PF SENSE

pfSense is a feature-rich and highly customisable 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.

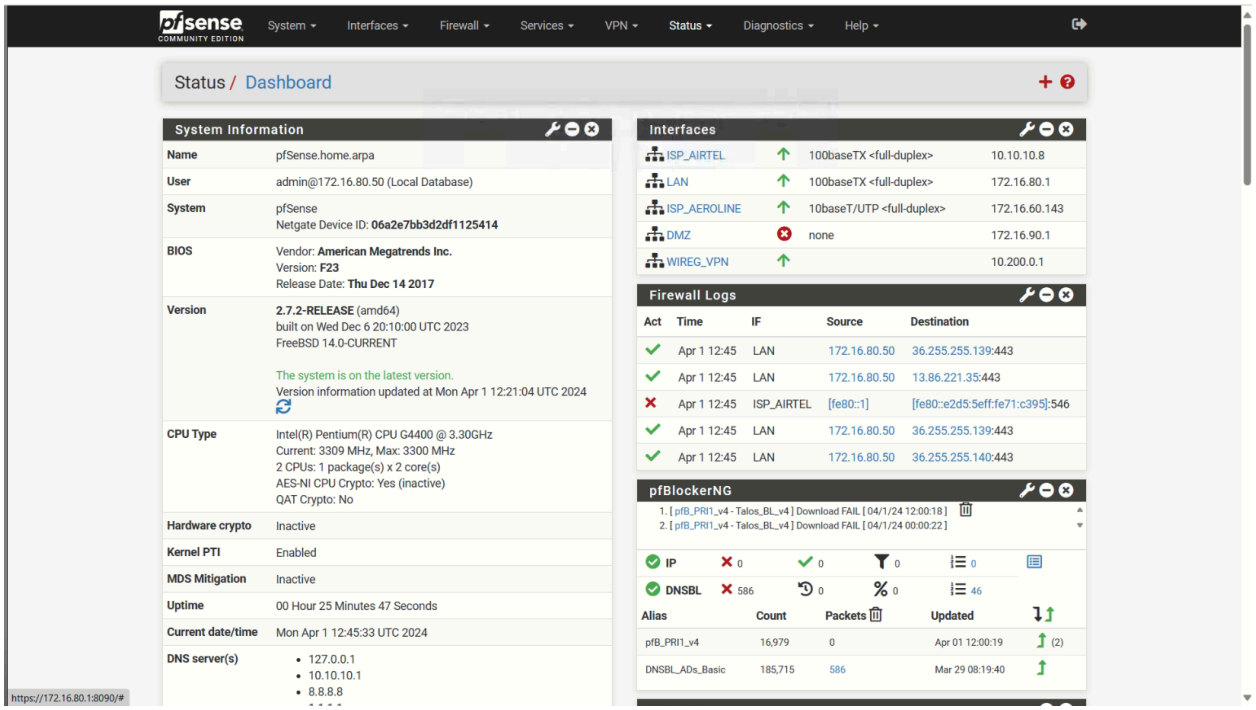
In addition to UTM, pfSense also includes load balancing and multi-WAN support, making it a versatile solution for organizations with multiple internet connections. This feature ensures that the network always has a backup internet connection, ensuring uninterrupted connectivity.

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 TO SET 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.
   - Press Enter to select the default keymap for most users with a standard PC keyboard.

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.

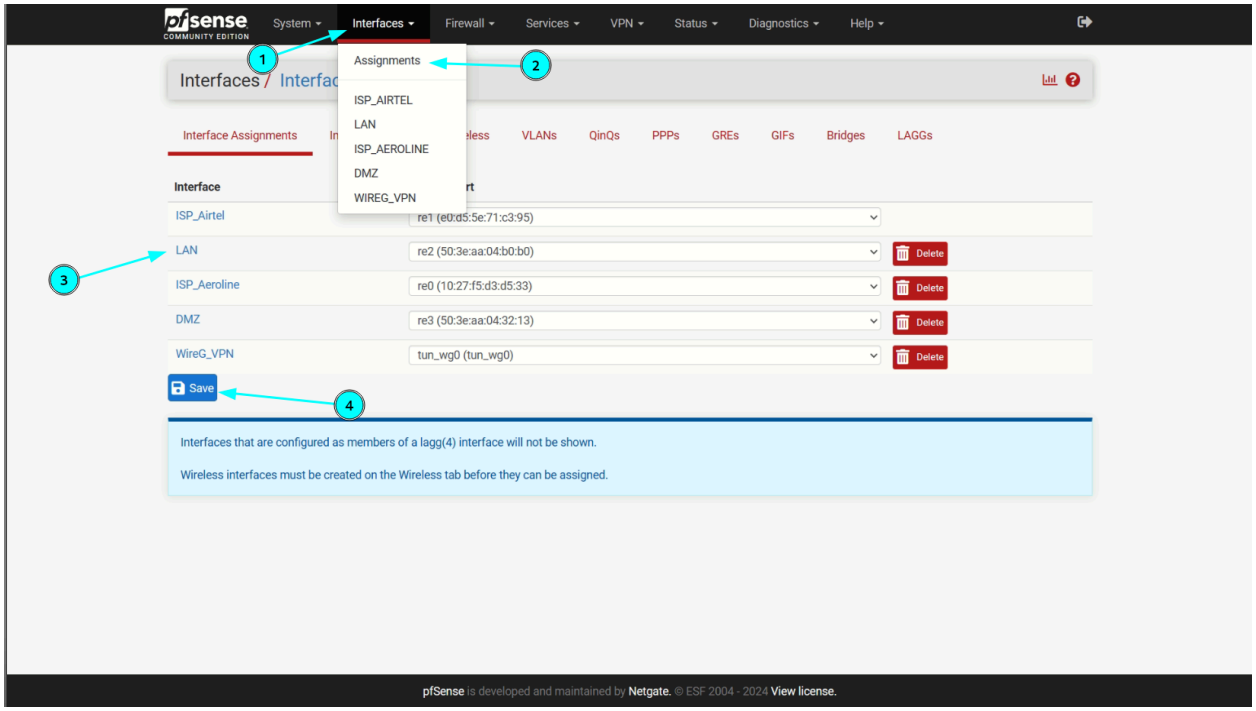
8. Initial Configuration:
   - After rebooting, access the pfSense web interface using the assigned IP address.

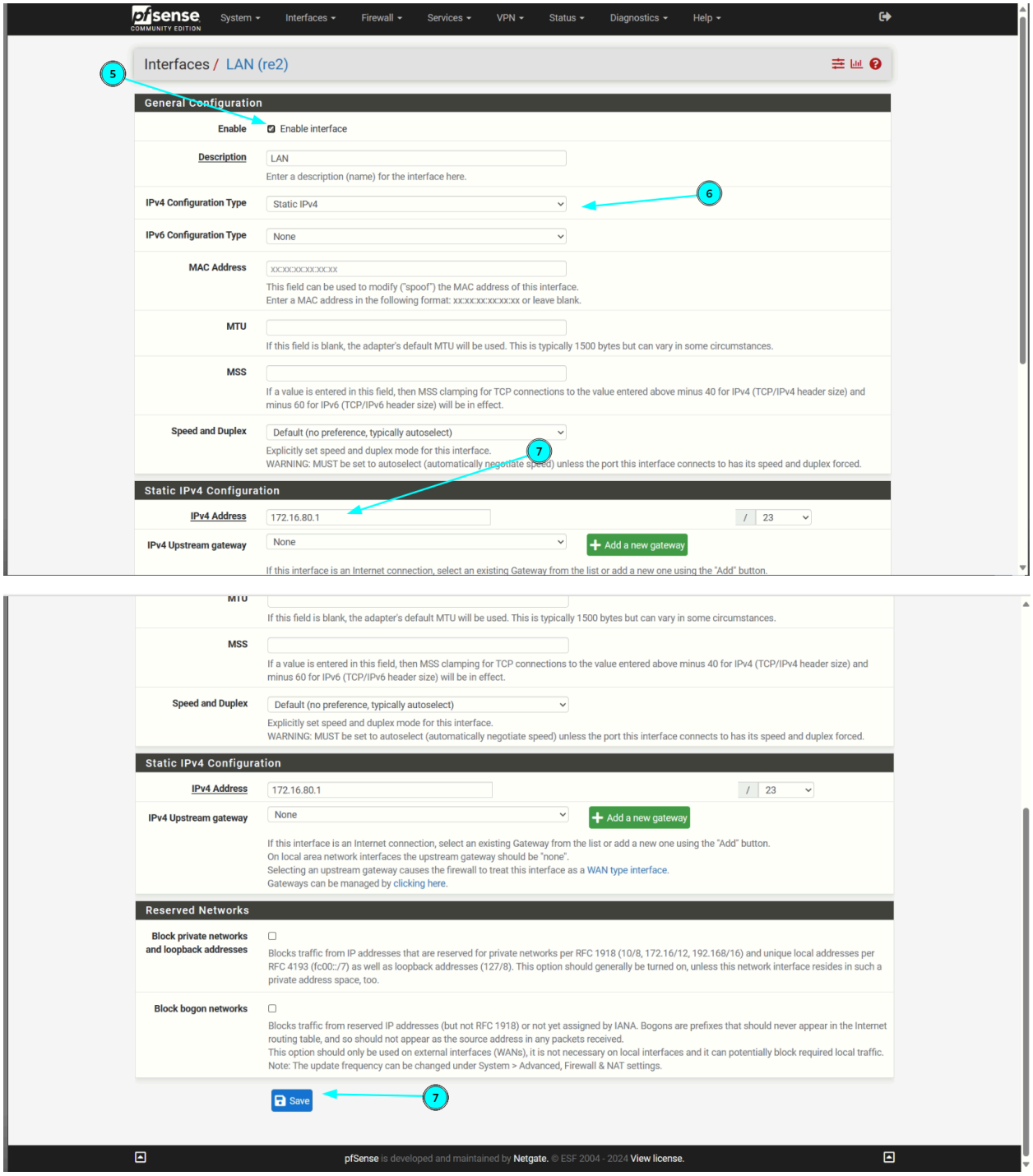
CONFIGURE LAN

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.
5. Log in using the default credentials:
    a. **Username**: admin
    b. **Password**: pfsense
6. **Change the LAN IP Address**:
7. We'll change it to **172.16.80.1**:
    a. Access the pfSense console (VGA, serial, or SSH from another interface).

b. Choose option **2** from the console menu.
c. Enter the new LAN IP address (**172.16.80.1**), and subnet mask (usually **/24**), and specify whether to enable DHCP.
d. 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:
    a. 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.

