370>
     da0    15 GB Disk <Intenso Alu Line>

           <  OK  >         <Cancel>
```

Figure 5. *Select the disk to install the OPNsense*

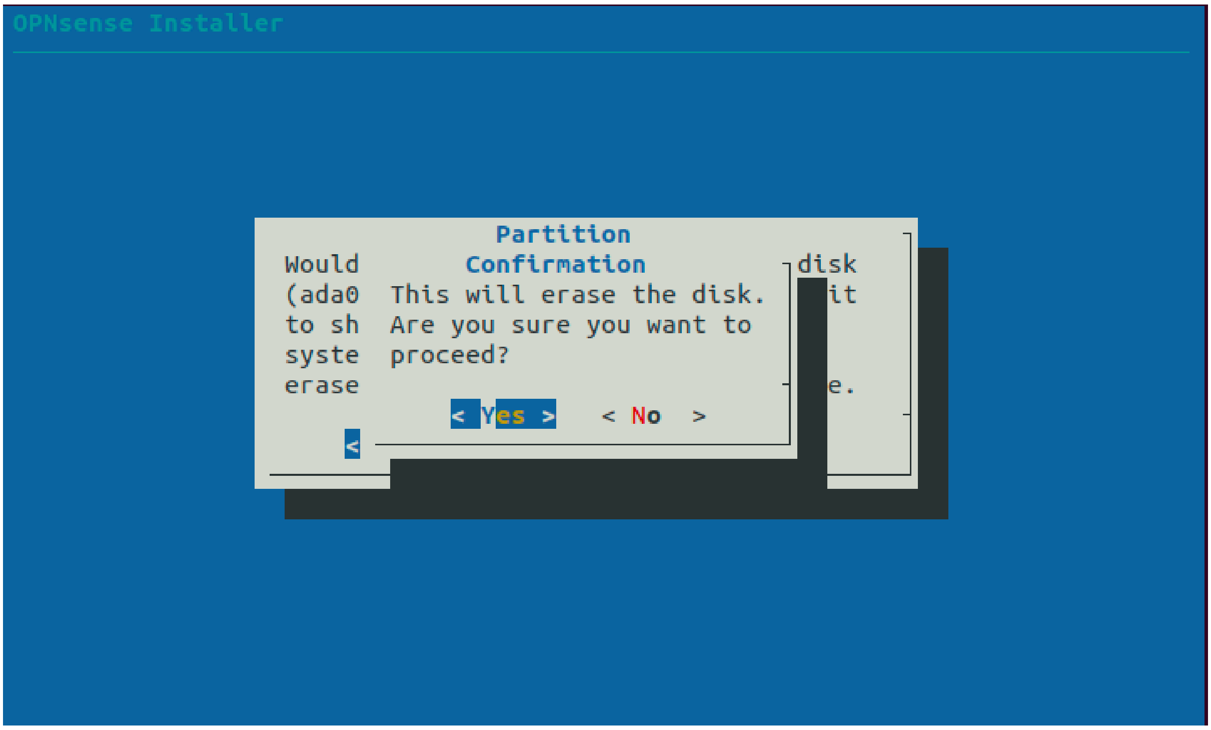
5. Select Entire Disk. You may select `Entire Disk` for partitioning



```
OPNsense Installer

                         Partition
          Would you like to use this entire disk
          (ada0) for HardenedBSD or partition it
          to share it with other operating
          systems? Using the entire disk will
          erase any data currently stored there.

              <Entire Disk>    < Partition >
```

Figure 6. *Selecting Entire Disk for partitioning*

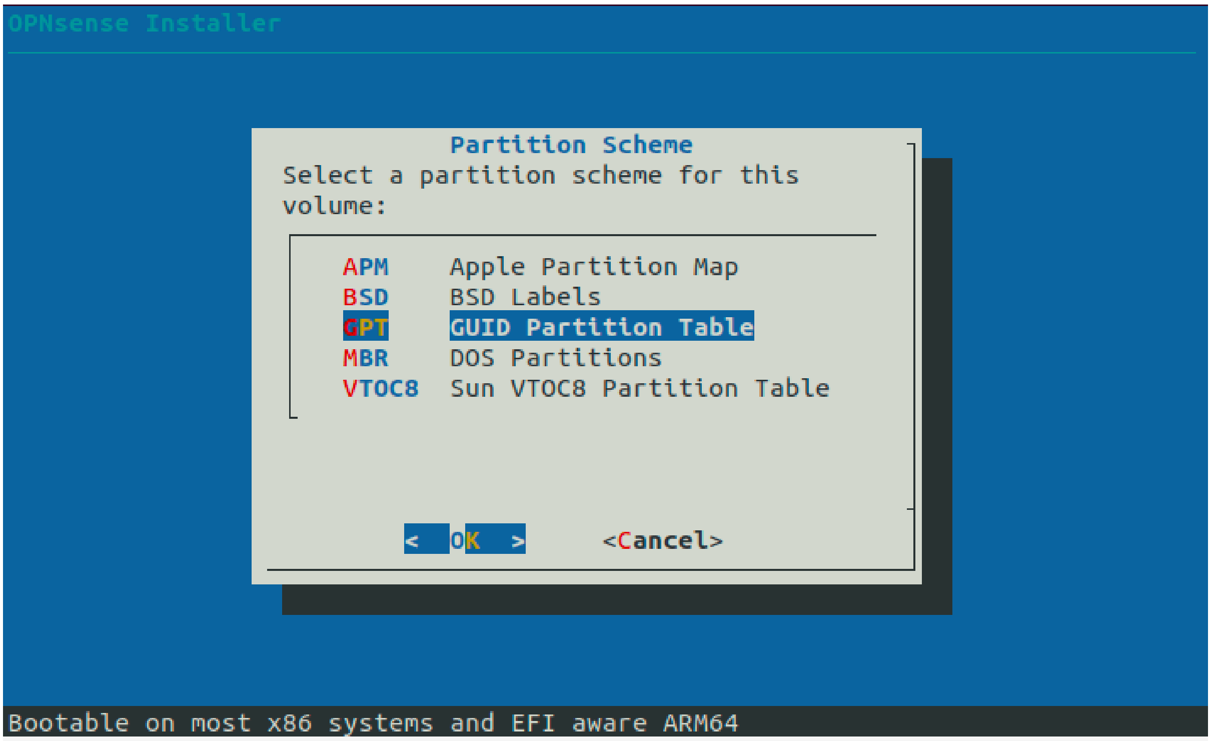
6. Partition Confirmation. Confirm the disk partitioning. Beware that this will erase all the data on the disk.



```
OPNsense Installer

                         Partition
          Would        Confirmation        disk
          (ada0  This will erase the disk.  it
          to sh  Are you sure you want to
          syste  proceed?
          erase                             e.
                    < Yes >   < No  >
               <
```

Figure 7. *Partition Confirmation*

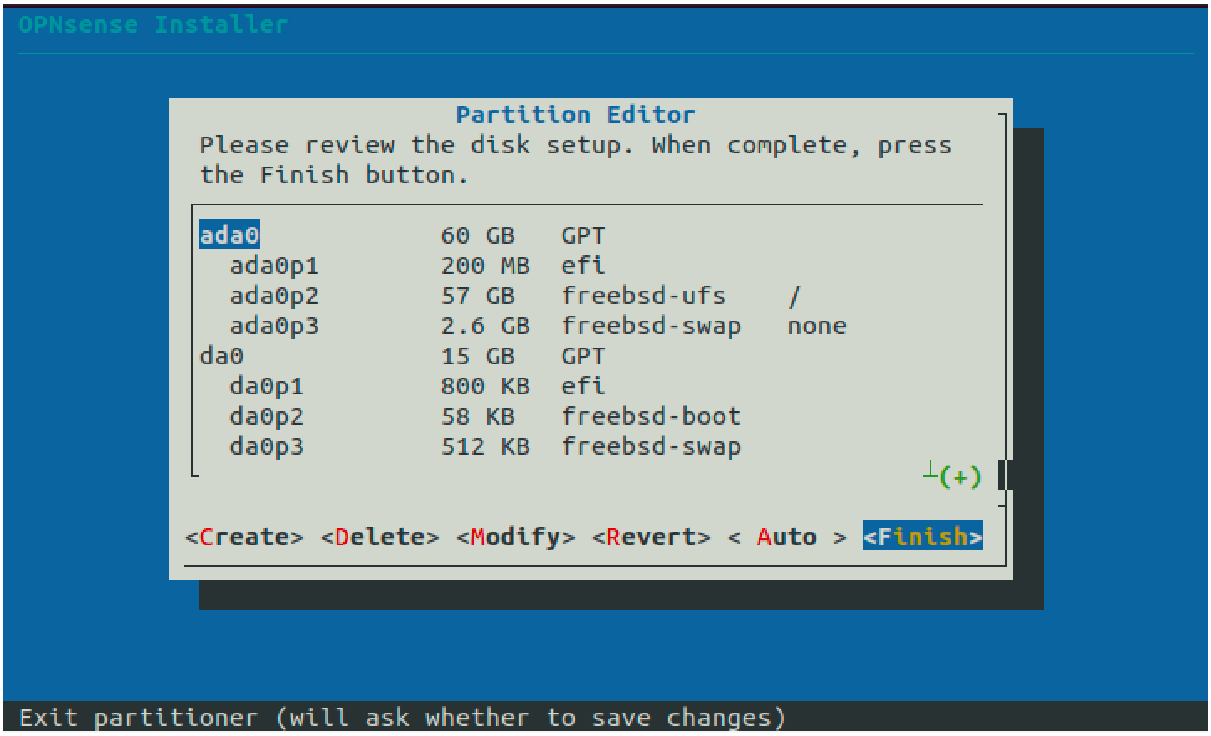
7. Selecting Partition Scheme. You may select `GPT.`



```
OPNsense Installer

                    Partition Scheme
  Select a partition scheme for this
  volume:

      APM     Apple Partition Map
      BSD     BSD Labels
      GPT     GUID Partition Table
      MBR     DOS Partitions
      VTOC8   Sun VTOC8 Partition Table

          <  OK  >        <Cancel>

Bootable on most x86 systems and EFI aware ARM64
```

Figure 8 . *Selecting Partition Scheme*

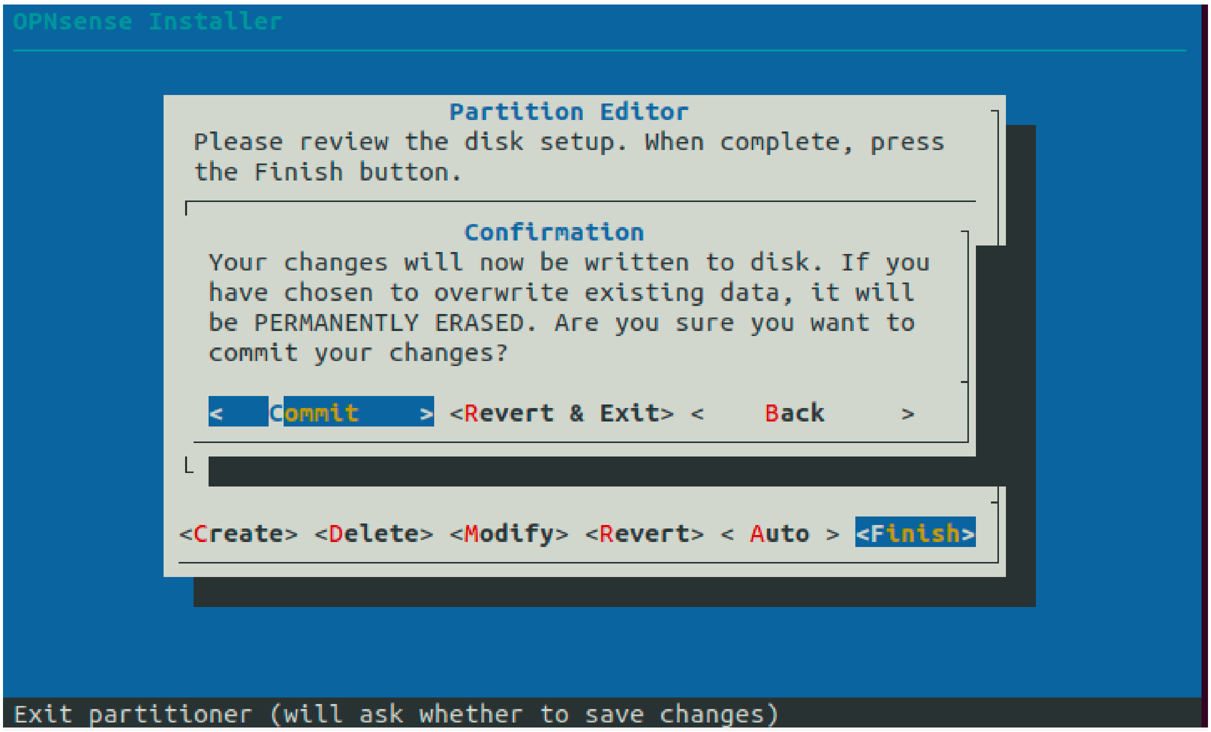
8. Review Partition Setup. After reviewing the disk partitioning setup, select `Finish`.



```
OPNsense Installer

                    Partition Editor
 Please review the disk setup. When complete, press
 the Finish button.

 ada0                60 GB    GPT
   ada0p1            200 MB   efi
   ada0p2            57 GB    freebsd-ufs    /
   ada0p3            2.6 GB   freebsd-swap   none
 da0                 15 GB    GPT
   da0p1             800 KB   efi
   da0p2             58 KB    freebsd-boot
   da0p3             512 KB   freebsd-swap
                                                  (+)

<Create> <Delete> <Modify> <Revert> < Auto > <Finish>

Exit partitioner (will ask whether to save changes)
```

Figure 9. *Review Partition Setup*

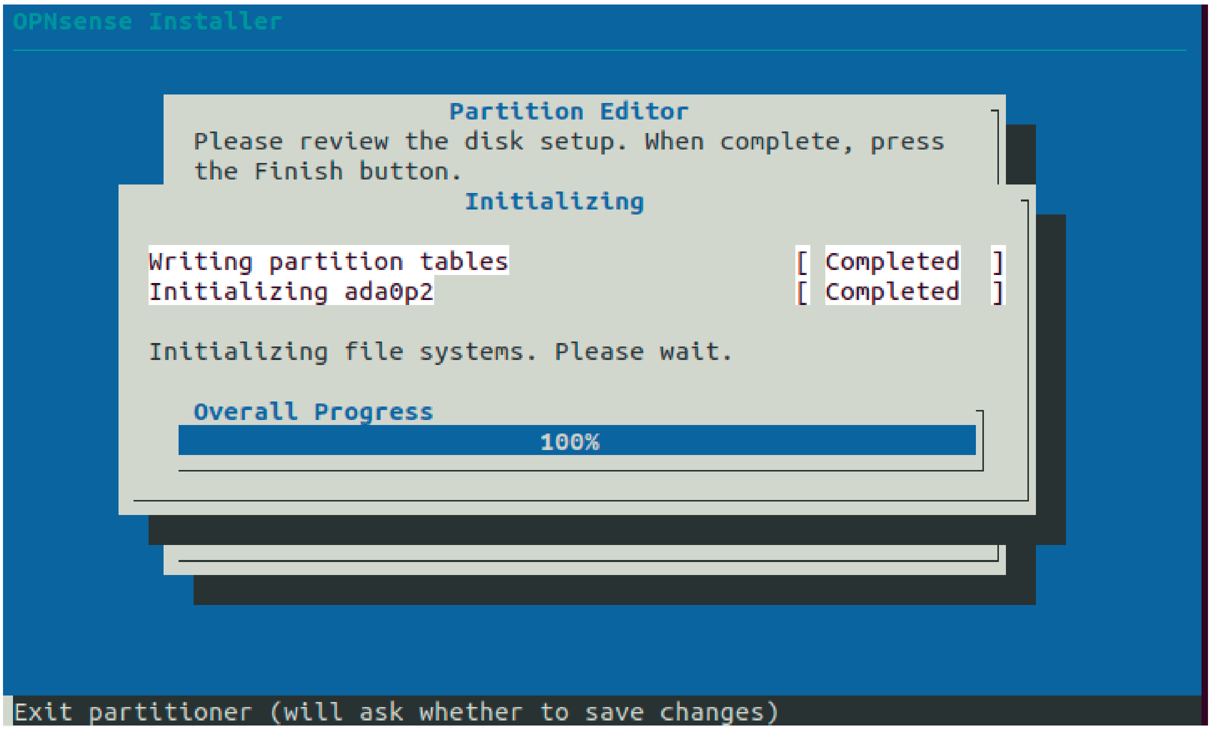
9. Confirm Partitioning. To confirm the disk partitioning, select `Commit`. Beware that this will permanently remove all files on the disk.



```
OPNsense Installer

                    Partition Editor
  Please review the disk setup. When complete, press
  the Finish button.

                     Confirmation
   Your changes will now be written to disk. If you
   have chosen to overwrite existing data, it will
   be PERMANENTLY ERASED. Are you sure you want to
   commit your changes?

   <  Commit  > <Revert & Exit> <    Back     >

<Create> <Delete> <Modify> <Revert> < Auto > <Finish>

Exit partitioner (will ask whether to save changes)
```

Figure 10. *Confirm Partitioning*

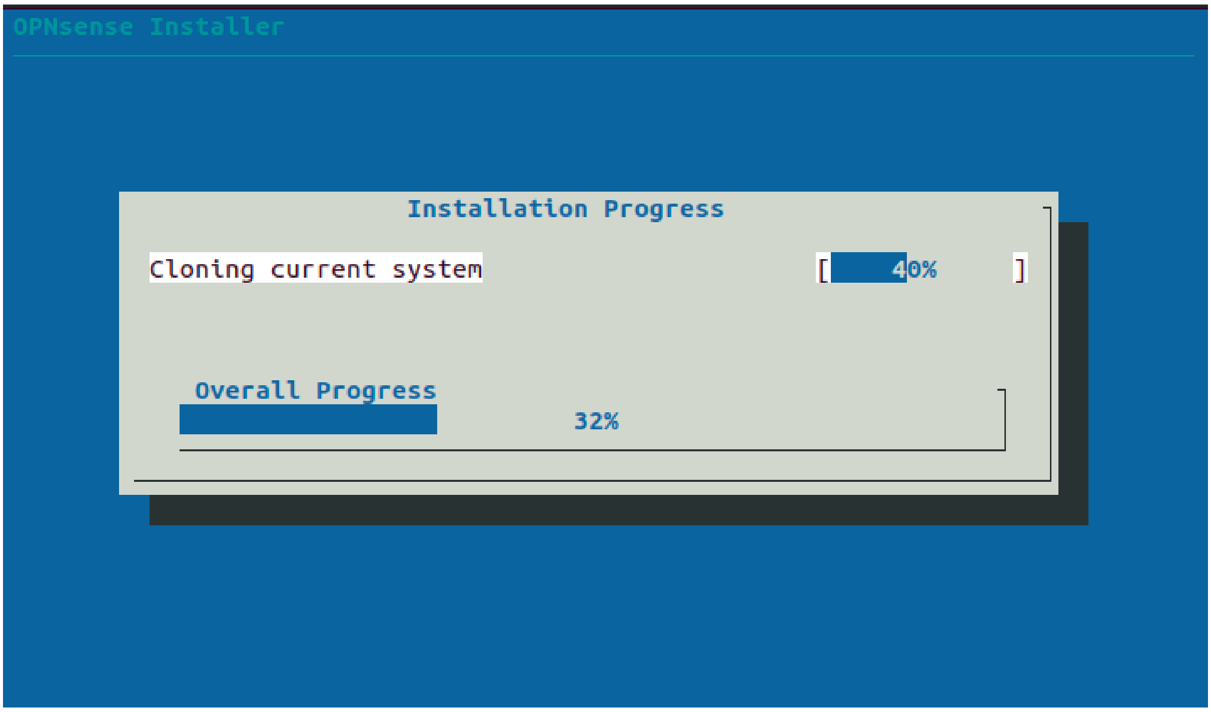
10. Initializing the disk. The initialization of the target disk will start.



```
OPNsense Installer

                    Partition Editor
  Please review the disk setup. When complete, press
  the Finish button.
                     Initializing

Writing partition tables                [ Completed  ]
Initializing ada0p2                     [ Completed  ]

Initializing file systems. Please wait.

   Overall Progress
                        100%

Exit partitioner (will ask whether to save changes)
```

Figure 11. *Initializing the disk.*

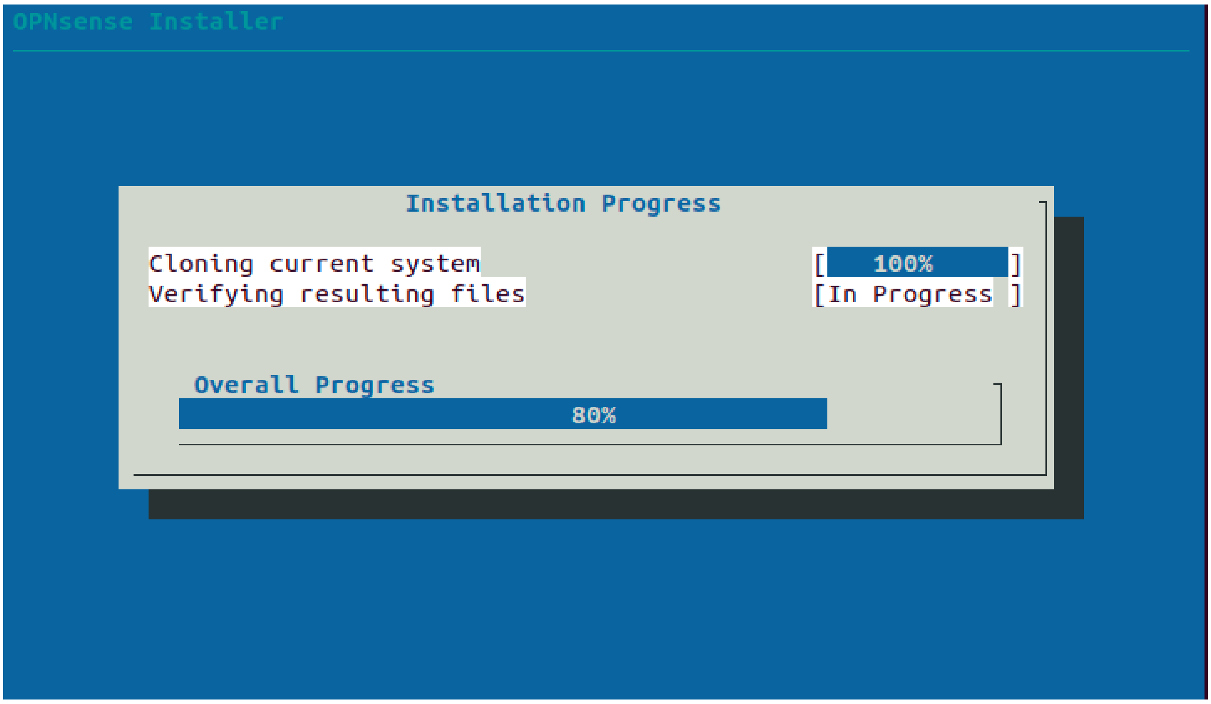
11. File Installation. OPNsense files installation will start.



```
OPNsense Installer

                    Installation Progress

  Cloning current system                     [   40%    ]


     Overall Progress
                          32%
```

Figure 12. *File Installation*

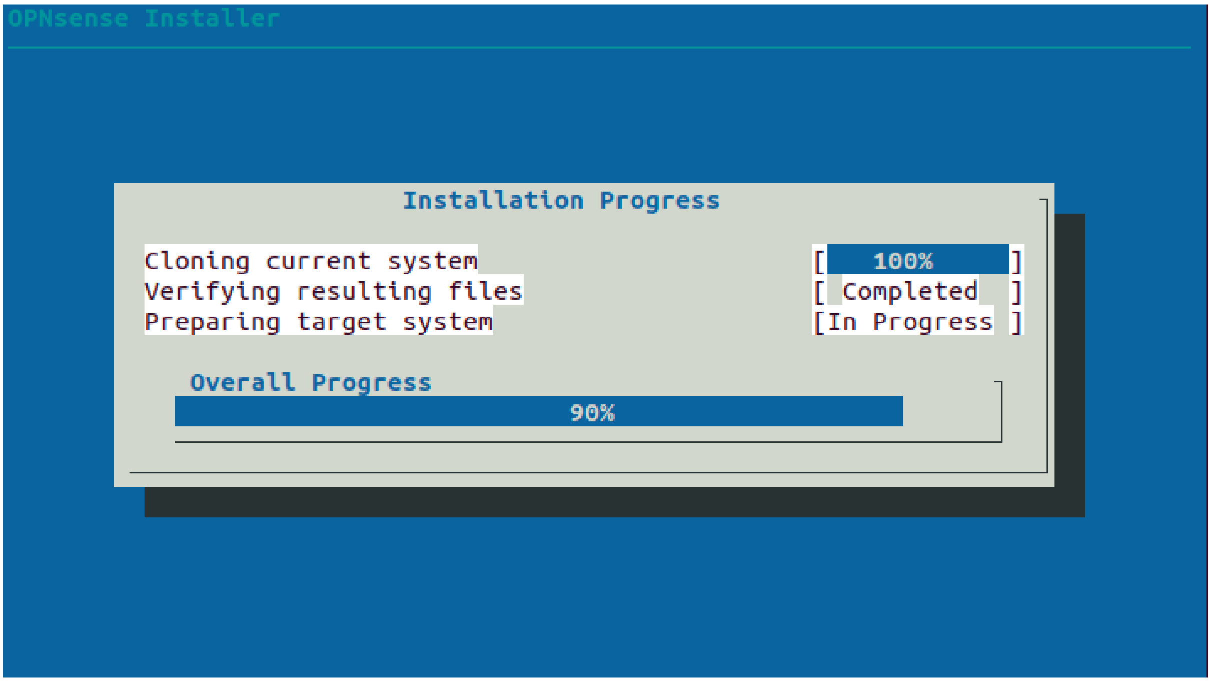
12. Verification of the installation. OPNsense installer verifies the installation.



```
OPNsense Installer

                    Installation Progress

  Cloning current system                     [   100%     ]
  Verifying resulting files                  [In Progress ]


     Overall Progress
                          80%
```

Figure 13. *Verification of the installation*

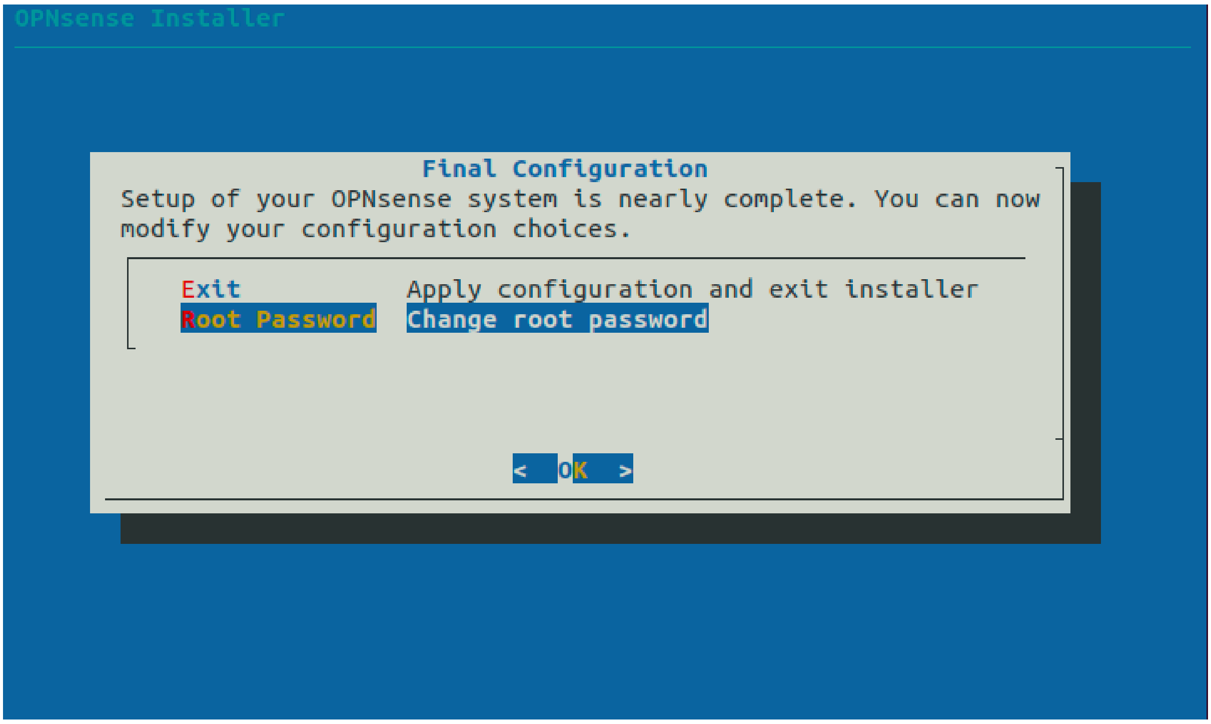
13. Preparing the target. OPNsense installer prepares the target system.



```
OPNsense Installer

                    Installation Progress

  Cloning current system                          [    100%    ]
  Verifying resulting files                       [ Completed   ]
  Preparing target system                         [In Progress ]

     Overall Progress
                          90%
```

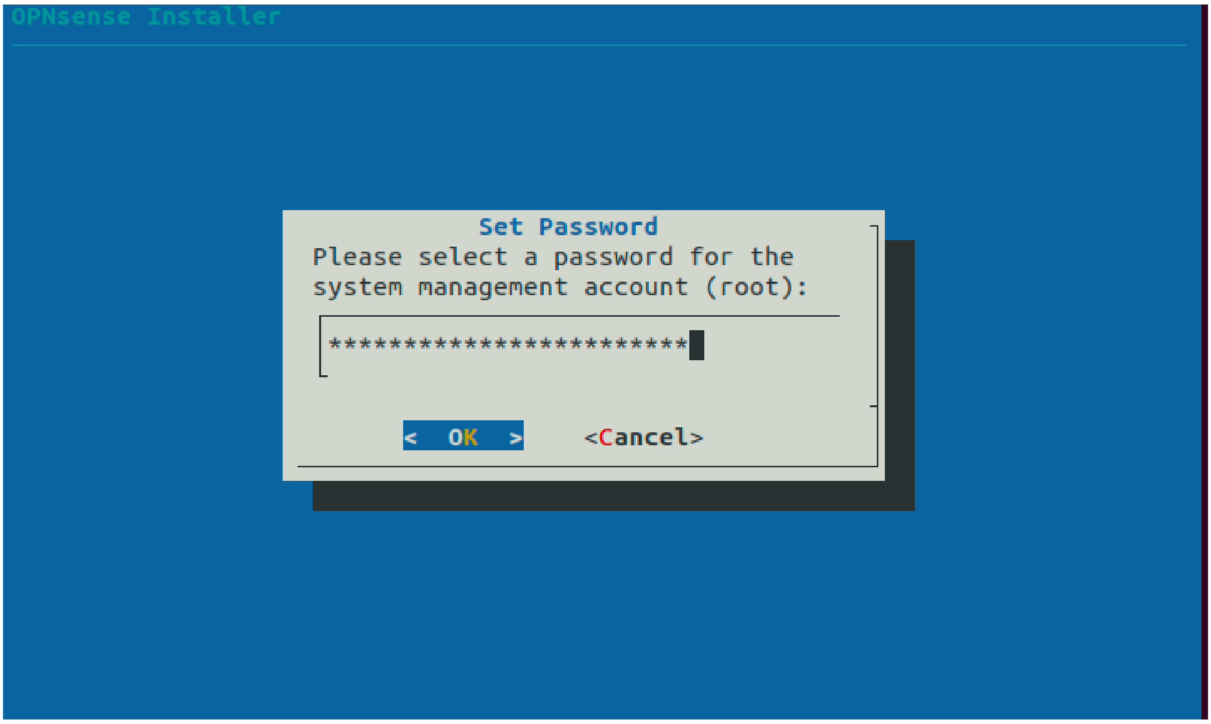
Figure 14. *Preparing the target*

14. Changing root password. Default OPNsense root password is `root`. It is recommended that you change it with a strong one.



```
OPNsense Installer

                     Final Configuration
 Setup of your OPNsense system is nearly complete. You can now
 modify your configuration choices.

     Exit           Apply configuration and exit installer
     Root Password  Change root password

                           <  OK  >
```

Figure 15. *Changing root password*



OPNsense Installer

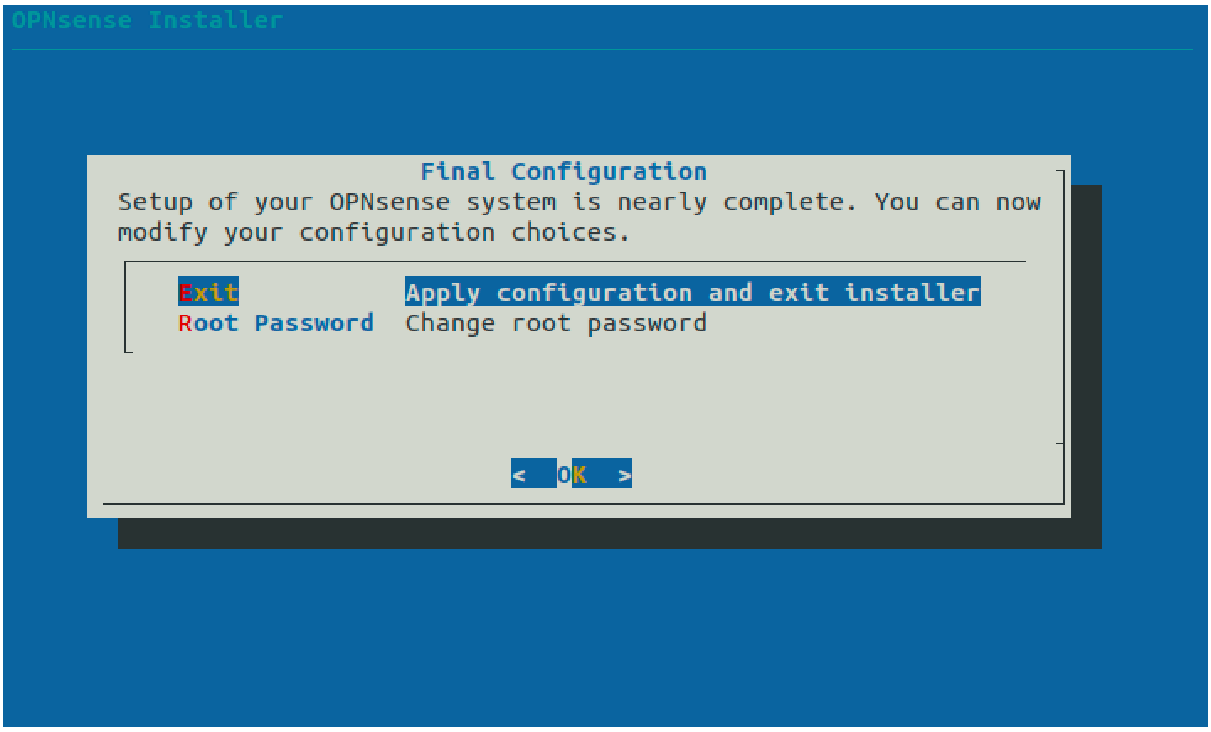
Set Password

Please select a password for the system management account (root):

```
************************
```

Figure 16. *Setting root password*

15. Final Configuration. To apply the configuration and exit installer, select `Exit` and then `OK`.



OPNsense Installer

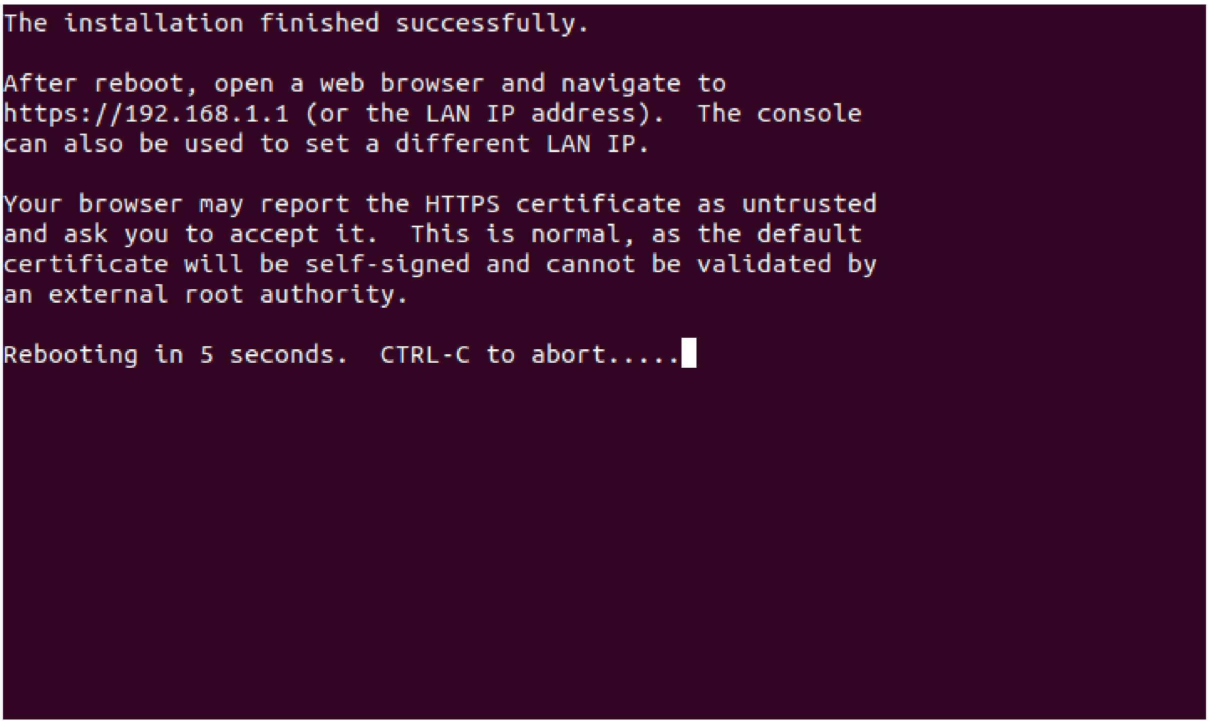
Final Configuration

Setup of your OPNsense system is nearly complete. You can now modify your configuration choices.

```
Exit             Apply configuration and exit installer
Root Password    Change root password
```

Figure 17. *Final Configuration*

16. Reboot. Installation of OPNsense from USB flash drive is finished successfully. The firewall needs to reboot. You should proceed to the initial configuration of your OPNsense firewall.



```
The installation finished successfully.

After reboot, open a web browser and navigate to
https://192.168.1.1 (or the LAN IP address).  The console
can also be used to set a different LAN IP.

Your browser may report the HTTPS certificate as untrusted
and ask you to accept it.  This is normal, as the default
certificate will be self-signed and cannot be validated by
an external root authority.

Rebooting in 5 seconds.  CTRL-C to abort.....
```

Figure 18. *Reboot*

📝**NOTE**
You may learn how to install OPNsense on Proxmox Virtual Environment by reading the OPNsense Installation Tutorial written by Zenarmor (formerly known as Sunny Valley Networks). Since OPNsense installation on different platforms has almost the same procedures, this article may be helpful for USB installation also.

Step 5: Completing OPNSense Initial Configuration

After installing the OPNsense the following initial configuration steps should be completed.

1. Network device assignments
2. IP address settings
3. Updating OPNsense Firewall
4. Accessing the OPNsense GUI
5. Initial configuration of OPNsense Firewall

You may find more information about the initial configuration steps on OPNsense Installation Tutorial written by Zenarmor.

How to Update OPNsense

OPNsense update is critical for cyber security. The sooner you update, the sooner you'll be able to rest assured that your network is more secure. Keeping your systems up-to-date by regular updates has the following benefits:

- Updates may provide new or improved features, as well as improved compatibility with various devices or applications. They may also improve the stability of the system and remove outdated features.
- They frequently include critical security patches. So that, you may keep hackers out and protect your network infrastructure against cyber attacks.
- They generally fix or remove software bugs.

The update schedule for OPNsense consists of two major releases per year, which are updated every two weeks. In addition to scheduled major updates, OPNsense is updated weekly to act quickly on known security threats. The version number of major releases consists of the year and month of release (e.g., `21.7` for the July 2021 release), with fortnightly updates adding a third number (e.g.`21.7.2` for the second update to 21.7).

Version	Release Date
23.7.5	September 26, 2023
23.7.4	September 14, 2023
23.7.3	August 30, 2023
23.7.2	August 23, 2023
23.7.1	August 08, 2023
23.7	July 31, 2023
23.7.r3	July 26, 2023
23.7.r2	July 24, 2023
23.7.r1	July 20, 2023

23.1.11	June 28, 2023
23.1.10	June 22, 2023
23.1.9	May 31, 2023
23.1.8	May 25, 2023
23.1.7	May 04, 2023
23.1.6	April 20, 2023
23.1.5	March 29, 2023
23.1.4	March 21, 2023
23.1.3	March 09, 2023
23.1.2	March 07, 2023
23.1.1	February 15, 2023
23.1	January 26, 2023
23.1.r2	January 19, 2023
23.1.r1	January 13, 2023

Table 1. *OPNsense 23.x Community Edition relase dates*

You may follow the announcements on the OPNsense forum (https://forum.opnsense.org/index.php?board=11.0) for all OPNsense releases. Also, major releases are announced on the OPNsense blog posts (https://opnsense.org/blog/). Full patch notes, fix notes, known issues, and limitations are shared on these announcements. Some updates may require a system reboot. Also, there may be issues or limitations that cause service interruptions on your system. Therefore, It is strongly recommended to read the release notes before upgrading the OPNsense system.

When there is an OPNsense release update available, you may see the update reminder on the OPNsense web UI dashboard. OPNsense manual update is a straightforward process that can be accomplished via both OPNsense web UI or console/CLI easily. In this OPNsense update guide, we will cover both methods briefly.

☢ **DANGER**

OPNsense automatic updates, especially for major releases are not recommended.

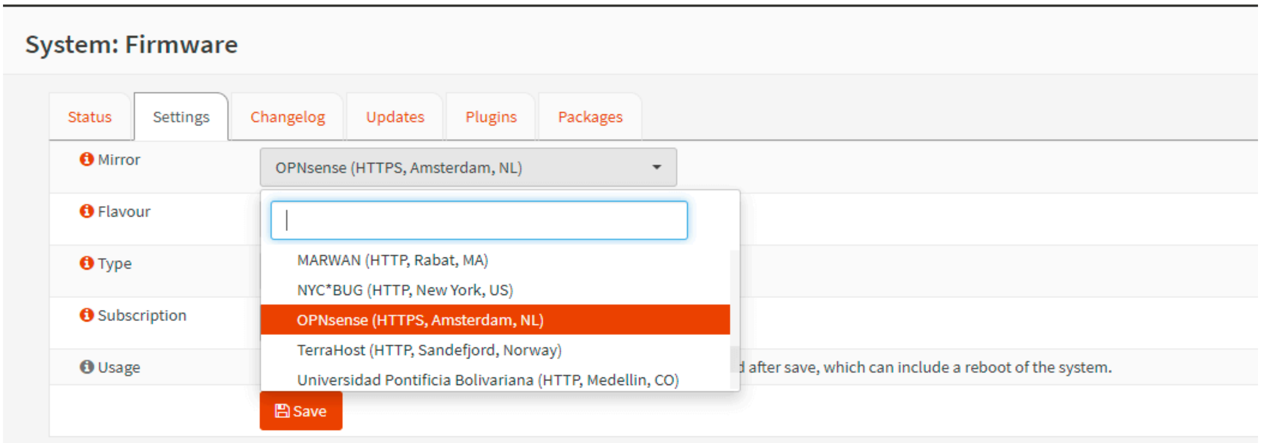
How to Update OPNsense Settings

You may change the OPNsense update settings according to your requirements by following the next steps:

1. Navigate to the **System -> Firmware -> Settings.**
2. Set the next options listed below as you need and then click **Save**` to apply the changes.
   - Firmware Mirror
   - Firmware Flavour
   - Release Type
   - Subscription

1. Firmware Mirror

You can specify the mirror site from which OPNsense attempts to obtain updates. If you're having trouble updating or searching for updates, or if your current mirror is running slowly, you can switch to another one here.



System: Firmware

Mirror: OPNsense (HTTPS, Amsterdam, NL)

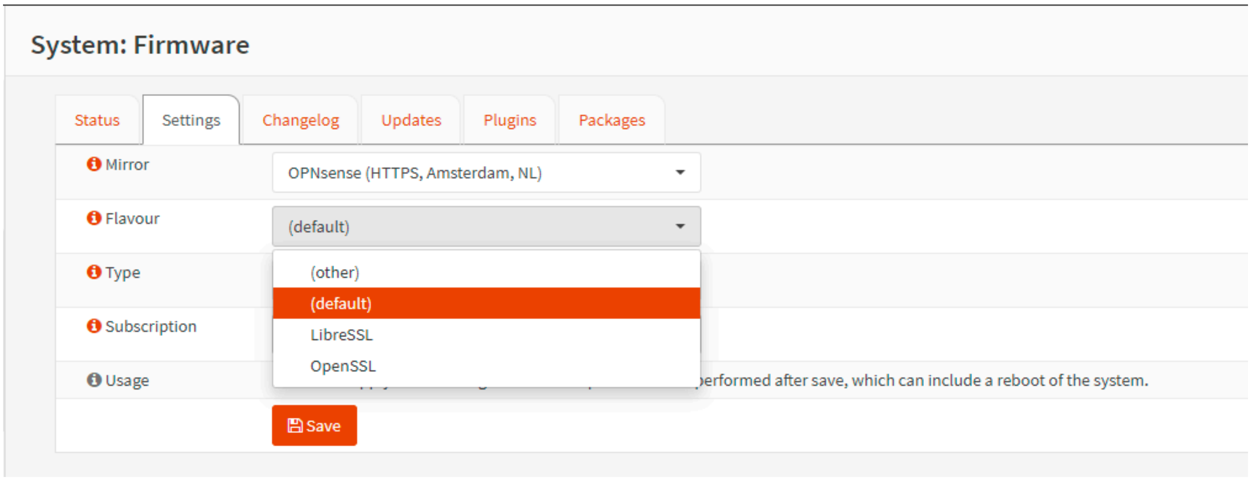
…d after save, which can include a reboot of the system.

Status
Settings
Changelog
Updates
Plugins
Packages
Mirror
Flavour
Type
Subscription
Usage
MARWAN (HTTP, Rabat, MA)
NYC*BUG (HTTP, New York, US)
OPNsense (HTTPS, Amsterdam, NL)
TerraHost (HTTP, Sandefjord, Norway)
Universidad Pontificia Bolivariana (HTTP, Medellin, CO)
Save

Figure 1. *Selecting OPNsense Mirror*

2. Firmware Flavour

OPNsense comes in a variety of firmware cryptography flavours. Currently, these flavours determine whether to use OpenSSL or LibreSSL. The default setting is OpenSSL.



System: Firmware

Mirror: OPNsense (HTTPS, Amsterdam, NL)

Flavour: (default)

Type

Subscription

Usage: erformed after save, which can include a reboot of the system.

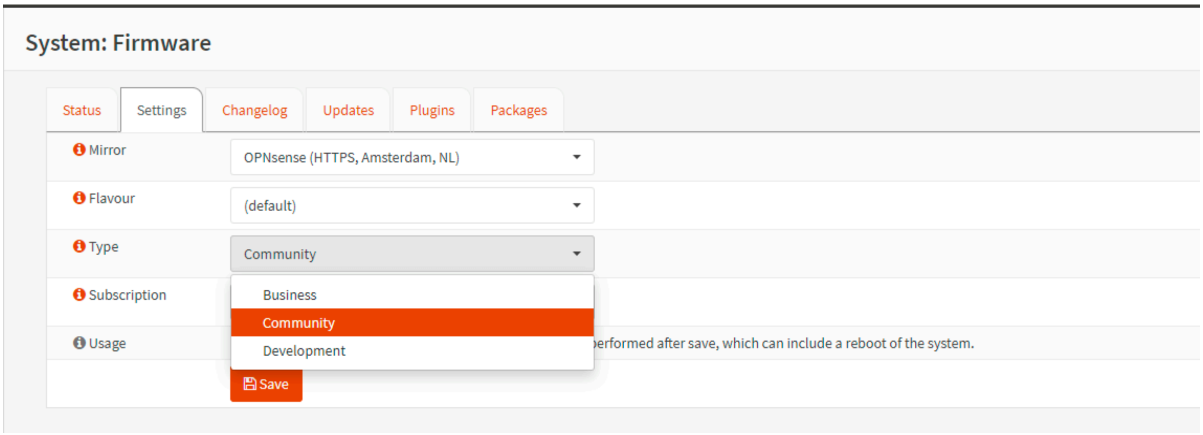
Figure 2. *Selecting OPNsense Flavour.*

3. Release Type

There are three options available for the release type of the OPNsense:

1. **Business**: OPNsense Business Edition is destined for businesses, enterprises, and professionals seeking a more selective upgrade path, additional commercial features, and a more commercial way to support the project than donating.
2. **Community**: This release is tested on a fortnightly basis and is suitable for production environments.
3. **Development**: This release is the most recent release but untested.

> ☢ **DANGER**
>
> Please keep this setting set to `Community` unless you fully understand the implications of changing it.



System: Firmware

Mirror: OPNsense (HTTPS, Amsterdam, NL)

Flavour: (default)

Type: Community

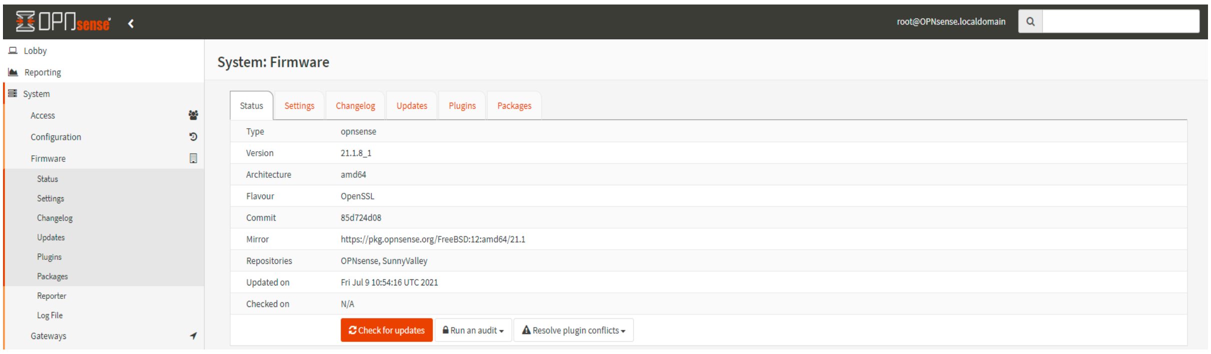
Subscription

Usage: erformed after save, which can include a reboot of the system.

Figure 3. *Selecting OPNsense Release Type*

4. Subscription

If you have a Business license, you should provide your subscription key in this field.



System: Firmware

Type	opnsense
Version	21.1.8_1
Architecture	amd64
Flavour	OpenSSL
Commit	85d724d08
Mirror	https://pkg.opnsense.org/FreeBSD:12:amd64/21.1
Repositories	OPNsense, SunnyValley
Updated on	Fri Jul 9 10:54:16 UTC 2021
Checked on	N/A

Figure 4. *Firmware Status*

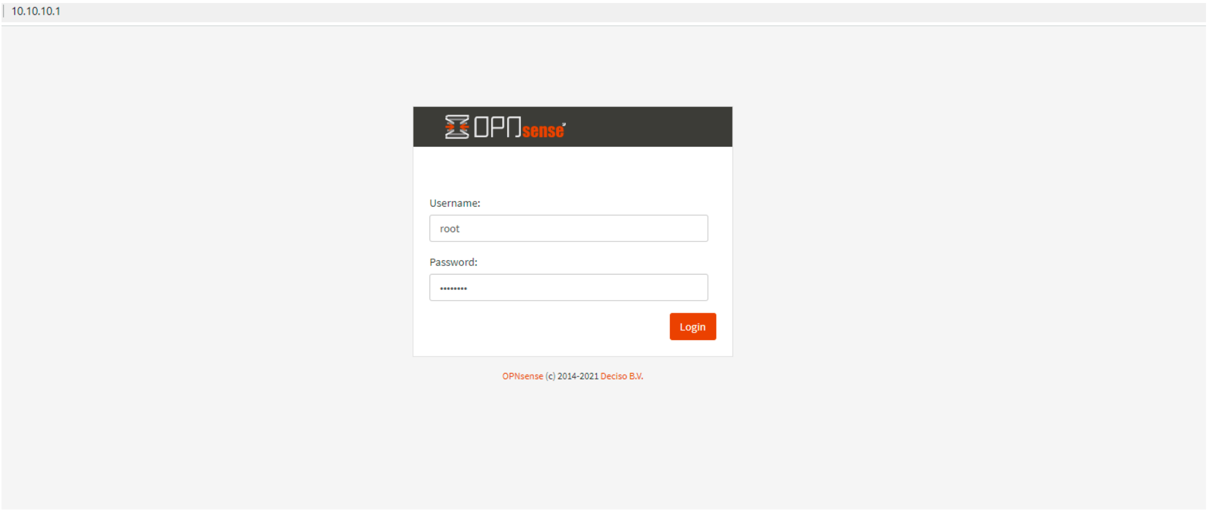
How to Update OPNsense

You may update the OPNsense firewall via either OPNsense web GUI or OPNsense console/command line(CLI). However, major release upgrades should be performed via console which is also known as an offline upgrade. You may find more information about the offline upgrade of the OPNsense below.

Updating OPNsense on Web GUI

To update the OPNsense node on the web GUI, follow the steps given below.

1. Login OPNsense web GUI as `root`.



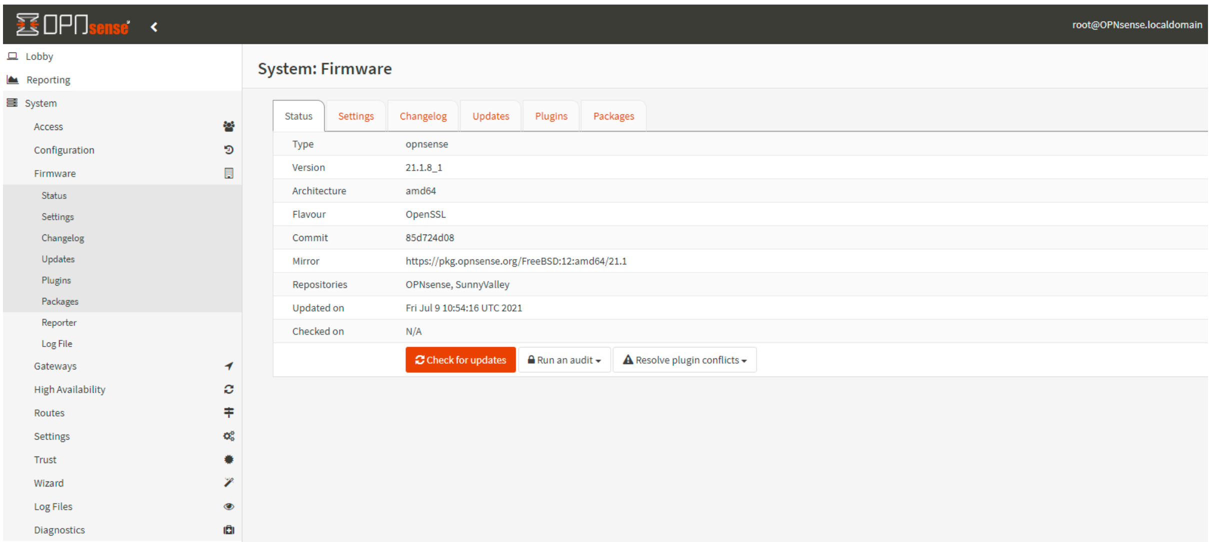
Username: root

Password: ••••••••

Figure 5. *OPNsense web login*

2. Navigate to the **System -> Firmware -> Updates -> Status.**

3. Click **Check for updates** button under the **Status** tab.



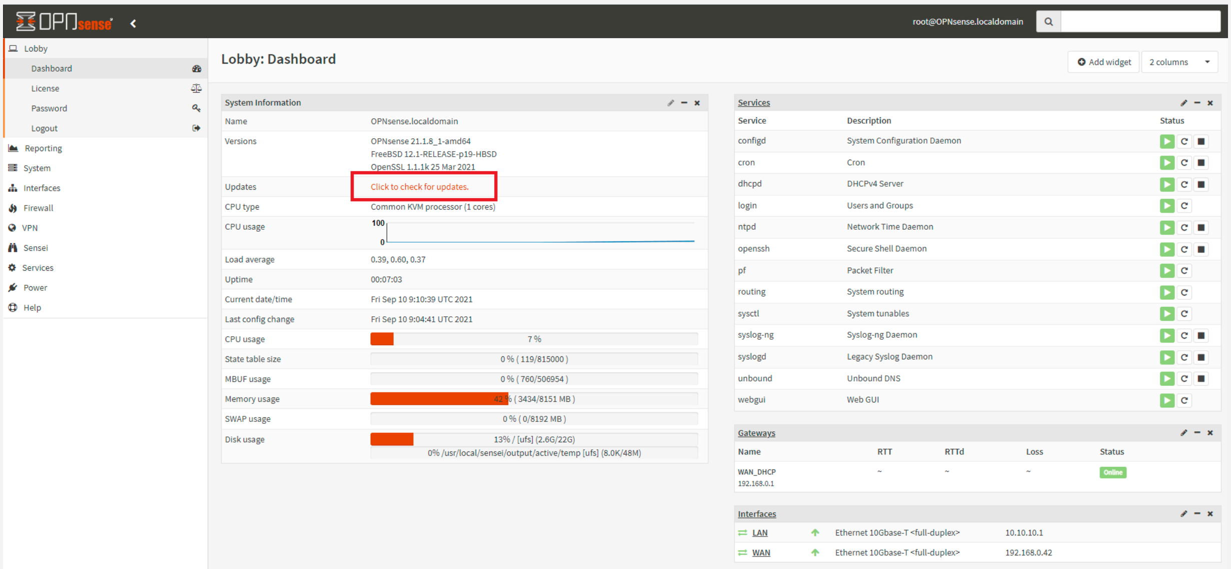
System: Firmware

Type	opnsense
Version	21.1.8_1
Architecture	amd64
Flavour	OpenSSL
Commit	85d724d08
Mirror	https://pkg.opnsense.org/FreeBSD:12:amd64/21.1
Repositories	OPNsense, SunnyValley
Updated on	Fri Jul 9 10:54:16 UTC 2021
Checked on	N/A

Figure 6. *Checking for OPNsense updates on Web GUI*

📝NOTE

You may click on the **Click to check for updates** link in the **System Information** pane on the Dashboard and then click on the **Update** button.



Lobby: Dashboard

System Information

Name	OPNsense.localdomain
Versions	OPNsense 21.1.8_1-amd64 FreeBSD 12.1-RELEASE-p19-HBSD OpenSSL 1.1.1k 25 Mar 2021
Updates	Click to check for updates.
CPU type	Common KVM processor (1 cores)
CPU usage	
Load average	0.39, 0.60, 0.37
Uptime	00:07:03
Current date/time	Fri Sep 10 9:10:39 UTC 2021
Last config change	Fri Sep 10 9:04:41 UTC 2021
CPU usage	7 %
State table size	0 % (119/815000)
MBUF usage	0 % (760/506954)
Memory usage	42 % (3434/8151 MB)
SWAP usage	0 % (0/8192 MB)
Disk usage	13% / [ufs] (2.6G/22G) 0% /usr/local/sensei/output/active/temp [ufs] (8.0K/48M)

Services

Service	Description	Status
configd	System Configuration Daemon	
cron	Cron	
dhcpd	DHCPv4 Server	
login	Users and Groups	
ntpd	Network Time Daemon	
openssh	Secure Shell Daemon	
pf	Packet Filter	
routing	System routing	
sysctl	System tunables	
syslog-ng	Syslog-ng Daemon	
syslogd	Legacy Syslog Daemon	
unbound	Unbound DNS	
webgui	Web GUI	

Gateways

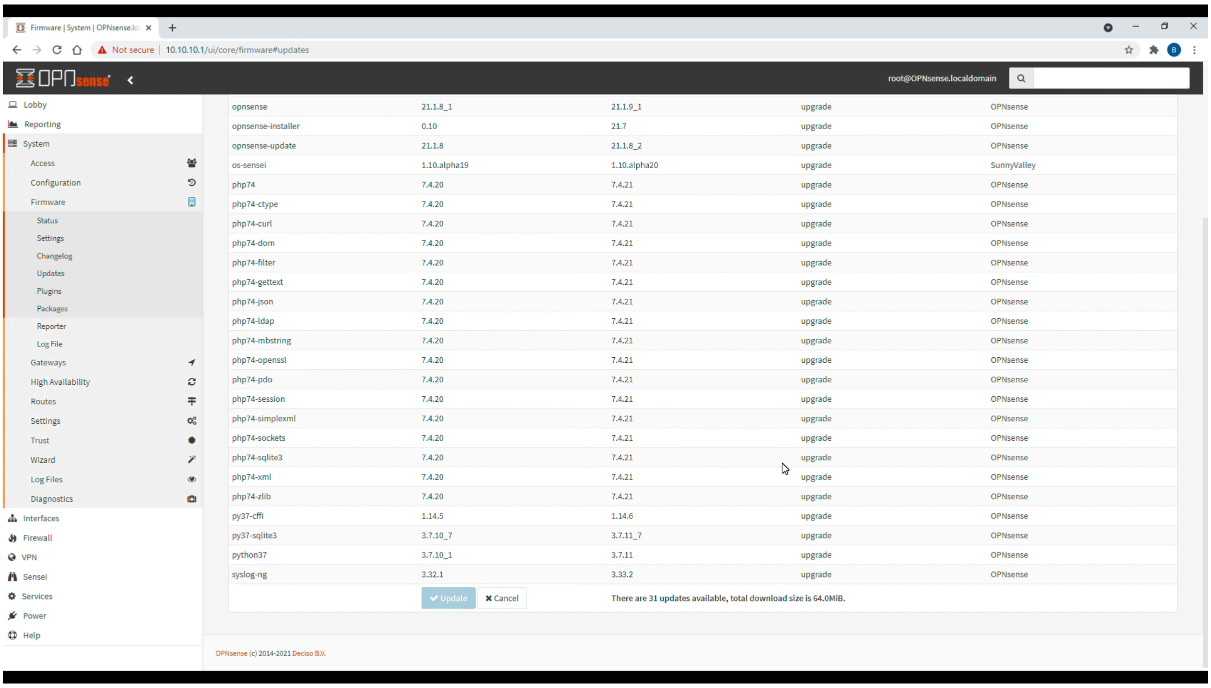
Name	RTT	RTTd	Loss	Status
WAN_DHCP 192.168.0.1	~	~	~	Online

Interfaces

LAN	Ethernet 10Gbase-T <full-duplex>	10.10.10.1
WAN	Ethernet 10Gbase-T <full-duplex>	192.168.0.42

Figure 7. *Checking for updates on OPNsense Dashboard*

4. When there is an update available, the **Update** button is displayed at the bottom of the update packages list.



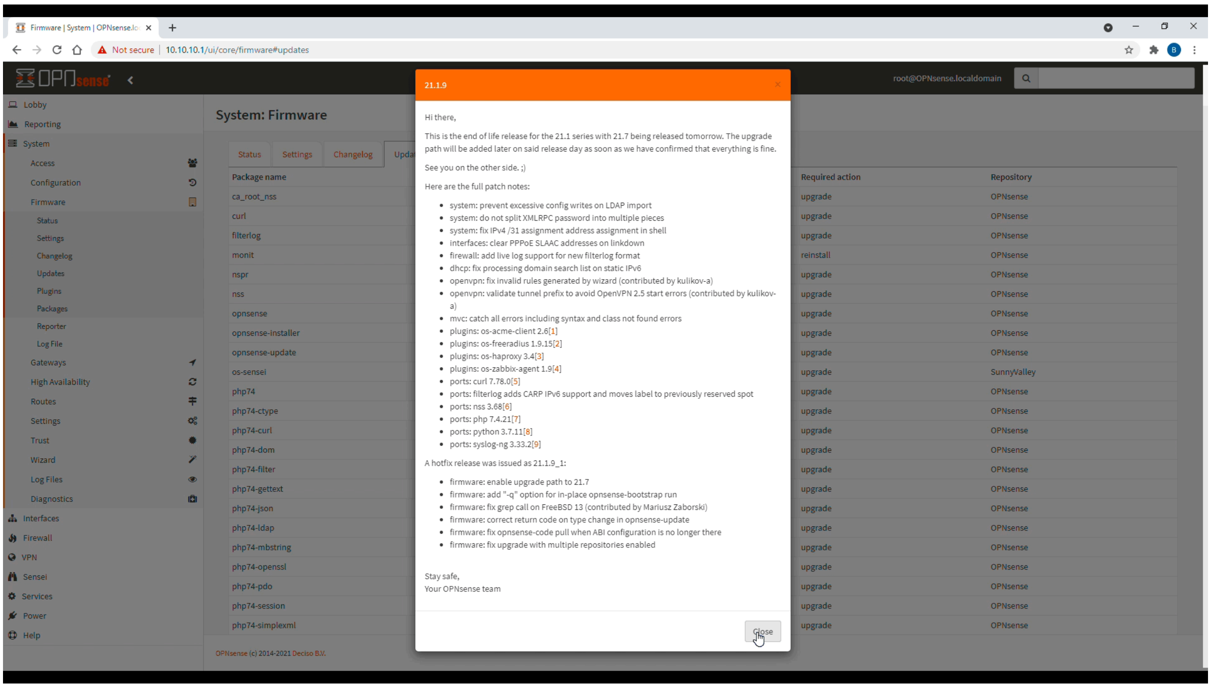
opnsense	21.1.8_1	21.1.9_1	upgrade	OPNsense
opnsense-installer	0.10	21.7	upgrade	OPNsense
opnsense-update	21.1.8	21.1.8_2	upgrade	OPNsense
os-sensei	1.10.alpha19	1.10.alpha20	upgrade	SunnyValley
php74	7.4.20	7.4.21	upgrade	OPNsense
php74-ctype	7.4.20	7.4.21	upgrade	OPNsense
php74-curl	7.4.20	7.4.21	upgrade	OPNsense
php74-dom	7.4.20	7.4.21	upgrade	OPNsense
php74-filter	7.4.20	7.4.21	upgrade	OPNsense
php74-gettext	7.4.20	7.4.21	upgrade	OPNsense
php74-json	7.4.20	7.4.21	upgrade	OPNsense
php74-ldap	7.4.20	7.4.21	upgrade	OPNsense
php74-mbstring	7.4.20	7.4.21	upgrade	OPNsense
php74-openssl	7.4.20	7.4.21	upgrade	OPNsense
php74-pdo	7.4.20	7.4.21	upgrade	OPNsense
php74-session	7.4.20	7.4.21	upgrade	OPNsense
php74-simplexml	7.4.20	7.4.21	upgrade	OPNsense
php74-sockets	7.4.20	7.4.21	upgrade	OPNsense
php74-sqlite3	7.4.20	7.4.21	upgrade	OPNsense
php74-xml	7.4.20	7.4.21	upgrade	OPNsense
php74-zlib	7.4.20	7.4.21	upgrade	OPNsense
py37-cffi	1.14.5	1.14.6	upgrade	OPNsense
py37-sqlite3	3.7.10_7	3.7.11_7	upgrade	OPNsense
python37	3.7.10_1	3.7.11	upgrade	OPNsense
syslog-ng	3.32.1	3.33.2	upgrade	OPNsense

✔ Update ✖ Cancel There are 31 updates available, total download size is 64.0MiB.

Firmware | System | OPNsense.lo
10.10.10.1/ui/core/firmware#updates
root@OPNsense.localdomain
OPNsense (c) 2014-2021 Deciso B.V.

Figure 8. *OPNsense available update packages list*

When there is a new release available, release notes will be displayed. After reading the notes, you may click the **Close** button to close the notification window.



21.1.9

Hi there,

This is the end of life release for the 21.1 series with 21.7 being released tomorrow. The upgrade path will be added later on said release day as soon as we have confirmed that everything is fine.

See you on the other side. ;)

Here are the full patch notes:

- system: prevent excessive config writes on LDAP import
- system: do not split XMLRPC password into multiple pieces
- system: fix IPv4 /31 assignment address assignment in shell
- interfaces: clear PPPoE SLAAC addresses on linkdown
- firewall: add live log support for new filterlog format
- dhcp: fix processing domain search list on static IPv6
- openvpn: fix invalid rules generated by wizard (contributed by kulikov-a)
- openvpn: validate tunnel prefix to avoid OpenVPN 2.5 start errors (contributed by kulikov-a)
- mvc: catch all errors including syntax and class not found errors
- plugins: os-acme-client 2.6[1]
- plugins: os-freeradius 1.9.15[2]
- plugins: os-haproxy 3.4[3]
- plugins: os-zabbix-agent 1.9[4]
- ports: curl 7.78.0[5]
- ports: filterlog adds CARP IPv6 support and moves label to previously reserved spot
- ports: nss 3.68[6]
- ports: php 7.4.21[7]
- ports: python 3.7.11[8]
- ports: syslog-ng 3.33.2[9]

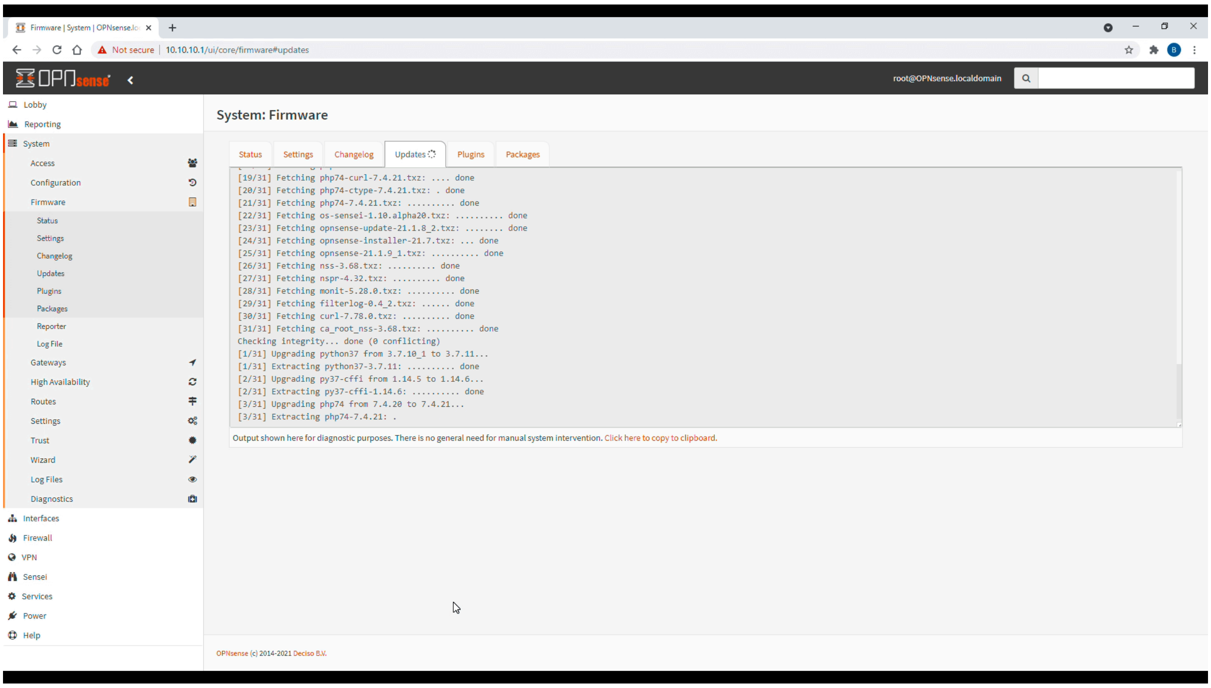
A hotfix release was issued as 21.1.9_1:

- firmware: enable upgrade path to 21.7
- firmware: add "-q" option for in-place opnsense-bootstrap run
- firmware: fix grep call on FreeBSD 13 (contributed by Mariusz Zaborski)
- firmware: correct return code on type change in opnsense-update
- firmware: fix opnsense-code pull when ABI configuration is no longer there
- firmware: fix upgrade with multiple repositories enabled

Stay safe,
Your OPNsense team

Figure 9. *OPNsense 21.1.9 Release notes*

5. Click **Update** button for update. This will fetch and update the packages on the OPNsense system.

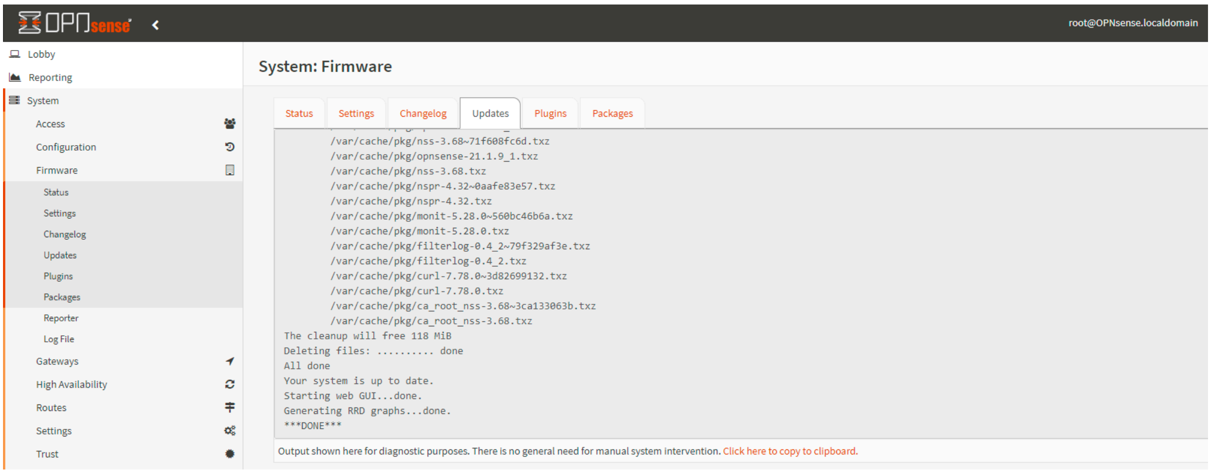


```
[19/31] Fetching php74-curl-7.4.21.txz: .... done
[20/31] Fetching php74-ctype-7.4.21.txz: . done
[21/31] Fetching php74-7.4.21.txz: .......... done
[22/31] Fetching os-sensei-1.10.alpha20.txz: .......... done
[23/31] Fetching opnsense-update-21.1.8_2.txz: ........ done
[24/31] Fetching opnsense-installer-21.7.txz: ... done
[25/31] Fetching opnsense-21.1.9_1.txz: .......... done
[26/31] Fetching nss-3.68.txz: .......... done
[27/31] Fetching nspr-4.32.txz: .......... done
[28/31] Fetching monit-5.28.0.txz: .......... done
[29/31] Fetching filterlog-0.4_2.txz: ...... done
[30/31] Fetching curl-7.78.0.txz: .......... done
[31/31] Fetching ca_root_nss-3.68.txz: .......... done
Checking integrity... done (0 conflicting)
[1/31] Upgrading python37 from 3.7.10_1 to 3.7.11...
[1/31] Extracting python37-3.7.11: .......... done
[2/31] Upgrading py37-cffi from 1.14.5 to 1.14.6...
[2/31] Extracting py37-cffi-1.14.6: .......... done
[3/31] Upgrading php74 from 7.4.20 to 7.4.21...
[3/31] Extracting php74-7.4.21: .
```

Output shown here for diagnostic purposes. There is no general need for manual system intervention. Click here to copy to clipboard.

Figure 10. *Fetching and updating the OPNsense packages*

6. When the OPNsense update is completed successfully, **DONE** message is displayed under the **Updates** pane.

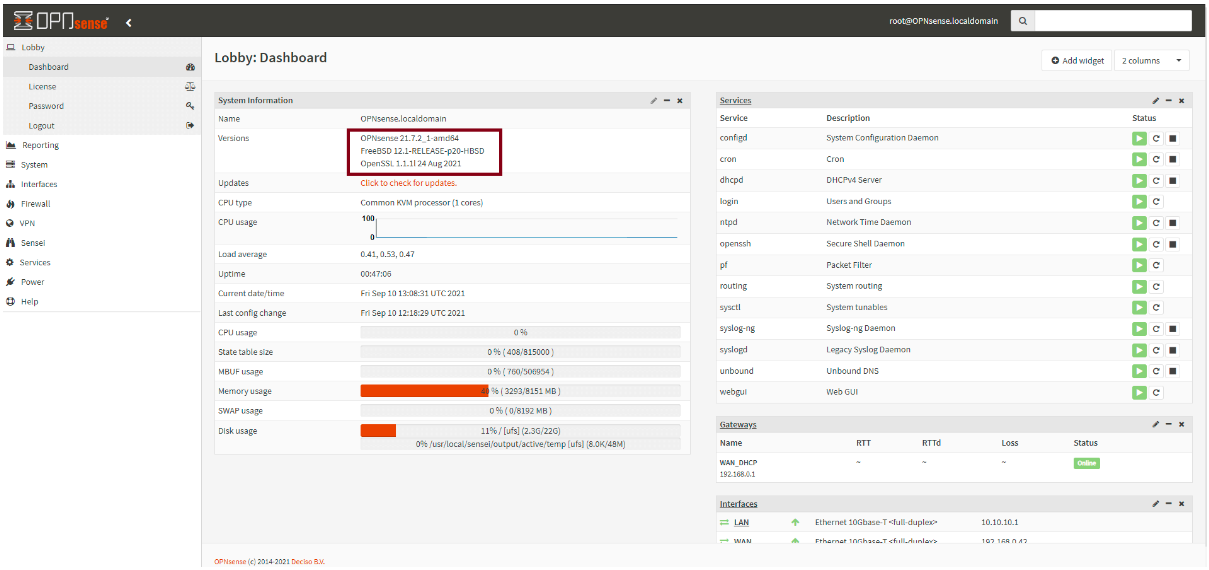


```
        /var/cache/pkg/nss-3.68~71f608fc6d.txz
        /var/cache/pkg/opnsense-21.1.9_1.txz
        /var/cache/pkg/nss-3.68.txz
        /var/cache/pkg/nspr-4.32~0aafe83e57.txz
        /var/cache/pkg/nspr-4.32.txz
        /var/cache/pkg/monit-5.28.0~560bc46b6a.txz
        /var/cache/pkg/monit-5.28.0.txz
        /var/cache/pkg/filterlog-0.4_2~79f329af3e.txz
        /var/cache/pkg/filterlog-0.4_2.txz
        /var/cache/pkg/curl-7.78.0~3d82699132.txz
        /var/cache/pkg/curl-7.78.0.txz
        /var/cache/pkg/ca_root_nss-3.68~3ca133063b.txz
        /var/cache/pkg/ca_root_nss-3.68.txz
The cleanup will free 118 MiB
Deleting files: .......... done
All done
Your system is up to date.
Starting web GUI...done.
Generating RRD graphs...done.
***DONE***
```

Output shown here for diagnostic purposes. There is no general need for manual system intervention. Click here to copy to clipboard.

Figure 11. *Updating the OPNsense is completed*

7. You may view the installed OPNsense version in the **System Information** pane on `Dashboard`.



Lobby: Dashboard

System Information

Name	OPNsense.localdomain
Versions	OPNsense 21.7.2_1-amd64 FreeBSD 12.1-RELEASE-p20-HBSD OpenSSL 1.1.1l 24 Aug 2021
Updates	Click to check for updates.
CPU type	Common KVM processor (1 cores)
CPU usage	100 0
Load average	0.41, 0.53, 0.47
Uptime	00:47:06
Current date/time	Fri Sep 10 13:08:31 UTC 2021
Last config change	Fri Sep 10 12:18:29 UTC 2021
CPU usage	0 %
State table size	0 % (408/815000)
MBUF usage	0 % (760/506954)
Memory usage	40 % (3293/8151 MB)
SWAP usage	0 % (0/8192 MB)
Disk usage	11% / [ufs] (2.3G/22G) 0% /usr/local/sensei/output/active/temp [ufs] (8.0K/48M)

Services

Service	Description	Status
configd	System Configuration Daemon	▶ ↻ ■
cron	Cron	▶ ↻ ■
dhcpd	DHCPv4 Server	▶ ↻ ■
login	Users and Groups	▶ ↻
ntpd	Network Time Daemon	▶ ↻ ■
openssh	Secure Shell Daemon	▶ ↻ ■
pf	Packet Filter	▶ ↻
routing	System routing	▶ ↻
sysctl	System tunables	▶ ↻
syslog-ng	Syslog-ng Daemon	▶ ↻ ■
syslogd	Legacy Syslog Daemon	▶ ↻ ■
unbound	Unbound DNS	▶ ↻ ■
webgui	Web GUI	▶ ↻

Gateways

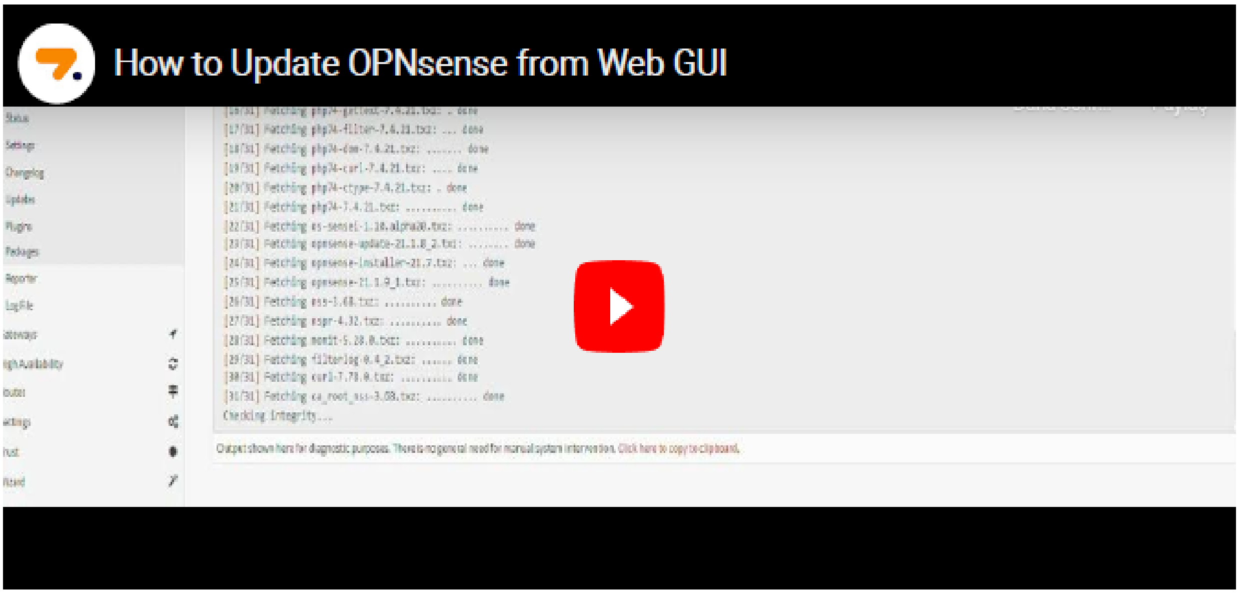
Name	RTT	RTTd	Loss	Status
WAN_DHCP 192.168.0.1	~	~	~	Online

Interfaces

LAN	↑	Ethernet 10Gbase-T <full-duplex>	10.10.10.1
WAN	↑	Ethernet 10Gbase-T <full-duplex>	192.168.0.42

OPNsense (c) 2014-2021 Deciso B.V.

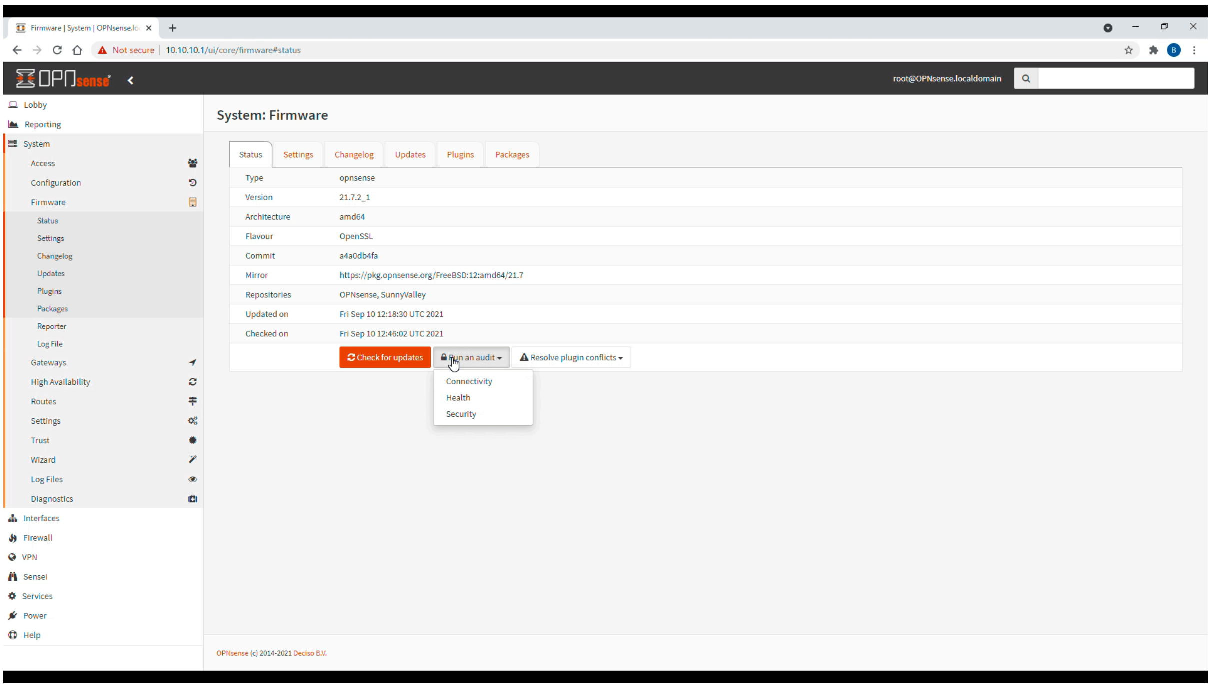
Figure 12. *Viewing the OPNsense version on Dashboard*



