PF SENSE

pfSense is a feature-rich and highly customizable firewall and router solution that provides a comprehensive set of network security features to organizations. It is an open source software that is available for free, making it an ideal solution for businesses that want to save on costs while ensuring their network is secure.

One of the key strengths of pfSense is its unified threat management (UTM) feature, which provides advanced security capabilities such as intrusion prevention, malware protection, and content filtering. The UTM feature uses a combination of technologies like stateful packet inspection, deep packet inspection, and application-level gateway to protect the network from various threats.

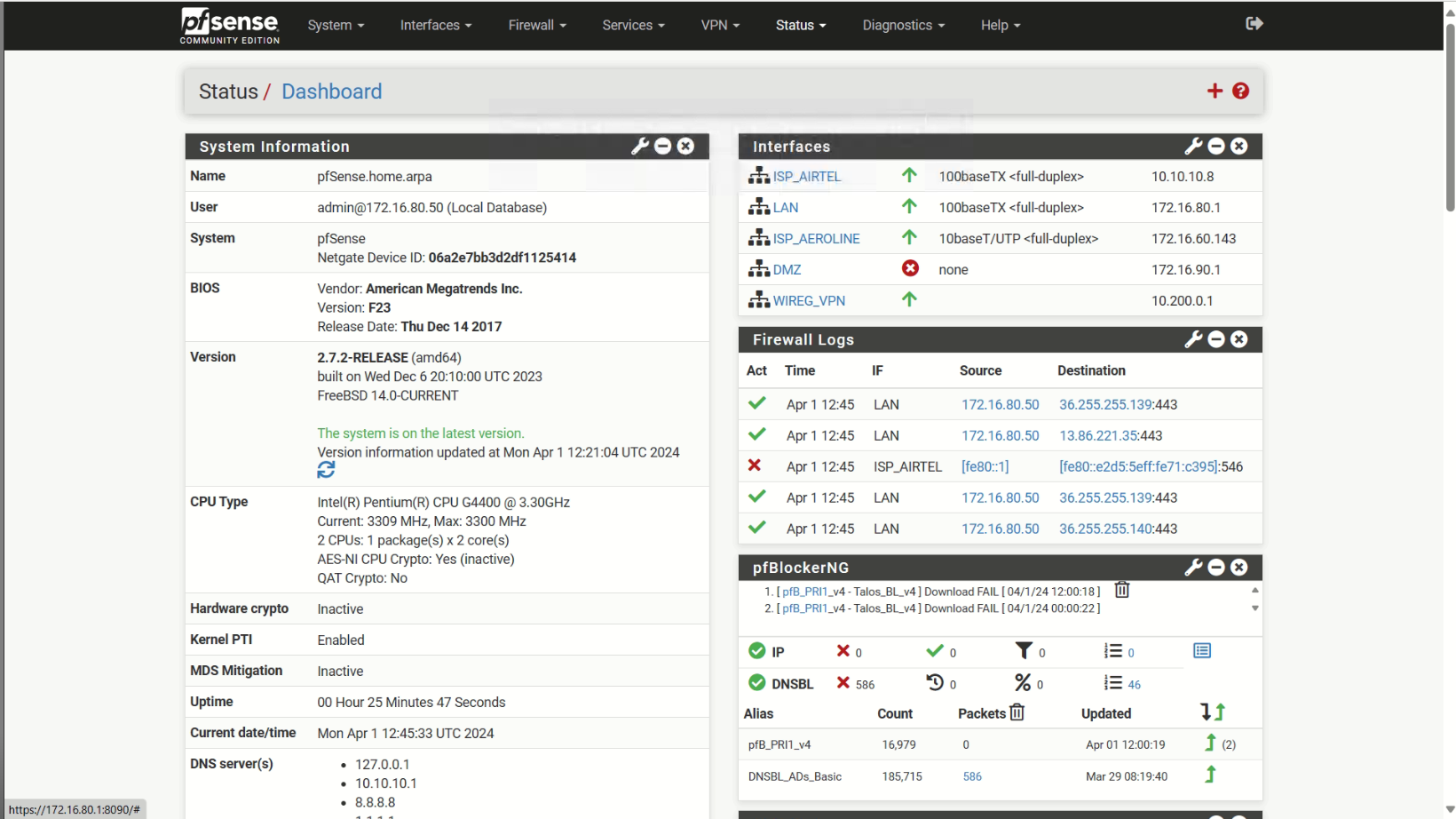
In addition to UTM, pfSense also includes load balancing and multi-WAN support, making it a versatile solution for organizations with multiple internet connections. This feature ensures that the network always has a backup internet connection, ensuring uninterrupted connectivity.

The open-source pfSense Community Edition is widely used and can turn any computer or virtual machine into a dedicated firewall/router for a network. The Community Edition is easy to install and configure, making it an ideal solution for small businesses or home networks.

There is also a pfSense Plus version that provides additional features and is tailored for enterprise and large business solutions. The pfSense Plus version includes features such as high availability, 24/7 support, and advanced reporting and monitoring.

Netgate, the company behind pfSense, is committed to providing comprehensive support, training, and professional services to help organizations implement effective network security solutions. Netgate offers various support plans that provide customers with access to technical support and software updates.

With pfSense, businesses can have peace of mind knowing that their network is protected by a reliable and powerful security solution that is backed by a company committed to customer satisfaction.



**HOW SETUP PFSENSE FIREWALL ON BARE METAL**

1. Prepare the Installation Media:

- Download the pfSense image suitable for your hardware architecture (usually AMD64).

- Create a bootable USB drive with the pfSense image using a tool like Rufus or Etcher.

2. Boot from the Installation Media:

- Insert the bootable USB drive into your dedicated hardware.

- Power on the system and configure it to boot from the USB drive.

3. Start the Installation:

- The pfSense installer will automatically launch.

- Follow the on-screen prompts to begin the installation process.

4. Select Language and Keyboard Layout:

- Choose your preferred installation language and keyboard layout.

- For most users with a standard PC keyboard, press Enter to select the default keymap.

5. Partition and Filesystem Selection:

- The installer will prompt you to select the filesystem for the firewall's target disk.

- You have a few options to choose from, including Auto (ZFS), Auto (UFS) BIOS, Auto (UFS) UEFI, or Manual.

6. Follow the Installation Steps:

- Depending on your choice, the installer will guide you through partitioning, formatting, and other settings.

- Specify the disk or partition where you want to install pfSense.

7. Complete the Installation:

- Once the installation is complete, the system will prompt you to reboot.

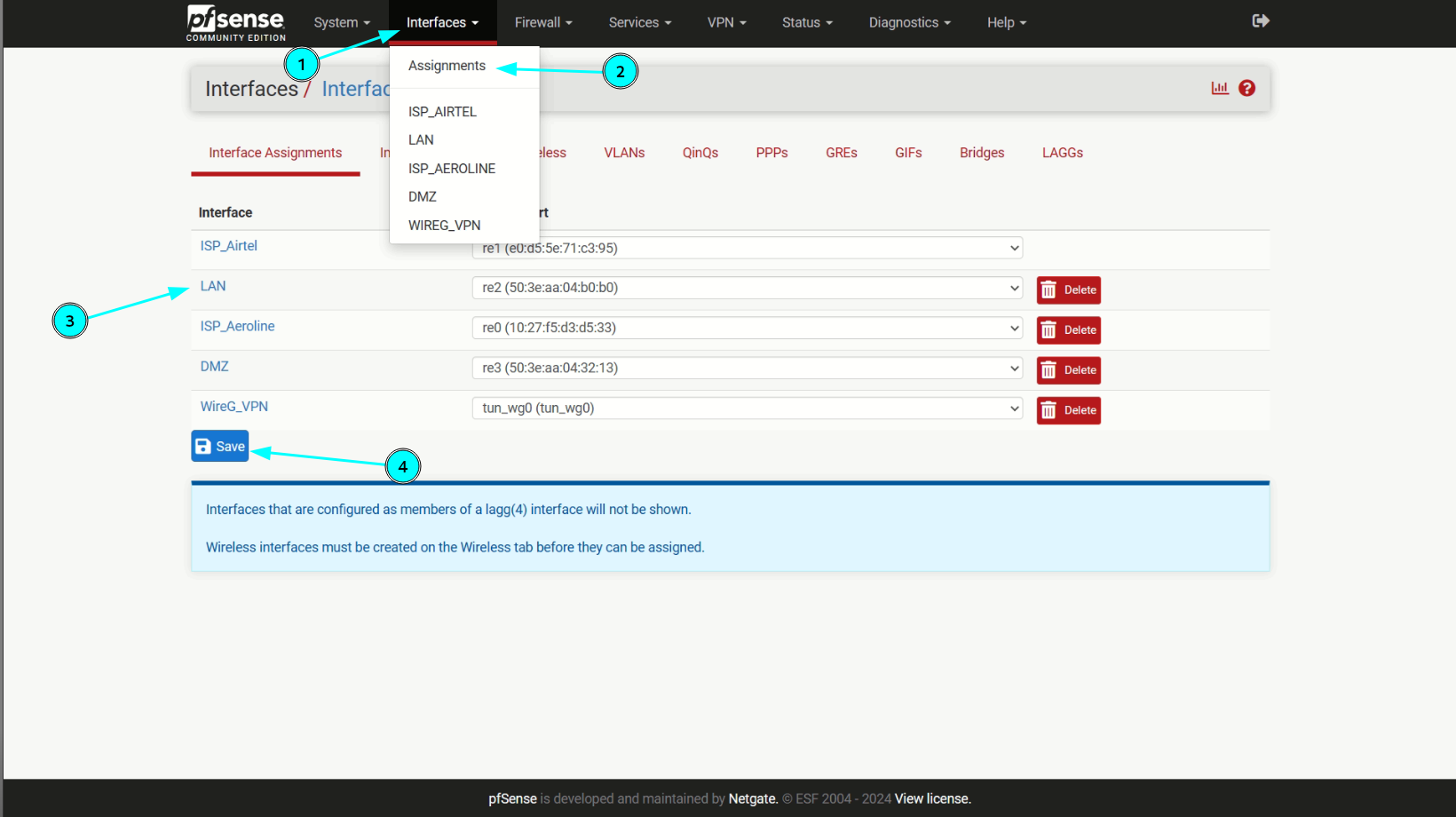
- Remove the installation media (USB drive) and let the system boot from the newly installed pfSense.