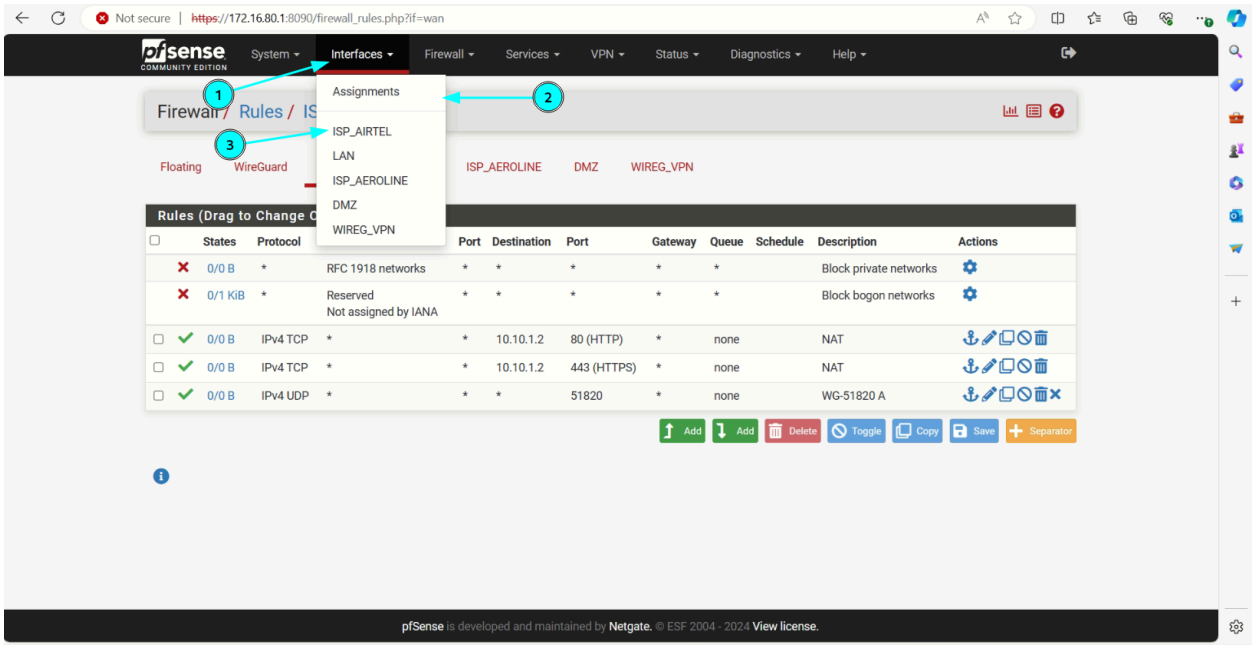
The ISP will assign an IP address dynamically.

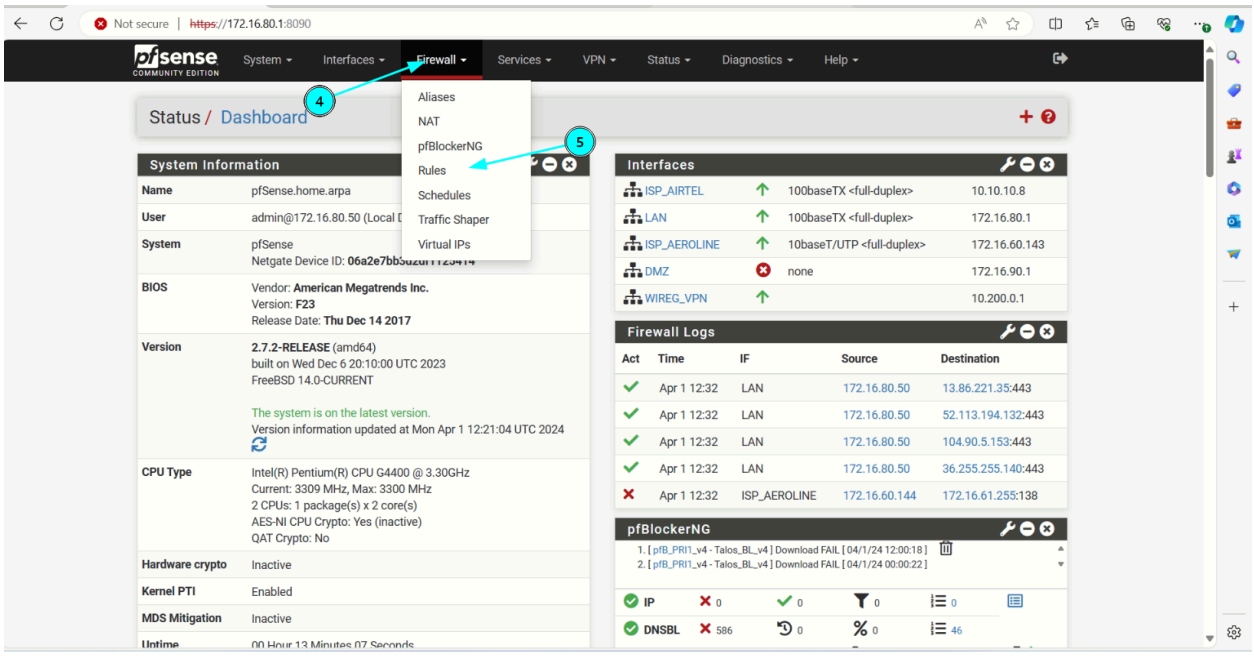
Configure Firewall Rules:

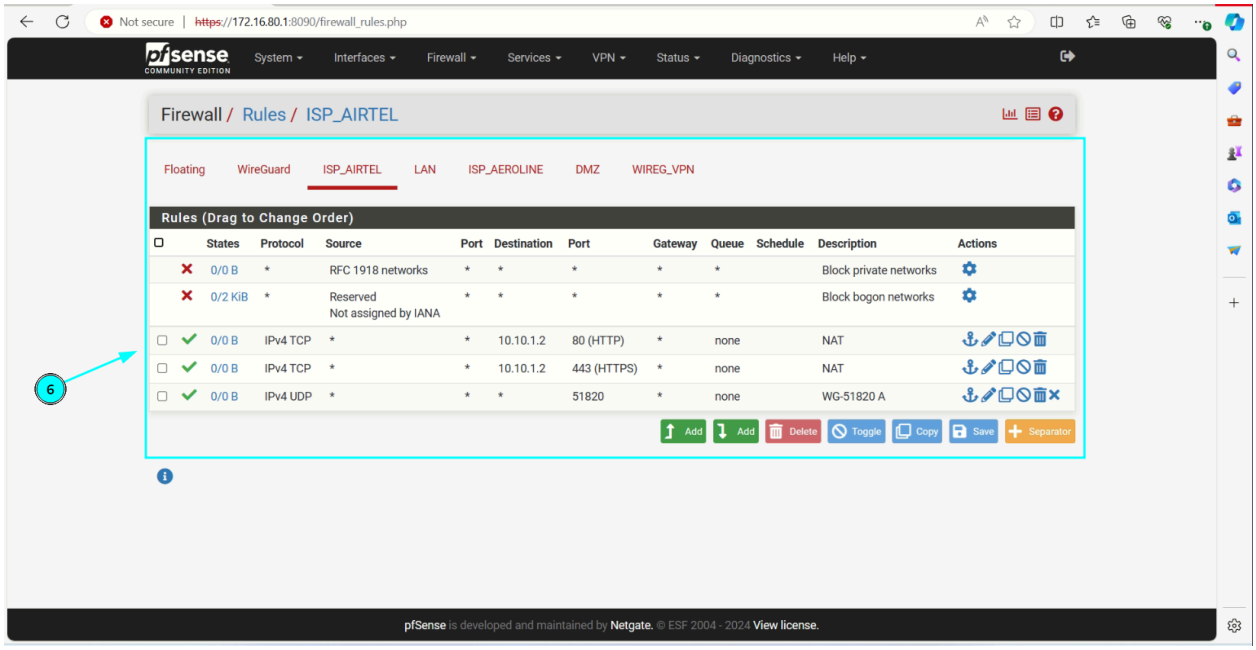
Create appropriate firewall rules for each WAN interface.

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**:

    a. Click **Add** to create a new gateway group.
    b. Fill in the options on the page as described in the **Gateway Group Options**.
    c. Save your settings.
2. **Load Balancing**:

    a. Any two gateways on the same tier are load-balanced.
    b. For example, if you have **Gateway A**, **Gateway B**, and **Gateway C** all on **Tier 1**, connections will be balanced between them.