```
[16/31] Fetching php74-gettext-7.4.21.txz: . done
[17/31] Fetching php74-filter-7.4.21.txz: ... done
[18/31] Fetching php74-dom-7.4.21.txz: ....... done
[19/31] Fetching php74-curl-7.4.21.txz: .... done
[20/31] Fetching php74-ctype-7.4.21.txz: . done
[21/31] Fetching php74-7.4.21.txz: .......... done
[22/31] Fetching os-sensei-1.10.alpha20.txz: .......... done
[23/31] Fetching opnsense-update-21.1.8_2.txz: ........ done
[24/31] Fetching opnsense-installer-21.7.txz: ... done
[25/31] Fetching opnsense-21.1.9_1.txz: .......... done
[26/31] Fetching nss-3.68.txz: .......... done
[27/31] Fetching nspr-4.32.txz: .......... done
[28/31] Fetching monit-5.28.0.txz: .......... done
[29/31] Fetching filterlog-0.4_2.txz: ...... done
[30/31] Fetching curl-7.78.0.txz: .......... done
[31/31] Fetching ca_root_nss-3.68.txz: .......... done
Checking integrity...
```

Output shown here for diagnostic purposes. There is no general need for manual system intervention. Click here to copy to clipboard.

8. After updating your OPNsense firewall, you may run the audit by clicking on the **Run Audit** dropdown menu on the Status pane of the **Systems: Firmware** page.

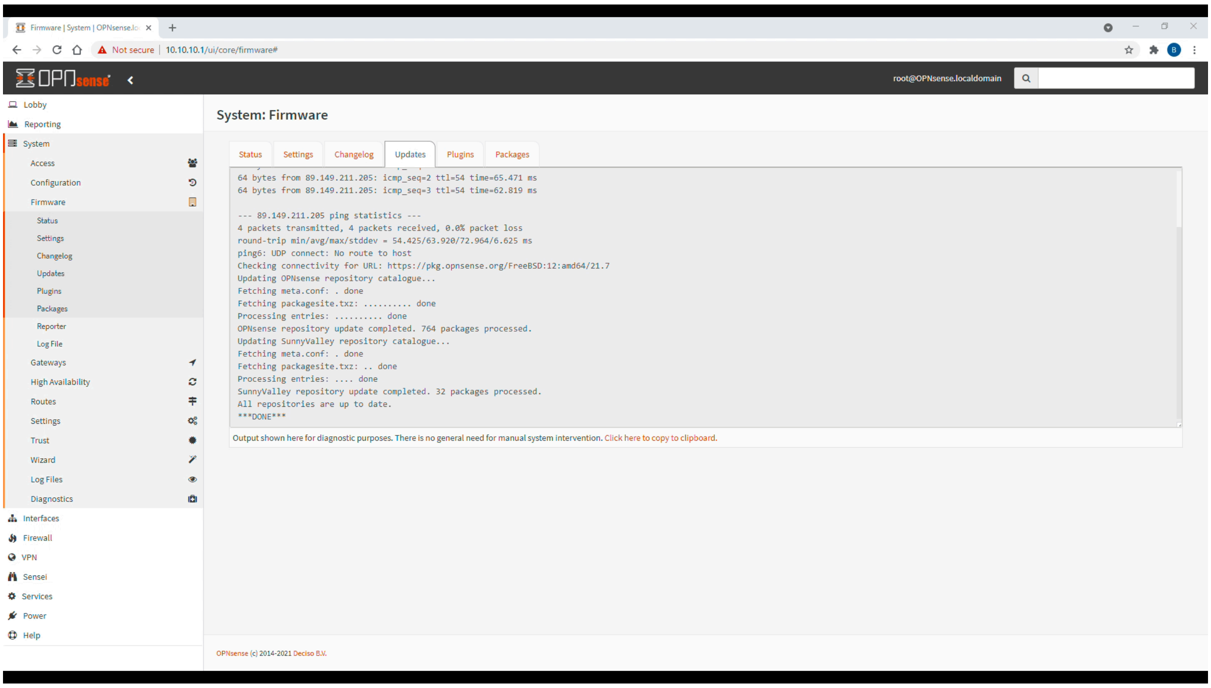


Type	opnsense
Version	21.7.2_1
Architecture	amd64
Flavour	OpenSSL
Commit	a4a0db4fa
Mirror	https://pkg.opnsense.org/FreeBSD:12:amd64/21.7
Repositories	OPNsense, SunnyValley
Updated on	Fri Sep 10 12:18:30 UTC 2021
Checked on	Fri Sep 10 12:46:02 UTC 2021

Figure 13. *Running Audit on OPNsense*

The following options are available for OPNsense audit:

1. **Connectivity**: Checks the mirror connection and updates the repositories

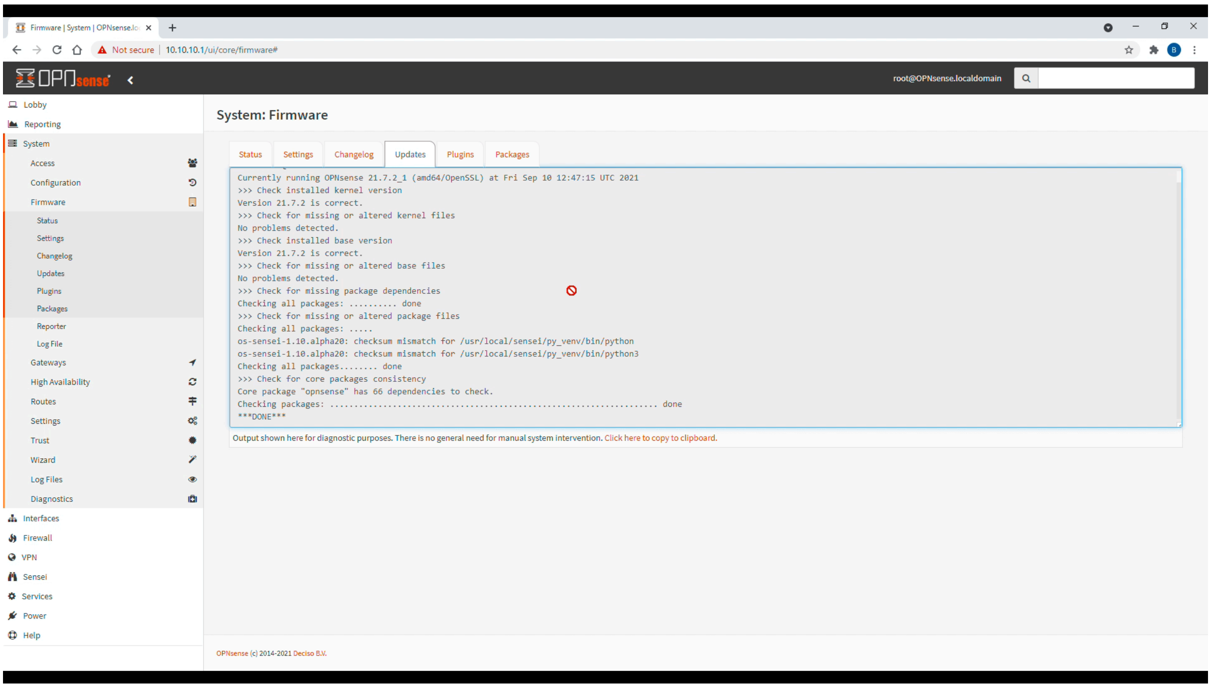


```
64 bytes from 89.149.211.205: icmp_seq=2 ttl=54 time=65.471 ms
64 bytes from 89.149.211.205: icmp_seq=3 ttl=54 time=62.819 ms

--- 89.149.211.205 ping statistics ---
4 packets transmitted, 4 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 54.425/63.920/72.964/6.625 ms
ping6: UDP connect: No route to host
Checking connectivity for URL: https://pkg.opnsense.org/FreeBSD:12:amd64/21.7
Updating OPNsense repository catalogue...
Fetching meta.conf: . done
Fetching packagesite.txz: .......... done
Processing entries: .......... done
OPNsense repository update completed. 764 packages processed.
Updating SunnyValley repository catalogue...
Fetching meta.conf: . done
Fetching packagesite.txz: .. done
Processing entries: .... done
SunnyValley repository update completed. 32 packages processed.
All repositories are up to date.
***DONE***
```

Output shown here for diagnostic purposes. There is no general need for manual system intervention. Click here to copy to clipboard.

Figure 14. *Connectivity Audit*

2. **Health**: Health audit checks for missing dependencies, missing kernel files, core package consistencies

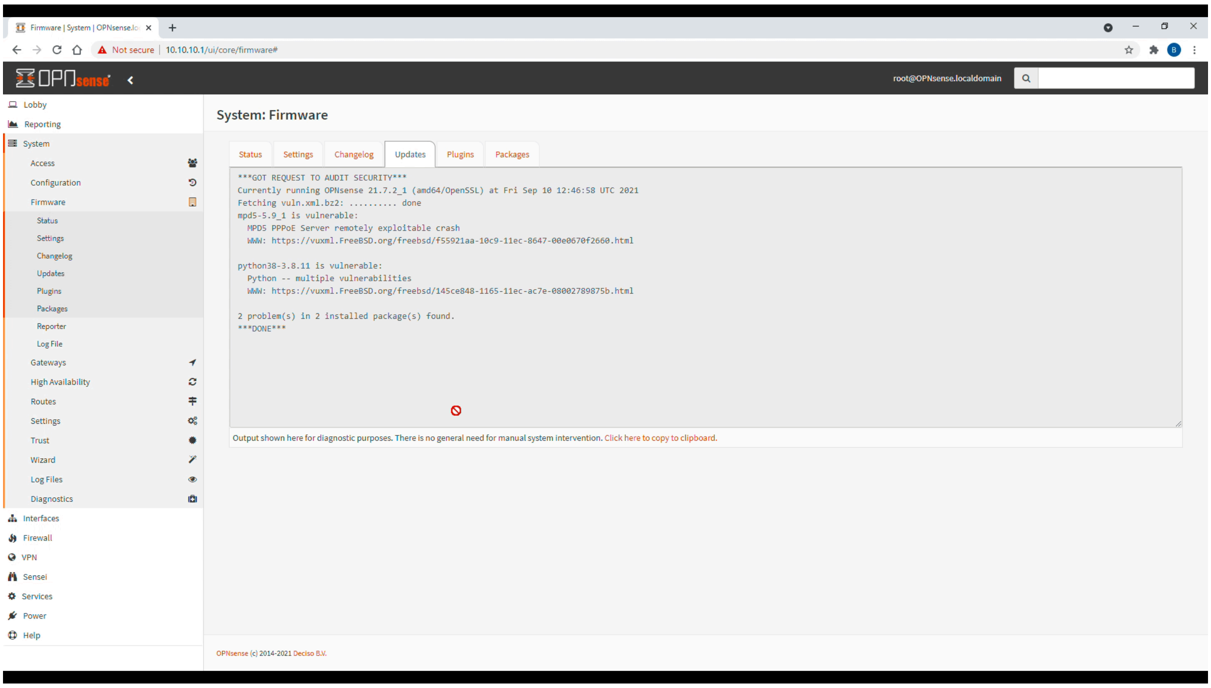


```
Currently running OPNsense 21.7.2_1 (amd64/OpenSSL) at Fri Sep 10 12:47:15 UTC 2021
>>> Check installed kernel version
Version 21.7.2 is correct.
>>> Check for missing or altered kernel files
No problems detected.
>>> Check installed base version
Version 21.7.2 is correct.
>>> Check for missing or altered base files
No problems detected.
>>> Check for missing package dependencies
Checking all packages: .......... done
>>> Check for missing or altered package files
Checking all packages: .....
os-sensei-1.10.alpha20: checksum mismatch for /usr/local/sensei/py_venv/bin/python
os-sensei-1.10.alpha20: checksum mismatch for /usr/local/sensei/py_venv/bin/python3
Checking all packages........ done
>>> Check for core packages consistency
Core package "opnsense" has 66 dependencies to check.
Checking packages: ............................................................. done
***DONE***
```

Output shown here for diagnostic purposes. There is no general need for manual system intervention. Click here to copy to clipboard.

Figure 15. *Health Audit*

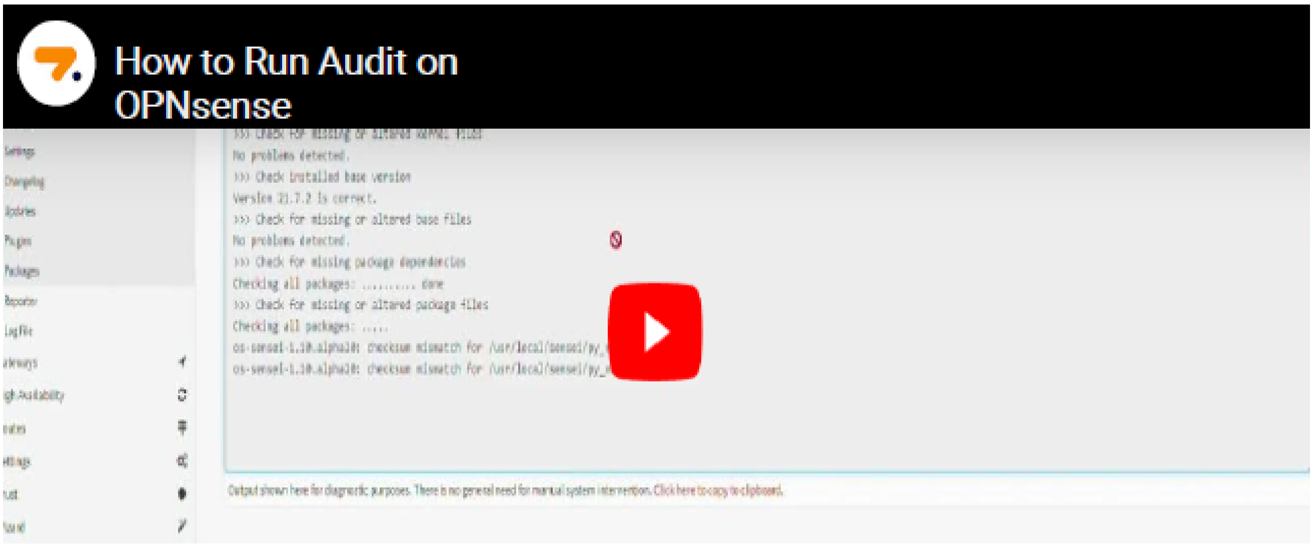
3. **Security**: Vulnerabilities on the OPNsense listed on the audit security report.



```
***GOT REQUEST TO AUDIT SECURITY***
Currently running OPNsense 21.7.2_1 (amd64/OpenSSL) at Fri Sep 10 12:46:58 UTC 2021
Fetching vuln.xml.bz2: .......... done
mpd5-5.9_1 is vulnerable:
  MPD5 PPPoE Server remotely exploitable crash
  WWW: https://vuxml.FreeBSD.org/freebsd/f55921aa-10c9-11ec-8647-00e0670f2660.html

python38-3.8.11 is vulnerable:
  Python -- multiple vulnerabilities
  WWW: https://vuxml.FreeBSD.org/freebsd/145ce848-1165-11ec-ac7e-08002789875b.html

2 problem(s) in 2 installed package(s) found.
***DONE***
```

Output shown here for diagnostic purposes. There is no general need for manual system intervention. Click here to copy to clipboard.

Figure 16. *Audit security report*



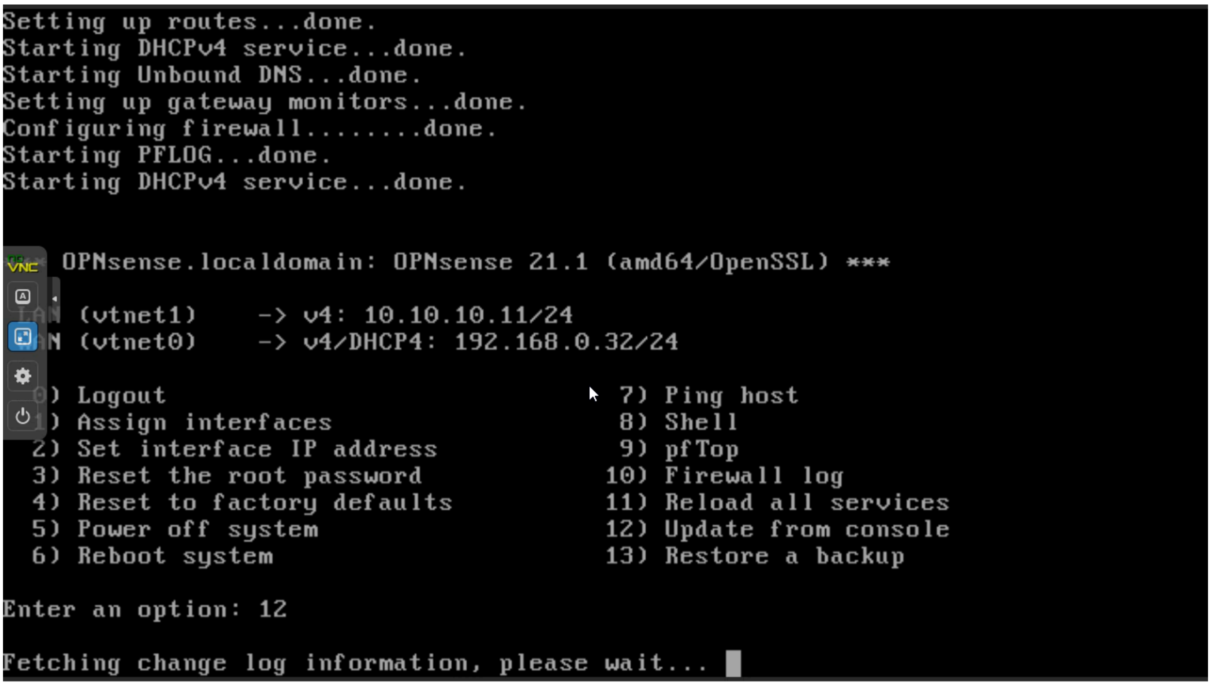
How to Run Audit on OPNsense

```
>>> Check for missing or altered kernel files
No problems detected.
>>> Check installed base version
Version 21.7.2 is correct.
>>> Check for missing or altered base files
No problems detected.
>>> Check for missing package dependencies
Checking all packages: .......... done
>>> Check for missing or altered package files
Checking all packages: .....
os-sensei-1.10.alpha10: checksum mismatch for /usr/local/sensei/py_
os-sensei-1.10.alpha10: checksum mismatch for /usr/local/sensei/py_
```

Output shown here for diagnostic purposes. There is no general need for manual system intervention. Click here to copy to clipboard.

Updating OPNsense on Console/CLI

1. Connect the OPNsense via VGA display or serial port.
2. Login as `root`. Then, the console menu will be displayed.
3. Select **12) Update from console**. Beware that reboot may be necessary. You're asked to proceed to continue. Type `y` and press enter. This will automatically fetch all available updates and apply them.



```
Setting up routes...done.
Starting DHCPv4 service...done.
Starting Unbound DNS...done.
Setting up gateway monitors...done.
Configuring firewall........done.
Starting PFLOG...done.
Starting DHCPv4 service...done.


    OPNsense.localdomain: OPNsense 21.1 (amd64/OpenSSL) ***

  LAN (vtnet1)     -> v4: 10.10.10.11/24
  WAN (vtnet0)     -> v4/DHCP4: 192.168.0.32/24

  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: 12

Fetching change log information, please wait...
```

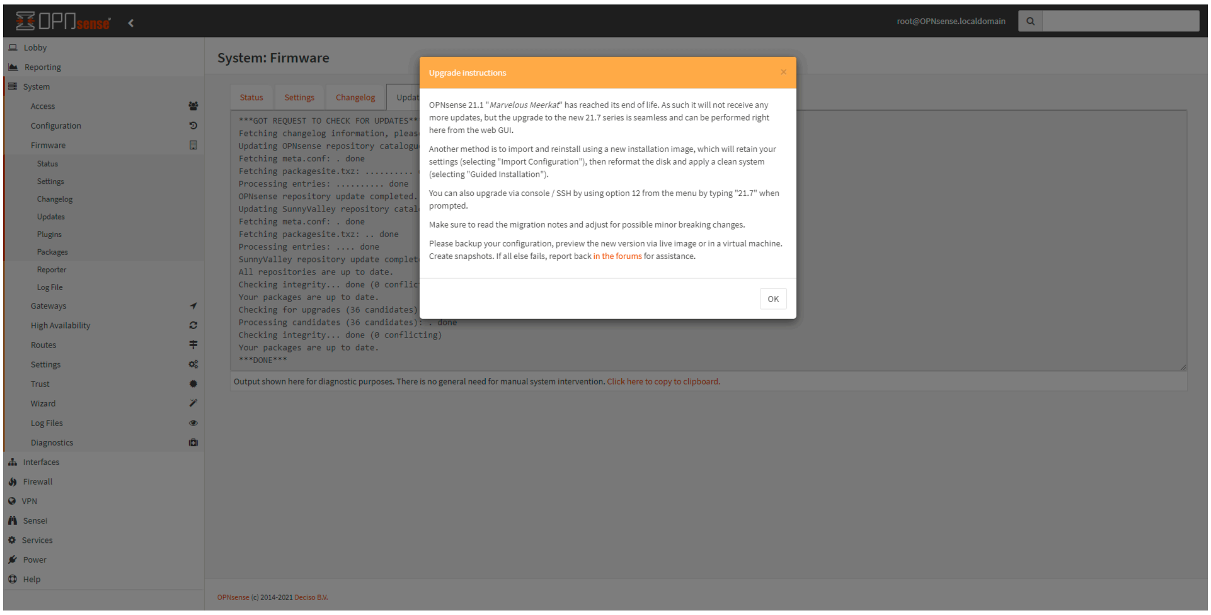
Figure 17. *Update OPNsense from console*

4. If necessary, OPNsense may reboot. Then, it will be on the desired release.

What is the Offline Upgrade of OPNsense?

Major updates of OPNsense are installed offline. That means no web interface or SSH is available to monitor the upgrade. OPNsense downloads all release files for an offline upgrade (kernel, packages, etc.), and then reboots. After a reboot, it will install all available updates, reboot again, and then you should be on the desired version. If something goes wrong, you'll need a second connection or direct access to revert or repair the VM. Major upgrades of OPNsense should be performed using a VGA display or serial port so that you can see what is going on.

If there is a major upgrade available for the OPNsense firewall, upgrade instructions are displayed similar to the Figure 18 below when you check for updates on OPNsense web GUI.



System: Firmware

```
***GOT REQUEST TO CHECK FOR UPDATES**
Fetching changelog information, pleas
Updating OPNsense repository catalogu
Fetching meta.conf: . done
Fetching packagesite.txz: .........
Processing entries: .......... done
OPNsense repository update completed.
Updating SunnyValley repository catal
Fetching meta.conf: . done
Fetching packagesite.txz: .. done
Processing entries: .... done
SunnyValley repository update complet
All repositories are up to date.
Checking integrity... done (0 conflic
Your packages are up to date.
Checking for upgrades (36 candidates)
Processing candidates (36 candidates): . done
Checking integrity... done (0 conflicting)
Your packages are up to date.
***DONE***
```

Output shown here for diagnostic purposes. There is no general need for manual system intervention. Click here to copy to clipboard.

Upgrade instructions

OPNsense 21.1 "*Marvelous Meerkat*" has reached its end of life. As such it will not receive any more updates, but the upgrade to the new 21.7 series is seamless and can be performed right here from the web GUI.

Another method is to import and reinstall using a new installation image, which will retain your settings (selecting "Import Configuration"), then reformat the disk and apply a clean system (selecting "Guided Installation").

You can also upgrade via console / SSH by using option 12 from the menu by typing "21.7" when prompted.

Make sure to read the migration notes and adjust for possible minor breaking changes.

Please backup your configuration, preview the new version via live image or in a virtual machine. Create snapshots. If all else fails, report back in the forums for assistance.

Figure 18. *OPNsense 21.7 major upgrade instructions*

How to connect OPNsense from the serial console

OPNsense can be controlled via serial in addition to the web user interface, monitor and SSH. Accessing OPNsense via serial is similar to SSH. You can access your OPNsense node at any time via serial, even when it is not accessible via the network. This makes it particularly useful for installing OPNsense, performing major system upgrades and performing emergency troubleshooting when there is a network outage.

Prerequisites

Requirements for the OPNsense serial access are as follows:

- A serial interface must be provided as part of the OPNsense installation (hardware or virtual)
- Software that can be used to connect to the serial interface, such as PuTTY, minicom, screen, etc.)

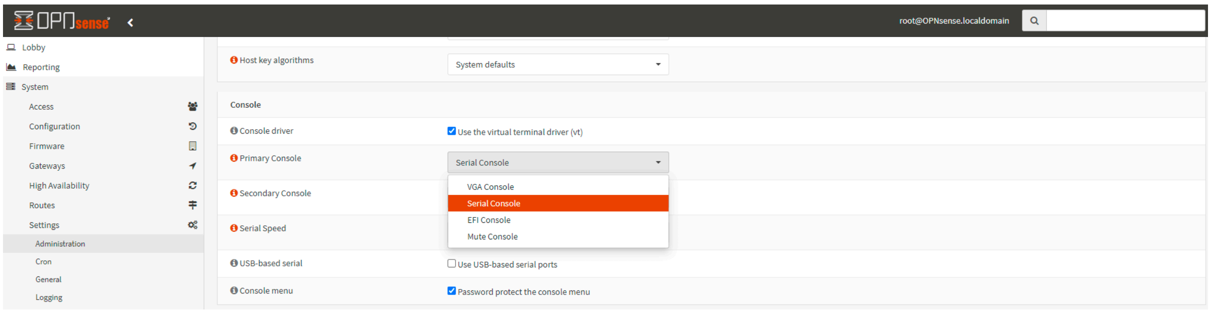
For a bare metal installation, you will also require the following:

- a null modem cable
- If your computer does not have an RS232 port, you will require a USB to RS232 converter.

Connecting to the serial console

If you previously installed OPNsense using a non-serial installer, serial access must be enabled. To enable serial access on OPNsense,

1. Login as `root` via the web interface.
2. Navigate to **System -> Settings -> Administration**.
3. Scroll down to **Console** and select **Serial console** as the primary or secondary console.
4. Click **Save** button at the bottom of the page.



Host key algorithms: System defaults

Console

Console driver: ☑ Use the virtual terminal driver (vt)

Primary Console: Serial Console

Secondary Console

Serial Speed

USB-based serial: □ Use USB-based serial ports

Console menu: ☑ Password protect the console menu

Figure 19. *Console settings on OPNsense*

DANGER

Please keep in mind that this is only required if you have already installed OPNsense and did not use the serial installer. Serial access is already available in all other cases (accessing BIOS, running the serial installer, connecting to a serial installation).

On Unix-like systems, use the `minicom` to connect to the serial console at 115200 baud. The device name can differ depending on the system and serial device. Here are some examples of names:

- /dev/cuau0 (serial port, FreeBSD or HardenedBSD)
- /dev/cuaU0 (usb-to-serial, FreeBSD or HardenedBSD)
- /dev/ttyS0 (serial port, Linux)
- /dev/ttyUSB0 (usb-to-serial, Linux)
- COM1, COM2, etc. (Windows)
- /dev/tty.usbmodem1112421 (usb-to-serial, macOS)

```
minicom -b 115200 -D /dev/ttyS0
```

📣 **INFO**

If you have a number of devices of the same type, as shown here:

```
ls /dev/ttyUSB*
 /dev/ttyUSB0 /dev/ttyUSB1
```

You may disconnect one of the serial devices to see which one is still active, or you may investigate the `dmesg` log to find out the vendor of the device node. To determine which device it is, look for a message that contains the phrase `now attached to ttyUSB1`. Following that, you may compare the previous output to the output of a tool such as `lsusb`.

📝**NOTE**

Since accessing the serial device is restricted, you should run the command as root on Linux / BSD.

If authentication is enabled and OPNsense is running, you will now be prompted for your username and password. Otherwise, the menu appears (at least after pressing enter). The credentials are identical to those required for SSH.

📝 **NOTE**

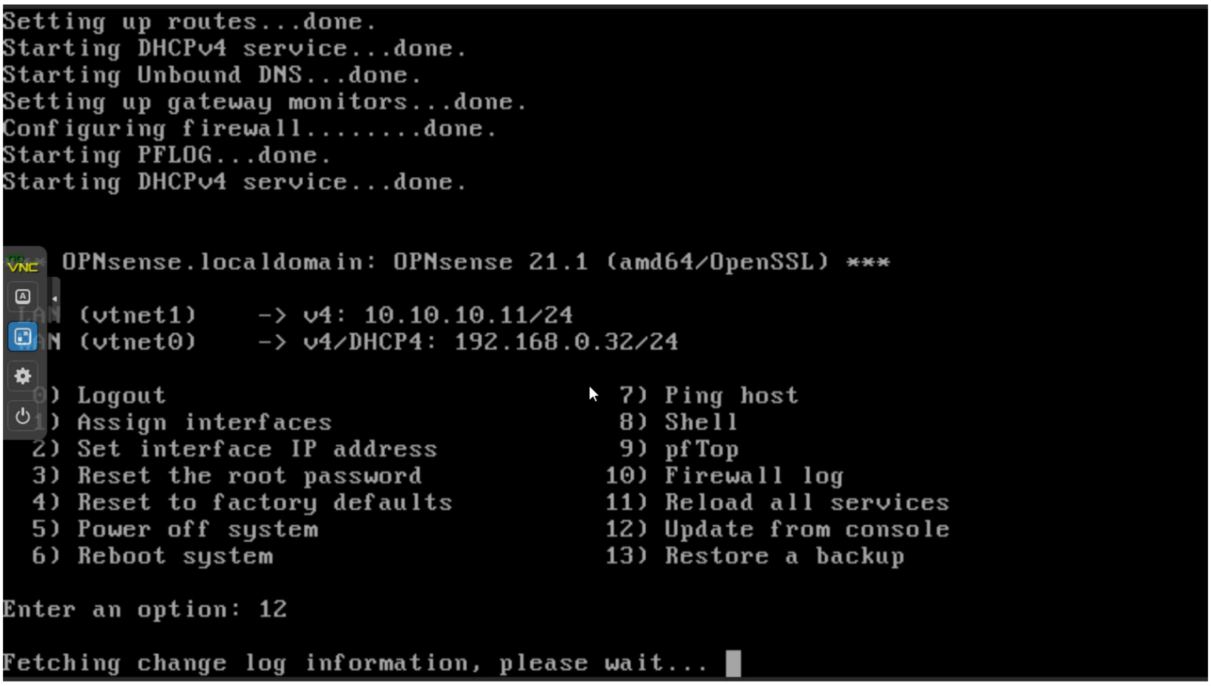
The screen does not always update automatically. If you connect but receive no output, try pressing `Enter` first before looking into the other (more complex) potentials.

Another issue is that when connecting via `screen`, you may be unable to scroll but you can still pipe the output using `more` or `less`.

Major Upgrade of OPNsense from Console/CLI

To deploy a major upgrade on an OPNsense firewall, you may follow the next instructions given below:

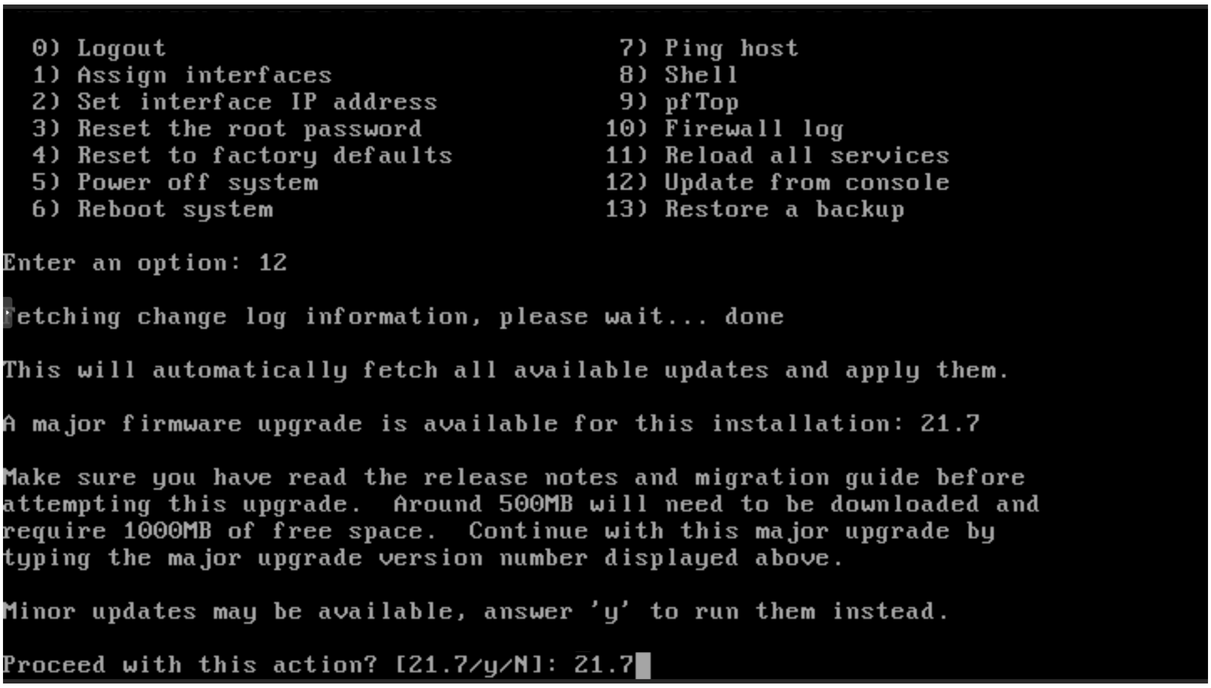
1. Connect the OPNsense via VGA display or serial port.
2. Login as `root`. Then, the console menu will be displayed.
3. Select **12) Update from console**. You're asked whether you want to upgrade to the most recent version or the next major release.



```
Setting up routes...done.
Starting DHCPv4 service...done.
Starting Unbound DNS...done.
Setting up gateway monitors...done.
Configuring firewall.......done.
Starting PFLOG...done.
Starting DHCPv4 service...done.


    OPNsense.localdomain: OPNsense 21.1 (amd64/OpenSSL) ***

     (vtnet1)     -> v4: 10.10.10.11/24
    N (vtnet0)    -> v4/DHCP4: 192.168.0.32/24

    ) Logout                              7) Ping host
    ) 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: 12

Fetching change log information, please wait...
```

Figure 20. *Update OPNsense from console*

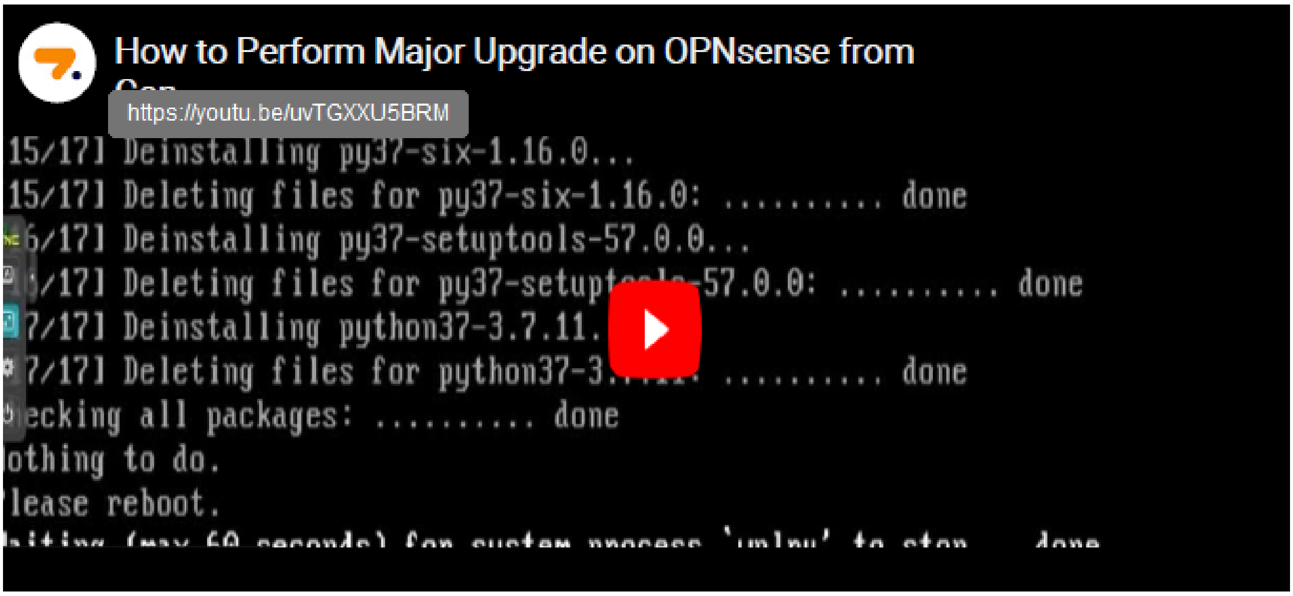
4. Type in the major release number (for example `21.7`) and press enter. All release files will be downloaded for an offline upgrade (kernel, packages etc.). Then, OPNsense will reboot.



```
  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: 12

Fetching change log information, please wait... done

This will automatically fetch all available updates and apply them.

A major firmware upgrade is available for this installation: 21.7

Make sure you have read the release notes and migration guide before
attempting this upgrade.  Around 500MB will need to be downloaded and
require 1000MB of free space.  Continue with this major upgrade by
typing the major upgrade version number displayed above.

Minor updates may be available, answer 'y' to run them instead.

Proceed with this action? [21.7/y/N]: 21.7
```

Figure 21. *Installing major updates for OPNsense 21.7 on console*

5. After a reboot, it will install all updates. Once the installation is completed, it will reboot again, at which point it should be on the preferred release.


How to Perform Major Upgrade on OPNsense from Con
https://youtu.be/uvTGXXU5BRM