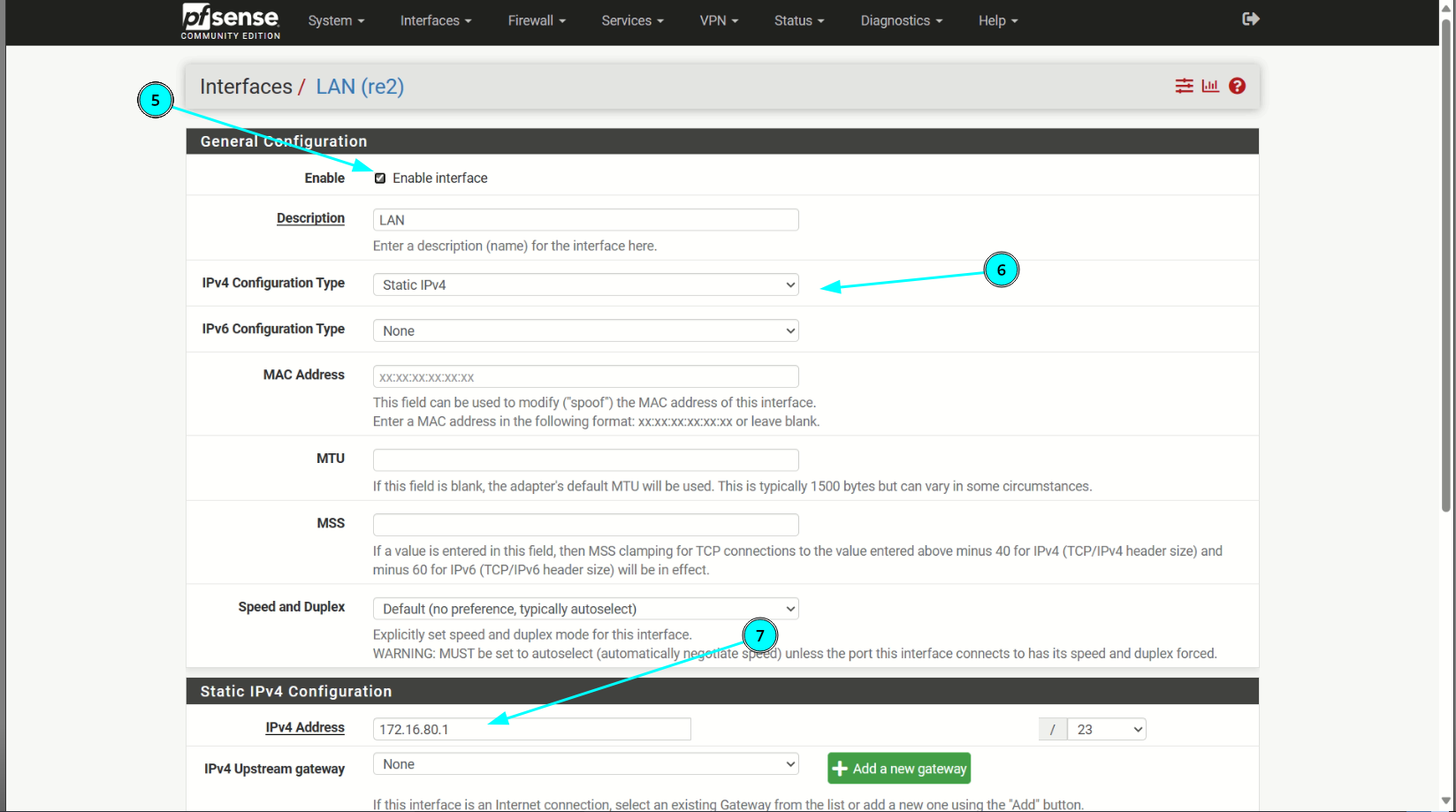
8. Initial Configuration:

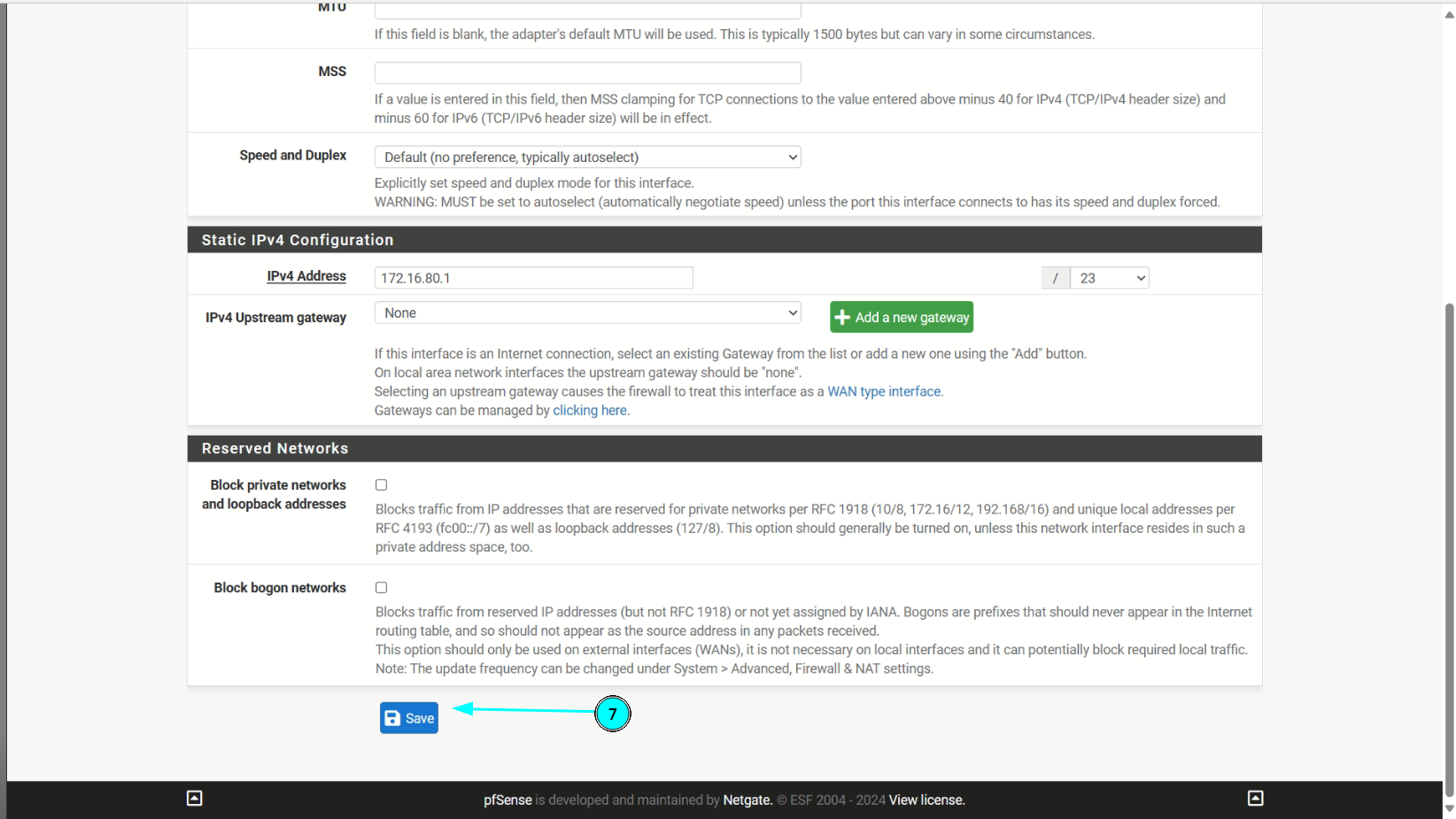
- After rebooting, access the pfSense web interface using the assigned IP address.

CONFIGURE LAN

1. **Access the pfSense Web Interface**:
2. Connect a client computer to the same network as the **LAN interface** of the pfSense firewall.
3. By default, the LAN IP address of a new pfSense installation is **192.168.1.1** with a **/24 mask** (255.255.255.0).
4. Open a web browser (such as Firefox, Safari, or Chrome) and navigate to [https://192.168.1.1](https://192.168.1.1/).
5. Log in using the default credentials:
   1. **Username**: admin
   2. **Password**: pfsense
6. **Change the LAN IP Address**:
7. We’ll change it to **172.16.80.1**:
   1. Access the pfSense console (VGA, serial, or SSH from another interface).
   2. Choose option **2** from the console menu.
   3. Enter the new LAN IP address (**172.16.80.1**), subnet mask (usually **/24**), and specify whether to enable DHCP.
   4. If DHCP is enabled, set the starting and ending address of the DHCP pool within the given subnet.
8. **Update Client Computers**:
9. If the DHCP server on the firewall is disabled, configure client computers on the LAN with static IP addresses:
   1. Set a statically configured IP address on client computers, such as **172.16.80.5**, with a subnet mask matching the one given to the firewall (e.g., **255.255.255.0**).







CONFIGURE MULTI WAN

**Set Up the Primary WAN Interface:**

If you haven’t already, configure the primary WAN interface (usually WAN):

Use the Setup Wizard to set up the initial WAN interface with the static IP address provided by your ISP. (I Used Airtel DHCP)

Ensure that the primary WAN interface is working correctly.

**Add the Additional WAN Interfaces:**

1-Navigate to Interfaces > Assignments.

2-If the additional WAN interfaces do not exist, click Add to create them.

3-Assign the interfaces (e.g., OPT1 for the second WAN).

4-Configure the Additional WAN Interfaces:

5-Visit the Interfaces menu entry for each additional WAN (e.g., Interfaces > OPT1).

6-Enable the interface.

