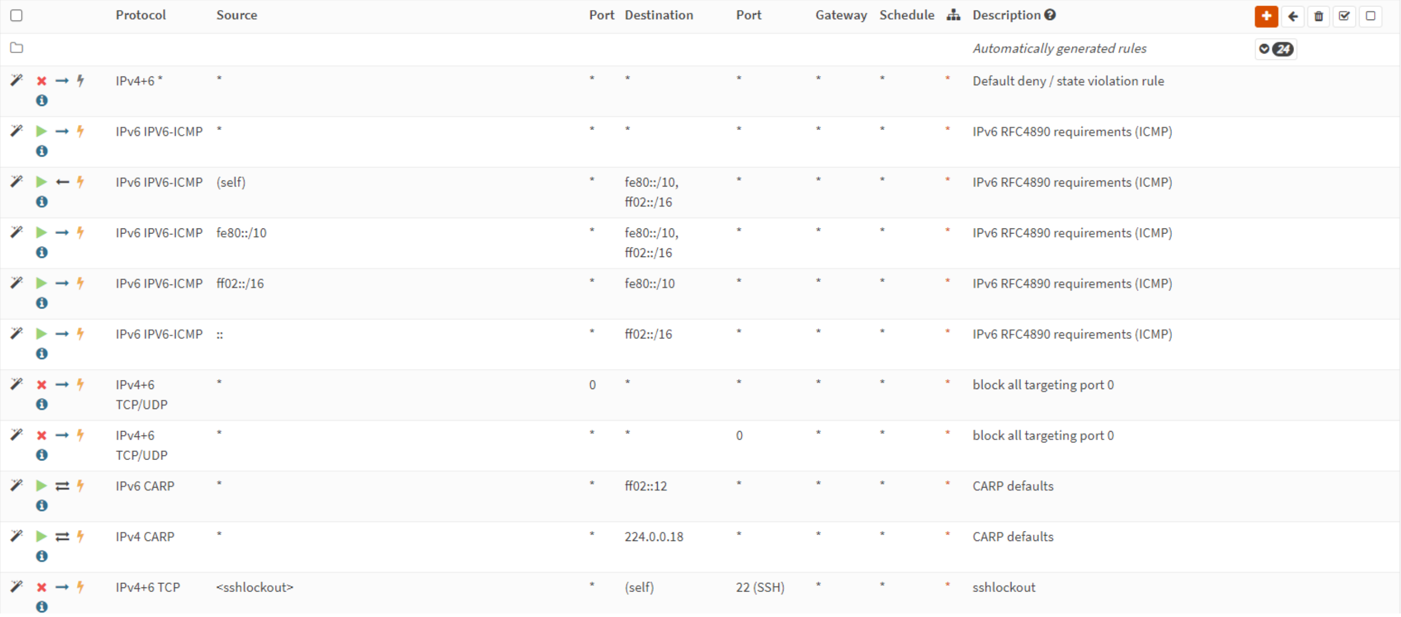
Firewall Configurations

Firewall Rules

Rules can be configured for each interface by navigating to the following page in your GUI...Firewall --> Rules --> Selected Interface. By default, OPNsense will generate sets of rules for each of your interfaces. You can clone, edit, delete, and rearrange the order of rules as desired. Here's an example of what my WAN rules look like:



□	Protocol	Source	Port	Destination	Port	Gateway	Schedule		Description ❓	
									Automatically generated rules	24
✗ → ℹ	IPv4+6 *	*	*	*	*	*	*	*	Default deny / state violation rule	
▶ → ℹ	IPv6 IPV6-ICMP	*	*	*	*	*	*	*	IPv6 RFC4890 requirements (ICMP)	
▶ ← ℹ	IPv6 IPV6-ICMP	(self)	*	fe80::/10, ff02::/16	*	*	*	*	IPv6 RFC4890 requirements (ICMP)	
▶ → ℹ	IPv6 IPV6-ICMP	fe80::/10	*	fe80::/10, ff02::/16	*	*	*	*	IPv6 RFC4890 requirements (ICMP)	
▶ → ℹ	IPv6 IPV6-ICMP	ff02::/16	*	fe80::/10	*	*	*	*	IPv6 RFC4890 requirements (ICMP)	
▶ → ℹ	IPv6 IPV6-ICMP	::	*	ff02::/16	*	*	*	*	IPv6 RFC4890 requirements (ICMP)	
✗ → ℹ	IPv4+6 TCP/UDP	*	0	*	*	*	*	*	block all targeting port 0	
✗ → ℹ	IPv4+6 TCP/UDP	*	*	*	0	*	*	*	block all targeting port 0	
▶ ⇄ ℹ	IPv6 CARP	*	*	ff02::12	*	*	*	*	CARP defaults	
▶ ⇄ ℹ	IPv4 CARP	*	*	224.0.0.18	*	*	*	*	CARP defaults	
✗ → ℹ	IPv4+6 TCP	<sshlockout>	*	(self)	22 (SSH)	*	*	*	sshlockout	

