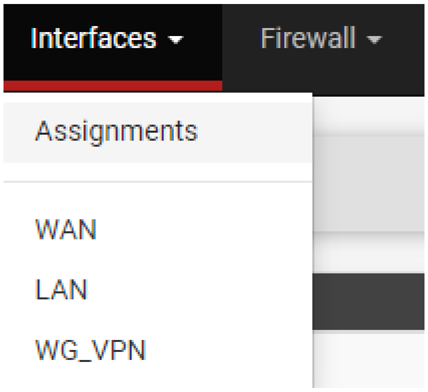
535 pfSense - VLANs and Multi-LAN Setup

Step 1: Accessing pfSense Web Interface

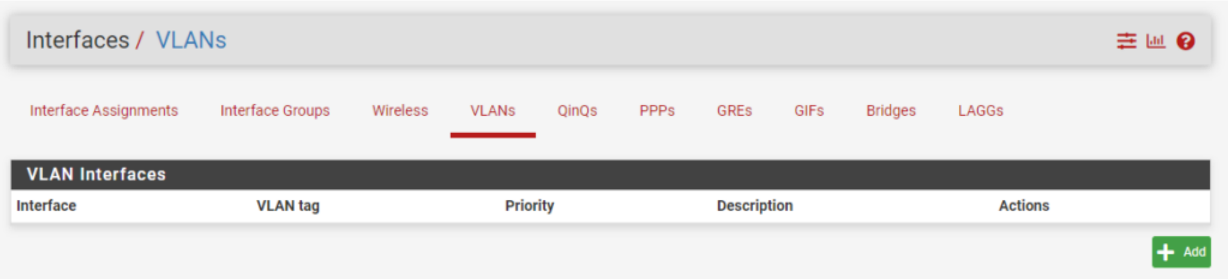
- I opened my preferred web browser and entered the LAN IP address of my pfSense firewall.



- After that, I logged in using my pfSense credentials.

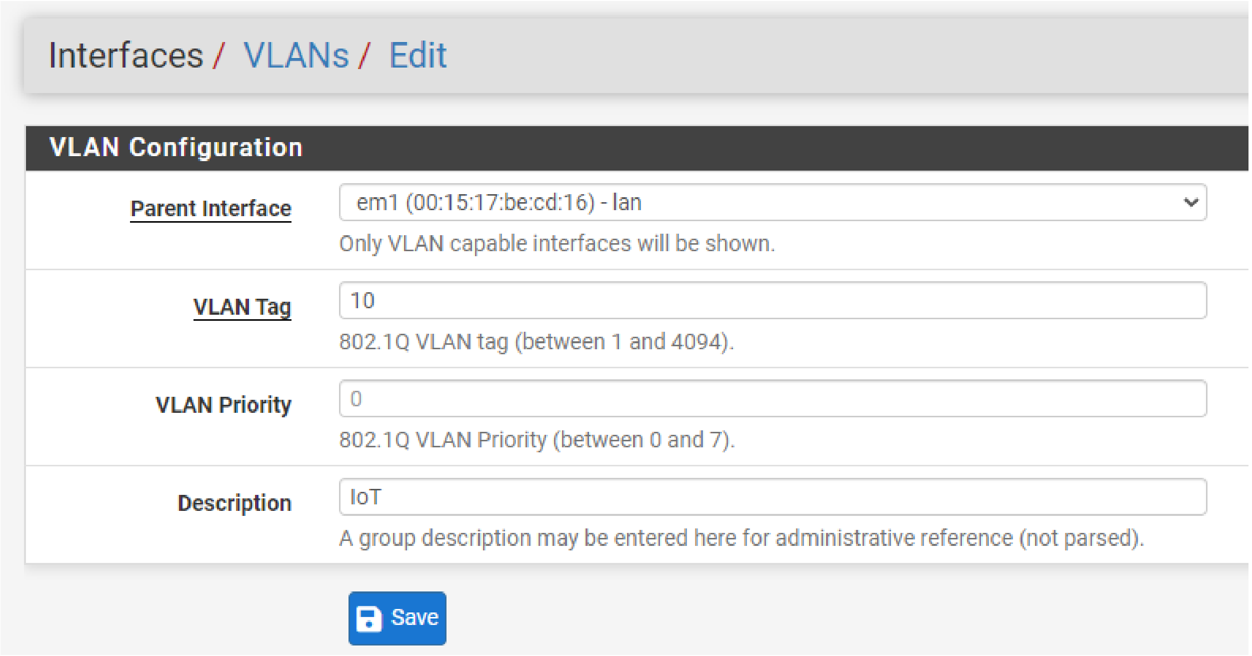
Step 2: Creating VLANs in pfSense.