7-Enter a suitable name, such as WAN2 (ISP Aeroline).

8-Assign IP Addresses:

**For the static IP address WAN interface:**

Configure the static IP address, subnet mask, gateway, and DNS servers.

For the dynamic IP address WAN interface:

Set the interface to DHCP mode.

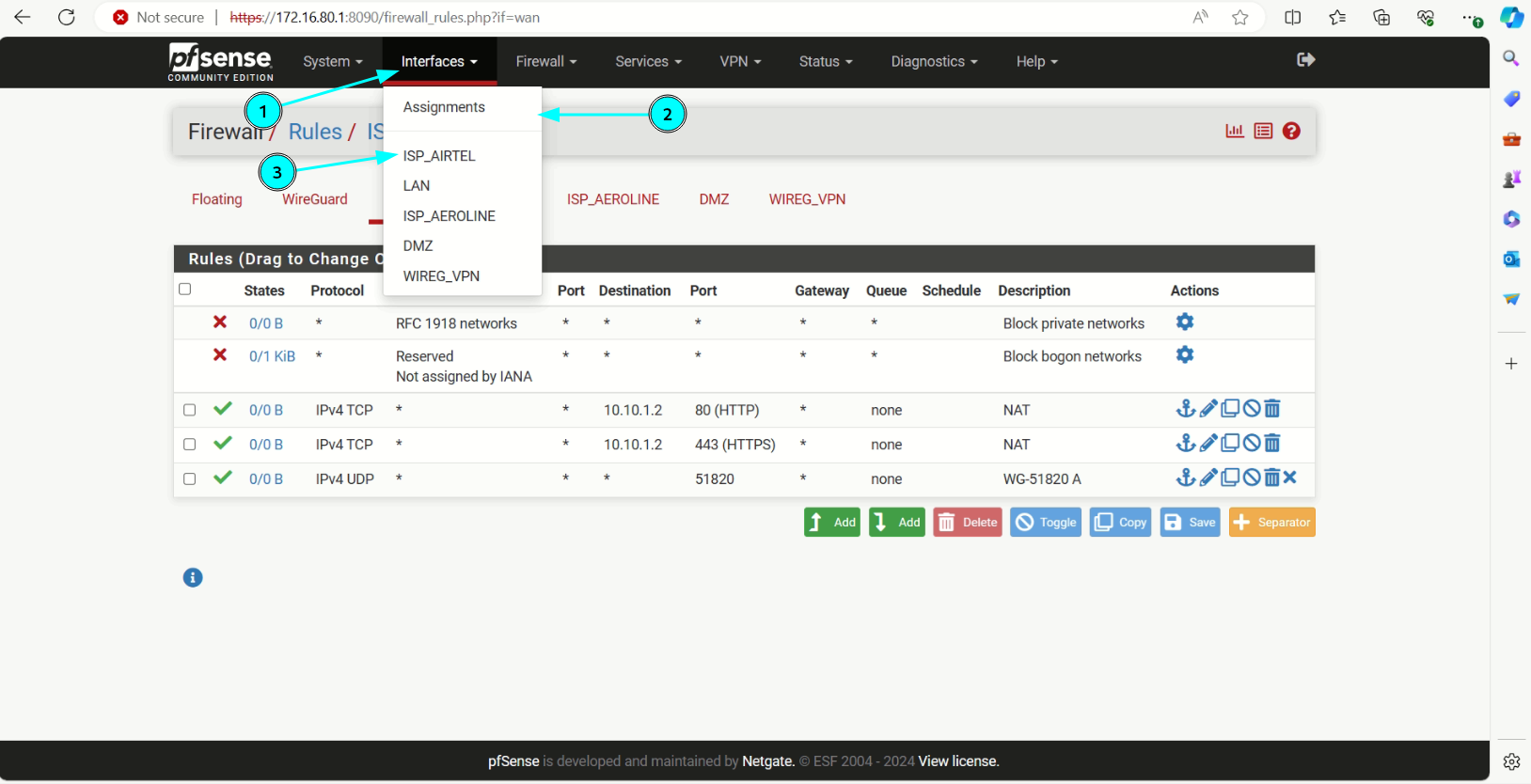
The ISP will assign an IP address dynamically.

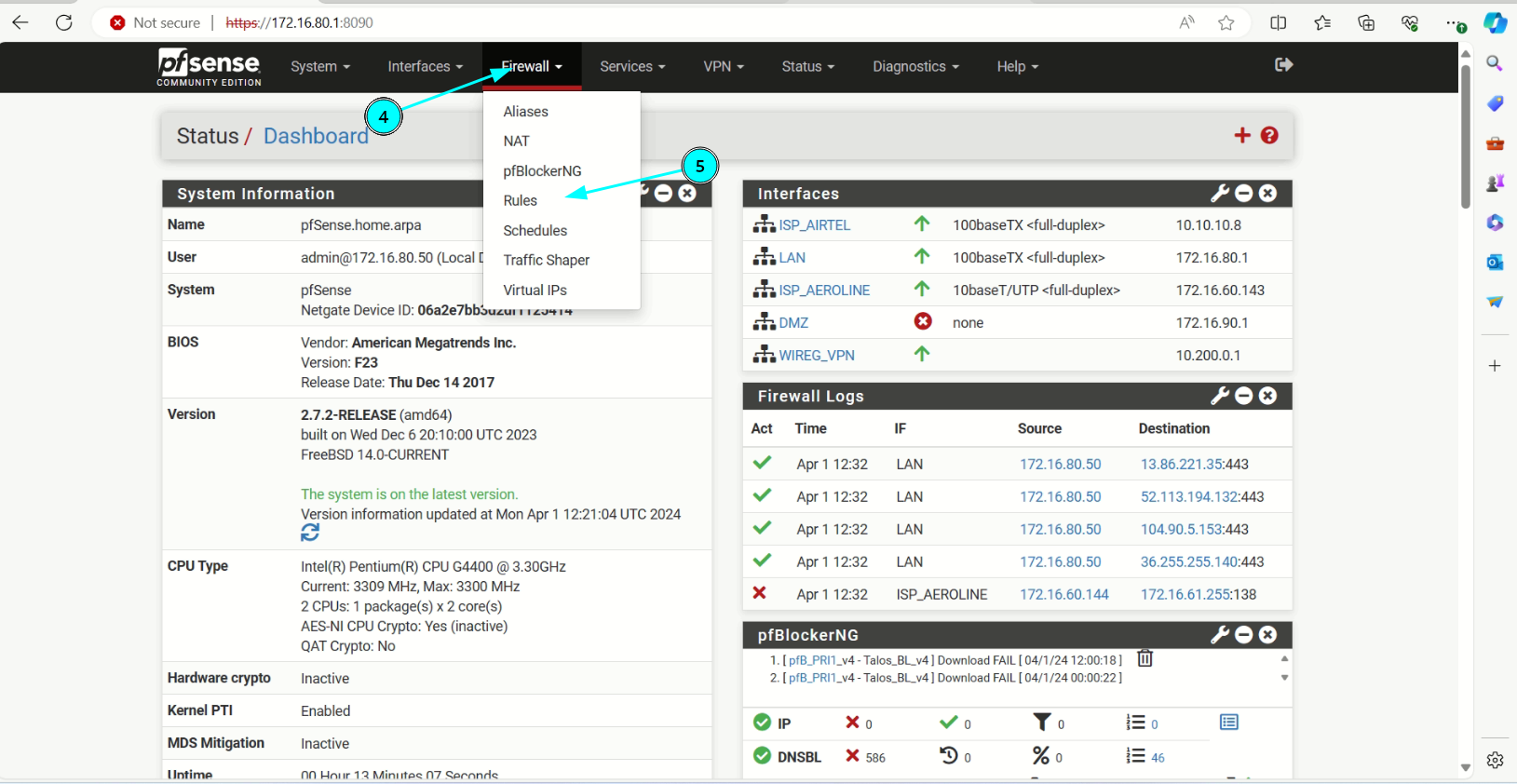
Configure Firewall Rules:

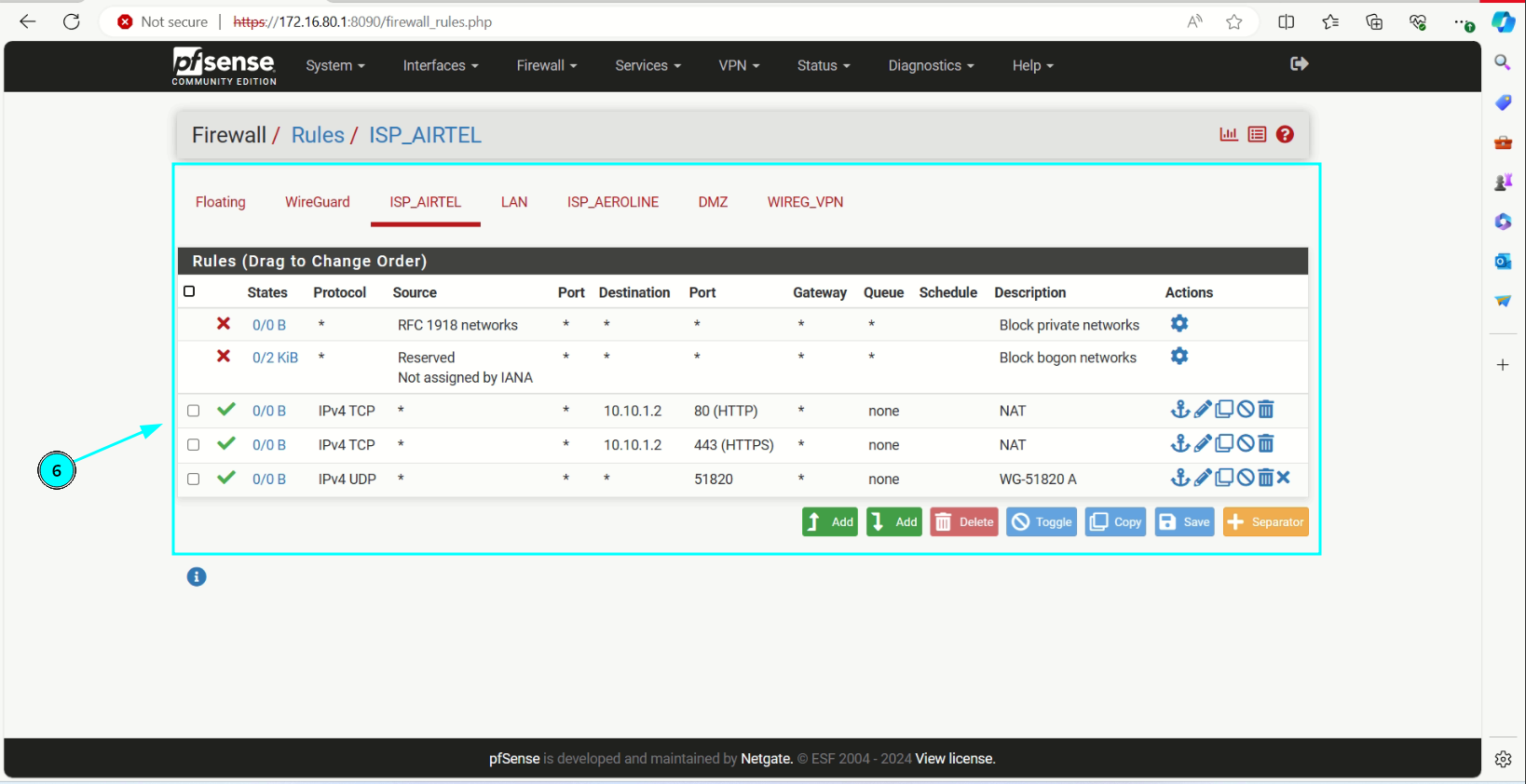
Create appropriate firewall rules for each WAN interface.