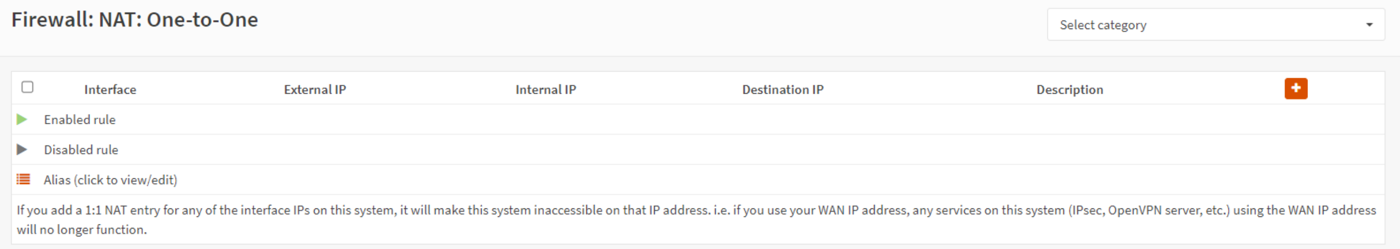
These are just a couple of rules out of the 24 that were generated. As of now, the only rules I've configured are for my LAN and homeLAB. I plan to host my NAS service with TrueNAS and am waiting on some SSDs to come in. Once I get it up and running, I'll update this page with rules accordingly.

Network Address Translation (NAT)

Another tab within the Firewall section is NAT, which allows you to configure and set up port forwarding. I'll most likely be using this more when I set up my NAS later this week.

In addition to port forwarding, you can configure rules for One-to-One connections, Outbound connections, and NPTv6:

One-to-One



Firewall: NAT: One-to-One

□	Interface	External IP	Internal IP	Destination IP	Description	+

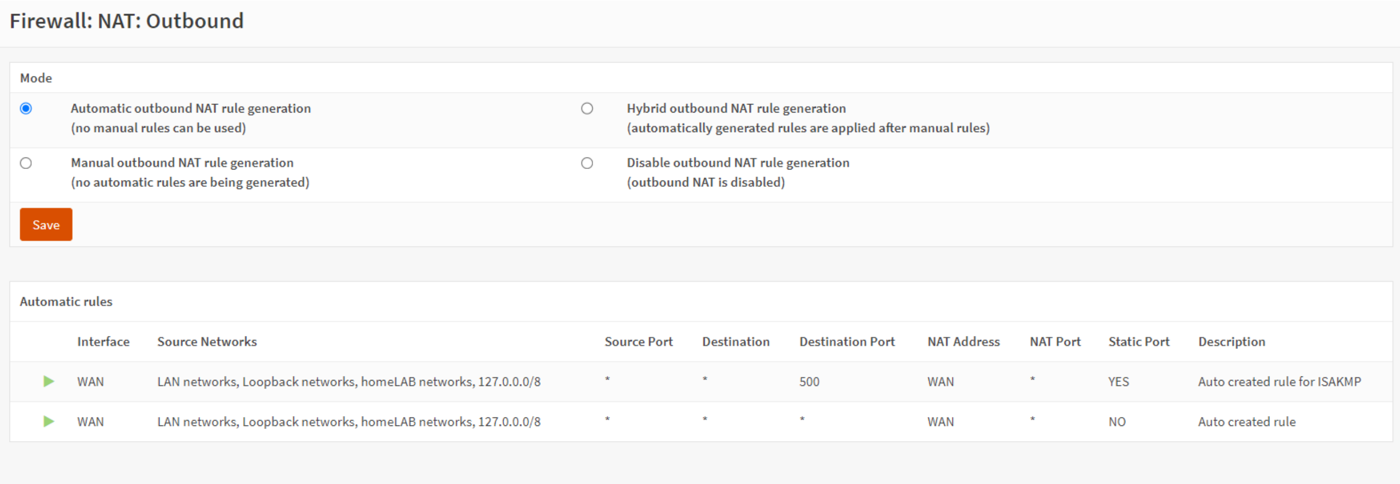
▶ Enabled rule

▶ 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.

Outbound



Firewall: NAT: Outbound

Mode

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

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

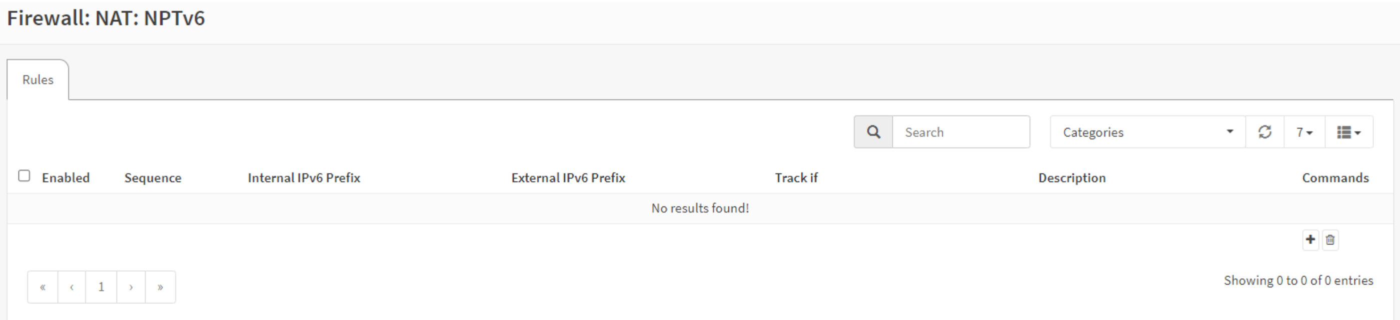
○ Manual outbound NAT rule generation
(no automatic rules are being generated)

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

Automatic rules

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

NPTv6



Firewall: NAT: NPTv6

□ Enabled	Sequence	Internal IPv6 Prefix	External IPv6 Prefix	Track if	Description	Commands
			No results found!			

Showing 0 to 0 of 0 entries