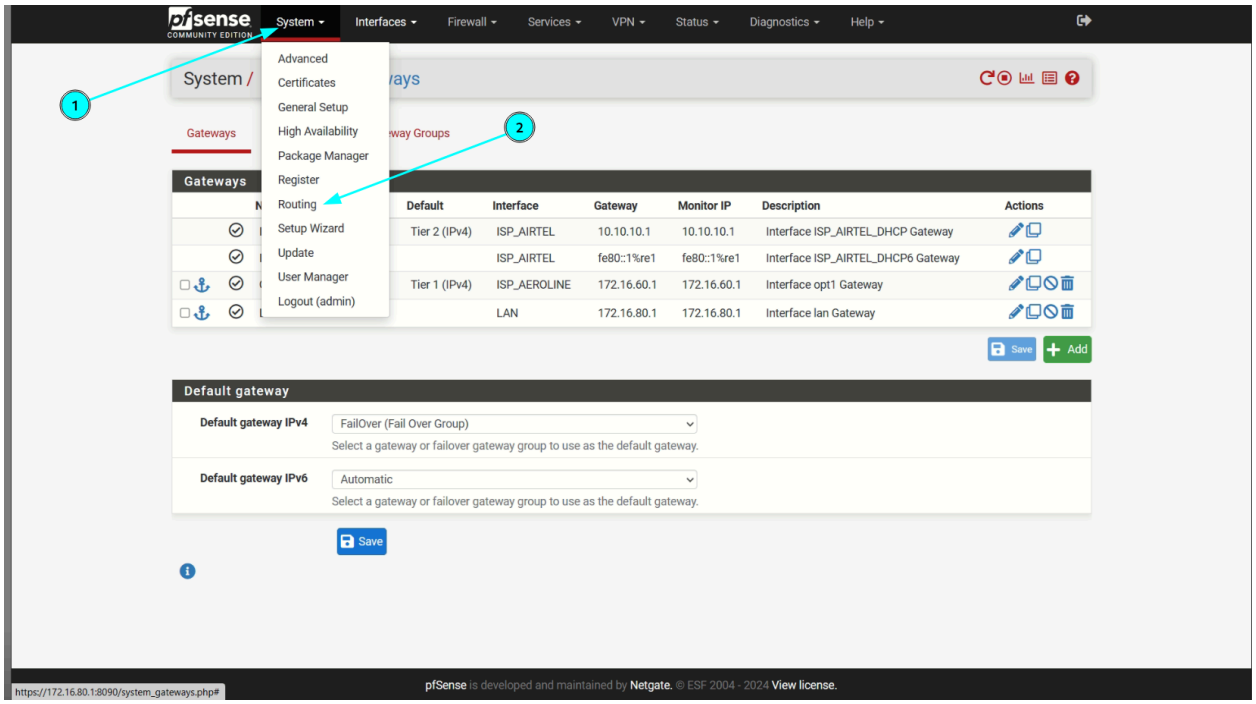
c. Gateways that are load balanced will automatically failover between each other. If one gateway fails, it is removed from the group, and the firewall load balances between the remaining online gateways.

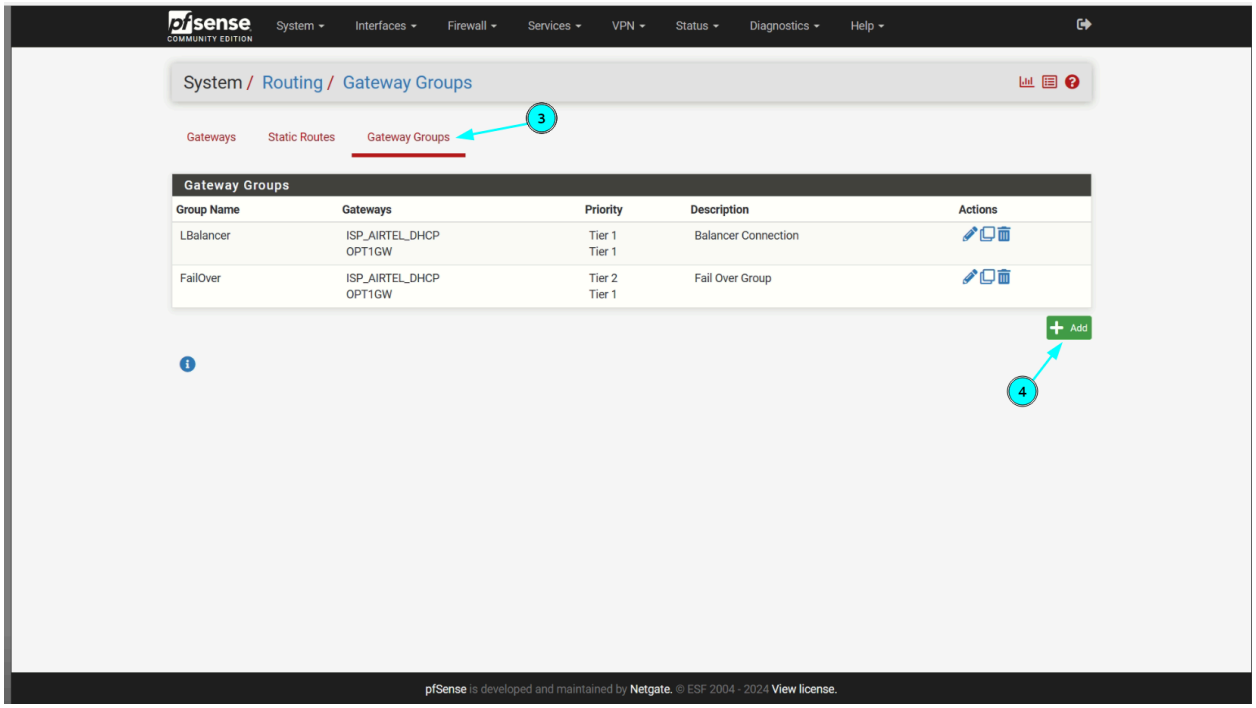
3. **Weighted Balancing**:

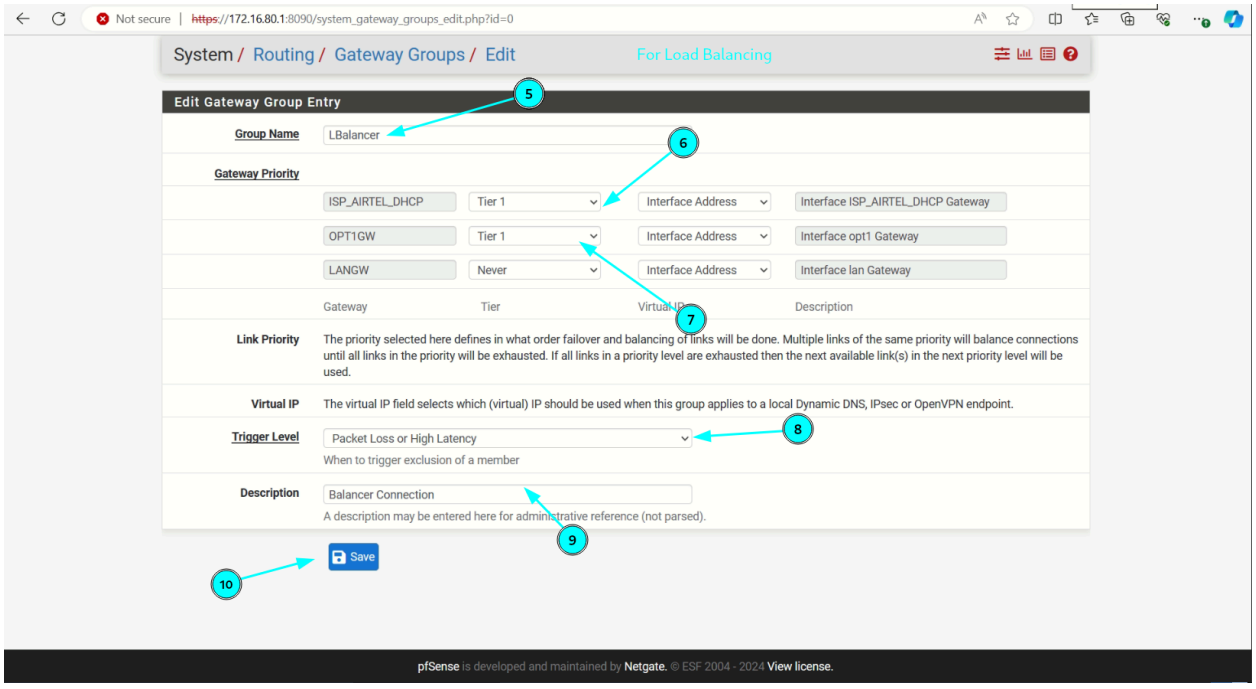
   a. If you need to balance WANs in a weighted fashion due to differing bandwidth, adjust the **Weight** parameter on the gateway.