For the static IP address WAN, allow necessary traffic (e.g., HTTP, HTTPS, DNS).

For the dynamic IP address WAN, allow outbound traffic.

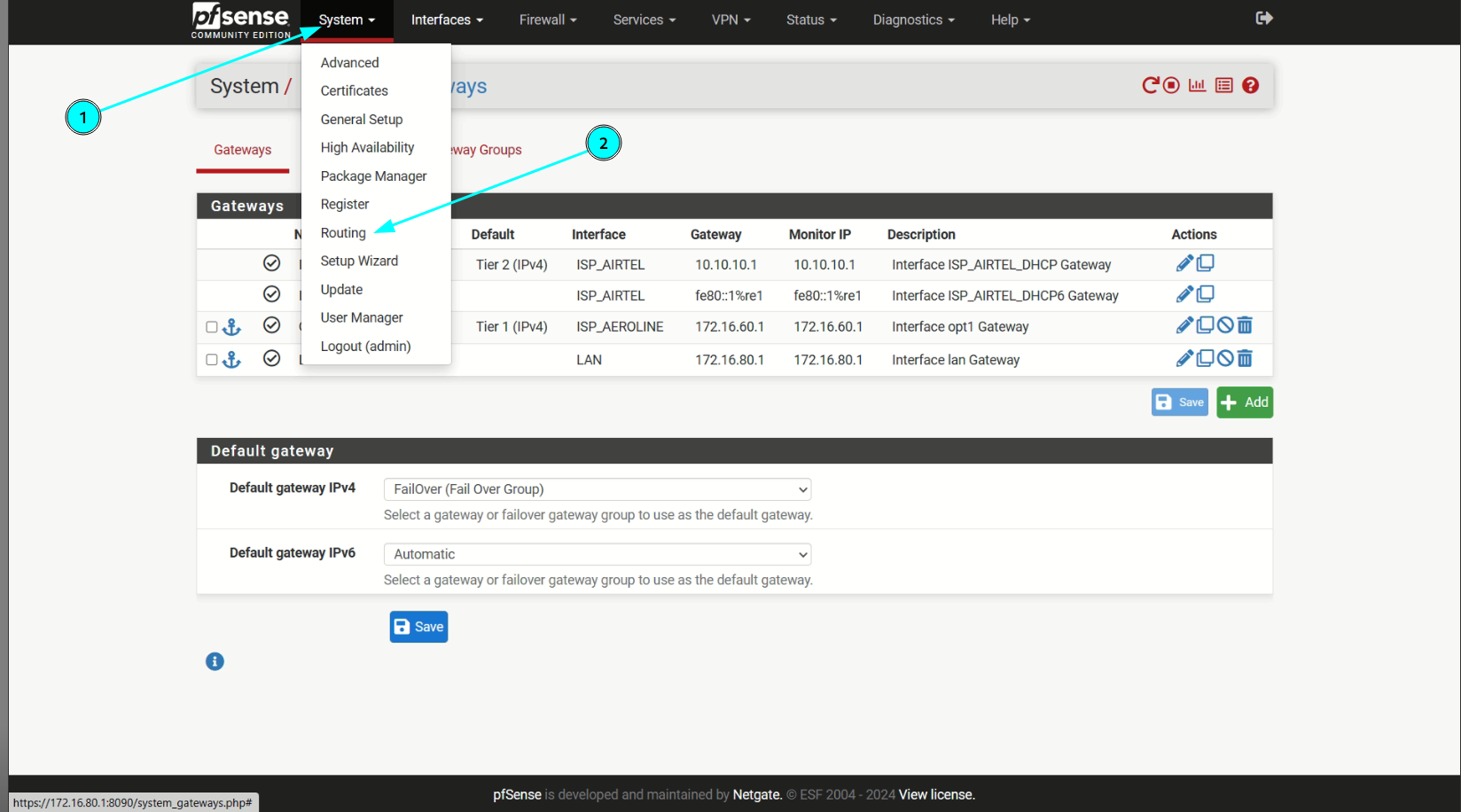


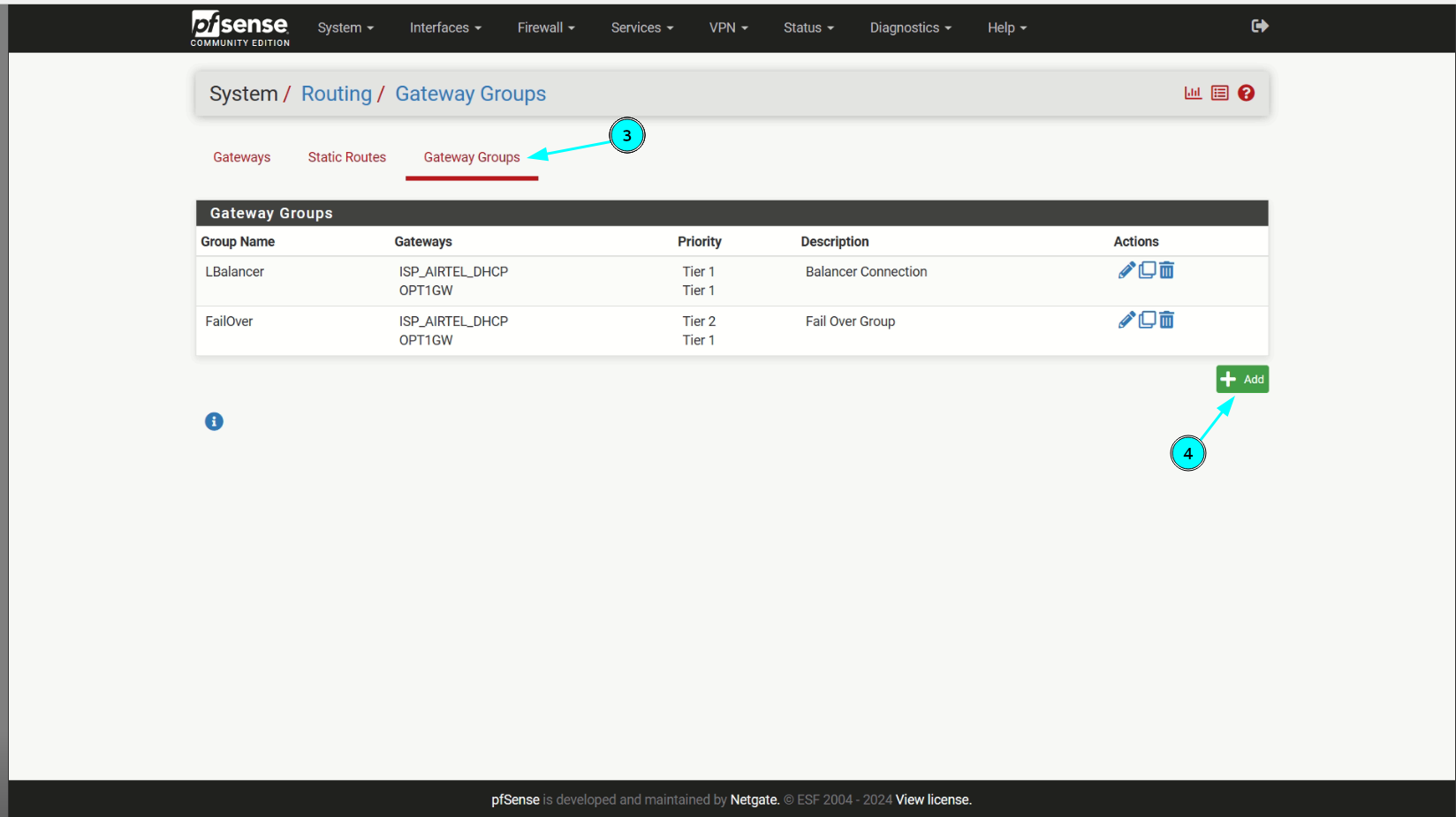


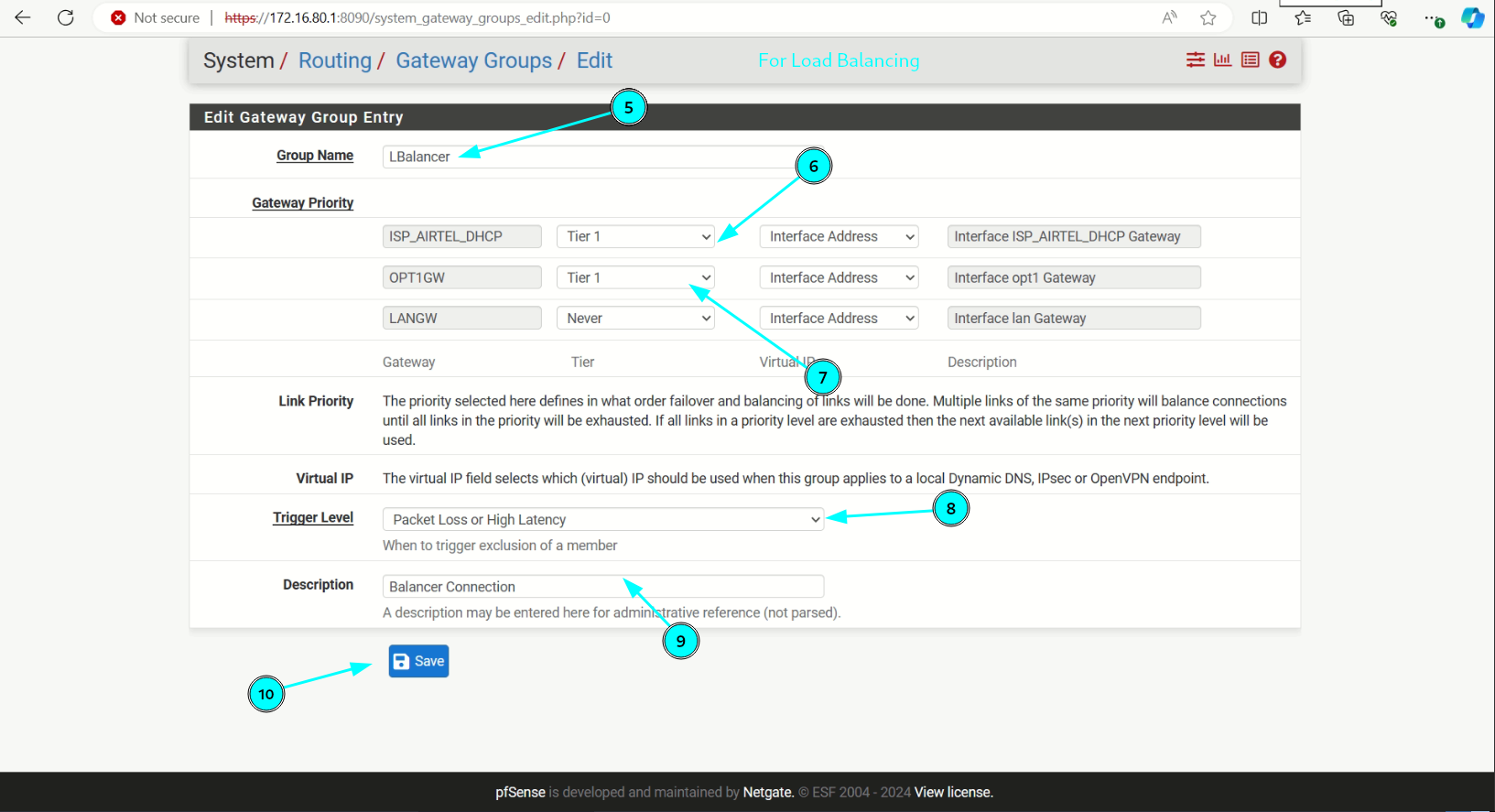


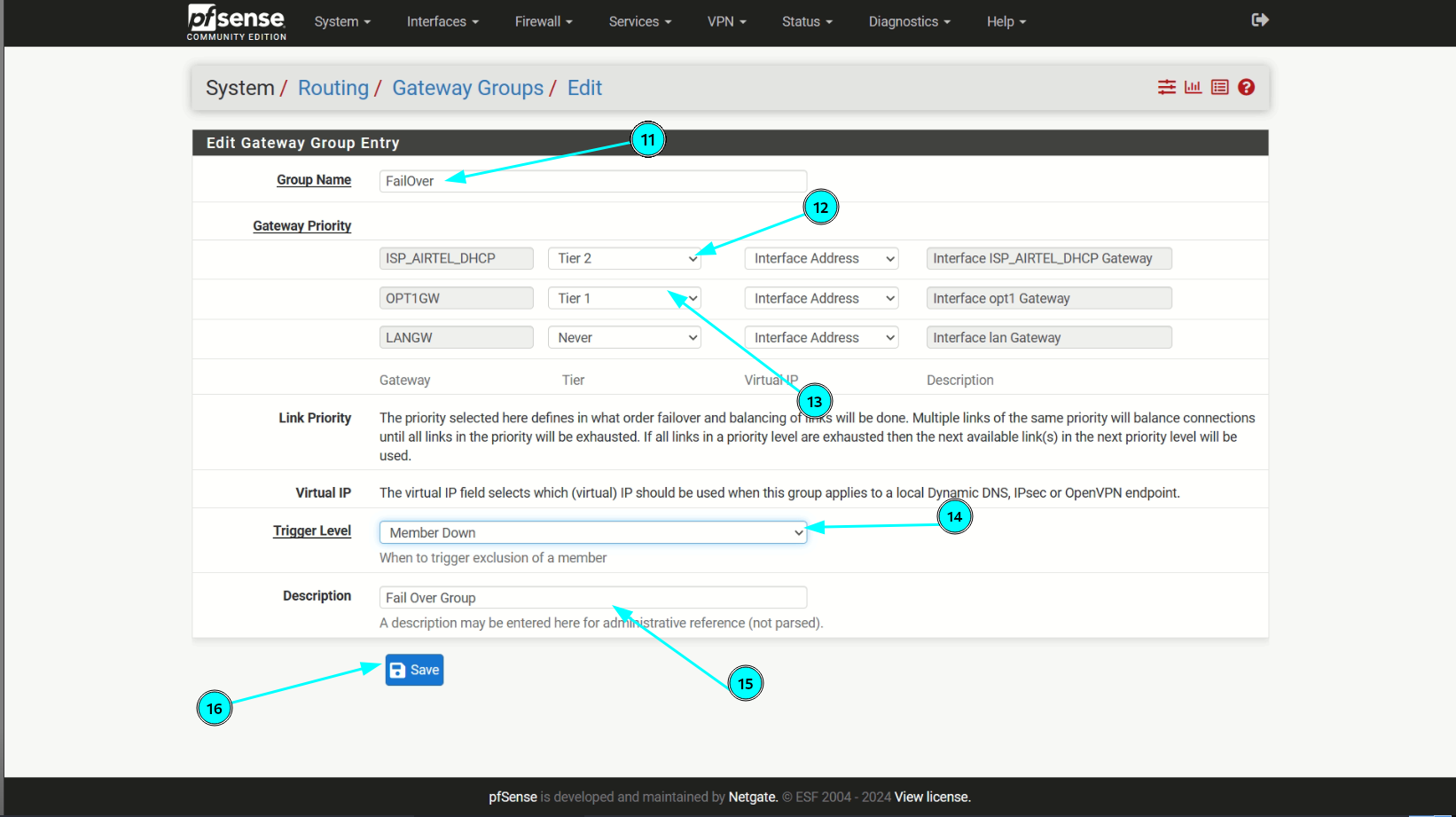
FAILOVER AND LOAD BALANCING

1. **Navigate to System > Routing > Gateway Groups**:  
   1. Click **Add** to create a new gateway group.
   2. Fill in the options on the page as described in the **Gateway Group Options**.
   3. Save your settings.
2. **Load Balancing**:  
   1. Any two gateways on the same tier are load-balanced.
   2. For example, if you have **Gateway A**, **Gateway B**, and **Gateway C** all on **Tier 1**, connections will be balanced between them.
   3. Gateways that are load balanced will automatically failover between each other. If one gateway fails, it is removed from the group, and the firewall load balances between the remaining online gateways.
3. **Weighted Balancing**:  
   1. If you need to balance WANs in a weighted fashion due to differing bandwidth, adjust the **Weight** parameter on the gateway.
4. **Failover**:  
   1. The firewall prefers gateways on a lower-numbered tier.
   2. For example:
      1. **Gateway A** (Tier 1)
      2. **Gateway B** (Tier 2)
   3. The firewall uses **Gateway A** first. If it goes down, it switches to **Gateway B**. If both **Gateway A** and **Gateway B** are down, it uses **Gateway C**.