- Navigating to Interfaces > Assignments, I selected the "VLANs" tab.
- Then, I clicked on the "Add" button to create a new VLAN.
- Choosing the parent interface as LAN, I segmented it into multiple VLANs, assigning unique VLAN Tags (e.g., 10, 20, 30) for each.
- I also provided descriptive names for easier identification.



VLAN Interfaces

Interface	VLAN tag	Priority	Description	Actions



Interfaces / VLANs / Edit

VLAN Configuration

Parent Interface: em1 (00:15:17:be:cd:16) - lan

Only VLAN capable interfaces will be shown.

VLAN Tag: 10

802.1Q VLAN tag (between 1 and 4094).

VLAN Priority: 0

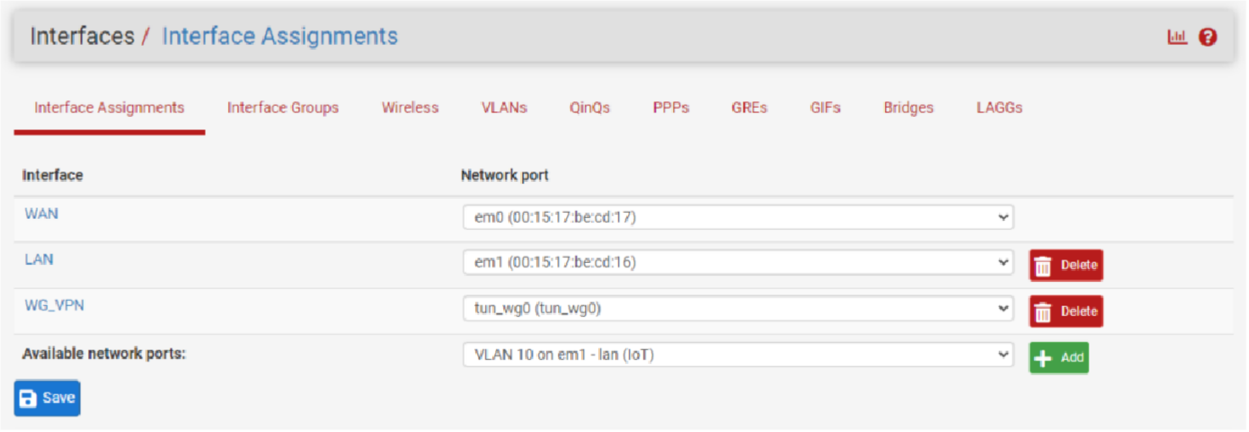
802.1Q VLAN Priority (between 0 and 7).

Description: IoT

A group description may be entered here for administrative reference (not parsed).

Step 3: Assigning VLANs to Physical Interfaces

- Switching to the "Interface Assignments" tab, I assigned each newly created VLAN to a new interface (e.g., OPT1, OPT2).
- Enabling and configuring each interface with appropriate IP settings, I set them as gateways for devices on respective VLANs.