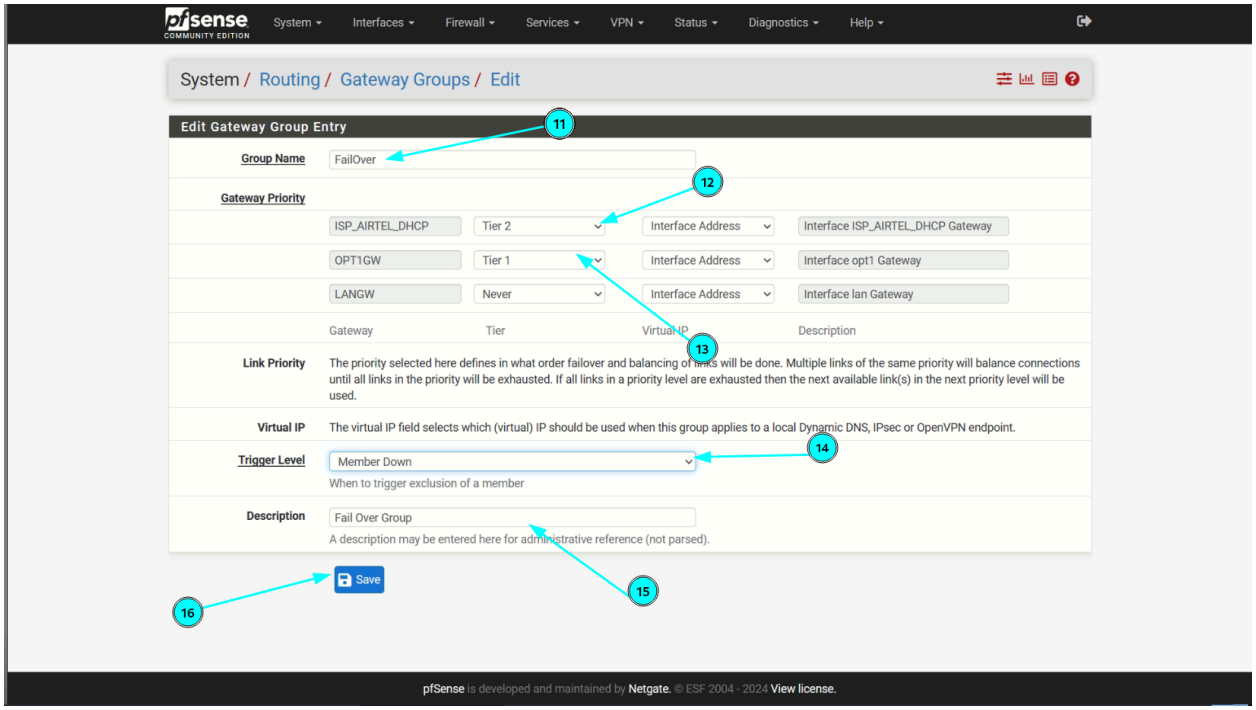
4. **Failover**:

   a. The firewall prefers gateways on a lower-numbered tier.
   b. For example:
      i. **Gateway A** (Tier 1)
      ii. **Gateway B** (Tier 2)
   c. 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**.



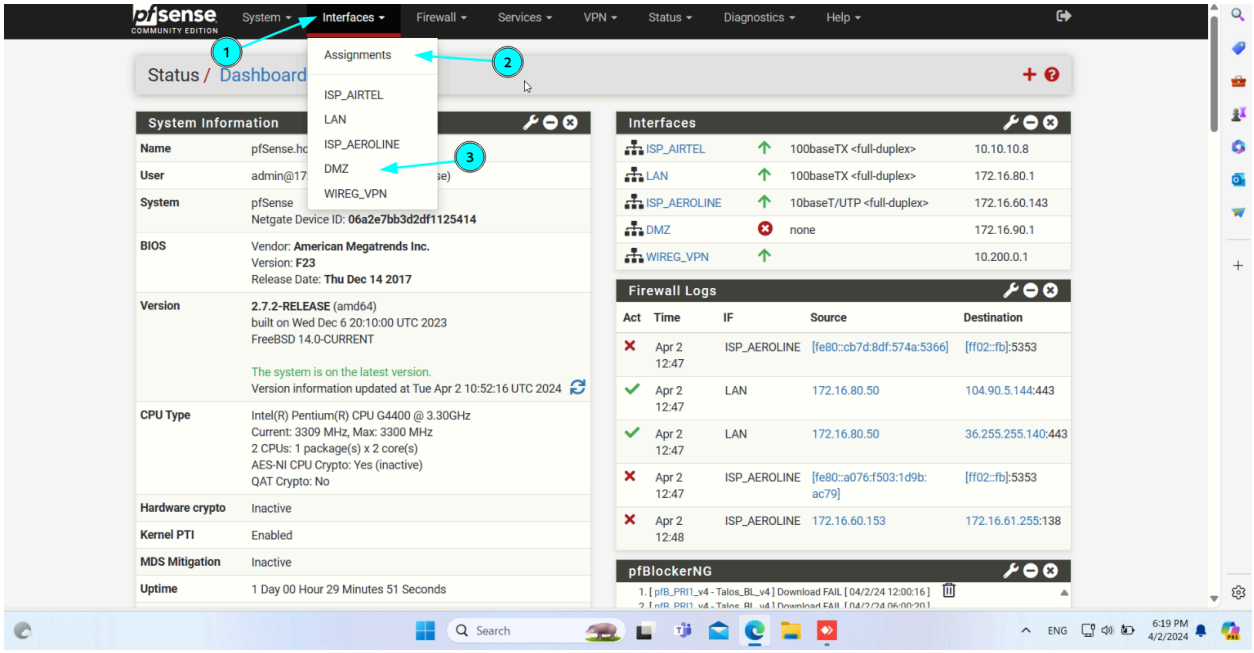

pfSense COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
System / Routing / Gateway Groups
Gateways
Static Routes
Gateway Groups
3
Gateway Groups
Group Name
Gateways
Priority
Description
Actions
LBalancer
ISP_AIRTEL_DHCP
OPT1GW
Tier 1
Tier 1
Balancer Connection
FailOver
ISP_AIRTEL_DHCP
OPT1GW
Tier 2
Tier 1
Fail Over Group
Add
4
pfSense is developed and maintained by Netgate. © ESF 2004 - 2024 View license.

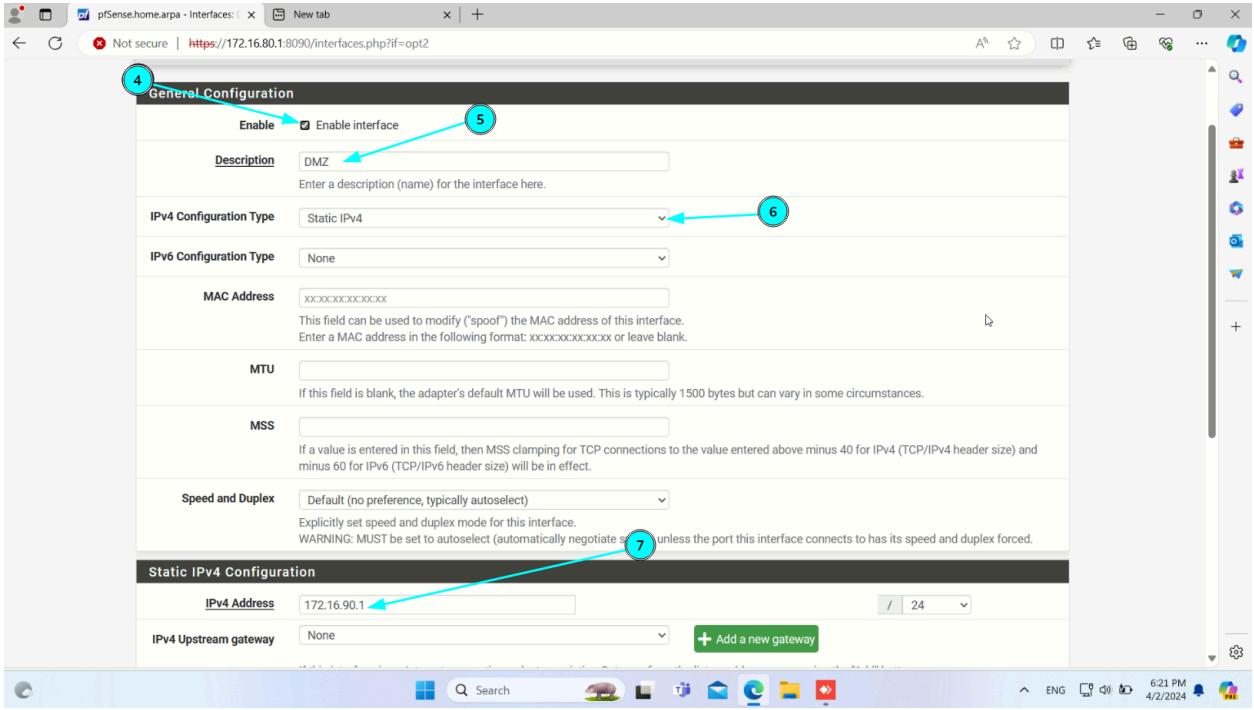

Not secure
https://172.16.80.1:8090/system_gateway_groups_edit.php?id=0
System / Routing / Gateway Groups / Edit
For Load Balancing
5
Edit Gateway Group Entry
Group Name
LBalancer
6
Gateway Priority
ISP_AIRTEL_DHCP
Tier 1
Interface Address
Interface ISP_AIRTEL_DHCP Gateway
OPT1GW
Tier 1
Interface Address
Interface opt1 Gateway
LANGW
Never
Interface Address
Interface lan Gateway
Gateway
Tier
Virtual IP
Description
7
Link Priority
The priority selected here defines in what order failover and balancing of links will be done. Multiple links of the same priority will balance connections until all links in the priority will be exhausted. If all links in a priority level are exhausted then the next available link(s) in the next priority level will be used.
Virtual IP
The virtual IP field selects which (virtual) IP should be used when this group applies to a local Dynamic DNS, IPsec or OpenVPN endpoint.
Trigger Level
Packet Loss or High Latency
8
When to trigger exclusion of a member
Description
Balancer Connection
A description may be entered here for administrative reference (not parsed).
9
Save
10
pfSense is developed and maintained by Netgate. © ESF 2004 - 2024 View license.