```
15/171] Deinstalling py37-six-1.16.0...
15/171] Deleting files for py37-six-1.16.0: .......... done
6/171] Deinstalling py37-setuptools-57.0.0...
/171] Deleting files for py37-setupt    -57.0.0: .......... done
7/171] Deinstalling python37-3.7.11.
7/171] Deleting files for python37-3.    .......... done
ecking all packages: .......... done
othing to do.
lease reboot.
aiting (max 60 seconds) for system process `vnlru' to stop... done
```

How to Manage Users and Authentication on OPNsense

OPNsense is a free and open-source firewall and router software that can secure and manage your network. Managing users and authentication is a critical component of running an OPNsense firewall. This encompasses both the creation and management of user accounts, as well as the configuration of authentication mechanisms.

OPNsense user management and authentication are critical for ensuring the integrity, confidentiality, and availability of network resources and firewall settings. It is a vital component of network security because it allows companies to manage access to important systems and ensures that only authorized individuals may modify network configurations. Organizations improve their overall network security posture and guard against possible attacks by employing strong identity and access management (IAM) procedures and effective authentication techniques.

In this article, we will provide you with information about user management and authentication types in OPNsense and present a comprehensive guide on how to implement them. The following topics are covered:

- Access / User Management
- Accessing the OPNsense Web Interface
- Authentication
- User Manager
- Adding a New User
- Setting User Permissions
- Enabling Two-Factor Authentication (Optional)
- Managing Existing Users
- Creating User Groups
- Authorization
- LDAP/Active Directory Integration (Optional)
- Setting Up Captive Portal (Optional)
- Enabling Local Certificate Authority (Optional)
- Configuring Authentication Servers (Radius)
- Password Policy (Optional)
- Authentication services
- Testing User Authentication

Now, let's begin our article by addressing the topic of User Management, which is our first heading.

1. Access / User Management

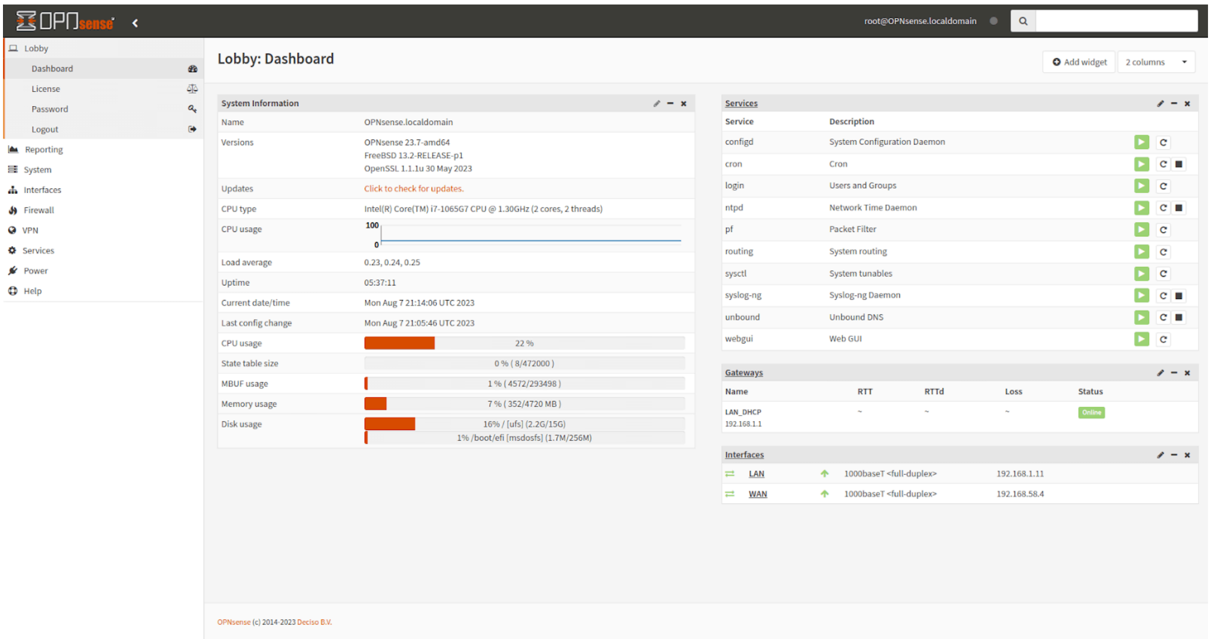
OPNsense offers robust access and user management capabilities, allowing administrators to control and secure their network environment effectively. Through the intuitive web interface, administrators can create and manage user accounts, assign privileges, and control access to various network resources. User authentication methods, such as local databases, LDAP, and RADIUS, provide flexibility in integrating with existing authentication systems. Additionally, role-based access control (RBAC) enables fine-grained permission assignment, ensuring that users only have the necessary access privileges for their specific tasks while maintaining overall network security.

Firstly, let's touch upon the topic of web interface access in order for us to manage user accounts

1.1 Accessing the OPNsense Web Interface

To access the OPNsense web interface and begin user management, you can follow these steps:

1. **Connect to the Network**: Ensure that your computer or device is connected to the same network as the OPNsense firewall.
2. **Open a Web Browser**: Launch your preferred web browser (e.g., Chrome, Firefox, Safari).
3. **Enter the IP Address**: In the address bar of the web browser, enter the IP address of the OPNsense firewall. This is typically the LAN IP address of the OPNsense firewall.
4. **Access the Web Interface**: Press Enter or Return to access the OPNsense web interface. You should now see the login page.
5. **Enter Login Credentials**: Enter the username and password for an authorized user account. The username is "root" by default, and the password is the one you selected during the installation procedure or the default password "OPNsense" on the OPNsense firewall.



Lobby: Dashboard

System Information

Name	OPNsense.localdomain
Versions	OPNsense 23.7-amd64 FreeBSD 13.2-RELEASE-p1 OpenSSL 1.1.1u 30 May 2023
Updates	Click to check for updates.
CPU type	Intel(R) Core(TM) i7-1065G7 CPU @ 1.30GHz (2 cores, 2 threads)
CPU usage	100 0
Load average	0.23, 0.24, 0.25
Uptime	05:37:11
Current date/time	Mon Aug 7 21:14:06 UTC 2023
Last config change	Mon Aug 7 21:05:46 UTC 2023
CPU usage	22 %
State table size	0 % (8/472000)
MBUF usage	1 % (4572/293498)
Memory usage	7 % (352/4720 MB)
Disk usage	16% / [ufs] (2.2G/15G) 1% /boot/efi [msdosfs] (1.7M/256M)

Services

Service	Description
configd	System Configuration Daemon
cron	Cron
login	Users and Groups
ntpd	Network Time Daemon
pf	Packet Filter
routing	System routing
sysctl	System tunables
syslog-ng	Syslog-ng Daemon
unbound	Unbound DNS
webgui	Web GUI

Gateways

Name	RTT	RTTd	Loss	Status
LAN_DHCP 192.168.1.1	~	~	~	Online

Interfaces

LAN	1000baseT <full-duplex>	192.168.1.11
WAN	1000baseT <full-duplex>	192.168.58.4

OPNsense (c) 2014-2023 Deciso B.V.

Figure 1. *OPNsense Dashboard*

You can now proceed with the management of your users.

2. Authentication

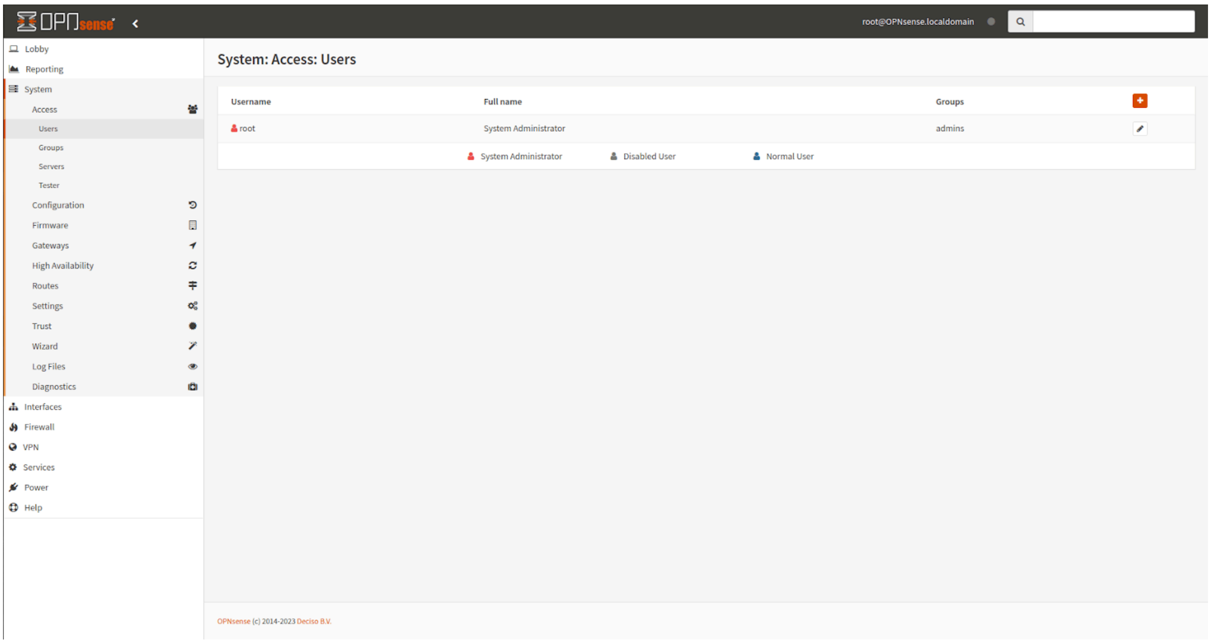
Authentication is a crucial aspect of OPNsense, ensuring secure access to network resources. This involves verifying the identity of users trying to log in, thus preventing unauthorized access. Once we understand authentication, we can move on to exploring the topic of user management, which encompasses creating, configuring, and controlling user accounts and their permissions within the system.

2.1 User Manager

To navigate to the **User Manager** section in OPNsense and add, edit, or delete users, you can follow these steps:

1. **Open the Web Interface**: Open the OPNsense web interface by entering the IP address of the firewall in the address bar of your web browser.
2. **Log in**: Enter the username and password for an authorized user account to log in to the web interface.
3. **Navigate to User Management**: Once logged in, navigate to the user management section of the web interface. This can usually be found under **System -> Access -> Users**

4. **Add Users**: To add a new user, click on the "**+**" sign at the bottom right corner of the form
5. **Edit Users**: To edit an existing user, click on the "**Edit**" icon (a pencil) next to the user's name
6. **Delete Users**: To delete a user, click on the "**Delete**" icon (a trash can) next to the user's name
7. **Define User Privileges**: In the user management section, you can define the privileges and access of each user to different parts of the GUI



System: Access: Users

Username	Full name	Groups
root	System Administrator	admins

System Administrator   Disabled User   Normal User

OPNsense (c) 2014-2023 Deciso B.V.

Figure 2. *OPNsense System: Access: Users*

Let's continue by adding a new user to our firewall.

2.2 Adding a New User

Adding a new user to your OPNsense firewall allows you to grant individuals access to your network management interface with specific permissions. This guide outlines the steps to create a new user account.

You can follow the Steps to create a **New User.**

Step 1: Log in to the OPNsense Web Interface

Using your administrative credentials, log in to the OPNsense web interface. This is the starting point for managing users and other settings.

Step 2: Navigate to the "User Manager" Section

Find and access the "User Manager" section within the web interface. This is where you'll be able to manage user accounts and their settings.

Step 3: Click on "Add" to Create a New User

To create a new user, click on the "Add" button. This initiates the process of adding a user account.

Step 4: Enter User Details

Now, provide the following details for the new user:

Username: Choose a unique username for the user. In this case, let's use "alex."

Password: Enter a secure password for the user. Make sure it follows password best practices.

Full Name: Provide the user's full name. For example, "Aleksandros."

E-Mail: Enter the user's email address, like "aleksandros@zenarmor.com."

Comment: Optionally, you can add a comment to provide additional information about the user.

Preferred Landing Page: This determines where the user will be directed after logging in. "**Default**" usually refers to the dashboard.

Language: Set the language preference for the user's interface.

Login Shell: This is the command interpreter that the user will use when they log in. "/sbin/nologin" restricts shell access.

In OPNsense, the login shell determines the command interpreter that is used when a user logs into the system. Here are some common login shell types that you might encounter:

1. **/bin/sh**: The Bourne shell is a simple and basic command interpreter that provides a standard set of commands for interacting with the system. It's a lightweight shell with limited features compared to more modern shells.

2. **/bin/csh**: The C shell is known for its C-like syntax and additional interactive features. It offers command-line editing, history, and other conveniences.
3. **/bin/tcsh**: This is an enhanced version of the C shell, providing improvements like better command-line editing and more advanced scripting capabilities.
4. **/sbin/nologin**: This is not a traditional shell but a way to restrict user access. When a user is set to use "/sbin/nologin," they cannot log in to the system. This is useful for system accounts or accounts that shouldn't have interactive shell access.

Expiration Date: Leave this blank if you don't want the user account to expire.

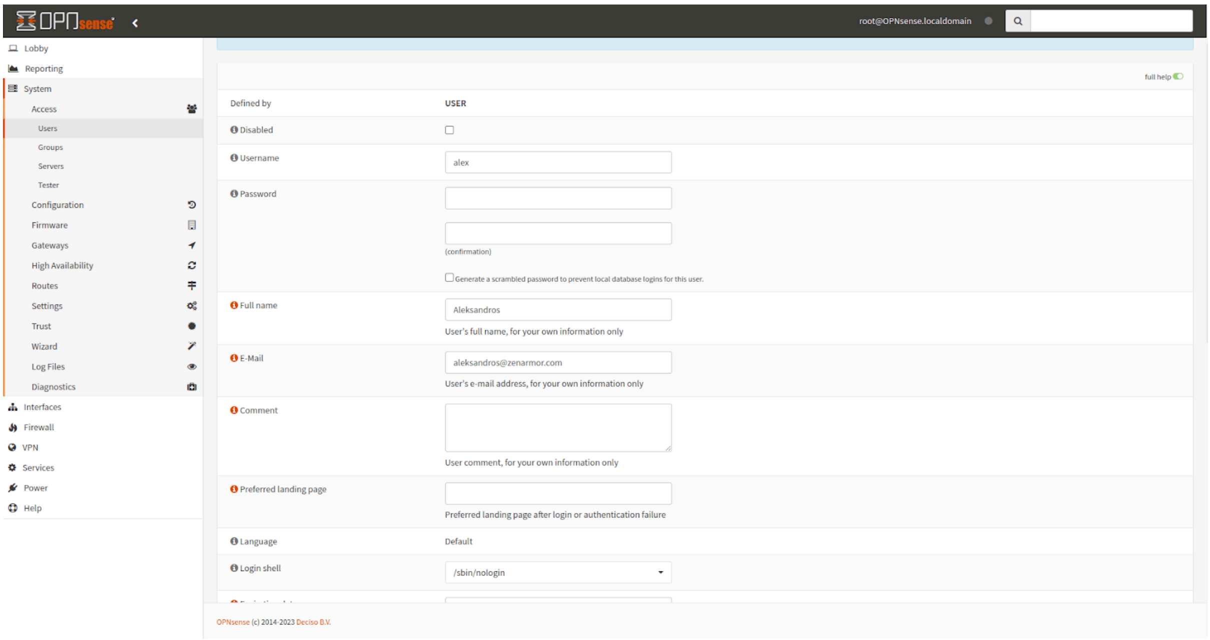
Group Memberships: Specify if the user should be a member of additional groups. For now, select "Not a member of any additional groups."

Certificate: If not creating a user certificate, you can leave this blank.

OTP Seed: If using OTP (one-time password) authentication, a secret seed is generated. You can leave this blank if not using OTP.

Authorized Keys: If using SSH keys for authentication, you can paste them here.

Step 5: Click "Save" to Create a New User

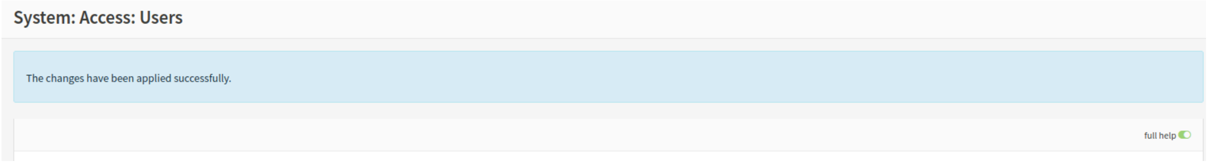


Defined by	USER
Disabled	□
Username	alex
Password	 (confirmation) □ Generate a scrambled password to prevent local database logins for this user.
Full name	Aleksandros User's full name, for your own information only
E-Mail	aleksandros@zenarmor.com User's e-mail address, for your own information only
Comment	User comment, for your own information only
Preferred landing page	Preferred landing page after login or authentication failure
Language	Default
Login shell	/sbin/nologin

OPNsense (c) 2014-2023 Deciso B.V.

Figure 3. *Adding users to OPNsense*

The user "alex" with the specified details is now created in OPNsense.



System: Access: Users

The changes have been applied successfully.

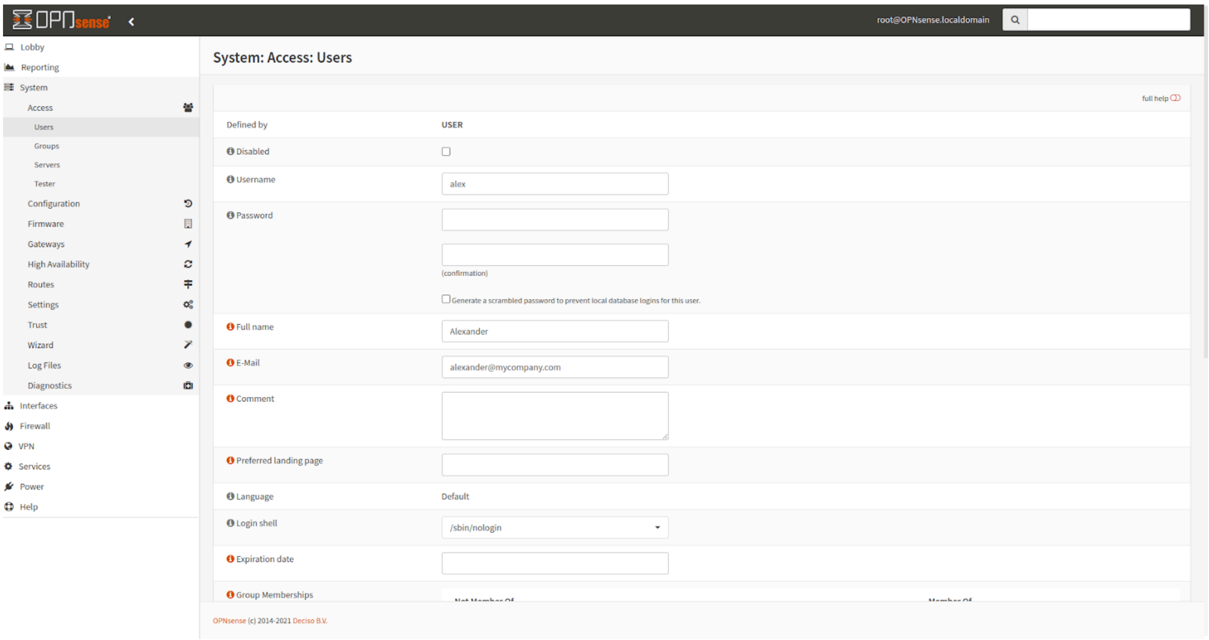
Figure 4. *New User is created*

2.3 Setting User Permissions

Assigning appropriate user groups in OPNsense is crucial for defining access rights and privileges. User groups allow administrators to apply common access settings to multiple users simultaneously, streamlining the management process. Here's how to set user permissions:

Create User Groups (if not already done): Before setting user permissions, create user groups in OPNsense that represent different levels of access or roles within the network. For example, you can have groups like "**Administrators**," "**Operators**," and "**Guests**," each with distinct privileges.

2.3.1 Creating User Groups



System: Access: Users

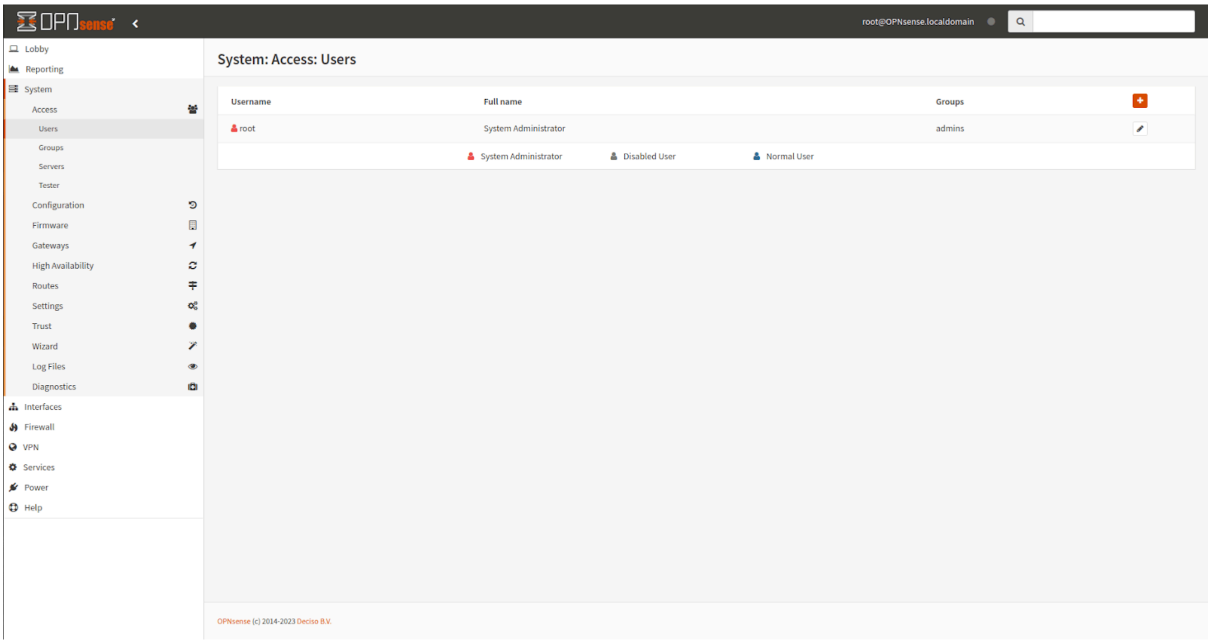
Defined by	USER
Disabled	□
Username	alex
Password	 (confirmation) □ Generate a scrambled password to prevent local database logins for this user.
Full name	Alexander
E-Mail	alexander@mycompany.com
Comment	
Preferred landing page	
Language	Default
Login shell	/sbin/nologin
Expiration date	
Group Memberships	Not Member Of / Member Of

OPNsense (c) 2014-2021 Deciso B.V.

Figure 15. *Creating User Groups on OPNsense*

Here's the step-by-step process to create a new group in OPNsense along with numbered steps and relevant screenshots. We have created a new group named "**Operators**".

1. Navigate to **System > Access > Groups**: Log in to the OPNsense web interface using your administrative credentials. From the main menu, go to "**System**," then select "**Access**," and finally choose "**Groups**".



System: Access: Users

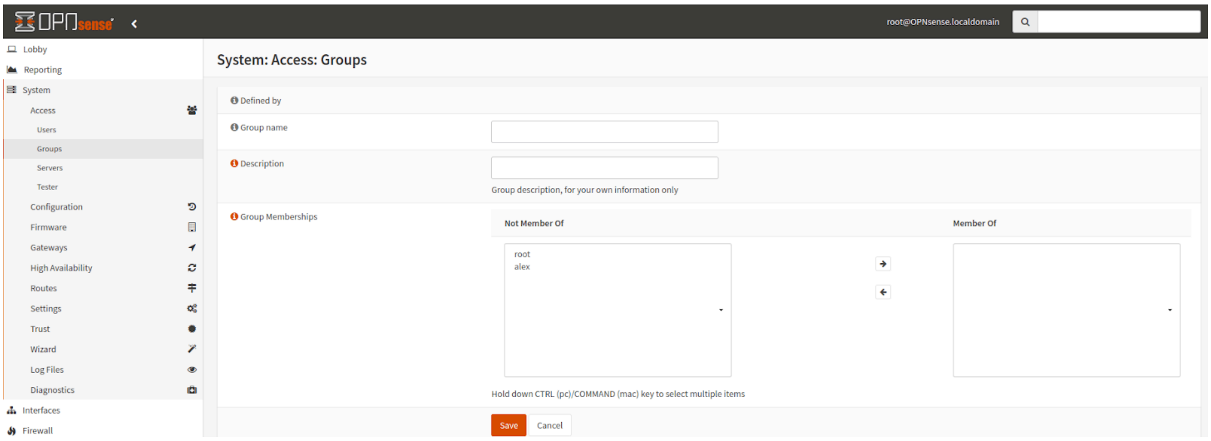
Username	Full name	Groups
root	System Administrator	admins

System Administrator   Disabled User   Normal User

OPNsense (c) 2014-2023 Deciso B.V.

Figure 5. *Adding a user to a group on OPNsense*

2. Click the **+** button to create a New Group: In the **Groups** section, look for the "**+**" button or "**Add**" option. This button allows you to initiate the process of creating a new group.



System: Access: Groups

Defined by

Group name

Description

Group description, for your own information only

Group Memberships

Not Member Of: root, alex

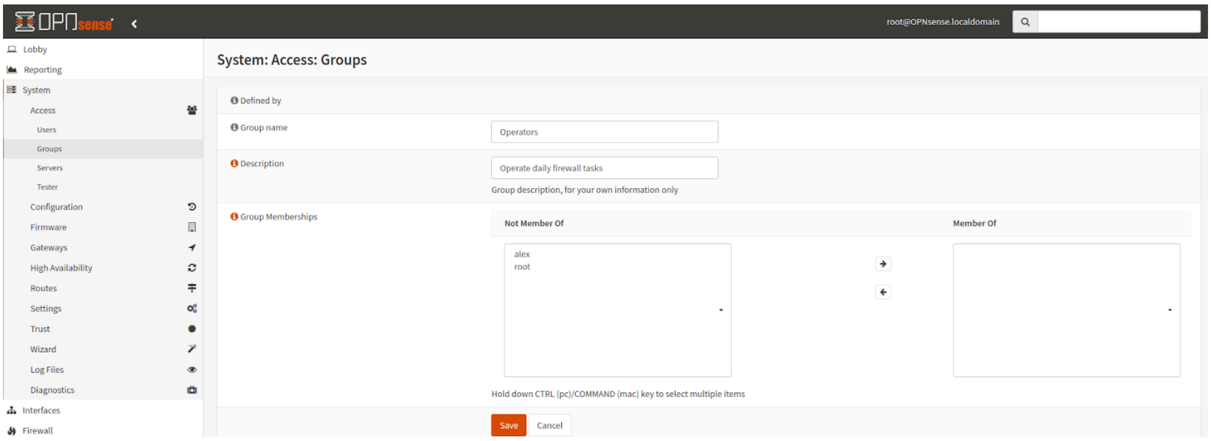
Member Of:

Hold down CTRL (pc)/COMMAND (mac) key to select multiple items

Figure 6. *Create a New Group on OPNsense*

3. **Enter Group Details**: A form will appear for you to enter details about the new group.
4. **Name**: Provide a name for the group, such as "**Operators**".

5. **Description**: Optionally, you can add a brief description of the group's purpose.



System: Access: Groups

Defined by

Group name: Operators

Description: Operate daily firewall tasks

Group description, for your own information only

Group Memberships

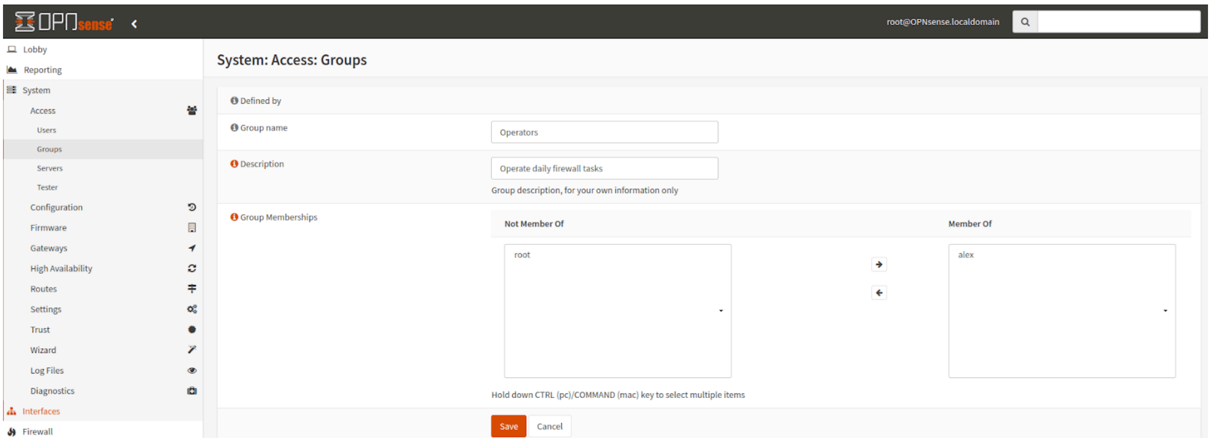
Not Member Of: alex, root

Member Of:

Hold down CTRL (pc)/COMMAND (mac) key to select multiple items

Figure 7. *Create a New Group on OPNsense*

6. **Select Users**: Look for an option to select users to add to the group. This could involve searching for users and checking boxes next to their names.



System: Access: Groups

Defined by

Group name: Operators

Description: Operate daily firewall tasks

Group description, for your own information only

Group Memberships

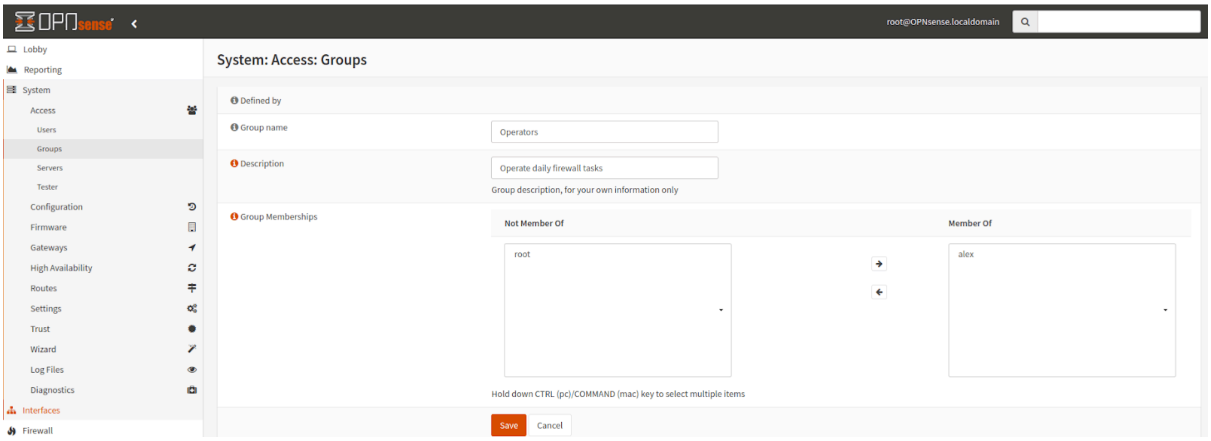
Not Member Of: root

Member Of: alex

Hold down CTRL (pc)/COMMAND (mac) key to select multiple items

Figure 8. *Select User for Group on OPNsense*

7. **Save the Group**: After selecting the users, locate the "**Save**" button or an equivalent option to finalize the group creation process.



System: Access: Groups

Defined by

Group name: Operators

Description: Operate daily firewall tasks

Group description, for your own information only

Group Memberships

Not Member Of: root

Member Of: alex

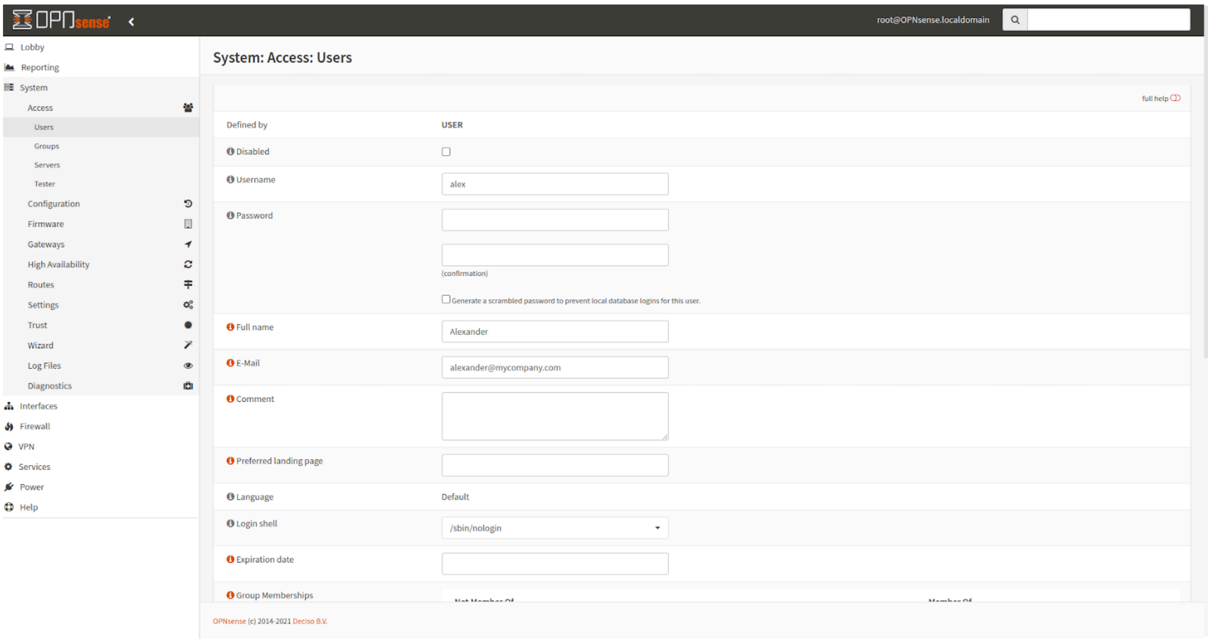
Hold down CTRL (pc)/COMMAND (mac) key to select multiple items

Figure 9. *Save the created group*

2.3.2 Assign Users to User Groups:

You can assign users to user groups to control their access and permissions. User groups can be configured to have specific privileges and restrictions. Here's how you can assign users to user groups in OPNsense:

1. **Access User Manager**: Log in to the OPNsense web interface using your administrative credentials. From the main menu, navigate to the "**User Manager**" section.
2. **Edit User Details**: Find and select the user account you want to assign to user groups. In this case, select the user "alex" that you created earlier. Click on the "**Edit**" option associated with the user.



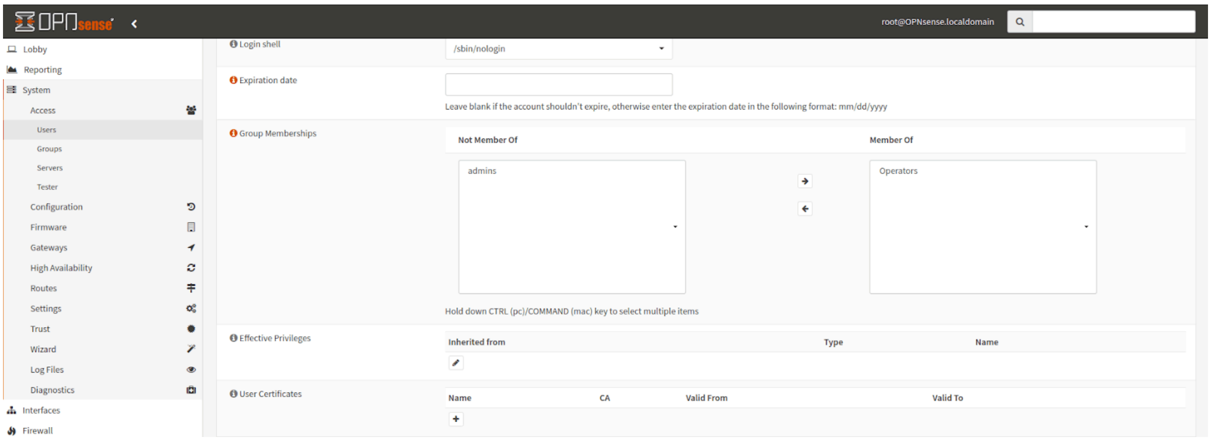
System: Access: Users

Defined by	USER
Disabled	□
Username	alex
Password	 (confirmation) □ Generate a scrambled password to prevent local database logins for this user.
Full name	Alexander
E-Mail	alexander@mycompany.com
Comment	
Preferred landing page	
Language	Default
Login shell	/sbin/nologin
Expiration date	
Group Memberships	Not Member Of / Member Of

OPNsense (c) 2014-2021 Deciso B.V.

Figure 10. *Edit User Details*

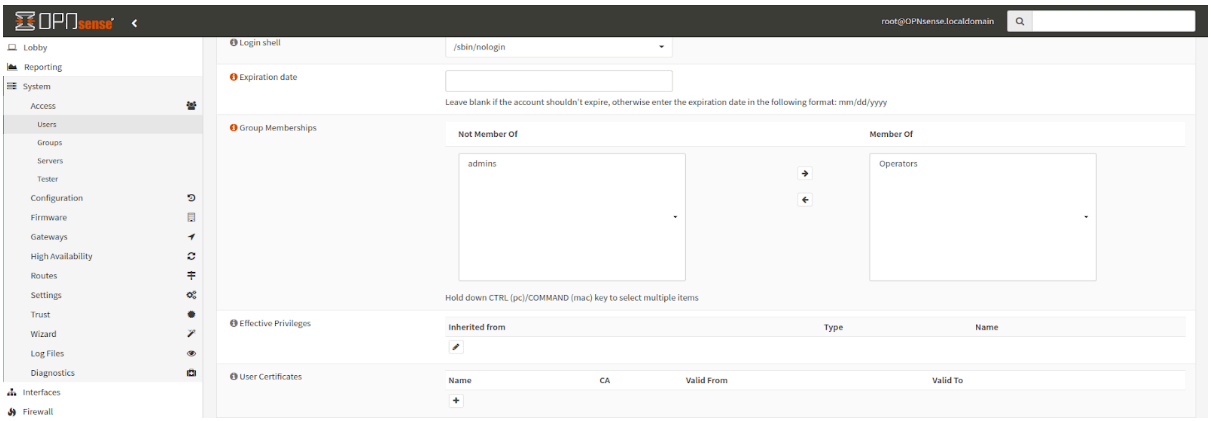
3. **Group Memberships**: In the user's editing page, locate the "**Group Memberships**" section. This is where you'll manage the user's group affiliations.



Login shell	/sbin/nologin
Expiration date	 Leave blank if the account shouldn't expire, otherwise enter the expiration date in the following format: mm/dd/yyyy
Group Memberships	Not Member Of: admins Member Of: Operators Hold down CTRL (pc)/COMMAND (mac) key to select multiple items
Effective Privileges	Inherited from / Type / Name
User Certificates	Name / CA / Valid From / Valid To

Figure 11. *Group Membership*

4. **Select User Groups**: In the "**Group Memberships**" section, you will see a list of available user groups. Check the boxes next to the appropriate user groups you want to assign to "alex." If you need to assign the user to multiple groups, hold down the **CTRL** key (PC) or **COMMAND** key (Mac) while clicking to select multiple groups.We have changed the group membership of alex user from operators to admins.



Login shell: /sbin/nologin

Expiration date:

Leave blank if the account shouldn't expire, otherwise enter the expiration date in the following format: mm/dd/yyyy

Group Memberships

Not Member Of	Member Of
admins	Operators

Hold down CTRL (pc)/COMMAND (mac) key to select multiple items

Effective Privileges

Inherited from	Type	Name

User Certificates

Name	CA	Valid From	Valid To

Figure 12. *Select Group*

Note that you can also use centralized authentication servers such as Radius or LDAP for user authentication on OPNsense

2.4 Enabling Two-Factor Authentication (Optional)

In the ever-evolving landscape of cybersecurity, ensuring the protection of sensitive data and network resources has become paramount. Two-factor authentication (2FA) emerges as a critical solution to fortify digital security. By requiring an additional layer of verification beyond the conventional password, 2FA safeguards against unauthorized access and potential breaches. For an in-depth exploration of the steps involved in enabling 2FA, you can refer to our previously authored article on the topic.

Using Google Authenticator, OPNsense provides full support for two-factor authentication (2FA) across the entire system. The following OPNsense services have 2FA support:

- Virtual Private Networking (OpenVPN & IPsec)
- Caching Proxy
- OPNsense Graphical User Interface
- Captive Portal

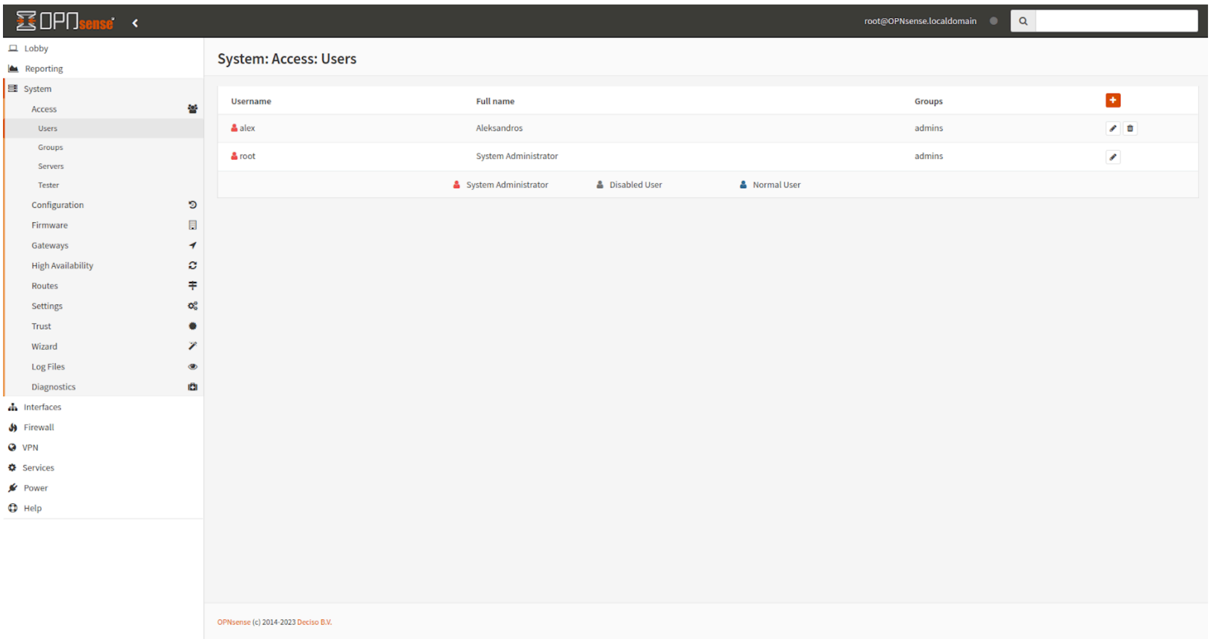
You may easily enable 2FA with Google Authenticator or FreeOTP for GUI and captive portal access in an OPNsense firewall.

2.5 Managing Existing Users

OPNsense provides an easy-to-use User Manager interface that allows administrators to edit or delete existing user accounts based on specific requirements. Follow the steps below to manage existing users:

Managing existing users in OPNsense involves several tasks, such as editing user details, changing passwords, modifying group assignments, and deleting users. Here's how you can manage existing users in OPNsense:

1. Go to **System > Access > Users.**



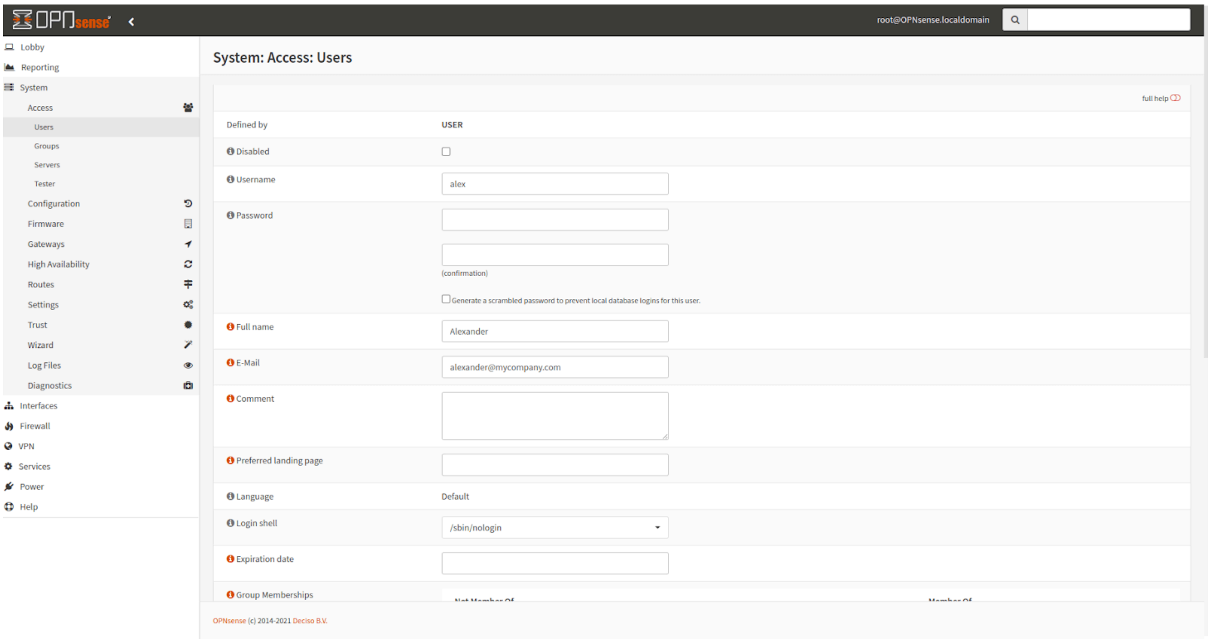
System: Access: Users

Username	Full name	Groups
alex	Aleksandros	admins
root	System Administrator	admins

System Administrator   Disabled User   Normal User

Figure 13. *Edit existing users on OPNsense*

2. Select the **user** that you want to edit or delete.
3. If you want to edit the user, click the **Edit** button.



System: Access: Users

Defined by	USER
Disabled	□
Username	alex
Password	 (confirmation) □ Generate a scrambled password to prevent local database logins for this user.
Full name	Alexander
E-Mail	alexander@mycompany.com
Comment	
Preferred landing page	
Language	Default
Login shell	/sbin/nologin
Expiration date	
Group Memberships	Not Member Of / Member Of

Figure 14. *Edit existing users on OPNsense*

4. In the **Edit** User dialog box, you can make changes to the user's name, password, email address, and privileges.
5. Click the **Save** button to save your changes.
6. If you want to delete the user, click the **Delete** button.
7. In the confirmation dialog box, click the **Delete** button to confirm.

Here are some additional details about editing and deleting existing users on OPNsense:

- When editing a user, you can change the user's name, password, email address, and privileges. You can also change the user's group membership.
- When deleting a user, all of the user's data will be deleted, including the user's configuration files, firewall rules, and VPN settings.
- If you delete a user who is a member of a group, the user will be removed from the group.
- While it is possible to add, edit, or delete users in the **User Manager** section of the web interface, it is not possible to delete the default user "**root**".

3. Authorization

Authorization refers to the process of granting or denying access to specific resources or actions based on a user's privileges and permissions. In the context of OPNsense, authorization plays a crucial role in controlling and managing user access to various features, services, and configurations within the firewall.

The primary purpose of authorization on OPNsense is to enforce security and access control policies. By implementing authorization mechanisms, you can ensure that only authorized users have the appropriate level of access to different parts of the firewall's interface and functionalities. This helps prevent unauthorized individuals from making unintended or potentially harmful changes to your network settings and configurations.

Having explored the significance of authorization within the OPNsense firewall ecosystem, it's imperative to recognize that the implementation of robust authorization mechanisms is inherently intertwined with effective user management. This is where **LDAP (Lightweight Directory Access Protocol)** integration steps onto the stage as a powerful tool. By seamlessly connecting OPNsense to an **LDAP directory** or an **Active Directory** (AD) server, you can not only streamline user authentication but also extend the realms of authorization across your network infrastructure.

3.1 LDAP/Active Directory Integration (Optional)

LDAP/Active Directory Integration on OPNsense allows you to streamline user authentication and access control by integrating your firewall with an LDAP or Active Directory server. This integration simplifies user management and enhances security through centralized authentication and authorization mechanisms.

By connecting OPNsense to your LDAP/Active Directory server, you can achieve the following benefits:

- **Centralized User Management**: Sync user accounts and credentials from your LDAP/Active Directory server to OPNsense, eliminating the need to manage user accounts separately on the firewall.
- **Single Sign-On** (SSO): Users can log in to OPNsense using their LDAP/Active Directory credentials, promoting a seamless user experience without requiring separate authentication.

- **Enhanced Security**: Leverage the security measures implemented on your LDAP/Active Directory server, ensuring consistent and robust authentication practices.
- **Access Control and Permissions**: Assign specific user groups and permissions based on your LDAP/Active Directory structure, enabling fine-grained control over who can access which resources on the firewall.
- **Reduced Administrative Overhead**: Changes in user accounts or passwords are reflected automatically, reducing the manual effort required for user management.

To implement LDAP Integration on OPNsense, follow the steps outlined in the official documentation or refer to our comprehensive guide. By successfully integrating LDAP/Active Directory with OPNsense, you'll enhance security, streamline user management, and establish a more efficient network infrastructure.

3.2 Setting Up Captive Portal (Optional)

The captive portal is a network security solution that automates the control and management of user access to public and private networks. Captive portals are commonly used for guest access management in open access networks, which are found in hotels, hospitals, airports, restaurants, and corporate networks. When the captive portal is enabled, access to the Internet is restricted unless the user provides personal information such as e-mail, name, and Social Security number, or authentication via a voucher via a web-based registration form completed in a web browser.

A captive portal in OPNsense is a powerful feature that enables network administrators to manage guest access and control user authentication on their network. It serves as an authentication gateway, typically used in public Wi-Fi networks or other controlled environments. With a captive portal, users connecting to the network are redirected to a login page where they need to provide credentials or agree to terms of use before gaining access to the internet or specific network resources. This feature allows administrators to ensure network security, track user activity, and implement access controls effectively.

In addition to its captive portal functionality, OPNsense offers user-based filtering, which enhances network security and control. User-based filtering allows administrators to implement specific Internet access policies based on individual user accounts. This feature enables network administrators to tailor internet access rights, content filtering, and bandwidth allocation according to different users or user groups.

3.3 Enabling Local Certificate Authority (Optional)

Enhance the security of your network infrastructure by setting up a **Local Certificate Authority** (CA) on OPNsense. In this guide, we'll delve into the process of enabling this crucial feature, ensuring robust encryption and authentication for your network communications.

Here are the step-by-step instructions to enable **Local Certificate Authority** on OPNsense:

1. **Log in to the OPNsense Web UI**: Use your credentials to access the OPNsense web interface.
2. **Navigate to Trust Authorities**: From the left-hand menu, go to System > Trust > Authorities.
3. **Create a Root Certificate**: Click the "+" (plus) sign located in the upper right corner to initiate the root certificate creation process.
4. **Fill Out the Form**:

Method: Choose "**Create an internal Certificate Authority**".

What are the other methods?

Let's touch a little bit here.

1. **Create an Internal Certificate**: This option allows you to establish your own private Certificate Authority (CA) within your network.
2. **Import an Existing Certificate**: With this option, you can import a pre-existing certificate from an external source.
3. **Create a Certificate Signing Request**: This option generates a **Certificate Signing Request (CSR)** that you can provide to a trusted external **Certificate Authority**.
4. **Sign a Certificate Signing Request**: This allows you to take on the role of a CA and sign a certificate with your internal CA's private key.

Descriptive Name: Enter a name that will help you identify the certificate (e.g., "Local CA").

Certificate Authority:

- If no internal Certificate Authorities have been defined, you need to add one before creating an internal certificate.

Type: **Client Certificate**

- Choose the type of certificate you want to generate. The type defines constraints on its usage.

In OPNsense, the following types of certificates can be generated:

1. **Client Certificate**: A certificate used to authenticate a client to a server. It is used to verify the identity of the client and establish a secure connection.
2. **Server Certificate**: A certificate used to authenticate a server to a client. It is used to verify the identity of the server and establish a secure connection.
3. **Combined Client/Server Certificate**: A certificate that can be used for both client and server authentication. It is used to verify the identity of both the client and server and establish a secure connection.
4. **Certificate Authority**: A certificate used to sign other certificates and establish a trust relationship between the certificate holder and the entities that rely on the certificate

Key Type: RSA

- Select **RSA** (Rivest-Shamir-Adleman) as the key type.
- **RSA**: RSA is a widely used asymmetric encryption algorithm. It is based on the mathematical properties of prime numbers and the difficulty of factoring large numbers. In the context of certificates, RSA is used for generating key pairs, where the private key is kept secret and the public key is used for encryption and verifying digital signatures.
- **Elliptic Curve**: **Elliptic Curve Cryptography (ECC)** is another type of asymmetric encryption algorithm that is based on the mathematics of elliptic curves. ECC offers the same level of security as RSA but with smaller key sizes, making it more efficient in terms of computation and storage requirements. It is commonly used in modern cryptographic protocols and systems.

Key Length (bits): 2048

- Choose the key length. In this case, select 2048 bits.

Digest Algorithm: SHA256

- Select the **digest algorithm**. It's recommended to use a stronger algorithm than SHA1 whenever possible.

Lifetime (days): 364

- Specify the lifetime of the certificate in days.

Private Key Location: Save on this firewall

- Select "**Save on this firewall**" to save the private key on the current firewall.
- If the certificate is for use on another device and you intend to download the private key later, you can choose the "**Download and do not save**" option.

Distinguished Name Fields

In the context of certificate creation, the "**Distinguished Name**" (DN) refers to a set of fields that provide information about the identity of the entity for which the certificate is issued. These fields are part of the X.509 standard for defining the format of public key certificates.

Here are the common DN fields and their explanations:

- **Country Code**: Enter the country code (e.g., AD for Andorra).
- **State or Province**: Enter the state or province (e.g., Sachsen).
- **City**: Enter the city (e.g., Leipzig).
- **Organization**: Enter the organization name (e.g., My Company Inc).
- **Email Address**: Enter the email address (e.g., admin@mycompany.com).
- **Common Name**: Enter the common name (e.g., internal-ca).

Alternative Names:

"**Alternative Names**" (also known as **Subject Alternative Names** or **SANs**) extension in a certificate allows you to specify additional identifiers for the entity associated with the certificate. These alternative names can include various types of identifiers, such as:

1. **DNS Names**: These are domain names or **fully qualified domain names (FQDNs)** that the certificate should be valid for. For example, you can include multiple subdomains like "www.example.com," "**mail.example.com**", and so on.
2. **IP Addresses**: You can specify one or more IP addresses (IPv4 or IPv6) for which the certificate is valid. This is especially useful in scenarios where the certificate needs to cover multiple IP addresses associated with a server.

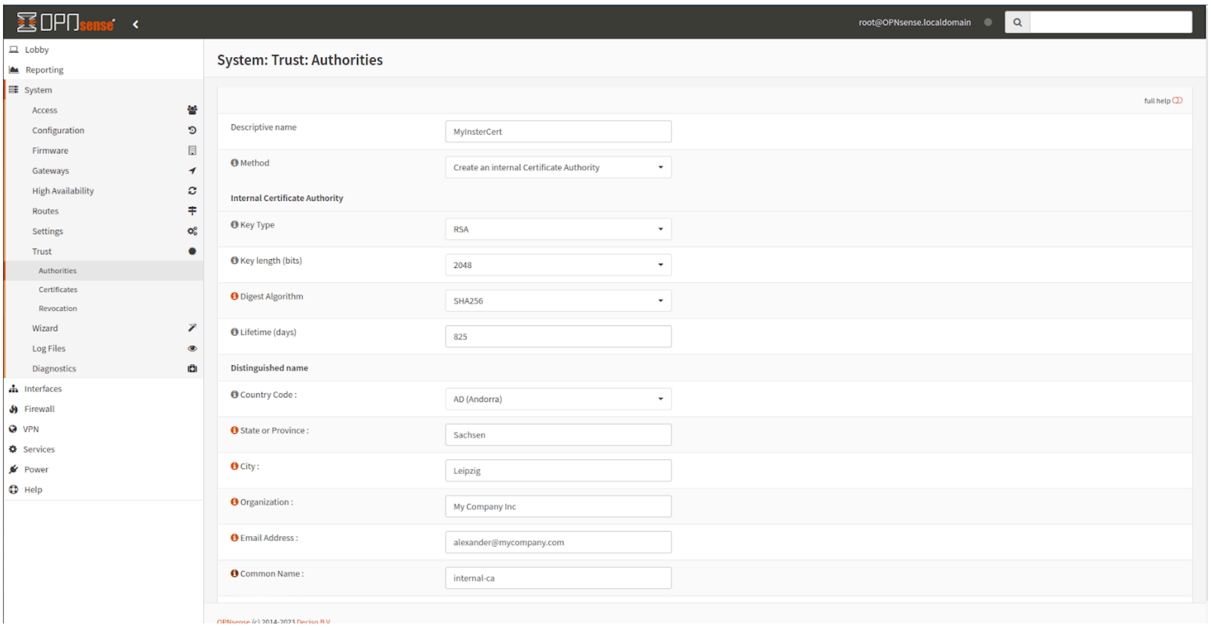
3. **Email Addresses**: If the certificate is used for email encryption or authentication, you can include email addresses as alternative names. This allows the certificate to be used for securing email communications.
4. **Uniform Resource Identifiers (URIs)**: URIs, such as web URLs, can be included as alternative names. This is relevant when the certificate is used for web services or applications that have specific URI requirements.

- If needed, you can add alternative names (e.g., DNS entries) for the certificate.

Including alternative names in a certificate is valuable because it allows a single certificate to be valid for multiple purposes or multiple domains. For example, a server certificate for a web server can include alternative names for different subdomains, ensuring that the same certificate can be used for various services hosted on different subdomains of a domain.

When configuring a certificate with alternative names, it's essential to ensure that all the specified names are accurate and relevant to the certificate's intended use. This flexibility simplifies certificate management for multi-domain environments and services that require multiple identifiers to function securely.

Once you've filled out all the necessary fields, review your selections and click "**Save**" to generate the certificate. This certificate can be used for various purposes, including client authentication and secure communications within your network environment.

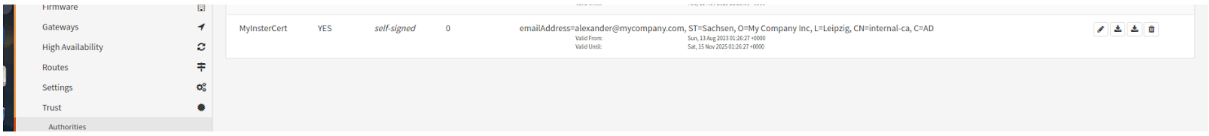


System: Trust: Authorities

Descriptive name	MyInsterCert
Method	Create an internal Certificate Authority
Internal Certificate Authority	
Key Type	RSA
Key length (bits)	2048
Digest Algorithm	SHA256
Lifetime (days)	825
Distinguished name	
Country Code :	AD (Andorra)
State or Province :	Sachsen
City :	Leipzig
Organization :	My Company Inc
Email Address :	alexander@mycompany.com
Common Name :	internal-ca

OPNsense (c) 2014-2023 Deciso B.V.

Figure 16. *Enabling Local Certificate Authority on OPNsense*



MyInsterCert YES *self-signed* 0 emailAddress=alexander@mycompany.com, ST=Sachsen, O=My Company Inc, L=Leipzig, CN=internal-ca, C=AD
Valid From: Sun, 13 Aug 2023 01:26:27 +0000
Valid Until: Sat, 15 Nov 2025 01:26:27 +0000

Figure 17. *Added Local Certificate Authority on OPNsense*

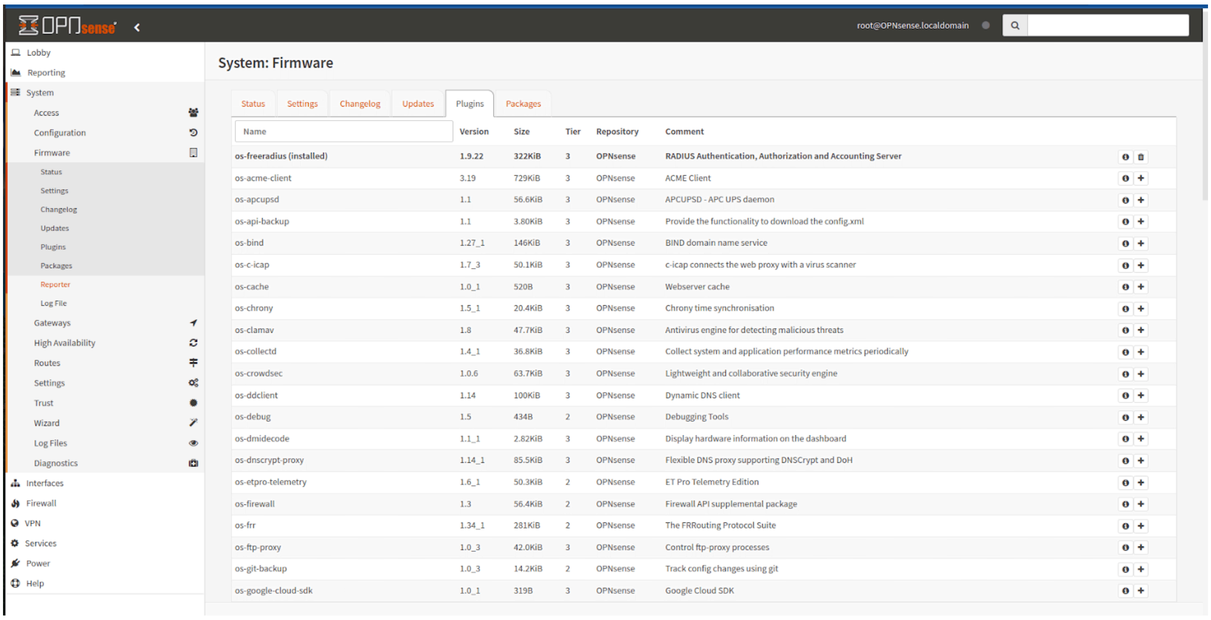
3.4 Configuring Authentication Servers (Radius)

Setting up authentication servers like **RADIUS** on OPNsense is an essential process to enhance security and manage user access efficiently. By configuring RADIUS authentication, administrators can centralize user authentication and provide an extra layer of protection. Let's walk through the step-by-step process of configuring RADIUS authentication to ensure a smooth and secure network environment.

Step 1: Install the FreeRADIUS Plugin (if not already installed)

The purpose of installing the FreeRADIUS plugin on OPNsense is to establish a robust framework for user authentication and access control. By centralizing authentication processes through **FreeRADIUS**, you can ensure that users' identities are verified before granting them access to network resources.

1. Log in to your OPNsense web interface.
2. Navigate to **"System" > "Firmware" > "Plugins"**.
3. Search for "**FreeRADIUS**" and install the plugin.



System: Firmware

Name	Version	Size	Tier	Repository	Comment
os-freeradius (installed)	**1.9.22**	**322KiB**	**3**	**OPNsense**	**RADIUS Authentication, Authorization and Accounting Server**
os-acme-client	3.19	729KiB	3	OPNsense	ACME Client
os-apcupsd	1.1	56.6KiB	3	OPNsense	APCUPSD - APC UPS daemon
os-api-backup	1.1	3.80KiB	3	OPNsense	Provide the functionality to download the config.xml
os-bind	1.27_1	146KiB	3	OPNsense	BIND domain name service
os-c-icap	1.7_3	50.1KiB	3	OPNsense	c-icap connects the web proxy with a virus scanner
os-cache	1.0_1	520B	3	OPNsense	Webserver cache
os-chrony	1.5_1	20.4KiB	3	OPNsense	Chrony time synchronisation
os-clamav	1.8	47.7KiB	3	OPNsense	Antivirus engine for detecting malicious threats
os-collectd	1.4_1	36.8KiB	3	OPNsense	Collect system and application performance metrics periodically
os-crowdsec	1.0.6	63.7KiB	3	OPNsense	Lightweight and collaborative security engine
os-ddclient	1.14	100KiB	3	OPNsense	Dynamic DNS client
os-debug	1.5	434B	2	OPNsense	Debugging Tools
os-dmidecode	1.1_1	2.82KiB	3	OPNsense	Display hardware information on the dashboard
os-dnscrypt-proxy	1.14_1	85.5KiB	3	OPNsense	Flexible DNS proxy supporting DNSCrypt and DoH
os-etpro-telemetry	1.6_1	50.3KiB	2	OPNsense	ET Pro Telemetry Edition
os-firewall	1.3	56.4KiB	2	OPNsense	Firewall API supplemental package
os-frr	1.34_1	281KiB	2	OPNsense	The FRRouting Protocol Suite
os-ftp-proxy	1.0_3	42.0KiB	3	OPNsense	Control ftp-proxy processes
os-git-backup	1.0_3	14.2KiB	2	OPNsense	Track config changes using git
os-google-cloud-sdk	1.0_1	319B	3	OPNsense	Google Cloud SDK

Figure 18. *Install the FreeRADIUS Plugin*

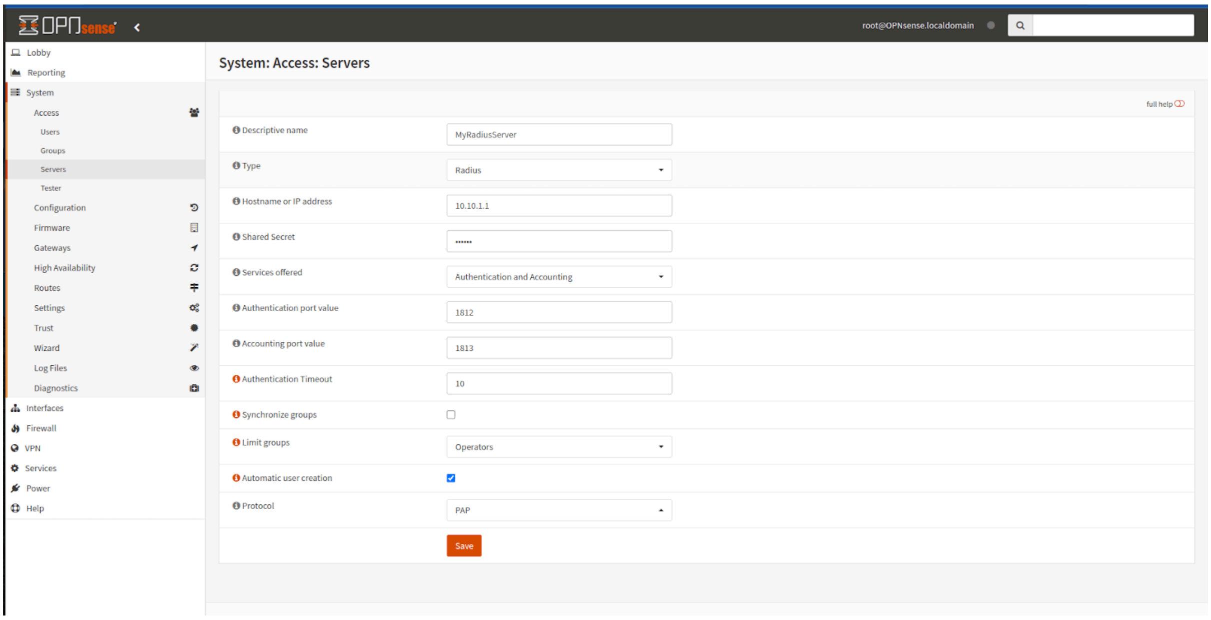
Step 2: Configure RADIUS Server

By configuring the RADIUS server, you enable a centralized authentication mechanism that bolsters network protection and simplifies user management.

Now, let's delve into the steps to configure the RADIUS server on your OPNsense firewall.

1. After installing the **FreeRADIUS** plugin, navigate to "**Services**" > "**FreeRADIUS**".
2. Click on the "**Servers**" tab.
3. Click the "**+**" button to add a new RADIUS server.

- **Server name**: Give your server a descriptive name.
- **IP Address**: Enter the IP address of your RADIUS server.
- **Shared Secret**: Enter a shared secret that will be used to secure communications between OPNsense and the RADIUS server.
- **Authentication Port**: Typically set to **1812**.
- **Accounting Port**: Typically set to **1813**.
- **Timeout**: Set a reasonable timeout value.
- **Retries**: Set the number of retries for requests.
- **Description**: Provide a brief description of the server configuration.
- **Synchronize groups**: Enable to synchronize groups, requires the option above.
- **Limit groups**: Select a list of groups that may be considered during sync 1.
- **Automatic user creation**: When groups are automatically synchronized, this offers the ability to automatically create the user when it doesn't exist

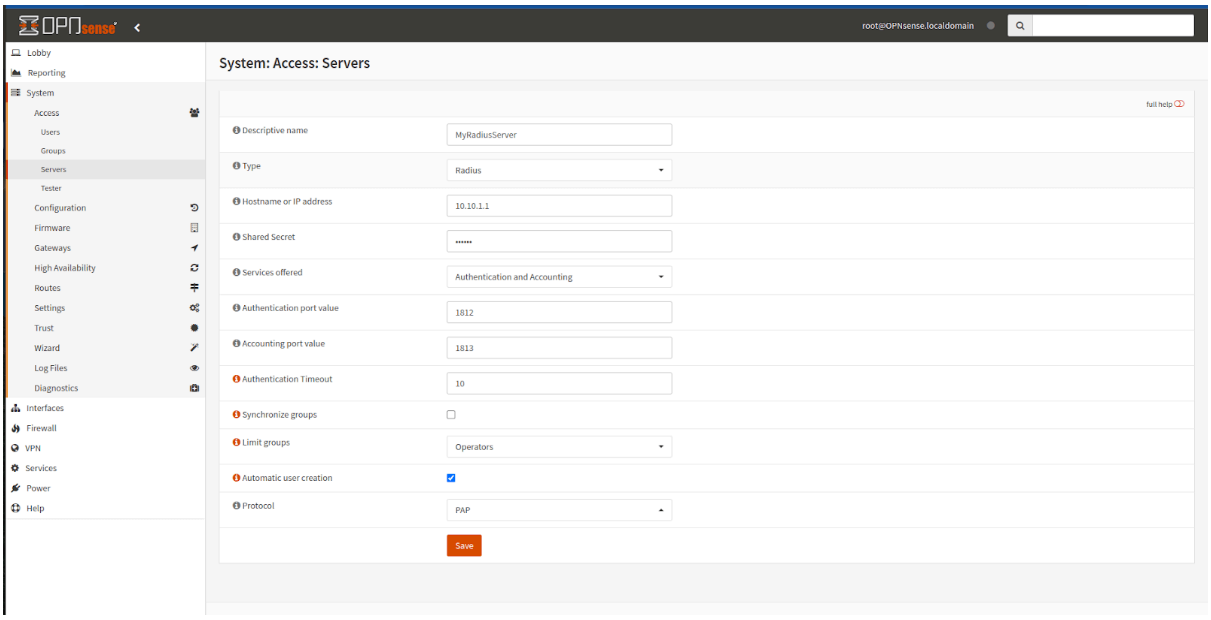


System: Access: Servers

Descriptive name	MyRadiusServer
Type	Radius
Hostname or IP address	10.10.1.1
Shared Secret	••••••
Services offered	Authentication and Accounting
Authentication port value	1812
Accounting port value	1813
Authentication Timeout	10
Synchronize groups	□
Limit groups	Operators
Automatic user creation	☑
Protocol	PAP

Figure 19. *Configure RADIUS Server*

4. Click "**Save**" to save the RADIUS server configuration.



System: Access: Servers

Descriptive name	MyRadiusServer
Type	Radius
Hostname or IP address	10.10.1.1
Shared Secret	••••••
Services offered	Authentication and Accounting
Authentication port value	1812
Accounting port value	1813
Authentication Timeout	10
Synchronize groups	□
Limit groups	Operators
Automatic user creation	☑
Protocol	PAP

Save

Figure 20. *Setting up authentication servers (RADIUS) in OPNsense*

Step 3: Configure FreeRADIUS Client

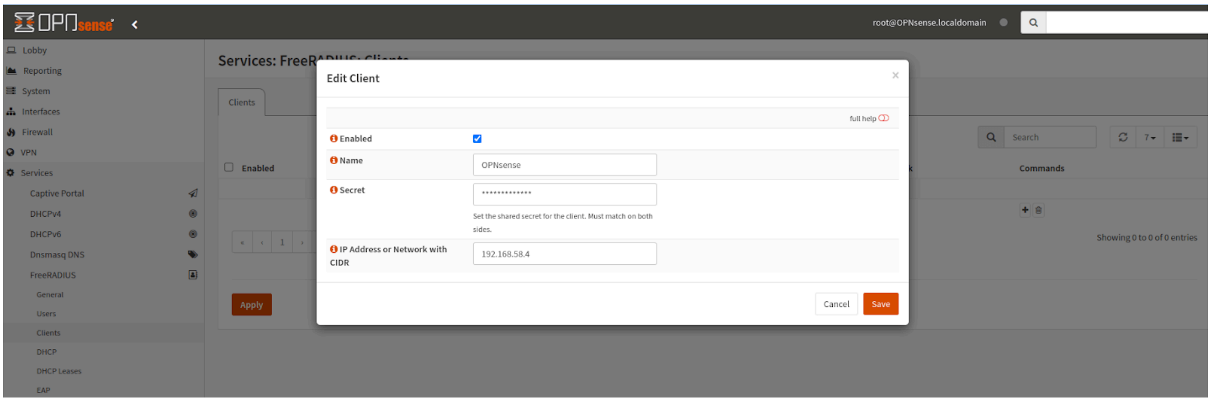
By configuring the **FreeRADIUS** client on your OPNsense firewall, you establish the necessary connection between the firewall and the RADIUS server, paving the way for centralized authentication and enhanced network security.

Follow the steps below to configure the **FreeRADIUS** client:

1. Still in the **FreeRADIUS** plugin section, click on the "**Clients**" tab.
2. Click the "**+**" button to add a new client.

- **Client name**: Give it a name (e.g., OPNsense).
- **IP Address**: Enter the IP address of the OPNsense firewall.
- **Shared Secret**: Use the same secure shared secret you configured for the local server.

3. Click "**Save**" to save the client configuration.



Edit Client

full help

Enabled ☑

Name: OPNsense

Secret: ••••••••••••••

Set the shared secret for the client. Must match on both sides.

IP Address or Network with CIDR: 192.168.58.4

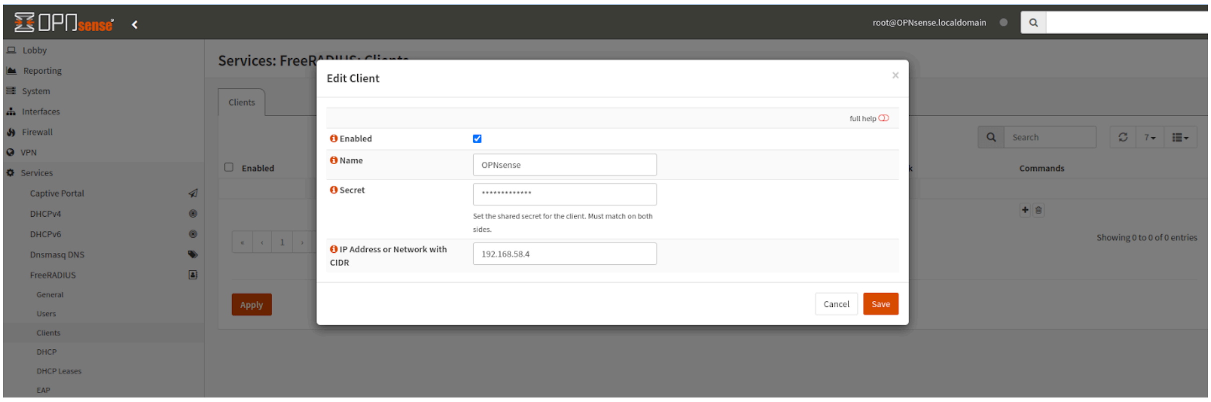
Cancel Save

Figure 21. *Configure FreeRADIUS Client*

Step 4: Configure Authentication Sources

By defining authentication sources, you determine where the firewall should look to verify user credentials. This flexibility allows you to integrate various authentication methods and services, including local user databases, external LDAP or Active Directory servers, and more. Follow the steps below to configure authentication sources on OPNsense:

1. Navigate to "**System**" > "**Access**" > "**Settings> Administration**" tab.
   iii. Under "**Authentication Servers,**" you can now select the local RADIUS server you configured from the drop-down list.
   iv. Click **Save** button to activate the settings.



Edit Client

full help

Enabled ☑

Name: OPNsense

Secret: ••••••••••••••

Set the shared secret for the client. Must match on both sides.

IP Address or Network with CIDR: 192.168.58.4

Cancel Save

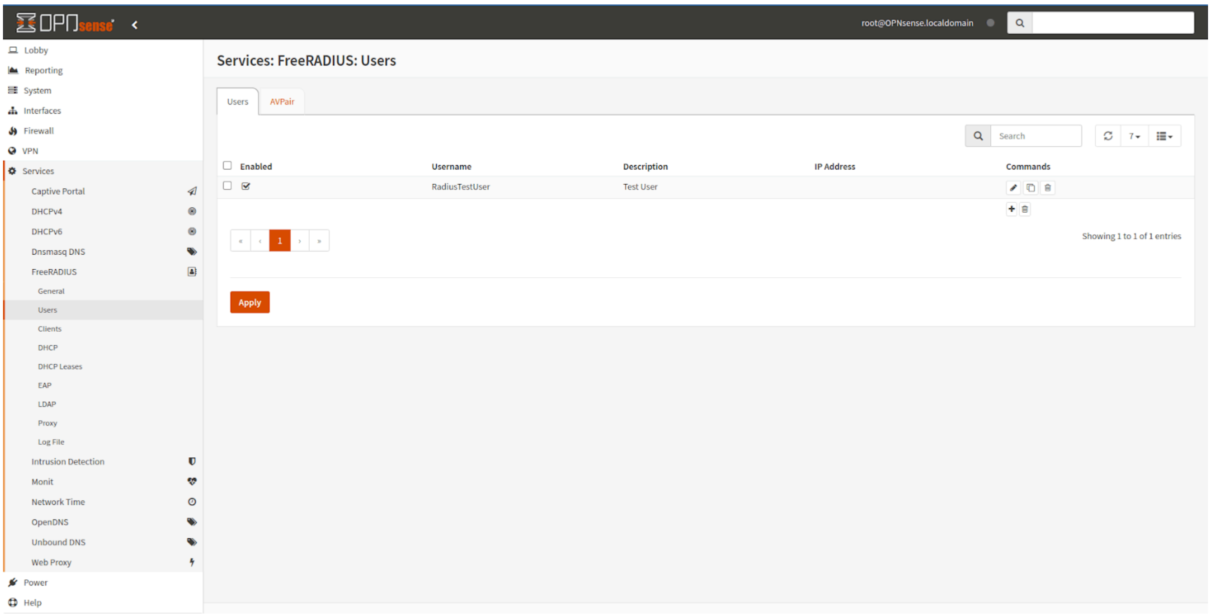
Figure 22. *Configure Authentication Sources*

Step 5: Test RADIUS Authentication

Test the setup by attempting to log in using a user that you've configured in the **FreeRADIUS Users** section. OPNsense should send authentication requests to the FreeRADIUS server running locally.

Remember, always refer to the official documentation and guidelines for your specific OPNsense version to ensure accuracy in configuration.

Here are the steps to test **RADIUS Authentication**



Services: FreeRADIUS: Users

□ Enabled	Username	Description	IP Address	Commands
□ ☑	RadiusTestUser	Test User		

Showing 1 to 1 of 1 entries

Figure 23. *Create a Test User in FreeRADIUS*

- Create a **Test User** in **FreeRADIUS** (if not done already):

Creating a test user in **FreeRADIUS** on your OPNsense firewall allows you to verify the functionality of the RADIUS server and test user authentication. Follow these steps to create a test user:

In the **FreeRADIUS** plugin section of OPNsense, navigate to the "Users" tab and create a test user with a username and password.

- **Attempt to Log In**: Using a device that's on the network where OPNsense is being used, follow these steps:
- Enter the **username** and **password** of the test user you created in the **FreeRADIUS Users** section.
- Click the "**Login**" button.
- **Observe the Result**: If the authentication is successful, you will be logged in to the OPNsense interface. If the authentication fails, you'll likely see an error message indicating that the login credentials are incorrect.

- **Check the RADIUS Logs (Optional)**: If you encounter any issues, you might want to check the RADIUS server logs to gather more information. In the FreeRADIUS plugin section of OPNsense, you can find a link to the FreeRADIUS logs. Look for any authentication-related entries to diagnose the problem.

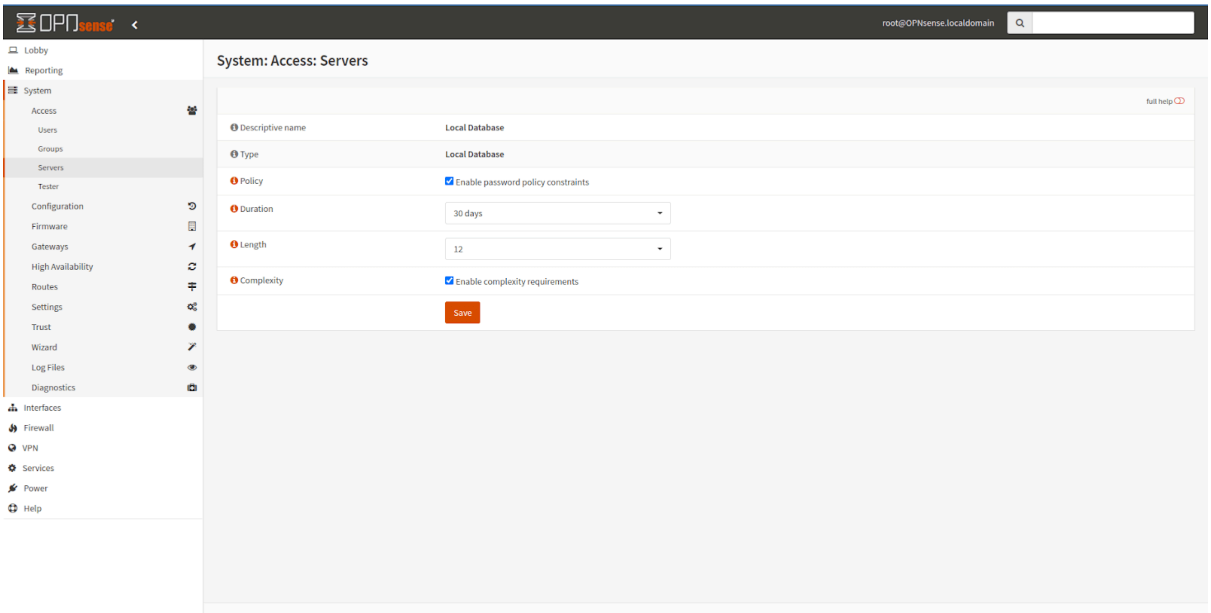
Troubleshooting:

If you're unable to log in successfully, you may follow the next troubleshooting steps and double-check the following configuration double-check the following:

- The RADIUS server IP, shared secret, and ports are correctly configured in both the RADIUS server settings and the OPNsense authentication server settings.
- The test user's credentials are correctly entered.
- The RADIUS server's firewall is not blocking incoming authentication requests from OPNsense.

3.5 Password Policy (Optional)

A well-defined password policy holds critical importance in maintaining the security and integrity of network resources. Strong password practices serve as the first line of defense against unauthorized access and potential breaches. By implementing a well-crafted password management policy, administrators can prevent unauthorized users from compromising the system and gain better control over user access.



System: Access: Servers

Descriptive name	Local Database
Type	Local Database
Policy	☑ Enable password policy constraints
Duration	30 days
Length	12
Complexity	☑ Enable complexity requirements
	Save

Figure 24. *Password Policy on OPNsense*

To set a password policy on OPNsense, follow these steps:

1. Access the OPNsense web interface and log in as an administrator.
2. Go to **System > Access > Servers**.
3. Click on the '**Edit**' icon (a pencil) for '**Local Database**' under the '**Servers**' section.
4. In the '**Local Database**' settings, you can configure the password policy for local users.
5. Set the desired password policy options, such as **password complexity requirements**, **minimum password length**, and **password expiration**.
6. Save the changes.

How to Install Plugins on OPNsense

OPNsense is a new FreeBSD-based firewall and routing system. It started out as a fork of pfSense® CE. Its story officially began in January 2015 with the publication of the release announcement for the first OPNsense release, the 15.1, on the official website.

OPNsense has a web-based interface and is compatible with the x86-64 platform. It has load balancing, virtual private network, and traffic shaping capabilities, and more can be added via plugins.

More information about OPNsense can be found in the Best Open-Source Firewalls article written by Zenarmor (formerly known as Sunny Valley Networks).

In this guide, we'll cover the available plugins for OPNsense and how you can install them on your firewall to enhance its capabilities. Also, we'll outline the best OPNsense plugins for securing your network. Finally, there will be a list of items to keep in mind while utilizing plugins for secure management.

What are OPNsense Plugins?

OPNsense® includes many features in the base system. However, in some cases, additional software may be required, which is either provided only as a binary package (without user interface) or as a plugin. Plugins are software packages that can be installed directly through the user interface and frequently include setup options accessible to the end-user.

The OPNsense community is welcoming and helpful. One appealing aspect of the OPNSense community is the large number of community plugins that have been created in a relatively short time. At the time of writing, OPNsense had over 70 different community-contributed plugins. These plugins help you to extend the functionality of your OPNsense firewall.

While some of the plugins are maintained and supported by the OPNsense team, many are supported by the community. Due to the fact that OPNsense® is a community-driven project, the amount of support available on these plugins may vary. There are also some third-party plugins that are available under a paid license. Zenarmor and Deciso are two vendors of these third-party plugins. OPNsense plugins are always available to everyone via web GUI as soon as they are upstreamed. The project maintains the plugin repository. If plugins are not kept up to date by their maintainer, they are removed at some point.

The following advantages come with OPNsense plugin support:

- Allow both community and third-party developers to extend the firewall capabilities.
- The application's size can be reduced by not loading unused features.
- New features can be easily added
- Because of incompatible software licenses, such as commercial packages, separate the source code from the OPNsense itself which is open-source.

OPNsense plugins can perform the following functions:

- Add more server software and their corresponding graphical user interfaces (GUIs).
- Develop new authentication methods for use in other subsystems.
- Change the menu, access control lists, and overall look and feel (themes)
- Increase the number of work tasks assigned to the backend services.
- Customize the start, stop, and early scripts.
- Other types of devices and interfaces can be added to the firewall.
- Bring in additional packages that will be automatically updated.
- Additional themes for the web interface
- Persistent /boot/loader.conf changes

A list of plugins that are currently available is given below:

Plugin Category/ Plugin Name	Description
benchmarks/iperf	Connection speed tester
databases/redis	Redis DB
devel/debug	Debugging Tools
devel/grid_example	A sample framework application
devel/helloworld	A sample framework application
dns/bind	BIND domain name service
dns/dnscrypt-proxy	Flexible DNS proxy supporting DNSCrypt and DoH

dns/dyndns	Dynamic DNS Support
dns/rfc2136	RFC-2136 Support
emulators/qemu-guest-agent	QEMU Guest Agent for OPNsense
ftp/tftp	TFTP server
mail/postfix	SMTP mail relay
mail/rspamd	Protect your network from spam
misc/theme-cicada	The cicada theme - dark grey
misc/theme-rebellion	A suitably dark theme
misc/theme-tukan	The tukan theme - blue/white
misc/theme-vicuna	The vicuna theme - dark anthrazit
net/chrony	Chrony time synchronisation
net/firewall	Firewall API supplemental package
net/freeradius	RADIUS Authentication, Authorization and Accounting Server
net/frr	The FRRouting Protocol Suite
net/ftp-proxy	Control ftp-proxy processes
net/google-cloud-sdk	Google Cloud SDK
net/haproxy	Reliable, high performance TCP/HTTP load balancer
net/igmp-proxy	IGMP-Proxy Service
net/mdns-repeater	Proxy multicast DNS between networks
net/ntopng	Traffic Analysis and Flow Collection
net/radsecproxy	RADIUS proxy provides both RADIUS UDP and TCP/TLS (RadSec) transport

net/realtek-re	Realtek re(4) vendor driver
net/relayd	Relayd Load Balancer
net/shadowsocks	Secure socks5 proxy
net/siproxd	Siproxd is a proxy daemon for the SIP protocol
net/sslh	sslh configuration front-end
net/tayga	Tayga NAT64
net/udpbroadcastrelay	Control ubpbroadcastrelay processes
net/upnp	Universal Plug and Play Service
net/vnstat	vnStat is a console-based network traffic monitor
net/wireguard	WireGuard VPN service kernel implementation
net/wireguard-go	WireGuard VPN service Go implementation (pending removal)
net/wol	Wake on LAN Service
net/zerotier	Virtual Networks That Just Work
net-mgmt/collectd	Collect system and application performance metrics periodically
net-mgmt/lldpd	LLDP allows you to know exactly on which port is a server
net-mgmt/net-snmp	Net-SNMP is a daemon for the SNMP protocol
net-mgmt/netdata	Real-time performance monitoring
net-mgmt/nrpe	Execute nagios plugins
net-mgmt/telegraf	Agent for collecting metrics and data
net-mgmt/zabbix-agent	Zabbix monitoring agent

net-mgmt/zabbix-proxy	Zabbix monitoring proxy
security/acme-client	ACME Client
security/clamav	Antivirus engine for detecting malicious threats
security/etpro-telemetry	ET Pro Telemetry Edition
security/intrusion-detection-content-et-open	IDS Proofpoint ET open ruleset complementary subset for ET Pro Telemetry edition
security/intrusion-detection-content-et-pro	IDS Proofpoint ET Pro ruleset (needs a valid subscription)
security/intrusion-detection-content-pt-open	IDS PT Research ruleset (only for non-commercial use)
security/intrusion-detection-content-snort-vrt	IDS Snort VRT ruleset (needs registration or subscription)
security/maltrail	Malicious traffic detection system
security/openconnect	OpenConnect Client
security/softether	Cross-platform Multi-protocol VPN Program (development only)
security/stunnel	Stunnel TLS proxy
security/tinc	Tinc VPN
security/tor	The Onion Router
security/wazuh-agent	Agent for the open source security platform Wazuh
sysutils/apcupsd	APCUPSD - APC UPS daemon
sysutils/api-backup	Provide the functionality to download the config.xml
sysutils/apuled	PC Engine APU LED control (development only)

sysutils/dmidecode	Display hardware information on the dashboard
sysutils/git-backup	Track config changes using git
sysutils/hw-probe	Collect hardware diagnostics
sysutils/lcdproc-sdeclcd	LCDProc for SDEC LCD devices
sysutils/mail-backup	Send configuration file backup by e-mail
sysutils/munin-node	Munin monitoring agent
sysutils/nextcloud-backup	Track config changes using NextCloud
sysutils/node_exporter	Prometheus exporter for machine metrics
sysutils/nut	Network UPS Tools
sysutils/puppet-agent	Manage Puppet Agent
sysutils/smart	SMART tools
sysutils/virtualbox	VirtualBox guest additions
sysutils/vmware	VMware tools
sysutils/xen	Xen guest utilities
vendor/sunnyvalley	Vendor repository for Sensei (Next Generation Firewall Extensions)
www/c-icap	c-icap connects the web proxy with a virus scanner
www/cache	Webserver cache
www/nginx	Nginx HTTP server and reverse proxy
www/web-proxy-sso	Kerberos authentication module

Table 1. *Currently available plugins on OPNsense*

Management of the Plugins on OPNsense

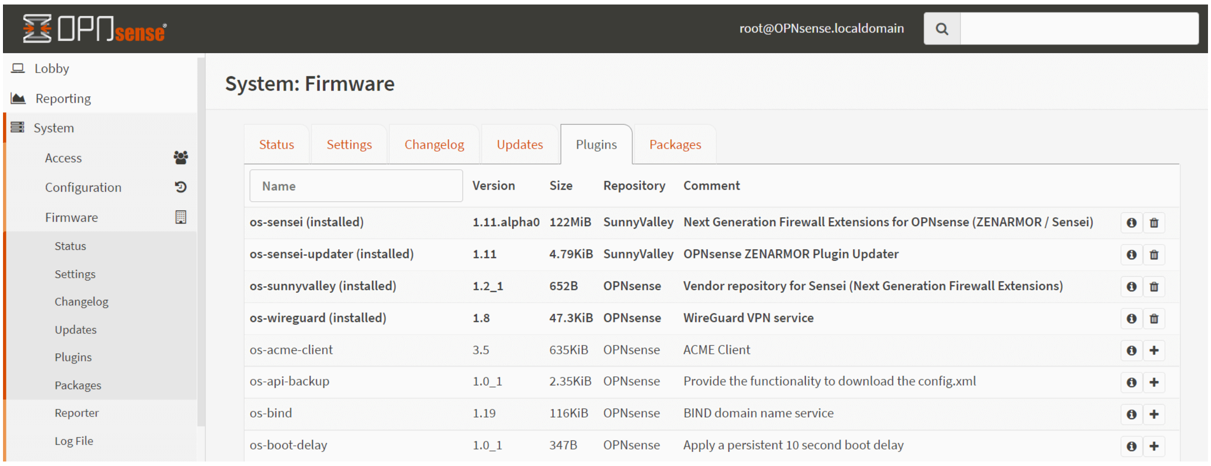
On OPNsense `Plugins` page you may perform the following tasks which will be explained below:

- Viewing available plugins
- Search for a plugin
- Viewing details of a plugin
- Install/Remove a plugin

Viewing Available Plugins

To view the available plugins on your OPNsense firewall, you may follow the steps below:

1. Click on the `System dropdown` menu on the OPNsense web UI.
2. Click on the `Firmware`.
3. Click on the `Plugins`.
4. You may scroll down to view all plugins.



Name	Version	Size	Repository	Comment
os-sensei (installed)	1.11.alpha0	122MiB	SunnyValley	Next Generation Firewall Extensions for OPNsense (ZENARMOR / Sensei)
os-sensei-updater (installed)	1.11	4.79KiB	SunnyValley	OPNsense ZENARMOR Plugin Updater
os-sunnyvalley (installed)	1.2_1	652B	OPNsense	Vendor repository for Sensei (Next Generation Firewall Extensions)
os-wireguard (installed)	1.8	47.3KiB	OPNsense	WireGuard VPN service
os-acme-client	3.5	635KiB	OPNsense	ACME Client
os-api-backup	1.0_1	2.35KiB	OPNsense	Provide the functionality to download the config.xml
os-bind	1.19	116KiB	OPNsense	BIND domain name service
os-boot-delay	1.0_1	347B	OPNsense	Apply a persistent 10 second boot delay

Figure 1. *Viewing plugins navigating to* `Systems> Firmware > Plugins` *on OPNsense UI.*

All available OPNsense plugins with the following details are displayed on `Plugins` page:

- **Name**: Name of the plugin, such as `os-sunnyvalley`.

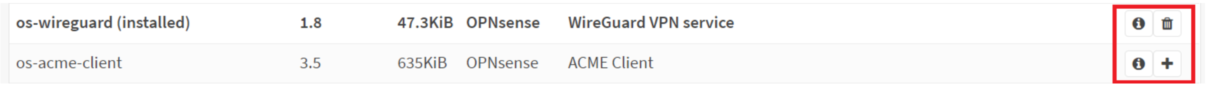
> 💡 **TIP**
>
> Installed plugins are captioned with **`(installed)`** at the end of the plugin name. They are also listed in bold font.

- **Version**: Release number of the plugin, such as **`1.2_1`**.
- **Size**: Size of the package in Bytes. KBytes or MBytes, such as **`652 B`**.

- **Repository**: Repository of the plugin, such as **`OPNsense`** or **`SunnyValley`**. All community plugins are released from the `OPNsense` repository.
- **Comment**: Description of the plugin, such as **`Vendor repository for Sensei (Next-Generation Firewall Extensions)`** in our example.

On `Plugins` page, there are 3 types of action buttons for each plugin:

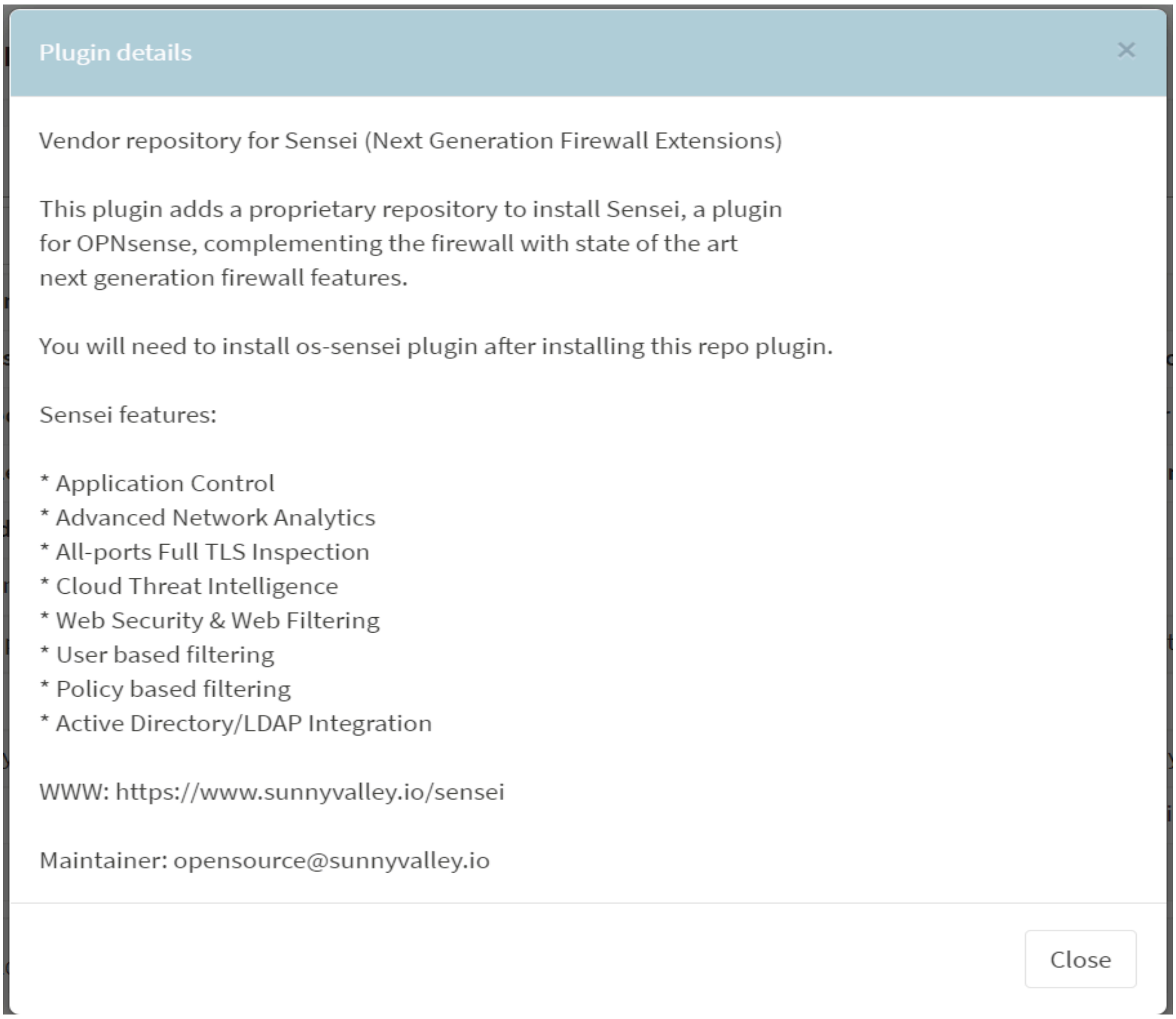
1. **Info**: Black circle button with **`i`** icon is used to view information details of the plugin
2. **Install**: Square button with the **+** icon is used to install a plugin.
3. **Remove**: Square button with a trash box icon is used to uninstall a plugin.



os-wireguard (installed)	**1.8**	**47.3KiB**	**OPNsense**	**WireGuard VPN service**	ℹ 🗑
os-acme-client	3.5	635KiB	OPNsense	ACME Client	ℹ +

Figure 2. *Action buttons for plugins on OPNsense*

You can view the details of a plugin for more information by clicking on the **`Info`** button at the end of the plugin row.



Plugin details

Vendor repository for Sensei (Next Generation Firewall Extensions)

This plugin adds a proprietary repository to install Sensei, a plugin
for OPNsense, complementing the firewall with state of the art
next generation firewall features.

You will need to install os-sensei plugin after installing this repo plugin.

Sensei features:

* Application Control
* Advanced Network Analytics
* All-ports Full TLS Inspection
* Cloud Threat Intelligence
* Web Security & Web Filtering
* User based filtering
* Policy based filtering
* Active Directory/LDAP Integration

WWW: https://www.sunnyvalley.io/sensei

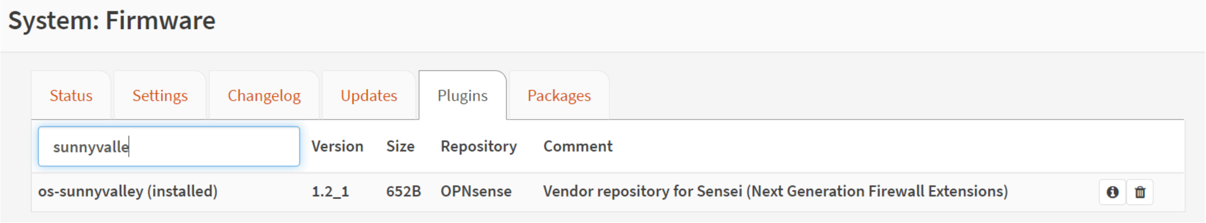
Maintainer: opensource@sunnyvalley.io

Figure 3. *Viewing* `os-sunnyvalley` *plugin information details on OPNsense*

How to Search for a Plugin

You can easily search for a plugin by typing on the search bar in the `Name` column on the **Plugins** page. You can follow the steps given below:

1. Navigate to the `System → Firmware → Plugins` on OPNsense web UI.
2. Type the plugin name on the search bar at the `Name` column, such as `sunnyvalley`. While you are typing, the plugins list will be updated automatically.



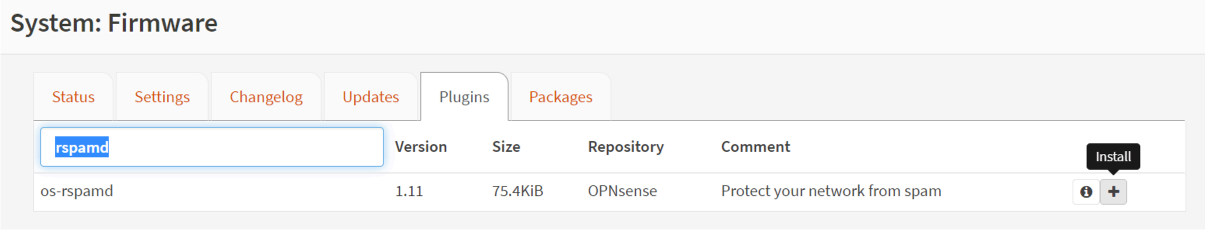
sunnyvalle	Version	Size	Repository	Comment
os-sunnyvalley (installed)	1.2_1	652B	OPNsense	Vendor repository for Sensei (Next Generation Firewall Extensions)

Figure 4. *Searching for a plugin on OPNsense*

How to Install a Plugin

It is very straightforward to install a plugin on the OPNsense firewall. You can easily and quickly install available plugins by following these instructions:

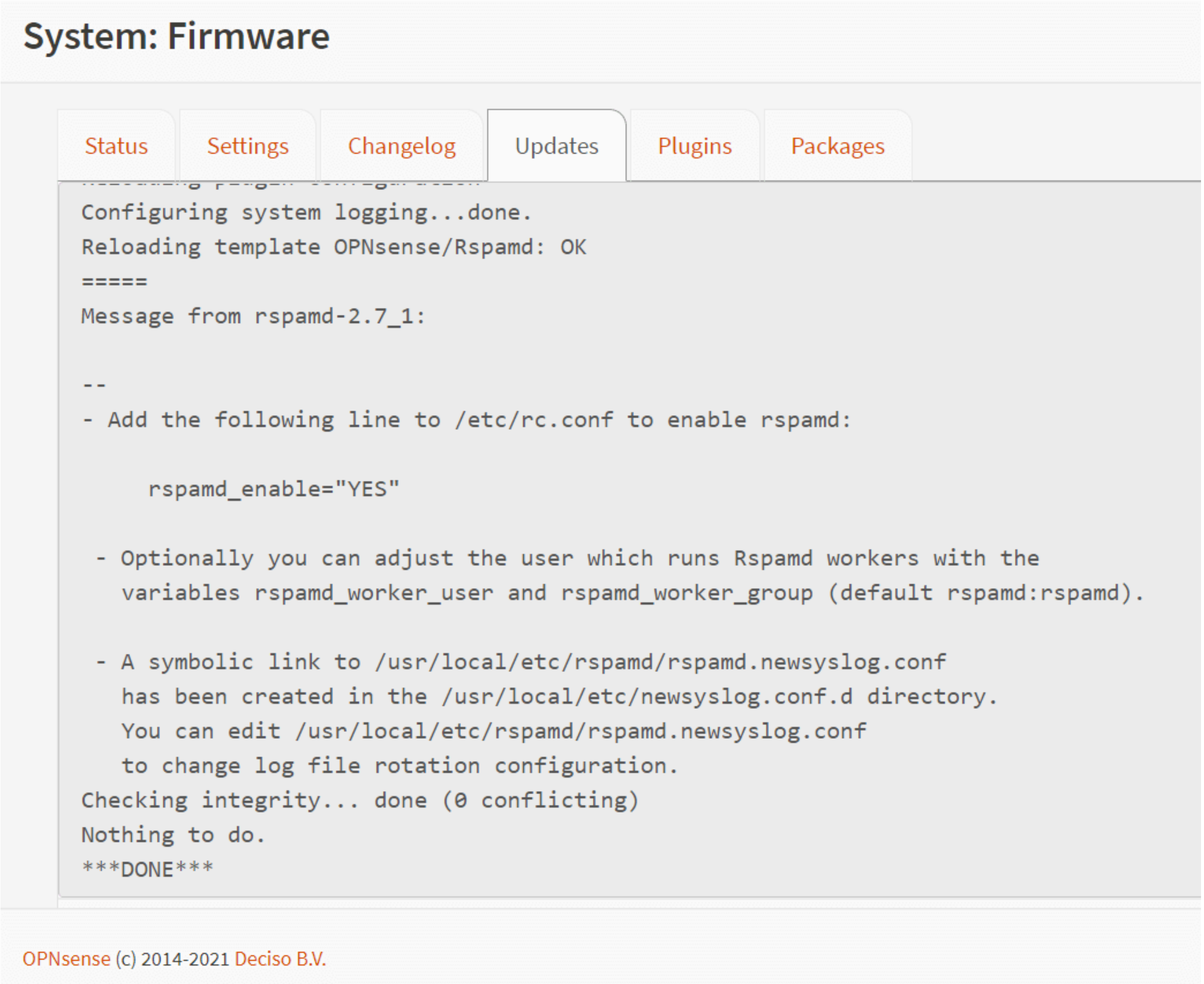
1. Be sure that your OPNsense system is up-to-date. Please, refer to the [How to Update OPNsense]() article written by Zenarmor for more information.
2. Navigate to the `System → Firmware → Plugins` on OPNsense web UI.
3. Search for the plugin you want to install, for example, `os-rspamd`.



rspamd	Version	Size	Repository	Comment
os-rspamd	1.11	75.4KiB	OPNsense	Protect your network from spam

Figure 5. *Installing the plugin on OPNsense*

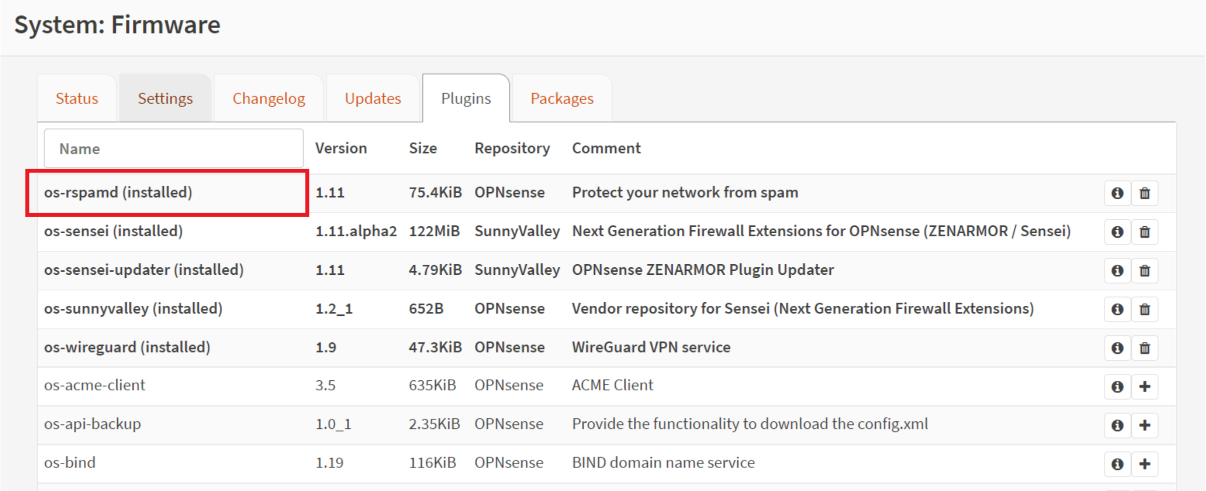
4. Click on the `Install` button. You will be redirected to the `Updates` page and the plugin will be installed.
5. After the plugin is installed successfully, you should see the output similar to the figure below.



```
Configuring system logging...done.
Reloading template OPNsense/Rspamd: OK
=====
Message from rspamd-2.7_1:

--
- Add the following line to /etc/rc.conf to enable rspamd:

     rspamd_enable="YES"

 - Optionally you can adjust the user which runs Rspamd workers with the
   variables rspamd_worker_user and rspamd_worker_group (default rspamd:rspamd).

 - A symbolic link to /usr/local/etc/rspamd/rspamd.newsyslog.conf
   has been created in the /usr/local/etc/newsyslog.conf.d directory.
   You can edit /usr/local/etc/rspamd/rspamd.newsyslog.conf
   to change log file rotation configuration.
Checking integrity... done (0 conflicting)
Nothing to do.
***DONE***
```

Figure 6. *Plugin installation output on the `Updates` page of OPNsense*

6. Click on the `Plugins` tab to view the installed plugins. You should see the plugin that you already added as installed like in the figure below.



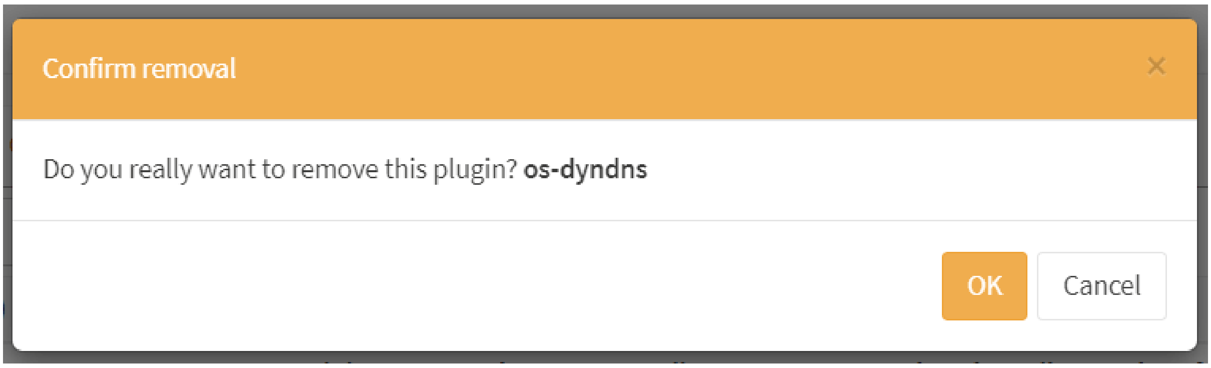
Name	Version	Size	Repository	Comment	
os-rspamd (installed)	1.11	75.4KiB	OPNsense	Protect your network from spam	ℹ 🗑
os-sensei (installed)	1.11.alpha2	122MiB	SunnyValley	Next Generation Firewall Extensions for OPNsense (ZENARMOR / Sensei)	ℹ 🗑
os-sensei-updater (installed)	1.11	4.79KiB	SunnyValley	OPNsense ZENARMOR Plugin Updater	ℹ 🗑
os-sunnyvalley (installed)	1.2_1	652B	OPNsense	Vendor repository for Sensei (Next Generation Firewall Extensions)	ℹ 🗑
os-wireguard (installed)	1.9	47.3KiB	OPNsense	WireGuard VPN service	ℹ 🗑
os-acme-client	3.5	635KiB	OPNsense	ACME Client	ℹ +
os-api-backup	1.0_1	2.35KiB	OPNsense	Provide the functionality to download the config.xml	ℹ +
os-bind	1.19	116KiB	OPNsense	BIND domain name service	ℹ +

Figure 7. *Viewing installed plugins on OPNsense*

How to Remove a Plugin

You can easily uninstall a plugin from your OPNsense firewall by following the steps below:

1. Navigate to the `System` → `Firmware` → `Plugins` on OPNsense web UI.
2. Search for the plugin you want to uninstall, for example, `os-dyndns`.
3. Click on the `Remove` button with a trash box icon next to the plugin. This will open a confirmation dialog box.

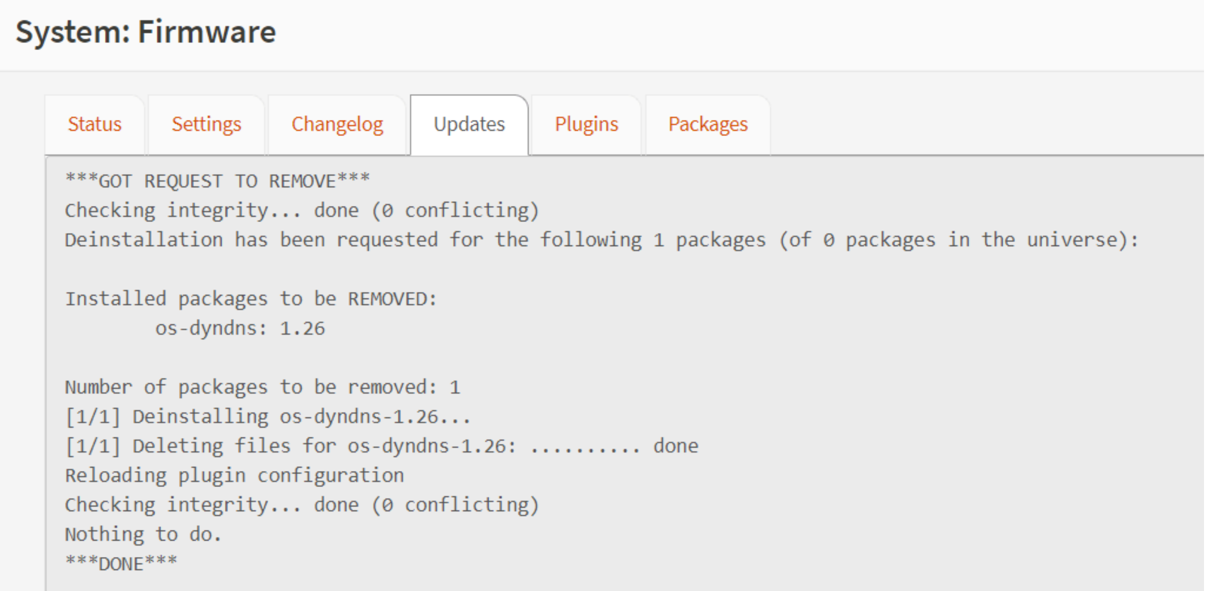


Confirm removal

Do you really want to remove this plugin? **os-dyndns**

Figure 8. *Confirming the plugin removal*

4. Click on `OK` to confirm the plugin uninstallation. This will redirect you to the `Update` page and remove the package. After removing the plugin successfully, you should see an output similar to below.



System: Firmware

```
***GOT REQUEST TO REMOVE***
Checking integrity... done (0 conflicting)
Deinstallation has been requested for the following 1 packages (of 0 packages in the universe):