Interfaces / Interface Assignments

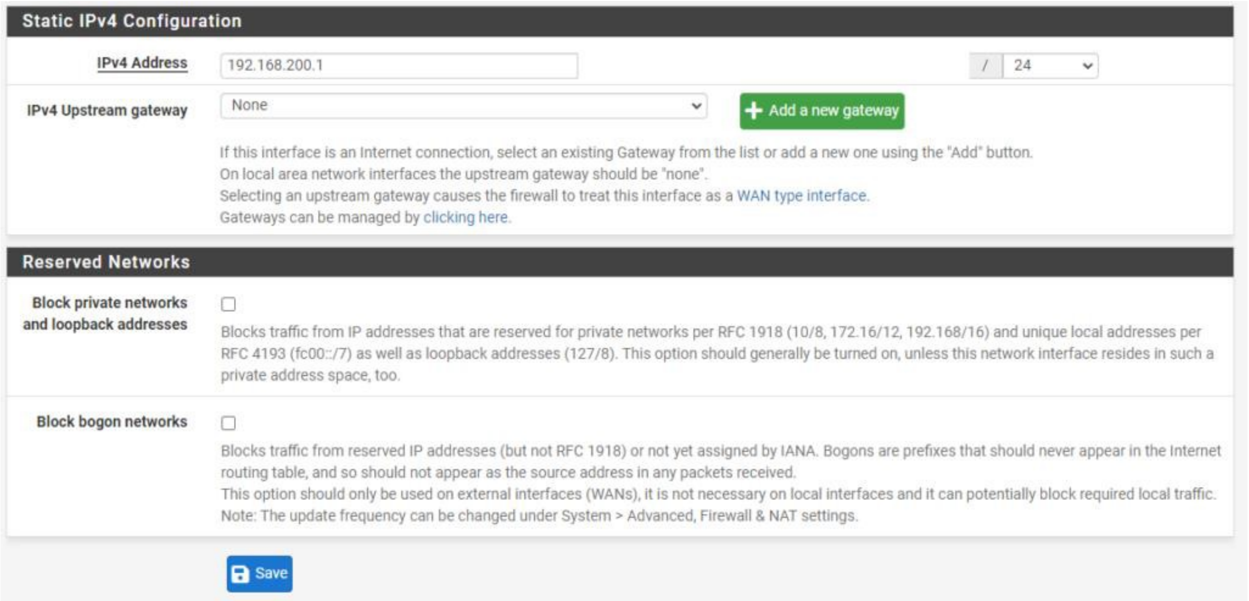
Interface	Network port
WAN	em0 (00:15:17:be:cd:17)
LAN	em1 (00:15:17:be:cd:16)
WG_VPN	tun_wg0 (tun_wg0)
Available network ports:	VLAN 10 on em1 - lan (IoT)

Step 4: Configuring Firewall Rules for Traffic Management

- Moving to Firewall > Rules, I managed traffic between VLANs by creating new rules under each VLAN interface.
- Implementing "pass" rules as needed, I ensured inter-VLAN routing where necessary while being cautious about security implications.

Step 5: Testing Inter-VLAN Routing and Connectivity

- Connecting devices to VLANs via managed switches or access points, I tested basic layer 3 connectivity by pinging pfSense interfaces of other VLANs.
- I attempted to access shared resources across VLANs based on configured rules, verifying restricted access between unauthorized VLANs.



Static IPv4 Configuration

IPv4 Address	192.168.200.1 / 24
IPv4 Upstream gateway	None

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.