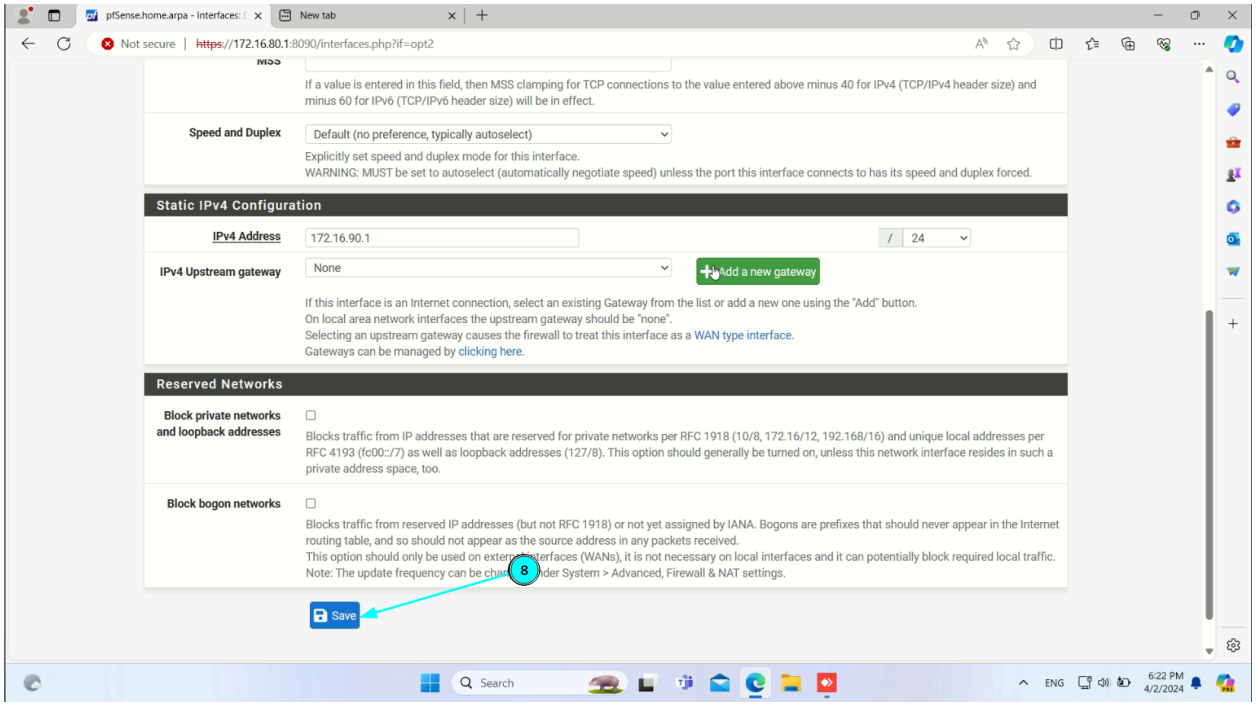


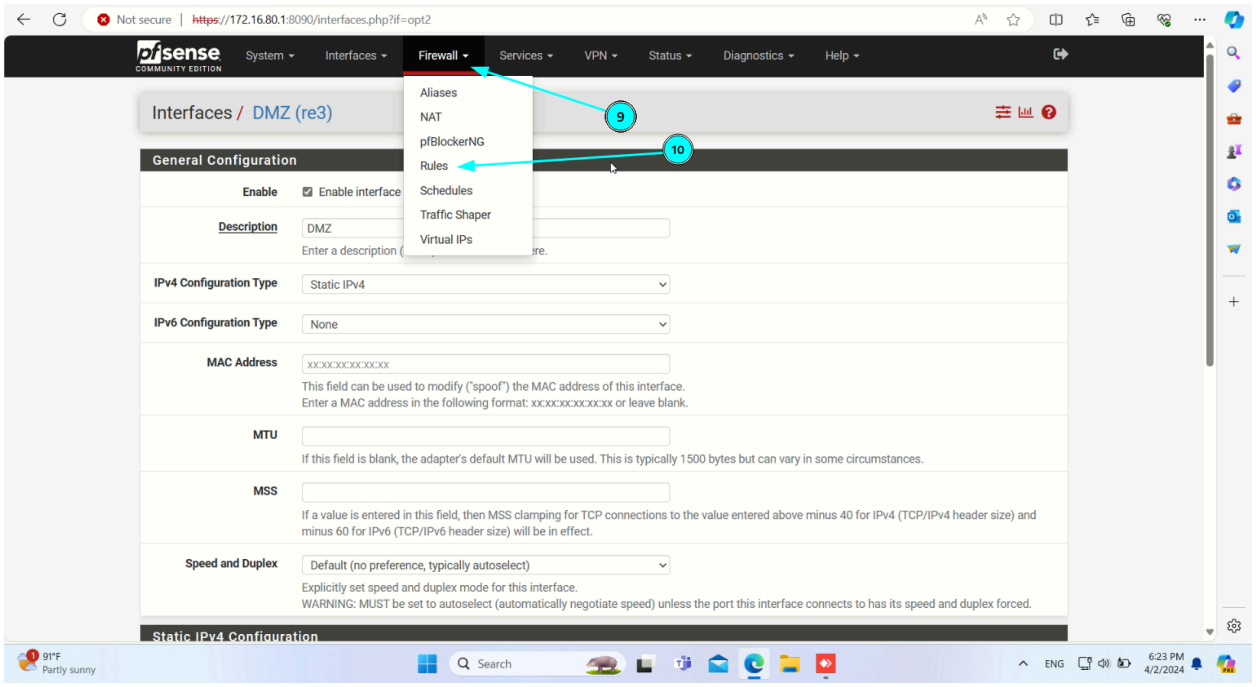
DMZ

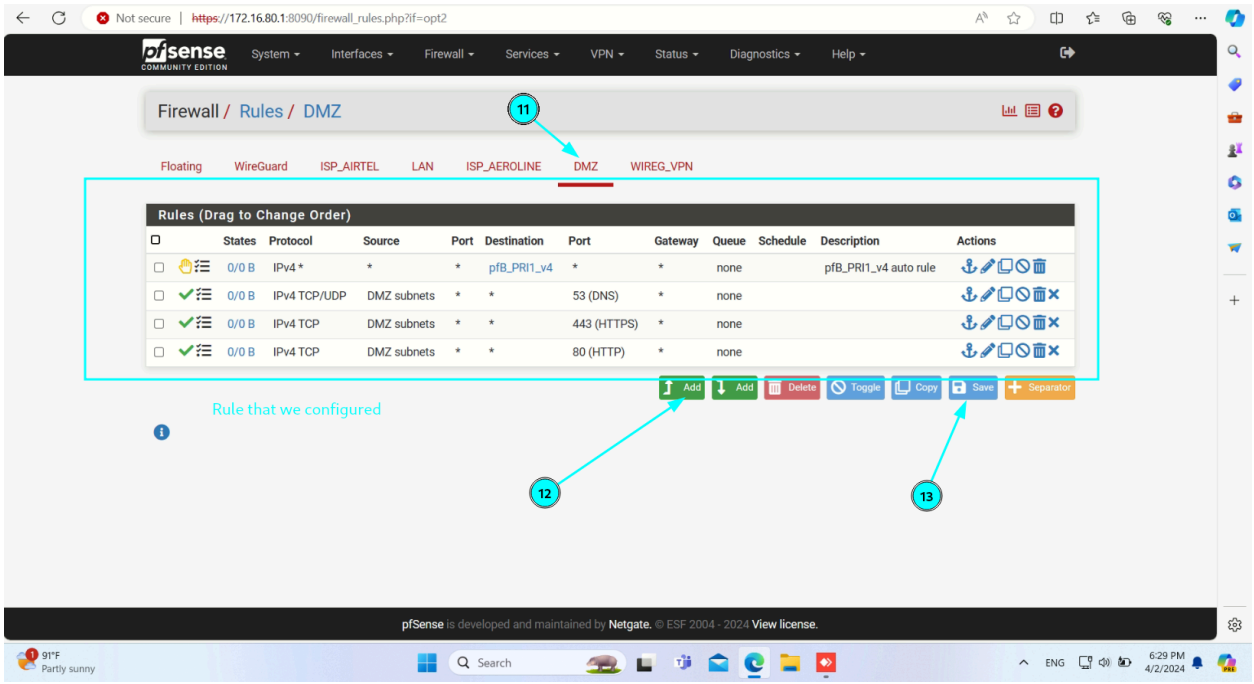
A DMZ, or Demilitarized Zone, is a specialized network segment designed to provide an additional layer of security for public-facing servers, such as web servers, mail servers, and FTP servers. By placing these servers in the DMZ, you can segregate them from your internal network, reducing the risk of 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.