Installed packages to be REMOVED:
        os-dyndns: 1.26

Number of packages to be removed: 1
[1/1] Deinstalling os-dyndns-1.26...
[1/1] Deleting files for os-dyndns-1.26: .......... done
Reloading plugin configuration
Checking integrity... done (0 conflicting)
Nothing to do.
***DONE***
```

Figure 9. *`os-dyndns` plugin removed*

Best OPNsense Plugins

In this section, we will outline the top OPNsense plugins which are the most widespread among the community. They are extremely beneficial and offer excellent network security solutions to protect your valuable assets from cyber threats. We choose plugins with distinct capabilities that do not overlap to protect you across multiple attack surfaces. Top OPNsense plugins are as follows:

1. Zenarmor
2. WireGuard
3. NGINX
4. Rspamd
5. Freeradius

1. Zenarmor

Zenarmor is a stand-alone instant firewall that can be installed almost anywhere. It offers cutting-edge, next-generation firewall features for open-source firewalls that aren't currently available in products like OPNsense and pfSense® software. Zenarmor provides Application Control, Network Analytics, and TLS Inspection, among other features to enhance your OPNsense firewall.

Zenarmor, which is based on a cloud-based web categorization of 300+ million websites divided into 60+ categories, allows administrators to create custom online filtering profiles and rules.

SVN Cloud is a massive database that serves millions of searches per day and contains reputation and security information on over 300 million websites, with more being added regularly. Zenarmor can respond to malware threats and viral outbreaks in real-time thanks to SVN Cloud.

Since 2017, there have been thousands of Zenarmor deployments in homes, small businesses, and some enterprise-level networks around the world. It doesn't matter who you are, whether an IT manager of an enterprise network or a parent who needs cyber hygiene at the home network to keep kids safe, let you give a chance to Zenarmor by installing `os-sunnyvalley` and `os-sensei` plugins respectively for free.

💡 **BEST PRACTICE**

Zenarmor NGFW Plug-in allows you to easily upgrade your firewall to a Next Generation Firewall in seconds. NG Firewalls empower you to combat modern-day cyber attacks that are becoming more sophisticated every day.

Some of the capabilities are layer-7 application/user aware blocking, granular filtering policies, commercial-grade web filtering utilizing cloud-delivered AI-based Threat Intelligence, parental controls, and the industry's best network analytics and reporting.

Zenarmor Free Edition is available at no cost for all OPNsense users.

2. WireGuard

WireGuard is a fast, simple, and modern VPN that employs cutting-edge cryptography. It intends to be faster, simpler, leaner, and more useful than other VPN protocols, such as IPsec or OpenVPN. WireGuard is planned to be a general-purpose VPN that can be used on embedded interfaces as well as supercomputers in a variety of situations.

It was originally designed for the Linux kernel, but it is now cross-platform and widely deployed. Although it is still in the early stages of development, it has the potential to be the most user-friendly, secure, and straightforward VPN solution in the cyber security world. If you need to provide remote connections for your users, you may find more information on the following articles written by Zenarmor:

- WireGuard VPN Guide
- How Do I Set Up WireGuard for OPNsense?

3. NGINX

NGINX is a high-performance edge web server with the smallest memory footprint and the essential features for constructing efficient and modern web infrastructure.

An HTTP server, HTTP and mail reverse proxy, load balancing, caching, request throttling, SSL offloading, compression, connection multiplexing, and reuse, and HTTP media streaming are all features of NGINX. If you need a fast and secure web service or a WAF, you can easily install the `os-nginx` plugin on your OPNsense system.

4. Rspamd

For spam protection, OPNsense also includes the 'rspamd' plugin. Rspamd is a spam filter that is fast, modular, and lightweight. It is designed to handle large amounts of mail and can be easily extended with custom `lua` filters.

It evaluates communications using a variety of rules including statistical analysis, regular expressions, and specialized services such as URL ban lists. Each message is examined and a spam score is assigned.

Based on the spam score and the user's settings, Rspamd suggests an action for the MTA to take with the message, such as passing, rejecting, or adding a header. It can process hundreds of messages per second and has a plethora of useful features.

5. Freeradius

The most widely used RADIUS server in the world is FreeRADIUS. It includes a RADIUS server, a PAM library, a client library licensed under the BSD license, and an Apache module. The server is quick, loaded with features, modular, and scalable.

It serves as the foundation for a variety of commercial offerings. It meets the AAA requirements of many Fortune 500 companies and Tier 1 ISPs. It is also widely used for Enterprise Wi-Fi and IEEE 802.1X network security, particularly in academic settings such as `eduroam`.

By installing the `os-freeradius` plugin on your OPNsense firewall, you will have an Authentication, Authorization, and Accounting Server on your network.

Things To Consider When Using a Plugin

You should consider the following tips when choosing and using a plugin to keep your firewall secure and efficient.

- **Do not install unnecessary plugins**: Every service on your system comes with its own security risk. To narrow the cyber attack surface remove the plugins entirely if you aren't using them. If you need one of them later, you can always reinstall the plugin easily.
- **Keep your system up-to-date**: Software updates not only provide new features but also patch security holes and fix the bugs. Therefore, you should always keep your firewall up-to-date. If you don't update your firewall when the new updates are released by OPNsense, you expose yourself to potential frustrations and security breaches.
- **Avoid Similar Plugins**: Plugins that overlap in services waste your system resources, such as disk, CPU, memory, and bandwidth while potentially posing additional security risks.
- **Read the documentation**: Before installing a plugin, you should understand what it can do and what effects it may have on your network. If you do not, you may find yourself in the middle of big trouble by causing service interruptions in your company.

How to Install OPNsense on Virtualbox

In this tutorial, we are going to explain how to install OPNsense on the VirtualBox environment. Before we jump on the how-to tasks let’s understand what Virtualbox is and what is OPNSense.

VirtualBox is a robust x86 and AMD64/Intel64 virtualization solution that can be used in both the office and at home. VirtualBox is not only a feature-rich, high-performance product for enterprise customers; it is also the only professional solution that is freely available as Open Source Software under the terms of the GNU General Public License (GPL) version

VirtualBox is currently available for Windows, Linux, Macintosh, and Solaris hosts, and it supports a wide range of guest operating systems, including but not limited to Windows.

VirtualBox is continuously developed, with frequent releases, and it has an ever-expanding list of features, supported guest operating systems, and platforms.

After giving an overview of Virtualbox let's define the OPNsense.

OPNsense is an open-source, easy-to-use, and easy-to-build firewall and routing platform built on FreeBSD. OPNsense has almost all of the functions found in pricey commercial firewalls, and in many cases, even more. It combines the benefits of open and verifiable sources with the comprehensive feature set of commercial products.

In 2014, OPNsense was born as a fork of pfSense® and m0n0wall, with the first official release in January 2015. The project has progressed swiftly while still preserving m0n0wall and pfSense characteristics. The project's development is driven by a strong focus on security and code quality.

OPNsense provides weekly security upgrades in tiny increments in order to respond to new emerging threats in a timely manner. Businesses may plan updates ahead of time thanks to a defined release cadence of two major releases per year. A roadmap is created for each major release to guide development and establish clear objectives.

💡 **BEST PRACTICE**

You can easily upgrade your OPNsense packet filtering firewall to a Next Generation Firewall in seconds by installing Zenarmor NGFW Plug-in that is one of the most popular OPNsense. NG Firewalls empower you to combat modern-day cyber attacks that are becoming more sophisticated every day.

Some of the capabilities are layer-7 application/user aware blocking, granular filtering policies, commercial-grade web filtering utilizing cloud-delivered AI-based Threat Intelligence, parental controls, and the industry's best network analytics and reporting.

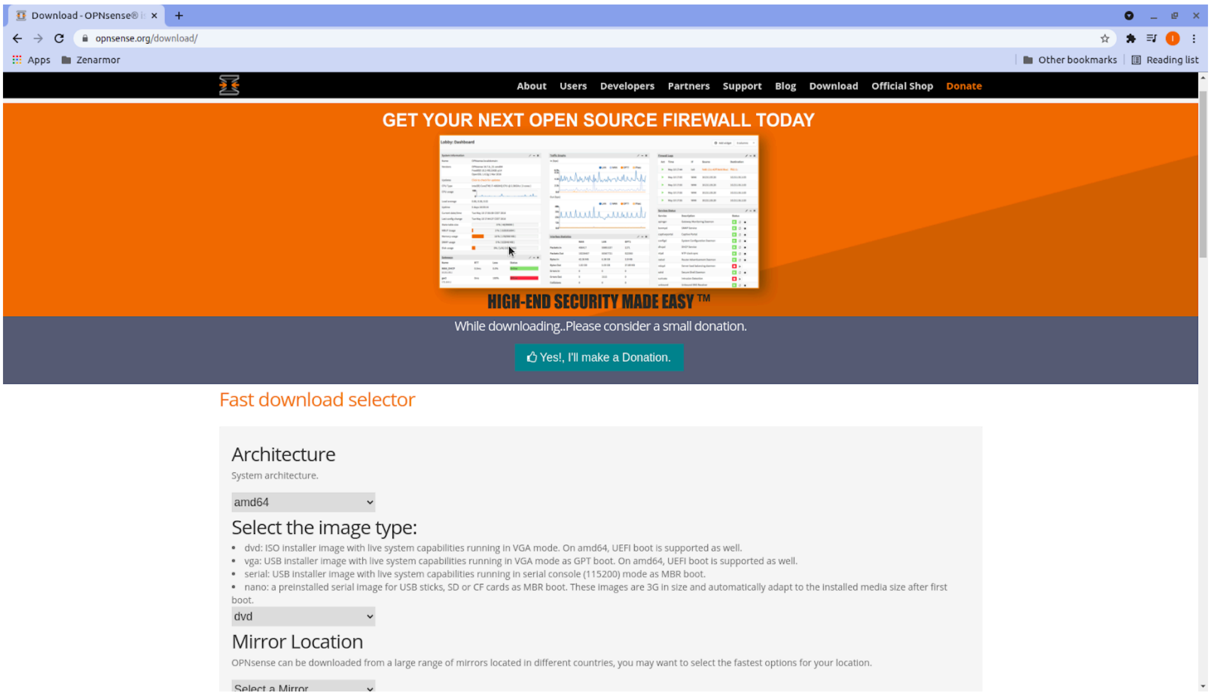
Zenarmor Free Edition is available at no cost for all OPNsense users.

In three basic steps, you can install OPNsense on VirtualBox.

1. The first one is downloading the OPNsense installer file
2. The second step is to configure VirtualBox Settings
3. The third step is to configure OPNsense Settings

1. Download OPNsense

We are going to start with downloading the OPNsense installer from `OPNsense.org`



While downloading..Please consider a small donation.

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.

Select a Mirror

Figure 1. *OPNsense download page*

- System Architecture is only available for amd64
- We will boot on Virtualbox then select the image type as DVD
- Select the Mirror Location as geographically close to you

After selection of 3 required fields, you can start to download by clicking on the Download.

When the downloading task is finished you need to extract the iso file to a preferred path on your computer.

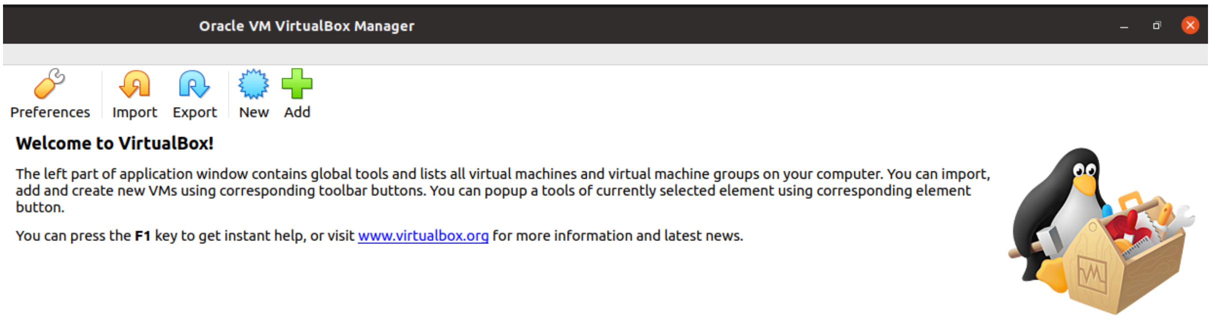
Now you have an OPNsense iso file to boot on Virtualbox. We assume that you have Virtualbox on your computer. Let's start to install our OPNsense as a VM instance.

2. Virtual Box Settings

You may follow the next step to complete the Virtual Box settings.

1. Create an OPNsense VM instance.

On VirtualBox, you can create a new VM instance by clicking on the **New** or by using the **CRTL+N** shortcut.



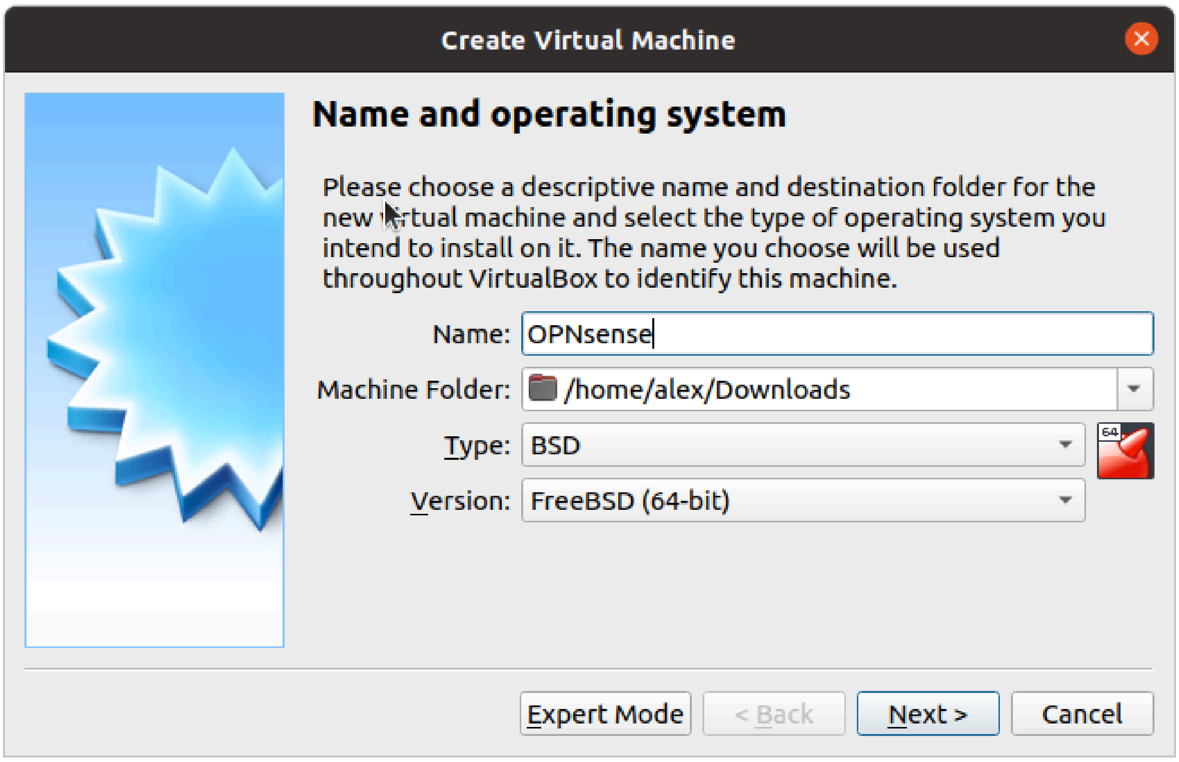
Welcome to VirtualBox!

The left part of application window contains global tools and lists all virtual machines and virtual machine groups on your computer. You can import, add and create new VMs using corresponding toolbar buttons. You can popup a tools of currently selected element using corresponding element button.

You can press the **F1** key to get instant help, or visit www.virtualbox.org for more information and latest news.

Figure 2. Create new Virtual Machine Instance

When you click to **New,** a **Create Virtual Machine** window will appear.



Create Virtual Machine

Name and operating system

Please choose a descriptive name and destination folder for the new virtual machine and select the type of operating system you intend to install on it. The name you choose will be used throughout VirtualBox to identify this machine.

Name: OPNsense

Machine Folder: /home/alex/Downloads

Type: BSD

Version: FreeBSD (64-bit)

Figure 3. Create Virtual Machine on VirtualBox

On that window

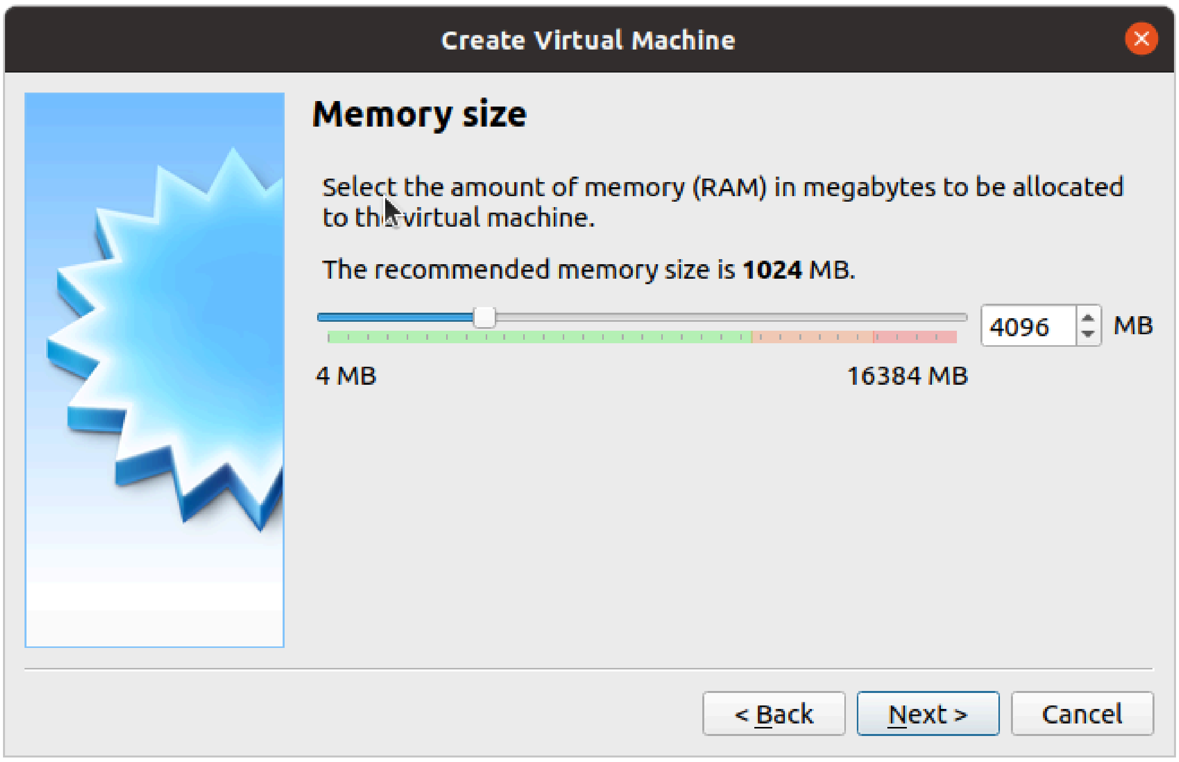
- Type the name of your OPNsense VM Instance
- Select the preferred folder to create VM files on it.
- Select the Types as BSD
- Lastly, Select the Version as FreeBSD (64-Bit)

Click **Next** to configure **Memory Settings.**

2. Configure the memory

The recommended memory size is 1024 MB

Depending on your computer’s memory capacity you can allocate more RAM for your VM instance.



Create Virtual Machine

Memory size

Select the amount of memory (RAM) in megabytes to be allocated to the virtual machine.

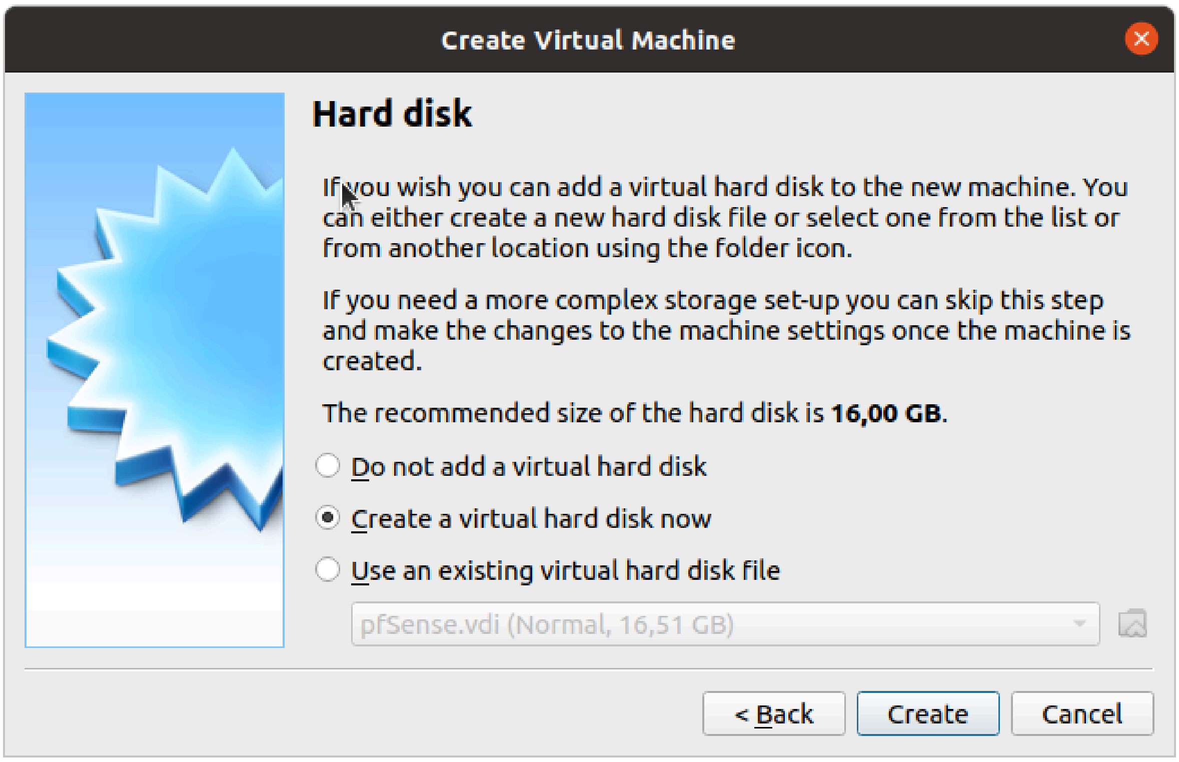
The recommended memory size is **1024** MB.

4096 MB

Figure 4. Configure Memory Size on VBox

Click **Next** to configure **Virtual Hard Disk Settings.**

3. Configure the Virtual Hard Disk



Create Virtual Machine

Hard disk

If you wish you can add a virtual hard disk to the new machine. You can either create a new hard disk file or select one from the list or from another location using the folder icon.

If you need a more complex storage set-up you can skip this step and make the changes to the machine settings once the machine is created.

The recommended size of the hard disk is **16,00 GB**.

○ Do not add a virtual hard disk

● Create a virtual hard disk now

○ Use an existing virtual hard disk file

pfSense.vdi (Normal, 16,51 GB)

Figure 5. Hard Disk Configuration on VirtualBox

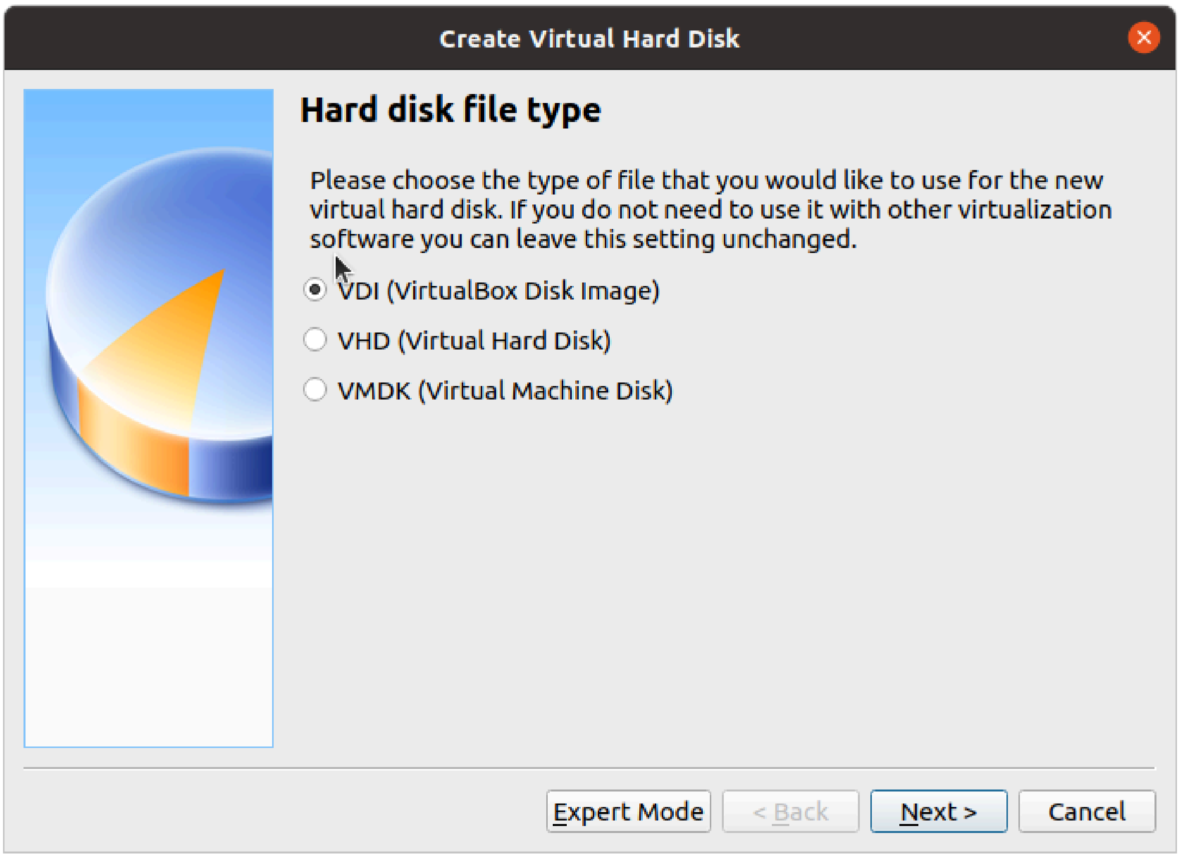
If you wish you can add a virtual hard disk to the new machine. You can either create a new hard disk file or select one from the list or from another location using the folder icon.

If you need a more complex storage setup you can skip this step and make the changes to the machine settings once the machine is created.

The recommended size of the hard disk is 16,00 GB.

We are creating VM Instance from scratch so that we will create a virtual hard disk now

Click **Create**.



Create Virtual Hard Disk

Hard disk file type

Please choose the type of file that you would like to use for the new virtual hard disk. If you do not need to use it with other virtualization software you can leave this setting unchanged.

● VDI (VirtualBox Disk Image)

○ VHD (Virtual Hard Disk)

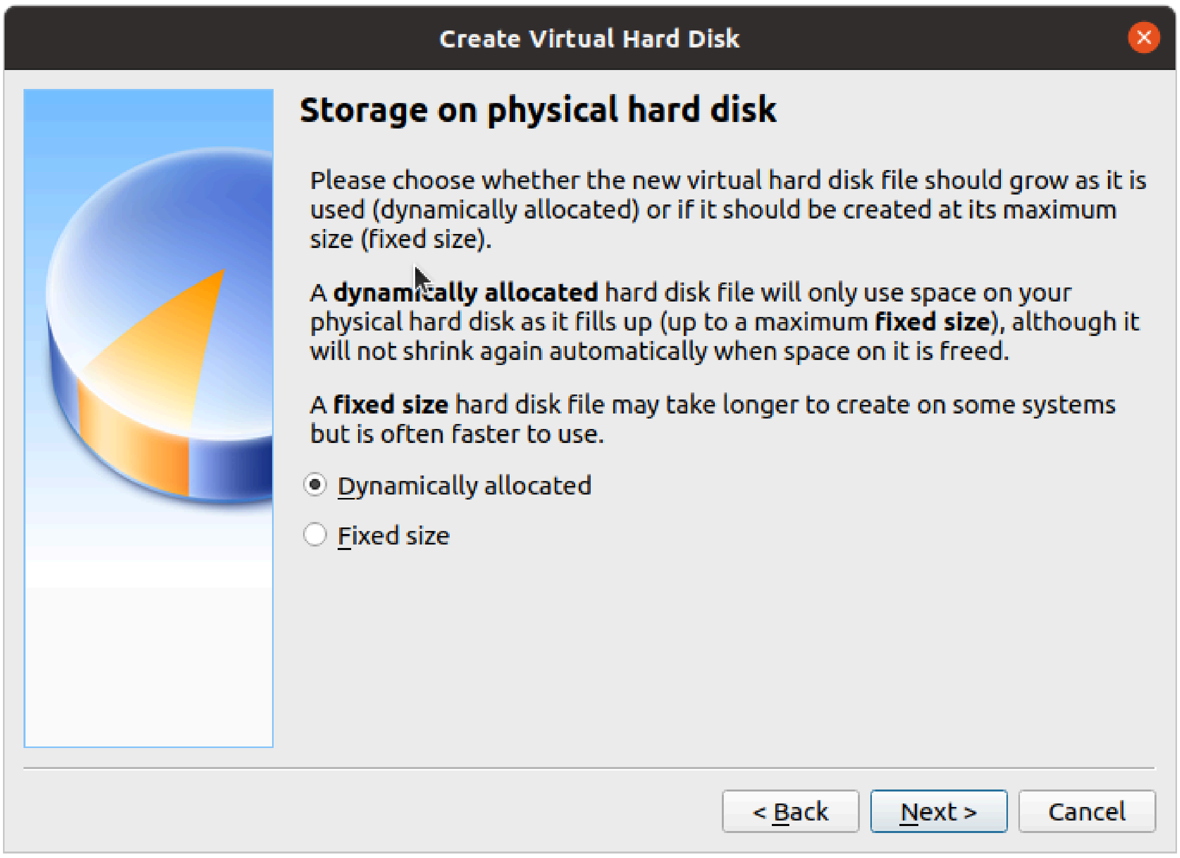
○ VMDK (Virtual Machine Disk)

Figure 6. Hard Disk File Type Selection on VirtualBox

Please choose the type of file that you would like to use for the new virtual hard disk. If you do not need to use it with other virtualization software you can leave this setting unchanged.

Let's go on as the default setting because we are not planning to use that disk in another virtualization environment. Select **VDI (VirtualBox Disk Image).**

Click **Next** to select **Storage Type**.



Create Virtual Hard Disk

Storage on physical hard disk

Please choose whether the new virtual hard disk file should grow as it is used (dynamically allocated) or if it should be created at its maximum size (fixed size).

A **dynamically allocated** hard disk file will only use space on your physical hard disk as it fills up (up to a maximum **fixed size**), although it will not shrink again automatically when space on it is freed.

A **fixed size** hard disk file may take longer to create on some systems but is often faster to use.

● Dynamically allocated

○ Fixed size

Figure 7. Storage on the physical hard disk on VirtualBox

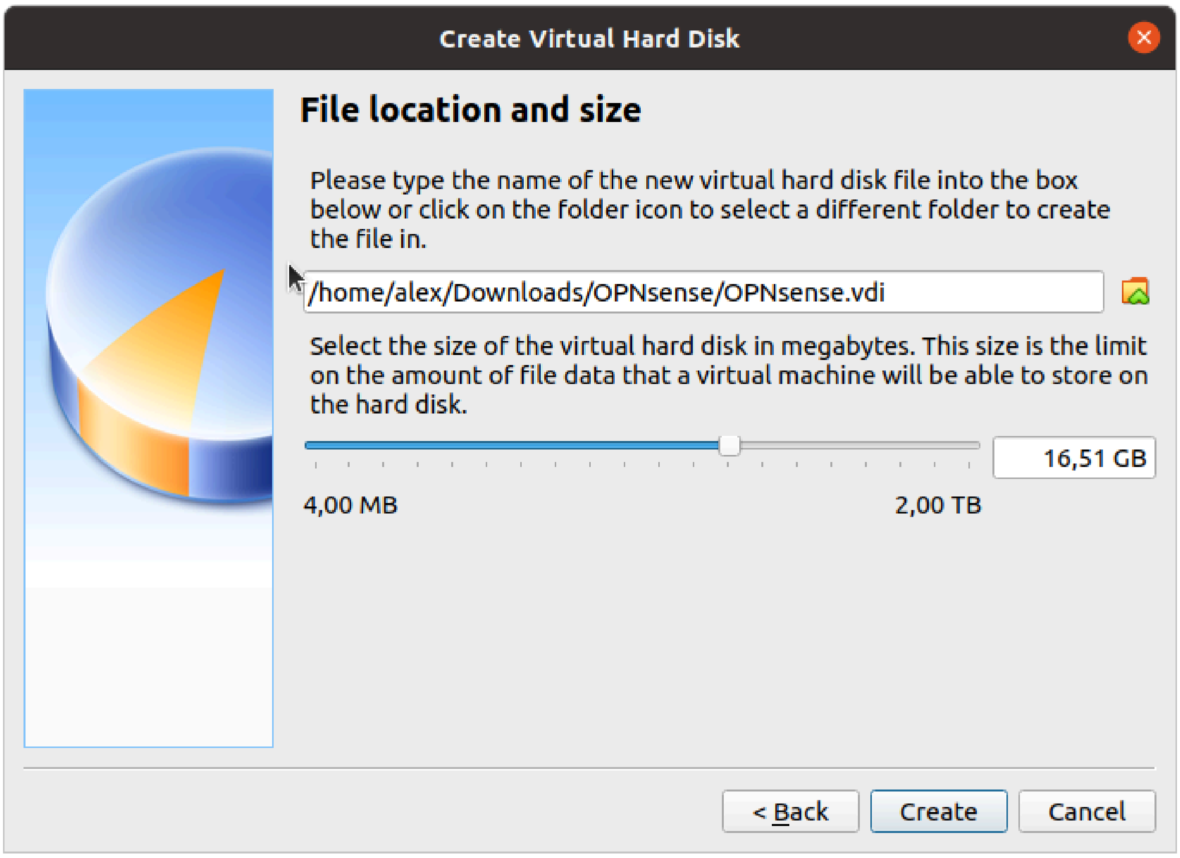
Please choose whether the new virtual hard disk file should grow as it is used (dynamically allocated) or if it should be created at its maximum size (fixed size).

A dynamically allocated hard disk file will only use space on your physical hard disk as it fills up (up to a maximum fixed size), although it will not shrink again automatically when space on it is freed.

A fixed-size hard disk file may take longer to create on some systems but is often faster to use.

We are going to use **Dynamically Allocated** disk for this tutorial.

Click **Next** to set **Files Location** and **Size**.



File location and size

Please type the name of the new virtual hard disk file into the box below or click on the folder icon to select a different folder to create the file in.

/home/alex/Downloads/OPNsense/OPNsense.vdi

Select the size of the virtual hard disk in megabytes. This size is the limit on the amount of file data that a virtual machine will be able to store on the hard disk.

16,51 GB

Figure 8. File Location and Size Settings on VirtualBox

Please type the name of the new virtual hard disk file into the box below or click on the folder icon to select a different folder to create the file in.

As you may remember when we are creating a VM we have chosen the Download Folder, we see here that the path of OPNsense is automatically created under that Download folder. You may continue as it is or you may change it now.

Select the size of the virtual hard disk in megabytes. This size is the limit on the amount of file data that a virtual machine will be able to store on the hard disk.

The more disk space you have you can allocate more. For this tutorial, 16GB is enough.

Click **Create** to finish the VM creation process.

Now you can start to configure VMBox Settings.

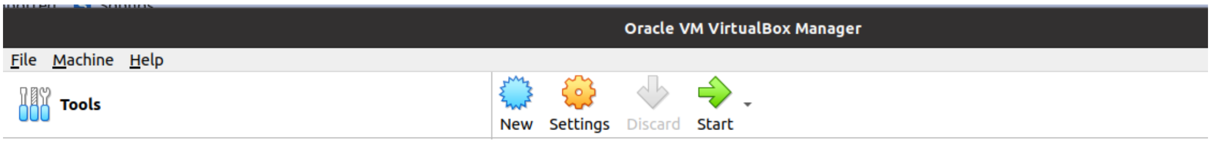
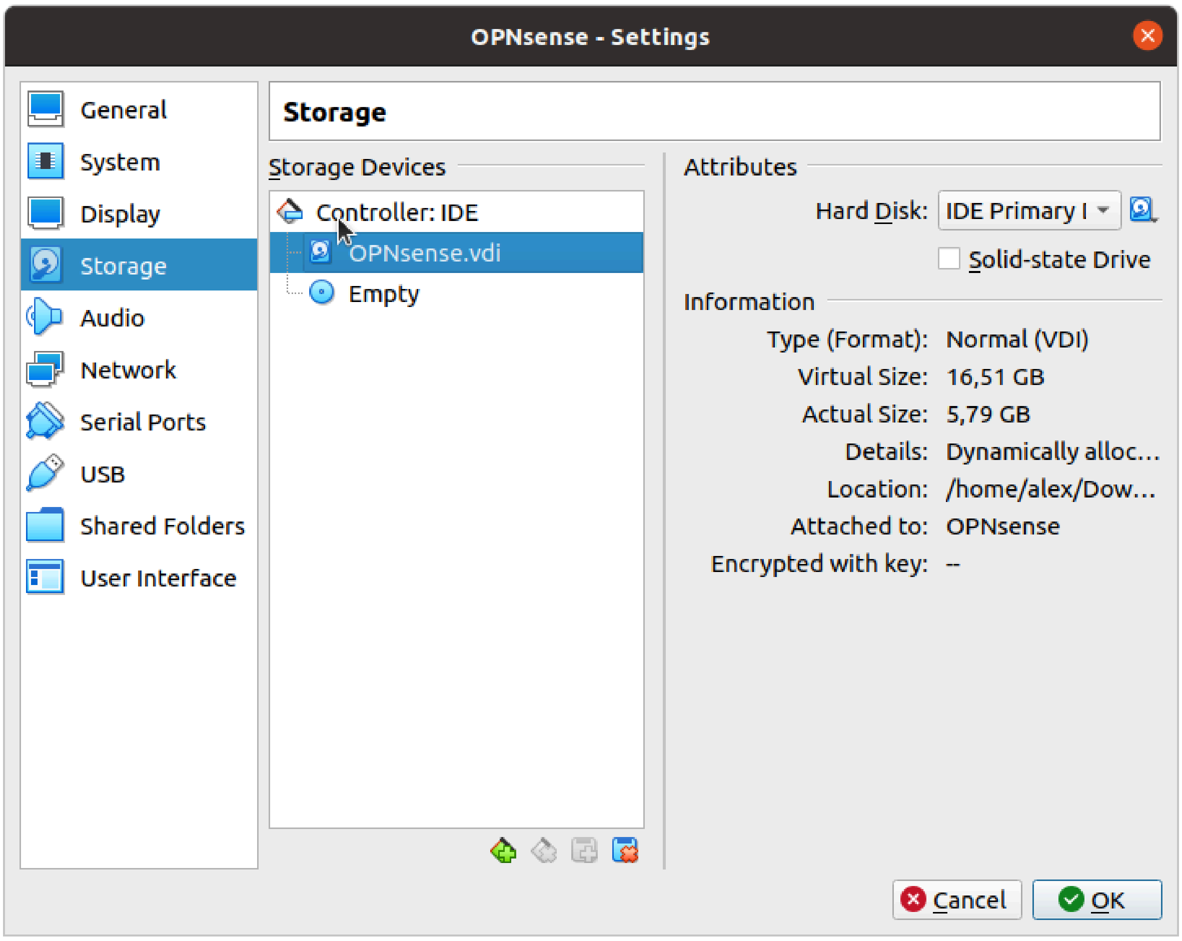


Figure 9. *VirtualBox - Settings*

Click **Settings**.

4. Attach the OPNsense ISO image to VirtualBox

We will start with storage settings.



Hard Disk: IDE Primary I

□ Solid-state Drive

Information

Type (Format): Normal (VDI)

Virtual Size: 16,51 GB

Actual Size: 5,79 GB

Details: Dynamically alloc...

Location: /home/alex/Dow...

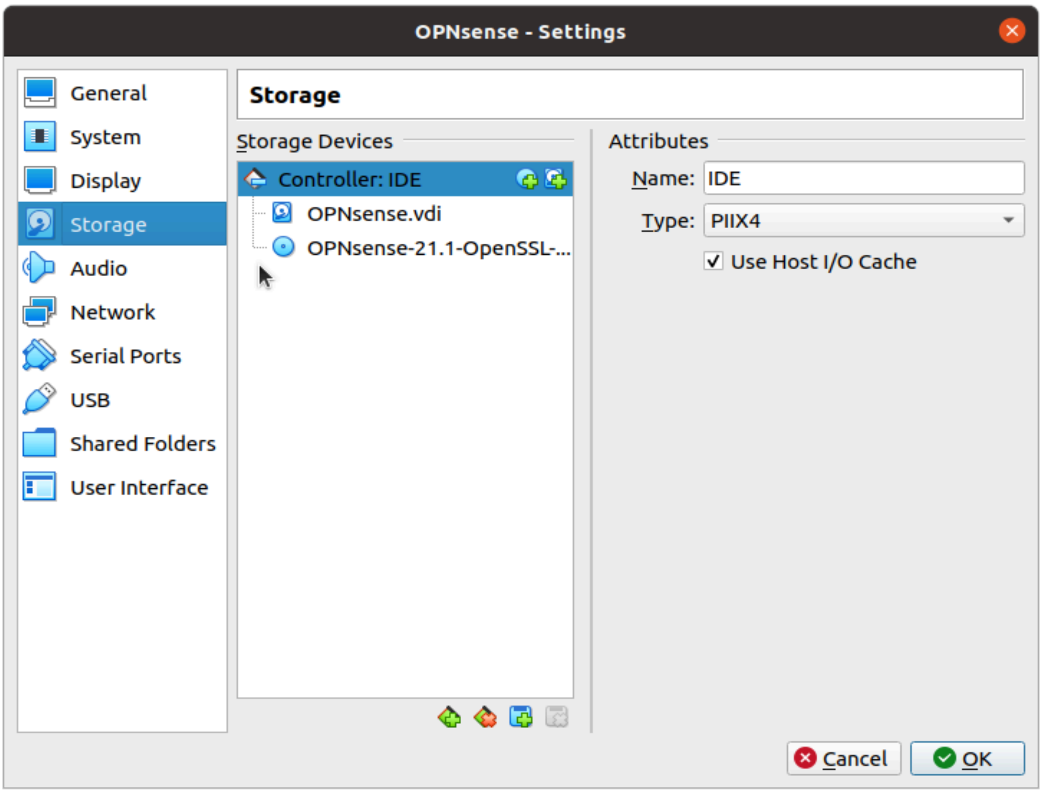
Attached to: OPNsense

Encrypted with key: --

Figure 10. VirtualBox Storage Settings

Firstly to attach the OPNsense ISO file:

Click the **Empty Disc** icon, select the ISO file from Attributes > Hard Disk Menu.



Controller: IDE
- OPNsense.vdi
- OPNsense-21.1-OpenSSL-...

Name: IDE

Type: PIIX4

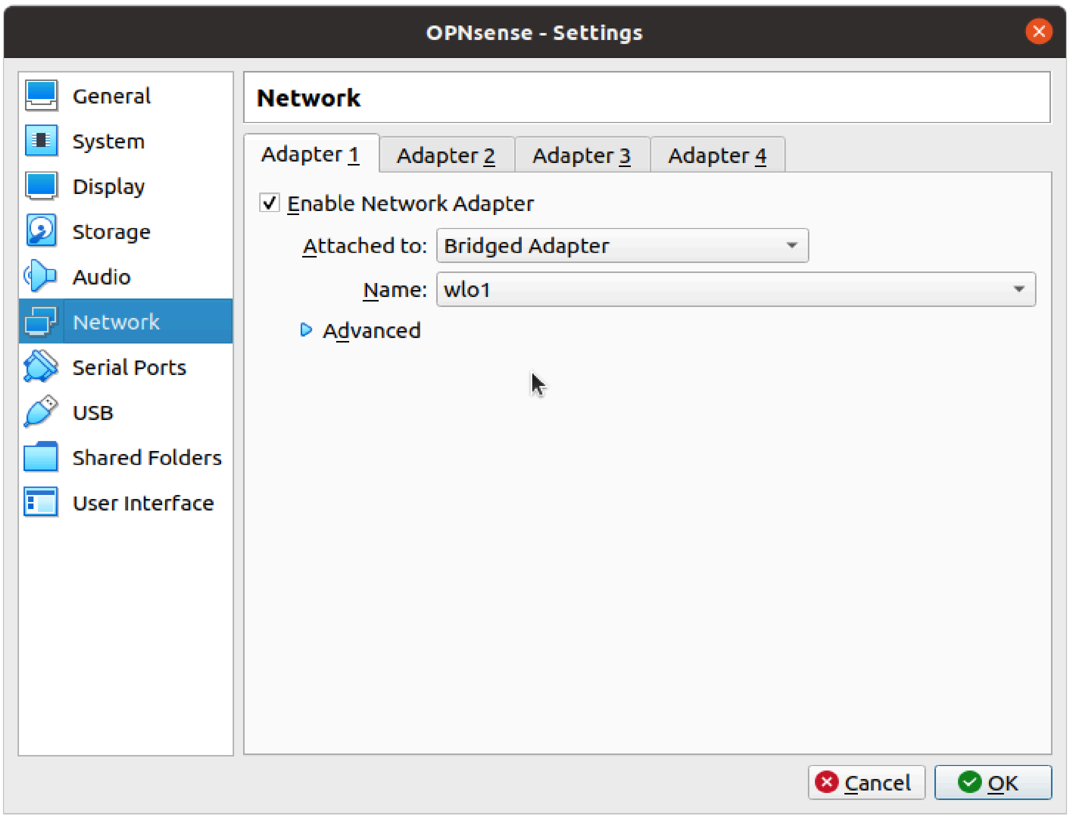
☑ Use Host I/O Cache

Figure 11 . *OPNsense Boot*

5. Connect the network interfaces to the Opnsense firewall

Now we can set the network adapters.

We will create 2 network adapters, the first one will be **Bridge Adapter**.



☑ Enable Network Adapter

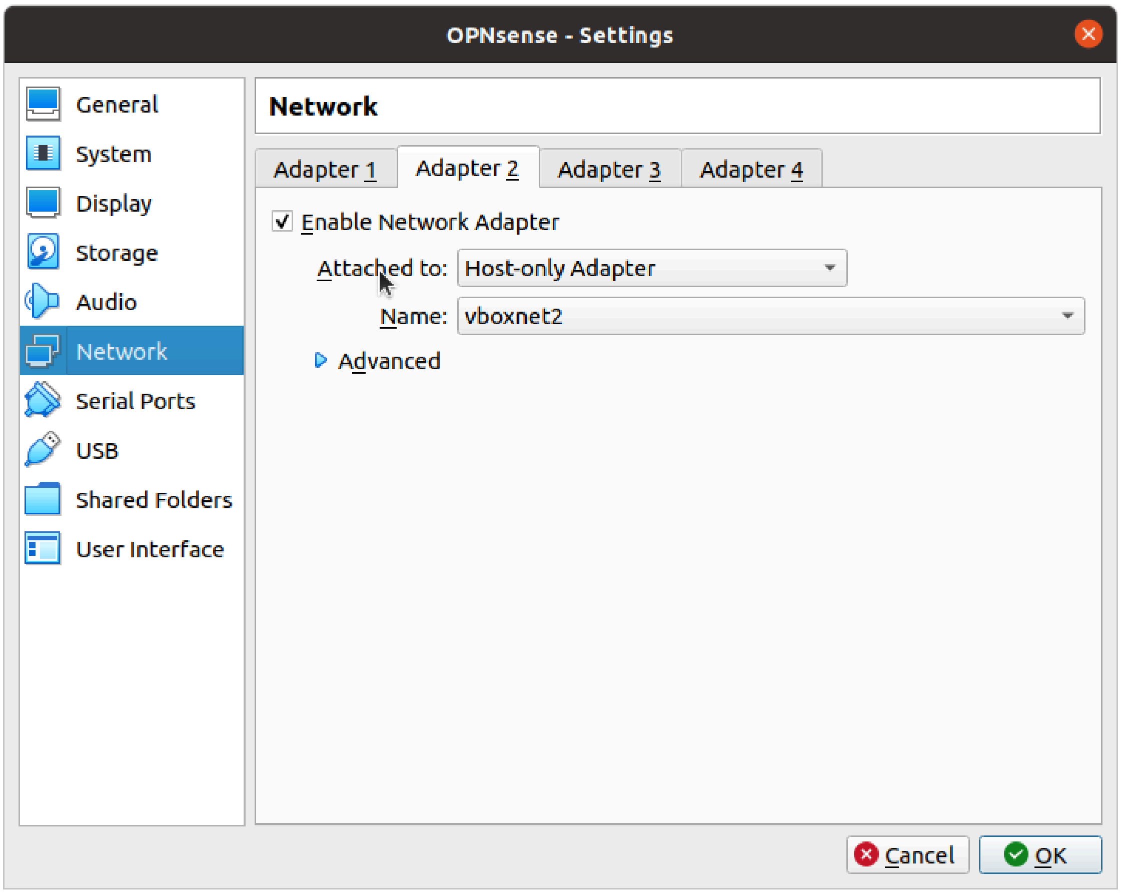
Attached to: Bridged Adapter

Name: wlo1

Figure 12. *VirtualBox Network Settings*

Select the **'Bridge Adapter'** option from the "**Attach to:** " drop-down menu.

Select the **network adapter** on the host system that traffic to from this network card will go through. We chose the wireless adapter.



☑ Enable Network Adapter

Attached to: Host-only Adapter

Name: vboxnet2

Figure 13. *Creating a second Network adapter on VirtualBox*

The second Network adapter will be **Host-only-Adapter**.

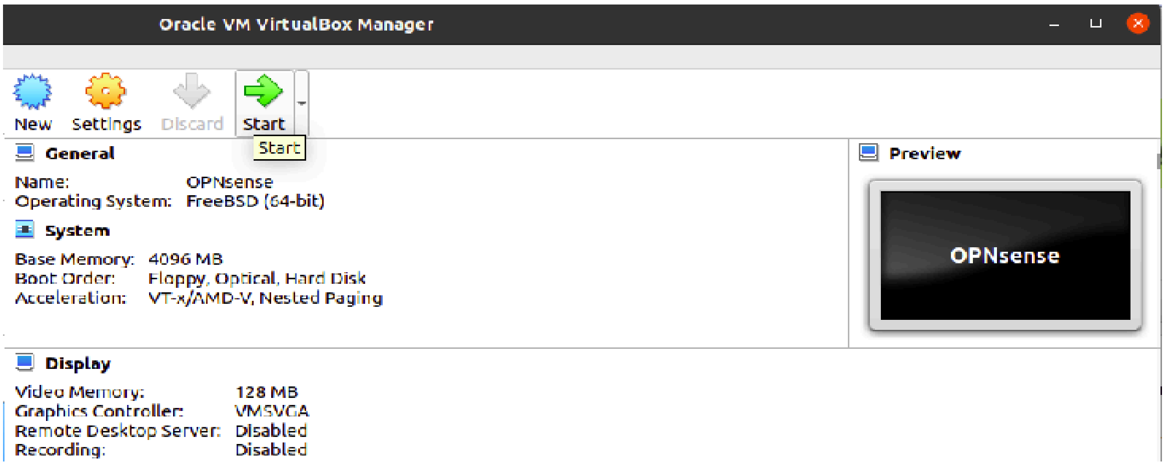
You should choose the created vboxnet interfaces. In this case vboxnet2.

3. OPNsense Firewall Installation on VirtualBox Settings

You can follow the next steps to install OPNsense firewall on your VirtualBox environment.

Start the OPNsense VM

After completing Network adapter settings, you can start your Virtual OPNsense Machine.



General

Name: OPNsense
Operating System: FreeBSD (64-bit)

System

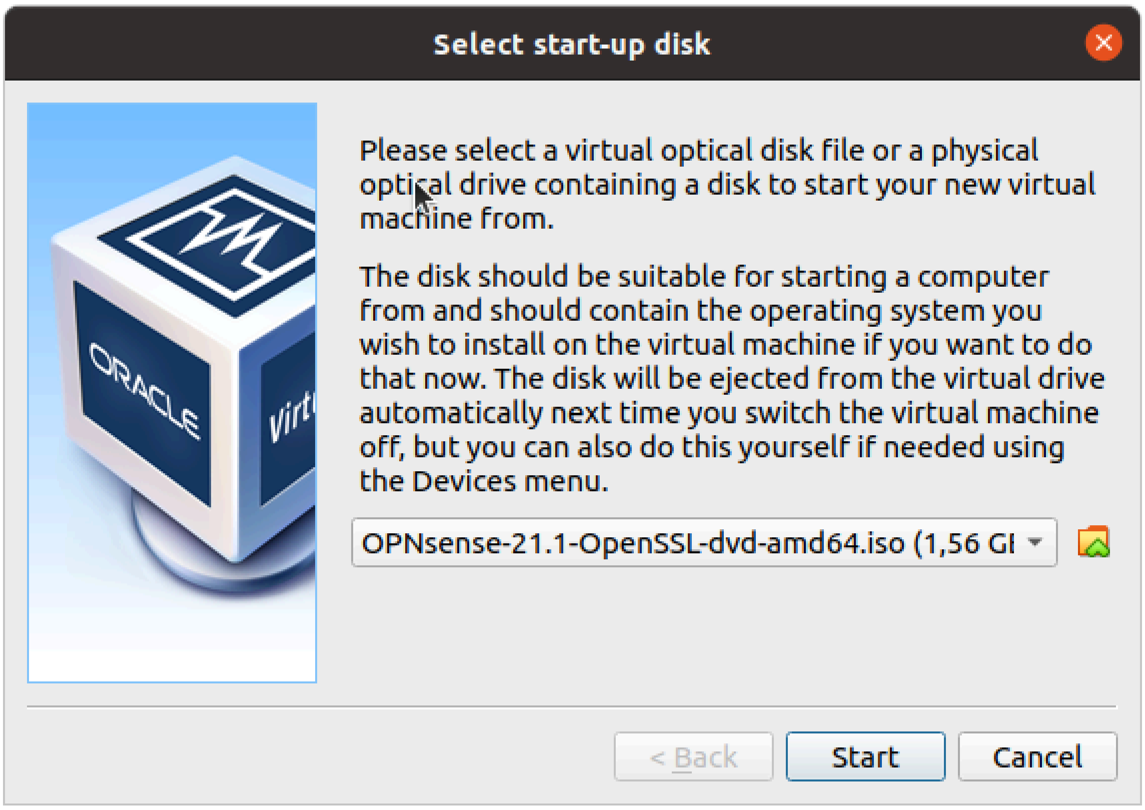
Base Memory: 4096 MB
Boot Order: Floppy, Optical, Hard Disk
Acceleration: VT-x/AMD-V, Nested Paging

Display

Video Memory: 128 MB
Graphics Controller: VMSVGA
Remote Desktop Server: Disabled
Recording: Disabled

Figure 14. *Click Start to boot Virtual OPNsense Machine*

Click **Start** to boot.



Please select a virtual optical disk file or a physical optical drive containing a disk to start your new virtual machine from.

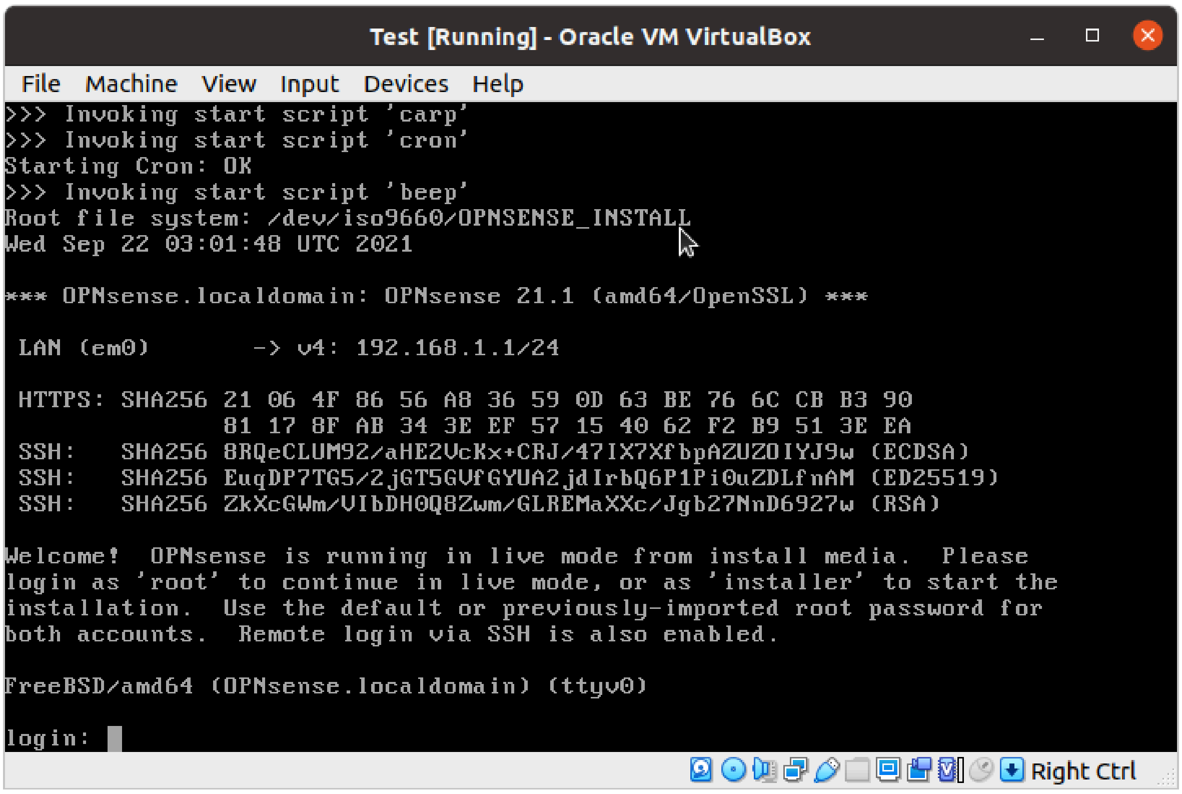
The disk should be suitable for starting a computer from and should contain the operating system you wish to install on the virtual machine if you want to do that now. The disk will be ejected from the virtual drive automatically next time you switch the virtual machine off, but you can also do this yourself if needed using the Devices menu.

OPNsense-21.1-OpenSSL-dvd-amd64.iso (1,56 GI

Figure 15. Select start-up disk on VirtualBox

You will be asked to locate the ISO file again. Locate it and click **Start**.

A black booting screen will be displayed and it will run automatically. You don't need to do anything until the login line appears.


Test [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Right Ctrl

```
>>> Invoking start script 'carp'
>>> Invoking start script 'cron'
Starting Cron: OK
>>> Invoking start script 'beep'
Root file system: /dev/iso9660/OPNSENSE_INSTALL
Wed Sep 22 03:01:48 UTC 2021

*** OPNsense.localdomain: OPNsense 21.1 (amd64/OpenSSL) ***

 LAN (em0)       -> v4: 192.168.1.1/24

 HTTPS: SHA256 21 06 4F 86 56 A8 36 59 0D 63 BE 76 6C CB B3 90
               81 17 8F AB 34 3E EF 57 15 40 62 F2 B9 51 3E EA
 SSH:   SHA256 8RQeCLUM92/aHE2VcKx+CRJ/47IX7XfbpAZUZOIYJ9w (ECDSA)
 SSH:   SHA256 EuqDP7TG5/2jGT5GVfGYUA2jdIrbQ6P1Pi0uZDLfnAM (ED25519)
 SSH:   SHA256 ZkXcGWm/VIbDH0Q8Zwm/GLREMaXXc/Jgb27NnD6927w (RSA)

Welcome!  OPNsense is running in live mode from install media.  Please
login as 'root' to continue in live mode, or as 'installer' to start the
installation.  Use the default or previously-imported root password for
both accounts.  Remote login via SSH is also enabled.

FreeBSD/amd64 (OPNsense.localdomain) (ttyv0)

login:
```

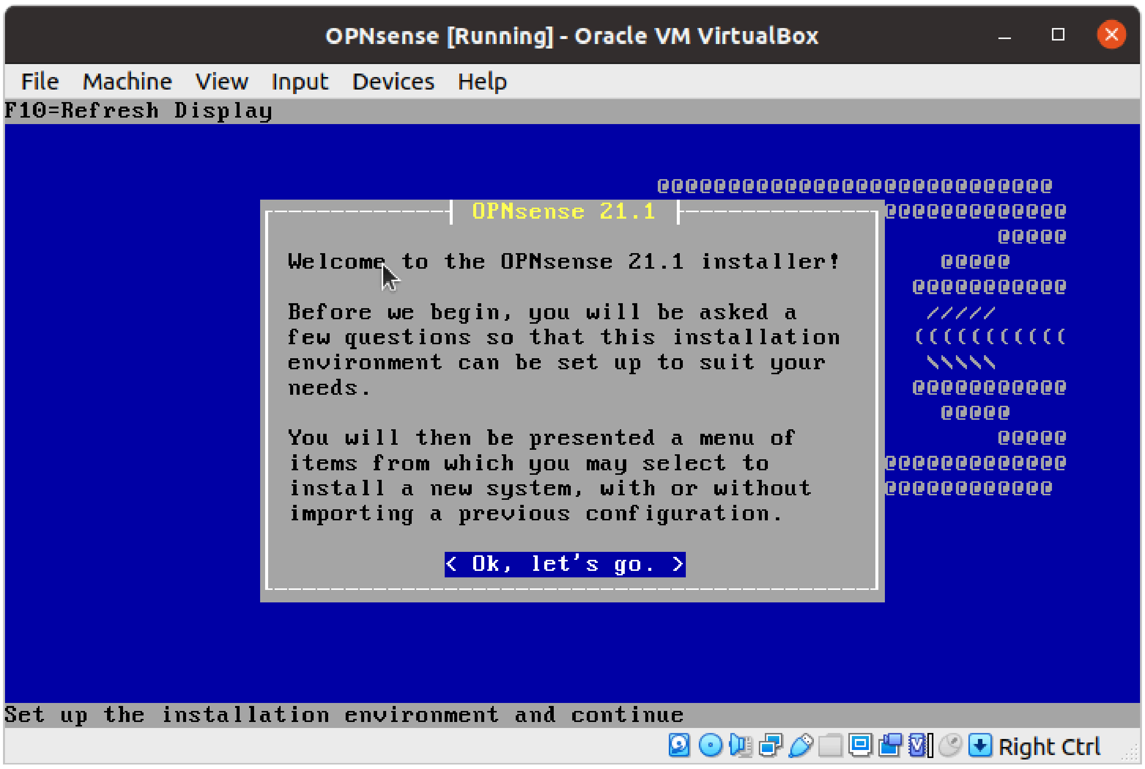
Figure 16. *First login for OPNsense Installer*

After network interfaces are defined automatically you can initiate the installation by providing a username and password.

For installation;

Default username is `installer`.

Default password is `opnsense`.



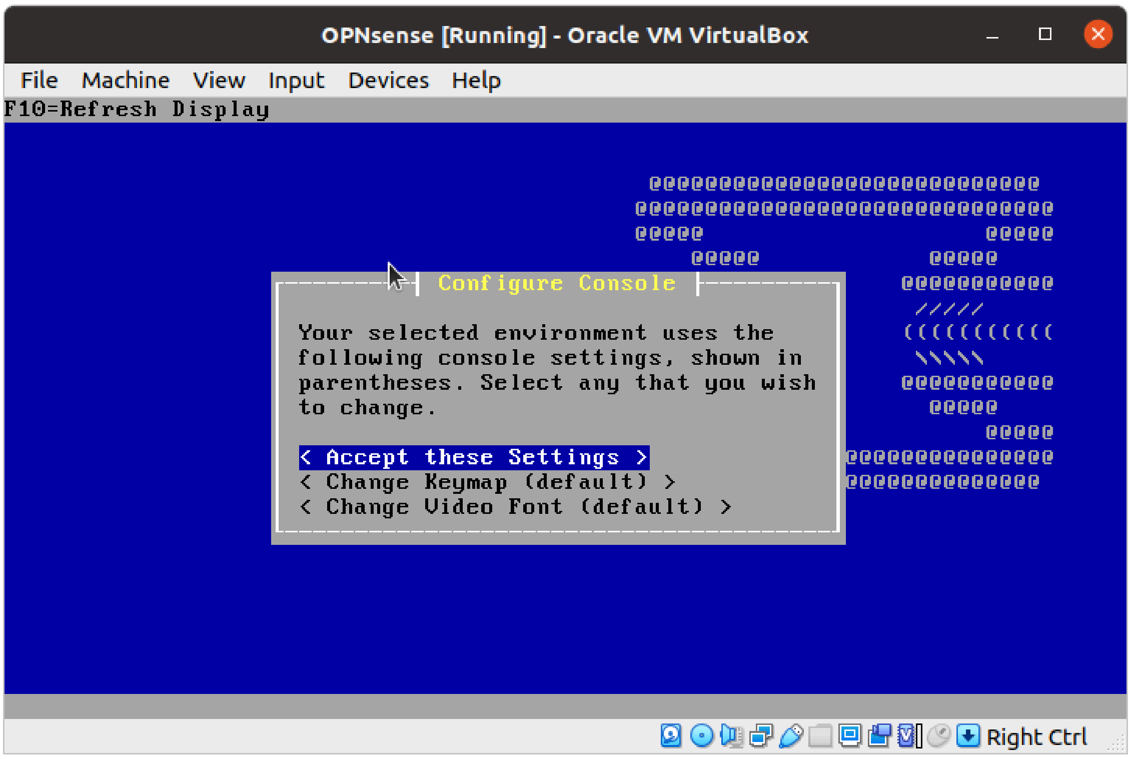
OPNsense [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Right Ctrl

```
F10=Refresh Display

OPNsense 21.1

Welcome to the OPNsense 21.1 installer!

Before we begin, you will be asked a
few questions so that this installation
environment can be set up to suit your
needs.

You will then be presented a menu of
items from which you may select to
install a new system, with or without
importing a previous configuration.

< Ok, let's go. >

Set up the installation environment and continue
```

Figure 17. *Welcome to OPNsense Installer*

The welcome screen will be displayed.

Click **OK**, Let's go.

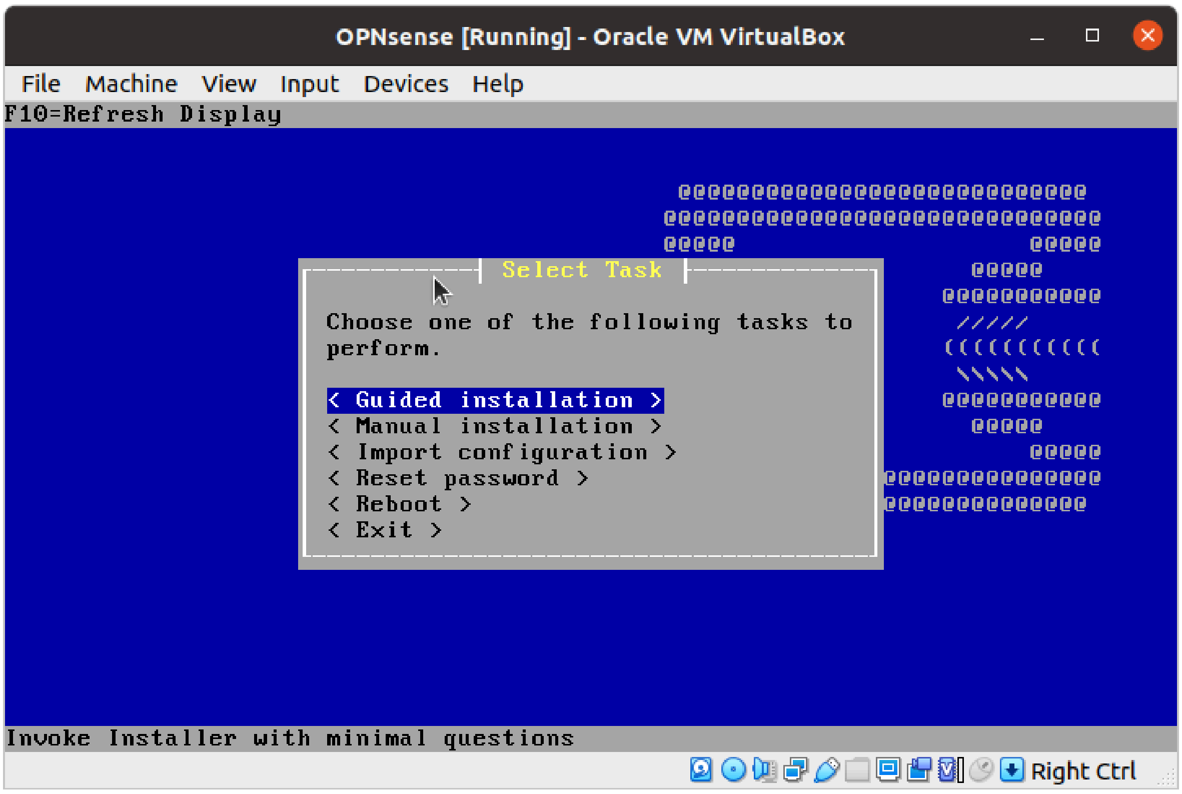


OPNsense [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Right Ctrl

```
F10=Refresh Display

Configure Console

Your selected environment uses the
following console settings, shown in
parentheses. Select any that you wish
to change.

< Accept these Settings >
< Change Keymap (default) >
< Change Video Font (default) >
```

Figure 18. *Configure Console*

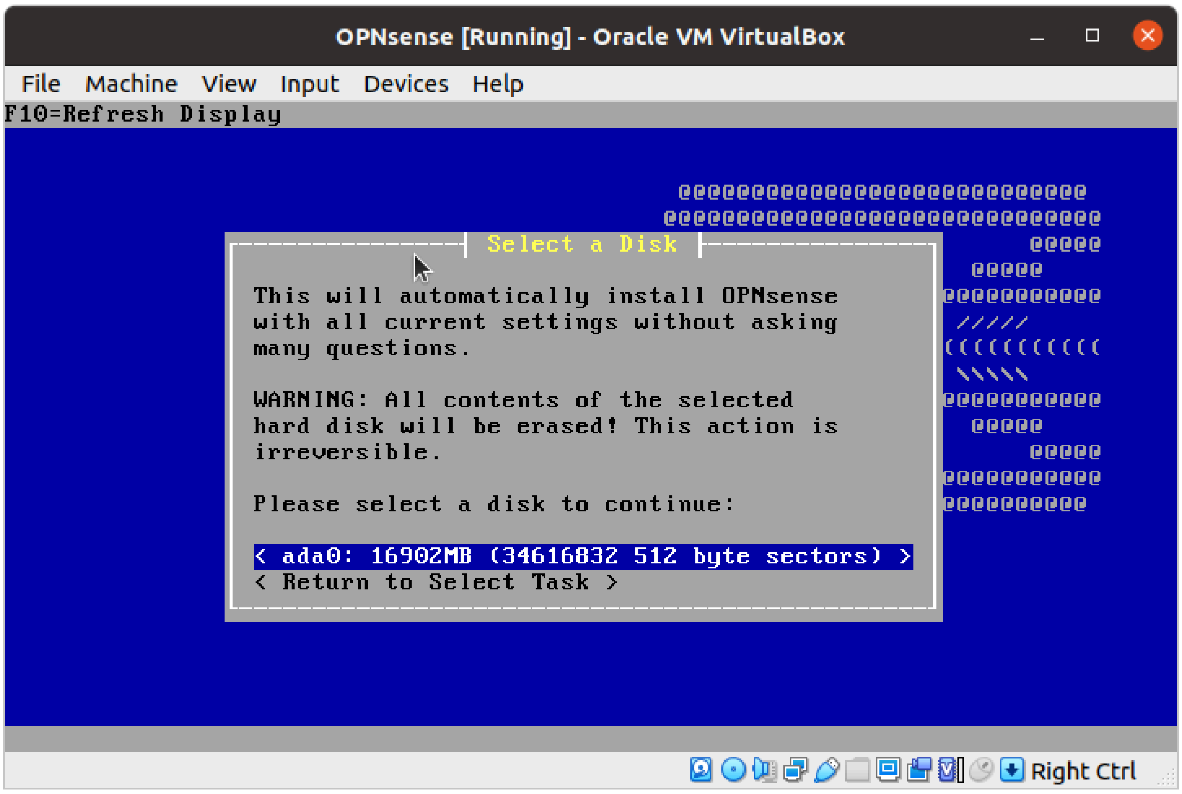
Click **Accept** these Settings.


OPNsense [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Right Ctrl

```
F10=Refresh Display

Select Task

Choose one of the following tasks to
perform.

< Guided installation >
< Manual installation >
< Import configuration >
< Reset password >
< Reboot >
< Exit >

Invoke Installer with minimal questions
```

Figure 19. *Guided Installation*

Select the **Guided installation** option.


OPNsense [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Right Ctrl

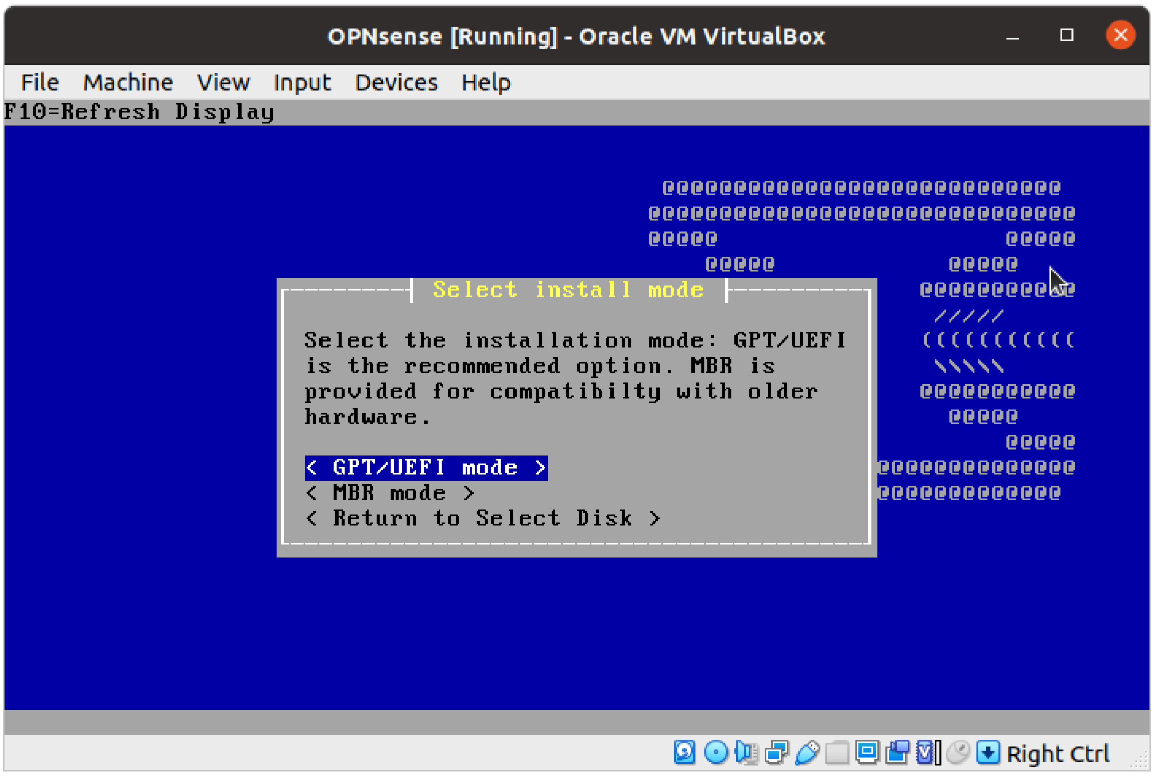
```
F10=Refresh Display

Select a Disk

This will automatically install OPNsense
with all current settings without asking
many questions.

WARNING: All contents of the selected
hard disk will be erased! This action is
irreversible.

Please select a disk to continue:

< ada0: 16902MB (34616832 512 byte sectors) >
< Return to Select Task >
```

Figure 20. *Select disk for OPNsense installation*

You will be asked to select a disk. Select the disk fie to create VBox on it.

⚠️ **WARNING**

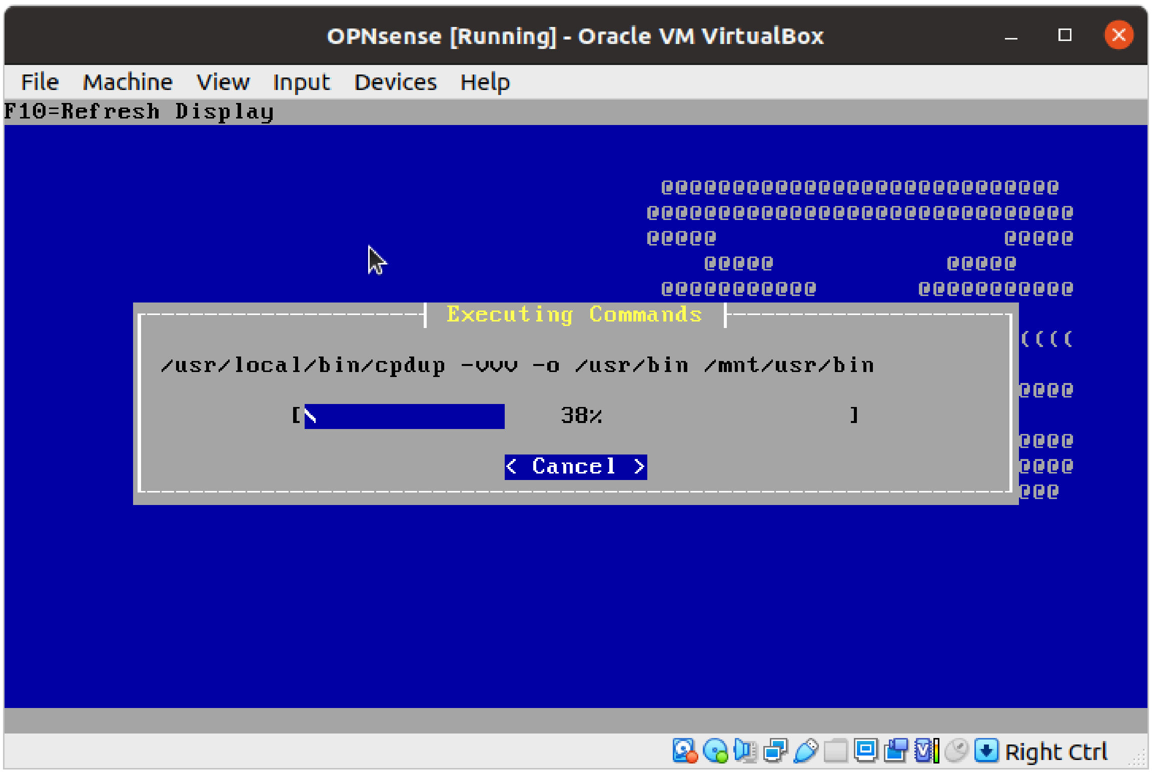
All contents of the selected hard disk will be erased. This action is irreversible.


OPNsense [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
F10=Refresh Display
Right Ctrl

```
Select install mode

Select the installation mode: GPT/UEFI
is the recommended option. MBR is
provided for compatibilty with older
hardware.

< GPT/UEFI mode >
< MBR mode >
< Return to Select Disk >
```

Figure 21. *Select Install Mode on OPNsense*

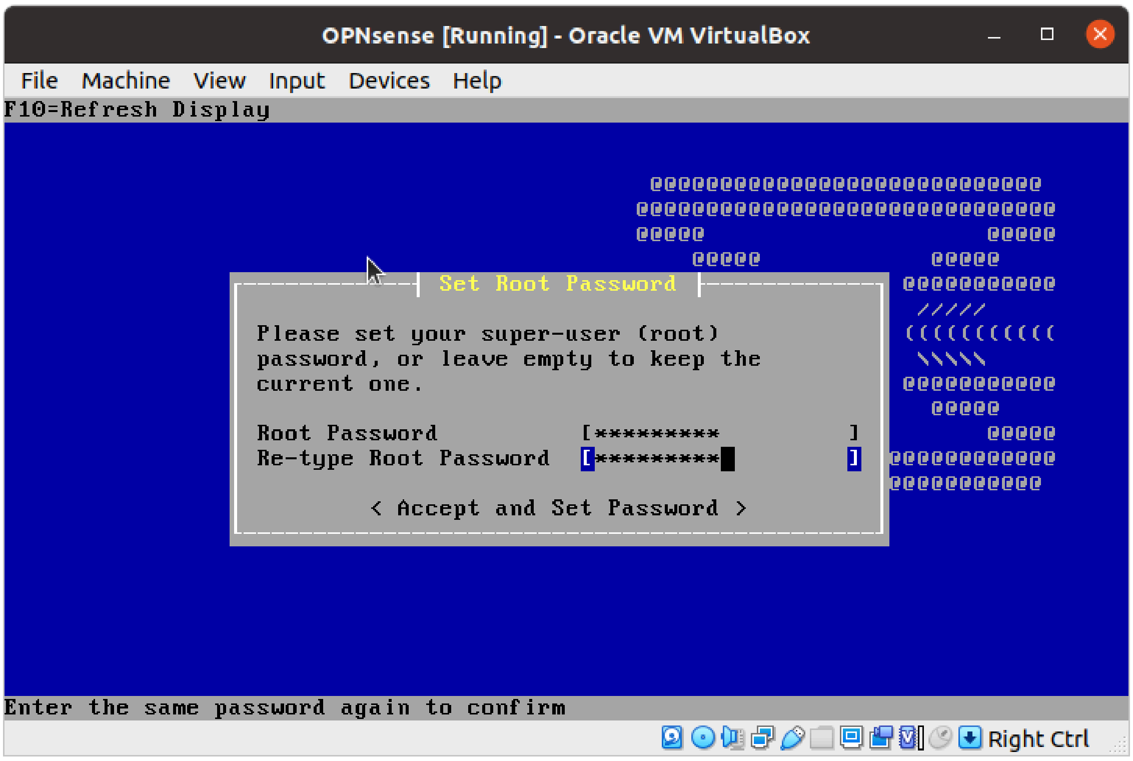
Select the **installation mode** as **GPT/UEFI mode**.


OPNsense [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
F10=Refresh Display
Right Ctrl

```
Executing Commands

/usr/local/bin/cpdup -vvv -o /usr/bin /mnt/usr/bin

[\             38%              ]

< Cancel >
```

Figure 22. *OPNsense installation - Executing Commands*

VBox will start to execute commands. This process can take up to a few minutes according to your Virtual Machine resources.



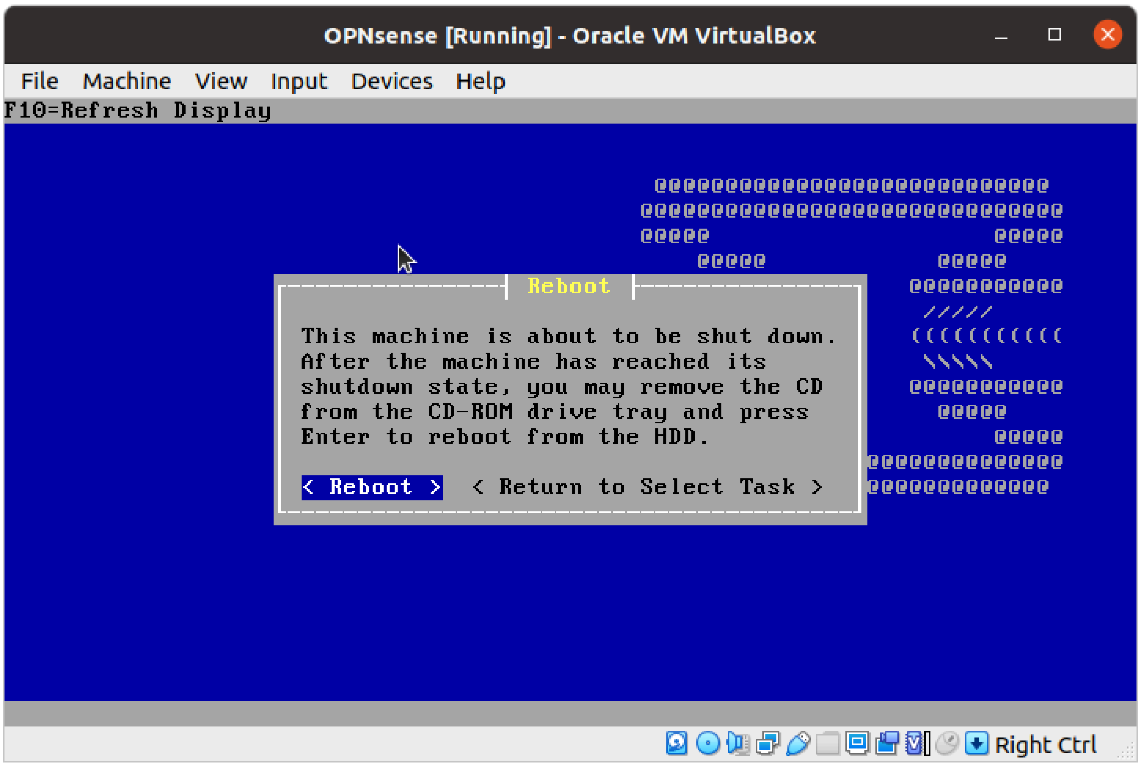
OPNsense [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Right Ctrl

```
F10=Refresh Display

Set Root Password

Please set your super-user (root)
password, or leave empty to keep the
current one.

Root Password           [**********        ]
Re-type Root Password   [**********        ]

        < Accept and Set Password >

Enter the same password again to confirm
```

Figure 23. *Change OPNsense root password*

When command execution is finished you will be asked to change the default password (opnsense).

You can change it now or you can continue by selecting **Accept** and **Set Password**.

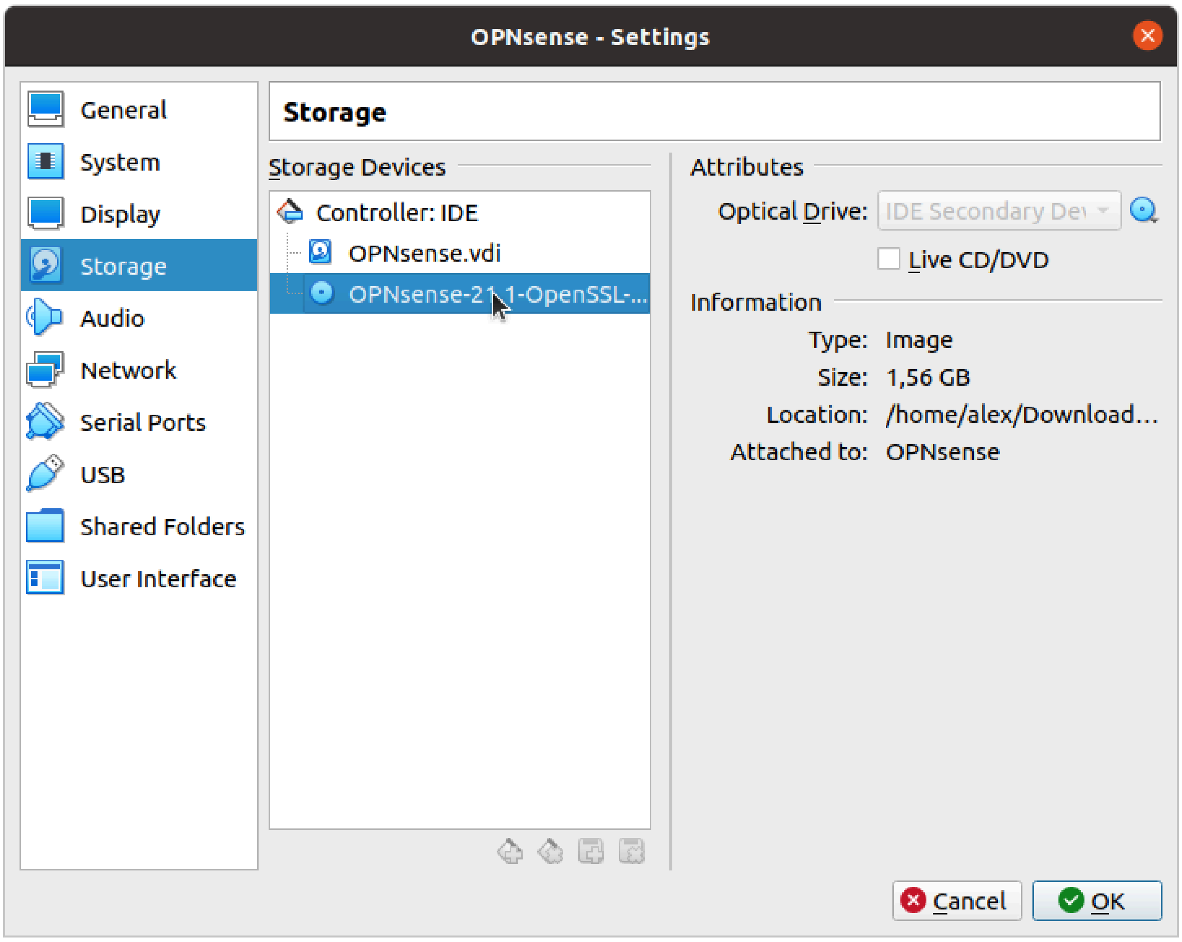


OPNsense [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Right Ctrl

```
F10=Refresh Display

Reboot

This machine is about to be shut down.
After the machine has reached its
shutdown state, you may remove the CD
from the CD-ROM drive tray and press
Enter to reboot from the HDD.

< Reboot >   < Return to Select Task >
```

Figure 24. *OPNsense Installation completed.Reboot*

While it is rebooting you should eject the DVD from VirtualBox. To prevent booting from a live cd you need to eject the disk immediately after clicking reboot.



Storage

Storage Devices

Controller: IDE
OPNsense.vdi
OPNsense-21.1-OpenSSL-...

Attributes

Optical Drive: IDE Secondary Dev

□ Live CD/DVD

Information

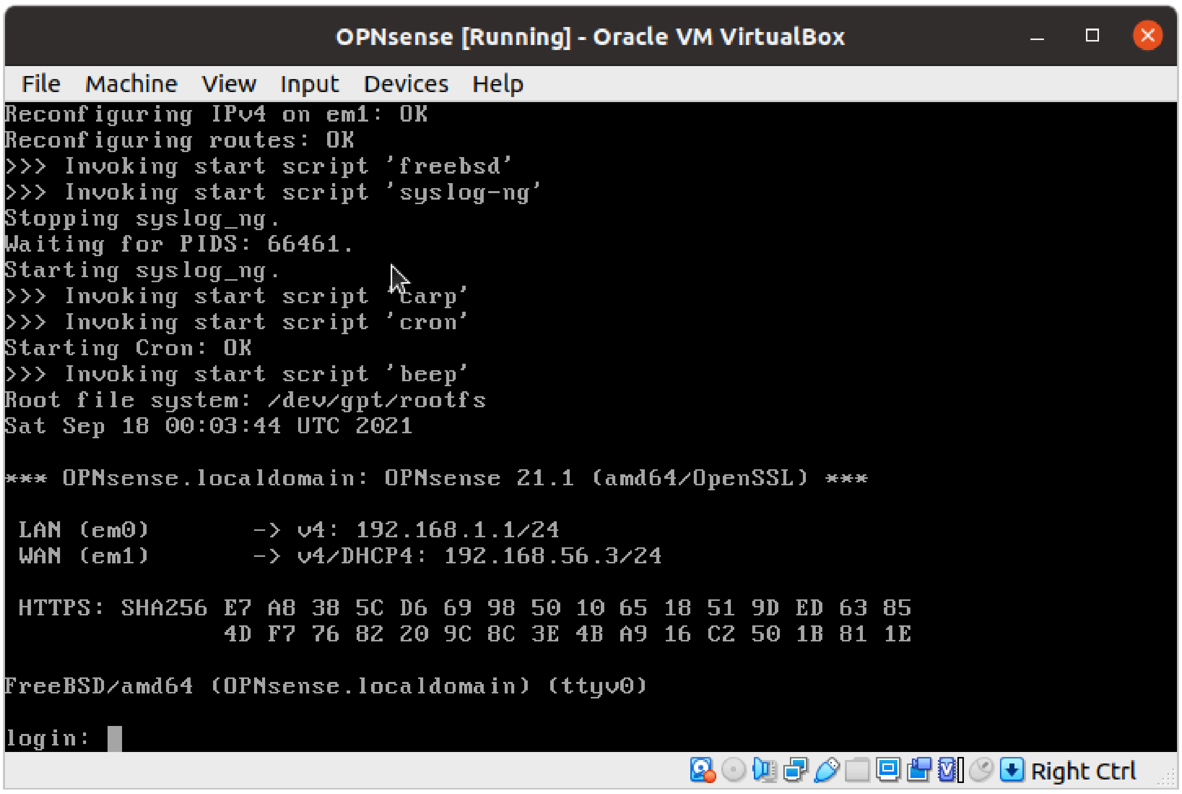
Type: Image
Size: 1,56 GB
Location: /home/alex/Download...
Attached to: OPNsense

Figure 25. *Remove Disk from VirtualBox*

Through **Attributes** Menu, click **Optical Drive** Icon and select **Remove Disk** from Virtual Machine.

Initial Configuration of OPNsense Firewall

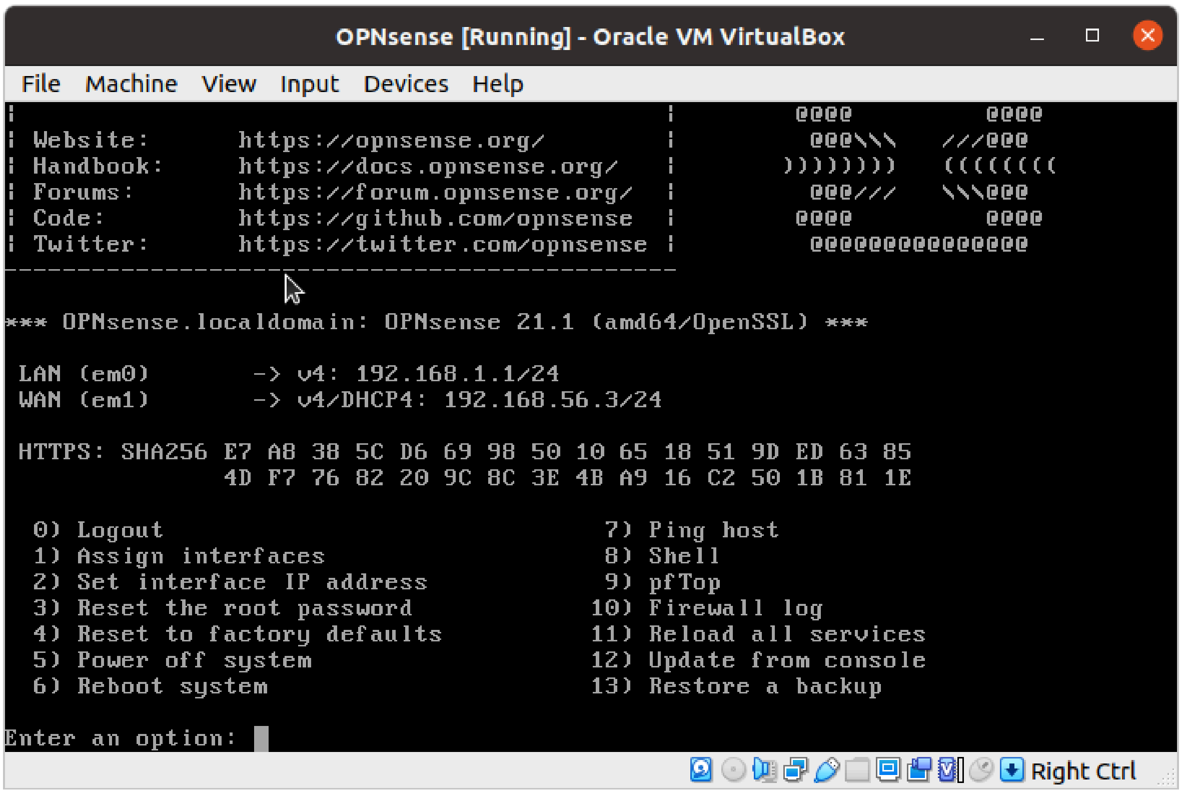
After reboot, you can login as root with the default password (**opnsense**) if you haven't changed it during installation.


OPNsense [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Right Ctrl

```
Reconfiguring IPv4 on em1: OK
Reconfiguring routes: OK
>>> Invoking start script 'freebsd'
>>> Invoking start script 'syslog-ng'
Stopping syslog_ng.
Waiting for PIDS: 66461.
Starting syslog_ng.
>>> Invoking start script 'carp'
>>> Invoking start script 'cron'
Starting Cron: OK
>>> Invoking start script 'beep'
Root file system: /dev/gpt/rootfs
Sat Sep 18 00:03:44 UTC 2021

*** OPNsense.localdomain: OPNsense 21.1 (amd64/OpenSSL) ***

 LAN (em0)        -> v4: 192.168.1.1/24
 WAN (em1)        -> v4/DHCP4: 192.168.56.3/24

 HTTPS: SHA256 E7 A8 38 5C D6 69 98 50 10 65 18 51 9D ED 63 85
               4D F7 76 82 20 9C 8C 3E 4B A9 16 C2 50 1B 81 1E

FreeBSD/amd64 (OPNsense.localdomain) (ttyv0)

login:
```

Figure 26. *Login as root after installation*

OPNsense menu will welcome you after login.


OPNsense [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Right Ctrl

```
|                                              |        @@@@         @@@@
| 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 21.1 (amd64/OpenSSL) ***

 LAN (em0)        -> v4: 192.168.1.1/24
 WAN (em1)        -> v4/DHCP4: 192.168.56.3/24

 HTTPS: SHA256 E7 A8 38 5C D6 69 98 50 10 65 18 51 9D ED 63 85
               4D F7 76 82 20 9C 8C 3E 4B A9 16 C2 50 1B 81 1E

  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 27. *Opnsense Menu*

Now, we have to set the interfaces and IP addresses.

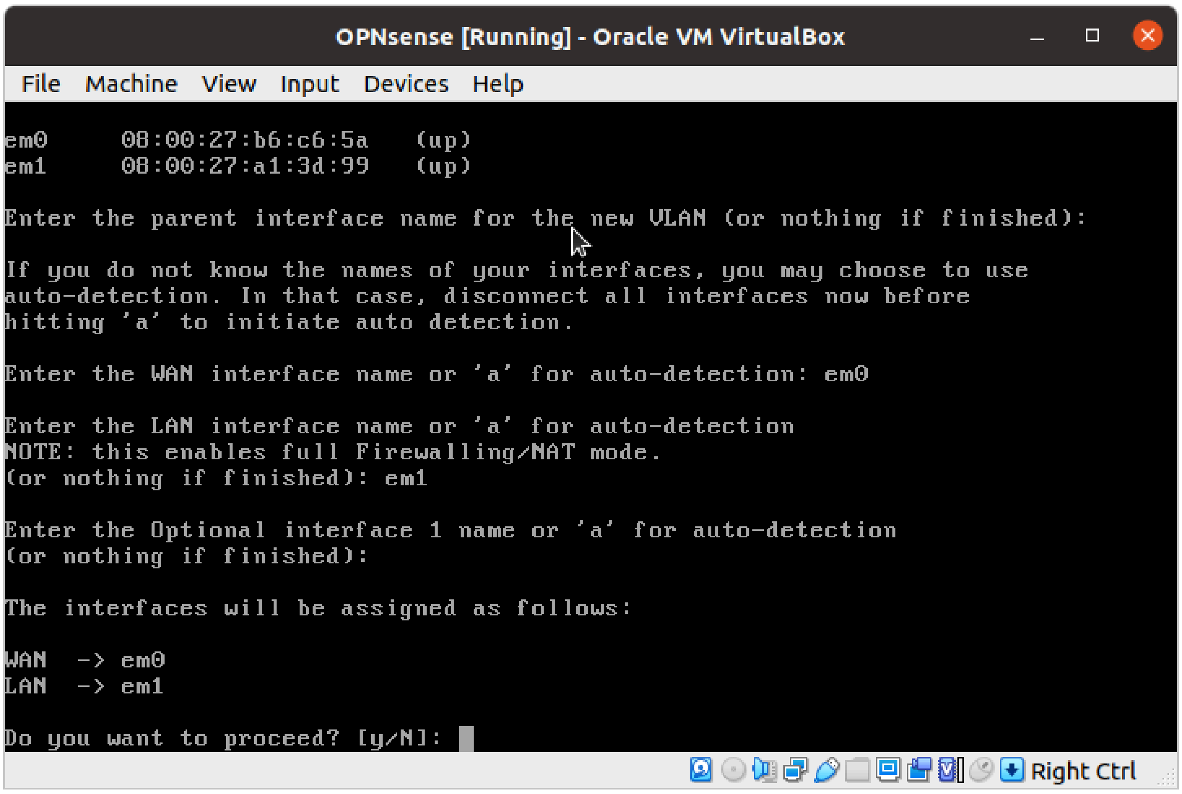
Enter an option: 1

Then click **Enter**

Change the interfaces if they are not properly detected.

For **WAN** interface **em0**

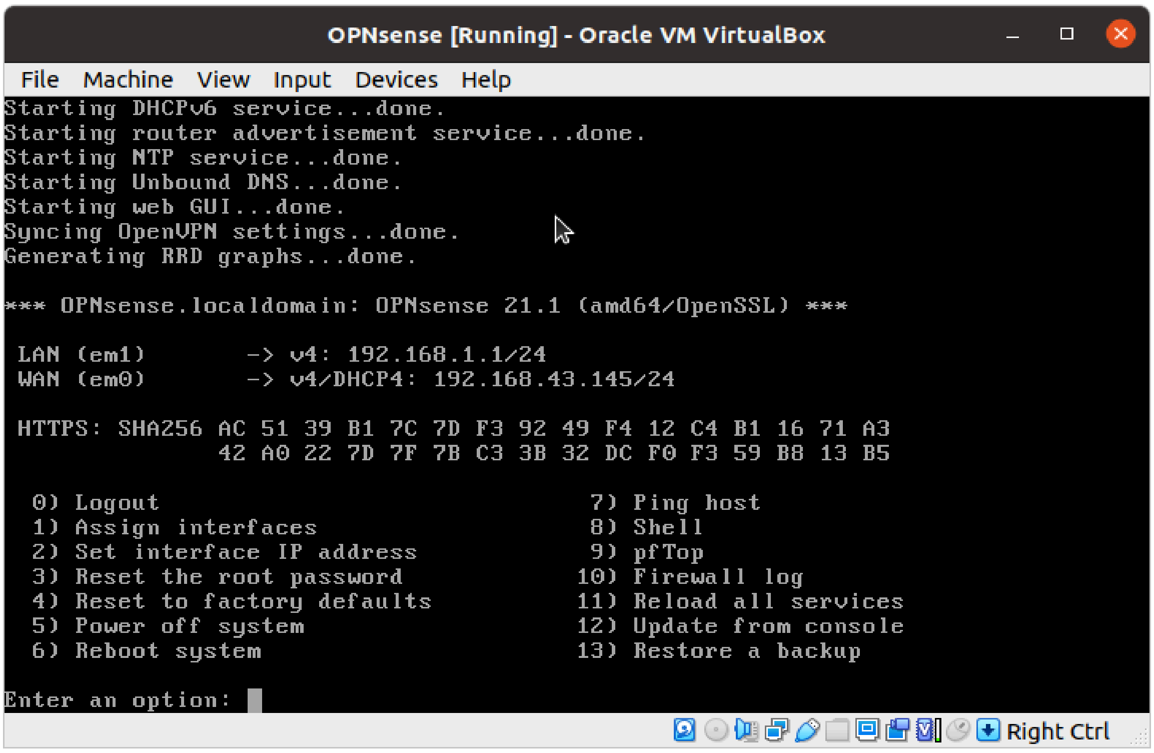
For **LAN** interface **em1**


OPNsense [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Right Ctrl

```
em0     08:00:27:b6:c6:5a    (up)
em1     08:00:27:a1:3d:99    (up)

Enter the parent interface name for the new VLAN (or nothing if finished):

If you do not know the names of your interfaces, you may choose to use
auto-detection. In that case, disconnect all interfaces now before
hitting 'a' to initiate auto detection.

Enter the WAN interface name or 'a' for auto-detection: em0

Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(or nothing if finished): em1

Enter the Optional interface 1 name or 'a' for auto-detection
(or nothing if finished):

The interfaces will be assigned as follows:

WAN  -> em0
LAN  -> em1

Do you want to proceed? [y/N]:
```

Figure 28. *Network Interface assignments on OPNsense*

Do you want to proceed [y/N]: y

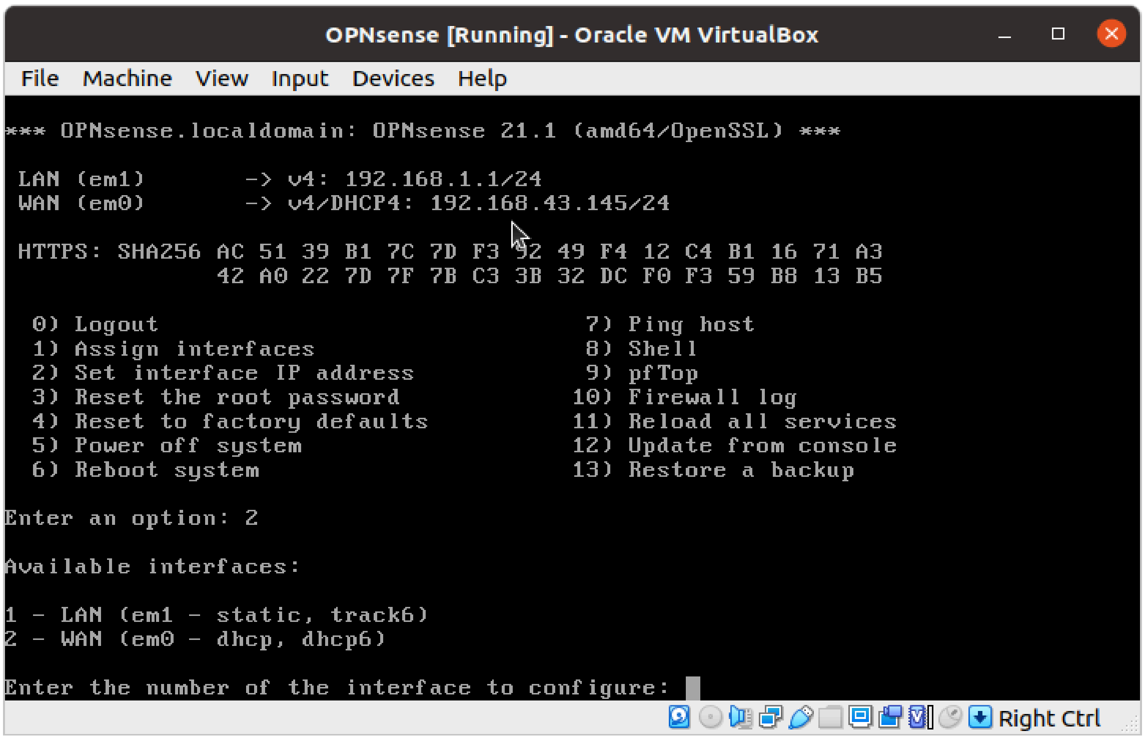


```
Starting DHCPv6 service...done.
Starting router advertisement service...done.
Starting NTP service...done.
Starting Unbound DNS...done.
Starting web GUI...done.
Syncing OpenVPN settings...done.
Generating RRD graphs...done.

*** OPNsense.localdomain: OPNsense 21.1 (amd64/OpenSSL) ***

 LAN (em1)       -> v4: 192.168.1.1/24
 WAN (em0)       -> v4/DHCP4: 192.168.43.145/24

 HTTPS: SHA256 AC 51 39 B1 7C 7D F3 92 49 F4 12 C4 B1 16 71 A3
               42 A0 22 7D 7F 7B C3 3B 32 DC F0 F3 59 B8 13 B5

  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 29. *Enter 2 to set IP Address*

Now we can set IP addresses.