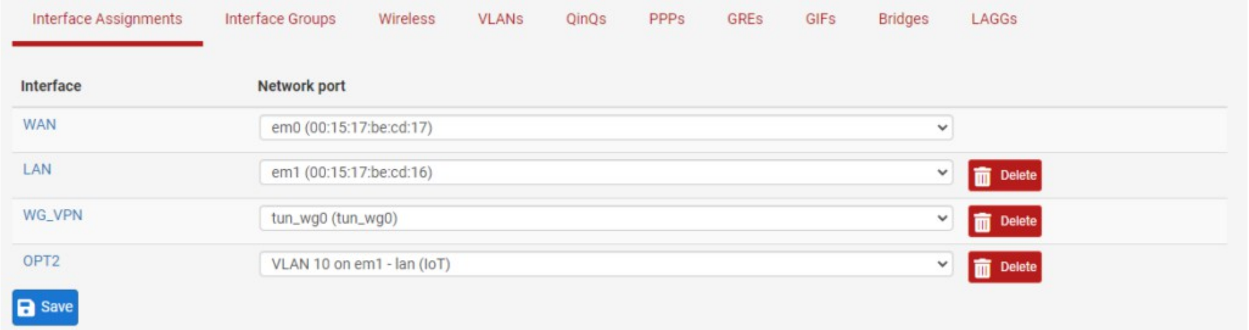
Reserved Networks

Block private networks and loopback addresses □

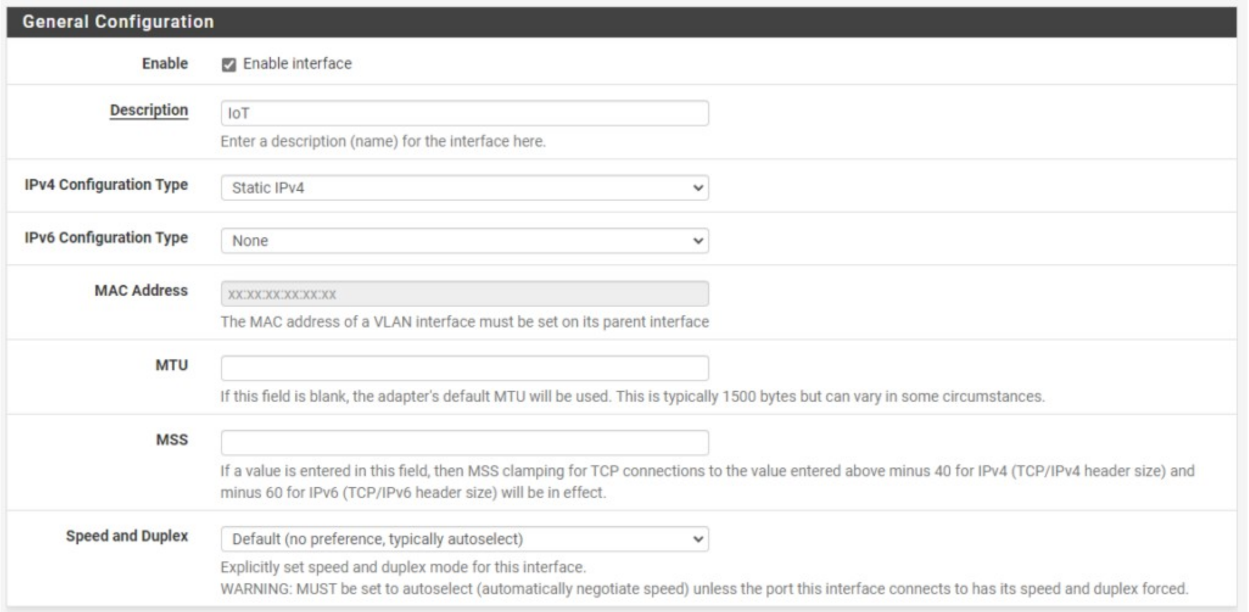
Blocks traffic from IP addresses that are reserved for private networks per RFC 1918 (10/8, 172.16/12, 192.168/16) and unique local addresses per RFC 4193 (fc00::/7) as well as loopback addresses (127/8). This option should generally be turned on, unless this network interface resides in such a private 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.



Interface	Network port
WAN	em0 (00:15:17:be:cd:17)
LAN	em1 (00:15:17:be:cd:16)
WG_VPN	tun_wg0 (tun_wg0)
OPT2	VLAN 10 on em1 - lan (IoT)

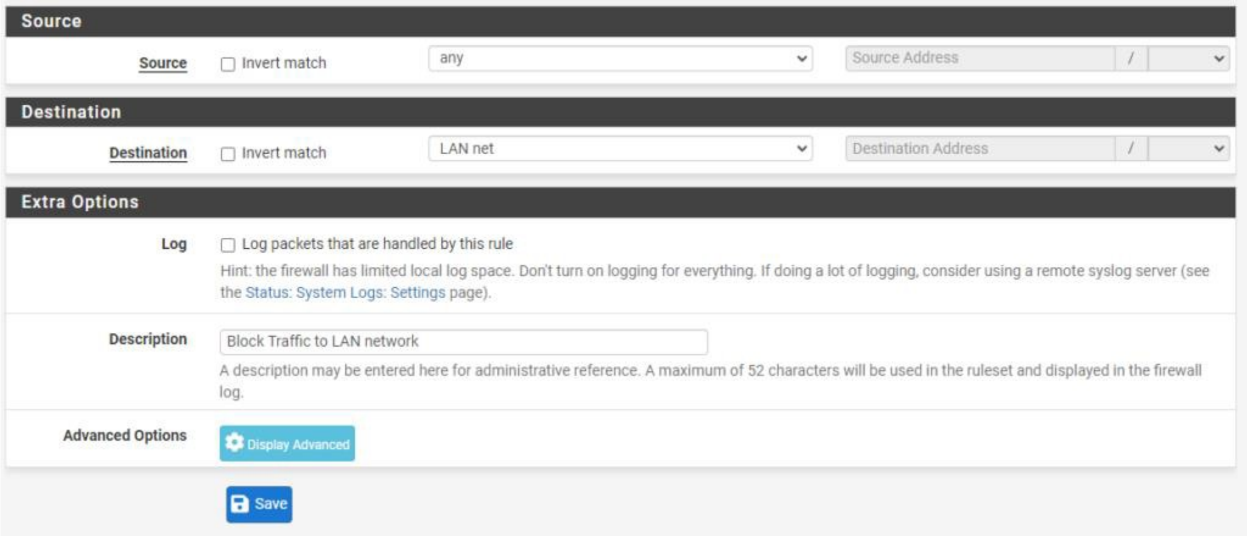


General Configuration

Enable	☑ Enable interface
Description	IoT 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 The MAC address of a VLAN interface must be set on its parent interface
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.