pfSense COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
Assignments
ISP_AIRTEL
LAN
ISP_AEROLINE
DMZ
WIREG_VPN
1
2
3
Status / Dashboard
System Information
Name
User
System
pfSense
Netgate Device ID: 06a2e7bb3d2df1125414
BIOS
Vendor: American Megatrends Inc.
Version: F23
Release Date: Thu Dec 14 2017
Version
2.7.2-RELEASE (amd64)
built on Wed Dec 6 20:10:00 UTC 2023
FreeBSD 14.0-CURRENT
The system is on the latest version.
Version information updated at Tue Apr 2 10:52:16 UTC 2024
CPU Type
Intel(R) Pentium(R) CPU G4400 @ 3.30GHz
Current: 3309 MHz, Max: 3300 MHz
2 CPUs: 1 package(s) x 2 core(s)
AES-NI CPU Crypto: Yes (inactive)
QAT Crypto: No
Hardware crypto
Inactive
Kernel PTI
Enabled
MDS Mitigation
Inactive
Uptime
1 Day 00 Hour 29 Minutes 51 Seconds
Interfaces
ISP_AIRTEL
100baseTX <full-duplex>
10.10.10.8
LAN
100baseTX <full-duplex>
172.16.80.1
ISP_AEROLINE
10baseT/UTP <full-duplex>
172.16.60.143
DMZ
none
172.16.90.1
WIREG_VPN
10.200.0.1
Firewall Logs
Act
Time
IF
Source
Destination
Apr 2 12:47
ISP_AEROLINE
[fe80::cb7d:8df:574a:5366]
[ff02::fb]:5353
Apr 2 12:47
LAN
172.16.80.50
104.90.5.144:443
Apr 2 12:47
LAN
172.16.80.50
36.255.255.140:443
Apr 2 12:47
ISP_AEROLINE
[fe80::a076:f503:1d9b:ac79]
[ff02::fb]:5353
Apr 2 12:48
ISP_AEROLINE
172.16.60.153
172.16.61.255:138
pfBlockerNG
1. [pfB_PRI1_v4 - Talos_BL_v4] Download FAIL [04/2/24 12:00:16]
Search
ENG
6:19 PM
4/2/2024


pfSense.home.arpa - Interfaces:
New tab
Not secure
https://172.16.80.1:8090/interfaces.php?if=opt2
4
5
6
7
General Configuration
Enable
Enable interface
Description
DMZ
Enter a description (name) for the interface here.
IPv4 Configuration Type
Static IPv4
IPv6 Configuration Type
None
MAC Address
xx:xx:xx:xx:xx:xx
This field can be used to modify ("spoof") the MAC address of this interface.
Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank.
MTU
If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.
MSS
If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.
Speed and Duplex
Default (no preference, typically autoselect)
Explicitly set speed and duplex mode for this interface.
WARNING: MUST be set to autoselect (automatically negotiate s
unless the port this interface connects to has its speed and duplex forced.
Static IPv4 Configuration
IPv4 Address
172.16.90.1
/ 24
IPv4 Upstream gateway
None
Add a new gateway
Search
ENG
6:21 PM
4/2/2024


pfSense.home.arpa - Interfaces:
New tab
Not secure | https://172.16.80.1:8090/interfaces.php?if=opt2
If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.
Speed and Duplex
Default (no preference, typically autoselect)
Explicitly set speed and duplex mode for this interface.
WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.
Static IPv4 Configuration
IPv4 Address
172.16.90.1
/ 24
IPv4 Upstream gateway
None
Add a new gateway
If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button.
On local area network interfaces the upstream gateway should be "none".
Selecting an upstream gateway causes the firewall to treat this interface as a WAN type interface.
Gateways can be managed by clicking here.
Reserved Networks
Block private networks and loopback addresses
Blocks traffic from IP addresses that are reserved for private networks per RFC 1918 (10/8, 172.16/12, 192.168/16) and unique local addresses per RFC 4193 (fc00::/7) as well as loopback addresses (127/8). This option should generally be turned on, unless this network interface resides in such a private address space, too.
Block bogon networks
Blocks traffic from reserved IP addresses (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and so should not appear as the source address in any packets received.
This option should only be used on external interfaces (WANs), it is not necessary on local interfaces and it can potentially block required local traffic.
Note: The update frequency can be changed under System > Advanced, Firewall & NAT settings.
8
Save
Search
ENG
6:22 PM
4/2/2024


Not secure | https://172.16.80.1:8090/interfaces.php?if=opt2
pfsense COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
Aliases
NAT
pfBlockerNG
Rules
Schedules
Traffic Shaper
Virtual IPs
9
10
Interfaces / DMZ (re3)
General Configuration
Enable
Enable interface
Description
DMZ
IPv4 Configuration Type
Static IPv4
IPv6 Configuration Type
None
MAC Address
This field can be used to modify ("spoof") the MAC address of this interface.
Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank.
MTU
If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.
MSS
If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.
Speed and Duplex
Default (no preference, typically autoselect)
Explicitly set speed and duplex mode for this interface.
WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.
Static IPv4 Configuration
91°F
Partly sunny
Search
ENG
6:23 PM
4/2/2024



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

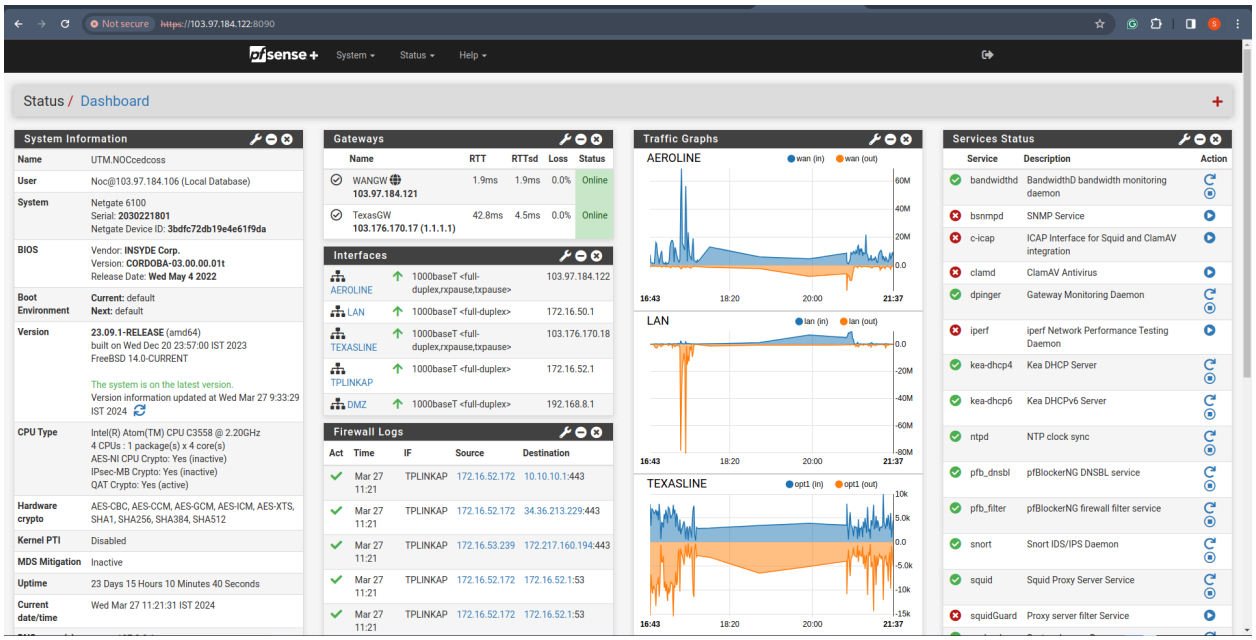
countries or IP address ranges. Enhanced Alias Table:
It lets you consolidate multiple IP address or URL lists into a single alias. Dashboard Widget: Provides a convenient widget for monitoring and managing

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

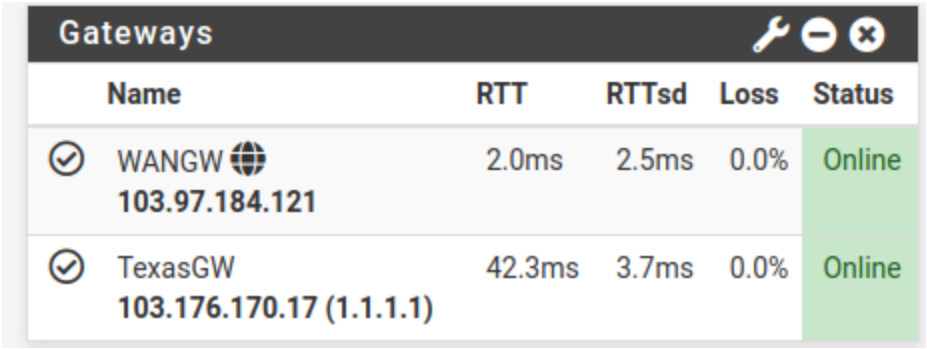
choose different actions for each list (deny both, deny inbound, deny outbound, permit inbound, permit outbound, or alias only).

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



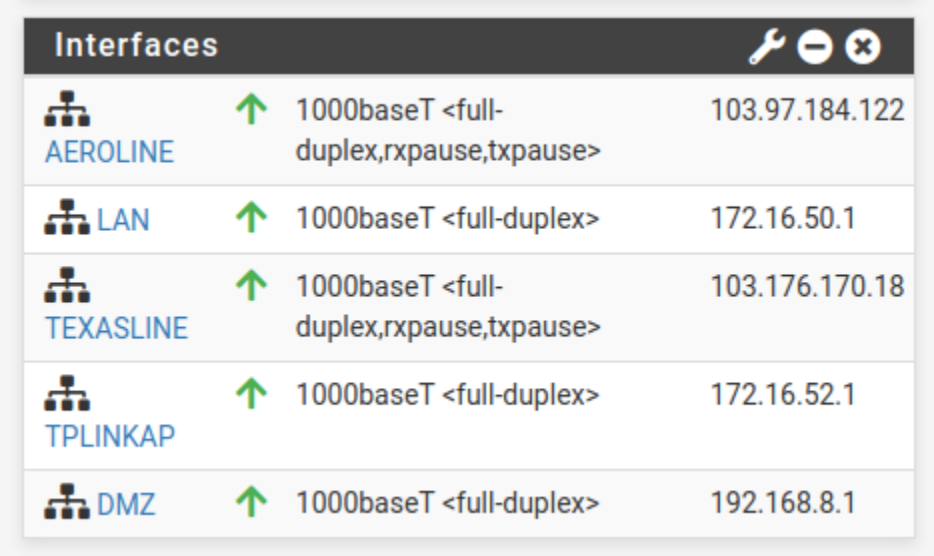
Gateways (Number of ISPs available)