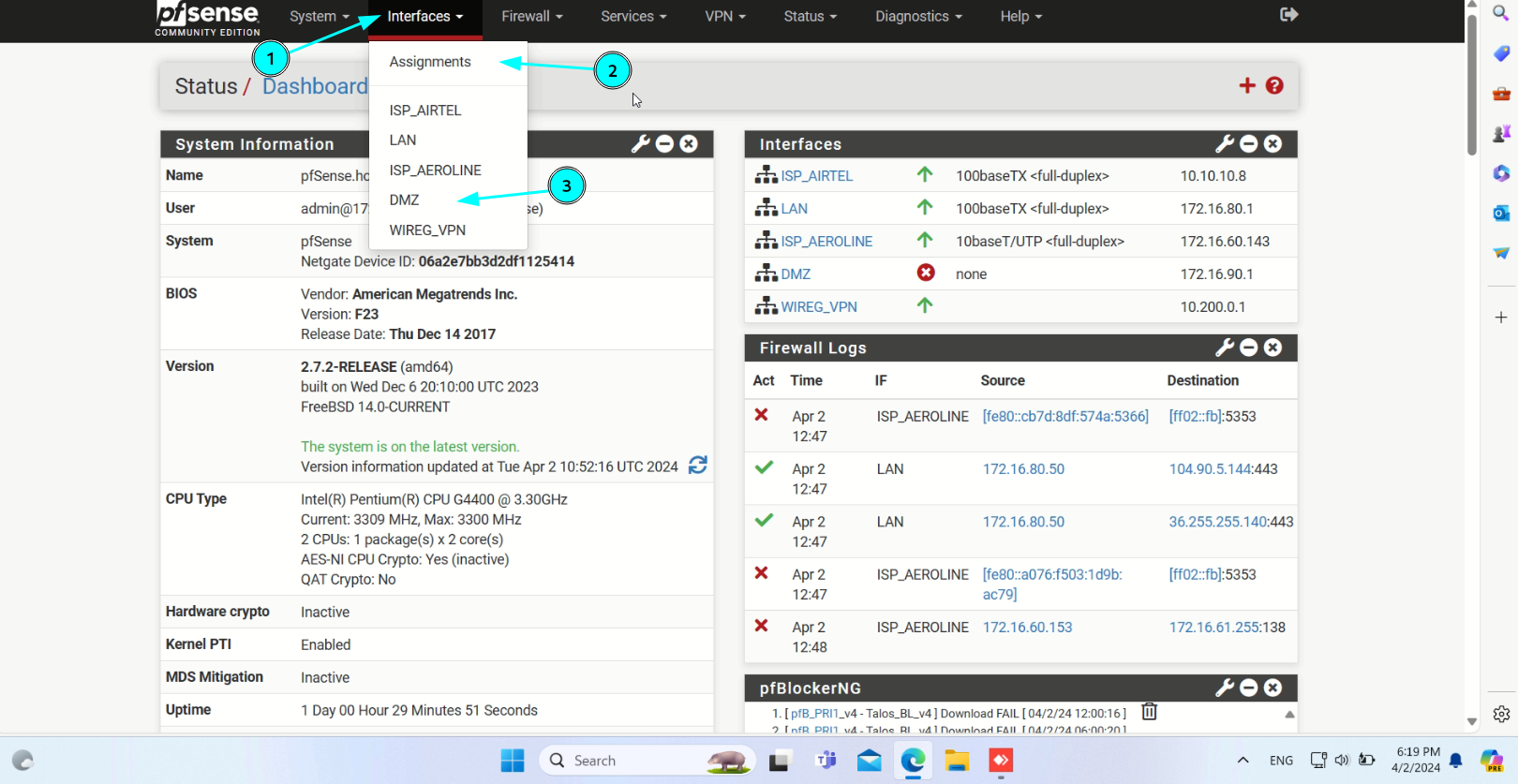


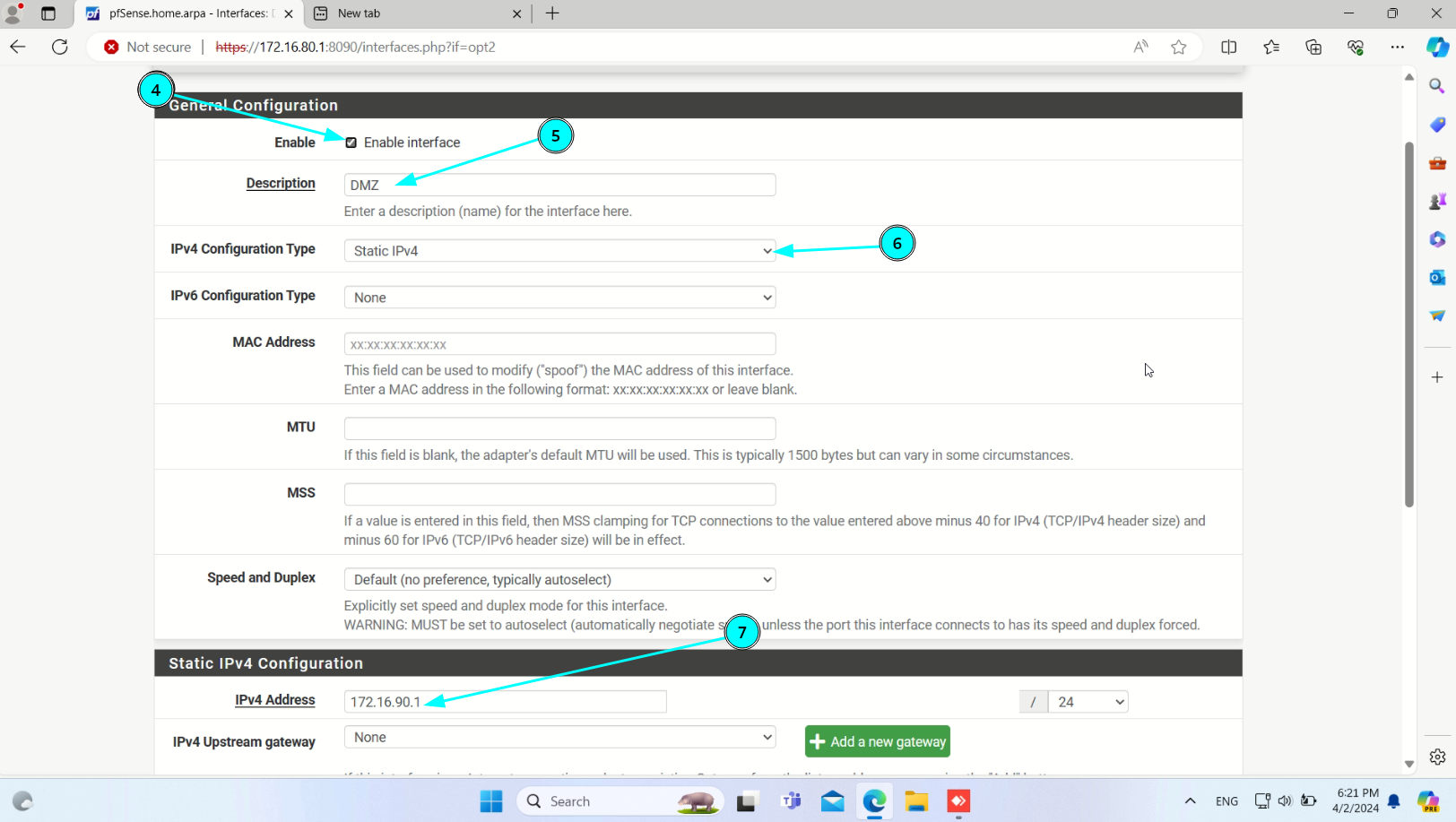


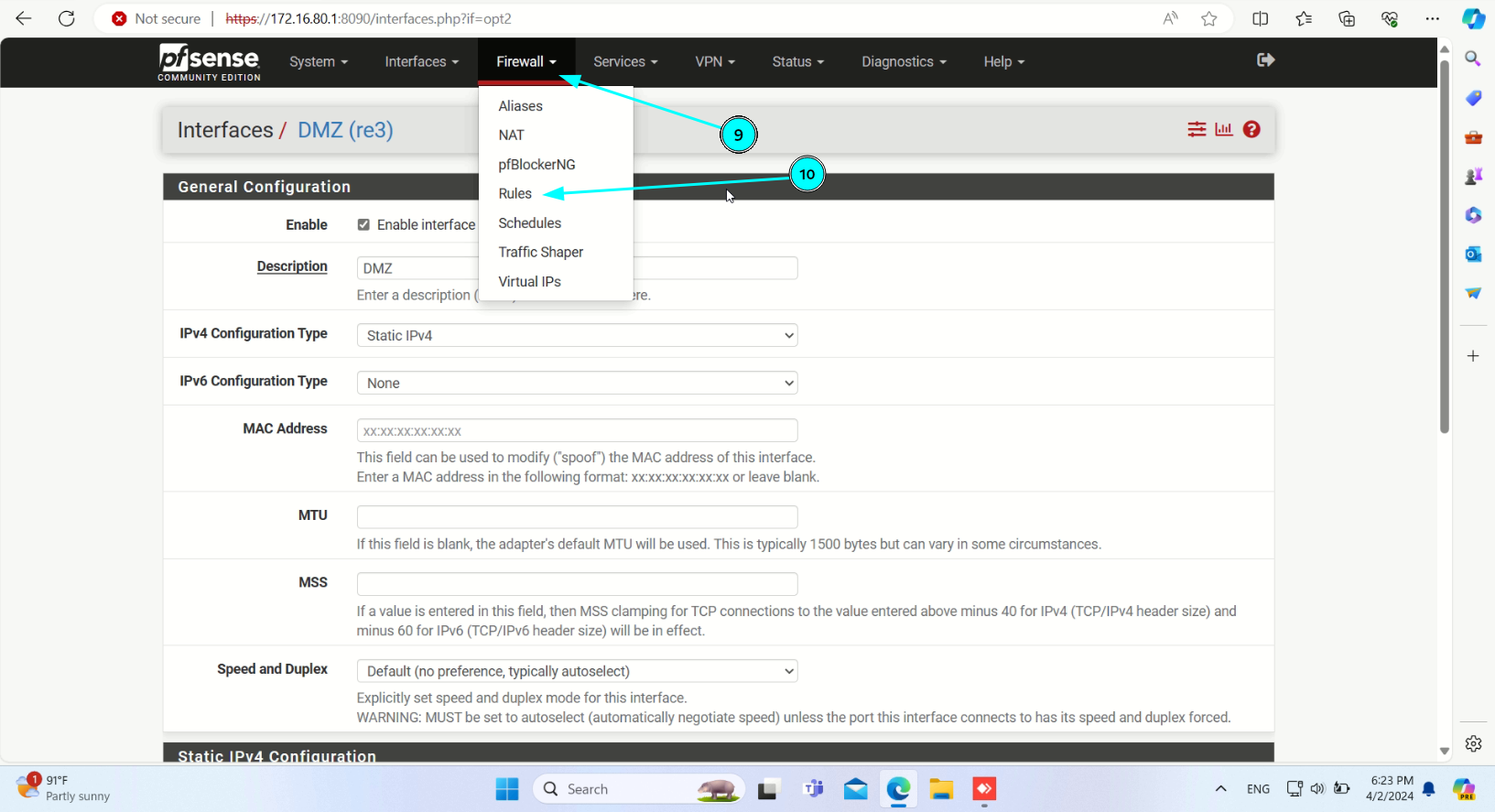
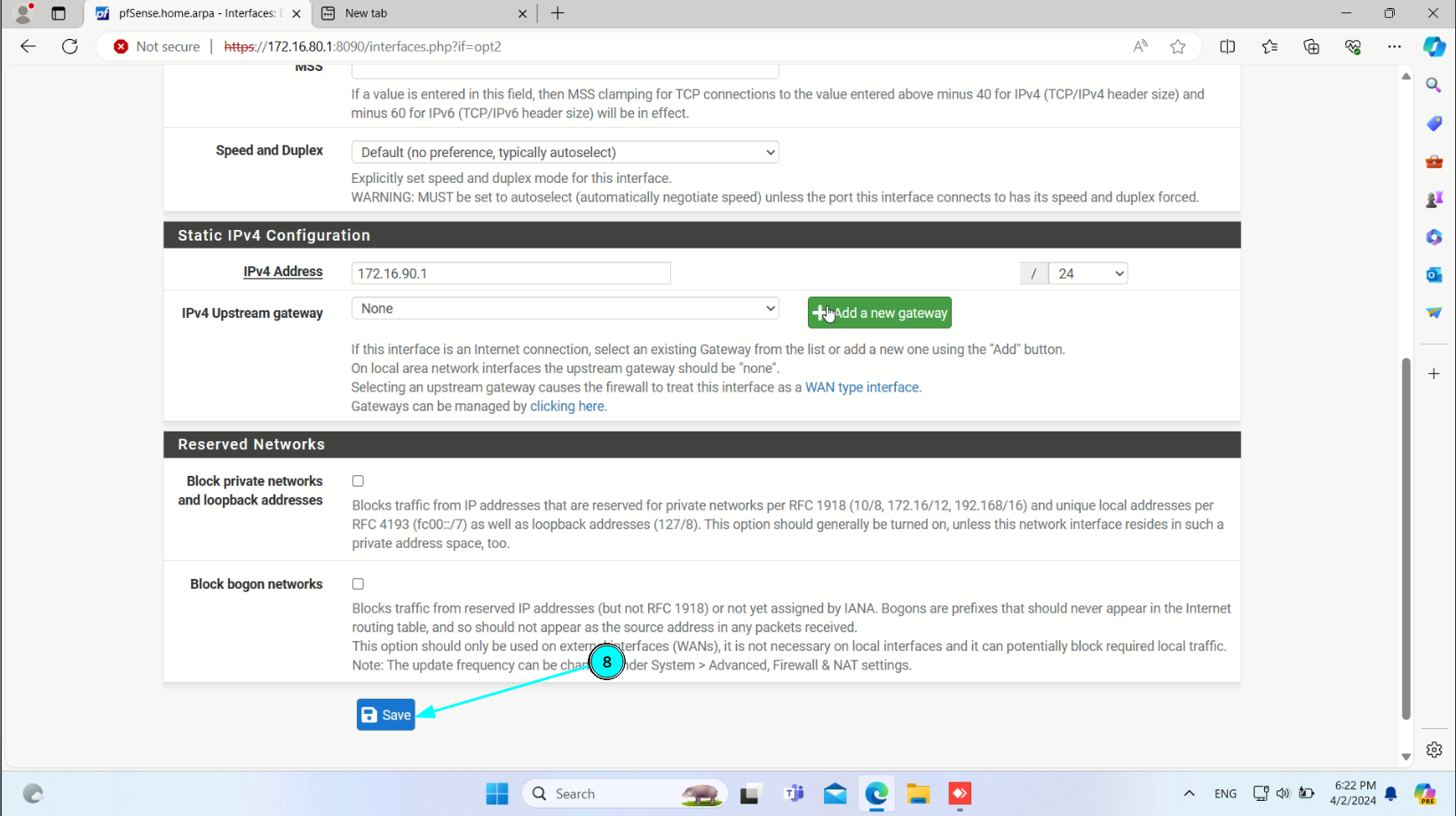


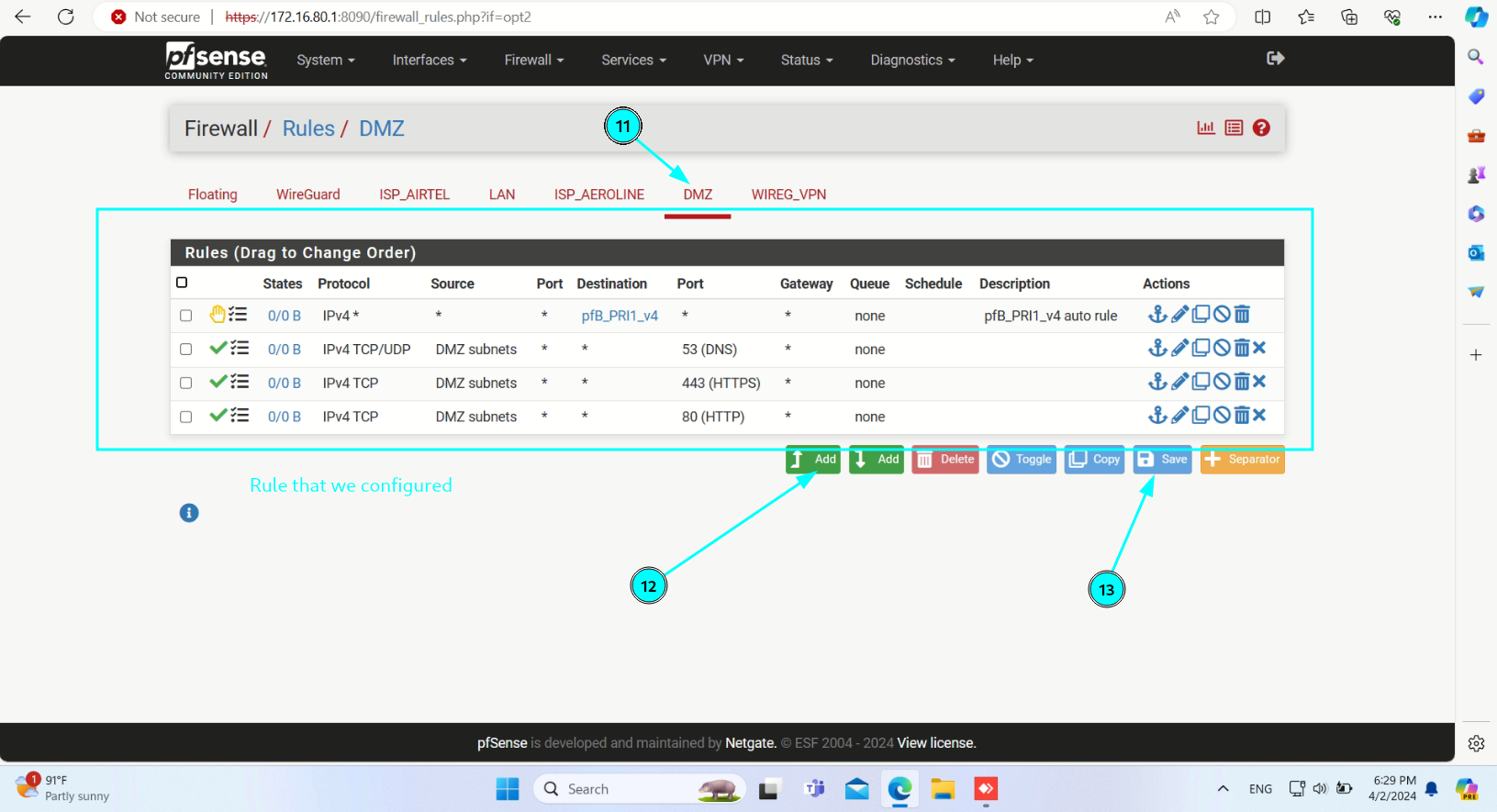
DMZ

A DMZ, or Demilitarized Zone, is a specialized network segment designed to provide an additional layer of security for public-facing servers, such as web servers, mail servers, and FTP servers. By placing these servers in the DMZ, you can segregate them from your internal network, reducing the risk of unauthorized access to sensitive data. The DMZ is different from the LAN network, which is primarily used for handling outbound traffic initiated by users. The DMZ, on the other hand, is designed to deal with inbound traffic from external sources. For example, you can open specific ports, such as HTTP/HTTPS, to allow internet users to access your web server within the DMZ. By deploying your public-facing servers in the DMZ, you can provide a secure and controlled environment for hosting your online services. This can help protect your organization from common security threats such as denial-of-service attacks, malware, and other forms of cybercrime.









**pfBlocker-NG**

pfBlocker-NG is a powerful package that can enhance the capabilities of pfSense, an open-source firewall and router platform. It provides IP/DNS-based filtering and was created by BBCan177. Let’s take a closer look at its features.