```
Enter an option: 2
```



```
*** OPNsense.localdomain: OPNsense 21.1 (amd64/OpenSSL) ***

 LAN (em1)       -> v4: 192.168.1.1/24
 WAN (em0)       -> v4/DHCP4: 192.168.43.145/24

 HTTPS: SHA256 AC 51 39 B1 7C 7D F3 92 49 F4 12 C4 B1 16 71 A3
               42 A0 22 7D 7F 7B C3 3B 32 DC F0 F3 59 B8 13 B5

  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: 2

Available interfaces:

1 - LAN (em1 - static, track6)
2 - WAN (em0 - dhcp, dhcp6)

Enter the number of the interface to configure:
```

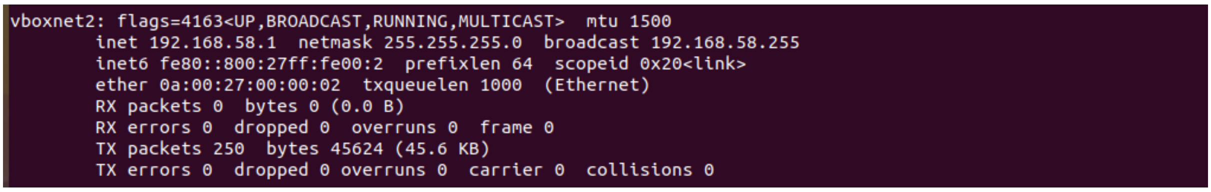
Figure 30. *Interface configuration*

Enter the number of the interface to configure:1

For LAN interface don't set DHCP

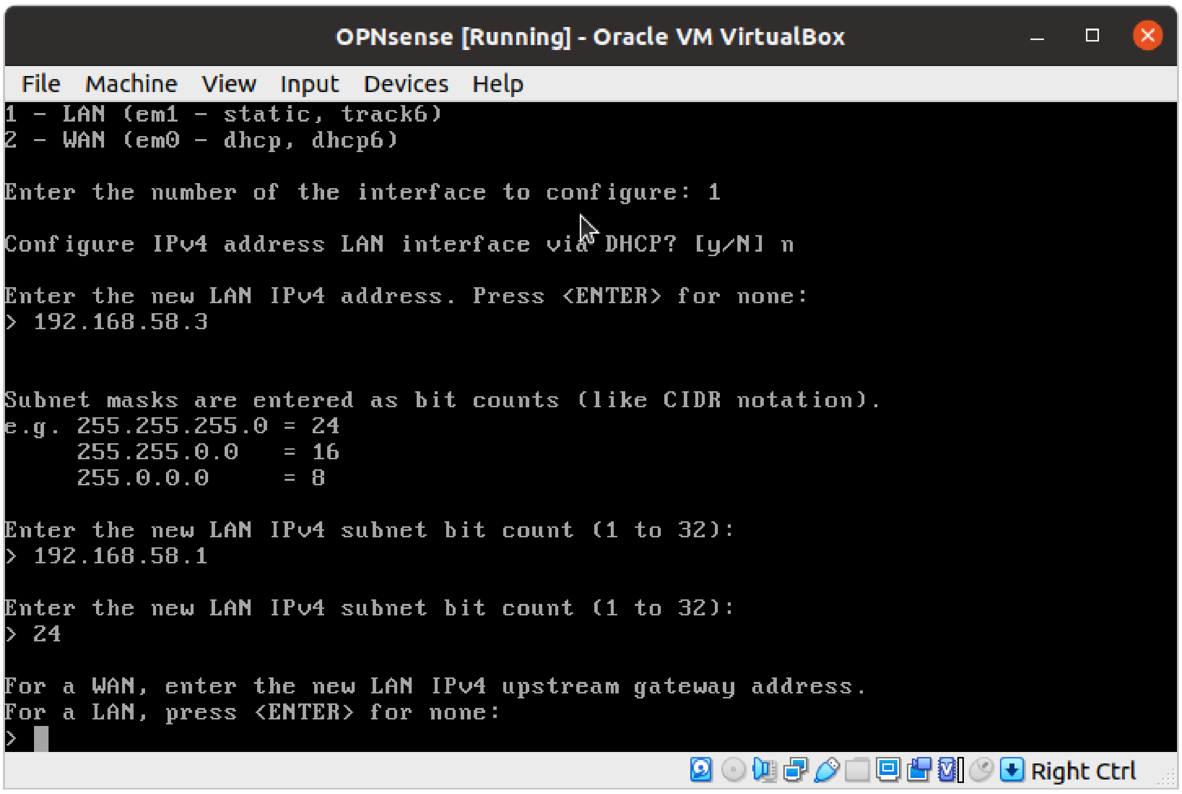
Configure IPv4 address LAN interface via DHCP [y/N] N

Our host-only adapter is using vboxnet2 then we need to give a static IP address from that IP block.



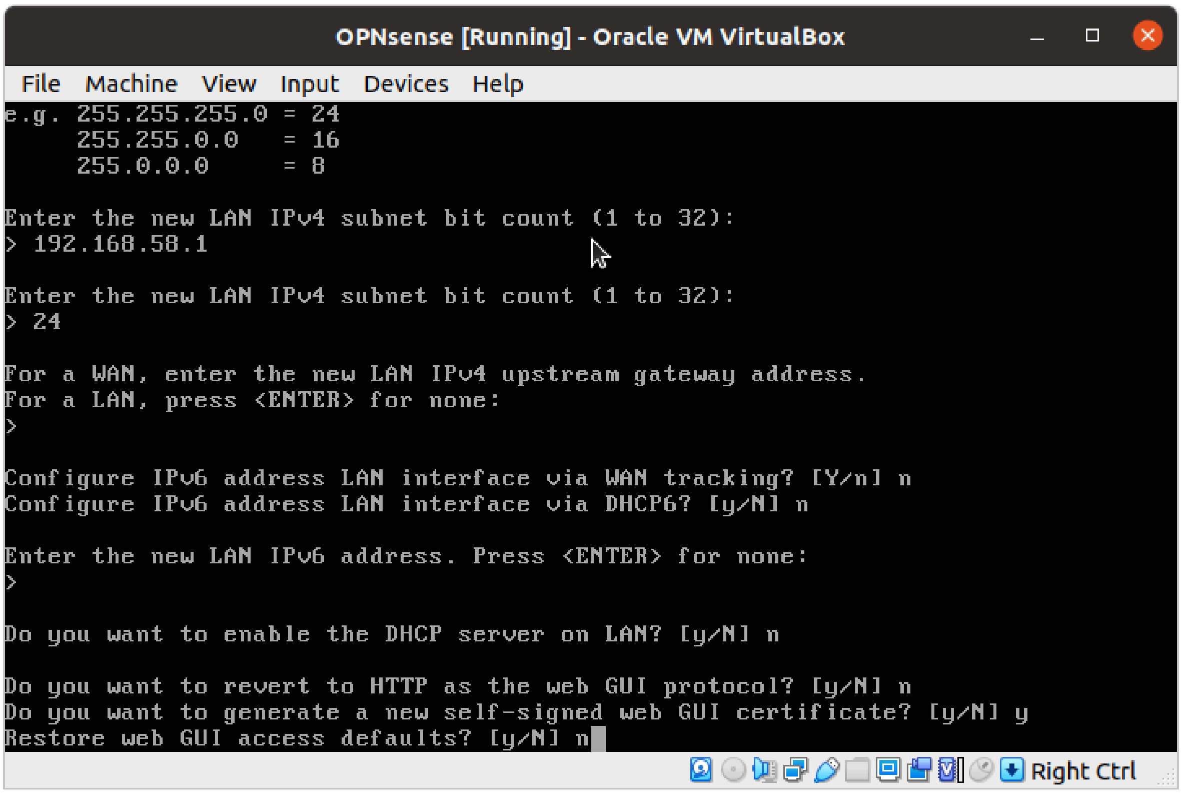
```
vboxnet2: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.58.1  netmask 255.255.255.0  broadcast 192.168.58.255
        inet6 fe80::800:27ff:fe00:2  prefixlen 64  scopeid 0x20<link>
        ether 0a:00:27:00:00:02  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 250  bytes 45624 (45.6 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Figure 31. *Host-only adapter interface*



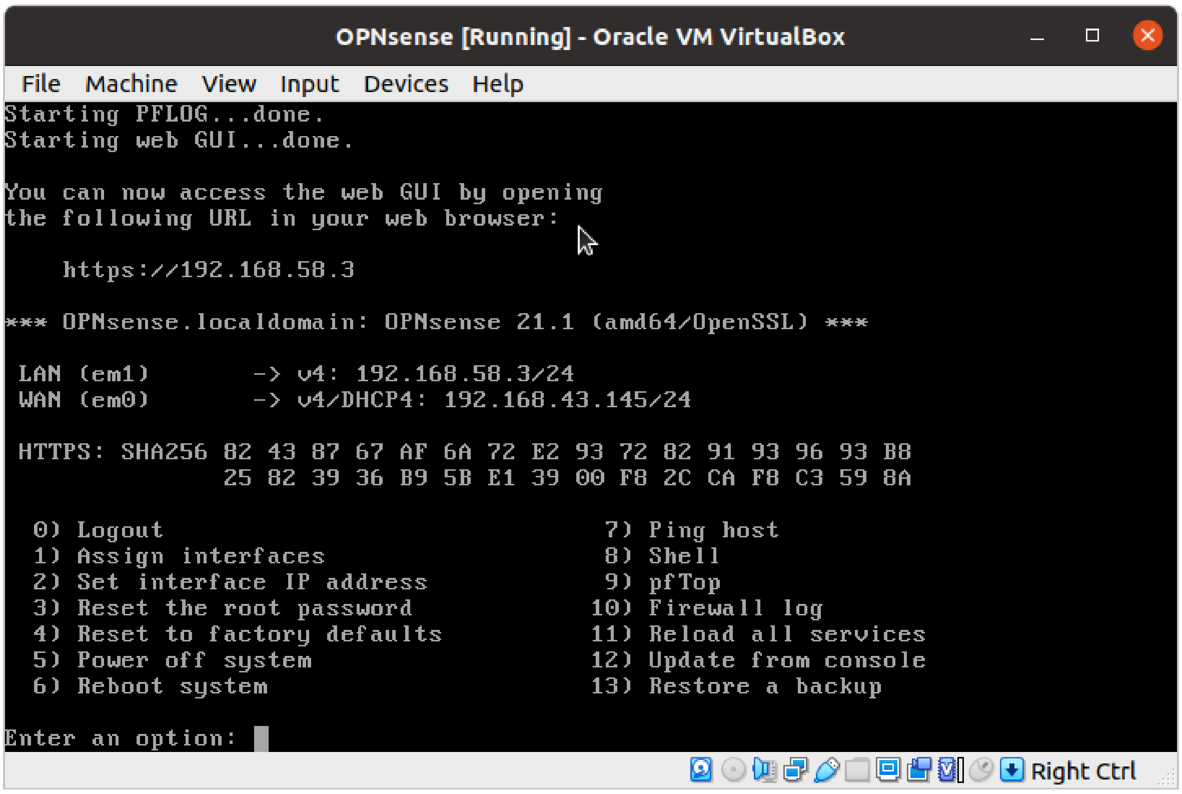
```
1 - LAN (em1 - static, track6)
2 - WAN (em0 - dhcp, dhcp6)

Enter the number of the interface to configure: 1

Configure IPv4 address LAN interface via DHCP? [y/N] n

Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.58.3


Subnet masks are entered as bit counts (like CIDR notation).
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new LAN IPv4 subnet bit count (1 to 32):
> 192.168.58.1

Enter the new LAN IPv4 subnet bit count (1 to 32):
> 24

For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>
```

Figure 32. *LAN Interface Settings...*


OPNsense [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Right Ctrl

```
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new LAN IPv4 subnet bit count (1 to 32):
> 192.168.58.1

Enter the new LAN IPv4 subnet bit count (1 to 32):
> 24

For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Configure IPv6 address LAN interface via WAN tracking? [Y/n] n
Configure IPv6 address LAN interface via DHCP6? [y/N] n

Enter the new LAN IPv6 address. Press <ENTER> for none:
>

Do you want to enable the DHCP server on LAN? [y/N] n

Do you want to revert to HTTP as the web GUI protocol? [y/N] n
Do you want to generate a new self-signed web GUI certificate? [y/N] y
Restore web GUI access defaults? [y/N] n
```

Figure 33. *LAN Interface Settings*


OPNsense [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Right Ctrl

```
Starting PFLOG...done.
Starting web GUI...done.

You can now access the web GUI by opening
the following URL in your web browser:

    https://192.168.58.3

*** OPNsense.localdomain: OPNsense 21.1 (amd64/OpenSSL) ***

 LAN (em1)       -> v4: 192.168.58.3/24
 WAN (em0)       -> v4/DHCP4: 192.168.43.145/24

 HTTPS: SHA256 82 43 87 67 AF 6A 72 E2 93 72 82 91 93 96 93 B8
               25 82 39 36 B9 5B E1 39 00 F8 2C CA F8 C3 59 8A

  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 34. *You can now access the web GUI by opening LAN IP address*

Type the LAN IP address of the Virtual Opnsense machine on your browser.

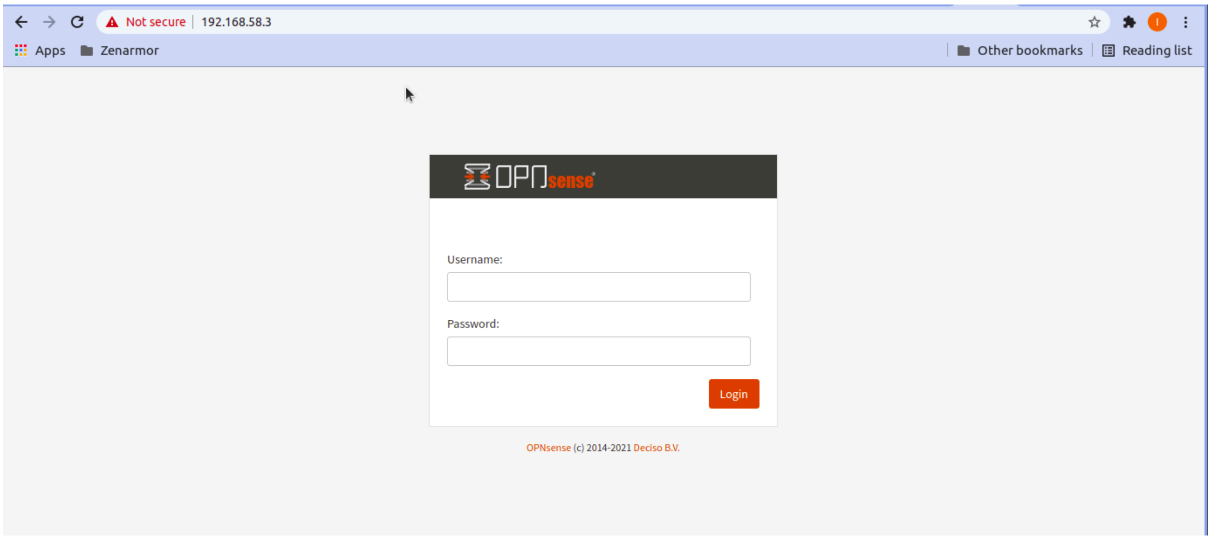
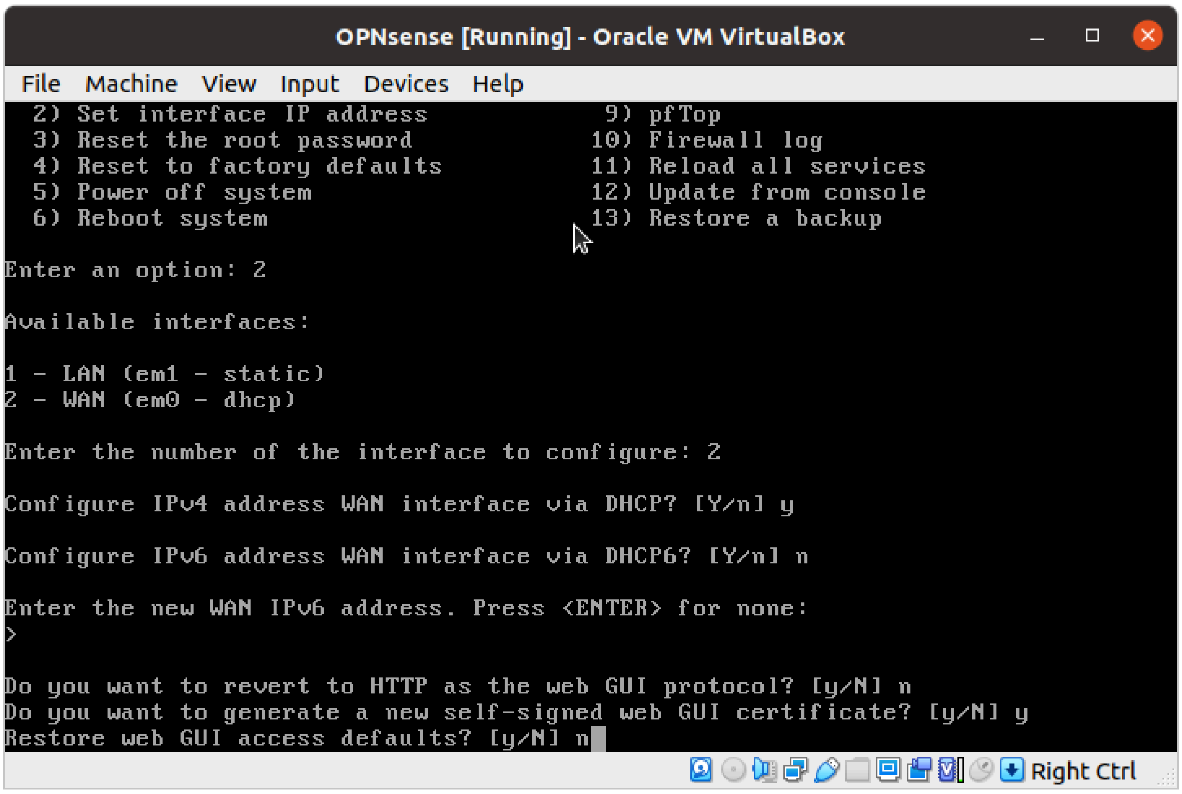


Figure 35. *OPNsense Login Page*

```
Username:root

Password:opnsense (if not changed)
```

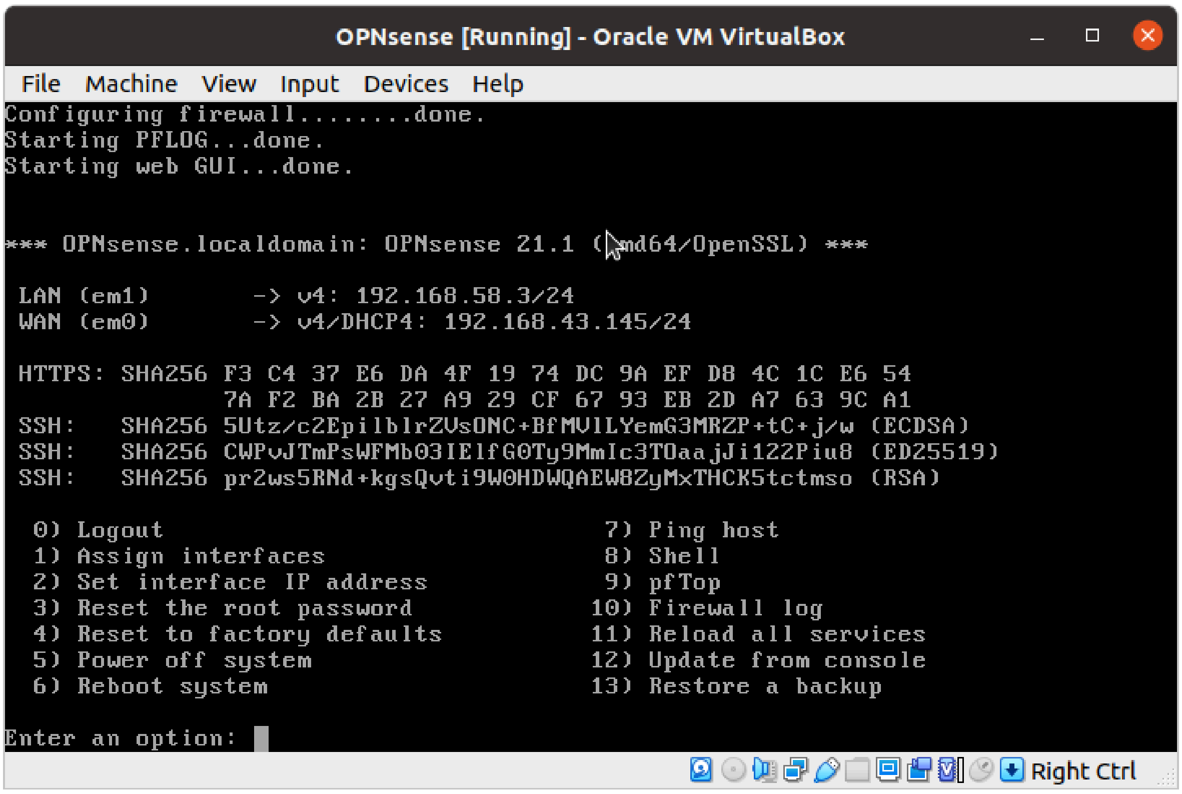
You can set the WAN interface now.

```
Configure IPv4 address WAN interface via DHCP? [y/N] y

Configure IPv6 address WAN interface via DHCP? [y/N] n

Enter for IPv6 Address

Do you want to revert to HTTP as the web GUI protocol? n

Do you want to generate a new self-signed GUI certificate? [y/N] y

Restore web GUI access defaults? [y/N] n
```


OPNsense [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Right Ctrl

```
  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: 2

Available interfaces:

1 - LAN (em1 - static)
2 - WAN (em0 - dhcp)

Enter the number of the interface to configure: 2

Configure IPv4 address WAN interface via DHCP? [Y/n] y

Configure IPv6 address WAN interface via DHCP6? [Y/n] n

Enter the new WAN IPv6 address. Press <ENTER> for none:
>

Do you want to revert to HTTP as the web GUI protocol? [y/N] n
Do you want to generate a new self-signed web GUI certificate? [y/N] y
Restore web GUI access defaults? [y/N] n
```

Figure 36. *WAN interface settings*


OPNsense [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Right Ctrl

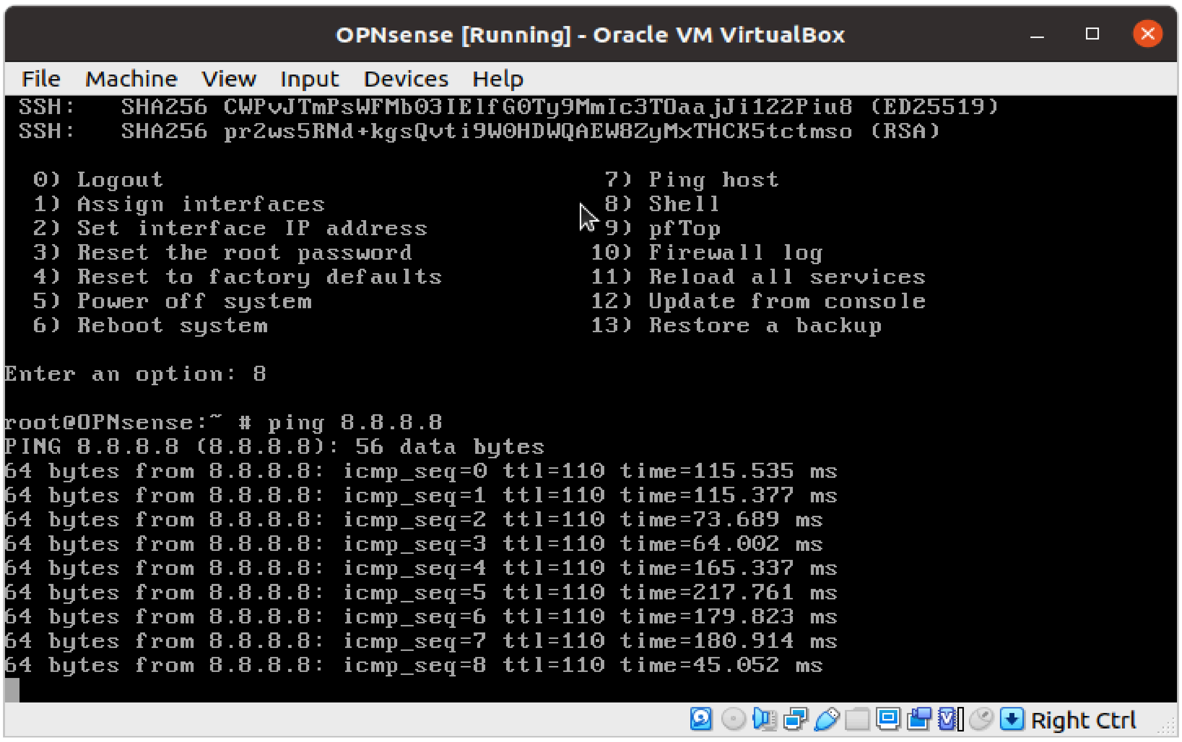
```
Configuring firewall.......done.
Starting PFLOG...done.
Starting web GUI...done.


*** OPNsense.localdomain: OPNsense 21.1 (amd64/OpenSSL) ***

 LAN (em1)       -> v4: 192.168.58.3/24
 WAN (em0)       -> v4/DHCP4: 192.168.43.145/24

 HTTPS: SHA256 F3 C4 37 E6 DA 4F 19 74 DC 9A EF D8 4C 1C E6 54
               7A F2 BA 2B 27 A9 29 CF 67 93 EB 2D A7 63 9C A1
 SSH:   SHA256 5Utz/c2EpilblrZVsONC+BfMVlLYemG3MRZP+tC+j/w (ECDSA)
 SSH:   SHA256 CWPvJTmPsWFMb03IElfG0Ty9MmIc3TOaajJi122Piu8 (ED25519)
 SSH:   SHA256 pr2ws5RNd+kgsQvti9W0HDWQAEW8ZyMxTHCK5tctmso (RSA)

  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 37. *OPNsense Shell command*

Interface and IP addresses configured

Lest test to ping the google by using menu 8.

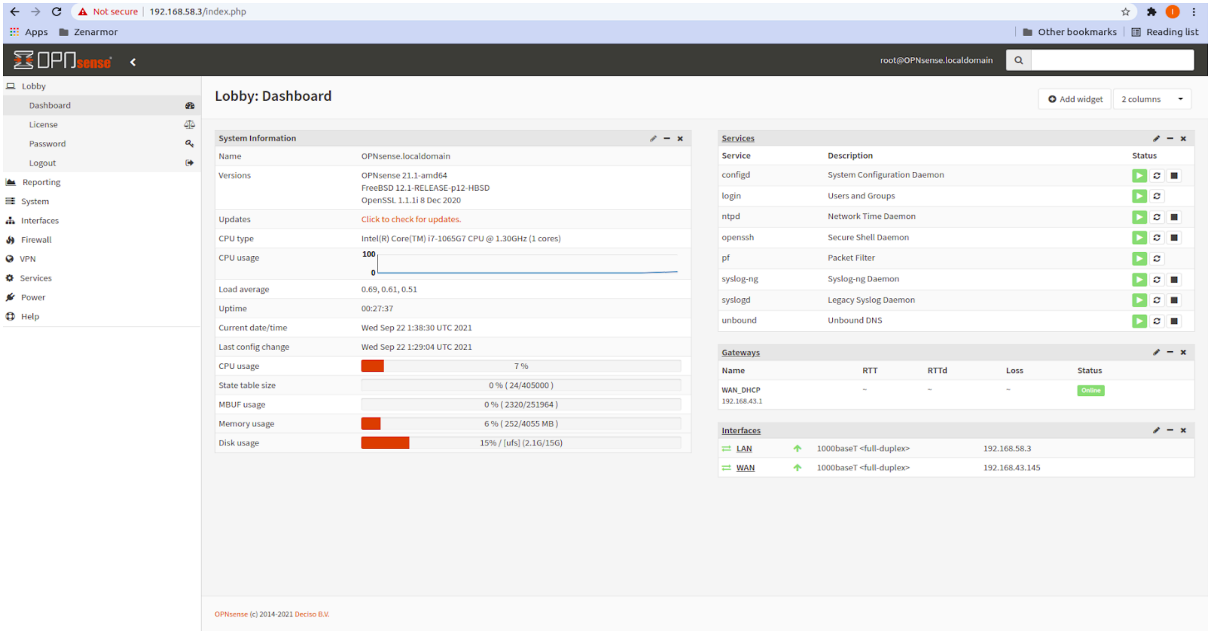
Enter an option 8


OPNsense [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Right Ctrl

```
SSH:    SHA256 CWPvJTmPsWFMb03IElfG0Ty9MmIc3TOaajJi122Piu8 (ED25519)
SSH:    SHA256 pr2ws5RNd+kgsQvti9WOHDWQAEW8ZyMxTHCK5tctmso (RSA)

  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: 8

root@OPNsense:~ # ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: icmp_seq=0 ttl=110 time=115.535 ms
64 bytes from 8.8.8.8: icmp_seq=1 ttl=110 time=115.377 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=110 time=73.689 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=110 time=64.002 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=110 time=165.337 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=110 time=217.761 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=110 time=179.823 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=110 time=180.914 ms
64 bytes from 8.8.8.8: icmp_seq=8 ttl=110 time=45.052 ms
```

Figure 38. *Check internet connection of OPNsense*

If ping works, congratulations you have successfully created your VİrtualBox OPNsense machine. You can update your VBox from GUI or by using menu 12 now.



Lobby: Dashboard

System Information

Name	OPNsense.localdomain
Versions	OPNsense 21.1-amd64 FreeBSD 12.1-RELEASE-p12-HBSD OpenSSL 1.1.1i 8 Dec 2020
Updates	Click to check for updates.
CPU type	Intel(R) Core(TM) i7-1065G7 CPU @ 1.30GHz (1 cores)
CPU usage	100 0
Load average	0.69, 0.61, 0.51
Uptime	00:27:37
Current date/time	Wed Sep 22 1:38:30 UTC 2021
Last config change	Wed Sep 22 1:29:04 UTC 2021
CPU usage	7 %
State table size	0 % (24/405000)
MBUF usage	0 % (2320/251964)
Memory usage	6 % (252/4055 MB)
Disk usage	15% / [ufs] (2.1G/15G)

Services

Service	Description	Status
configd	System Configuration Daemon	▶ ⟳ ■
login	Users and Groups	▶ ⟳
ntpd	Network Time Daemon	▶ ⟳ ■
openssh	Secure Shell Daemon	▶ ⟳ ■
pf	Packet Filter	▶ ⟳
syslog-ng	Syslog-ng Daemon	▶ ⟳ ■
syslogd	Legacy Syslog Daemon	▶ ⟳ ■
unbound	Unbound DNS	▶ ⟳ ■

Gateways

Name	RTT	RTTd	Loss	Status
WAN_DHCP 192.168.43.1	~	~	~	Online

Interfaces

LAN	↑	1000baseT <full-duplex>	192.168.58.3
WAN	↑	1000baseT <full-duplex>	192.168.43.145

OPNsense (c) 2014-2021 Deciso B.V.

Figure 39. *OPNsense Dashboard*

You can find more information about accessing the OPNsense Web GUI and initial configuration of the OPNsense firewall on the OPNsense Installation on Proxmox VE Tutorial.

It is strongly recommended to update the OPNsense firewall after completing the installation. Please, refer to How to Update OPNsense article written by Zenarmor.

Lastly, it may be helpful for you to read the How to Configure the OPNsense Firewall Rules article to protect your network infrastructure.

How to Configure VLANs on OPNsense

VLANs, or Virtual Local Area Networks, are a crucial concept in modern network management. They enable the creation of logically separate networks within a single physical network infrastructure, akin to having multiple isolated networks without the need for extra hardware.

There are many benefits to using VLANs. They improve network performance through effective traffic management, increase security by isolating sensitive data, and streamline network administration. VLANs encourage scalability and flexibility as well, enabling enterprises to modify their networks as necessary.

OPNsense is a strong network firewall solution that includes VLAN capabilities. It improves network efficiency and offers a strong defense against potential attacks by making it simple for network managers to establish, monitor, and secure VLANs.

You may create and configure the VLAN interface on your OPNsense node easily by following the 5 main steps:

1. Preparing the Network Environment
2. Creating VLANs in OPNsense
3. Configuring VLAN Interfaces
4. Configuring Firewall Rules for VLANs
5. Testing the VLAN Configuration

1. Preparing the Network Environment

Examining your network hardware and topology is crucial before getting started with OPNsense's VLAN configuration. Decide which network switches, routers and other components are in your configuration. Determining how VLANs might be strategically utilized to improve network segmentation and management will depend on understanding the physical configuration.

The next step is choosing which interfaces will be used for your LAN and WAN connections, respectively. The LAN interface connects to the internal network devices, whereas the WAN interface connects to the external Internet, often through a modem or router. Consider using distinct physical network ports or adapters for each interface for best performance.

Set aside one interface for WAN and at least one other interface for LAN in the recommended interface configuration. The easiest way to preserve network segregation and boost security is to have distinct interfaces for WAN and LAN, even though it is possible to use a single interface for both. The risk of potential conflicts is lower because of this design, which allows for a more seamless data flow.

By carefully assessing your network hardware, identifying appropriate interfaces, and following the recommended configuration, you lay the groundwork for configuring VLANs in OPNsense effectively. This preparation ensures that your network is ready to leverage the advantages of VLANs, such as improved security, traffic management, and network scalability.

2. Creating VLANs in OPNsense

Several steps are required to configure VLANs (virtual local area networks) on OPNsense. VLANs enable the segmentation of a physical network infrastructure into virtual networks. A basic overview of OPNsense VLAN configuration is provided below. You may add new VLAN interface on your OPNsense node easily by following the 5 main steps:

1. Accessing the **OPNsense Web User Interface**
2. Navigating to "**Interfaces > Other Types > VLAN**"
3. Adding a **New VLAN**
4. Selecting the **Parent Interface and Configuring VLAN Tagging**
5. Assigning **Logical Interfaces** to the VLAN

1. Accessing the OPNsense Web User Interface

To begin configuring VLAN settings in OPNsense, you must first access the web-based user interface by following the next steps:

1. Launch your preferred web browser and enter the OPNsense IP address or hostname in the address bar.

2. Log in with your administrator credentials to access the OPNsense web interface.

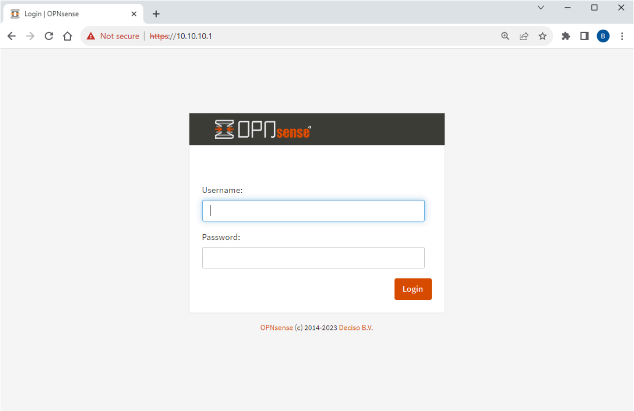

Login | OPNsense
Not secure | https://10.10.10.1
OPNsense
Username:
Password:
Login
OPNsense (c) 2014-2023 Deciso B.V.

Figure 1. *OPNsense Login page*

2. Navigating to "Interfaces > Other Types > VLAN"

After you have accessed the OPNsense web interface, follow these steps to get to the VLAN configuration section:

1. Navigate to the "**Interfaces**" section in the top menu.
2. Select "**Other Types**" from the drop-down menu.
3. Choose "**VLAN**" from the sub-menu.

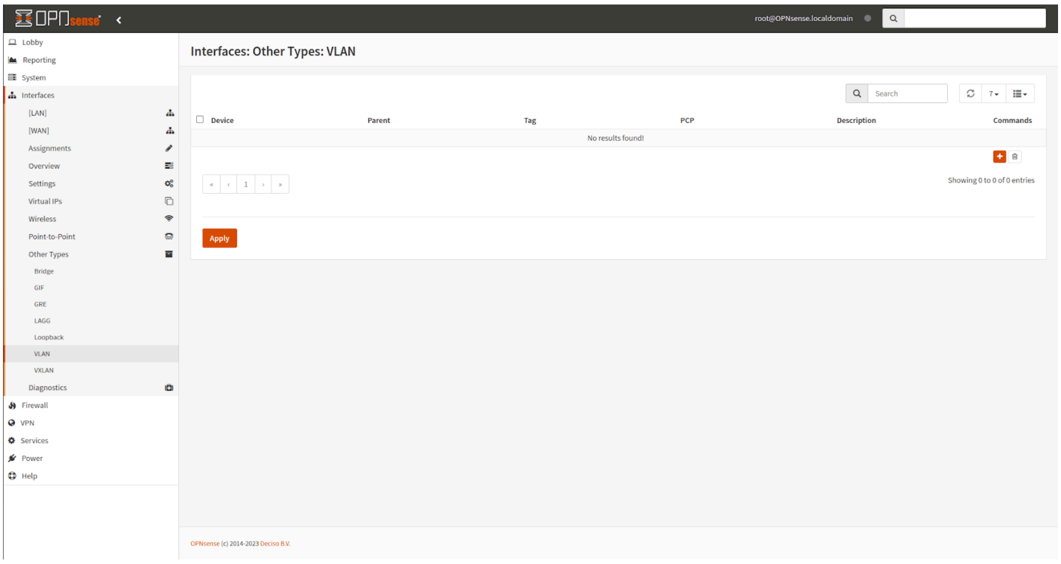


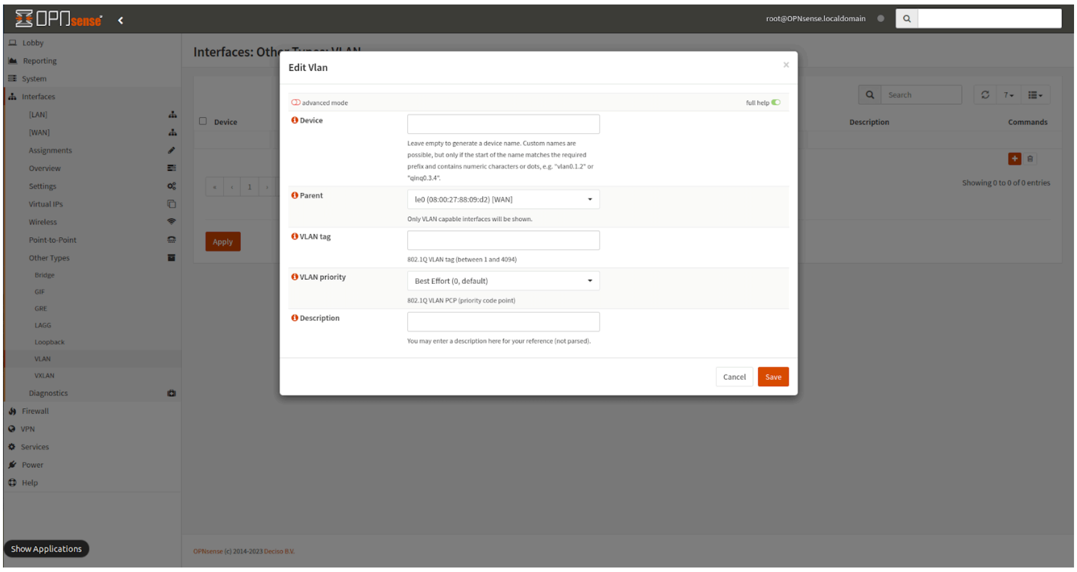
Figure 2. *VLAN Interfaces on OPNsense*

3. Adding a New VLAN

On OPNsense, adding new VLANs is a simple process that allows you to create virtual LANs for efficient traffic management and network segmentation. In order to create a new VLAN, you may continue to follow next steps:

1. Click on the "**Add**" button.

2. Provide a **descriptive name** for the VLAN to aid in identification. The description is optional.



Edit Vlan

Device: Leave empty to generate a device name. Custom names are possible, but only if the start of the name matches the required prefix and contains numeric characters or dots, e.g. "vlan0.1.2" or "qinq0.3.4".

Parent: le0 (08:00:27:88:09:d2) [WAN]
Only VLAN capable interfaces will be shown.

VLAN tag: 802.1Q VLAN tag (between 1 and 4094)

VLAN priority: Best Effort (0, default)
802.1Q VLAN PCP (priority code point)

Description: You may enter a description here for your reference (not parsed).

Figure 3. Adding VLAN Interface on OPNsense*

4. Selecting the Parent Interface and Configuring VLAN Tagging

The first step in creating a new VLAN in OPNsense is to choose the parent interface to which the VLAN will be connected. The **physical interface** that will carry the **VLAN-tagged traffic** is known as the **parent interface**. Here are the steps for selecting the parent interface and Configuring the VLAN Tagging.

1. Choose the **parent interface** from the available physical ports where the VLAN should reside.
2. Specify a **tag number** (other than 1) to differentiate the VLAN traffic from other networks.
3. Set the **VLAN priority** if necessary for **quality of service (QoS)** purposes.OPNsense supports 8 different VLAN priority types:
   i. ***Best Effort (0, default)***: This is the default priority. Traffic with this priority will be treated equally, regardless of the type of traffic.
   ii. ***Background* (1, lowest)**
   iii. ***Excellent Effort* (2)**
   iv. ***Critical applications* (3)**
   v. ***Video (4)***: This priority is used for video traffic. It will be given higher priority than Best Effort and Voice traffic, so that video streaming is not interrupted.

vi. ***Voice (5)***: This priority is used for voice traffic. It will be given higher priority than Best Effort traffic, so that voice calls are not interrupted by other types of traffic.

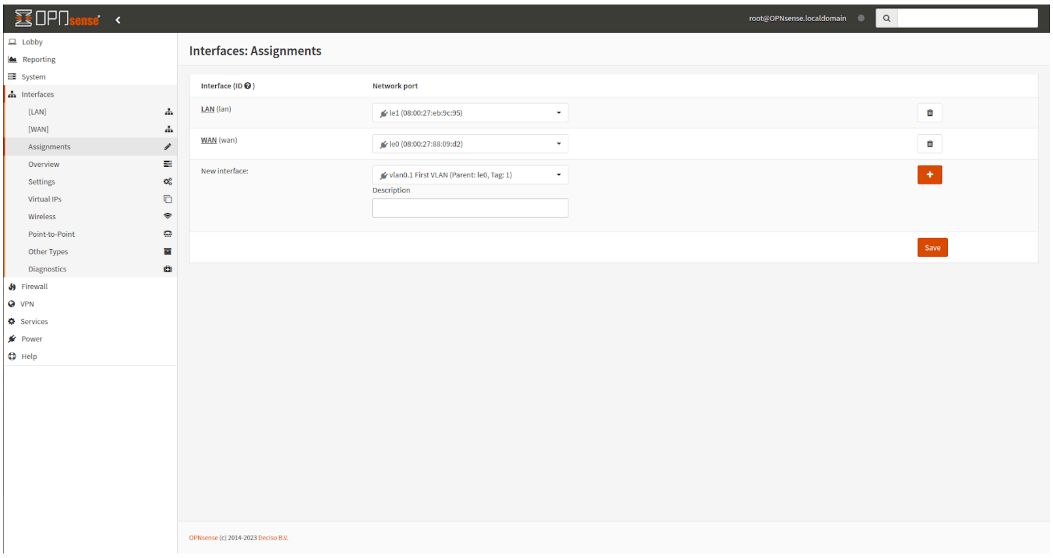
vii. ***Internetwork Control (6)***: This priority is used to control traffic. It is used for protocols such as DHCP, DNS, and NTP. It will be given higher priority than Best Effort, Voice, and Video traffic so that these protocols can function properly.

viii. ***Network Control (7)***: This priority is used for network control traffic. It is used for protocols such as routing and switching. It will be given higher priority than Best Effort, Voice, Video, and Control traffic so that these protocols can function properly.

5. Assigning Logical Interfaces to the VLAN

After configuring the basic VLAN settings and specifying the parent interface, the next step is to assign logical interfaces to the newly created VLAN. These logical interfaces are used to manage VLAN traffic and apply various settings as needed. Multiple VLANs can be assigned to a single parent interface or spread across multiple parent interfaces. Because of this flexibility, you can define separate routing, firewalling, and other networking rules for each VLAN. To assign logical interfaces to a VLAN in OPNsense, you may follow the next steps:

1. Go to **Interfaces > Assignments.**



Interfaces: Assignments

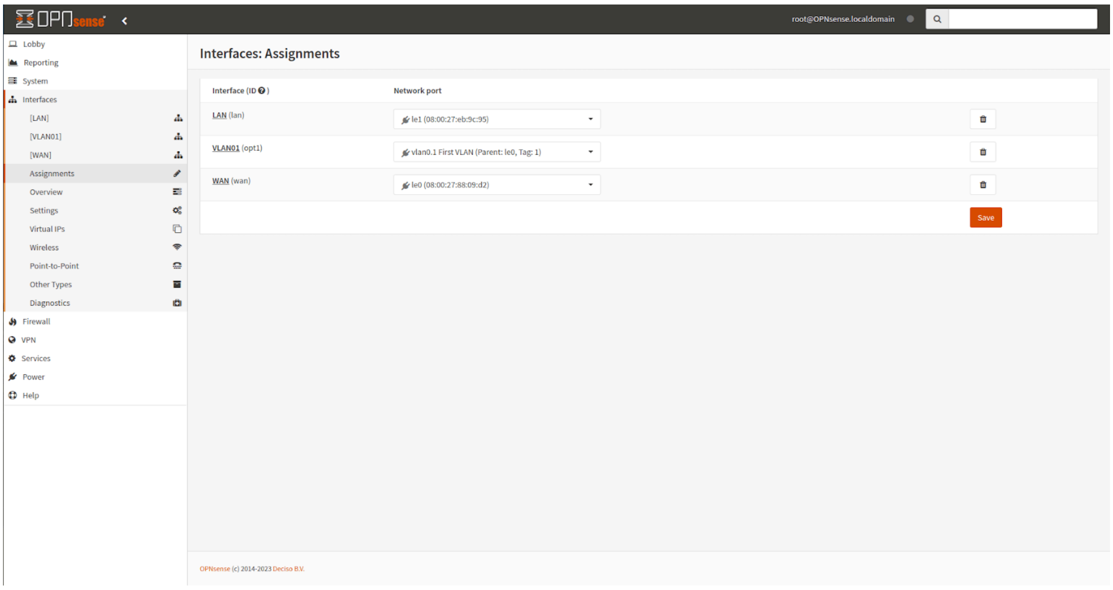
Interface (ID ?)	Network port
LAN (lan)	le1 (08:00:27:eb:9c:95)
WAN (wan)	le0 (08:00:27:88:09:d2)
New interface:	vlan0.1 First VLAN (Parent: le0, Tag: 1) Description

OPNsense (c) 2014-2023 Deciso B.V.

Figure 4. *Assigning VLAN Interface on OPNsense*

2. Select the **VLAN** that you want to configure.

3. In the **Parent Interface** field, select the physical interface where the VLAN was created.
4. In the **New Interface** field, select the logical interface that you want to add.
5. Click the **+** button to add the logical interface.



Interfaces: Assignments

Interface (ID ?)	Network port
LAN (lan)	le1 (08:00:27:eb:9c:95)
VLAN01 (opt1)	vlan0.1 First VLAN (Parent: le0, Tag: 1)
WAN (wan)	le0 (08:00:27:88:09:d2)

Figure 5. *Interface Assignments on OPNsense*

The logical interface will now be associated with the VLAN. This means that traffic on the logical interface will be tagged with the VLAN ID of the VLAN.

This method allows you to effectively create VLANs in OPNsense. These logically distinct networks optimize traffic flow inside your network infrastructure, improve network management, and increase security.

3. Configuring VLAN Interfaces

Once you have completed the VLAN setup in OPNsense, follow these steps to configure the VLAN interfaces. Configuring VLAN settings might seem complex initially, but with the right guidance, you can effectively harness the benefits of network segmentation.

You may configure VLAN interface on your OPNsense node easily by following the 5 main steps:

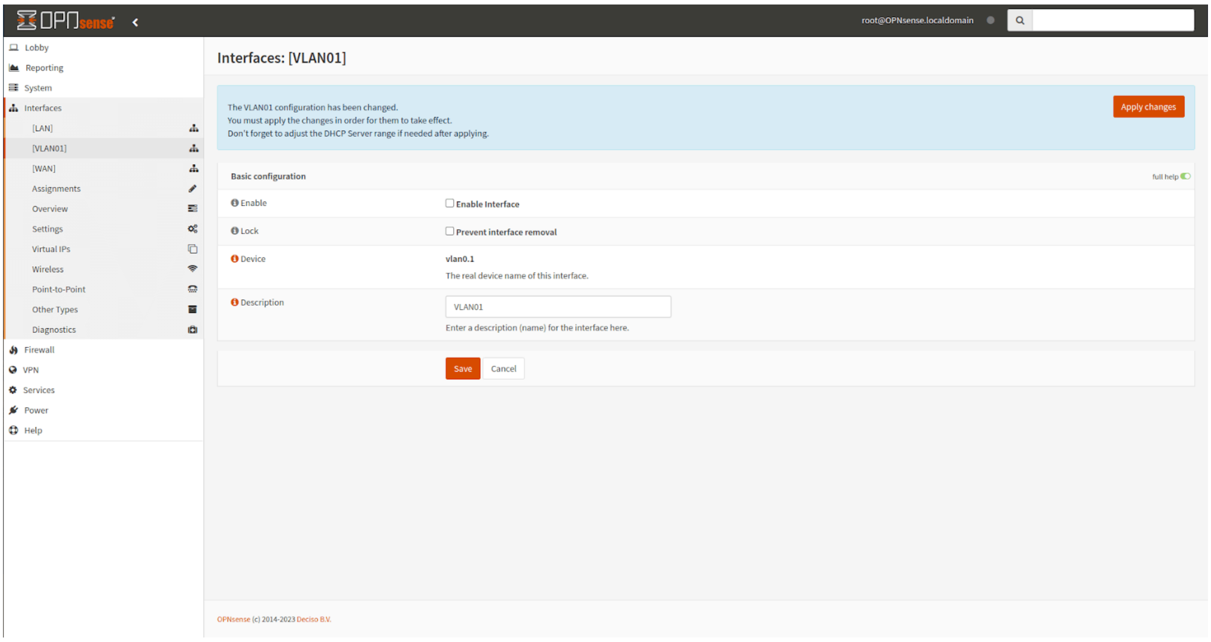
1. Accessing the VLAN Interface Settings
2. Enabling the VLAN Interface
3. Naming the VLAN Interface
4. Setting Up a Static IPv4 Address for the VLAN
5. DHCP Configuration for Automatic IP Address Assignment

So, let's dive into the details and learn how to configure VLAN settings for your network on OPNsense by following the next steps.

1. Accessing the VLAN Interface Settings

To access the VLAN Interface settings in OPNsense, follow these steps:

1. Log in to the OPNsense web interface as an **administrator**.
2. Navigate to the **Interfaces** section in the top menu.
3. Locate and click on the **VLAN interface** you wish to configure (e.g., "VLAN01").



Interfaces: [VLAN01]

The VLAN01 configuration has been changed.
You must apply the changes in order for them to take effect.
Don't forget to adjust the DHCP Server range if needed after applying.

Basic configuration

Enable: □ Enable Interface

Lock: □ Prevent interface removal

Device: vlan0.1
The real device name of this interface.

Description: VLAN01
Enter a description (name) for the interface here.

Figure 6. *Editing VLAN Interface on OPNsense*

2. Enabling the VLAN Interface

You may easily enable the VLAN interface on OPNsense by following next steps:

1. Check the box to enable the VLAN interface on the interface settings page.
2. Ensure that the interface is set to remain active (prevent removal) unless you have specific reasons to change this later.

3. Naming the VLAN Interface

Naming your VLAN interface is an important step in network configuration and management. To name the VLAN interface in OPNsense provide a descriptive name for the VLAN interface to easily identify it in the network settings. Consistency in naming can help manage multiple VLANs efficiently. Providing brief explanations about the fields that need to be entered or determined for the configuration will help with setting up the adjustments.

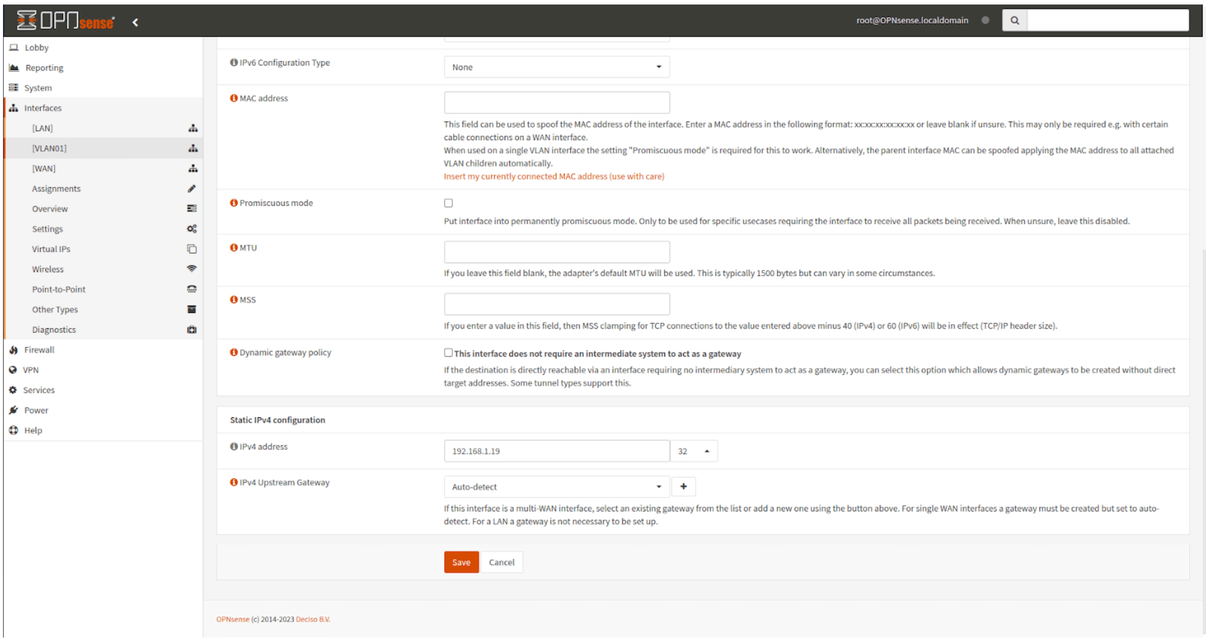
You may configure the following options for your new VLAN interface:

- ***Block private networks***: This option blocks traffic from IP addresses that are reserved for private networks. This is useful for security purposes, as it prevents unauthorized access to your network.
- ***Block bogon networks***: This option blocks traffic from IP addresses that are not yet assigned by IANA. This is also a security measure, as it prevents malicious traffic from reaching your network.
- ***IPv4 Configuration Type***: This setting specifies how the IPv4 address for the interface will be configured. You can choose between static or DHCP.
- ***IPv6 Configuration Type***: This setting specifies how the IPv6 address for the interface will be configured. You can choose between static or DHCP.
- ***MAC address***: This is the MAC address of the interface. You can leave this blank if you are not sure what it is.
- ***Promiscuous mode***: This setting allows the interface to receive all packets, even those that are not addressed to it. This can be useful for troubleshooting purposes, but it should be disabled unless necessary.
- ***MTU***: This is the maximum transmission unit for the interface. This is the size of the largest packet that can be sent over the interface.
- ***MSS***: This is the maximum segment size for TCP connections. This is the size of the largest TCP segment that can be sent over the interface.
- ***Dynamic gateway policy***: This setting specifies whether the interface should use a dynamic gateway. A dynamic gateway is a gateway that is automatically configured by the router.
- ***Static IPv4 configuration***: This section allows you to configure a static IPv4 address for the interface.
- ***IPv4 Upstream Gateway***: This is the IP address of the gateway for the interface. The gateway is the device that routes traffic between your network and the rest of the internet.

4. Setting Up a Static IPv4 Address for the VLAN

Setting up a static IPv4 address for your VLAN interface is an important step toward ensuring proper network communication. You can set up a static IPv4 address for your VLAN interface on OPNsense by following the next steps:

1. Choose "**Static IPv4**" as the configuration type for the VLAN interface.
2. Enter the IP address of your choice for the interface (e.g., 192.168.1.19).



IPv6 Configuration Type: None

MAC address:

This field can be used to spoof the MAC address of the interface. Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank if unsure. This may only be required e.g. with certain cable connections on a WAN interface.
When used on a single VLAN interface the setting "Promiscuous mode" is required for this to work. Alternatively, the parent interface MAC can be spoofed applying the MAC address to all attached VLAN children automatically.
Insert my currently connected MAC address (use with care)

Promiscuous mode: □

Put interface into permanently promiscuous mode. Only to be used for specific usecases requiring the interface to receive all packets being received. When unsure, leave this disabled.

MTU:

If you leave this field blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.

MSS:

If you enter a value in this field, then MSS clamping for TCP connections to the value entered above minus 40 (IPv4) or 60 (IPv6) will be in effect (TCP/IP header size).

Dynamic gateway policy: □ **This interface does not require an intermediate system to act as a gateway**

If the destination is directly reachable via an interface requiring no intermediary system to act as a gateway, you can select this option which allows dynamic gateways to be created without direct target addresses. Some tunnel types support this.

Static IPv4 configuration

IPv4 address: 192.168.1.19 / 32

IPv4 Upstream Gateway: Auto-detect

If this interface is a multi-WAN interface, select an existing gateway from the list or add a new one using the button above. For single WAN interfaces a gateway must be created but set to auto-detect. For a LAN a gateway is not necessary to be set up.

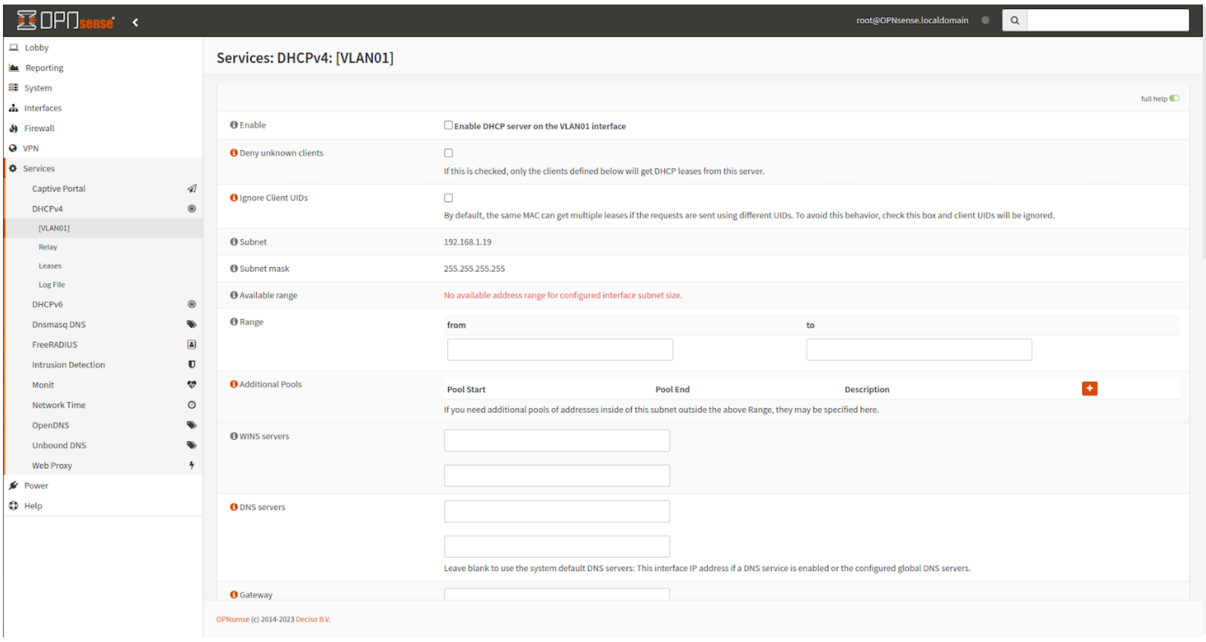
OPNsense (c) 2014-2023 Deciso B.V.

Figure 7. *Static IPv4 of VLAN Interface on OPNsense*

5. DHCP Configuration for Automatic IP Address Assignment

Configuring **DHCP (Dynamic Host Configuration Protocol)** for automatic IP address assignment on your VLAN interface in OPNsense is critical for providing seamless network connectivity to devices. To enable automatic IP address assignment for devices on the VLAN follow the next steps:

1. Go to **Services > DHCPv4 > [VLAN Name]**.



Services: DHCPv4: [VLAN01]

Enable: □ **Enable DHCP server on the VLAN01 interface**

Deny unknown clients: □

If this is checked, only the clients defined below will get DHCP leases from this server.

Ignore Client UIDs: □

By default, the same MAC can get multiple leases if the requests are sent using different UIDs. To avoid this behavior, check this box and client UIDs will be ignored.

Subnet: 192.168.1.19

Subnet mask: 255.255.255.255

Available range: No available address range for configured interface subnet size.

Range: **from** **to**

Additional Pools: **Pool Start** **Pool End** **Description**

If you need additional pools of addresses inside of this subnet outside the above Range, they may be specified here.

WINS servers:

DNS servers:

Leave blank to use the system default DNS servers: This interface IP address if a DNS service is enabled or the configured global DNS servers.

Gateway:

OPNsense (c) 2014-2023 Deciso B.V.

Figure 8. *DHCP Configuration on OPNsense*

2. Check the "**Enable DHCP server on the VLAN interface**" checkbox.
3. Define the range of IP addresses to be assigned to devices on the VLAN (e.g., `192.168.1.100-192.168.1.200`). Please note that the steps and input values might vary based on your specific network setup and requirements. Here's a general overview of the process and some example input values:
    - ***Enable***: This option enables the DHCP server on the VLAN01 interface.
    - ***Deny unknown clients***: If this option is checked, only the clients defined below will get DHCP leases from this server.
    - ***Ignore Client UIDs***: By default, the same MAC can get multiple leases if the requests are sent using different UIDs. To avoid this behavior, check this box and client UIDs will be ignored.
    - ***Subnet***: This is the subnet that the DHCP server will be serving addresses for.
    - ***Subnet mask***: This is the subnet mask for the subnet.
    - ***Available range***: This is the range of addresses that are available for DHCP leases.
    - ***Range***: This is a specific range of addresses that can be used for DHCP leases.
    - ***Additional Pools***: This is where you can define additional pools of addresses that can be used for DHCP leases.
    - ***WINS servers***: This is the list of WINS servers that the DHCP server will provide to clients.
    - ***DNS servers***: This is the list of DNS servers that the DHCP server will provide to clients.
    - ***Gateway***: This is the gateway that the DHCP server will provide to clients.
    - ***Domain name***: This is the domain name that the DHCP server will provide to clients.
    - ***Domain search list***: This is a list of domain names that the DHCP server will provide to clients.
    - ***Default lease time (seconds)***: This is the default lease time for DHCP leases.
    - ***Maximum lease time (seconds)***: This is the maximum lease time for DHCP leases.
    - ***Response delay (seconds)***: This is the minimum number of seconds that the DHCP server will wait before responding to a DHCP request.
    - ***Interface MTU***: This is the MTU that the DHCP server will use.

- ***Failover peer IP***: This is the IP address of the other DHCP server that is part of a failover cluster.
- ***Failover split***: This is the percentage of DHCP requests that will be handled by the primary DHCP server.
- ***Static ARP***: This option allows you to define static ARP entries.
- ***Dynamic DNS***: This option allows you to configure Dynamic DNS.
- ***MAC Address Control***: This option allows you to control which clients can get DHCP leases.
- ***NTP servers***: This option allows you to configure the NTP servers that the DHCP server will use.
- ***TFTP server***: This option allows you to configure the TFTP server that the DHCP server will use.
- ***LDAP URI***: This option allows you to configure the LDAP server that the DHCP server will use.
- ***Network booting***: This option allows you to enable network booting.
- ***WPAD***: This option allows you to configure the WPAD server that the DHCP server will use.
- ***Enable OMAPI***: This option allows you to enable the OMAPI interface.
- ***Additional Options***: This is where you can configure additional DHCP options.

When VLAN interfaces are configured on OPNsense, your network gains effective communication and IP address management. Devices inside the VLAN can automatically acquire IP addresses by turning on DHCP, which streamlines network administration. Your business can increase security, enhance traffic flow, and efficiently manage network resources to serve a variety of applications and user groups with a well-structured VLAN configuration. Properly configured VLANs will simplify resource sharing and data sharing between various departments and devices.

4.Configuring Firewall Rules for VLANs

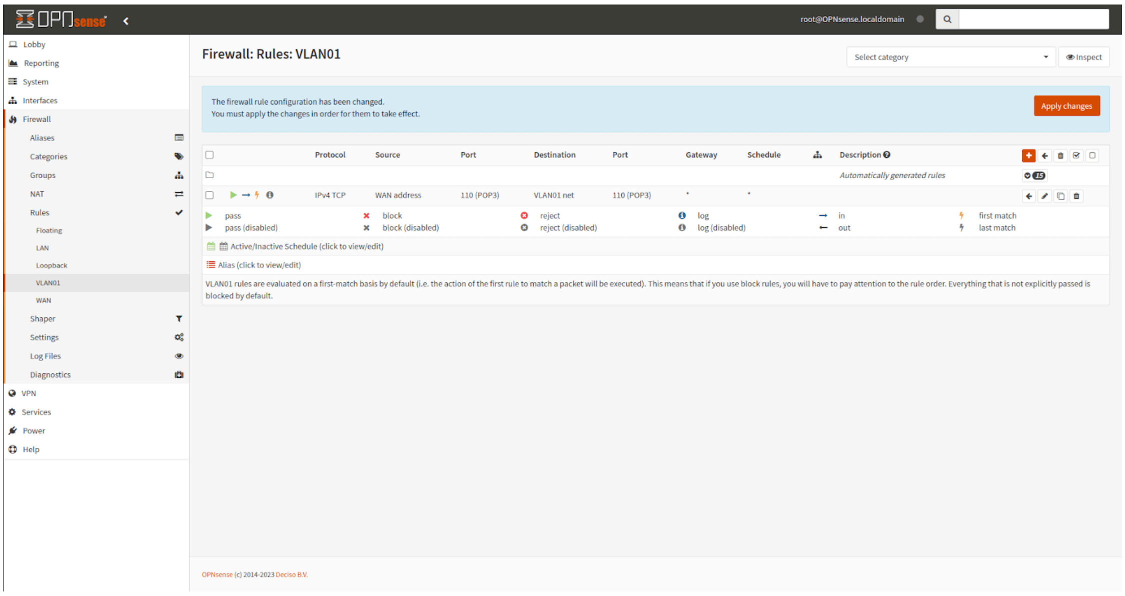
Firewall rules on OPNsense regulate traffic flow between different network segments, including VLANs. They specify which traffic is allowed or denied based on source, destination, port, and protocol. By default, newly created VLAN interfaces have all traffic blocked to ensure security. You should configure firewall rules on the OPNsense node for your newly created VLAN interface.

To expedite the process, copy the basic rules from the LAN interface as a starting point. Cloning helps maintain consistency and saves time in setting up new rules for each VLAN.

After cloning, update the cloned rules to apply to the specific VLAN interface. Modify the interface from LAN to the corresponding VLAN interface (e.g., DMZ). Update source and destination settings to allow traffic between VLANs and other networks as needed.

To allow desired traffic on the VLAN, you may follow the following steps:

1. Create **new rules** to allow the desired traffic flow within the VLAN and between VLANs.



Firewall: Rules: VLAN01

The firewall rule configuration has been changed.
You must apply the changes in order for them to take effect.

□	Protocol	Source	Port	Destination	Port	Gateway	Schedule		Description
									Automatically generated rules
□	IPv4 TCP	WAN address	110 (POP3)	VLAN01 net	110 (POP3)	*	*		

▶ pass	✖ block	⊗ reject	ℹ log	→ in	ϟ first match
▶ pass (disabled)	✖ block (disabled)	⊗ reject (disabled)	ℹ log (disabled)	← out	ϟ last match

Active/Inactive Schedule (click to view/edit)

Alias (click to view/edit)

VLAN01 rules are evaluated on a first-match basis by default (i.e. the action of the first rule to match a packet will be executed). This means that if you use block rules, you will have to pay attention to the rule order. Everything that is not explicitly passed is blocked by default.

Figure 9. *Firewall Rule Configuration on OPNsense*

2. Fine-tune rules to meet the unique requirements of each VLAN.
3. Regularly review and update firewall rules to adapt to changing network needs.

5. Testing the VLAN Configuration

Test communication between devices on different VLANs to ensure proper segregation and connectivity. Verify that devices on separate VLANs can communicate as intended. Troubleshooting steps for common VLAN issues on OPNsense are as follows:

- If connectivity issues arise, check VLAN configurations and firewall rules.
- Verify that VLAN interfaces are enabled, and correct rules are in place.
- Review logs and error messages for insights into potential issues.

Zenarmor - The best in network security!

Configuring VLANs on OPNsense empowers network administrators with improved performance, security, and scalability. By effectively segregating and managing traffic, businesses can streamline their network operations and protect sensitive data.

If you're familiar with configuring VLANs in OPNsense and are now transitioning to Zenarmor, you'll find that Zenarmor offers a powerful feature called Exempted VLANs & Networks. This feature allows you to define specific VLANs and IP/Network addresses that are exempted from Zenarmor processing. Essentially, any traffic associated with these exempted VLANs and addresses bypasses Zenarmor's packet processing entirely, being directly forwarded at the interface level. The key distinction from policy-based whitelisting is that these addresses won't generate any activity reports, ensuring a seamless experience.

A particularly beneficial aspect is that devices within the exempted VLANs and networks are excluded from Zenarmor's license count, meaning they won't contribute to license calculation. This is a handy feature to keep your licensing strategy precise and effective.

However, it's important to note that the Exempted VLANs & Networks feature is available exclusively in premium Zenarmor Editions.

To configure Exempted VLANs & Networks in Zenarmor, follow these straightforward steps:

1. Open your OPNsense web UI and navigate to the Zenarmor section.
2. From the left-hand sidebar, select the Settings menu.
3. Look for the Exempted VLANs & Networks option and click on it.
4. Add VLAN ID by clicking on the **Exempt VLAN ID** button.

For the best and most reliable service and support, sign up with Zenarmor today. Experience seamless VLAN implementation and bolstered network defense to safeguard your organization's critical assets. Don't wait; take the next step toward a robust and secure network environment by signing up with Zenarmor!

How To Configure OPNsense Network Address Translation

Network address translation is the process of mapping one [Internet Protocol (IP) address] to another by modifying the header of IP packets while they are in transit across a router. As part of this technique, NAT settings can expose only one IP address for an entire network to the outside world, effectively masking the entire internal network and increasing security. Network address translation is widely used in remote-access scenarios because it conserves addresses while also increasing security. This improves security while also reducing the number of IP addresses required by a business.

Network Address Translation (NAT) is a method of separating external and internal networks (WANs and LANs) and sharing an external IP address among clients on the internal network. NAT can be used on both IPv4 and IPv6 networks. Network Prefix Translation is also available for IPv6.

💡 **BEST PRACTICE**

In addition the its NAT features, OPNsense also provides next-generation firewall capabilities such as web control and application control. This is provided by an external tool called Zenarmor.

Zenarmor NGFW Plug-in for OPNsense is one of the most popular OPNsense plug-ins and allows you to easily upgrade your firewall to a Next Generation Firewall in seconds. NG Firewalls empower you to combat modern-day cyber attacks that are becoming more sophisticated every day.

Some of the capabilities are layer-7 application/user aware blocking, granular filtering policies, commercial-grade web filtering utilizing cloud-delivered AI-based Threat Intelligence, parental controls, and the industry's best network analytics and reporting.

Zenarmor Free Edition is available at no cost for all OPNsense users.

The majority of the options below make use of three distinct addresses: the source, destination, and redirect address. These addresses will be used for the following purposes:

Address	Description
Source	From where the traffic is coming. This is frequently left on "any".
Destination	Where the traffic is going. This is typically your external IP address for incoming traffic from the outside world.
Redirect	Where traffic should be rerouted

⚠ **CAUTION**

Disabling **`pf`** disables **NAT** on OPNsense.

- **BINAT**: NAT typically operates in only one direction. But, if your networks are of equal size, you can also use bidirectional BINAT. This can help to simplify your setup. You can only use regular NAT if your networks are not of equal size.
- **NAT reflection**: When a user on the internal network attempts to connect to a local server by using the external IP address rather than the internal one, NAT reflection can rewrite the request to use the internal IP address, avoiding a detour and applying rules designed for actual outside traffic.
- **Pool Options**: When there are multiple IPs to choose from, this option allows you to control which IP is used. The default, Round Robin, simply sends packets to one server after another. This option has no effect if you only have one external IP address.

OPNsense firewall provides the following types of NAT configurations:

- Port Forwarding NAT (DNAT)
- One-to-One NAT (1:1 NAT)
- Outbound NAT (SNAT)

In this article, we will cover all these NAT configurations on OPNsense shortly and give the following real-world examples.

- Port forwarding configuration in OPNsense for a web server accessible from the Internet.
- Port forwarding configuration in OPNsense for ssh and RDP servers accessible by a specific IP

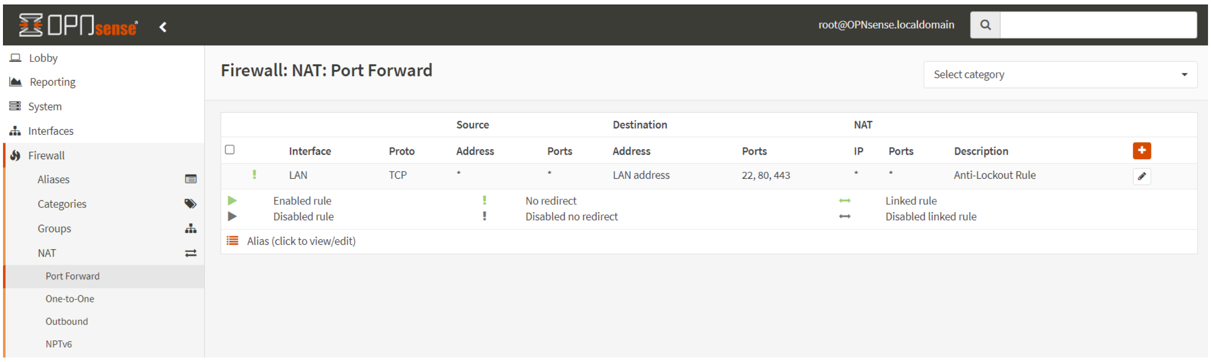
- Outbound NAT configuration in OPNsense for allowing specific local servers to access a remote service.

Port forwarding in OPNsense

Any connections to the internal network from the Internet are blocked by the OPNsense firewall. You may use the OPNsense port forwarding feature to allow certain services(ports) from the external network.

Port forwarding is also known as "Destination NAT" or "DNAT." When multiple servers in a LAN share the same external IP address, any connection that is not initiated by one of the servers will fail because the firewall will not know where to send the traffic. This can be remedied by establishing port forwarding rules. For example, to make your organization's web server behind the firewall accessible from the internet, you must redirect HTTP(s) ports (80/443) to the server.

To configure the port forwarding in OPNsense you may navigate to **`Firewall` -> NAT -> `Port Forward`**. An overview of port forwarding rules can be found here.



Firewall: NAT: Port Forward

			Source		Destination		NAT			
□		Interface	Proto	Address	Ports	Address	Ports	IP	Ports	Description
	!	LAN	TCP	*	*	LAN address	22, 80, 443	*	*	Anti-Lockout Rule

▶ Enabled rule
▶ Disabled rule
! No redirect
! Disabled no redirect
⟷ Linked rule
⟷ Disabled linked rule
Alias (click to view/edit)

Figure 1. *Port forwarding configuration in OPNsense*

To add new port forwarding rules, you may click the **+** button in the upper right corner.

The following fields are available when adding a port forwarding rule:

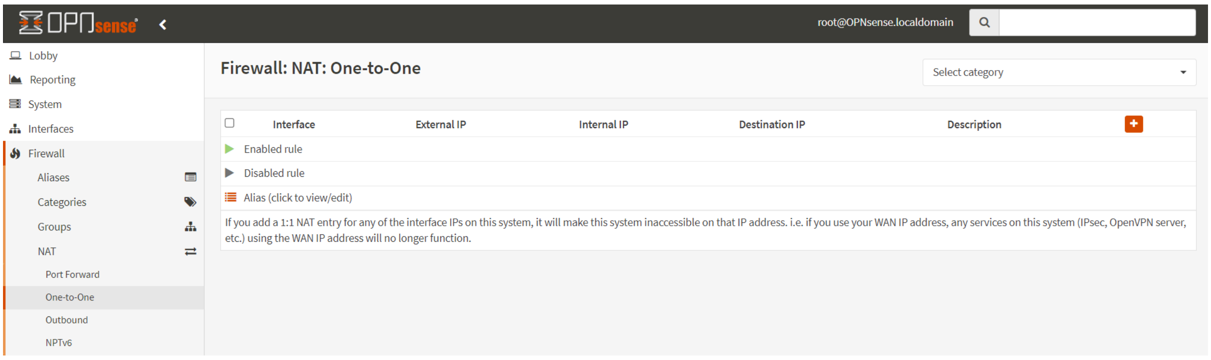
Option	Description
Disabled	Check this option to disable the rule without removing it.
No RDR (NOT)	Enabling this option prevents traffic matching this rule from being redirected and a redirect rule is not created. Hint: this option is rarely used; don't use it unless you're sure you know what you're doing.
Interface	Which interface the rule should apply to. The majority of the time, this will be WAN.
TCP/IP version	IPv4, IPv6 or both.
Protocol	In typical scenarios, this will be TCP
Source	Where the traffic comes from. Click **`Advanced`** to see the other source settings
Source / Invert	Invert match in **`Source`** field.
Source port range	When applicable, the source port on which we should match. This is almost always random and almost never equals the destination port range (and should almost always be 'any').
Destination / Invert	Invert match in **`Destination`** field.
Destination	Where the traffic is going
Destination port range	Service port(s) the traffic is using. For this mapping, specify the port or port range for the packet's destination when using the TCP or UDP protocols.
Redirect target IP	Where to redirect the traffic to. Enter the internal IP address of the server to which the ports will be mapped.

Redirect target port	Which port to use (when using TCP and/or UDP). Enter the port number for the machine with the IP address you entered above. In the case of a port range, specify the range's starting port (the end port will be calculated automatically).
Pool Options	This option is explained in the previous section. The default is to use Round robin. Only Round Robin types are compatible with Host Aliases. Subnets of any type can be used. **Round Robin**: Iterates over the translation addresses. **Random**: Chooses an address at random from the translation address pool. **Source Hash**: Determines the translation address by hashing the source address, ensuring that the redirection address is always the same for a given source. **Bitmask**: Uses the subnet mask while keeping the last portion the same; 172.16.10.50 -> x.x.x.50. **Sticky Address**: When using the Random or Round Robin pool types, the Sticky Address option ensures that a specific source address is always mapped to the same translation address.
Description	A description to easily find the rule in the overview.
Set local tag	You can mark a packet matching this rule and use this mark to match on other NAT/filter rules.
Match local tag	Check for a tag set by another rule.
No XMLRPC sync	Prevent this rule from being synced to a backup host. (Checking this on the backup host has no effect.)
NAT reflection	This option is explained in the previous section. Leave this on the default unless you have a good reason not to.
Filter rule association	Associate this with a regular firewall rule.

One-to-one NAT

One-to-one NAT, as the name suggests, will translate two IP addresses one-to-one rather than one-to-many, as is more common.

To configure the One-to-One NAT in OPNsense you may navigate to **`Firewall` -> NAT -> `One-to-One`**. An overview of 1:1 NAT rules can be found here.



Firewall: NAT: One-to-One

□	Interface	External IP	Internal IP	Destination IP	Description

▶ Enabled rule

▶ Disabled rule

☰ Alias (click to view/edit)

If you add a 1:1 NAT entry for any of the interface IPs on this system, it will make this system inaccessible on that IP address. i.e. if you use your WAN IP address, any services on this system (IPsec, OpenVPN server, etc.) using the WAN IP address will no longer function.

Figure 2. *One-to-One NAT configuration in OPNsense*

To add new One-to-One NAT rules, you may click the **+** button in the upper right corner.

The following fields are available when adding a 1:1 mapping rule:

Option	Description
Disabled	Check this option to disable the rule without removing it.
Interface	Which interface the rule should apply to. The majority of the time, this will be WAN.
Type	BINAT (default) or NAT.
External network	Enter the starting address of the external subnet for the 1:1 mapping or network. If no subnet mask is provided, the subnet mask from the internal address below will be applied to this IP address. This is the address or network to/from which traffic will be translated.
Protocol	In typical scenarios, this will be TCP

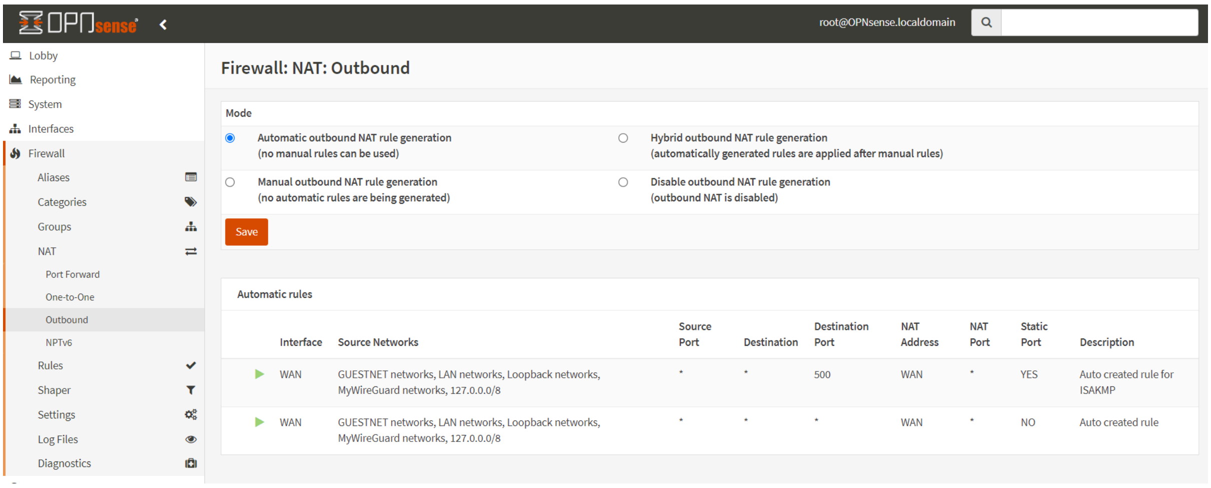
Source	Enter the internal subnet for the 1:1 mapping. The subnet size specified for the source will be applied to the external subnet, when none is provided.
Source / Invert	Invert match in **`Source`** field.
Destination / Invert	Invert match in **`Destination`** field.
Destination	The destination network packages should match, when used to map external networks, this is usually any
Description	A description to easily find the rule in the overview.
NAT reflection	This option is explained in the previous section. Leave this on the default unless you have a good reason not to.

Outbound NAT

Outbound NAT is also known as `Source NAT` or `SNAT`. When a client on an internal network sends an outbound request, the gateway must change the source IP to the gateway's external IP, because the outside server will be unable to respond otherwise.

If you only have one external IP address, you should leave the Outbound NAT options set to automatic. If you have multiple IP addresses, however, you may want to change the settings and add some custom rules.

To configure the Outbound NAT in OPNsense you may navigate to **`Firewall` -> NAT -> `Outbound`**. An overview of outbound rules can be found here.



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	GUESTNET networks, LAN networks, Loopback networks, MyWireGuard networks, 127.0.0.0/8	*	*	500	WAN	*	YES	Auto created rule for ISAKMP
▶	WAN	GUESTNET networks, LAN networks, Loopback networks, MyWireGuard networks, 127.0.0.0/8	*	*	*	WAN	*	NO	Auto created rule

Figure 3. *Outbound NAT configuration in OPNsense*

The following modes are available for outbound NAT configuration in OPNsense:

Outbound NAT Mode	**Description**
Automatic outbound NAT rule generation	The default and is good for most cases.
Manual outbound NAT rule generation	No automatic rules are generated. Outbound NAT rules are created manually.
Hybrid outbound NAT rule generation	Automatic rules are added, but manual rules can also be added.
Disable outbound NAT rule generation	Disables outbound NAT. This is used for transparent bridges, for example.

To add new Outbound NAT rules, you may select either the `Manual outbound NAT rule generation` or `Hybrid outbound NAT rule generation` option and then click **Save** button.

New rules can be added, by clicking the **+** button in the upper right corner.

The following fields are available when adding an outbound rule:

Option	Description
Disabled	Check this option to disable the rule without removing it.
Do not NAT	Enabling this option will disable NAT for traffic matching this rule and stop processing Outbound NAT rules.Hint: this option is rarely used; don't use it unless you're sure you know what you're doing.
Interface	Which interface the rule should apply to. The majority of the time, this will be WAN.
TCP/IP version	IPv4 or IPv6.
Protocol	In typical scenarios, this will be TCP
Source	The source network to match
Source / Invert	Invert match in **`Source`** field.
Source port range	When applicable, the source port on which we should match. This is almost always random and almost never equals the destination port range (and should almost always be 'any').
Destination / Invert	Invert match in **`Destination`** field.
Destination	Enter the destination network for the outbound NAT mapping.
Destination port range	Service port the traffic is using.
Translation / target	Packets matching this rule will be mapped to the IP address given here.If you want this rule to apply to another IP address rather than the IP address of the interface chosen above, select it here (you will need to define Virtual IP addresses on the interface first).