Gateways

	Name	RTT	RTTsd	Loss	Status
✓	WANGW **103.97.184.121**	2.0ms	2.5ms	0.0%	Online
✓	TexasGW **103.176.170.17 (1.1.1.1)**	42.3ms	3.7ms	0.0%	Online

Number of Output or Interfaces



Interfaces

AEROLINE	↑	1000baseT <full-duplex,rxpause,txpause>	103.97.184.122
LAN	↑	1000baseT <full-duplex>	172.16.50.1
TEXASLINE	↑	1000baseT <full-duplex,rxpause,txpause>	103.176.170.18
TPLINKAP	↑	1000baseT <full-duplex>	172.16.52.1
DMZ	↑	1000baseT <full-duplex>	192.168.8.1

Firewall Logs

Firewall Logs

Act	Time	IF	Source	Destination
✓	Mar 27 11:25	TPLINKAP	172.16.53.217	172.16.52.1:53
✓	Mar 27 11:25	TPLINKAP	172.16.53.217	172.16.52.1:53
✓	Mar 27 11:25	LAN	172.16.50.244	10.10.10.1:443
✓	Mar 27 11:25	LAN	172.16.50.244	10.10.10.1:443
✓	Mar 27 11:25	TPLINKAP	172.16.53.153	172.16.52.1:53

VPN Services

WireGuard

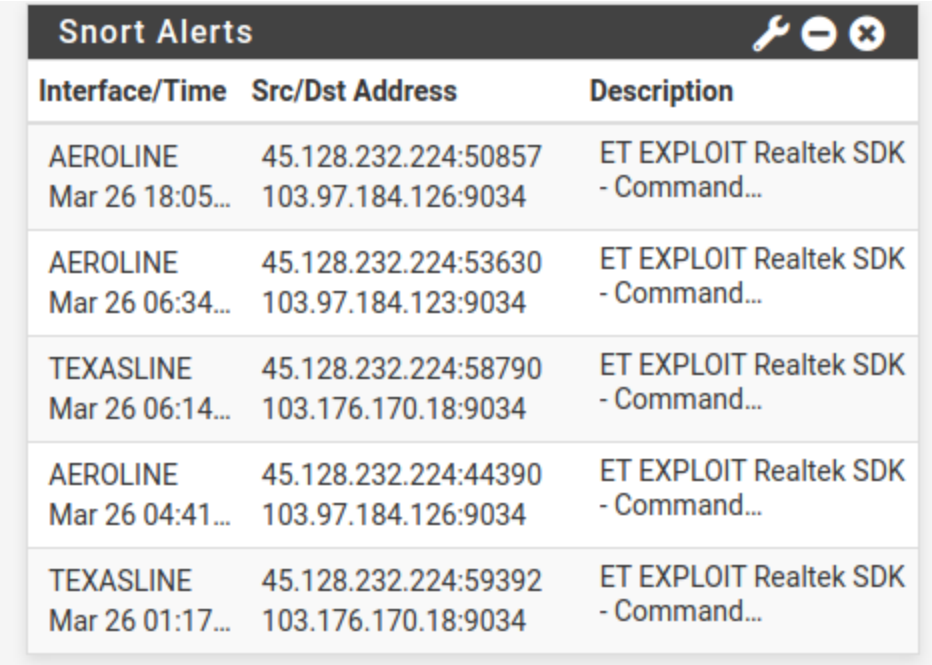
Tunnel	Description	Active Peers	Listen Port	RX	TX
↑ tun_wg0	EldecoVP	1	51820	1.45 GiB	2.79 GiB

NTP Status

NTP Status

Server Time	10:54:10 IST
Sync Source	40.81.94.65 (stratum 3)