Verification and Troubleshooting:

- I reviewed firewall rules to ensure correct setup for traffic flow between VLANs.
- Checking for proper VLAN tagging on devices connected to VLAN-capable switches or Wi-Fi access points, I addressed any discrepancies.
- Examining the pfSense system and firewall logs for blocked packets, I troubleshooted connectivity issues, ensuring smooth operation.
- Addressing any IP address conflicts, I ensured each VLAN interface in pfSense had a unique subnet to prevent conflicts.



Source

Source □ Invert match any Source Address /

Destination

Destination □ Invert match LAN net Destination Address /

Extra Options

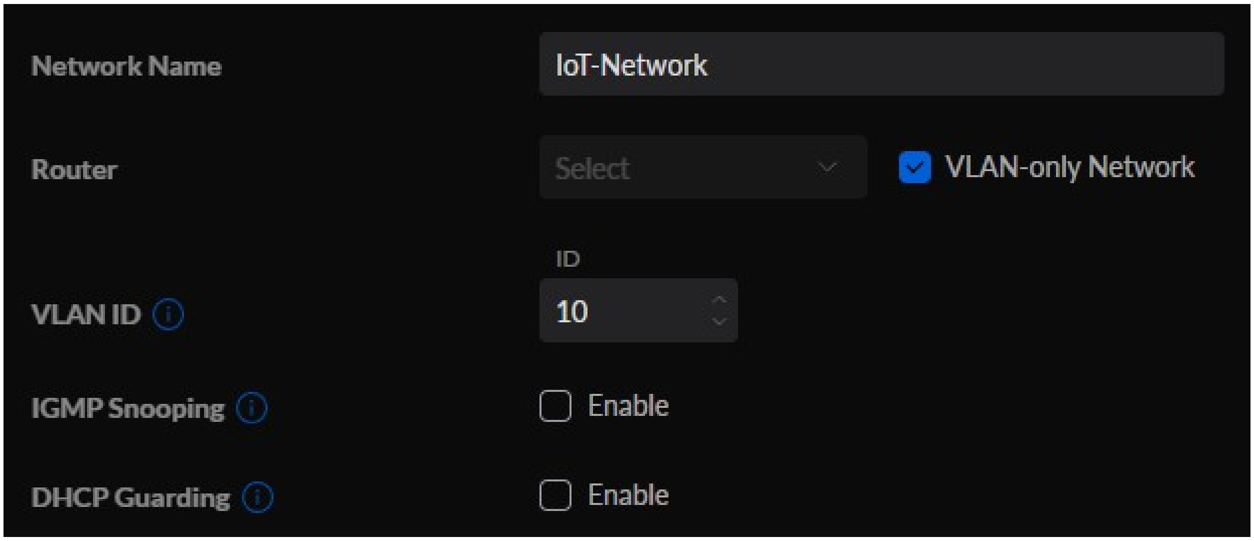
Log □ Log packets that are handled by this rule

Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).

Description: Block Traffic to LAN network

A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

Advanced Options



Network Name: IoT-Network

Router: Select ☑ VLAN-only Network

VLAN ID: ID 10

IGMP Snooping: □ Enable

DHCP Guarding: □ Enable

Firewall • Services •

Aliases

NAT

Rules

Schedules

Traffic Shaper

Virtual IPs

Firewall/ Rules/ IDT

Floallng WireGuard WAN LAN WG_VPN IOT

Rules (Drag to Change Order)

D	Stales	Protoccl	source	Port	Destination	Porl	oa1eway	Queue	schedule	oescrlpllon	Actions

No rules are currenUy defined for this Interface
All incoming connections on this interface will be blocked until pass rules are added Click the buUon lo add a new rule

mmmmlilDIEJ:iEIMI

Edit Firewall Rule

Action	Block 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 rt from the list.
Interface	IDT Choose the interlace from which packets must come to match this rule.
Address Family	1Pv4+1Pv6 Select the Internet Protocol version this rule applies to.
Protocol	Any Choose which IP protocol this rule should match.