Log	Put packets matching this rule in the logs. Use this sparingly to avoid overflowing the logs.
Pool Options	This option is explained in the previous section. The default is to use Round robin. Only Round Robin types are compatible with Host Aliases. Subnets of any type can be used. **Round Robin**: Iterates over the translation addresses. **Random**: Chooses an address at random from the translation address pool. **Source Hash**: Determines the translation address by hashing the source address, ensuring that the redirection address is always the same for a given source. **Bitmask**: Uses the subnet mask while keeping the last portion the same; 172.16.10.50 -> x.x.x.50. **Sticky Address**: When using the Random or Round Robin pool types, the Sticky Address option ensures that a specific source address is always mapped to the same translation address.
Translation / port	Which port to use on the target
Static-port	Prevents pf(4) from modifying the source port on TCP and UDP packets.
Set local tag	Set a tag that other NAT rules and filters can check for.
Match local tag	Check for a tag set by another rule
No XMLRPC sync	Prevent this rule from being synced to a backup host. (Checking this on the backup host has no effect.)
Description	A description to easily find the rule in the overview.

Real-World Examples for NAT Configurations in OPNsense

In this section we will give some real world scenarios for NAT configuration on OPNsense firewall:

- Port Forwarding for Web Servers
- Port Forwarding for SSH and RDP Services on Custom Ports
- Outbound NAT for Accessing a Remote Service via External IP

How to Configure Port Forwarding For Web Services

Businesses that provide a service to their customers via the Internet must make their applications or web servers accessible from the Internet. Assume your company has two separate web servers in the DMZ network and one public IP address. Both the HTTP and HTTPS ports on these web servers should be accessible from anywhere in the world using the same public IP address. To accomplish this, you may define the port forwarding rules in your OPNsense. You may configure your rules in such a way that while requests coming to 80 and 443 ports are redirected to the first web server, the second web server is accessible via 81 and 8443 ports. For this configuration, you may follow the next steps below.

Server Name	External IP	External Port	Local IP	Local Port
WebServer1	Public Internet IP	80	10.10.10.13	80
WebServer1	Public Internet IP	443	10.10.10.13	443
WebServer2	Public Internet IP	81	10.10.10.14	80
WebServer2	Public Internet IP	8443	10.10.10.14	443

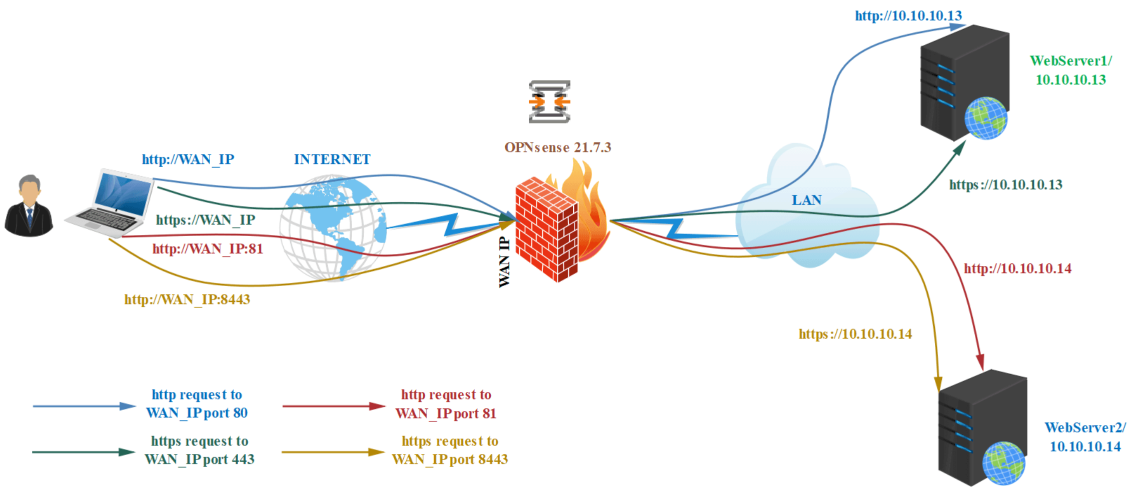


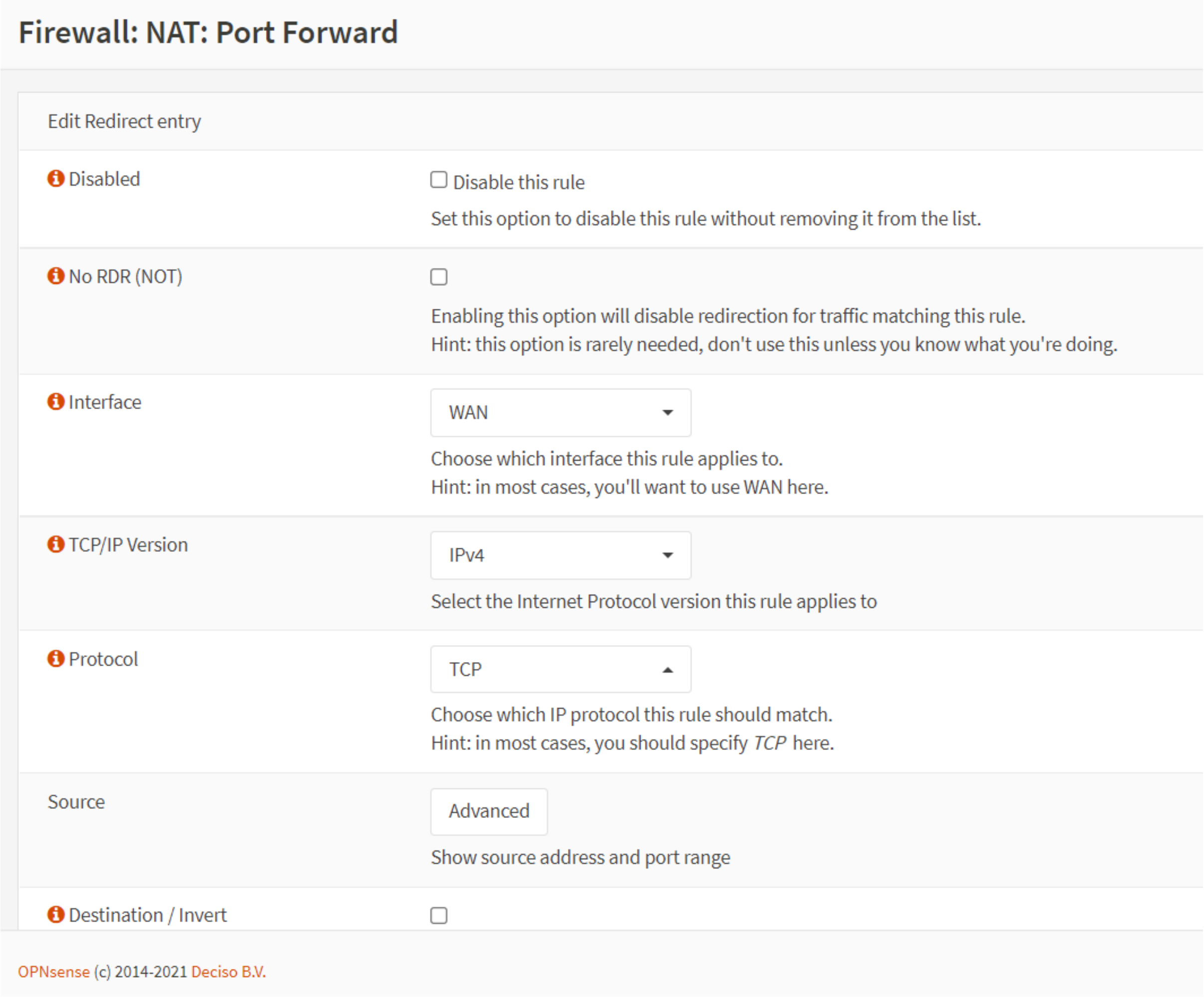
Figure 4. *Port Forwarding topology for web services*

After completing the port forwarding configurations on your OPNsense firewall, HTTP(80) and HTTPS(443) requests for your WAN IP will be redirected to the WebServer1(10.10.10.13), while port 81 and port 8443 requests for your WAN IP will be redirected to the WebServer2(10.10.10.14).

Port Forwarding For HTTPS(443) Service of WebServer1

You may follow the instructions below to add a port forwarding rule for HTTPS service of WebServer1.

1. Navigate to **`Firewall`** **->** **`NAT`** **->** **`Port Forward`** in your OPNsense Web UI.
2. Click the **+** button in the upper right corner. This will open the port forwarding configuration window.



Firewall: NAT: Port Forward

Edit Redirect entry

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

No RDR (NOT)
□
Enabling this option will disable redirection for traffic matching this rule.
Hint: this option is rarely needed, don't use this unless you know what you're doing.

Interface
WAN
Choose which interface this rule applies to.
Hint: in most cases, you'll want to use WAN here.

TCP/IP Version
IPv4
Select the Internet Protocol version this rule applies to

Protocol
TCP
Choose which IP protocol this rule should match.
Hint: in most cases, you should specify *TCP* here.

Source
Advanced
Show source address and port range

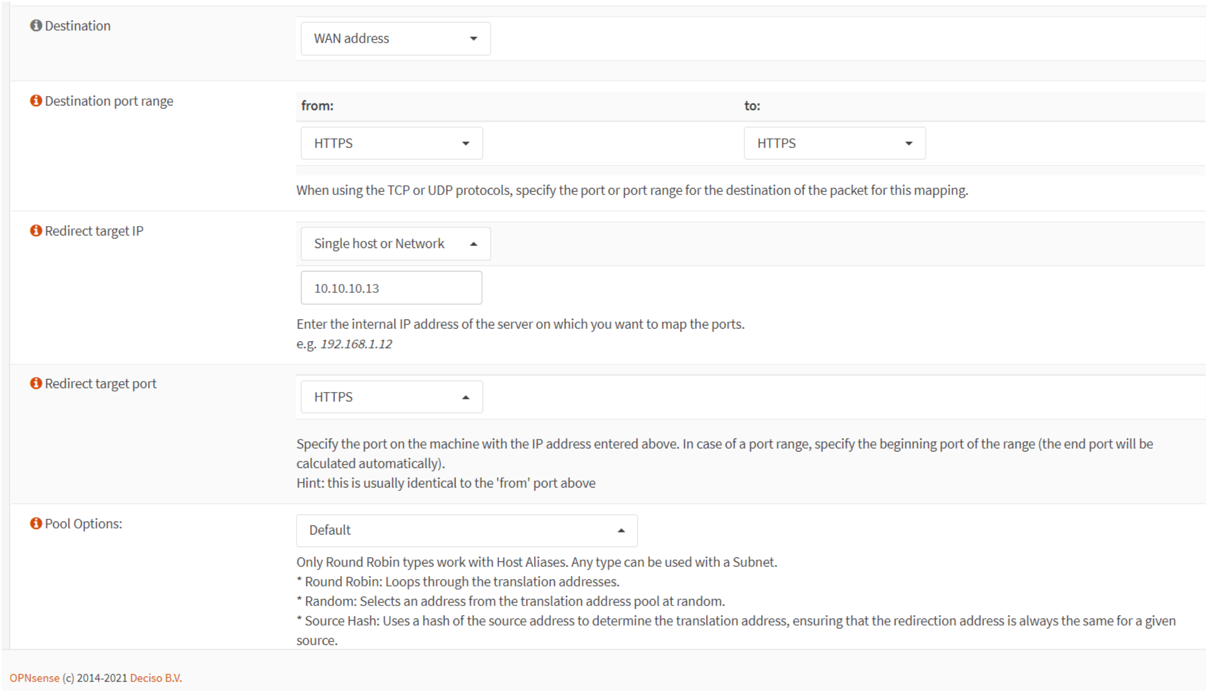
Destination / Invert
□

OPNsense (c) 2014-2021 Deciso B.V.

Figure 5. *Port forwarding rule configuration for HTTPS in OPNsense-1*

3. Set the Interface to `WAN`.
4. Set the TCP/IP Version to `IPv4`.
5. Set the Protocol to `TCP`.
6. Set the Destination to `WAN Address`.
7. Set the Destination Port Range to **HTTPS**.
8. Select `Single Host or Network` from the Redirect Target IP dropdown menu. Then, set the field to the private IP address of the WebServer1, such as **10.10.10.13**.

9. Set the Redirect Target Port to **HTTPS**.



Destination: WAN address

Destination port range: from: HTTPS to: HTTPS

When using the TCP or UDP protocols, specify the port or port range for the destination of the packet for this mapping.

Redirect target IP: Single host or Network

10.10.10.13

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

Redirect target port: HTTPS

Specify the port on the machine with the IP address entered above. In case of a port range, specify the beginning port of the range (the end port will be calculated automatically).
Hint: this is usually identical to the 'from' port above

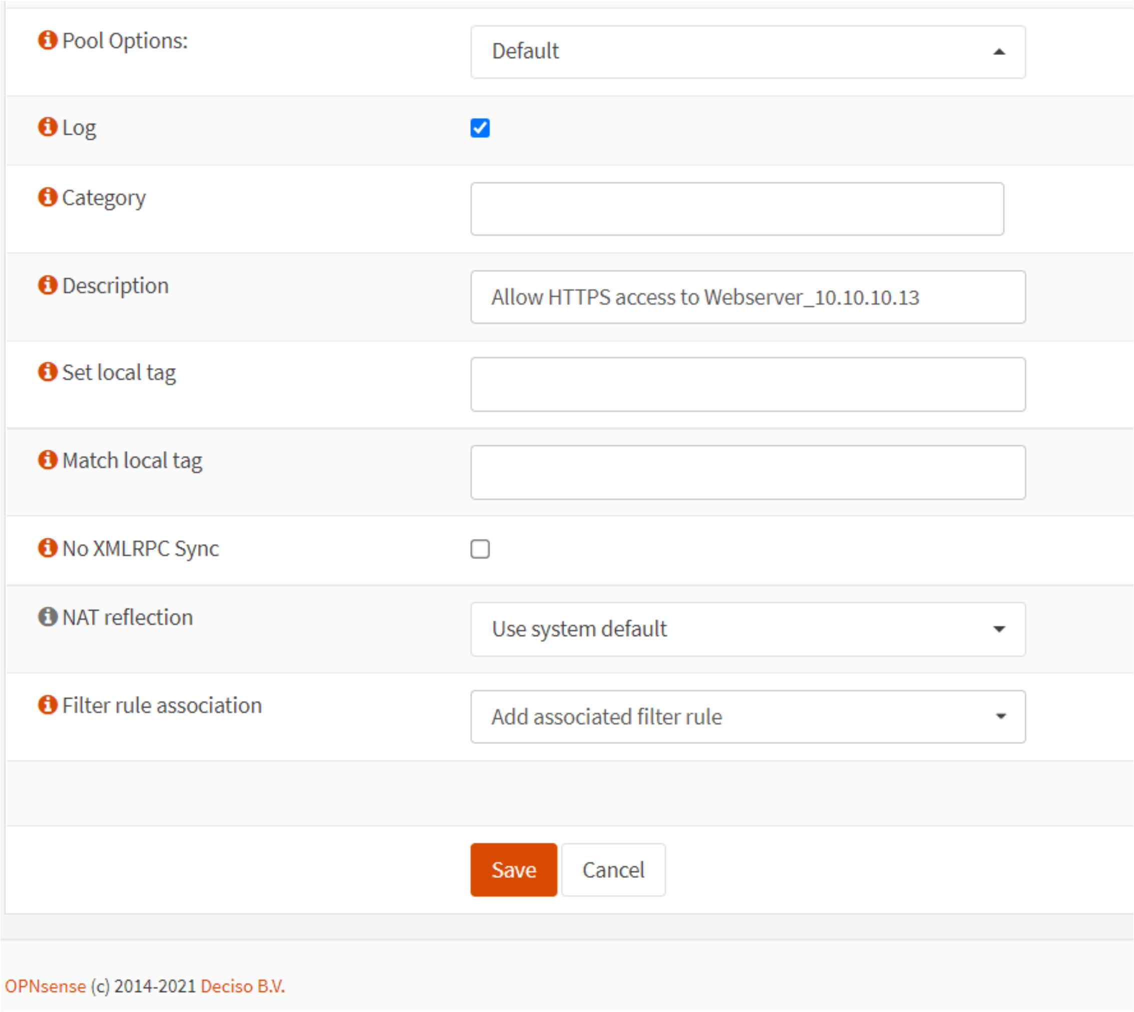
Pool Options: Default

Only Round Robin types work with Host Aliases. Any type can be used with a Subnet.
* Round Robin: Loops through the translation addresses.
* Random: Selects an address from the translation address pool at random.
* Source Hash: Uses a hash of the source address to determine the translation address, ensuring that the redirection address is always the same for a given source.

OPNsense (c) 2014-2021 Deciso B.V.

Figure 6. *Port forwarding rule configuration for HTTPS in OPNsense-2*

10. You may enable logging by clicking the check box in the Log option.
11. Fill in the Description field, such as `Allow HTTPS access to Webserver_10.10.10.13`.
12. Select Add `associated filter rule` from the Filter rule association option.
13. Leave other options as default.
14. Click **Save** button at the bottom of the page.



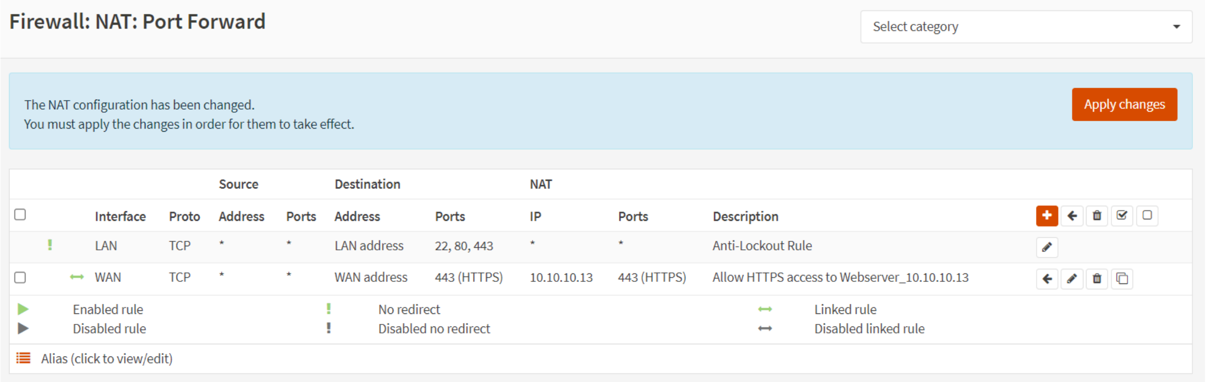
Pool Options:	Default
Log	☑
Category	
Description	Allow HTTPS access to Webserver_10.10.10.13
Set local tag	
Match local tag	
No XMLRPC Sync	☐
NAT reflection	Use system default
Filter rule association	Add associated filter rule

OPNsense (c) 2014-2021 Deciso B.V.

Figure 7. *Port forwarding rule configuration for HTTPS in OPNsense-3*

Port Forwarding For HTTP(80) Service of WebServer1

To create a port forwarding rule for the HTTP(80) service of the WebServer1, you may clone the port forwarding rule for the HTTPS(443) service created above and change the related settings by following the step given below.



Firewall: NAT: Port Forward

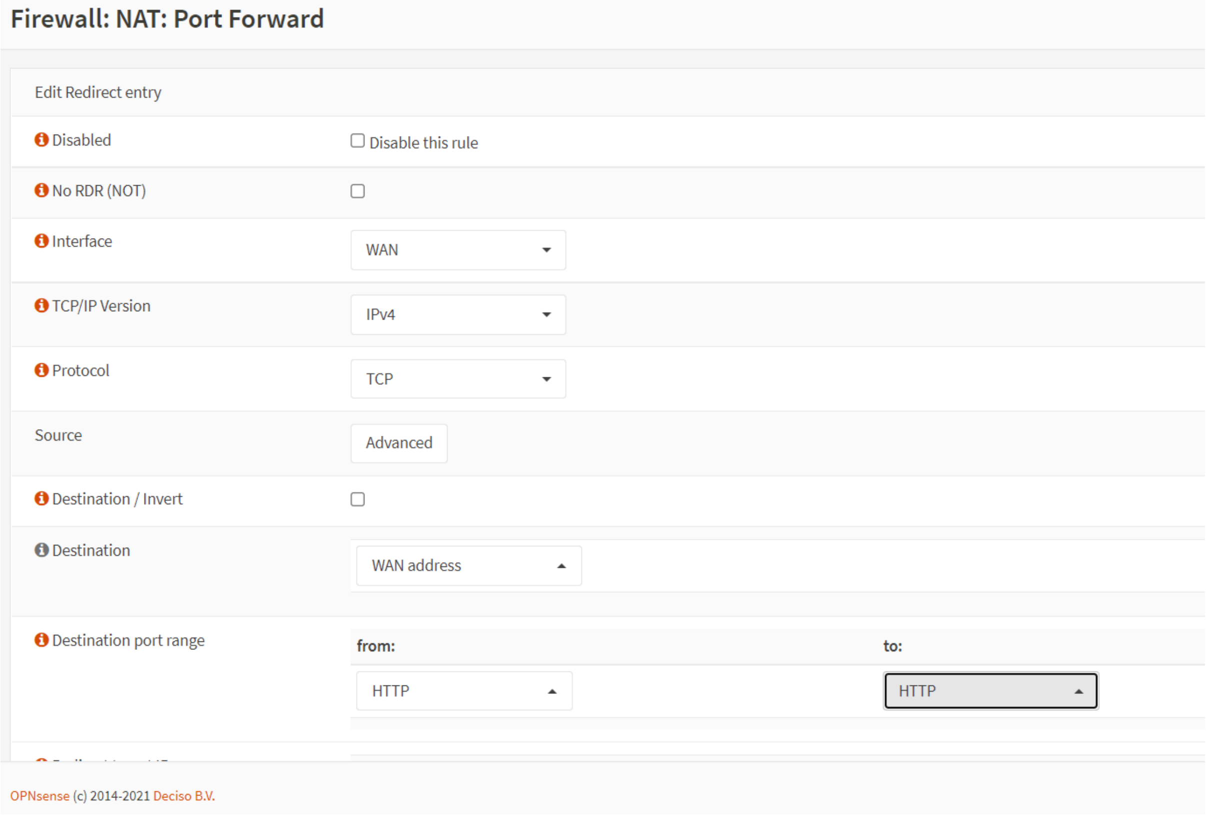
The NAT configuration has been changed.
You must apply the changes in order for them to take effect.

				Source		Destination		NAT		
☐		Interface	Proto	Address	Ports	Address	Ports	IP	Ports	Description
	!	LAN	TCP	*	*	LAN address	22, 80, 443	*	*	Anti-Lockout Rule
☐	⟷	WAN	TCP	*	*	WAN address	443 (HTTPS)	10.10.10.13	443 (HTTPS)	Allow HTTPS access to Webserver_10.10.10.13

▶ Enabled rule
▶ Disabled rule
! No redirect
! Disabled no redirect
⟷ Linked rule
⟷ Disabled linked rule
☰ Alias (click to view/edit)

Figure 8. *Port forwarding rules list in OPNsense*

1. Click the clone icon to copy the port forwarding rule for the HTTPS(443) service created above.
2. Change the Destination Port Range option to **HTTP**.



Firewall: NAT: Port Forward

Edit Redirect entry

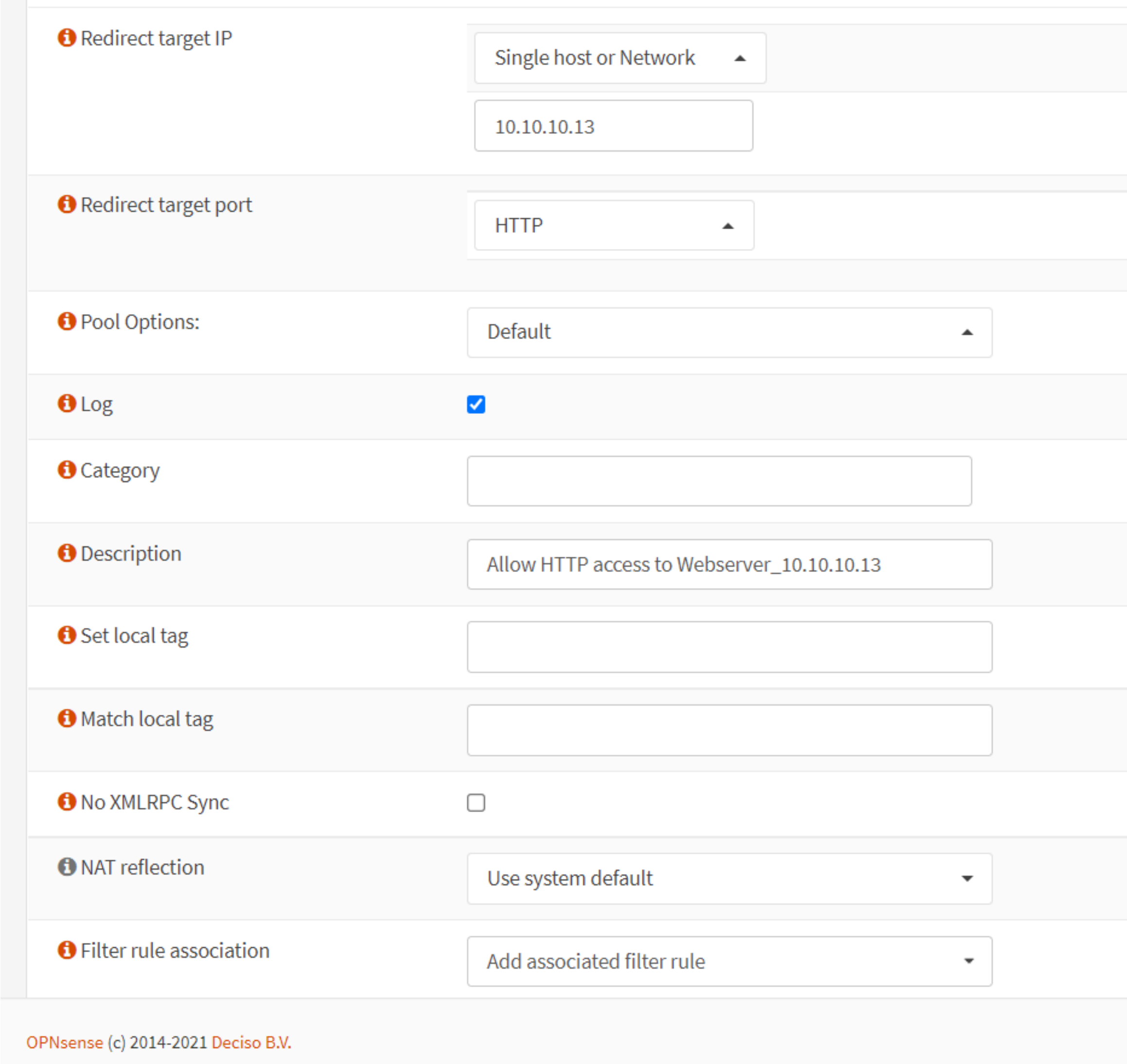
Disabled	□ Disable this rule
No RDR (NOT)	□
Interface	WAN
TCP/IP Version	IPv4
Protocol	TCP
Source	Advanced
Destination / Invert	□
Destination	WAN address
Destination port range	from: HTTP to: HTTP

OPNsense (c) 2014-2021 Deciso B.V.

Figure 9. *Port forwarding rule configuration for HTTP in OPNsense-1*

3. Set the Redirect Target Port to **HTTP**.
4. Change the Description field to `Allow HTTP access to Webserver_10.10.10.13`.
5. Verify that the Filter rule association option is set to Add `associated filter rule`
6. Leave other options as they are.

7. Click **Save** button at the bottom of the page.



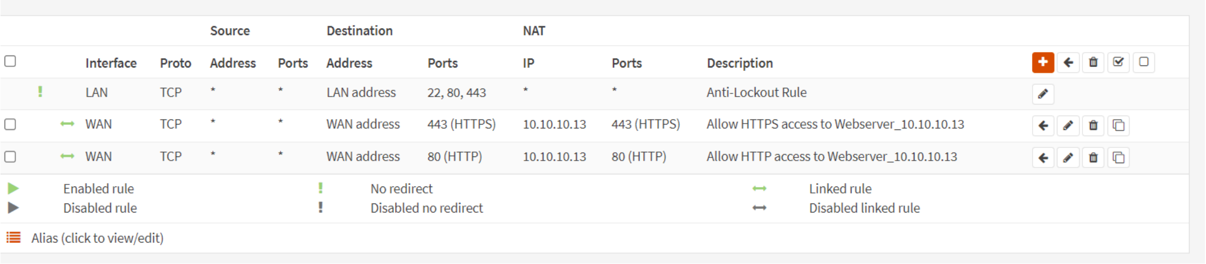
Redirect target IP	Single host or Network 10.10.10.13
Redirect target port	HTTP
Pool Options:	Default
Log	☑
Category	
Description	Allow HTTP access to Webserver_10.10.10.13
Set local tag	
Match local tag	
No XMLRPC Sync	☐
NAT reflection	Use system default
Filter rule association	Add associated filter rule

OPNsense (c) 2014-2021 Deciso B.V.

Figure 10. *Port forwarding rule configuration for HTTP in OPNsense-2*

Port Forwarding For HTTP Service of WebServer2 on Custom External Port(81)

To create a port forwarding rule for the HTTP service of the WebServer2 on custom port(81), you may clone the port forwarding rule for the HTTP(80) service created above and change the related settings by following the step given below.



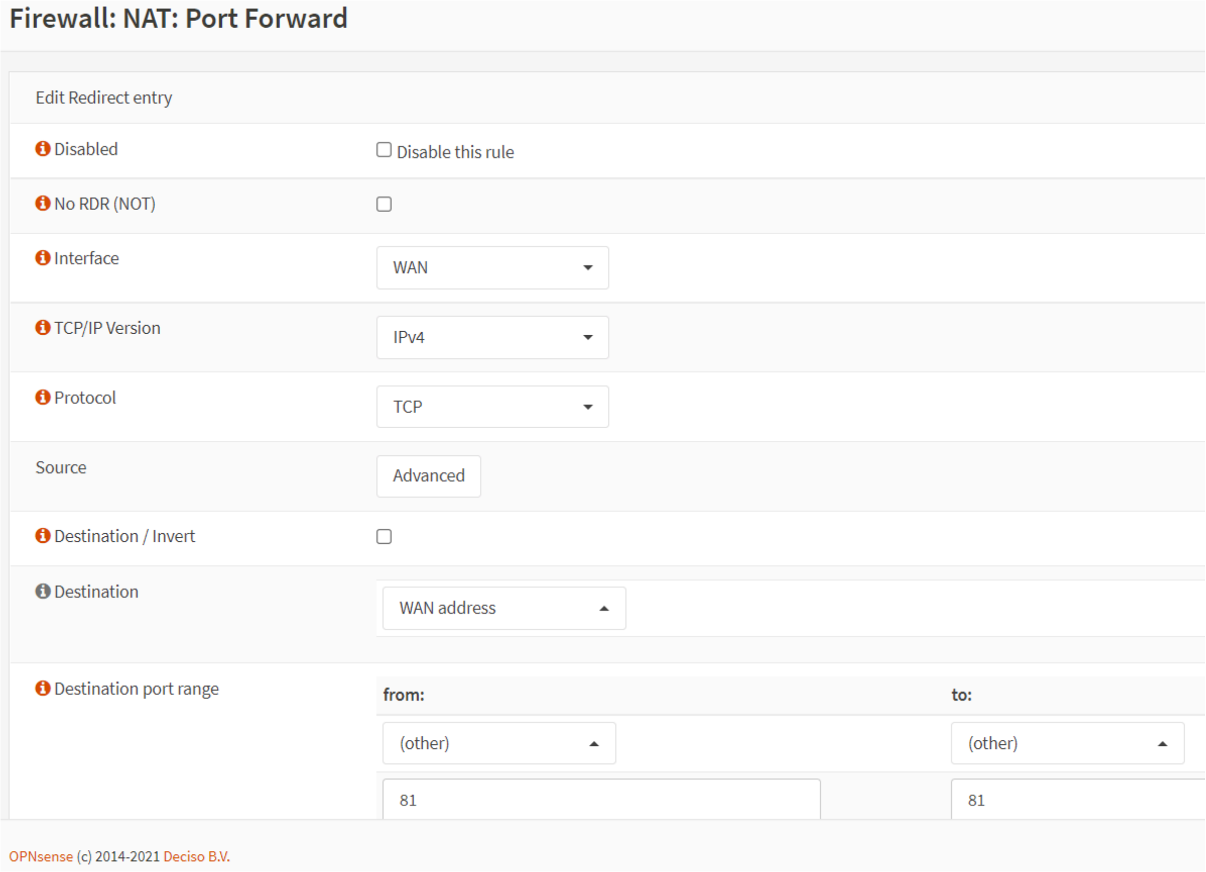
				Source		Destination		NAT		
☐		Interface	Proto	Address	Ports	Address	Ports	IP	Ports	Description
	!	LAN	TCP	*	*	LAN address	22, 80, 443	*	*	Anti-Lockout Rule
☐	⟷	WAN	TCP	*	*	WAN address	443 (HTTPS)	10.10.10.13	443 (HTTPS)	Allow HTTPS access to Webserver_10.10.10.13
☐	⟷	WAN	TCP	*	*	WAN address	80 (HTTP)	10.10.10.13	80 (HTTP)	Allow HTTP access to Webserver_10.10.10.13

▶ Enabled rule
▶ Disabled rule
! No redirect
! Disabled no redirect
⟷ Linked rule
⟷ Disabled linked rule

Alias (click to view/edit)

Figure 11. *Port forwarding rules list in OPNsense*

1. Click the clone icon to copy the port forwarding rule for the HTTP(80) service created above.
2. Change the Destination Port Range option to **`other`** and enter **`81`** to the related field.



Firewall: NAT: Port Forward

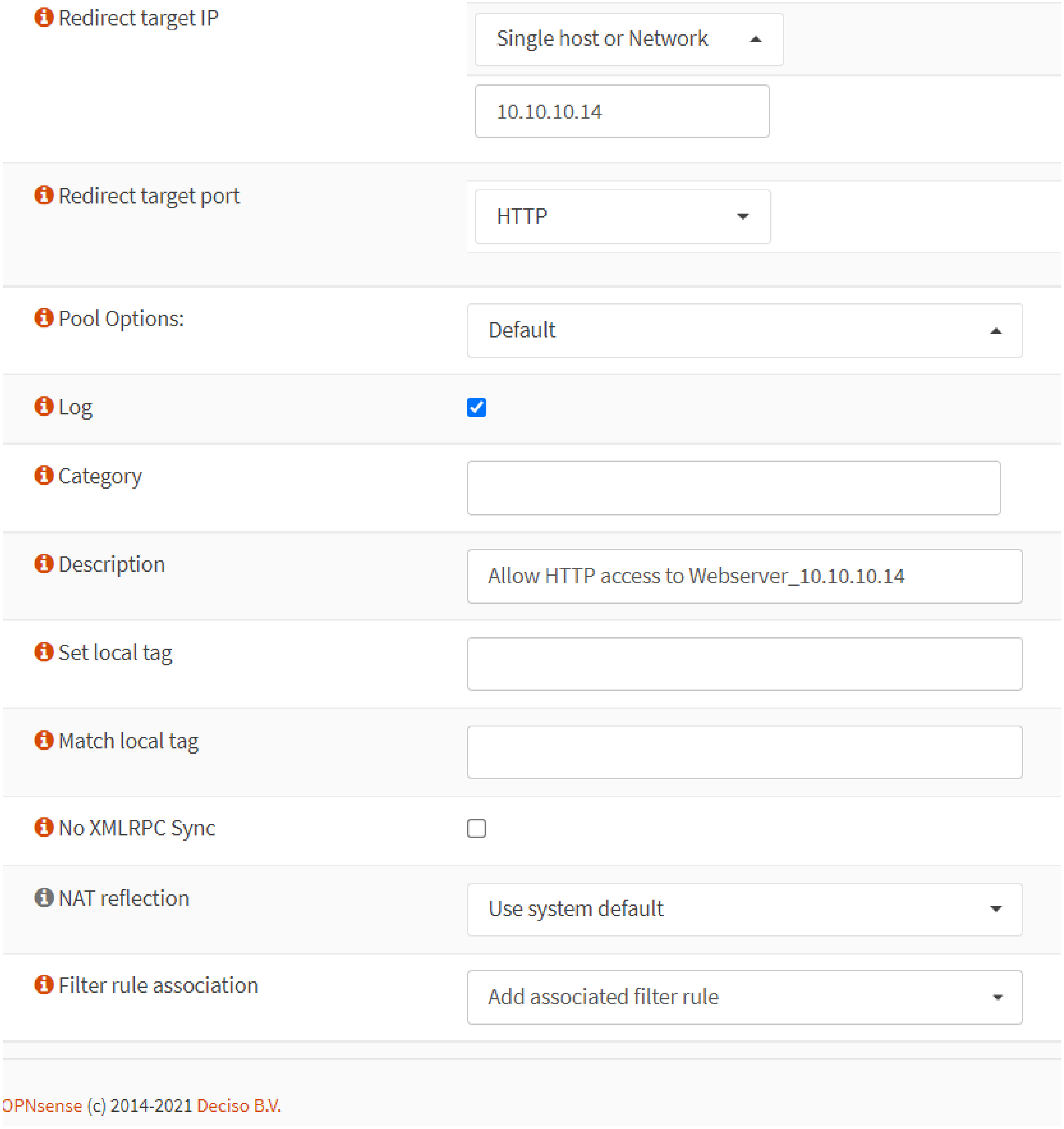
Edit Redirect entry

Disabled	☐ Disable this rule
No RDR (NOT)	☐
Interface	WAN
TCP/IP Version	IPv4
Protocol	TCP
Source	Advanced
Destination / Invert	☐
Destination	WAN address
Destination port range	from: (other) 81 to: (other) 81

OPNsense (c) 2014-2021 Deciso B.V.

Figure 12. *Port forwarding rule configuration for HTTP(81) in OPNsense-1*

3. Set the Redirect Target IP to **`10.10.10.14.`**
4. Set the Redirect Target Port to **HTTP**.
5. Change the Description field to `Allow HTTP access to Webserver_10.10.10.14`.
6. Verify that the Filter rule association option is set to Add `associated filter rule`
7. Leave other options as they are.
8. Click **`Save`** button at the bottom of the page.



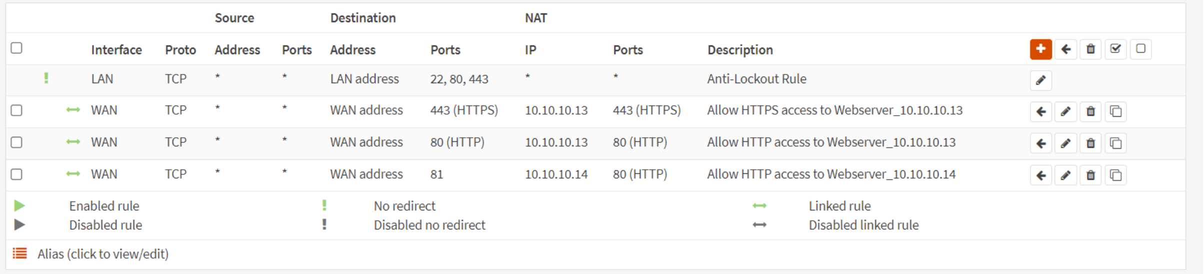
Redirect target IP	Single host or Network 10.10.10.14
Redirect target port	HTTP
Pool Options:	Default
Log	☑
Category	
Description	Allow HTTP access to Webserver_10.10.10.14
Set local tag	
Match local tag	
No XMLRPC Sync	□
NAT reflection	Use system default
Filter rule association	Add associated filter rule

OPNsense (c) 2014-2021 Deciso B.V.

Figure 13. *Port forwarding rule configuration for HTTP(81) in OPNsense-2*

Port Forwarding For HTTPS Service of WebServer2 on Custom External Port (8443)

To create a port forwarding rule for the HTTPS service of the WebServer2 on a custom external port(8443), you may clone the port forwarding rule for the HTTP(81) service created above and change the related settings by following the step given below.



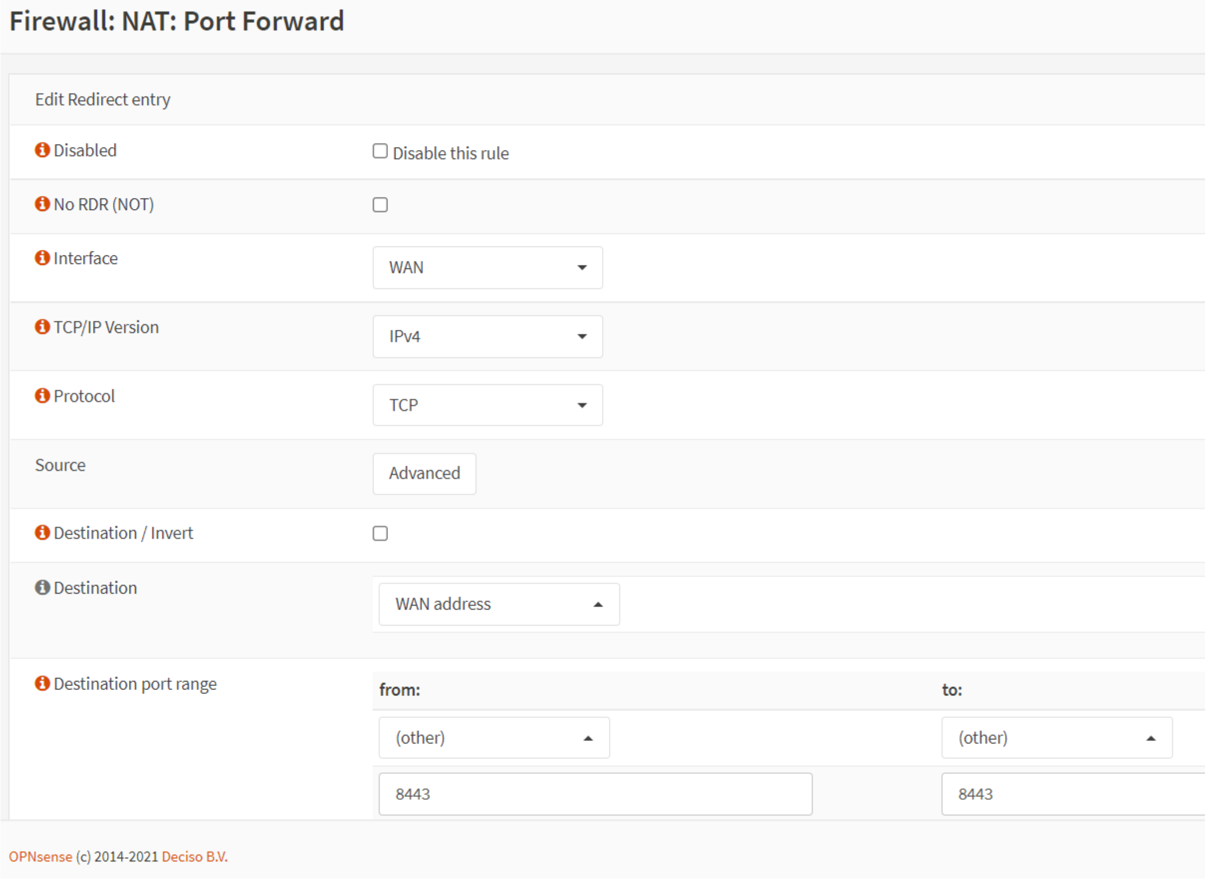
				Source		Destination		NAT		
□		Interface	Proto	Address	Ports	Address	Ports	IP	Ports	Description
	!	LAN	TCP	*	*	LAN address	22, 80, 443	*	*	Anti-Lockout Rule
□	⟷	WAN	TCP	*	*	WAN address	443 (HTTPS)	10.10.10.13	443 (HTTPS)	Allow HTTPS access to Webserver_10.10.10.13
□	⟷	WAN	TCP	*	*	WAN address	80 (HTTP)	10.10.10.13	80 (HTTP)	Allow HTTP access to Webserver_10.10.10.13
□	⟷	WAN	TCP	*	*	WAN address	81	10.10.10.14	80 (HTTP)	Allow HTTP access to Webserver_10.10.10.14

▶ Enabled rule ! No redirect ⟷ Linked rule
▶ Disabled rule ! Disabled no redirect ⟷ Disabled linked rule

☰ Alias (click to view/edit)

Figure 14. *Port forwarding rules list in OPNsense*

1. Click the clone icon to copy the port forwarding rule for the HTTP(81) service created above.
2. Change the Destination Port Range option to **8443**.



Firewall: NAT: Port Forward

Edit Redirect entry

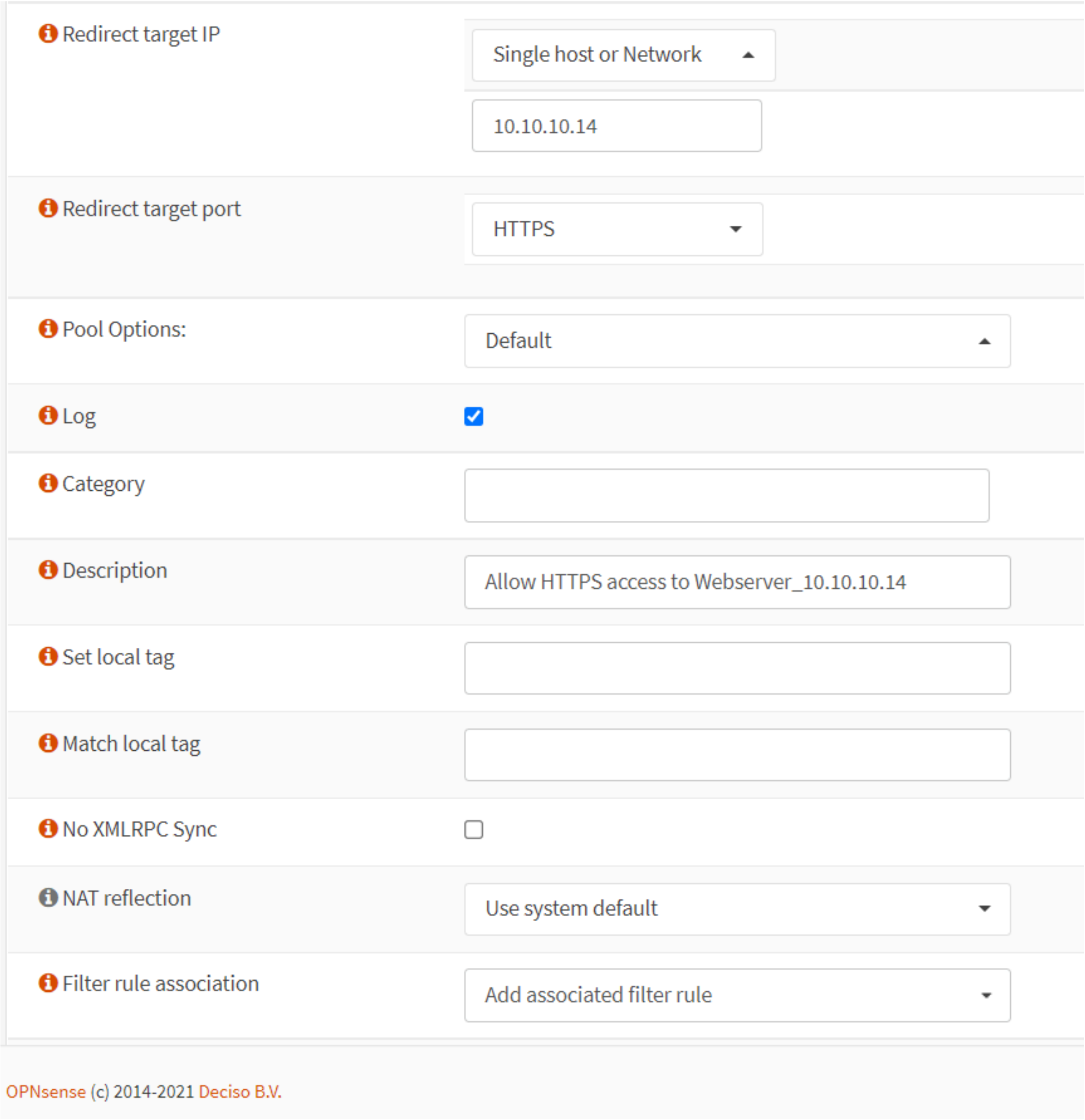
Disabled	□ Disable this rule
No RDR (NOT)	□
Interface	WAN
TCP/IP Version	IPv4
Protocol	TCP
Source	Advanced
Destination / Invert	□
Destination	WAN address
Destination port range	from: (other) 8443 — to: (other) 8443

OPNsense (c) 2014-2021 Deciso B.V.

Figure 15. *Port forwarding rule configuration for HTTP(8443) in OPNsense-1*

3. Set the Redirect Target Port to **HTTPS**.
4. Change the Description field to `Allow HTTPS access to Webserver_10.10.10.14`.
5. Verify that the Filter rule association option is set to Add `associated filter rule`
6. Leave other options as they are.

7. Click **Save** button at the bottom of the page.

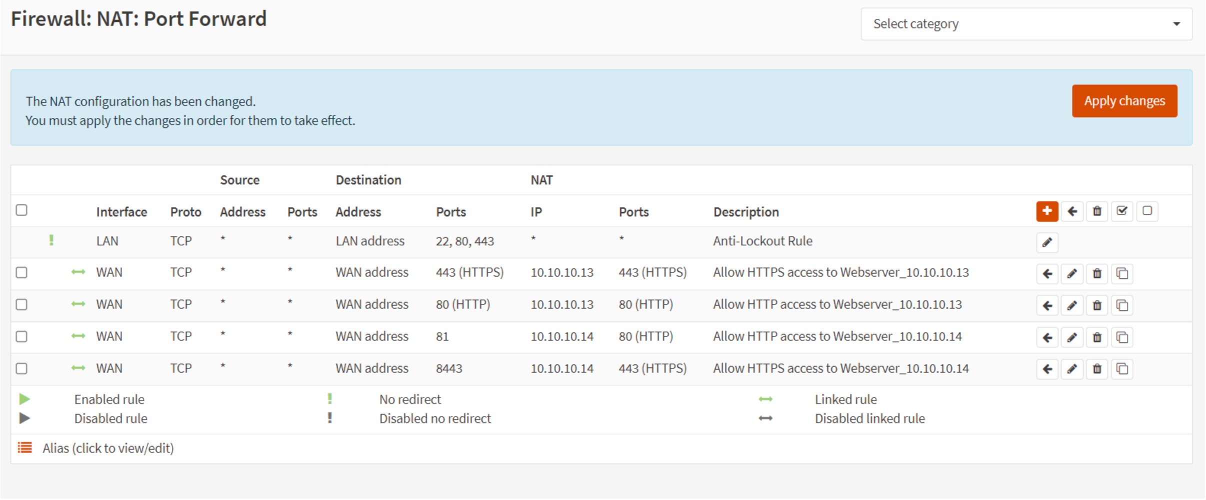


Redirect target IP	Single host or Network 10.10.10.14
Redirect target port	HTTPS
Pool Options:	Default
Log	☑
Category	
Description	Allow HTTPS access to Webserver_10.10.10.14
Set local tag	
Match local tag	
No XMLRPC Sync	□
NAT reflection	Use system default
Filter rule association	Add associated filter rule

OPNsense (c) 2014-2021 Deciso B.V.

Figure 16. *Port forwarding rule configuration for HTTP(8443) in OPNsense-2*

Now, you have completed the port forwarding configurations of both web servers. Your port forwarding rules list should look like this.



Firewall: NAT: Port Forward

The NAT configuration has been changed.
You must apply the changes in order for them to take effect.

			Source		Destination		NAT		
□	Interface	Proto	Address	Ports	Address	Ports	IP	Ports	Description
!	LAN	TCP	*	*	LAN address	22, 80, 443	*	*	Anti-Lockout Rule
□ ↔	WAN	TCP	*	*	WAN address	443 (HTTPS)	10.10.10.13	443 (HTTPS)	Allow HTTPS access to Webserver_10.10.10.13
□ ↔	WAN	TCP	*	*	WAN address	80 (HTTP)	10.10.10.13	80 (HTTP)	Allow HTTP access to Webserver_10.10.10.13
□ ↔	WAN	TCP	*	*	WAN address	81	10.10.10.14	80 (HTTP)	Allow HTTP access to Webserver_10.10.10.14
□ ↔	WAN	TCP	*	*	WAN address	8443	10.10.10.14	443 (HTTPS)	Allow HTTPS access to Webserver_10.10.10.14

▶ Enabled rule
▶ Disabled rule
! No redirect
! Disabled no redirect
↔ Linked rule
↔ Disabled linked rule

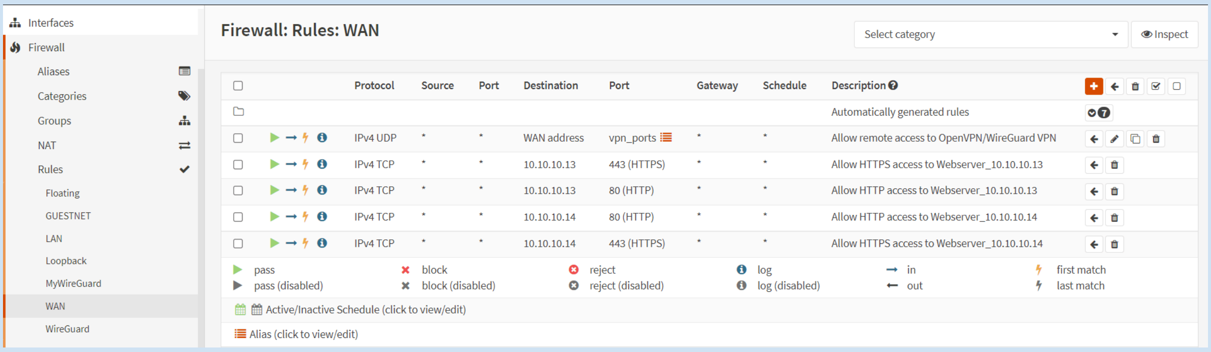
☰ Alias (click to view/edit)

Figure 17. *Port forwarding rules list for web servers in OPNsense*

8. Click **`Apply Changes`** at the upper right of the page to activate the settings.

📣 INFO

Since we have selected the **`Add associated filter rule`** option, the related firewall rules are created on the WAN interface automatically. To view the automatically added associated rules, navigate to the **`Firewall -> Rules -> WAN`**. Firewall rules list on WAN interfaces should look like this:



Firewall: Rules: WAN

□		Protocol	Source	Port	Destination	Port	Gateway	Schedule	Description
									Automatically generated rules
□	▶ → ϟ ℹ	IPv4 UDP	*	*	WAN address	vpn_ports ☰	*	*	Allow remote access to OpenVPN/WireGuard VPN
□	▶ → ϟ ℹ	IPv4 TCP	*	*	10.10.10.13	443 (HTTPS)	*	*	Allow HTTPS access to Webserver_10.10.10.13
□	▶ → ϟ ℹ	IPv4 TCP	*	*	10.10.10.13	80 (HTTP)	*	*	Allow HTTP access to Webserver_10.10.10.13
□	▶ → ϟ ℹ	IPv4 TCP	*	*	10.10.10.14	80 (HTTP)	*	*	Allow HTTP access to Webserver_10.10.10.14
□	▶ → ϟ ℹ	IPv4 TCP	*	*	10.10.10.14	443 (HTTPS)	*	*	Allow HTTPS access to Webserver_10.10.10.14

▶ pass
▶ pass (disabled)
✖ block
✖ block (disabled)
⊗ reject
⊗ reject (disabled)
ℹ log
ℹ log (disabled)
→ in
← out
ϟ first match
ϟ last match

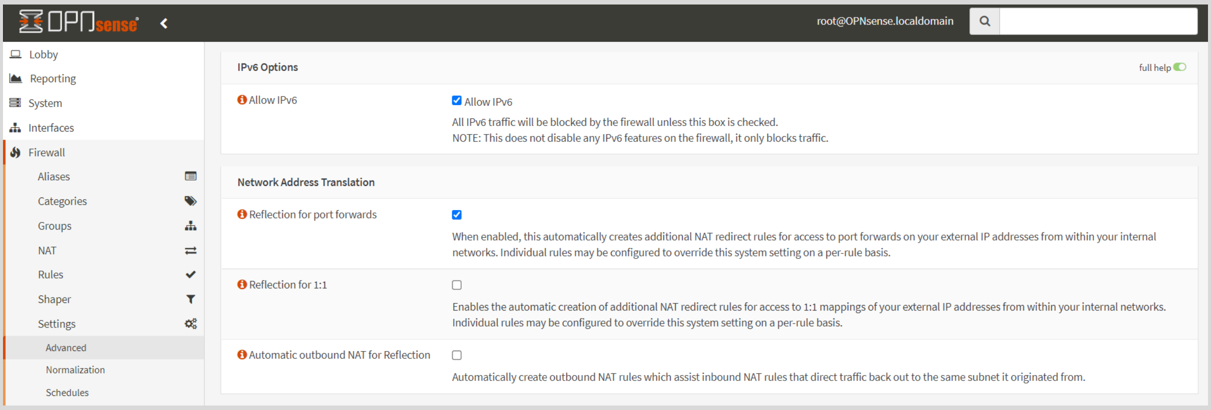
Active/Inactive Schedule (click to view/edit)

☰ Alias (click to view/edit)

Figure 18. *WAN firewall rules for web server port forwarding in OPNsense*

💡 TIP

Although internal users should access the web servers by connecting to the private IP address (local IP) of the servers, they may try to connect to a local server by using the public IP addresses. To allow local users to access the public IP addresses of these servers, you must allow the NAT reflection. For NAT reflection, first you should enable the NAT reflection by checking on the **`Reflection for port forwards`** option on the **`Firewall -> Settings ->Advanced`** page.



IPv6 Options

Allow IPv6 — ☑ Allow IPv6
All IPv6 traffic will be blocked by the firewall unless this box is checked.
NOTE: This does not disable any IPv6 features on the firewall, it only blocks traffic.

Network Address Translation

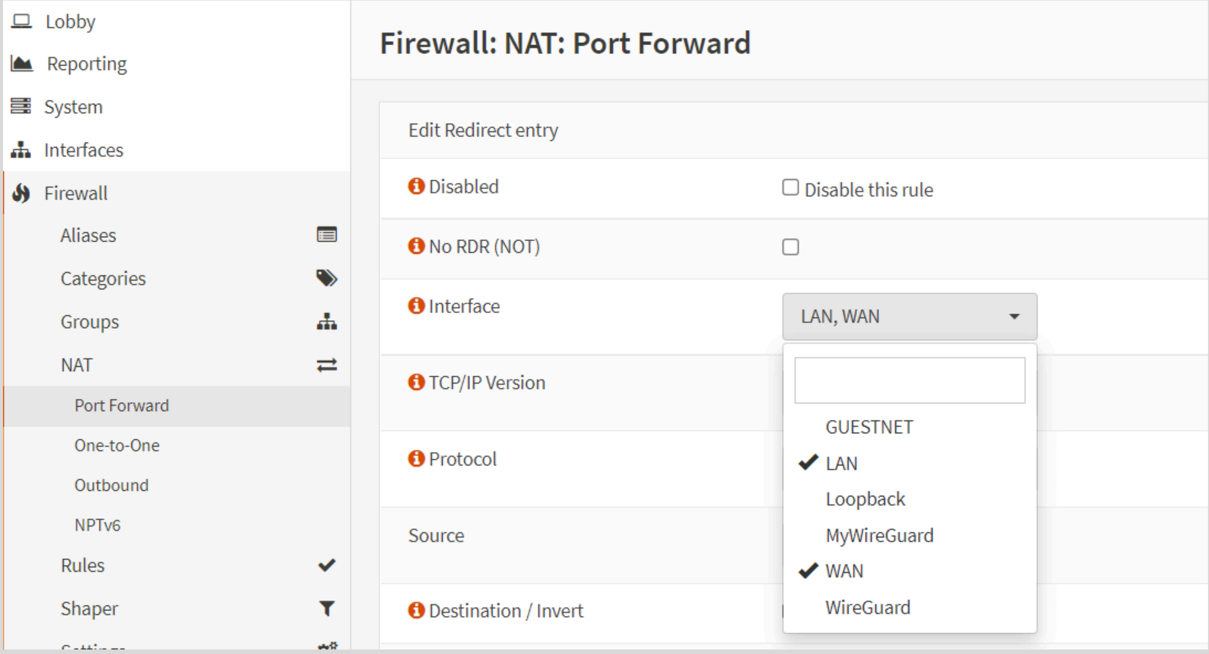
Reflection for port forwards — ☑
When enabled, this automatically creates additional NAT redirect rules for access to port forwards on your external IP addresses from within your internal networks. Individual rules may be configured to override this system setting on a per-rule basis.

Reflection for 1:1 — □
Enables the automatic creation of additional NAT redirect rules for access to 1:1 mappings of your external IP addresses from within your internal networks. Individual rules may be configured to override this system setting on a per-rule basis.

Automatic outbound NAT for Reflection — □
Automatically create outbound NAT rules which assist inbound NAT rules that direct traffic back out to the same subnet it originated from.

Figure 19. *Enabling Reflection for port forwards*

Then, you should select the interface where the local users are, such as LAN, as well as the WAN interface during the port forwarding rule configuration.



Firewall: NAT: Port Forward

Edit Redirect entry

Disabled — □ Disable this rule

No RDR (NOT) — □

Interface — LAN, WAN

TCP/IP Version

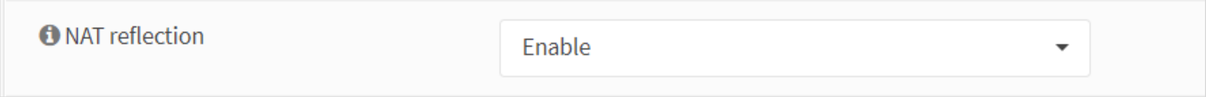
Protocol

Source

Destination / Invert

Figure 20. *NAT reflection*

Ensure that NAT reflection is enabled in the port forwarding rule configuration.



NAT reflection — Enable

Figure 21. *NAT reflection is enabled in port forwarding rule*

How to Configure Port Forwarding For SSH and RDP Services on Custom Ports

Assume that a web administrator needs remote(SSH & RDP) access to the web servers from his home. He is using a static public IP address at home. Since management services such as SSH and RDP are critical and pose a high security risk, it is recommended that they are not accessible from the entire Internet.As a result, you will create a port forwarding rule to allow the web administrator's IP address to connect to the web servers. Also, because the default ports are already in use for accessing other servers, you must enable SSH and RDP services on custom ports.

Server Name	External IP	External Port	Local IP	Local Port	Client IP
WebServer1	Public Internet IP	2222	10.10.10.13	22	1.1.1.1
WebServer2	Public Internet IP	5555	10.10.10.14	3389	1.1.1.1

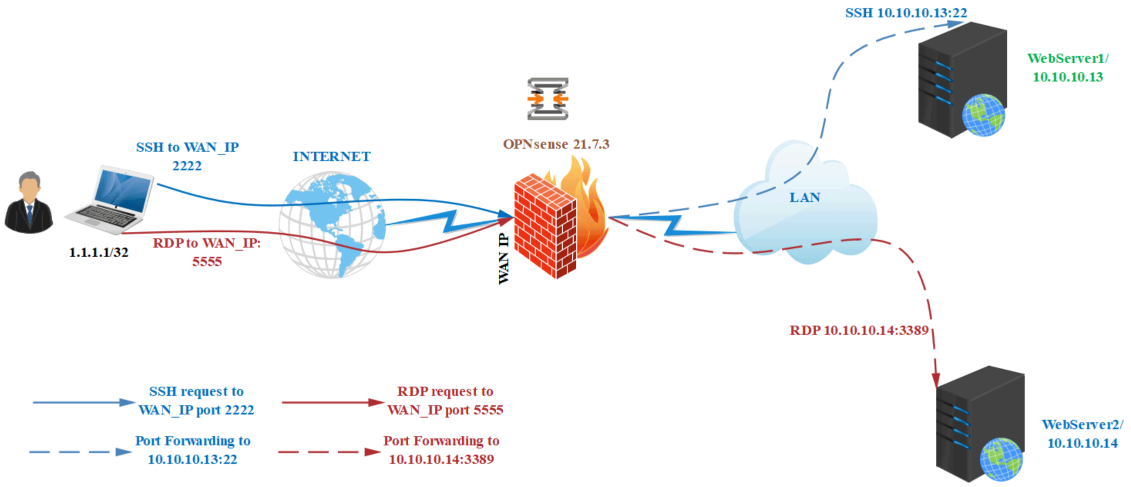


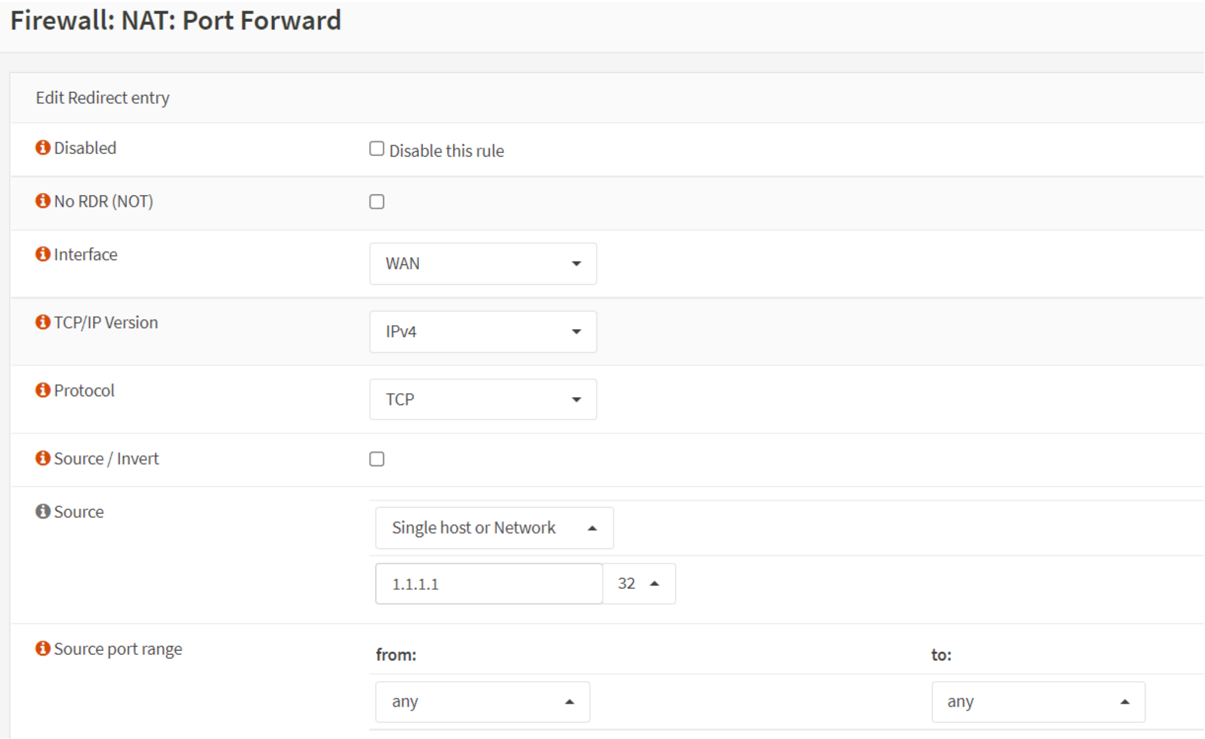
Figure 22. *Port Forwarding topology for SSH and RDP services*

After completing the port forwarding configurations in your OPNsense firewall, port 2222 requests coming from web administrator IP address(1.1.1.1) to your WAN IP will be redirected to the WebServer1(10.10.10.13),while port 5555 requests coming from web administrator IP address(1.1.1.1) to your WAN IP will be redirected to the WebServer2(10.10.10.14).

Port Forwarding For SSH Service of WebServer1 on Custom External Port(2222)

To create a port forwarding rule for the SSH service of the WebServer1 on custom port(2222), you may clone the port forwarding rule for the HTTP(80) service created above and change the related settings by following the step given below.

1. Click the clone icon to copy the port forwarding rule for the HTTP(80) service created above.
2. Click the `Advanced` button in the `Source` option. This will displays the details of the Source option.
3. Select `Single Host or Network` from the Source dropdown menu.
4. Enter the Web Administrator's static public IP address, such as 1.1.1.1/32.
5. Leave Source Port Range as **any**.



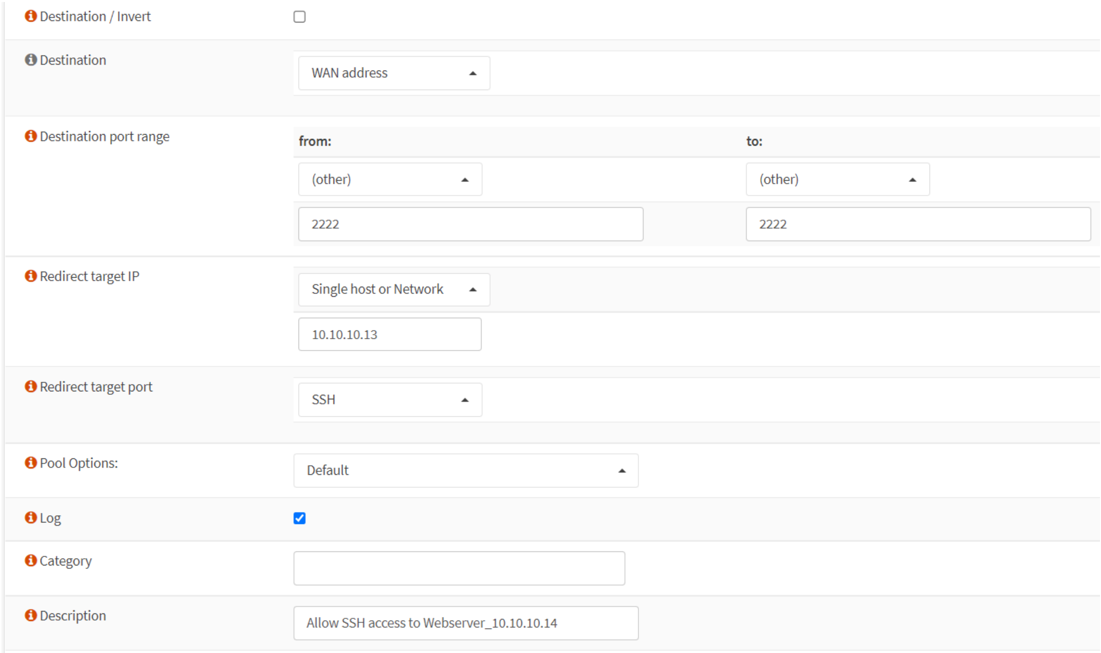
Firewall: NAT: Port Forward

Edit Redirect entry

Disabled	□ Disable this rule
No RDR (NOT)	□
Interface	WAN
TCP/IP Version	IPv4
Protocol	TCP
Source / Invert	□
Source	Single host or Network 1.1.1.1 / 32
Source port range	from: any to: any

Figure 23. *Port forwarding rule configuration for SSH(2222) in OPNsense-1*

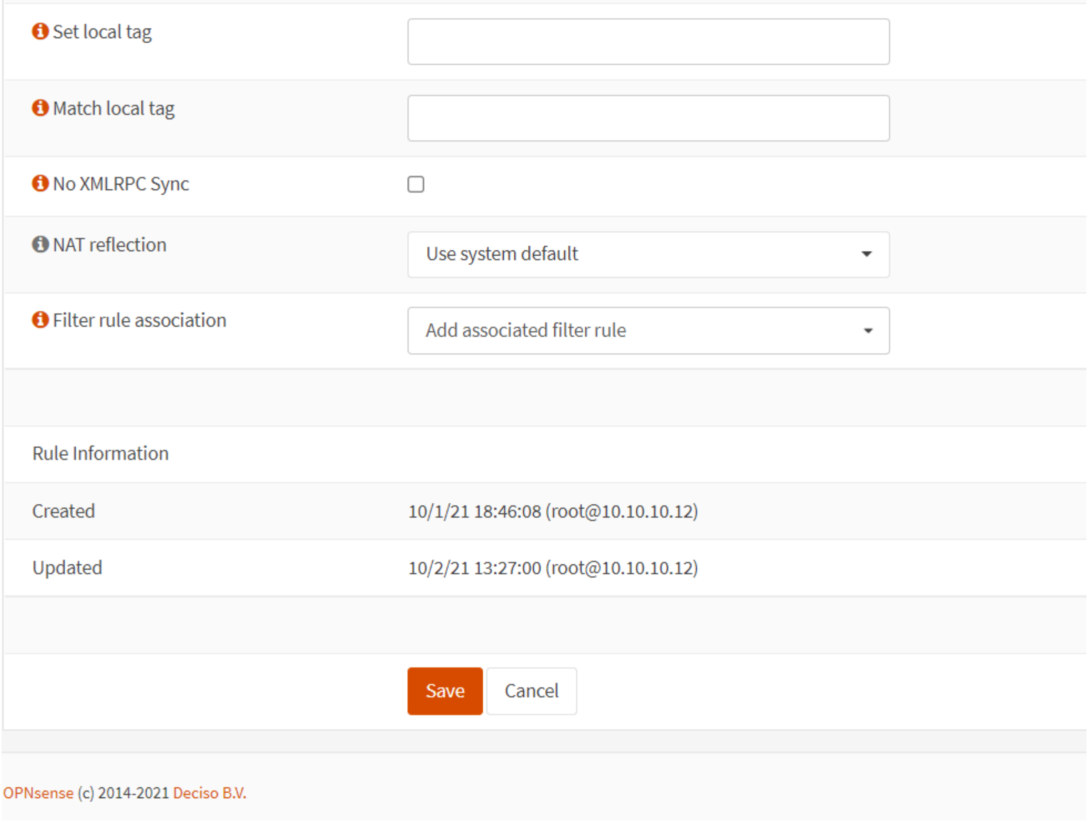
6. Change the Destination Port Range option to **2222**.
7. Set the Redirect Target Port to **SSH**.
8. Change the Description field to `Allow SSH access to Webserver_10.10.10.13`.



Destination / Invert	☐
Destination	WAN address
Destination port range	from: (other) 2222 to: (other) 2222
Redirect target IP	Single host or Network 10.10.10.13
Redirect target port	SSH
Pool Options:	Default
Log	☑
Category	
Description	Allow SSH access to Webserver_10.10.10.14

Figure 24. *Port forwarding rule configuration for SSH(2222) in OPNsense-2*

9. Verify that the Filter rule association option is set to `Add associated filter rule`
10. Leave other options as they are.
11. Click **Save** button at the bottom of the page.



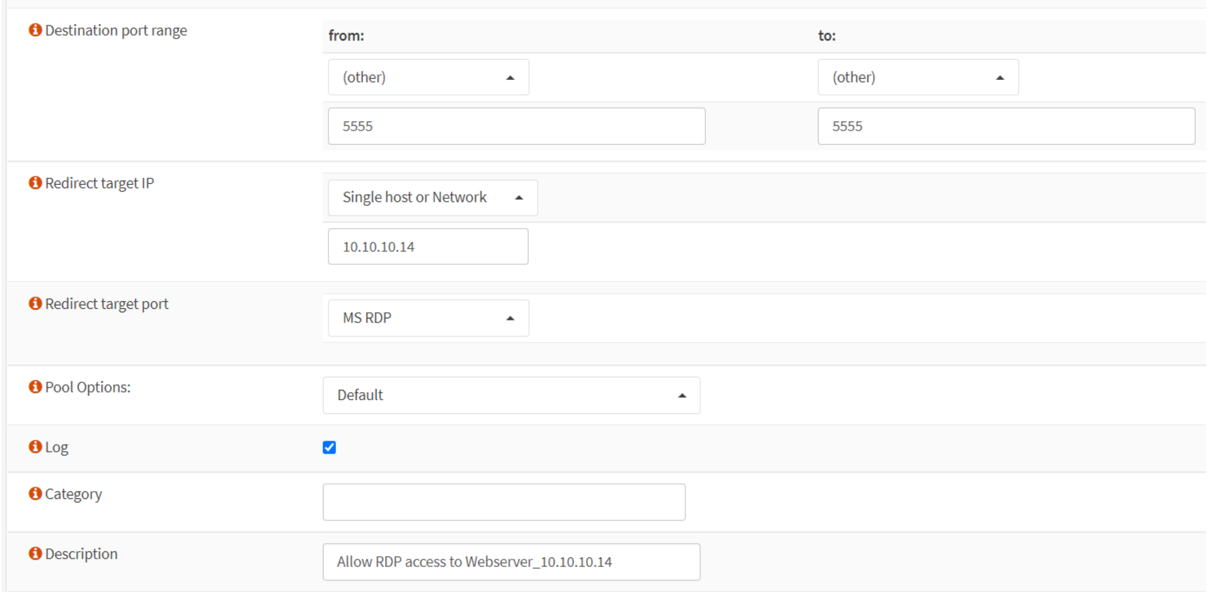
Set local tag	
Match local tag	
No XMLRPC Sync	☐
NAT reflection	Use system default
Filter rule association	Add associated filter rule
Rule Information	
Created	10/1/21 18:46:08 (root@10.10.10.12)
Updated	10/2/21 13:27:00 (root@10.10.10.12)

Figure 25. *Port forwarding rule configuration for SSH(2222) in OPNsense-3*

Port Forwarding For RDP Service of WebServer2 on Custom External Port(5555)

To create a port forwarding rule for the RDP service of the WebServer2 on custom port(5555), you may clone the port forwarding rule for the SSH(2222) service created above and change the related settings by following the step given below.

1. Click the clone icon to copy the port forwarding rule for the SSH(2222) service created above in the port forward rules list.
2. Change the Destination Port Range option to **5555**.
3. Set the Redirect Target IP to WebServer2 local IP address, such as 10.10.10.14.
4. Set the Redirect Target Port to `MS RDP`.
5. Change the Description field to `Allow RDP access to Webserver_10.10.10.14`.



Destination port range — from: (other) 5555 — to: (other) 5555

Redirect target IP: Single host or Network, 10.10.10.14

Redirect target port: MS RDP

Pool Options: Default

Log: ☑

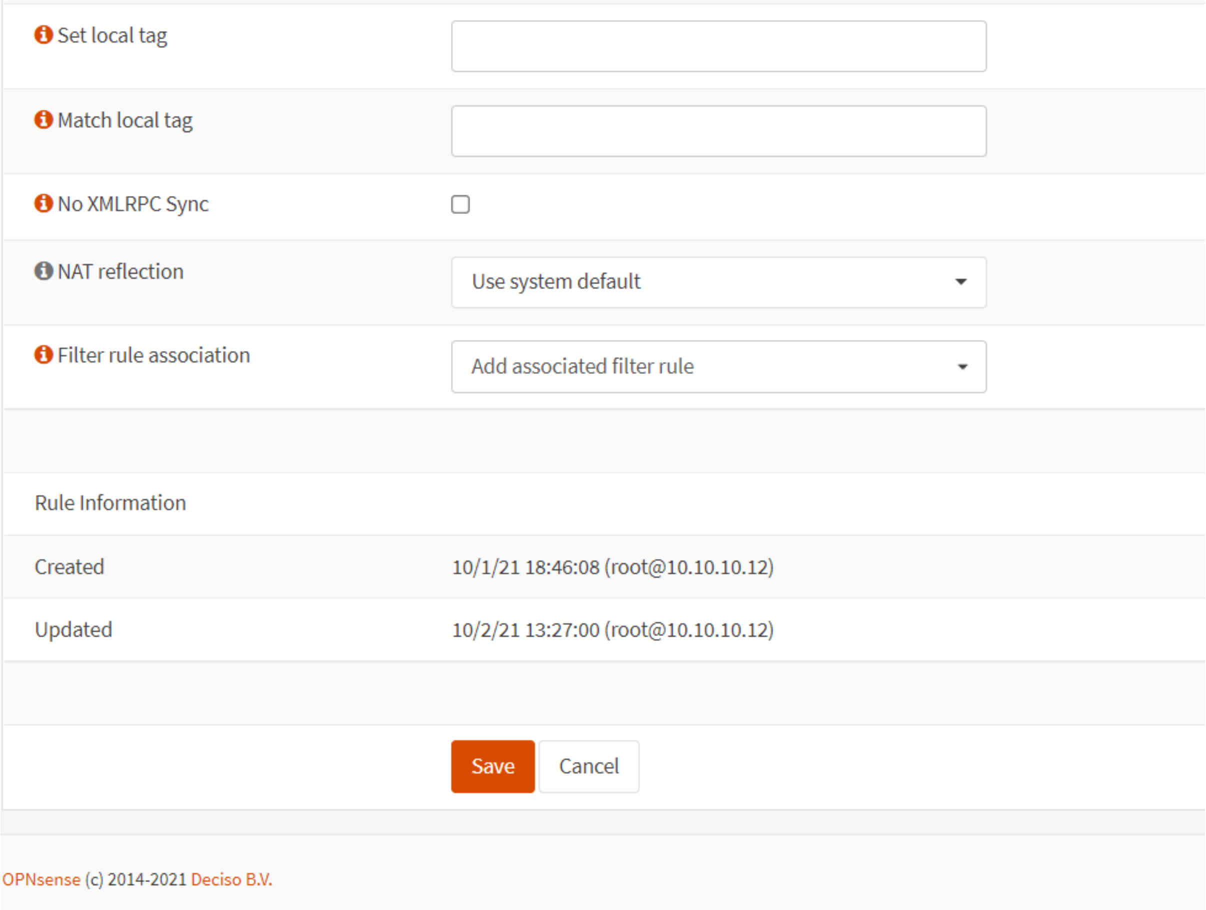
Category:

Description: Allow RDP access to Webserver_10.10.10.14

Figure 26. *Port forwarding rule configuration for MS-RDP(5555) in OPNsense-1*

6. Verify that the Filter rule association option is set to Add `associated filter rule`
7. Leave other options as they are.

8. Click **Save** button at the bottom of the page.



Set local tag	
Match local tag	
No XMLRPC Sync	□
NAT reflection	Use system default
Filter rule association	Add associated filter rule

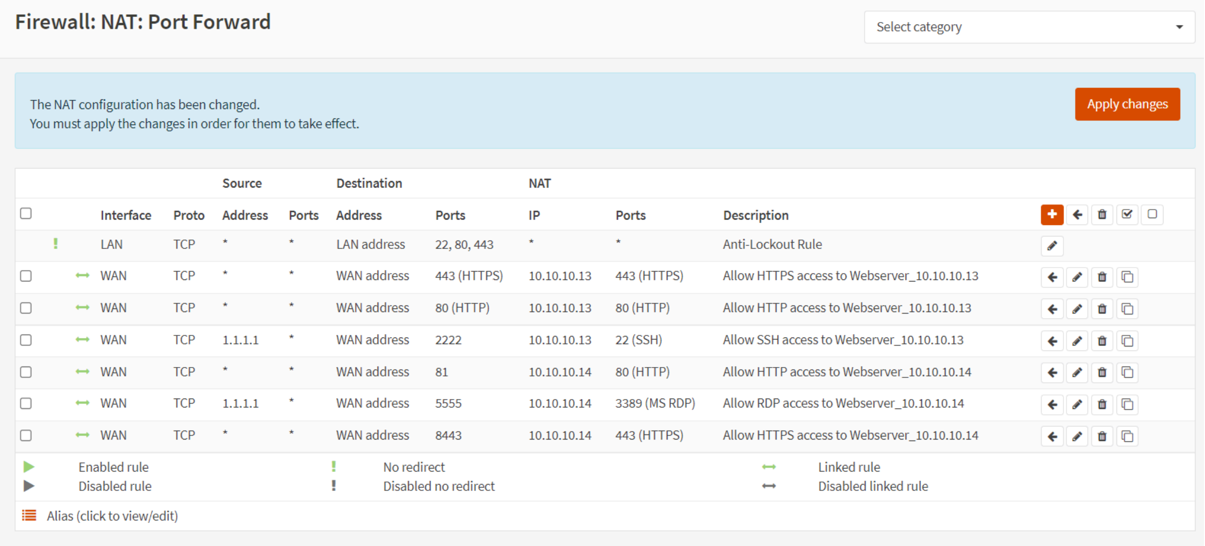
Rule Information

Created	10/1/21 18:46:08 (root@10.10.10.12)
Updated	10/2/21 13:27:00 (root@10.10.10.12)

OPNsense (c) 2014-2021 Deciso B.V.

Figure 27. *Port forwarding rule configuration for SSH(2222) in OPNsense-3*

Now, you have completed the port forwarding rule configurations of both management services. Your port forwarding rules list should look like this.



Firewall: NAT: Port Forward

The NAT configuration has been changed.
You must apply the changes in order for them to take effect.