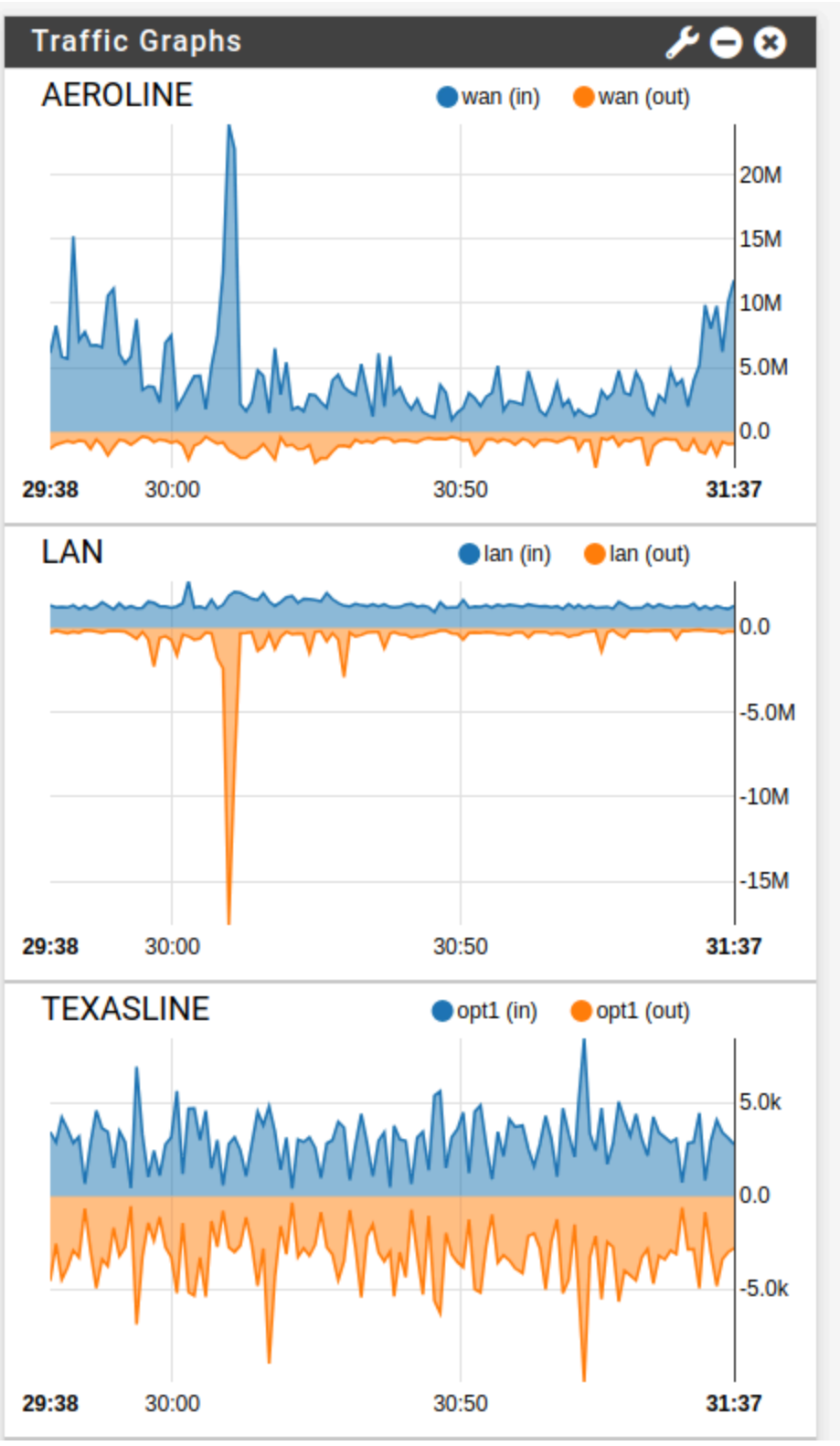
SNORT Logs

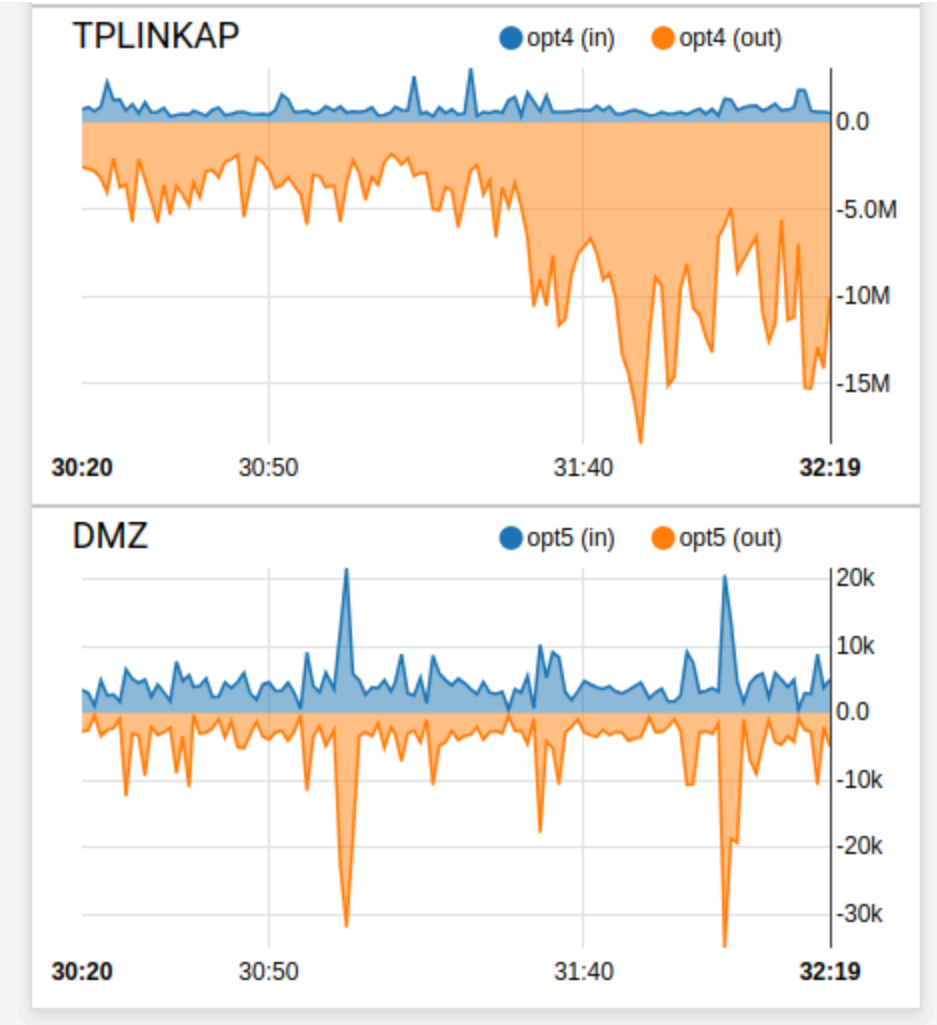


Snort Alerts

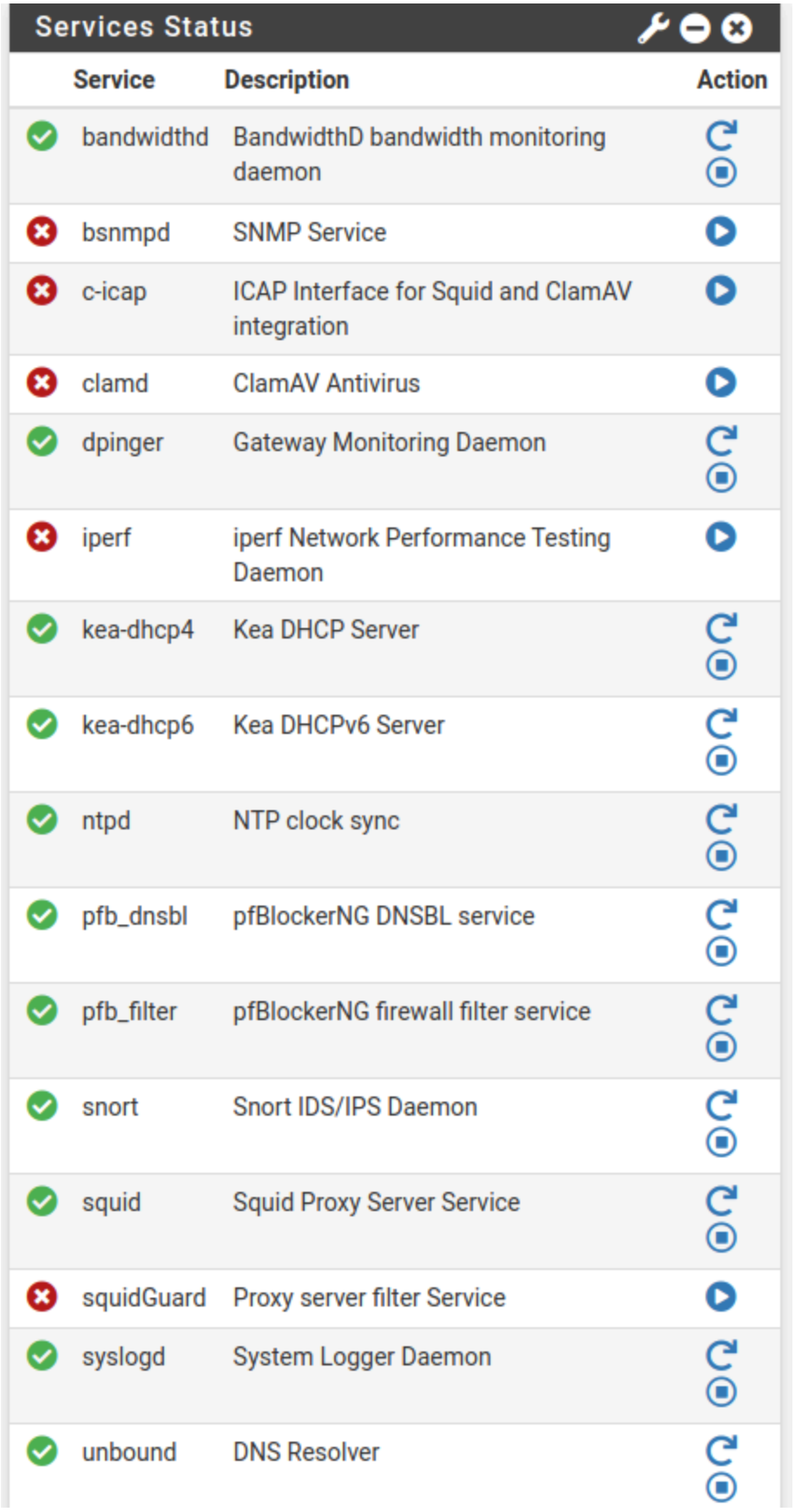
Interface/Time	Src/Dst Address	Description
AEROLINE Mar 26 18:05...	45.128.232.224:50857 103.97.184.126:9034	ET EXPLOIT Realtek SDK - Command...
AEROLINE Mar 26 06:34...	45.128.232.224:53630 103.97.184.123:9034	ET EXPLOIT Realtek SDK - Command...
TEXASLINE Mar 26 06:14...	45.128.232.224:58790 103.176.170.18:9034	ET EXPLOIT Realtek SDK - Command...
AEROLINE Mar 26 04:41...	45.128.232.224:44390 103.97.184.126:9034	ET EXPLOIT Realtek SDK - Command...
TEXASLINE Mar 26 01:17...	45.128.232.224:59392 103.176.170.18:9034	ET EXPLOIT Realtek SDK - Command...

Traffic Graph of INPUT and OUTPUT

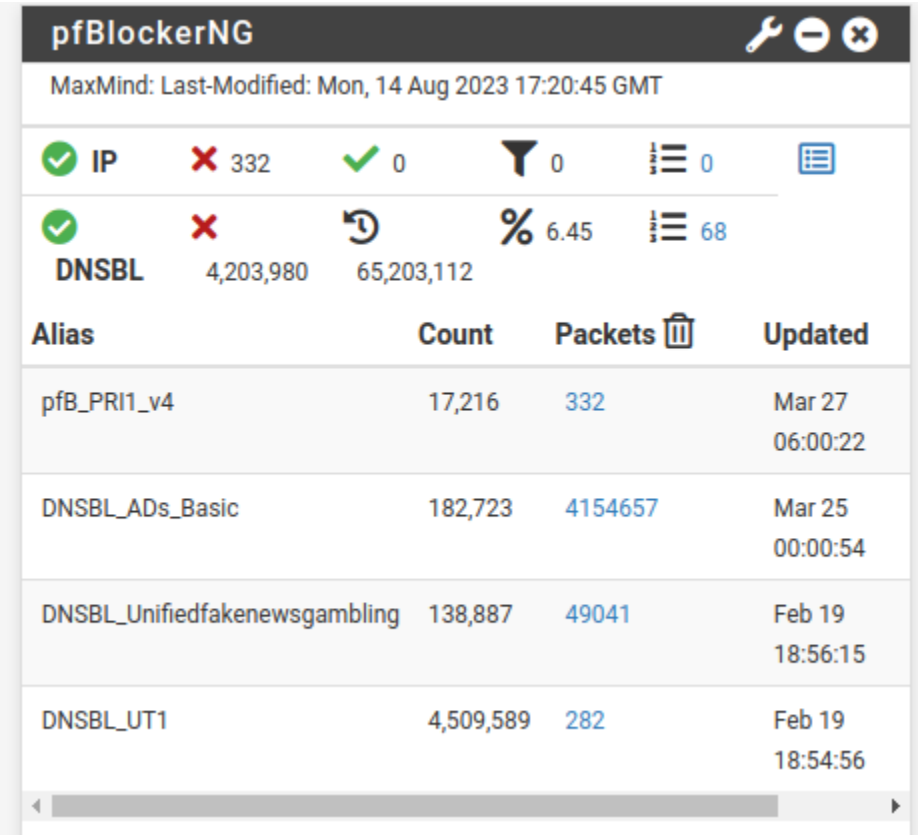

Traffic Graphs
AEROLINE
wan (in)
wan (out)
20M
15M
10M
5.0M
0.0
29:38
30:00
30:50
31:37
LAN
lan (in)
lan (out)
0.0
-5.0M
-10M
-15M
29:38
30:00
30:50
31:37
TEXASLINE
opt1 (in)
opt1 (out)
5.0k
0.0
-5.0k
29:38
30:00
30:50
31:37



Number Of Services that are Enable or Disable


Services Status
Service
Description
Action
bandwidthd
BandwidthD bandwidth monitoring daemon
bsnmpd
SNMP Service
c-icap
ICAP Interface for Squid and ClamAV integration
clamd
ClamAV Antivirus
dpinger
Gateway Monitoring Daemon
iperf
iperf Network Performance Testing Daemon
kea-dhcp4
Kea DHCP Server
kea-dhcp6
Kea DHCPv6 Server
ntpd
NTP clock sync
pfb_dnsbl
pfBlockerNG DNSBL service
pfb_filter
pfBlockerNG firewall filter service
snort
Snort IDS/IPS Daemon
squid
Squid Proxy Server Service
squidGuard
Proxy server filter Service
syslogd
System Logger Daemon
unbound
DNS Resolver

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.