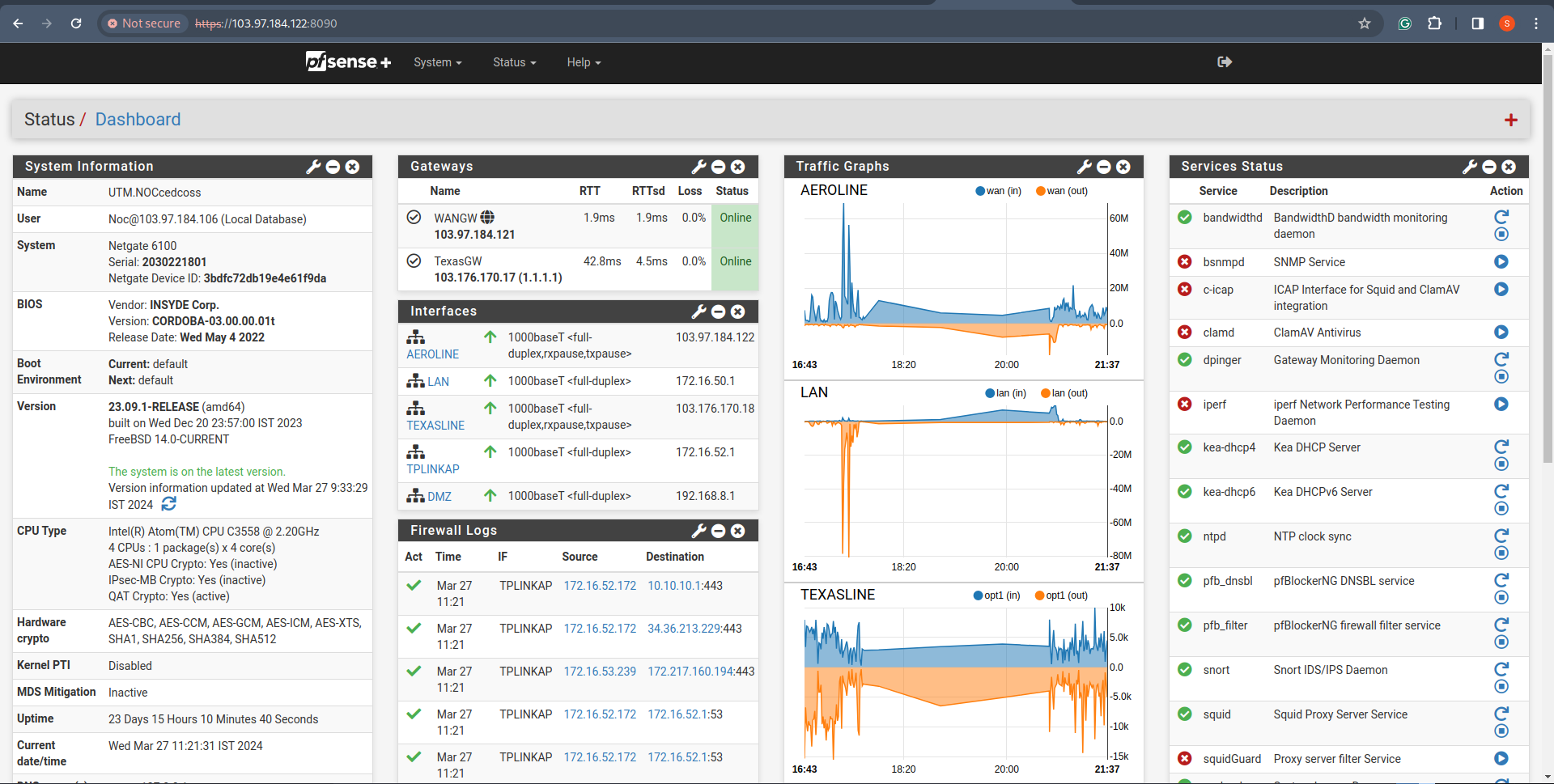
Functionality: IP/DNS-Based Filtering:   
pfBlocker-NG can filter network traffic based on IP addresses and domain names. Geographical/Country Blocking: You can block traffic from specific

countries or IP address ranges. Enhanced Alias Table:   
It lets you consolidate multiple IP address or URL lists into a single alias. Dashboard Widget: Provides a convenient widget for monitoring and managing

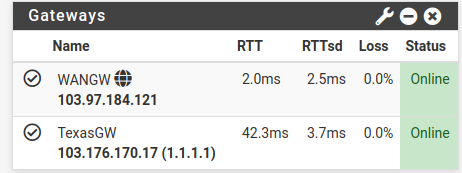
blocked IPs and domains. XMLRPC Sync:  
 Allows you to synchronize pfBlocker configuration across multiple pfSense devices. Features: Frequently Updated Lists: pfBlocker-NG supports various block lists, including Spamhaus DROP and EDROP, DShield Most Active Attacking IPs, and iblocklist.com lists. Customizable Blocking Rules: You can choose different actions for each list (deny both, deny inbound, deny outbound, permit inbound, permit outbound, or alias only).

Network Lists:   
Configure what to block and how to block using network lists. Memory Optimization: Adjust table size to avoid memory errors. Integration with Firewall Rules: pfBlocker requires at least one firewall entry (any interface) to be active. Check the front page widget for verification. Floating Rules: Use aliases for customized filter entries and floating rules.

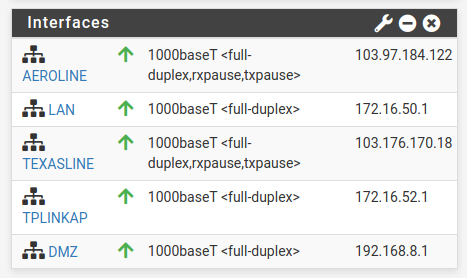
FIREWALL SERVICES AND STATUS



Gateways (Number of ISPs available)



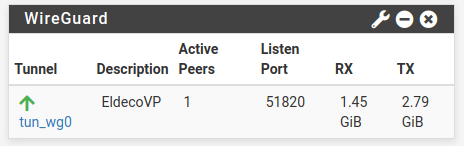
Number of Output or Interfaces



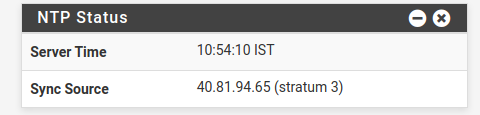
Firewall Logs



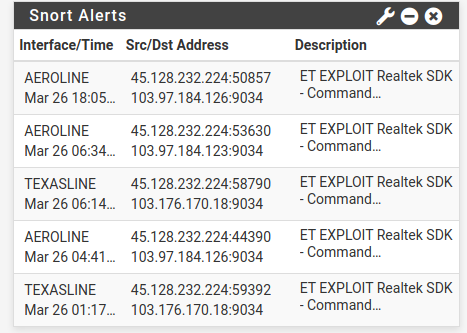
VPN Services



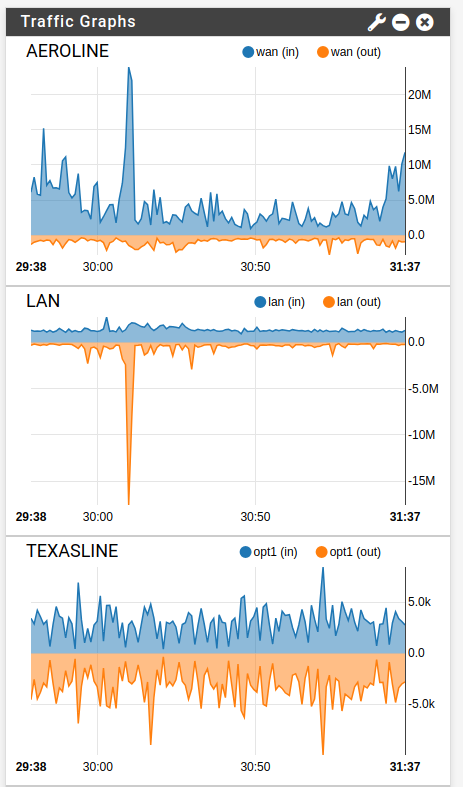
NTP Status

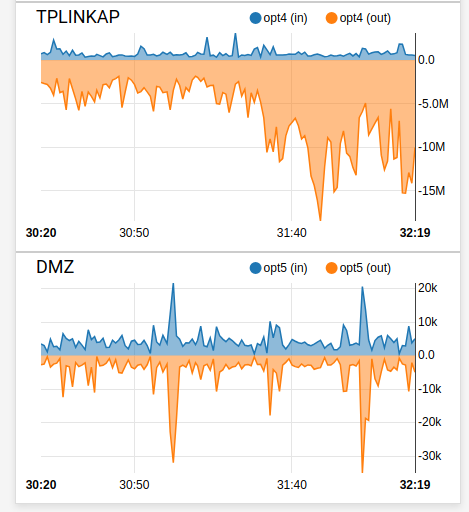


SNORT Logs

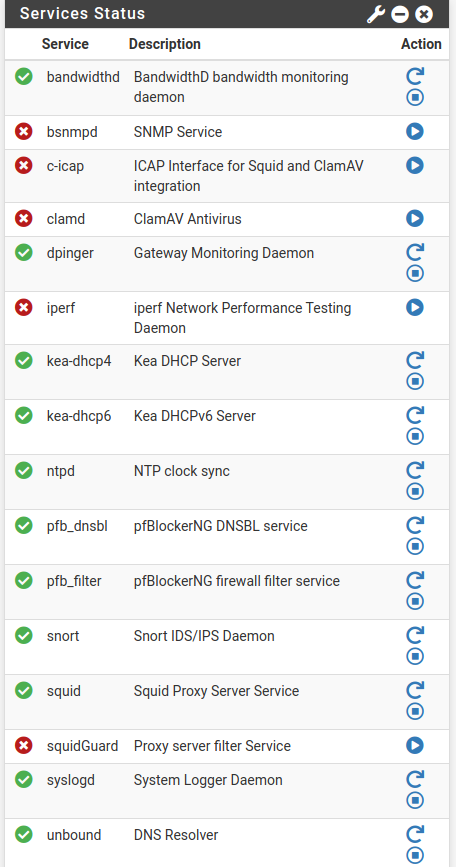


Traffic Graph of INPUT and OUTPUT

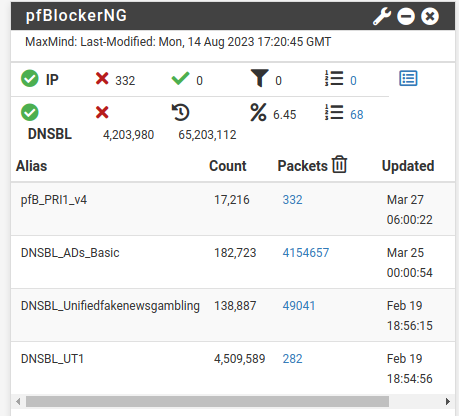




Number Of Services that are Enable or Disable



PFBlockerNG



It enhances security by blocking access to known malicious websites and preventing users on a network from inadvertently visiting them. It offers various features such as custom blocklists, whitelisting, logging, and extensive configuration options to tailor its behaviour to specific needs. PFBlockerNG is a powerful tool for network administrators looking to enhance security and control over their network traffic.