				Source		Destination		NAT		
□		Interface	Proto	Address	Ports	Address	Ports	IP	Ports	Description
	!	LAN	TCP	*	*	LAN address	22, 80, 443	*	*	Anti-Lockout Rule
□	⟷	WAN	TCP	*	*	WAN address	443 (HTTPS)	10.10.10.13	443 (HTTPS)	Allow HTTPS access to Webserver_10.10.10.13
□	⟷	WAN	TCP	*	*	WAN address	80 (HTTP)	10.10.10.13	80 (HTTP)	Allow HTTP access to Webserver_10.10.10.13
□	⟷	WAN	TCP	1.1.1.1	*	WAN address	2222	10.10.10.13	22 (SSH)	Allow SSH access to Webserver_10.10.10.13
□	⟷	WAN	TCP	*	*	WAN address	81	10.10.10.14	80 (HTTP)	Allow HTTP access to Webserver_10.10.10.14
□	⟷	WAN	TCP	1.1.1.1	*	WAN address	5555	10.10.10.14	3389 (MS RDP)	Allow RDP access to Webserver_10.10.10.14
□	⟷	WAN	TCP	*	*	WAN address	8443	10.10.10.14	443 (HTTPS)	Allow HTTPS access to Webserver_10.10.10.14

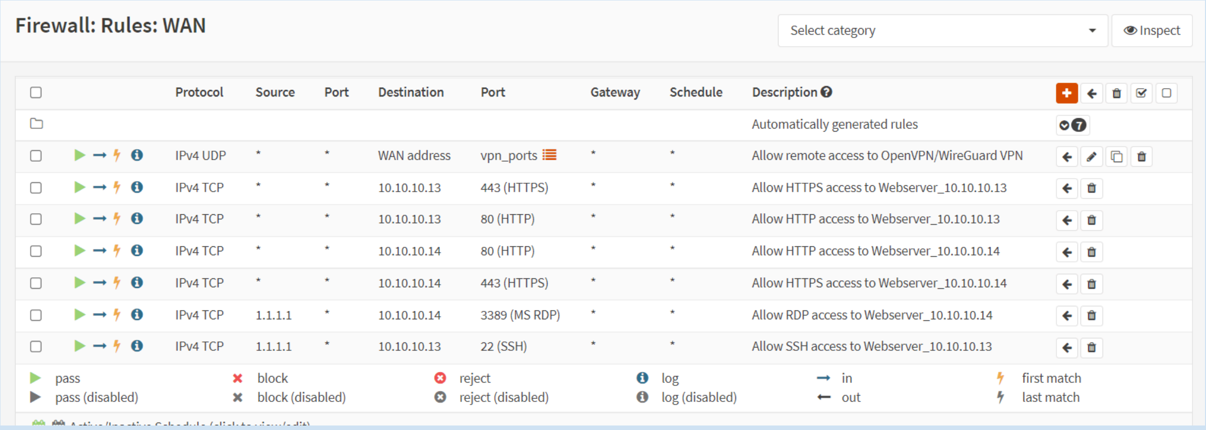
▶ Enabled rule
▶ Disabled rule
! No redirect
! Disabled no redirect
⟷ Linked rule
⟷ Disabled linked rule
☰ Alias (click to view/edit)

Figure 28. *Port forwarding rules list for web servers in OPNsense*

9. Click **Apply Changes** at the upper right of the page to activate the settings.

📣 **INFO**

Since we have selected the **`Add associated filter rule`** option, the related firewall rules are created on the WAN interface automatically. To view the automatically added associated rules, navigate to the **`Firewall -> Rules -> WAN`**. Firewall rules list on WAN interfaces should look like this:



Firewall: Rules: WAN

Select category ▾ | Inspect

□		Protocol	Source	Port	Destination	Port	Gateway	Schedule	Description
									Automatically generated rules
□	▶ → ϟ ℹ	IPv4 UDP	*	*	WAN address	vpn_ports	*	*	Allow remote access to OpenVPN/WireGuard VPN
□	▶ → ϟ ℹ	IPv4 TCP	*	*	10.10.10.13	443 (HTTPS)	*	*	Allow HTTPS access to Webserver_10.10.10.13
□	▶ → ϟ ℹ	IPv4 TCP	*	*	10.10.10.13	80 (HTTP)	*	*	Allow HTTP access to Webserver_10.10.10.13
□	▶ → ϟ ℹ	IPv4 TCP	*	*	10.10.10.14	80 (HTTP)	*	*	Allow HTTP access to Webserver_10.10.10.14
□	▶ → ϟ ℹ	IPv4 TCP	*	*	10.10.10.14	443 (HTTPS)	*	*	Allow HTTPS access to Webserver_10.10.10.14
□	▶ → ϟ ℹ	IPv4 TCP	1.1.1.1	*	10.10.10.14	3389 (MS RDP)	*	*	Allow RDP access to Webserver_10.10.10.14
□	▶ → ϟ ℹ	IPv4 TCP	1.1.1.1	*	10.10.10.13	22 (SSH)	*	*	Allow SSH access to Webserver_10.10.10.13

▶ pass ✖ block ⊗ reject ℹ log → in ϟ first match
▶ pass (disabled) ✖ block (disabled) ⊗ reject (disabled) ℹ log (disabled) ← out ϟ last match

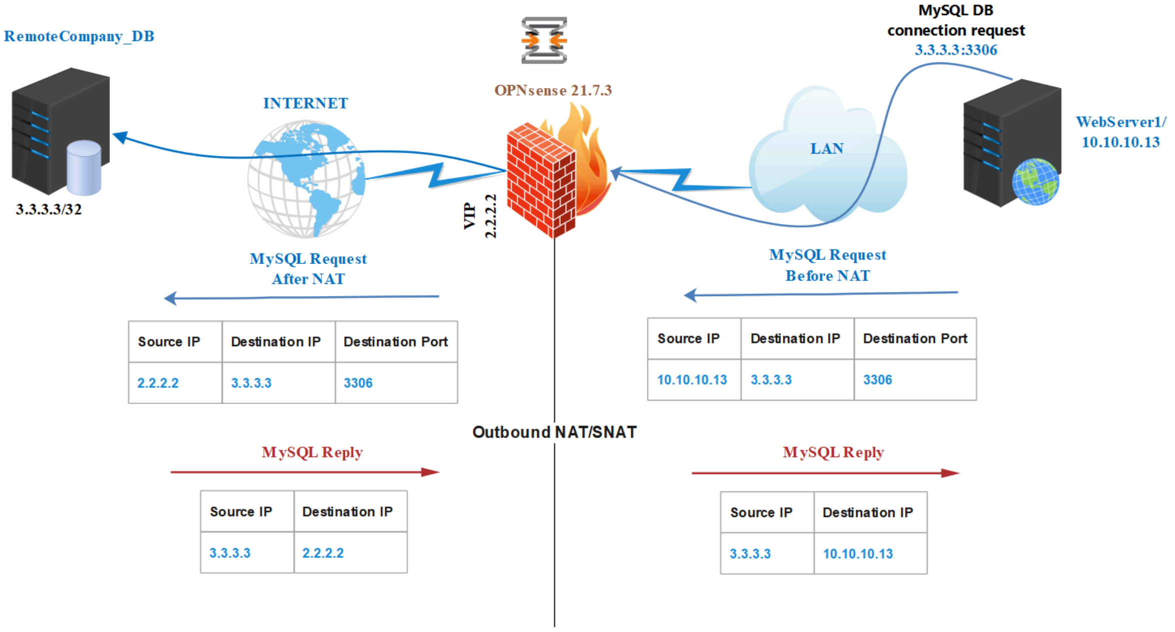
Figure 29. *WAN firewall rules for SSH and RDP access in OPNsense*

Outbound NAT For Accessing a Remote Service Via Specific External IP Address

Assume that one of your application servers (WebServer1 with the IP address 10.10.10.13) needs to connect to a MySQL database on another company network via the Internet. However, in accordance with the agreements between your company and the other company, you must ensure that the remote MySQL DB server(public IP address: 3.3.3.3) is only accessible by WebServer1 and that no other devices in your LAN can access the remote DB.

To accomplish this, firstly you need a second public IP address which will be used for providing WebServer1 access to the remote MySQL database. Because, your first public IP address is being used for Internet access of the local users and servers. We will use the **`2.2.2.2`** as our second IP address and WebServer1 will connect to the remote MySQL database with this external IP address.

Packet Type	**Source IP Before NAT**	**Destination IP Before NAT**	**Source IP After NAT**	**Destination IP After NAT**
MySQL Request	10.10.10.13	3.3.3.3	2.2.2.2	3.3.3.3
MySQL Reply	3.3.3.3	2.2.2.2	3.3.3.3	10.10.10.13



Source IP	Destination IP	Destination Port
2.2.2.2	3.3.3.3	3306

Source IP	Destination IP	Destination Port
10.10.10.13	3.3.3.3	3306

Source IP	Destination IP
3.3.3.3	2.2.2.2

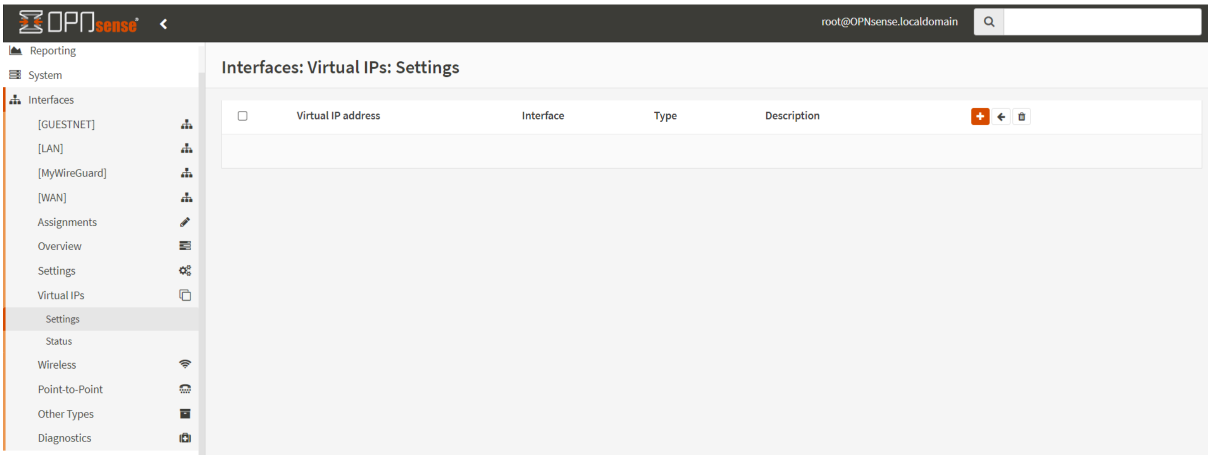
Source IP	Destination IP
3.3.3.3	10.10.10.13

Figure 30. *Outbound NAT/SNAT topology for accessing remote Database server*

You may follow the next steps given below:

1. Define an alias, such as `RemoteCompany_DB`. For more information about creating an alias, please refer to [How to Configure OPNsense Firewall]() article.
2. To create a Virtual IP address for your second public IP address, navigate to the **`Interfaces`** -> **`Virtual IPs`** -> **`Settings`**.

3. Click the **+** icon to add Virtual IP address.

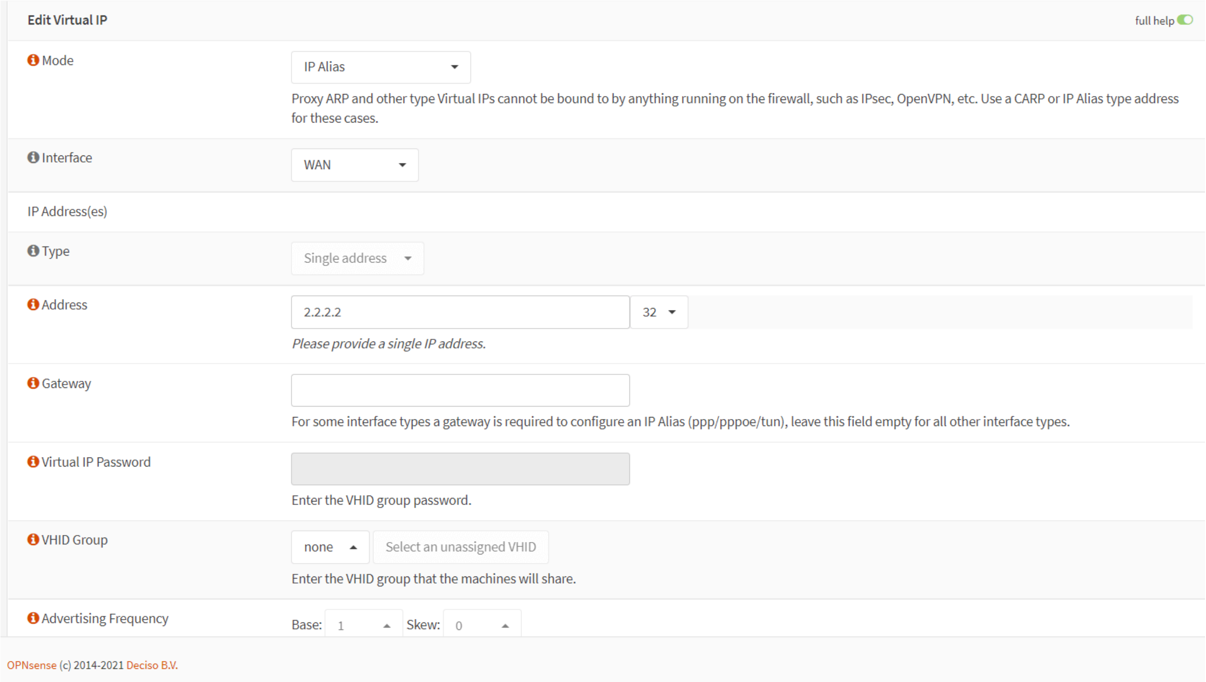


Interfaces: Virtual IPs: Settings

□	Virtual IP address	Interface	Type	Description	+ ← 🗑

Figure 31. *Adding Virtual IP address in OPNsense*

4. Select `IP Alias` as Mode.
5. Select `WAN` as Interface.
6. Set Address to your second public IP address which is used for accessing the database server by your WebServer1, such as **`2.2.2.2/32.`**
7. Enter `WAN VIP_2.2.2.2` in the Description field.
8. Leave other options as default.
9. Click **`Save`**.



Edit Virtual IP

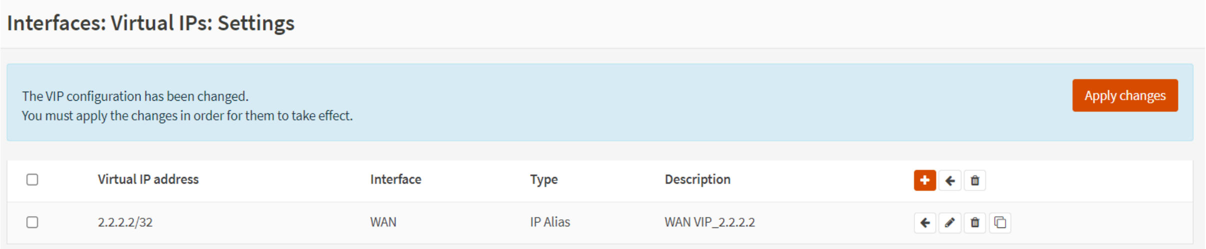
full help

Mode	IP Alias Proxy ARP and other type Virtual IPs cannot be bound to by anything running on the firewall, such as IPsec, OpenVPN, etc. Use a CARP or IP Alias type address for these cases.
Interface	WAN
IP Address(es)	
Type	Single address
Address	2.2.2.2 / 32 *Please provide a single IP address.*
Gateway	 For some interface types a gateway is required to configure an IP Alias (ppp/pppoe/tun), leave this field empty for all other interface types.
Virtual IP Password	 Enter the VHID group password.
VHID Group	none · Select an unassigned VHID Enter the VHID group that the machines will share.
Advertising Frequency	Base: 1 Skew: 0

OPNsense (c) 2014-2021 Deciso B.V.

Figure 32. *Setting Virtual IP address configuration in OPNsense*

10. Click **Apply Changes** to activate the VIPs settings.



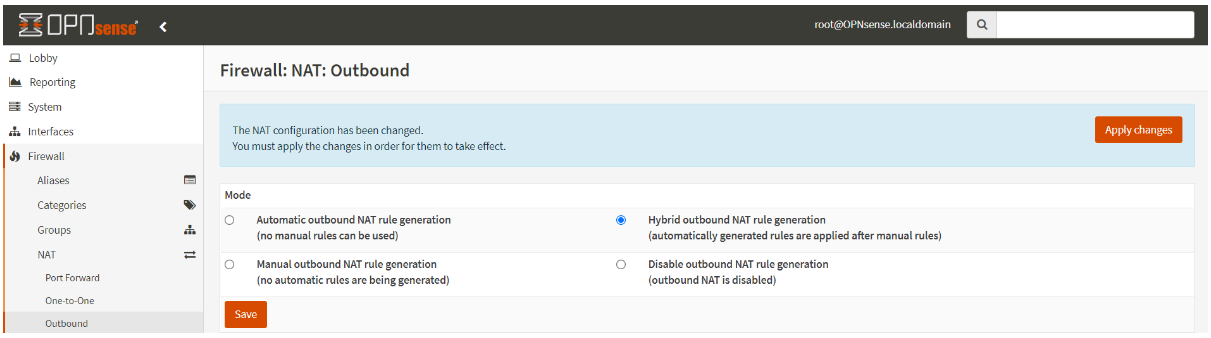
Interfaces: Virtual IPs: Settings

The VIP configuration has been changed.
You must apply the changes in order for them to take effect.

□	Virtual IP address	Interface	Type	Description
□	2.2.2.2/32	WAN	IP Alias	WAN VIP_2.2.2.2

Figure 33. *Virtual IP address settings in OPNsense*

11. Navigate to the **Firewall -> NAT -> Outbound** to define Outbound NAT.
12. Select `Hybrid outbound NAT rule generation` option.
13. Click **Save** button.



Firewall: NAT: Outbound

The NAT configuration has been changed.
You must apply the changes in order for them to take effect.

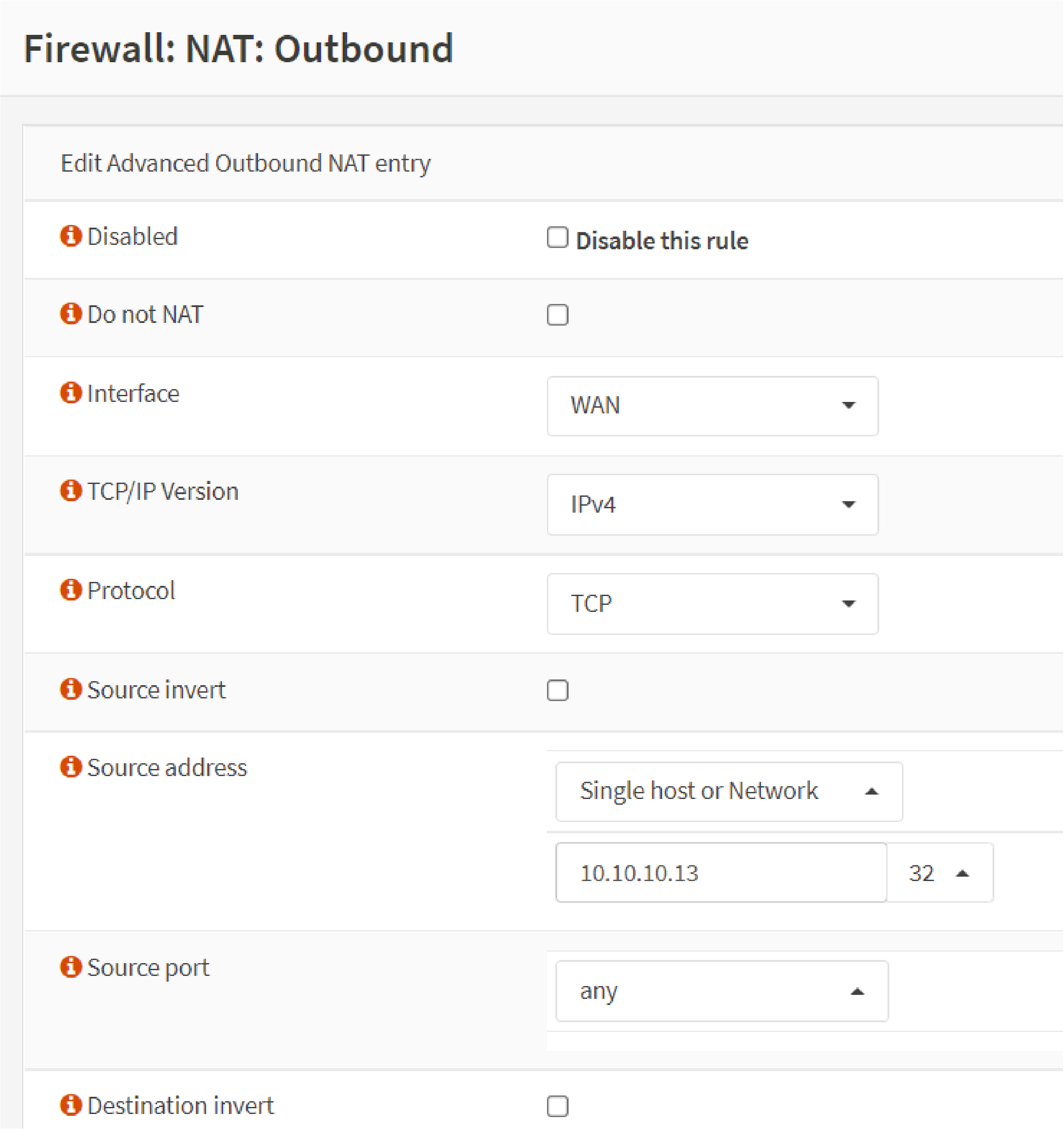
Mode

○ 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)

Figure 34. *Setting Outbound NAT mode in OPNsense*

14. Click **+** icon to add a manual Outbound NAT rule.
15. Set Interface to `WAN`.
16. Set TCP/IP Version to `IPv4`.
17. Set Protocol `TCP`.
18. Set Source add to `Single Host` or `Network`
19. Enter the WebServer1 IP address such as **10.10.10.13/32**.

20. Set Source Port to **any**.



Firewall: NAT: Outbound

Edit Advanced Outbound NAT entry

Disabled	□ **Disable this rule**
Do not NAT	□
Interface	WAN
TCP/IP Version	IPv4
Protocol	TCP
Source invert	□
Source address	Single host or Network 10.10.10.13 / 32
Source port	any
Destination invert	□

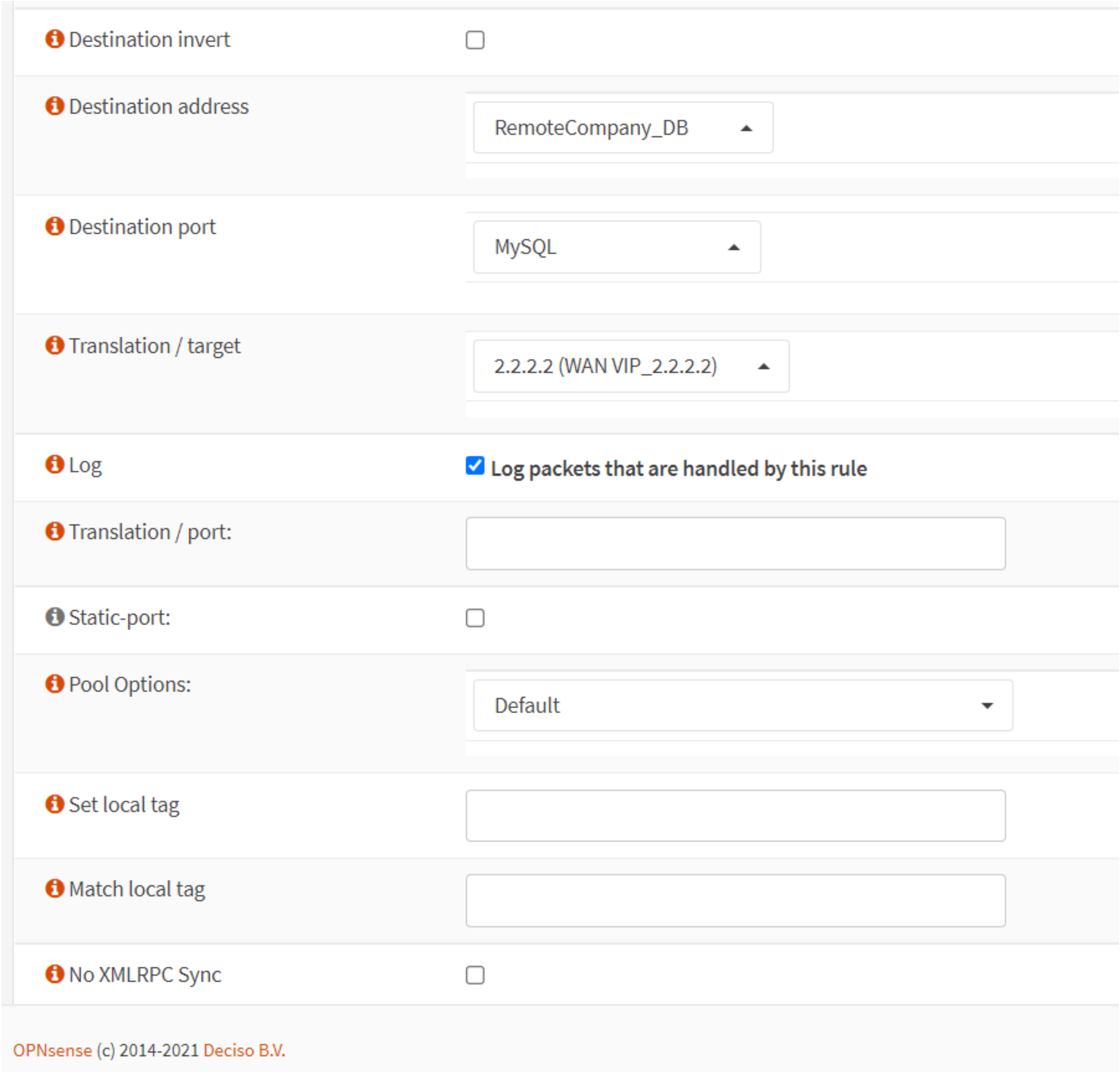
Figure 35. *Defining Outbound NAT rule in OPNsense -1*

21. Select Destination Address as `RemoteCompany_DB`.

22. Select Destination Port as `MySQL`.

23. Select **`2.2.2.2 (WAN IP_2.2.2.2)`** for Translation / target

24. Enable Logging.



Destination invert	□
Destination address	RemoteCompany_DB ▲
Destination port	MySQL ▲
Translation / target	2.2.2.2 (WAN VIP_2.2.2.2) ▲
Log	☑ **Log packets that are handled by this rule**
Translation / port:	
Static-port:	□
Pool Options:	Default ▼
Set local tag	
Match local tag	
No XMLRPC Sync	□

OPNsense (c) 2014-2021 Deciso B.V.

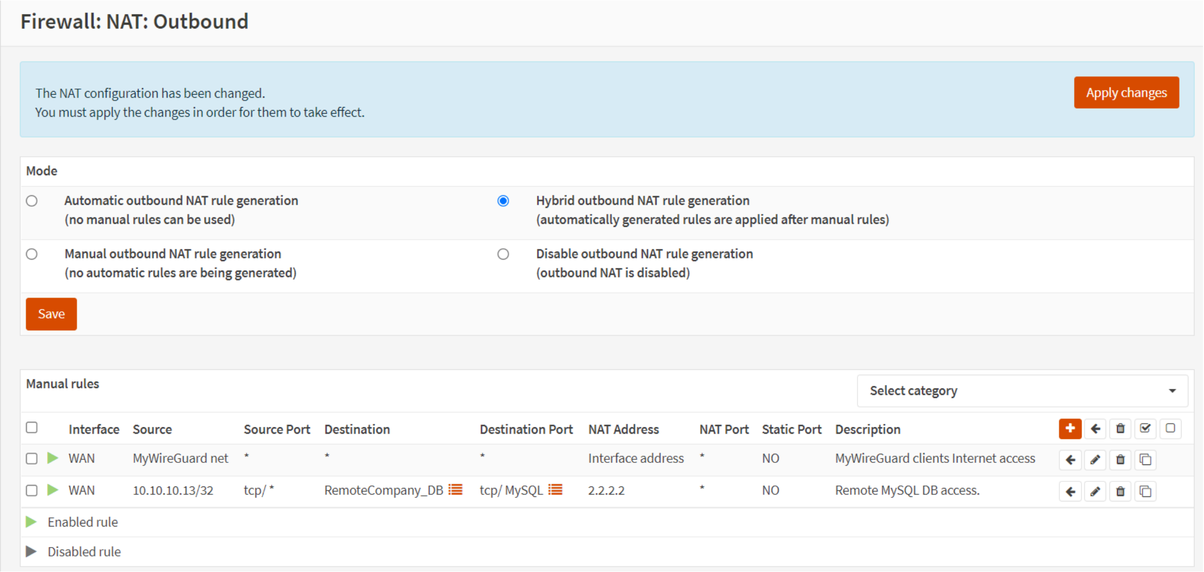
Figure 36. *Defining Outbound NAT rule in OPNsense -2*

25. Enter `Remote MySQL DB access` in Description field.

26. Click **`Save`**

27. Click **`Apply Changes`** to activate the Outbound NAT rule.

Your Outbound NAT rules list should look something like this:



Firewall: NAT: Outbound

The NAT configuration has been changed.
You must apply the changes in order for them to take effect.

Apply changes

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)

Save

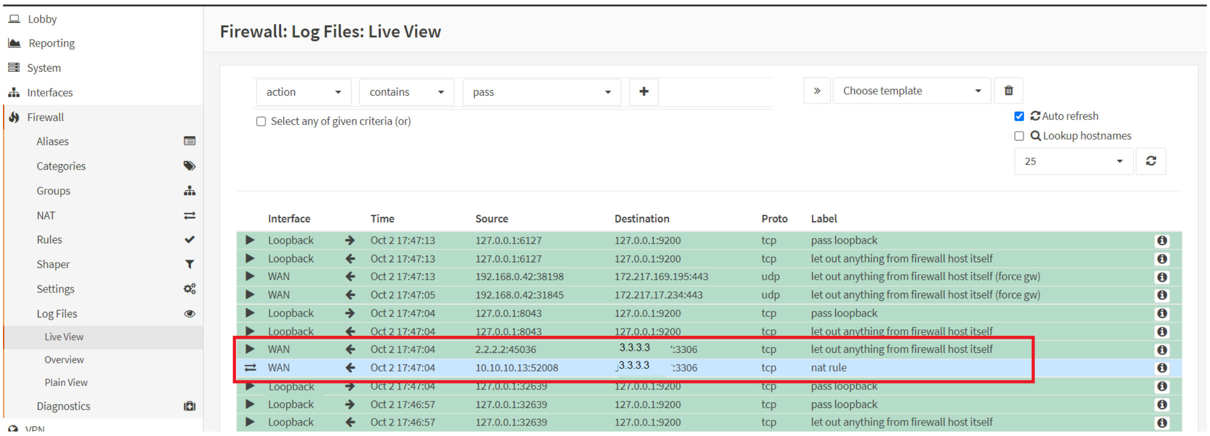
Manual rules | Select category

□		Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description
□	▶	WAN	MyWireGuard net	*	*	*	Interface address	*	NO	MyWireGuard clients Internet access
□	▶	WAN	10.10.10.13/32	tcp/ *	RemoteCompany_DB	tcp/ MySQL	2.2.2.2	*	NO	Remote MySQL DB access.

▶ Enabled rule
▶ Disabled rule

Figure 37. *Manual Outbound NAT rules in OPNsense*

When WebServer1 tries to connect to a remote database server, you should see that it connects the DB using `2.2.2.2` IP address in your firewall logs. To view the firewall logs navigate to `Firewall` -> `Log Files` -> `Live View`. Your logs look like this.



Firewall: Log Files: Live View

action | contains | pass | Choose template

□ Select any of given criteria (or)

☑ Auto refresh
□ Lookup hostnames
25

	Interface		Time	Source	Destination	Proto	Label
▶	Loopback	→	Oct 2 17:47:13	127.0.0.1:6127	127.0.0.1:9200	tcp	pass loopback
▶	Loopback	←	Oct 2 17:47:13	127.0.0.1:6127	127.0.0.1:9200	tcp	let out anything from firewall host itself
▶	WAN	←	Oct 2 17:47:13	192.168.0.42:38198	172.217.169.195:443	udp	let out anything from firewall host itself (force gw)
▶	WAN	←	Oct 2 17:47:05	192.168.0.42:31845	172.217.17.234:443	udp	let out anything from firewall host itself (force gw)
▶	Loopback	→	Oct 2 17:47:04	127.0.0.1:8043	127.0.0.1:9200	tcp	pass loopback
▶	Loopback	←	Oct 2 17:47:04	127.0.0.1:8043	127.0.0.1:9200	tcp	let out anything from firewall host itself
▶	WAN	←	Oct 2 17:47:04	2.2.2.2:45036	3.3.3.3 :3306	tcp	let out anything from firewall host itself
⇄	WAN	←	Oct 2 17:47:04	10.10.10.13:52008	3.3.3.3 :3306	tcp	nat rule
▶	Loopback	→	Oct 2 17:47:04	127.0.0.1:32639	127.0.0.1:9200	tcp	pass loopback
▶	Loopback	→	Oct 2 17:46:57	127.0.0.1:32639	127.0.0.1:9200	tcp	pass loopback
▶	Loopback	←	Oct 2 17:46:57	127.0.0.1:32639	127.0.0.1:9200	tcp	let out anything from firewall host itself

Figure 38. *Firewall Live Log View in OPNsense*

How to Configure OPNsense Firewall Rules

OPNsense is a FreeBSD-based firewall and routing platform that is open source, easy to use, and easy to build. It is becoming more widespread especially among the home networks and small businesses. Because it is secure, reliable, simple to use, and managed with an intuitive web user interface and one of the best open source firewalls..

In this article, we will cover the basics of packet filtering configuration of OPNsense firewall shortly and explain how packet filtering firewall rules are configured with simple examples for new OPNsense firewall users.

💡 **BEST PRACTICE**

In addition the its effective L4 packet filtering and routing features, OPNsense also provides next-generation firewall capabilities such as web control and application control. This is provided by an external tool called Zenarmor.

Zenarmor NGFW Plug-in for OPNsense is one of the most popular OPNsense plug-ins and allows you to easily upgrade your firewall to a Next Generation Firewall in seconds. NG Firewalls empower you to combat modern-day cyber attacks that are becoming more sophisticated every day.

Some of the capabilities are layer-7 application/user aware blocking, granular filtering policies, commercial-grade web filtering utilizing cloud-delivered AI-based Threat Intelligence, parental controls, and the industry's best network analytics and reporting.

Zenarmor Free Edition is available at no cost for all OPNsense users.

How does OPNsense Firewall Work?

Basic terms of the OPNsense firewall and how OPNsense firewall works are described below briefly.

Rules

OPNsense includes a stateful packet filter that can be used to deny or allow network packets from and/or to specific networks, as well as influence how a packet is forwarded.

OPNsense firewall rules are the policies that apply to your network, organized by an interface.

Some components and basics of a firewall rule are explained below.

Actions

Rules can be assigned to one of three types of actions:

- **Pass**: Allow traffic
- **Block**: Deny traffic without informing the client that it has been dropped (which is usually recommended for untrusted networks)
- **Reject**: Deny traffic and notify the client. (Only TCP and UDP support rejecting packets, which results in an RST in the case of TCP and an ICMP UNREACHABLE in the case of UDP.)

📣 **INFO**

When access is denied on internal networks, it may be more practical to use reject so that the client does not have to wait for a time-out.

If a packet is received from untrusted networks, it is not recommended to communicate back if traffic is not permitted.

Allow All Rule

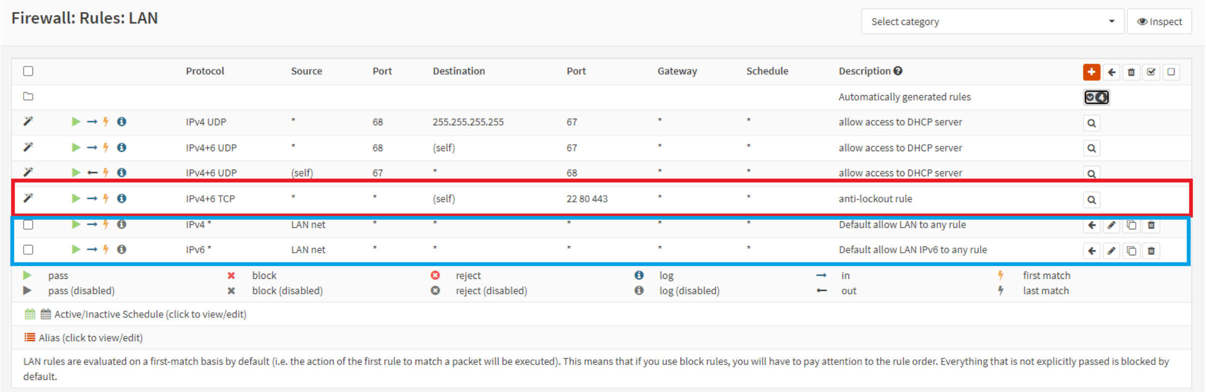
After installing the OPNsense firewall and configuring its LAN/WAN interfaces, it automatically creates a web administration anti-lockout rule and a `allow all` rule for IPv4 and IPv6. These rules prevent you from locking yourself out of OPNsense web UI and provide LAN with unrestricted Internet access. When a device is plugged directly into the router (or a switch connected to the router), and it will access the internet or the network behind the OPNsense.

If the `allow all` rule is deleted or disabled, all traffic to the Internet and other local networks behind the firewall will be blocked, except for access to the OPNsense web administration interface.

Although the anti-lockout rule is a practical solution, since generally there would not be any threat from the internal home network, it is not advisable for organization networks. Because the anti-lockout rule allows any device to access the management interfaces of the OPNsense firewall such as SSH console and Web GUI. This rule brings huge IT security gaps and may cause critical data leakage in a company network. Therefore it should be disabled and another `allow` rule should be defined for firewall management. In the next section, we will create a rule to allow firewall administrators to access their firewalls as an example.

To see the default rules on OPNsense Firewall Web UI,

1. Navigate to the **`Firewall` -> Rules -> LAN**.
2. Click drop-down menu icon on the `Automatically generated rules` line at the top of the rule list.



Firewall: Rules: LAN

Select category | Inspect

		Protocol	Source	Port	Destination	Port	Gateway	Schedule	Description
□									Automatically generated rules
	▶ → ⚡ ℹ	IPv4 UDP	*	68	255.255.255.255	67	*	*	allow access to DHCP server
	▶ → ⚡ ℹ	IPv4+6 UDP	*	68	(self)	67	*	*	allow access to DHCP server
	▶ ← ⚡ ℹ	IPv4+6 UDP	(self)	67	*	68	*	*	allow access to DHCP server
	▶ → ⚡ ℹ	IPv4+6 TCP	*	*	(self)	22 80 443	*	*	anti-lockout rule
□	▶ → ⚡ ℹ	IPv4 *	LAN net	*	*	*	*	*	Default allow LAN to any rule
□	▶ → ⚡ ℹ	IPv6 *	LAN net	*	*	*	*	*	Default allow LAN IPv6 to any rule

▶ pass ▶ pass (disabled) ✖ block ✖ block (disabled) ⊗ reject ⊗ reject (disabled) ℹ log ℹ log (disabled) → in ← out ⚡ first match ⚡ last match

Active/Inactive Schedule (click to view/edit)

Alias (click to view/edit)

LAN rules are evaluated on a first-match basis by default (i.e. the action of the first rule to match a packet will be executed). This means that if you use block rules, you will have to pay attention to the rule order. Everything that is not explicitly passed is blocked by default.

Figure 1. *Default Anti-lockout and **`allow LAN to any`** rules on OPNsense firewall*

How Does OPNsense Process the Rules?

Firewall rules are evaluated in order, beginning with the Floating rules section, then all rules belonging to interface groups, and finally all interface rules.

Internal (automatic) rules are usually the first to be registered.

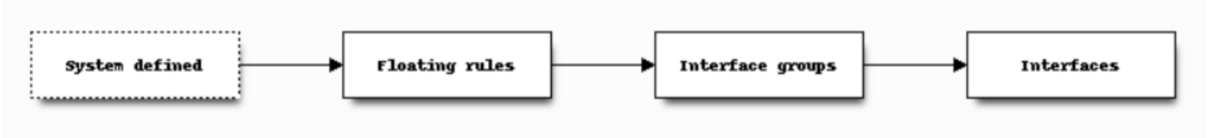


Figure 2. *OPNsense firewall rule process order*

Rules can be set to `quick` or not, with `quick` being the default setting. When the rule is set to `quick`, it is handled on a "first match" basis, which means that the first rule that matches the packet takes precedence over rules that follow in sequence.

When the quick isn't set, the last match wins. This is useful for rules that define expected behavior. For example, the default `deny` rule of the OPNsense makes use of this property (if no rule applies, drop traffic).

Because firewall rules are processed from top to bottom of the rule list, the order of the rules in the list is important. No subsequent rules are processed when the network packet matches any rule, whether it is a `allow` or `block` or `reject` rule. The first match wins, and all subsequent rules are ignored.

When defining the firewall rules, it's a good idea to put the most specific rules at the top of the list and the most general rules at the bottom. For example, all devices in a LAN are generally allowed surfing on the Internet and the first rule may allow LAN devices access to HTTP(s) service port on the Internet.

The more specific network traffic is allowed or denied first, while network traffic that does not match any of the specific rules is handled by the latest rule. The latest rule may be either `deny all` or `allow all` rule which may block or allow all other unspecified network traffic.

Direction

Traffic can be matched in either the in[coming] or out[going] direction; OPNsense default is to filter in the in[coming] direction. In that case, you would configure the policy on the interface from which the traffic originates.

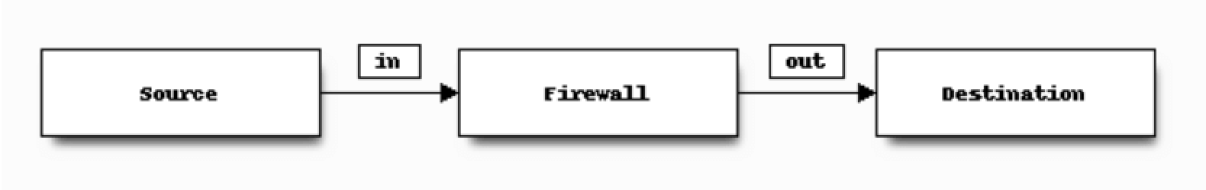


Figure 3. *OPNsense firewall rule direction*

For instance, if you want to allow HTTPS traffic from any host on the internet, you would typically configure a policy on the WAN interface that allows port 443 to the host in question.

Settings

Descriptive settings aid in the identification of rules while having no effect on traffic flow. Using descriptive names makes it easier to identify traffic in the live log view.

Settings	**Description**
Category	The category this rule belongs to can be used as a filter in the overview
Description	Descriptive text

The following are the most commonly used `Basic` settings:

Settings	**Description**
Action	The action to perform, allow, block, or reject.
Disabled	Disabling a rule without removing it can be useful for testing and making it easier to enable less frequently used policies.
Interface	This rule applies to the interface[s]. This field can be easily copied between interfaces and changed to the new target interface.
TCP/IP Version	This rule is applicable to IPv4, IPv6, or both.
Protocol	TCP and UDP are the most commonly used protocols.

Source	Source network or address. When combining IPv4 and IPv6 in a single rule, you can use aliases that contain both address families as the source network or address.
Source / Invert	Invert source selection (for example, not 172.16.0.0/24)
Destination	Destination network or address. Similar to the source you can use aliases here as well.
Destination / Invert	When the filter should be inverted, you can mark this checkbox.
Destination port range	You can select a TCP and/or UDP service by name (HTTP, HTTPS) or number (range). You can also use aliases here to simplify management.
Log	When this rule applies, make a log entry. You can use **`Firewall`** **>** **`Log Files`** **>** **`Live View`** to monitor if your rule applies.

Aliases

Aliases are especially helpful for condensing firewall rules and minimizing changes.

Aliases are the named lists of hosts, networks, or ports. By selecting the alias name multiple networks, hosts or ports can be used as a single entity in the firewall configuration.

On OPNsense firewall, there are predefined aliases such as **`SSH`**, **`HTTP`**, **`HTTPS`**, **`LAN net`**, **`LAN interface`**, etc.

Using predefined aliases is not only practical, but they also aid in the comprehension of firewall rules. The benefits of aliases on the OPNsense firewall are as follows:

- Rules that are easier to read, understand, and maintain can be written.
- Because a single alias contains multiple items, the overall number of rules you need to write is reduced. An effective aliases definition aids in the consolidation of multiple rules into a single rule.
- The fewer firewall rules, the higher firewall performance.

In summary, the use of aliases is critical for reducing complexity and the number of rules that must be created.

To add, modify or remove an alias on the OPNsense firewall, navigate to the **`Firewall -> Aliases`** on web GUI.

You don't need to go to the **`Aliases`** pages to view the alias content in a rule. When viewing a firewall rule for an interface, hovering the mouse over the alias will display a tooltip. The contents of the alias, as well as the description, will be displayed in the tooltip.

Alias Types

The following alias types are available in OPNsense:

Type	Description
Hosts	Single hosts by IP or Fully Qualified Domain Name or host exclusions (starts with "!" sign)
Networks	Entire network p.e. 192.168.1.1/24 or network exclusion eg !192.168.1.0/24
Ports	Port numbers or a port range like 20:30
MAC addresses	MAC address or partial mac addresses like f4:90:ea
URL (IPs)	A table of IP addresses that are fetched once
URL Tables (IPs)	A table of IP addresses that are fetched at regular intervals.
GeoIP	Select countries or whole regions
Network group	Combine different network type aliases into one
External (advanced)	Externally managed alias, this only handles the placeholder. Content is set from another source (plugin, API call, etc)

Hosts Hosts can be specified as a single IP address, a range (separated by a minus sign, for example, 10.0.0.1-10.0.0.10), or a fully qualified domain name. Hosts type aliases can be used for host exclusion. To exclude hosts from Network Group Aliases, you can define a host alias that begins with "!" sign (eg !172.16.0.1).|

In a host alias, you can enter multiple values of any combination of IP addresses, hostnames, and FQDNs separated by commas, such as:

`youtube.com`, **`172.168.1.1`**, **`192.168.10.1`**, **`web_server`**.

Valid host alias examples are listed below:

- IPv4 address: 172.16.1.10 or !172.16.1.10 (IPv6 addresses are allowed too)
- IP address range: 172.16.1.10-172.16.1.15
- Local hostname (no domain name): dbserver or !dbserver
- Fully qualified domain name (FQDN): youtube.com or !youtube.com

Networks

Classless Inter-Domain Routing is used to specify network aliases (CIDR).

A /32 specifies a single IPv4 host, a /128 specifies a single IPv6 host, a /24 specifies 255.255.255.0, and a /64 specifies a standard IPv6 network.

Exclusion hosts or networks can be included in network type aliases. Exclusion addresses begin with a "!" sign (for example,!172.16.0.0/24) and are used to exclude hosts or networks from current Alias or Network Group Alias.

Aside from the CIDR notation, a wildcard mask could be used to match host or network ranges.

> 💡 **TIP**
>
> To match all routers ending at .1 in the 172.16.X.1 networks, use a wildcard definition like 172.16.0.1/0.0.255.0

Ports

Ports can be specified as a single number or as a range of numbers separated by a colon (`:`).

For example, to add a range of 20 to 25, enter 20:25 in the Port(s) section.

You may enter a number between 0 and 65,535.

You can enter multiple ports as well as port ranges, such as:

21, 8000:8080

MAC addresses

MAC addresses or partial mac addresses can be specified as MAC addresses aliases. For example, to match all addresses from Deciso, you can define an alias for `F4:90:EA`.

URL tables

URL tables can be used to retrieve an IP address list from a remote server. There are several free IP lists available, the most notable of which are Spamhaus' "Don't Route Or Peer" lists.

GeoIP

With GeoIP alias, you can block or allow one or more countries or entire continents. Toggle the all checkbox to select all countries within the specified region.

To use GeoIP, you should configure a source in the **`Firewall Aliases -> GeoIP`** settings tab the most commonly used source is `MaxMind`. To obtain the GeoIP address ranges required to fully configure the GeoIP alias, you must sign up for MaxMind's GeoIP service.

Network Group

Network Group alias combines multiple network type aliases into one. It accepts additional host type aliases (networks, hosts, etc.). Although nesting is possible with other alias types, this type only displays valid aliases to simplify administration. A Networks type alias can do the same thing but using a different presentation. The main advantage of using a `Network Group` alias is that it prevents you from grouping incompatible aliases together.

External

The contents of external alias types are not managed by OPNsense standard alias service. They are very useful to push new entries from external programs. Specific lockout features or external tools feeding access control to your firewall are examples.

In Firewall Diagnostics pfTables, you can always inspect the current contents of the external alias and immediately add or remove entries.

> 💡 **TIP**
>
> Because OPNsense will not touch external alias types, you can use pfctl directly in scripts to manage their contents. (For example, pfctl -t MyAlias -T add 10.0.0.3 will add 10.0.0.3 to MyAlias.)

Nesting Aliases

Aliases can be nestled inside aliases for all alias types. If you want to group several aliases together, this may be useful.

For example, if you have aliases for "webserver" and "emailserver," you could create a third alias called "dmzservers" that includes both "webserver" and "emailserver". This allows you to use the "webserver" and "emailserver" aliases in their own specific firewall rules while also having broader firewall rules that apply to both servers.

How to Configure Firewall Rules in OPNsense

In this section, we will go over the fundamentals of OPNsense firewall configuration and walk you through the process of configuring a firewall rule step by step. To configure your OPNsense firewall, you may perform the following task.

- Define an alias
- Create a firewall rule
- Select a firewall rule
- Move a firewall rule
- Delete a firewall rule
- Enable/Disable a firewall rule
- Edit a firewall rule
- Clone a firewall rule
- Enable/Disable logging for a firewall rule

1. The Use of Aliases in pf Firewall Rules

Aliases can be used in firewall rules to make it easier to manage large lists. For example, we may require a list of remote IP addresses that should have access to specific services; if anything changes, we simply update the list.

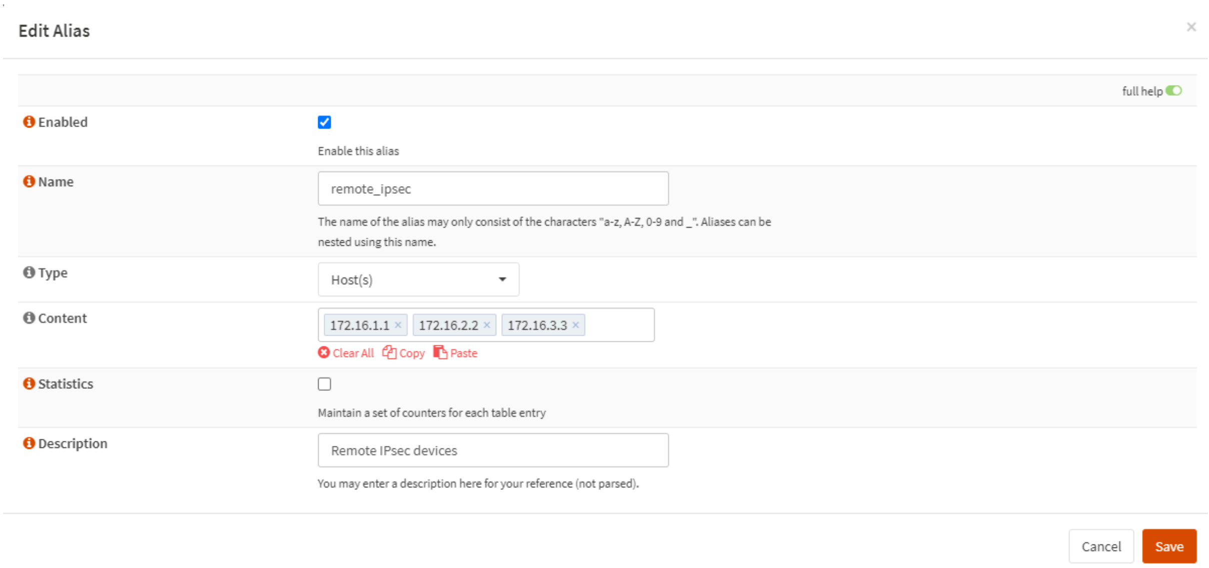
> 📣 **INFO**
>
> The list icon identifies a rule with an alias on OPNsense Web UI.

Let's make a simple alias that will allow three remote IP addresses to connect to an IPSec server for a site-to-site VPN tunnel connection. Alias name will be remote_ipsec. To define and update the related firewall rule this alias will be used.

- 172.16.1.1
- 172.16.2.2
- 172.16.3.3

To create an alias on OPNsense firewall Web GUI, follow the next steps given below:

1. Navigate to the **`Firewall`** **->** **`Aliases`** page. You will notice there are 4 pre-defined aliases in the list by default.
2. Click on the "**+**" button at the right bottom of the pane
3. Enter the `Name` of the alias.
4. Select `Host(s)` in the Type dropdown menu.
5. Enter the IP addresses separated by comma `,` in the `Content` field.
6. Type a `Description` that will assist you in understanding the purpose or details of the alias.

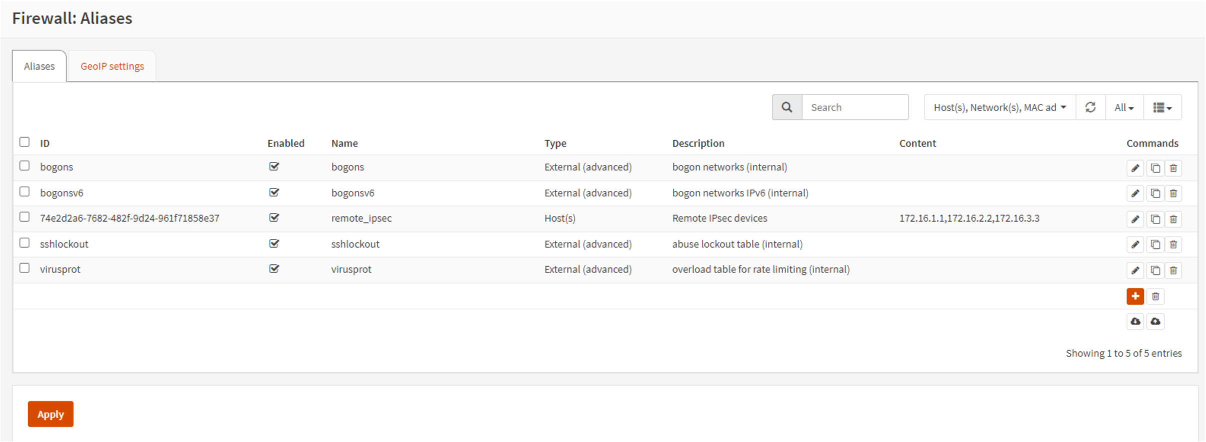


Edit Alias

Enabled	☑ Enable this alias
Name	remote_ipsec The name of the alias may only consist of the characters "a-z, A-Z, 0-9 and _". Aliases can be nested using this name.
Type	Host(s)
Content	172.16.1.1 × 172.16.2.2 × 172.16.3.3 × Clear All Copy Paste
Statistics	☐ Maintain a set of counters for each table entry
Description	Remote IPsec devices You may enter a description here for your reference (not parsed).

Figure 4. *Defining an alias on OPNsense firewall*

7. Click **`Save`**. The new alias is on the list now.
8. Click the **`Apply`** button to apply the changes in order to use the alias in the firewall rules.



Firewall: Aliases

☐ ID	Enabled	Name	Type	Description	Content	Commands
☐ bogons	☑	bogons	External (advanced)	bogon networks (internal)		
☐ bogonsv6	☑	bogonsv6	External (advanced)	bogon networks IPv6 (internal)		
☐ 74e2d2a6-7682-482f-9d24-961f71858e37	☑	remote_ipsec	Host(s)	Remote IPsec devices	172.16.1.1,172.16.2.2,172.16.3.3	
☐ sshlockout	☑	sshlockout	External (advanced)	abuse lockout table (internal)		
☐ virusprot	☑	virusprot	External (advanced)	overload table for rate limiting (internal)		

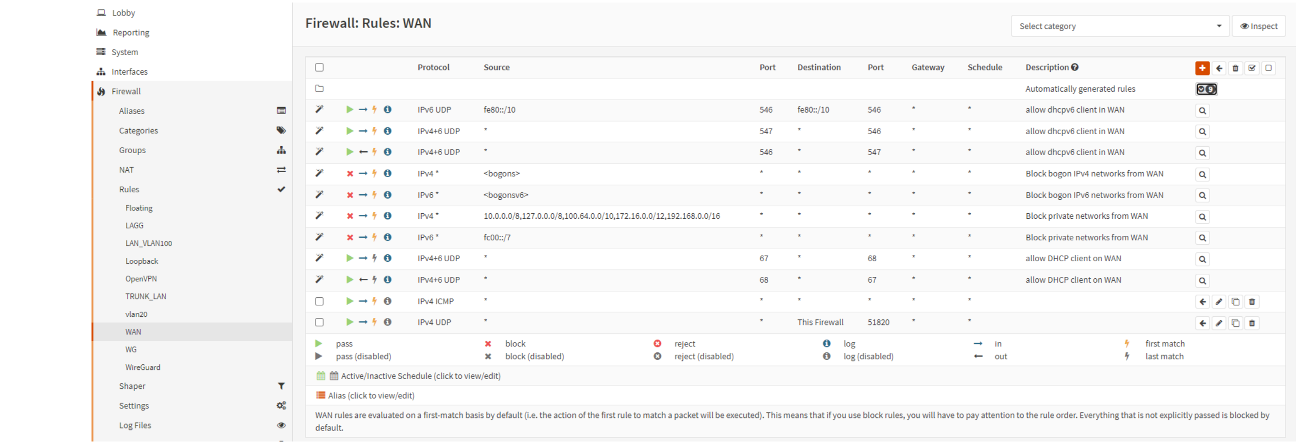
Showing 1 to 5 of 5 entries

Figure 5. *Aliases list on OPNsense firewall*

2. Creating a Firewall Rule

You can easily create a packet filtering firewall rule on OPNsense by following the steps given below.

1. Navigate to the **`Firewall->Rules`** on OPNsense web GUI.
2. Select the interface that you want to define a rule, such as WAN, LAN, VLAN10 or WireGuard, etc. This will list the existing firewall rules on the selected interface.



Firewall: Rules: WAN

		Protocol	Source	Port	Destination	Port	Gateway	Schedule	Description
□									
									Automatically generated rules
	▶ →	IPv6 UDP	fe80::/10	546	fe80::/10	546	*	*	allow dhcpv6 client in WAN
	▶ →	IPv4+6 UDP	*	547	*	546	*	*	allow dhcpv6 client in WAN
	▶ ←	IPv4+6 UDP	*	546	*	547	*	*	allow dhcpv6 client in WAN
	✖ →	IPv4 *	<bogons>	*	*	*	*	*	Block bogon IPv4 networks from WAN
	✖ →	IPv6 *	<bogonsv6>	*	*	*	*	*	Block bogon IPv6 networks from WAN
	✖ →	IPv4 *	10.0.0.0/8,127.0.0.0/8,100.64.0.0/10,172.16.0.0/12,192.168.0.0/16	*	*	*	*	*	Block private networks from WAN
	✖ →	IPv6 *	fc00::/7	*	*	*	*	*	Block private networks from WAN
	▶ →	IPv4+6 UDP	*	67	*	68	*	*	allow DHCP client on WAN
	▶ ←	IPv4+6 UDP	*	68	*	67	*	*	allow DHCP client on WAN
□	▶ →	IPv4 ICMP	*	*	*	*	*	*	
□	▶ →	IPv4 UDP	*	*	This Firewall	51820	*	*	

▶ pass ✖ block ⊗ reject ℹ log → in ϟ first match
▶ pass (disabled) ✖ block (disabled) ⊗ reject (disabled) ℹ log (disabled) ← out ϟ last match

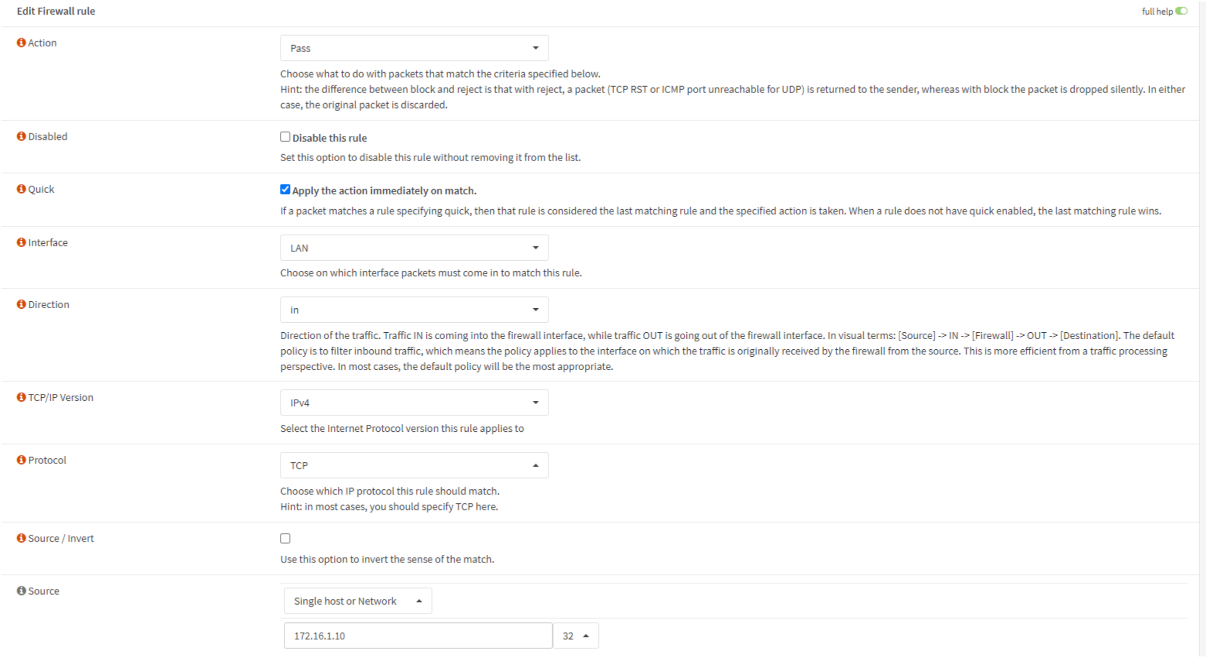
Active/Inactive Schedule (click to view/edit)

Alias (click to view/edit)

WAN rules are evaluated on a first-match basis by default (i.e. the action of the first rule to match a packet will be executed). This means that if you use block rules, you will have to pay attention to the rule order. Everything that is not explicitly passed is blocked by default.

Figure 6. *WAN interface firewall rules on OPNsense*

3. Click the orange square with **+** icon at the top right corner of the rule list. This will redirect you to the rule configuration page.
4. Select `Pass` to allow a connection or select `Block` or `Reject` to deny a connection for the `Action` option.
5. Set the `Source` either by entering a single host/network or selecting one of the existing aliases.
6. Specify the source port or port range. Usually, it is left as **any** by default.



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.

Quick: ☑ Apply the action immediately on match.

If a packet matches a rule specifying quick, then that rule is considered the last matching rule and the specified action is taken. When a rule does not have quick enabled, the last matching rule wins.

Interface: LAN

Choose on which interface packets must come in to match this rule.

Direction: in

Direction of the traffic. Traffic IN is coming into the firewall interface, while traffic OUT is going out of the firewall interface. In visual terms: [Source] -> IN -> [Firewall] -> OUT -> [Destination]. The default policy is to filter inbound traffic, which means the policy applies to the interface on which the traffic is originally received by the firewall from the source. This is more efficient from a traffic processing perspective. In most cases, the default policy will be the most appropriate.

TCP/IP Version: IPv4

Select the Internet Protocol version this rule applies to

Protocol: TCP

Choose which IP protocol this rule should match.
Hint: in most cases, you should specify TCP here.

Source / Invert: □

Use this option to invert the sense of the match.

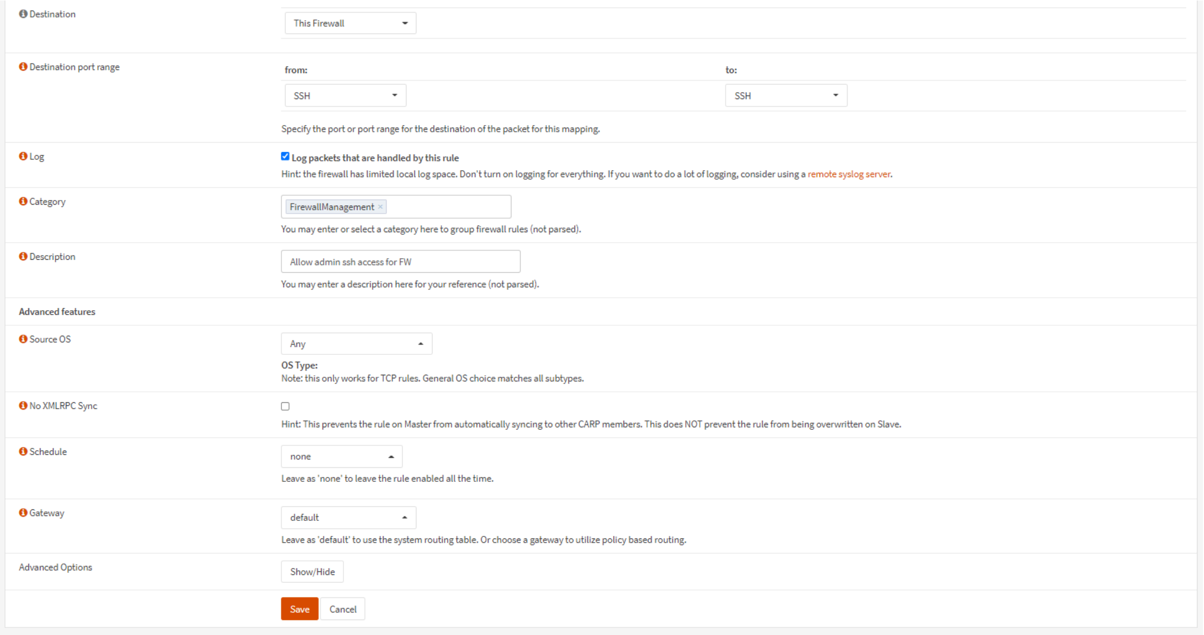
Source: Single host or Network

172.16.1.10 / 32

Figure 7. *Creating a firewall rule on OPNsense-1*

7. Set the `Destination` either by entering a single host/network or selecting one of the existing aliases.
8. Specify the destination port or port range.
9. You may enable logging.
10. You may enter or select a category to group firewall rules.

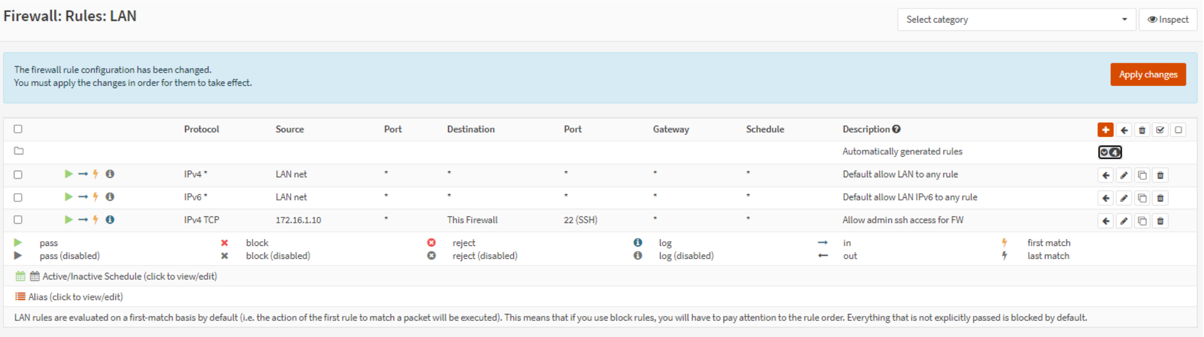
11. You should also to enter a description for the rule which may be useful for rule maintenance.
12. You may leave other fields as default or set them properly as you wish.
13. Click the **Save** button to save the rule. This will take you to the interface rule list.



Destination	This Firewall
Destination port range	from: SSH to: SSH Specify the port or port range for the destination of the packet for this mapping.
Log	☑ **Log packets that are handled by this rule** Hint: the firewall has limited local log space. Don't turn on logging for everything. If you want to do a lot of logging, consider using a remote syslog server.
Category	FirewallManagement × You may enter or select a category here to group firewall rules (not parsed).
Description	Allow admin ssh access for FW You may enter a description here for your reference (not parsed).
Advanced features	
Source OS	Any **OS Type:** Note: this only works for TCP rules. General OS choice matches all subtypes.
No XMLRPC Sync	☐ Hint: This prevents the rule on Master from automatically syncing to other CARP members. This does NOT prevent the rule from being overwritten on Slave.
Schedule	none Leave as 'none' to leave the rule enabled all the time.
Gateway	default Leave as 'default' to use the system routing table. Or choose a gateway to utilize policy based routing.
Advanced Options	Show/Hide
	Save Cancel

Figure 8. *Creating firewall rule on OPNsense-2 (Allows admin IP establish an SSH connection to the firewall)*

14. Click **`Apply`** button to apply the changes and activate the newly created rule.



Firewall: Rules: LAN

The firewall rule configuration has been changed.
You must apply the changes in order for them to take effect.

☐		Protocol	Source	Port	Destination	Port	Gateway	Schedule	Description
									Automatically generated rules
☐	▶ → ϟ ℹ	IPv4 *	LAN net	*	*	*	*	*	Default allow LAN to any rule
☐	▶ → ϟ ℹ	IPv6 *	LAN net	*	*	*	*	*	Default allow LAN IPv6 to any rule
☐	▶ → ϟ ℹ	IPv4 TCP	172.16.1.10	*	This Firewall	22 (SSH)	*	*	Allow admin ssh access for FW

▶ pass ✖ block ⊗ reject ℹ log → in ϟ first match
▶ pass (disabled) ✖ block (disabled) ⊗ reject (disabled) ℹ log (disabled) ← out ϟ last match

Active/Inactive Schedule (click to view/edit)

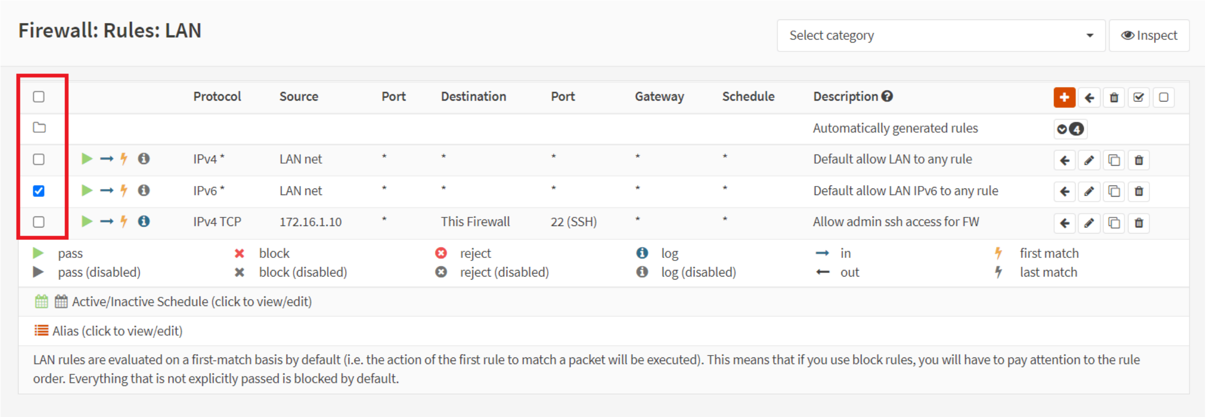
Alias (click to view/edit)

LAN rules are evaluated on a first-match basis by default (i.e. the action of the first rule to match a packet will be executed). This means that if you use block rules, you will have to pay attention to the rule order. Everything that is not explicitly passed is blocked by default.

Figure 9. *Applying the changes and activate the newly created rule*

3. Selecting Firewall Rules

To perform a task, such as enabling, disabling, deleting, or moving, etc, on some of the firewall rules on an interface, you may select them by clicking on the checkbox icon at the first column of the rule list. You can also select all rules by clicking on the checkbox icon header bar of the list.



Firewall: Rules: LAN

Select category | Inspect

□		Protocol	Source	Port	Destination	Port	Gateway	Schedule	Description
									Automatically generated rules
□	▶ → ϟ ℹ	IPv4 *	LAN net	*	*	*	*	*	Default allow LAN to any rule
☑	▶ → ϟ ℹ	IPv6 *	LAN net	*	*	*	*	*	Default allow LAN IPv6 to any rule
□	▶ → ϟ ℹ	IPv4 TCP	172.16.1.10	*	This Firewall	22 (SSH)	*	*	Allow admin ssh access for FW

▶ pass ▶ pass (disabled) ✖ block ✖ block (disabled) ⊗ reject ⊗ reject (disabled) ℹ log ℹ log (disabled) → in ← out ϟ first match ϟ last match

Active/Inactive Schedule (click to view/edit)

Alias (click to view/edit)

LAN rules are evaluated on a first-match basis by default (i.e. the action of the first rule to match a packet will be executed). This means that if you use block rules, you will have to pay attention to the rule order. Everything that is not explicitly passed is blocked by default.

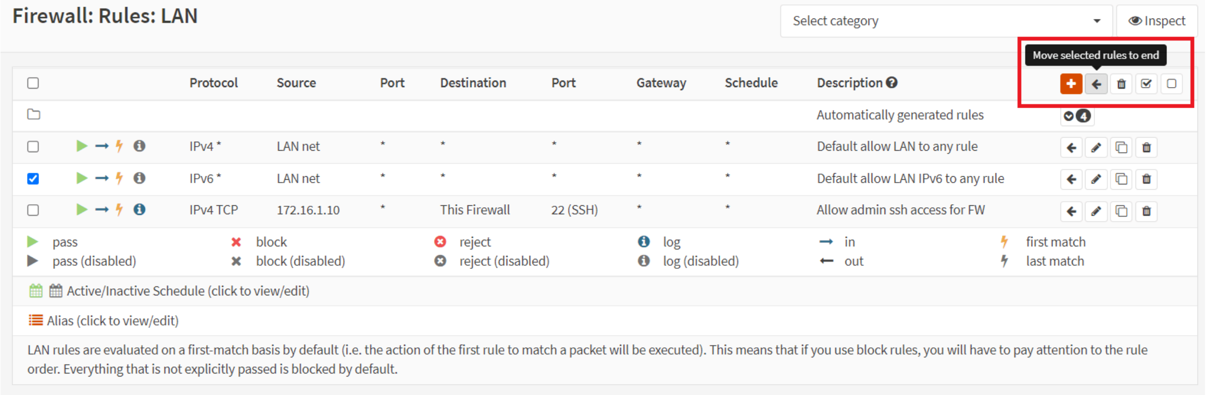
Figure 10. *Selecting firewall rules on OPNsense firewall*

4. Moving a Firewall Rule

To block or allow network traffic, you may need to reorder the firewall rules on the list.

To move some of the rules at the end of the list,

1. Select the rules that you want to move to the bottom of the list.
2. Click on the **`left arrow`** icon on the header bar of the list.
3. Click on the **`Apply Changes`** button to activate the new rule order setting.



Firewall: Rules: LAN

Select category | Inspect

Move selected rules to end

□		Protocol	Source	Port	Destination	Port	Gateway	Schedule	Description
									Automatically generated rules
□	▶ → ϟ ℹ	IPv4 *	LAN net	*	*	*	*	*	Default allow LAN to any rule
☑	▶ → ϟ ℹ	IPv6 *	LAN net	*	*	*	*	*	Default allow LAN IPv6 to any rule
□	▶ → ϟ ℹ	IPv4 TCP	172.16.1.10	*	This Firewall	22 (SSH)	*	*	Allow admin ssh access for FW

▶ pass ▶ pass (disabled) ✖ block ✖ block (disabled) ⊗ reject ⊗ reject (disabled) ℹ log ℹ log (disabled) → in ← out ϟ first match ϟ last match

Active/Inactive Schedule (click to view/edit)

Alias (click to view/edit)

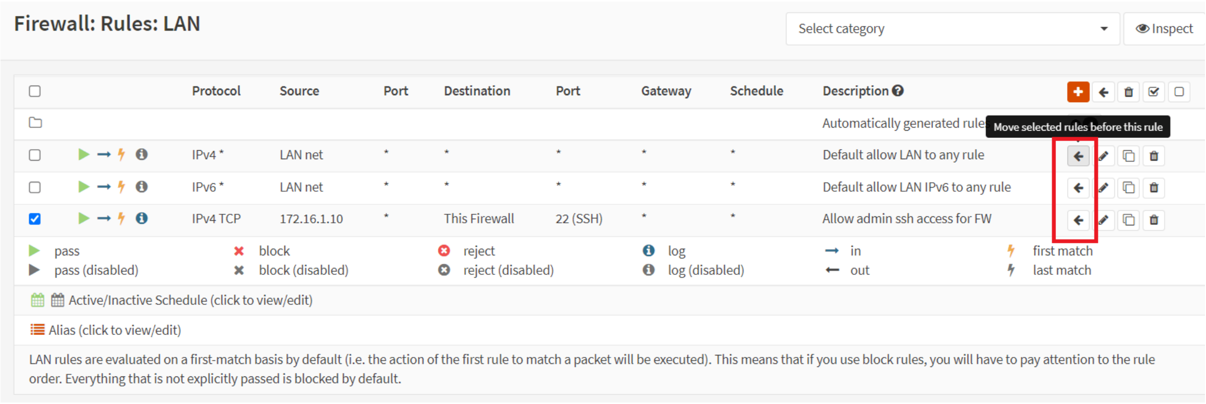
LAN rules are evaluated on a first-match basis by default (i.e. the action of the first rule to match a packet will be executed). This means that if you use block rules, you will have to pay attention to the rule order. Everything that is not explicitly passed is blocked by default.

Figure 11. *Moving selected rule to the bottom of the rule list*

To move some of the rules before a specific rule,

1. Select the rules that you want to move.
2. Click on the **`left arrow`** icon on the rule that you want to move the selected rule before.
3. Click on the **`Apply Changes`** button to activate the new rule order setting.

For example, to move the last rule to the top in the next figure given below, click the **left arrow** icon of the first rule after selecting the last rule.



Firewall: Rules: LAN

Select category ▾ | Inspect

□		Protocol	Source	Port	Destination	Port	Gateway	Schedule	Description
									Automatically generated rules
□	▶ → ⚡ ℹ	IPv4 *	LAN net	*	*	*	*	*	Default allow LAN to any rule
□	▶ → ⚡ ℹ	IPv6 *	LAN net	*	*	*	*	*	Default allow LAN IPv6 to any rule
☑	▶ → ⚡ ℹ	IPv4 TCP	172.16.1.10	*	This Firewall	22 (SSH)	*	*	Allow admin ssh access for FW

▶ pass ✖ block ⊗ reject ℹ log → in ⚡ first match
▶ pass (disabled) ✖ block (disabled) ⊗ reject (disabled) ℹ log (disabled) ← out ⚡ last match

Active/Inactive Schedule (click to view/edit)

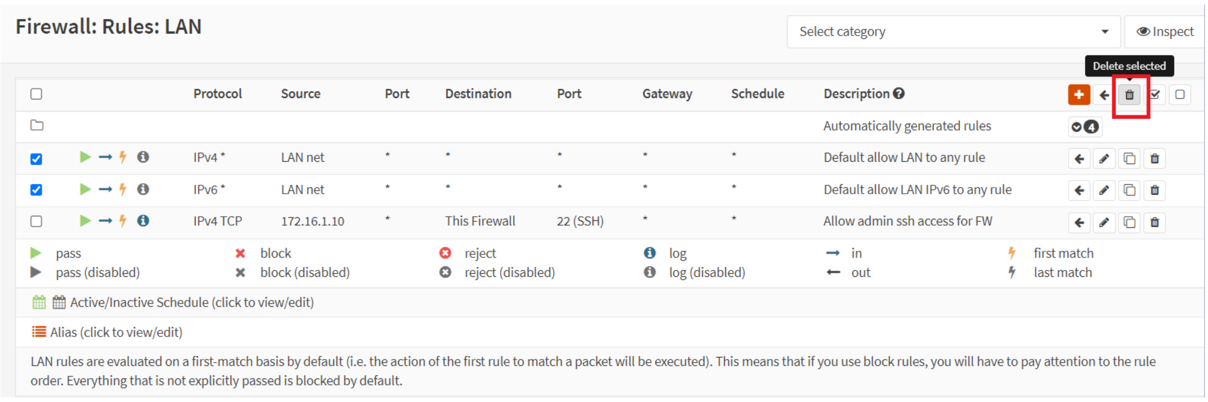
Alias (click to view/edit)

LAN rules are evaluated on a first-match basis by default (i.e. the action of the first rule to match a packet will be executed). This means that if you use block rules, you will have to pay attention to the rule order. Everything that is not explicitly passed is blocked by default.

Figure 12. *Moving selected rule(s) to a specific position in the rule list*

5. Deleting Firewall Rules

You may delete firewall rules either by clicking on the **trash** icon on the header bar of the rule list after selecting the rules that you wish to remove or by clicking on the **trash** icon at the end of the related rule. Lastly, Click on the **Apply Changes** button to activate the new rule settings.



Firewall: Rules: LAN

Select category ▾ | Inspect

□		Protocol	Source	Port	Destination	Port	Gateway	Schedule	Description
									Automatically generated rules
☑	▶ → ⚡ ℹ	IPv4 *	LAN net	*	*	*	*	*	Default allow LAN to any rule
☑	▶ → ⚡ ℹ	IPv6 *	LAN net	*	*	*	*	*	Default allow LAN IPv6 to any rule
□	▶ → ⚡ ℹ	IPv4 TCP	172.16.1.10	*	This Firewall	22 (SSH)	*	*	Allow admin ssh access for FW

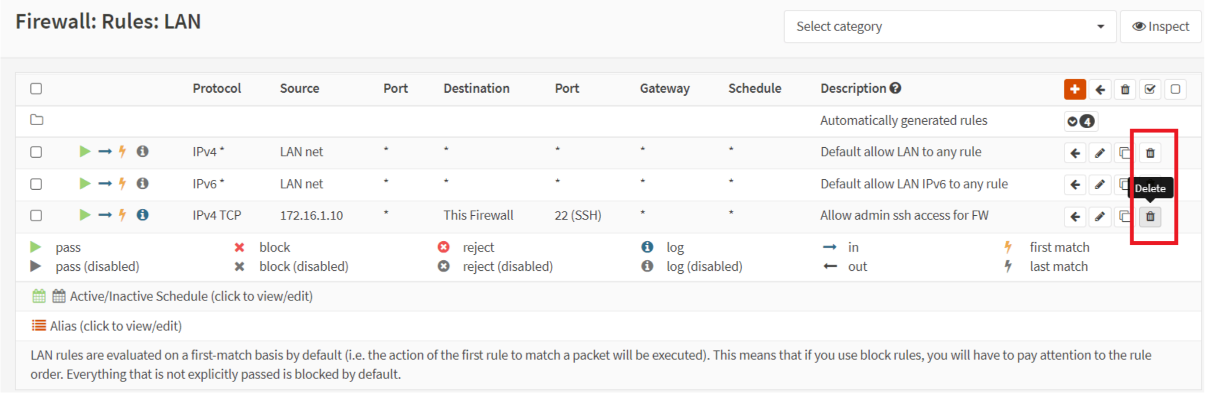
▶ pass ✖ block ⊗ reject ℹ log → in ⚡ first match
▶ pass (disabled) ✖ block (disabled) ⊗ reject (disabled) ℹ log (disabled) ← out ⚡ last match

Active/Inactive Schedule (click to view/edit)

Alias (click to view/edit)

LAN rules are evaluated on a first-match basis by default (i.e. the action of the first rule to match a packet will be executed). This means that if you use block rules, you will have to pay attention to the rule order. Everything that is not explicitly passed is blocked by default.

Figure 13. *Deleting multiple firewall rules*



Firewall: Rules: LAN

Select category ▾ | 👁 Inspect

☐		Protocol	Source	Port	Destination	Port	Gateway	Schedule	Description
🗀									Automatically generated rules
☐	▶ → ϟ ℹ	IPv4 *	LAN net	*	*	*	*	*	Default allow LAN to any rule
☐	▶ → ϟ ℹ	IPv6 *	LAN net	*	*	*	*	*	Default allow LAN IPv6 to any rule
☐	▶ → ϟ ℹ	IPv4 TCP	172.16.1.10	*	This Firewall	22 (SSH)	*	*	Allow admin ssh access for FW

▶ pass ✖ block ✖ reject ℹ log → in ϟ first match
▶ pass (disabled) ✖ block (disabled) ✖ reject (disabled) ℹ log (disabled) ← out ϟ last match

Active/Inactive Schedule (click to view/edit)

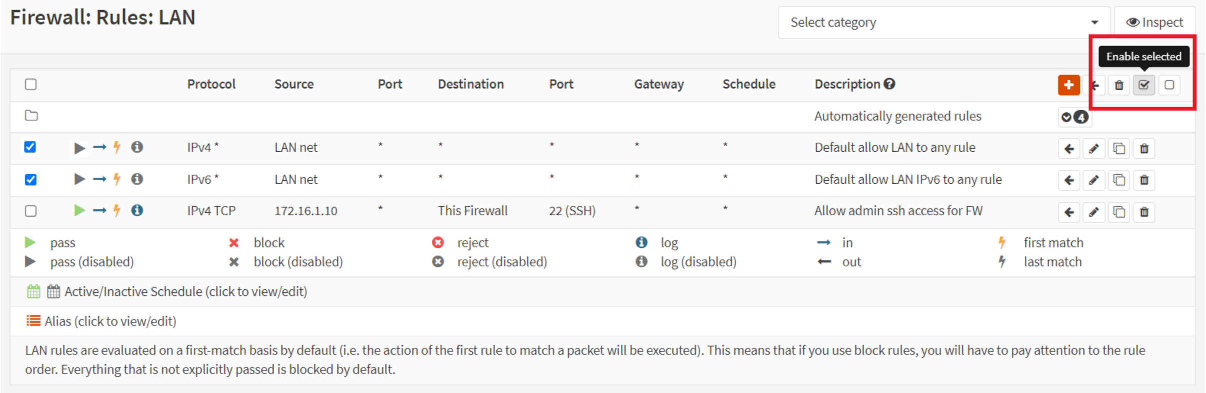
Alias (click to view/edit)

LAN rules are evaluated on a first-match basis by default (i.e. the action of the first rule to match a packet will be executed). This means that if you use block rules, you will have to pay attention to the rule order. Everything that is not explicitly passed is blocked by default.

Figure 14. *Deleting a specific firewall rule*

6. Enabling Firewall Rules

To enable some of the disabled firewall rules, click on the square box with a check icon on the header bar of the rule list after selecting the rules that you wish to enable.



Firewall: Rules: LAN

Select category ▾ | 👁 Inspect

☐		Protocol	Source	Port	Destination	Port	Gateway	Schedule	Description
🗀									Automatically generated rules
☑	▶ → ϟ ℹ	IPv4 *	LAN net	*	*	*	*	*	Default allow LAN to any rule
☑	▶ → ϟ ℹ	IPv6 *	LAN net	*	*	*	*	*	Default allow LAN IPv6 to any rule
☐	▶ → ϟ ℹ	IPv4 TCP	172.16.1.10	*	This Firewall	22 (SSH)	*	*	Allow admin ssh access for FW

▶ pass ✖ block ✖ reject ℹ log → in ϟ first match
▶ pass (disabled) ✖ block (disabled) ✖ reject (disabled) ℹ log (disabled) ← out ϟ last match

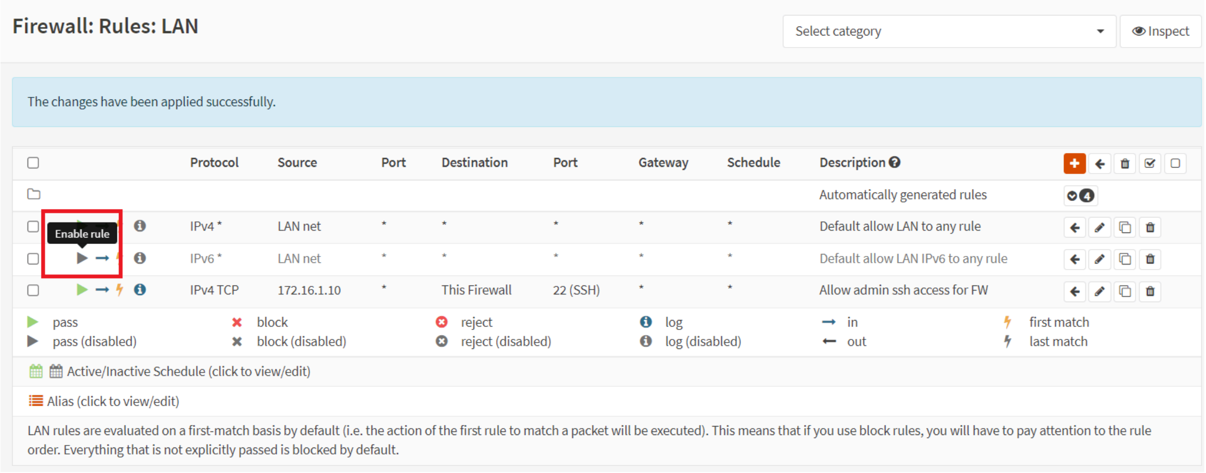
Active/Inactive Schedule (click to view/edit)

Alias (click to view/edit)

LAN rules are evaluated on a first-match basis by default (i.e. the action of the first rule to match a packet will be executed). This means that if you use block rules, you will have to pay attention to the rule order. Everything that is not explicitly passed is blocked by default.

Figure 15. *Enabling multiple firewall rules*

To enable a specific firewall rule, click on the `action` icon with solid grey color at the beginning of the related rule.



Firewall: Rules: LAN

Select category ▾ | 👁 Inspect

The changes have been applied successfully.

☐		Protocol	Source	Port	Destination	Port	Gateway	Schedule	Description
🗀									Automatically generated rules
☐	ℹ	IPv4 *	LAN net	*	*	*	*	*	Default allow LAN to any rule
☐	▶ → ℹ	IPv6 *	LAN net	*	*	*	*	*	Default allow LAN IPv6 to any rule
☐	▶ → ϟ ℹ	IPv4 TCP	172.16.1.10	*	This Firewall	22 (SSH)	*	*	Allow admin ssh access for FW

▶ pass ✖ block ✖ reject ℹ log → in ϟ first match
▶ pass (disabled) ✖ block (disabled) ✖ reject (disabled) ℹ log (disabled) ← out ϟ last match

Active/Inactive Schedule (click to view/edit)

Alias (click to view/edit)

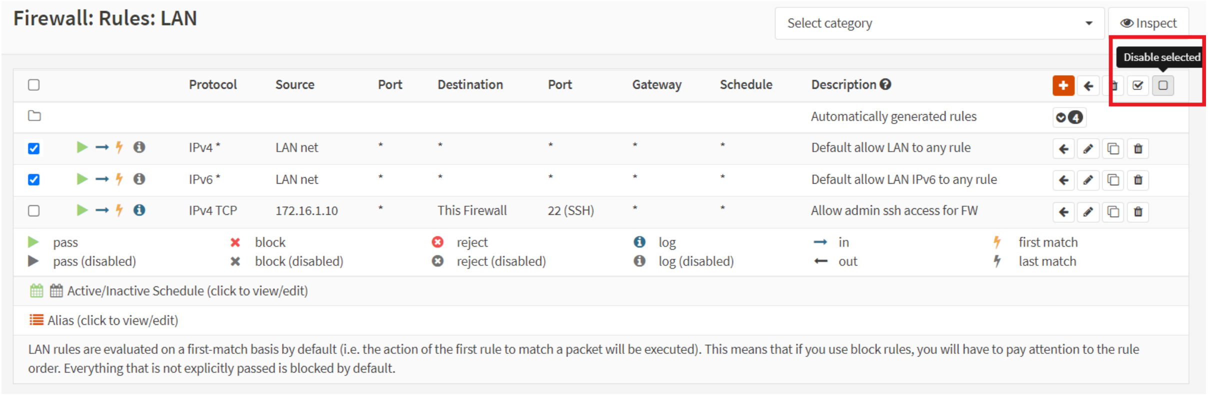
LAN rules are evaluated on a first-match basis by default (i.e. the action of the first rule to match a packet will be executed). This means that if you use block rules, you will have to pay attention to the rule order. Everything that is not explicitly passed is blocked by default.

Figure 16. *Enabling a specific firewall rule*

Lastly, Click on the **`Apply Changes`** button to activate the new rule settings.

7. Disabling Firewall Rules

To disable some of the disabled firewall rules, click on the empty square box icon on the header bar of the rule list after selecting the rules that you wish to enable.



Firewall: Rules: LAN

Select category ▾ | 👁 Inspect

Disable selected

□		Protocol	Source	Port	Destination	Port	Gateway	Schedule	Description
									Automatically generated rules
☑	▶ → ϟ ℹ	IPv4 *	LAN net	*	*	*	*	*	Default allow LAN to any rule
☑	▶ → ϟ ℹ	IPv6 *	LAN net	*	*	*	*	*	Default allow LAN IPv6 to any rule
□	▶ → ϟ ℹ	IPv4 TCP	172.16.1.10	*	This Firewall	22 (SSH)	*	*	Allow admin ssh access for FW

▶ pass	✖ block	⊗ reject	ℹ log	→ in	ϟ first match
▶ pass (disabled)	✖ block (disabled)	⊗ reject (disabled)	ℹ log (disabled)	← out	ϟ last match

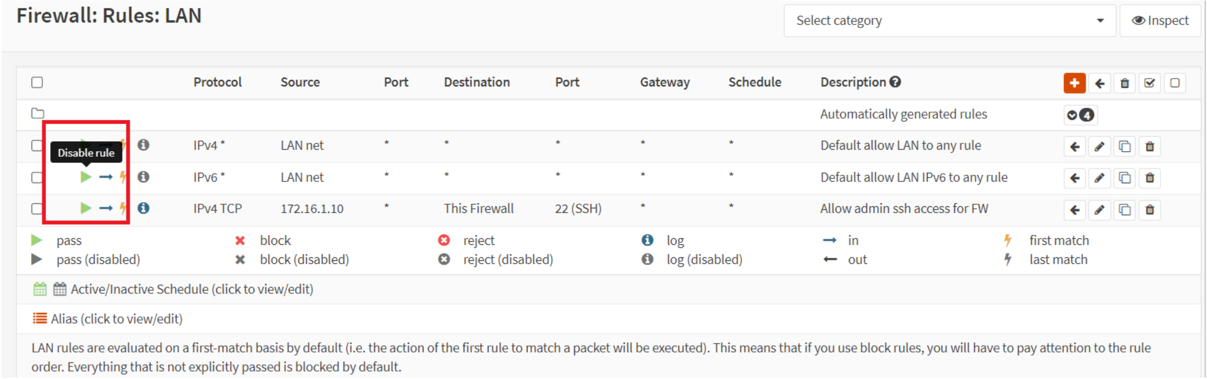
Active/Inactive Schedule (click to view/edit)

Alias (click to view/edit)

LAN rules are evaluated on a first-match basis by default (i.e. the action of the first rule to match a packet will be executed). This means that if you use block rules, you will have to pay attention to the rule order. Everything that is not explicitly passed is blocked by default.

Figure 17. *Disabling multiple firewall rules*

To disable a specific firewall rule, click on the `action` icon with green or red color at the beginning of the related rule.



Firewall: Rules: LAN

Select category ▾ | 👁 Inspect

□		Protocol	Source	Port	Destination	Port	Gateway	Schedule	Description
									Automatically generated rules
□	Disable rule ℹ	IPv4 *	LAN net	*	*	*	*	*	Default allow LAN to any rule
□	▶ → ϟ ℹ	IPv6 *	LAN net	*	*	*	*	*	Default allow LAN IPv6 to any rule
□	▶ → ϟ ℹ	IPv4 TCP	172.16.1.10	*	This Firewall	22 (SSH)	*	*	Allow admin ssh access for FW

▶ pass	✖ block	⊗ reject	ℹ log	→ in	ϟ first match
▶ pass (disabled)	✖ block (disabled)	⊗ reject (disabled)	ℹ log (disabled)	← out	ϟ last match

Active/Inactive Schedule (click to view/edit)

Alias (click to view/edit)

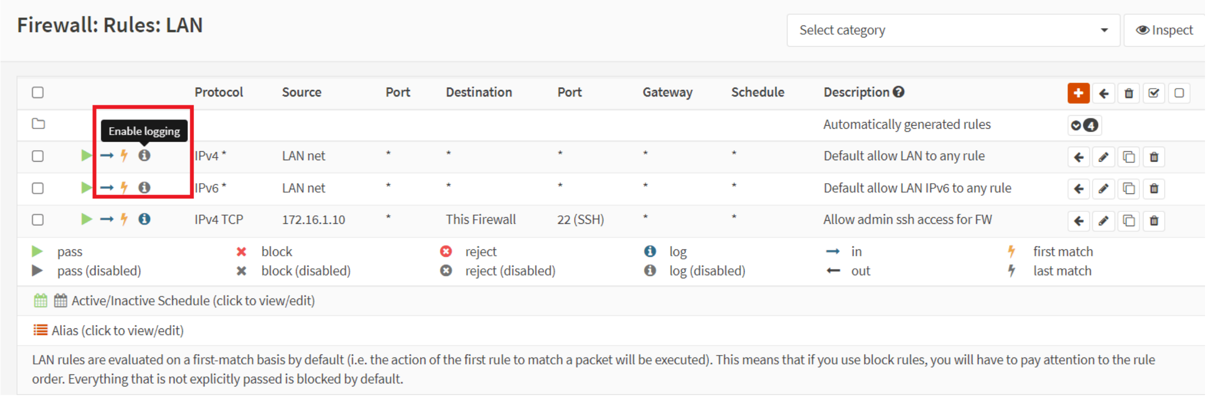
LAN rules are evaluated on a first-match basis by default (i.e. the action of the first rule to match a packet will be executed). This means that if you use block rules, you will have to pay attention to the rule order. Everything that is not explicitly passed is blocked by default.

Figure 18. *Disabling a specific firewall rule*

Lastly, Click on the **`Apply Changes`** button to activate the new rule settings.

8. Enabling/Disabling logging for a Firewall Rule

To enable logging for a firewall rule, click on the solid grey circle with **`i`** icon on the rule. This will turn the grey color to the blue. And then Click on the **`Apply Changes`** button to enable the logging for the rule



Firewall: Rules: LAN

Select category ▾ | Inspect

□		Protocol	Source	Port	Destination	Port	Gateway	Schedule	Description
									Automatically generated rules
□	Enable logging	IPv4 *	LAN net	*	*	*	*	*	Default allow LAN to any rule
□		IPv6 *	LAN net	*	*	*	*	*	Default allow LAN IPv6 to any rule
□		IPv4 TCP	172.16.1.10	*	This Firewall	22 (SSH)	*	*	Allow admin ssh access for FW

pass / pass (disabled) — block / block (disabled) — reject / reject (disabled) — log / log (disabled) — in / out — first match / last match

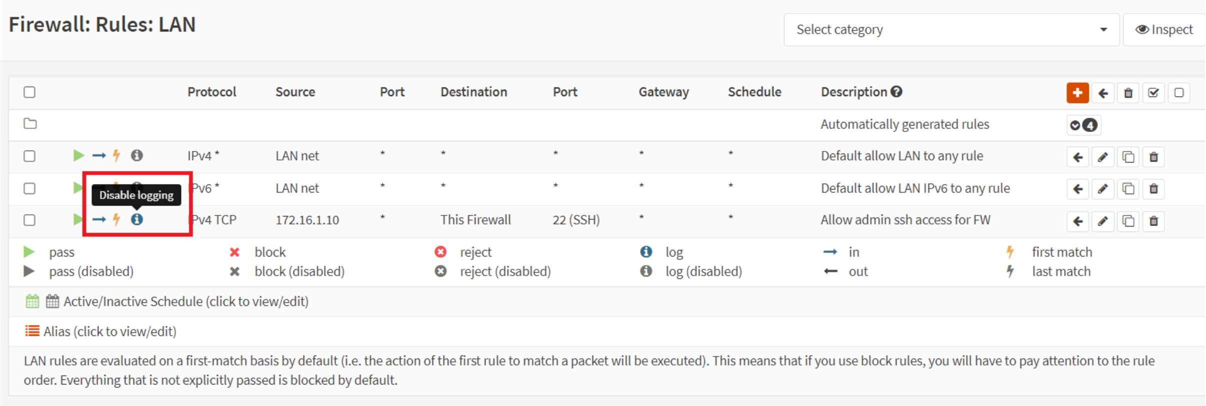
Active/Inactive Schedule (click to view/edit)

Alias (click to view/edit)

LAN rules are evaluated on a first-match basis by default (i.e. the action of the first rule to match a packet will be executed). This means that if you use block rules, you will have to pay attention to the rule order. Everything that is not explicitly passed is blocked by default.

Figure 19. *Enabling logging for a firewall rule*

To disable logging for a firewall rule, click on the blue circle with the `i` icon on the rule. This will turn the blue color to grey. And then click on the **`Apply Changes`** button to enable the logging for the rule.



Firewall: Rules: LAN

Select category ▾ | Inspect

□		Protocol	Source	Port	Destination	Port	Gateway	Schedule	Description
									Automatically generated rules
□		IPv4 *	LAN net	*	*	*	*	*	Default allow LAN to any rule
□	Disable logging	IPv6 *	LAN net	*	*	*	*	*	Default allow LAN IPv6 to any rule
□		IPv4 TCP	172.16.1.10	*	This Firewall	22 (SSH)	*	*	Allow admin ssh access for FW

pass / pass (disabled) — block / block (disabled) — reject / reject (disabled) — log / log (disabled) — in / out — first match / last match

Active/Inactive Schedule (click to view/edit)

Alias (click to view/edit)

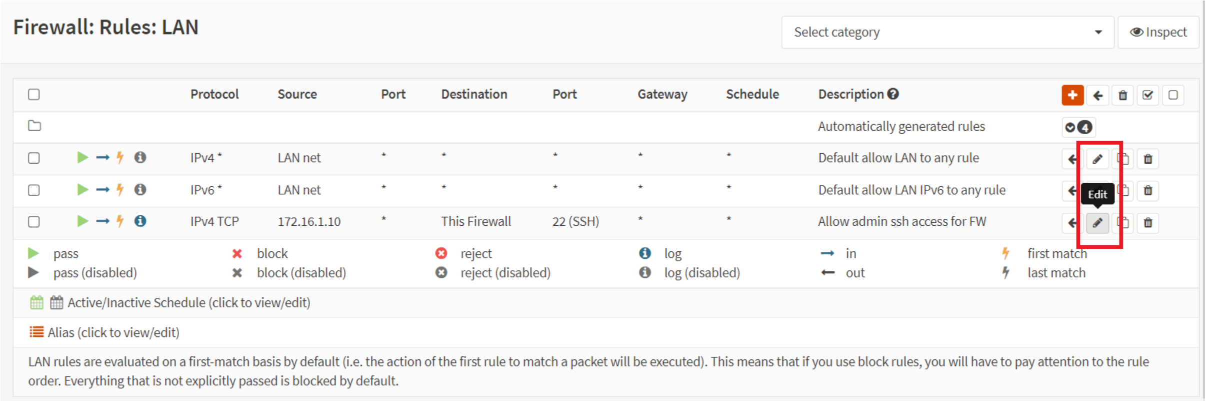
LAN rules are evaluated on a first-match basis by default (i.e. the action of the first rule to match a packet will be executed). This means that if you use block rules, you will have to pay attention to the rule order. Everything that is not explicitly passed is blocked by default.

Figure 20. *Disabling logging for a firewall rule*

9. Editing Firewall Rules

To edit a firewall rule, click on the **`pencil`** icon on the actions column of the rule that you wish to edit. This will redirect you to the firewall rule editing page. After making the changes to the rule settings, click the **`Save`** button at the bottom of the page.

Lastly, Click on the **`Apply Changes`** button to activate the new rule settings.



Firewall: Rules: LAN

Select category | 👁 Inspect

□		Protocol	Source	Port	Destination	Port	Gateway	Schedule	Description
									Automatically generated rules
□	▶ → ϟ ℹ	IPv4 *	LAN net	*	*	*	*	*	Default allow LAN to any rule
□	▶ → ϟ ℹ	IPv6 *	LAN net	*	*	*	*	*	Default allow LAN IPv6 to any rule
□	▶ → ϟ ℹ	IPv4 TCP	172.16.1.10	*	This Firewall	22 (SSH)	*	*	Allow admin ssh access for FW

▶ pass ✖ block ⊗ reject ℹ log → in ϟ first match
▶ pass (disabled) ✖ block (disabled) ⊗ reject (disabled) ℹ log (disabled) ← out ϟ last match

Active/Inactive Schedule (click to view/edit)

Alias (click to view/edit)

LAN rules are evaluated on a first-match basis by default (i.e. the action of the first rule to match a packet will be executed). This means that if you use block rules, you will have to pay attention to the rule order. Everything that is not explicitly passed is blocked by default.

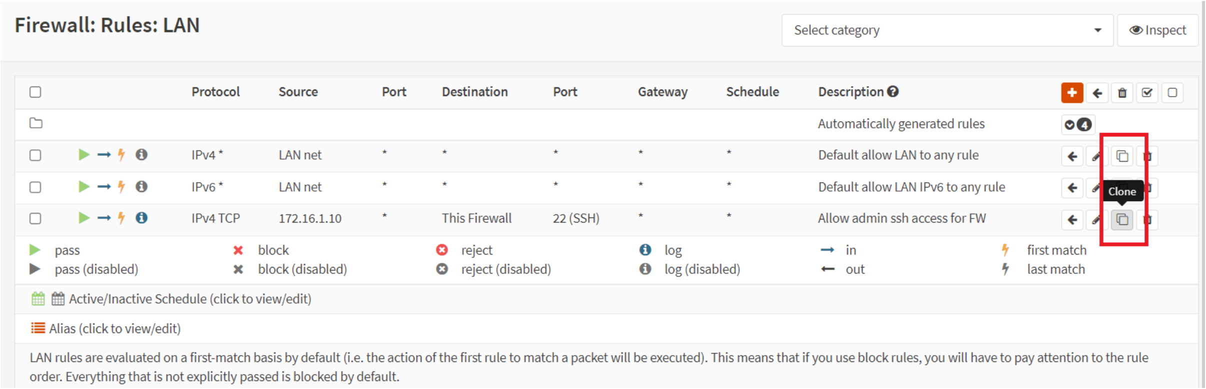
Figure 21. *Editing a firewall rule*

10. Cloning a Firewall Rule

Sometimes you may need to define very similar firewall rules with only a few different options, such as destination or interface. In such cases, cloning a rule is a very useful feature of the OPNsense.

To clone a firewall rule, click on the clone icon with two cascaded squares. This will redirect you to the firewall rule editing page. After making the changes to the rule settings, click the **`Save`** button at the bottom of the page. Your new rule is created now.

Lastly, Click on the **`Apply Changes`** button to activate the new rule on the firewall.



Firewall: Rules: LAN

Select category | 👁 Inspect

□		Protocol	Source	Port	Destination	Port	Gateway	Schedule	Description
									Automatically generated rules
□	▶ → ϟ ℹ	IPv4 *	LAN net	*	*	*	*	*	Default allow LAN to any rule
□	▶ → ϟ ℹ	IPv6 *	LAN net	*	*	*	*	*	Default allow LAN IPv6 to any rule
□	▶ → ϟ ℹ	IPv4 TCP	172.16.1.10	*	This Firewall	22 (SSH)	*	*	Allow admin ssh access for FW

▶ pass ✖ block ⊗ reject ℹ log → in ϟ first match
▶ pass (disabled) ✖ block (disabled) ⊗ reject (disabled) ℹ log (disabled) ← out ϟ last match

Active/Inactive Schedule (click to view/edit)

Alias (click to view/edit)

LAN rules are evaluated on a first-match basis by default (i.e. the action of the first rule to match a packet will be executed). This means that if you use block rules, you will have to pay attention to the rule order. Everything that is not explicitly passed is blocked by default.

Figure 22. *Cloning a firewall rule*

OPNsense Firewall Rules Examples

Some common firewall rules examples which might be very useful for home users and small businesses to get their firewalls ready are given below.

1. Allowing Only Specific DNS Servers

One of the firewall rules you should define for preventing cyber threats is to block your LAN devices accessing the DNS servers except for your own DNS servers or specific external DNS that offer content filtering/blocking. These rules keep clients from going rogue and circumventing the filtering/blocking policies you've put in place for your LAN or home network.

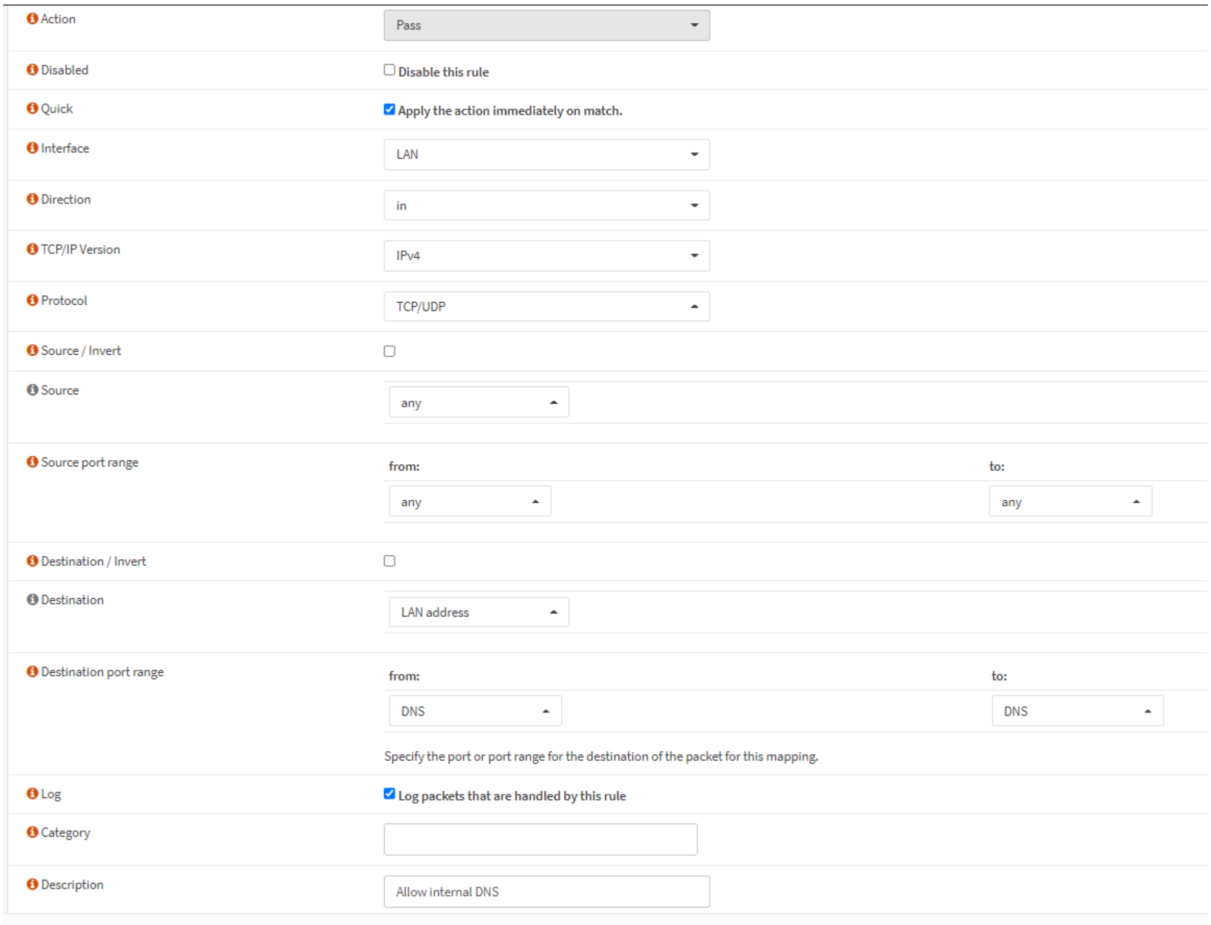
To restrict the DNS service in your network for increasing the cybersecurity, you may follow the next two main steps:

1. Define a rule to Allow the internal DNS server(s), by following the instructions below.

Option	Value
Action	Pass
Protocol	TCP/UDP
Source	any
Source Port	any
Destination	LAN address
Destination Port	DNS (53)
Description	Allow internal DNS

- Select `Pass` for the allow rule.
- Select `TCP/UDP` for the `Protocol`.
- Select the source address and source port of **any**. This captures all traffic on the LAN interface bound for the specified destination.
- You may choose the LAN address of the OPNsense as the destination address. Or, enter the IP address of your own DNS server on LAN.

- Select **DNS** predefined port alias for the destination port.



Action	Pass	
Disabled	□ Disable this rule	
Quick	☑ Apply the action immediately on match.	
Interface	LAN	
Direction	in	
TCP/IP Version	IPv4	
Protocol	TCP/UDP	
Source / Invert	□	
Source	any	
Source port range	from: any	to: any
Destination / Invert	□	
Destination	LAN address	
Destination port range	from: DNS Specify the port or port range for the destination of the packet for this mapping.	to: DNS
Log	☑ Log packets that are handled by this rule	
Category		
Description	Allow internal DNS	

Figure 23. Allow Internal DNS firewall rule

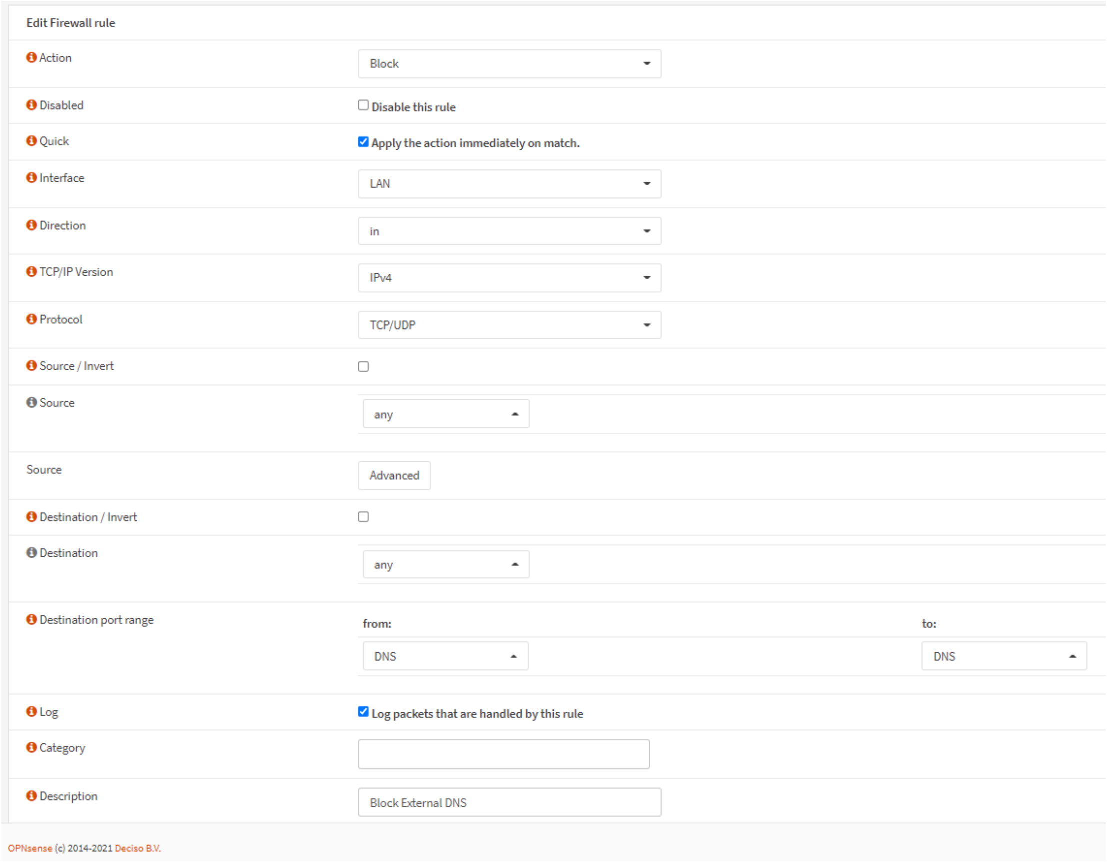
Because the DNS service is advertised on each interface's IP address, the LAN address is used as the destination. The IP address of the interface is also used as the gateway address for devices on that network. When you look at the DHCP information for each device, you'll notice that the LAN address serves as both the gateway server and the DNS server.

Depending on your network configuration, the DNS IP address may differ from the gateway IP address. However, for this example, it is assumed that we're using the DNS server configuration in OPNsense.

2. Define the rule to deny the external DNS server(s), by following the instructions below.

Option	Value
Action	Block
Protocol	TCP/UDP
Source	any
Source Port	any
Destination	any
Destination Port	DNS (53)
Description	Block external DNS

- Select "**Block**" for the deny rule.
- Select `TCP/UDP` for the `Protocol`.
- The source address and port on the LAN network must be configured to any device.
- The destination must be **any** for that block rule since we want to block attempts to use any other DNS server.
- Choose destination port **DNS**.



Edit Firewall rule

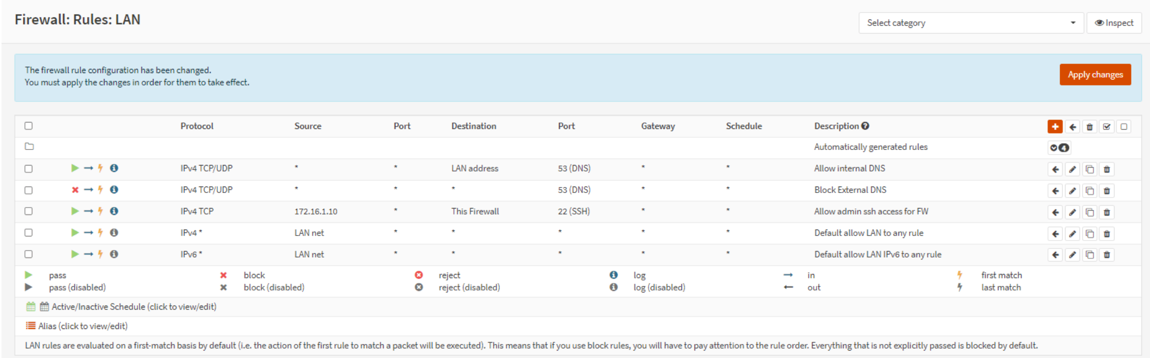
Action	Block
Disabled	□ Disable this rule
Quick	☑ Apply the action immediately on match.
Interface	LAN
Direction	in
TCP/IP Version	IPv4
Protocol	TCP/UDP
Source / Invert	□
Source	any
Source	Advanced
Destination / Invert	□
Destination	any
Destination port range	from: DNS to: DNS
Log	☑ Log packets that are handled by this rule
Category	
Description	Block External DNS

OPNsense (c) 2014-2021 Deciso B.V.

Figure 24. *Block external DNS server rule*

Recall that any attempt to contact the specified DNS server in the above **`allow`** rule is successful because of the rule order processing and rule treatment for that request ceases. However, if a device attempts to access a DNS external server, the **`block`** rule will be reached as it does not pass the **`allow`** rule which prohibits that server access.

The first rule permits access to your local DNS server whilst the second rule blocks access to all other DNS servers irrespective of whether local or remote. You may need to move these rules to the top of your rule list. Don't forget to click on the **`Apply Changes`** button to activate the newly created DNS rules.



Firewall: Rules: LAN

The firewall rule configuration has been changed.
You must apply the changes in order for them to take effect.

□		Protocol	Source	Port	Destination	Port	Gateway	Schedule	Description
									Automatically generated rules
□	▶ → ϟ ℹ	IPv4 TCP/UDP	*	*	LAN address	53 (DNS)	*	*	Allow internal DNS
□	✖ → ϟ ℹ	IPv4 TCP/UDP	*	*	*	53 (DNS)	*	*	Block External DNS
□	▶ → ϟ ℹ	IPv4 TCP	172.16.1.10	*	This Firewall	22 (SSH)	*	*	Allow admin ssh access for FW
□	▶ → ϟ ℹ	IPv4 *	LAN net	*	*	*	*	*	Default allow LAN to any rule
□	▶ → ϟ ℹ	IPv6 *	LAN net	*	*	*	*	*	Default allow LAN IPv6 to any rule

▶ pass ✖ block ⊗ reject ℹ log → in ϟ first match
▶ pass (disabled) ✖ block (disabled) ⊗ reject (disabled) ℹ log (disabled) ← out ϟ last match

Active/Inactive Schedule (click to view/edit)

Alias (click to view/edit)

LAN rules are evaluated on a first-match basis by default (i.e. the action of the first rule to match a packet will be executed). This means that if you use block rules, you will have to pay attention to the rule order. Everything that is not explicitly passed is blocked by default.

Figure 25. *Internal and external DNS firewall rules on the list*

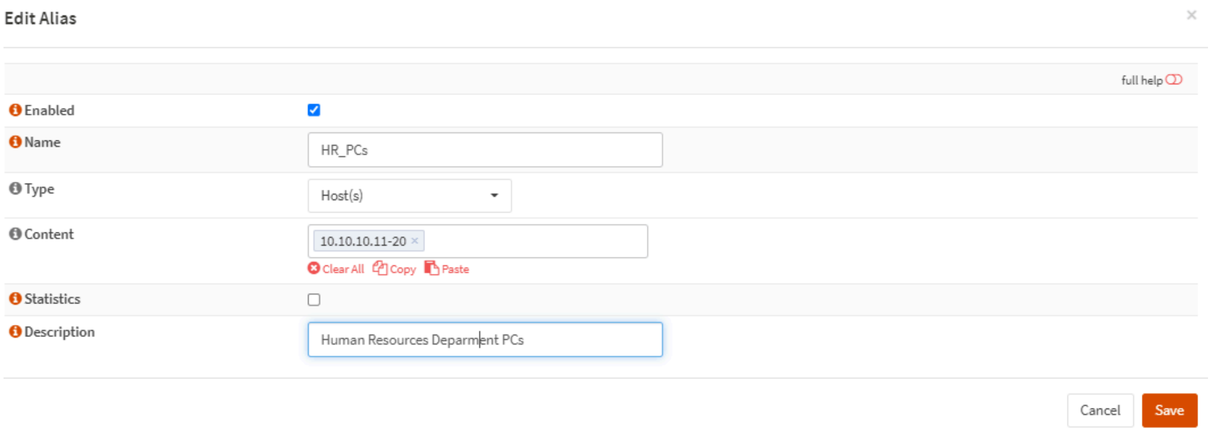
2. Allowing Local Services between different Network Segments(VLANs)

As a rule of thumb, you should isolate critical servers from client devices by implementing network segmentation in your infrastructure. OPNsense firewall allows you to build internal zones separating functional areas so as to minimize attack surfaces and prevent threats from propagating beyond the zone.

For example, human resources (HR) database servers should only be accessible by HR department staff computers in a company network. To define the required OPNsense firewall rules, you may follow the next steps given below.

Option	**Value**
Action	Pass
Protocol	TCP
Source	HR_PCs
Source Port	any
Destination	HR_DBserver
Destination Port	MySQL
Description	Allow access to HR Database Server

- Define an Hosts alias, such as HR_PCs, for the HR client devices(such as 10.10.10.11-10.10.10.20).

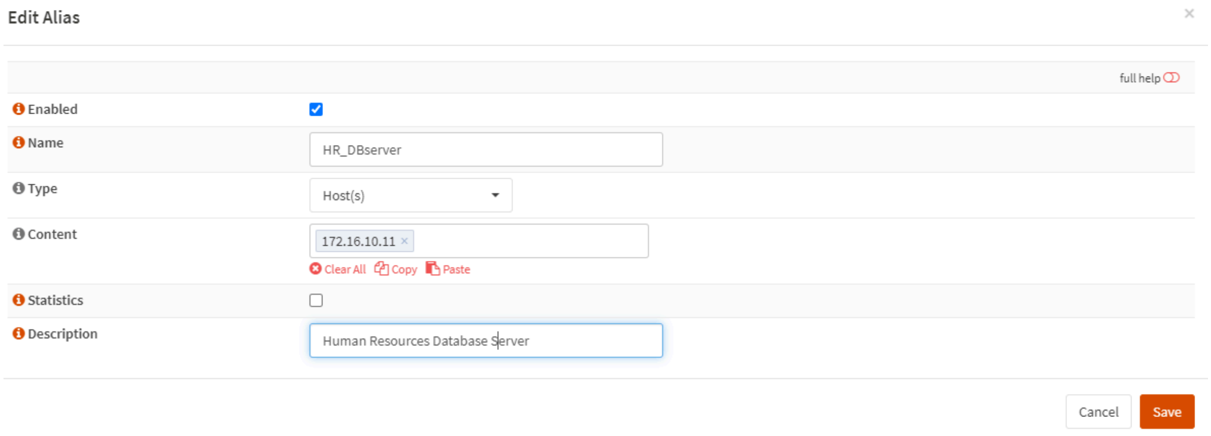


Edit Alias

Enabled	☑
Name	HR_PCs
Type	Host(s)
Content	10.10.10.11-20
Statistics	□
Description	Human Resources Deparment PCs

Figure 26. *Defining an alias for Human Resources PCs*

- Define a Hosts alias, such as HR_DBserver, for the HR Database Server(such as 172.16.10.20)

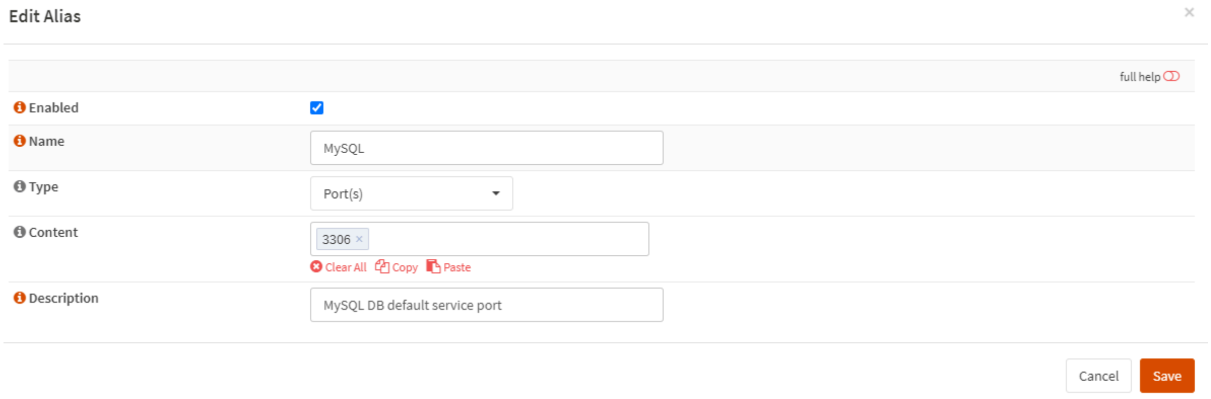


Edit Alias

Enabled	☑
Name	HR_DBserver
Type	Host(s)
Content	172.16.10.11 ×
Statistics	☐
Description	Human Resources Database Server

Figure 27. *Defining an alias for Human Resources Database Server*

- Define a Port alias, such as MySQL, for the HR Database Server MySQL service(the default port for MySQL)

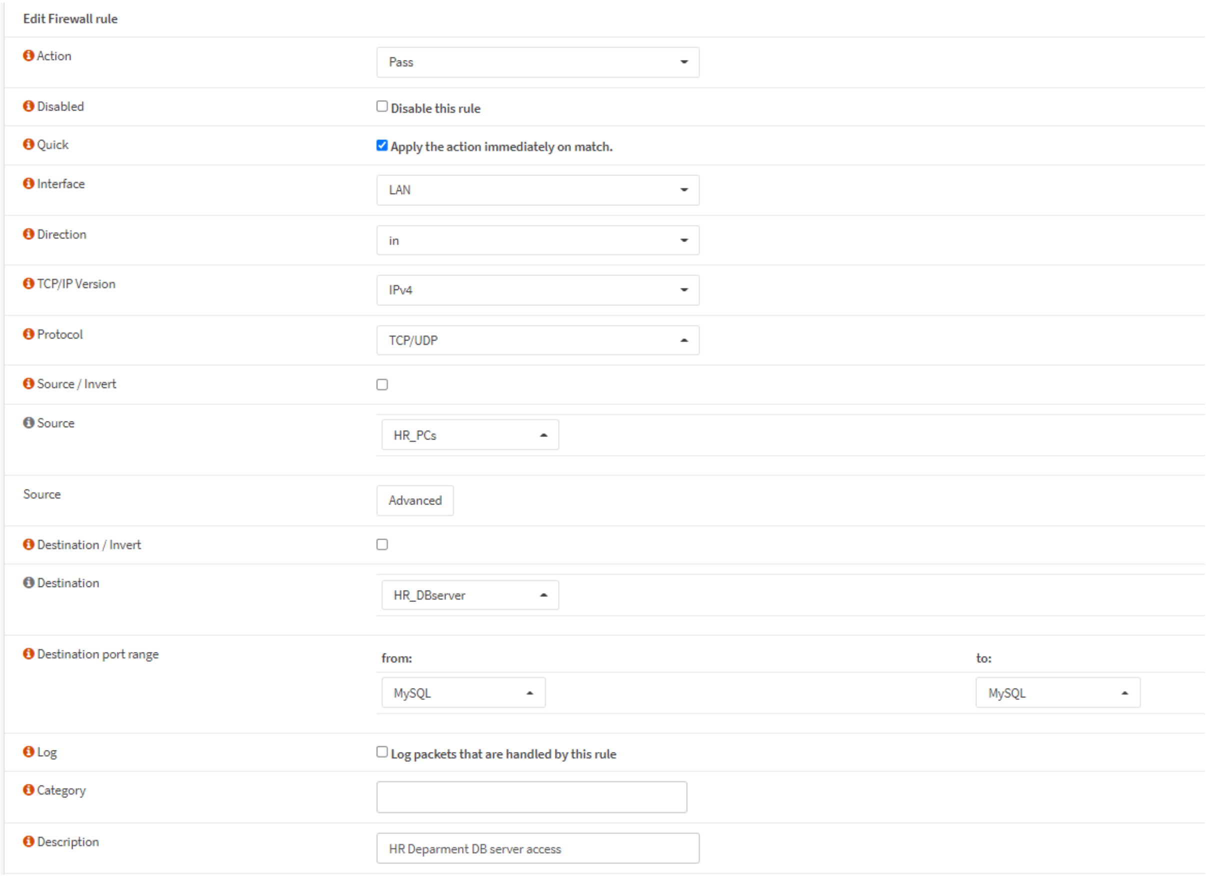


Edit Alias

Enabled	☑
Name	MySQL
Type	Port(s)
Content	3306 ×
Description	MySQL DB default service port

Figure 28. *Defining an alias for MySQL default service port(3306/TCP)*

- Navigate to the interface in which the HR client device resides, such as LAN, on the Firewall Rules. Then we need to allow access to port **3306**.
- Select `Pass` for the allow rule.
- Set the `HR_PCs` as the source.
- Set `TCP` as the Protocol
- Set `HR_DBserver` on the destination
- Set `MySQL` as the destination port range.

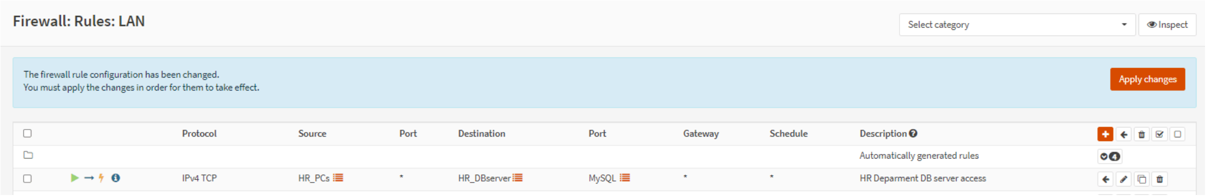


Edit Firewall rule

Action	Pass
Disabled	□ Disable this rule
Quick	☑ Apply the action immediately on match.
Interface	LAN
Direction	in
TCP/IP Version	IPv4
Protocol	TCP/UDP
Source / Invert	□
Source	HR_PCs
Source	Advanced
Destination / Invert	□
Destination	HR_DBserver
Destination port range	from: MySQL to: MySQL
Log	□ Log packets that are handled by this rule
Category	
Description	HR Deparment DB server access

Figure 29. *Defining HR Database server access rule*

This rule provides network access from your HR staff PCs to the HR Database server. There should be either **`Deny all`** rule at the end of the list or another deny rule for preventing other devices' access to the HR DB server. Don't forget to apply changes to activate the rules.



Firewall: Rules: LAN

The firewall rule configuration has been changed.
You must apply the changes in order for them to take effect.

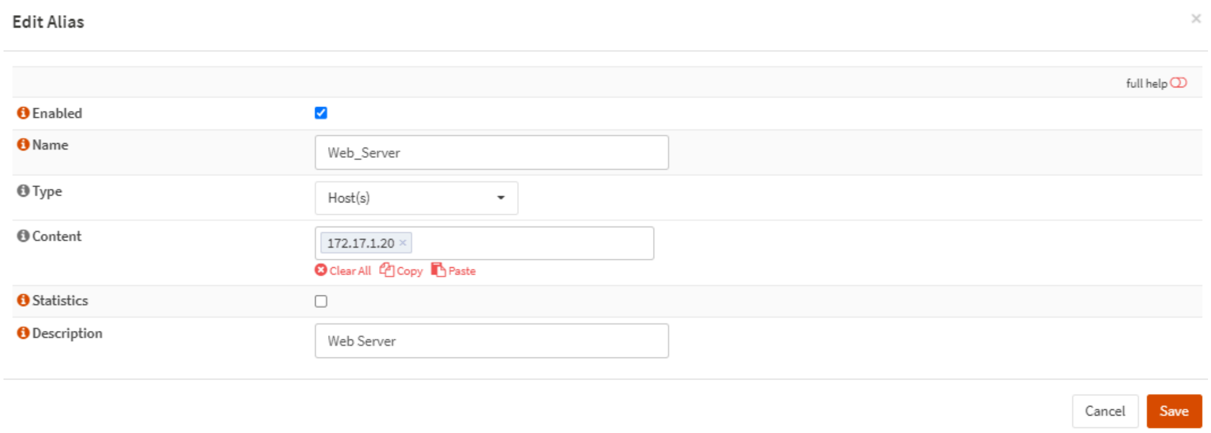
□		Protocol	Source	Port	Destination	Port	Gateway	Schedule	Description
									Automatically generated rules
□	▶ → ϟ	IPv4 TCP	HR_PCs	*	HR_DBserver	MySQL	*	*	HR Deparment DB server access

Figure 30. *HR Database server access rule*

It is recommended to create a DMZ network that grants external sources restricted access to publicly available information while protecting the internal networks from outside attacks. As a second example, we will allow internal clients to access the webserver located in the DMZ network.

Option	Value
Action	Pass
Protocol	TCP
Source	LAN net
Source Port	any
Destination	Web_server
Destination Port	HTTPS
Description	Allow access to Web Server

- Define a Hosts alias, such as Web_server, for the Web server location in DMZ(such as 172.17.1.20).



Edit Alias

Enabled ☑

Name Web_Server

Type Host(s)

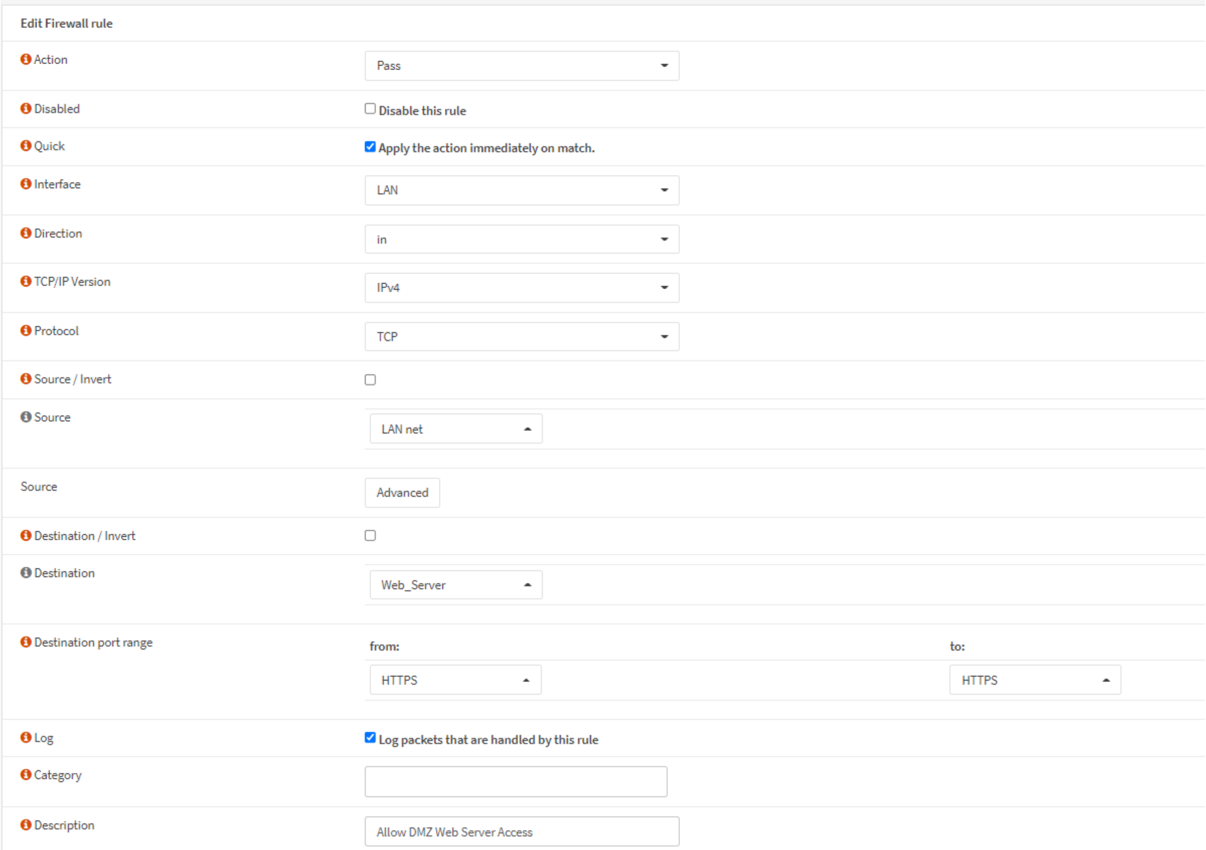
Content 172.17.1.20

Statistics □

Description Web Server

Figure 31. *Defining an alias for a Web Server on the DMZ network*

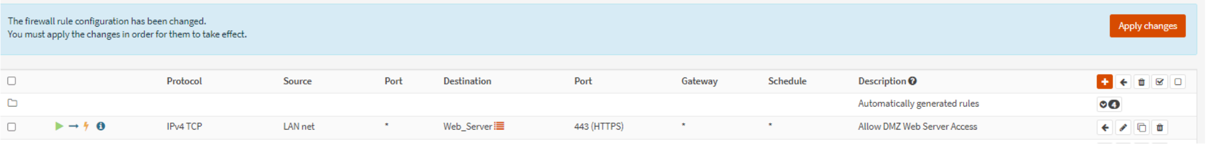
- Navigate to the LAN interface. Then we need to allow access to HTTPS port **443**.
- Select `Pass` for allow rule.
- Set the LANnet as the source.
- Set Web_server on the destination
- Set HTTPS as the destination port.



Edit Firewall rule

Action	Pass	
Disabled	□ Disable this rule	
Quick	☑ Apply the action immediately on match.	
Interface	LAN	
Direction	in	
TCP/IP Version	IPv4	
Protocol	TCP	
Source / Invert	□	
Source	LAN net	
Source	Advanced	
Destination / Invert	□	
Destination	Web_Server	
Destination port range	from: HTTPS	to: HTTPS
Log	☑ Log packets that are handled by this rule	
Category		
Description	Allow DMZ Web Server Access	

Figure 32. *Defining DMZ Web Server access rule*



The firewall rule configuration has been changed.
You must apply the changes in order for them to take effect.

□		Protocol	Source	Port	Destination	Port	Gateway	Schedule	Description
									Automatically generated rules
□		IPv4 TCP	LAN net	*	Web_Server	443 (HTTPS)	*	*	Allow DMZ Web Server Access

Figure 33. *Allow DMZ Web Server access rule*

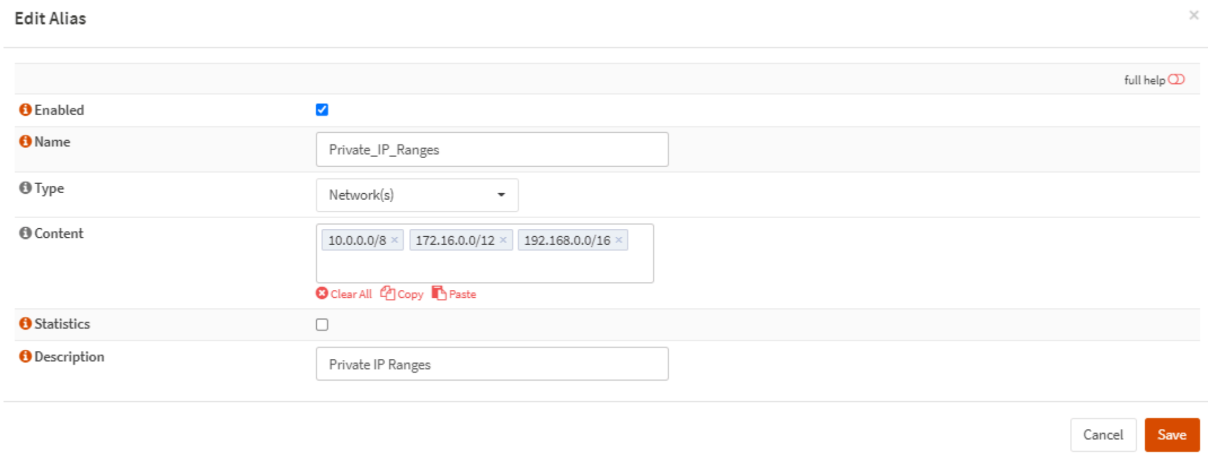
3. Block Access to Other VLANs

It is advised to block any unnecessary service access between internal networks(VLANs). By default, traffics between different VLANs is not allowed unless there is a `allow all` rule at the bottom of the firewall rule list.

However, home users may generally want a `allow all` rule to allow all traffic that is not specifically forbidden. Therefore, they should define a specific rule to block connections between the VLANs in their home networks. Otherwise, any device on a network can communicate with any other device on other VLANs which means that all advantages of the network segmentation are lost.

To define the required OPNsense firewall rule, you may follow the next steps given below.

1. Create an alias, such as `Private_IP_Ranges` for all private IP address ranges by navigating to the **`Firewall -> Aliases`**.



Edit Alias

Enabled ☑

Name: Private_IP_Ranges

Type: Network(s)

Content: 10.0.0.0/8 × 172.16.0.0/12 × 192.168.0.0/16 ×

Statistics □

Description: Private IP Ranges

Figure 34. *Defining an alias for Private IP ranges*

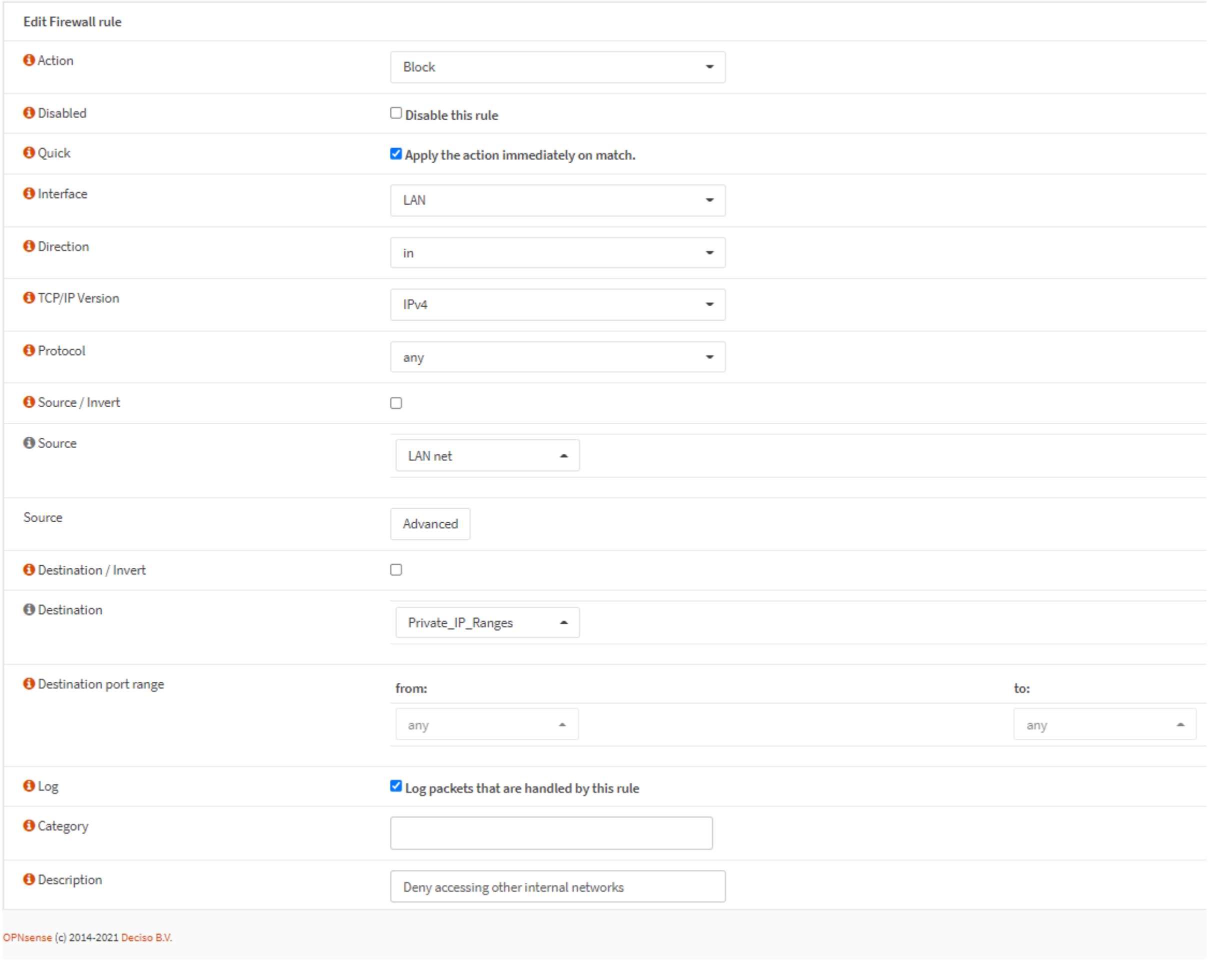
Option	Value
Action	Block
Protocol	any
Source	LAN net
Source Port	any
Destination	Private_IP_Ranges
Destination Port	any
Description	Block access to all other private networks

2. Select "**Block**" for the deny rule.

3. The source address and port on the LAN network must be configured to **any** device.

4. The destination must be `PrivateNetworks` for that block rule since we want to block attempts to use any other internal networks.

5. Choose destination port **any**.



Edit Firewall rule

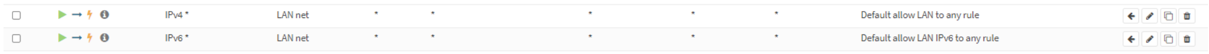
Action	Block
Disabled	□ Disable this rule
Quick	☑ Apply the action immediately on match.
Interface	LAN
Direction	in
TCP/IP Version	IPv4
Protocol	any
Source / Invert	□
Source	LAN net
Source	Advanced
Destination / Invert	□
Destination	Private_IP_Ranges
Destination port range	from: any to: any
Log	☑ Log packets that are handled by this rule
Category	
Description	Deny accessing other internal networks

OPNsense (c) 2014-2021 Deciso B.V.

Figure 35. *Deny accessing other internal networks*

4. Allowing All Traffic

At the bottom of the OPNsense firewall rule list, there is an implicit **`deny all`** rule by default. Therefore, firewall administrators define a rule for each of the required services to **`allow`** access. However, it may be cumbersome to identify the ports for all services and define the rule properly especially for home users. Though it is not advisable for company networks, home users may prefer to define the block rules at the beginning of the firewall rules first and then allow all traffic. Since, they may not have enough technical knowledge or time to troubleshoot the blocking connections when their kids or wifes using their smart devices, play stations, or laptops.



□	▶ → ϟ ℹ	IPv4 *	LAN net	*	*	*	*	*	Default allow LAN to any rule
□	▶ → ϟ ℹ	IPv6 *	LAN net	*	*	*	*	*	Default allow LAN IPv6 to any rule

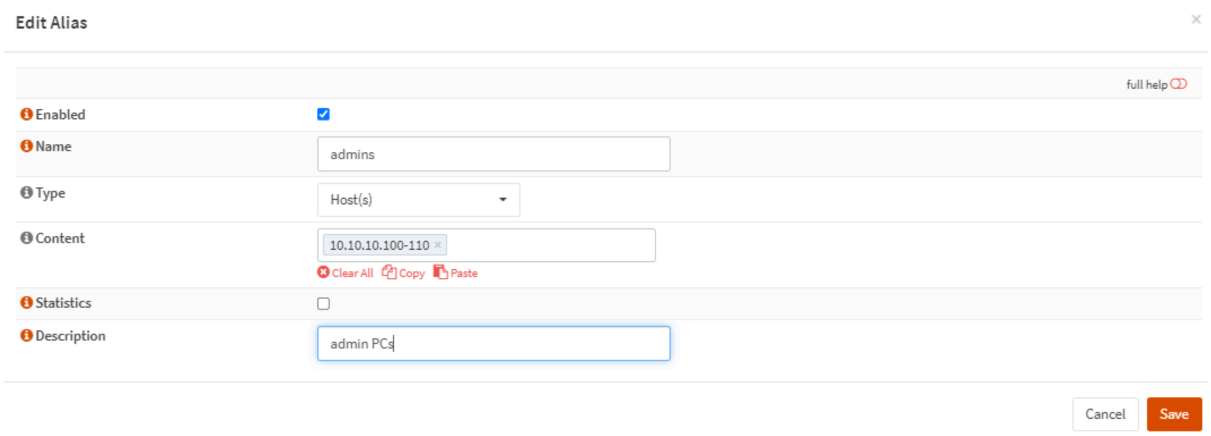
Figure 36. *Allow all rules*

5. Allowing unrestricted access for administrator

In case of any IT service outage, the administrator should access any device from his/her PC or a server that he can physically access for quick troubleshooting. Therefore, it is a suitable approach to defining a rule which allows unrestricted access for an administrator at the top of the rule list before the **`block`** rules.

To define the required OPNsense firewall rule, you may follow the next steps given below.

1. Create an alias, such as `admins` for all administrator devices/servers by navigating to the **`Firewall`** **->** **`Aliases`**.



Edit Alias

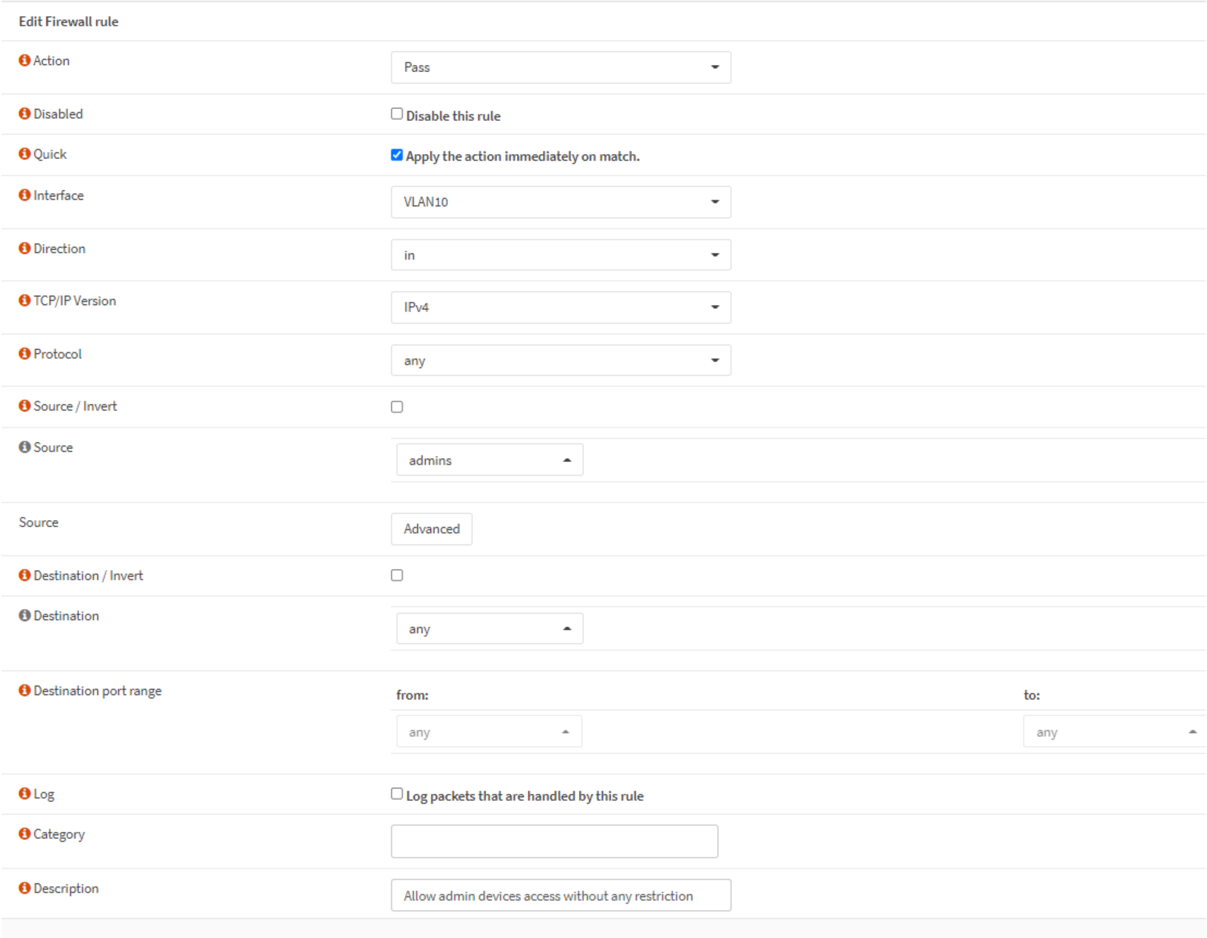
Enabled	☑
Name	admins
Type	Host(s)
Content	10.10.10.100-110
Statistics	□
Description	admin PCs

Figure 37. *Defining an alias for admin devices*

Option	Value
Action	Pass
Interface	VLAN10
Protocol	any
Source	admins
Source Port	any
Destination	any
Destination Port	any
Description	Allow admin devices access to anywhere without any restriction

2. Navigate to the interface in which the admin devices reside, such as VLAN10, on the Firewall Rules. Then we need to allow access to anywhere.

3. Select `Pass` for the allow rule.
4. Select `admins` as Source.
5. Select **any** as Source port, destination and destination port range.



Edit Firewall rule

Action	Pass
Disabled	□ Disable this rule
Quick	☑ Apply the action immediately on match.
Interface	VLAN10
Direction	in
TCP/IP Version	IPv4
Protocol	any
Source / Invert	□
Source	admins
Source	Advanced
Destination / Invert	□
Destination	any
Destination port range	from: any to: any
Log	□ Log packets that are handled by this rule
Category	
Description	Allow admin devices access without any restriction

Figure 38. *Allow admin devices access without any restriction*

6. Blocking All Devices in LAN from accessing a malicious IP on Internet

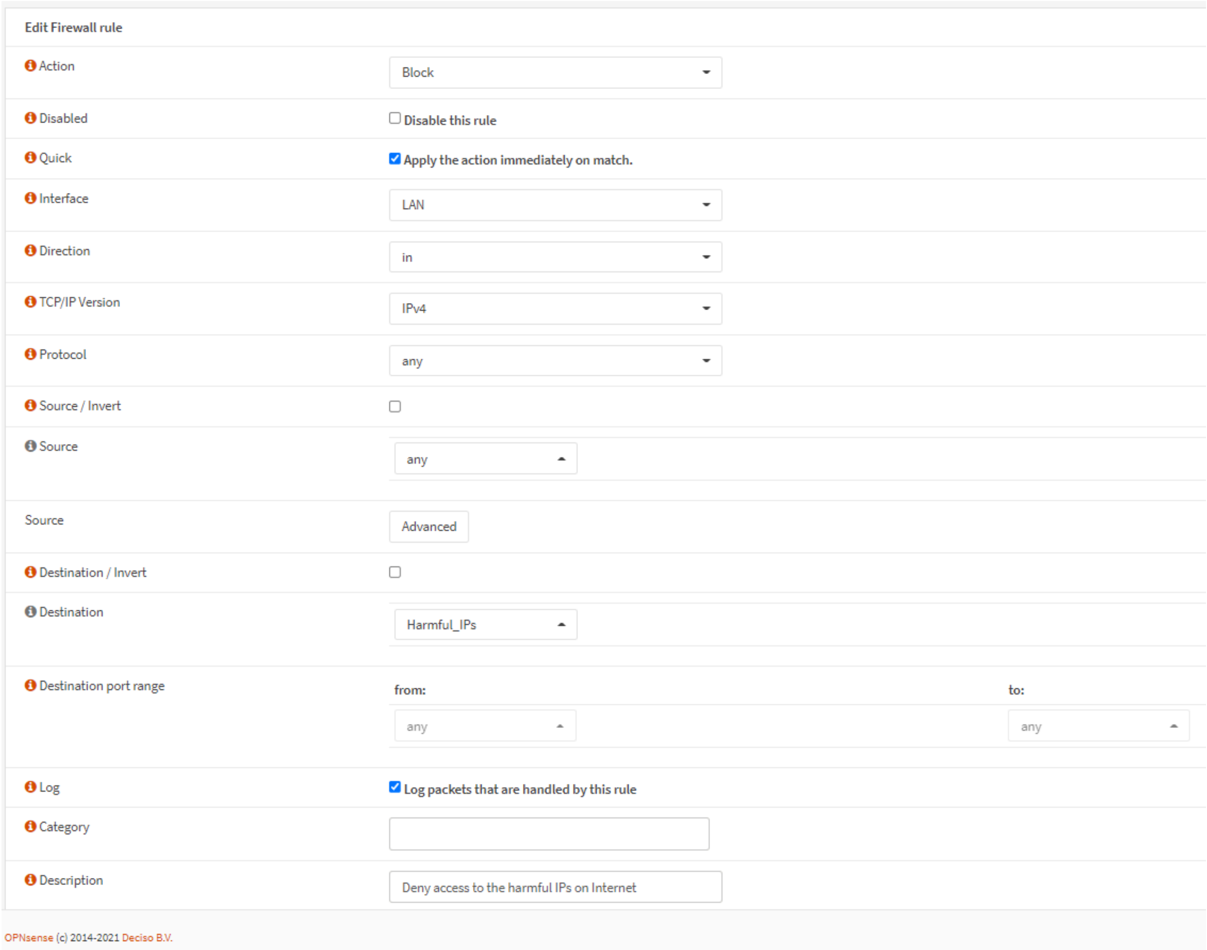
Sometimes you may notice that there is a cyber threat that comes from a malicious IP, such as a phishing server, on the Internet. To block all clients and servers in your internal network from reaching the harmful IP address on the Internet, you may define a specific block rule at the top of the rule list before the `allow` rules. You may also put all suspicious IPs you detected in a Hosts alias, such as `Harmful-IPs`.

1. Create an alias, such as `Harmful_IPs` for malicious IP addresses by navigating to the **`Firewall -> Aliases`**.
2. Navigate to the LAN interface on the Firewall Rules.
3. Select `Block` for the deny rule.

4. Select **any** as the Source.
5. Select **any** as Source port.
6. Select `Harmful_IPs` as destination.
7. Select **any** as the destination port range.

Option	**Value**
Action	Block
Interface	LAN
Protocol	any
Source	LAN net
Source Port	any
Destination	Harmful_IPs
Destination Port	any
Description	Block access to the harmful hosts/servers on the Internet

8.



Edit Firewall rule

Action	Block
Disabled	□ Disable this rule
Quick	☑ Apply the action immediately on match.
Interface	LAN
Direction	in
TCP/IP Version	IPv4
Protocol	any
Source / Invert	□
Source	any
Source	Advanced
Destination / Invert	□
Destination	Harmful_IPs
Destination port range	from: any to: any
Log	☑ Log packets that are handled by this rule
Category	
Description	Deny access to the harmful IPs on Internet

OPNsense (c) 2014-2021 Deciso B.V.

Figure 39. *Defining a rule to Deny access to the harmful IPs on the Internet*

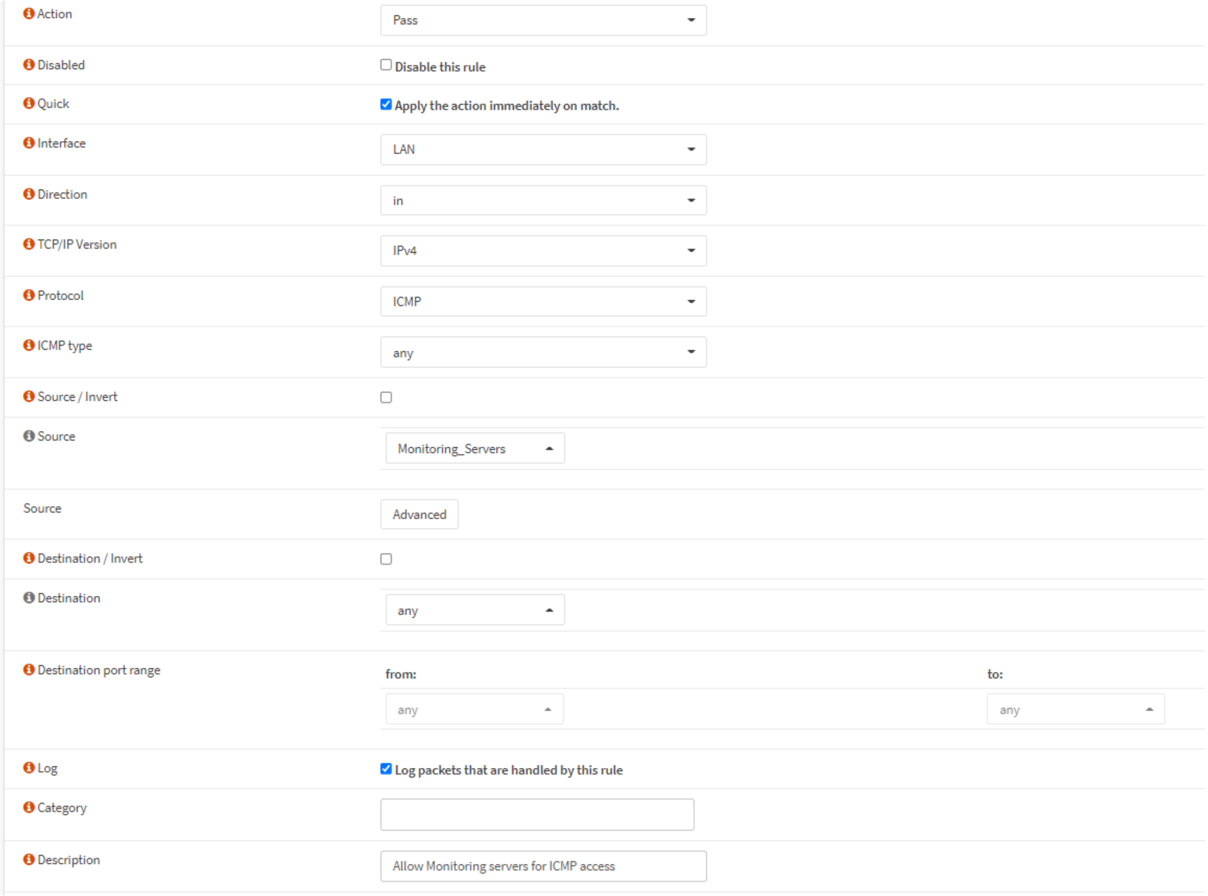
7. Allowing ICMP messages for troubleshooting

If you use the **`deny all`** rule at the end of the firewall rule list, any of the devices cannot ping anywhere in other networks. However, for troubleshooting or monitoring purposes you may need to allow ICMP messages for a specific PC or server. To accomplish this, you may define the following **`allow`** rules and alias, such as `Monitoring-servers`.

Option	Value
Action	Pass
Interface	LAN
Protocol	ICMP
ICMP type	any

Source	Monitoring_Servers
Source Port	any
Destination	any
Description	Allow ICMP echo request messages

1. Create an alias, such as `Monitoring_Servers` for monitoring servers by navigating to the **`Firewall -> Aliases`**.
2. Navigate to the interface where monitoring servers reside on the Firewall Rules.
3. Select `Pass` for the allow rule.
4. Select `Monitoring_Servers` as the source.
5. Select `ICMP` as protocol.
6. Select **any** as type.
7. Select **any** as the destination.
8. Select **any** as the destination port range.



Action	Pass
Disabled	□ Disable this rule
Quick	☑ Apply the action immediately on match.
Interface	LAN
Direction	in
TCP/IP Version	IPv4
Protocol	ICMP
ICMP type	any
Source / Invert	□
Source	Monitoring_Servers
Source	Advanced
Destination / Invert	□
Destination	any
Destination port range	from: any to: any
Log	☑ Log packets that are handled by this rule
Category	
Description	Allow Monitoring servers for ICMP access

Figure 40. *Allowing Monitoring servers for ICMP access*

8. Allowing WireGuard/OpenVPN VPN Server access from the Internet

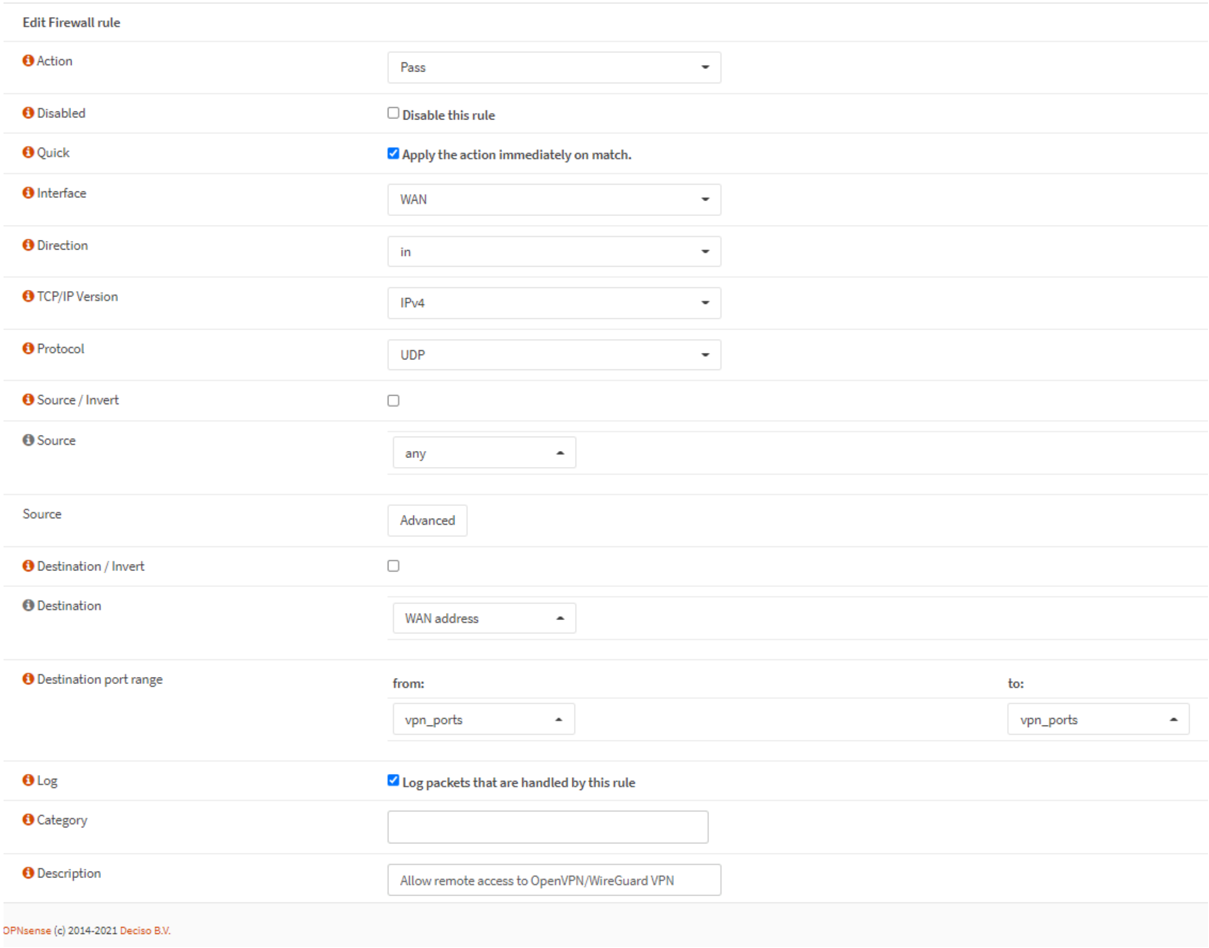
You may have a WireGuard or OpenVPN VPN server to access the internal home/company network remotely. However, your WireGuard and OpenVPN VPN server should be accessible from the Internet. To allow access to the WireGuard/OpenVPN VPN service, you should define a firewall rule and may define an alias for the VPN service port, such as vpn_port.

> 📣 **INFO**
>
> **`OpenVPN`** server listen port is **`1194 UDP`** by default.
>
> **`WireGuard VPN`** server listen port is **`51820 UDP`** by default.

Option	**Value**
Action	Pass
Interface	WAN
Protocol	UDP
Source	any
Source Port	any
Destination	WAN address
Destination Port	vpn_port
Description	Allow remote access to OpenVPN/WireGuard VPN

1. Create an alias, such as `vpn_port` for monitoring servers by navigating to the **`Firewall`** -> **`Aliases`**.
2. Navigate to the WAN interface on the Firewall Rules.
3. Select `Pass` for the allow rule.
4. Select `UDP` as the Protocol.
5. Select **any** as the source
6. Select **any** as the source port.
7. Select **any** as type.
8. Select `WAN address` as the destination.

9. Select `vpn_port` as the destination port range.

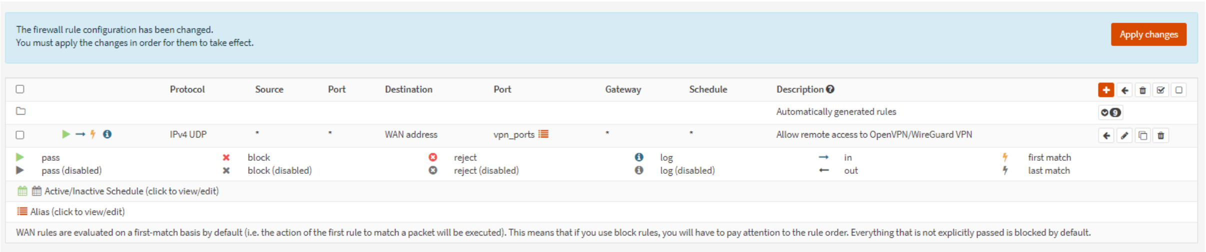


Edit Firewall rule

Action	Pass	
Disabled	□ Disable this rule	
Quick	☑ Apply the action immediately on match.	
Interface	WAN	
Direction	in	
TCP/IP Version	IPv4	
Protocol	UDP	
Source / Invert	□	
Source	any	
Source	Advanced	
Destination / Invert	□	
Destination	WAN address	
Destination port range	from: vpn_ports	to: vpn_ports
Log	☑ Log packets that are handled by this rule	
Category		
Description	Allow remote access to OpenVPN/WireGuard VPN	

OPNsense (c) 2014-2021 Deciso B.V.

Figure 41. *Defining firewall rule for VPN access*



The firewall rule configuration has been changed.
You must apply the changes in order for them to take effect.

□		Protocol	Source	Port	Destination	Port	Gateway	Schedule	Description
									Automatically generated rules
□	▶ → ϟ ℹ	IPv4 UDP	*	*	WAN address	vpn_ports	*	*	Allow remote access to OpenVPN/WireGuard VPN

▶ pass ✖ block ⊗ reject ℹ log → in ϟ first match
▶ pass (disabled) ✖ block (disabled) ⊗ reject (disabled) ℹ log (disabled) ← out ϟ last match

Active/Inactive Schedule (click to view/edit)

Alias (click to view/edit)

WAN rules are evaluated on a first-match basis by default (i.e. the action of the first rule to match a packet will be executed). This means that if you use block rules, you will have to pay attention to the rule order. Everything that is not explicitly passed is blocked by default.

Figure 42. *OpenVPN and WireGuard VPN server access rule*

9. Allowing a Web Server access from the Internet

You may have a web server publicly available from the Internet on your home/company network. To allow access to the web service, you should first define NAT port forwarding rules by navigating to **`Firewall > NAT > Port Forward`** page, and then define a packet filtering firewall rule.

Option	**Value**
Action	Pass
Interface	WAN
Protocol	TCP
Source	any
Source Port	any
Destination	WAN address
Destination Port	HTTPS
Redirect target IP	172.16.10.10
Redirect target port	HTTPS
Description	Allow Internet access to the web server
Filter rule association	Add associated filter rule (or Pass)

1. Navigate to the WAN interface on the Firewall Rules.
2. Select `Pass` for the allow rule.
3. Select `TCP` as the Protocol.
4. Select **any** as the source
5. Select **any** as the source port.
6. Select `WAN address` as the destination.
7. Enter Redirect target IP
8. Enter Redirect target port

About Us

To better meet the network security demands of today's perimeter-less, hyper-distributed enterprise, Zenarmor has changed how network security is delivered and managed.

With its industry-first technology, Zenarmor® provides agile and scalable secure access service wherever there is network connectivity: at core, edge and across all access levels; for your home, enterprise or carrier class networks. Zenarmor can be deployed both in the cloud or on premise, providing a high level of flexibility to meet the unique security needs of today's hyper-distributed and perimeter-less enterprises.

With its powerful and nimble technology, Zenarmor is the only platform that can seamlessly integrate and scale with an operator's network infrastructure, as well as being able to be deployed standalone to reliably deliver the enterprise-grade level of network security necessary to protect today's omnipresent business and users.

Sunny Valley Cyber Security Inc., the company that innovates instant network security and created Zenarmor, is backed by Arché Gruppe.

zenarmor

10080 N. Wolfe Rd. Ste SW3-200
Cupertino, CA 95014

T: +1 (650) 288 4488

E: hi@zenarmor.com