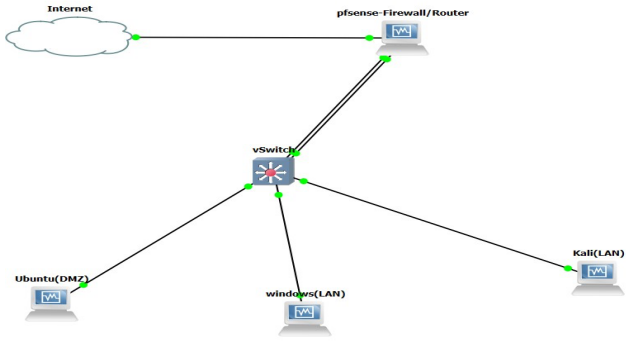
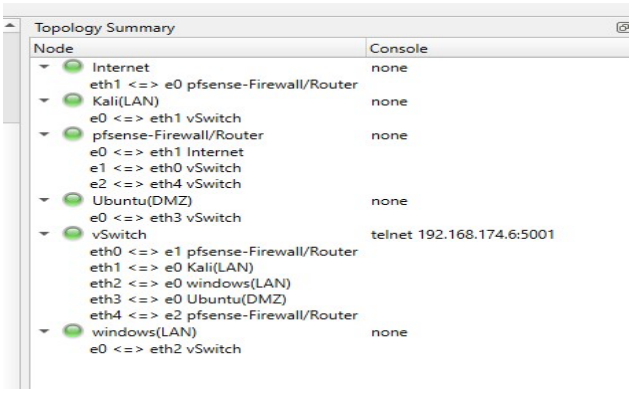
Network Environment Setup

1GNS3 Topology Diagram

The Comprehensive GNS3 design provides a depiction of the virtual network topology created using GNS3. The pfSense Router/Firewall in the centre of the design has three interfaces; the Internet cloud for WAN connections to the Internet, the LAN connection for all of the internal Hosts, and DMC (or the demilitarised zone) potentially connected to a uniquely configured Ubuntu Server. Other virtual devices have also been created to allow Kali Linux testing and allow the Ubuntu Server (DMC) to function as a testing platform. A summary panel of the Topology at the bottom of the design shows a comprehensive list of virtual appliances that were included in this lab environment along with the switches and where each is connected to the network. An illustration of the pfSense Console Menu from the virtual machine demonstrates what interface assignments have been applied to pfSense. The WAN (em0) interface receives its DHCP Address from the ISP Provider, while pfSense's LAN (em1) interface is configured with a Static IP Address range of 192.168.10.0/24. The OPT1 (em2) interface has been modified and now serves as the DMZ interface. The IP Address assigned to the OPT1 (em2) is 192.168.20.0/24. From the numerous interface assignments provided, the pfSense router has segmented the pfSense Router into three unique network zones; WAN, LAN, and DMZ.



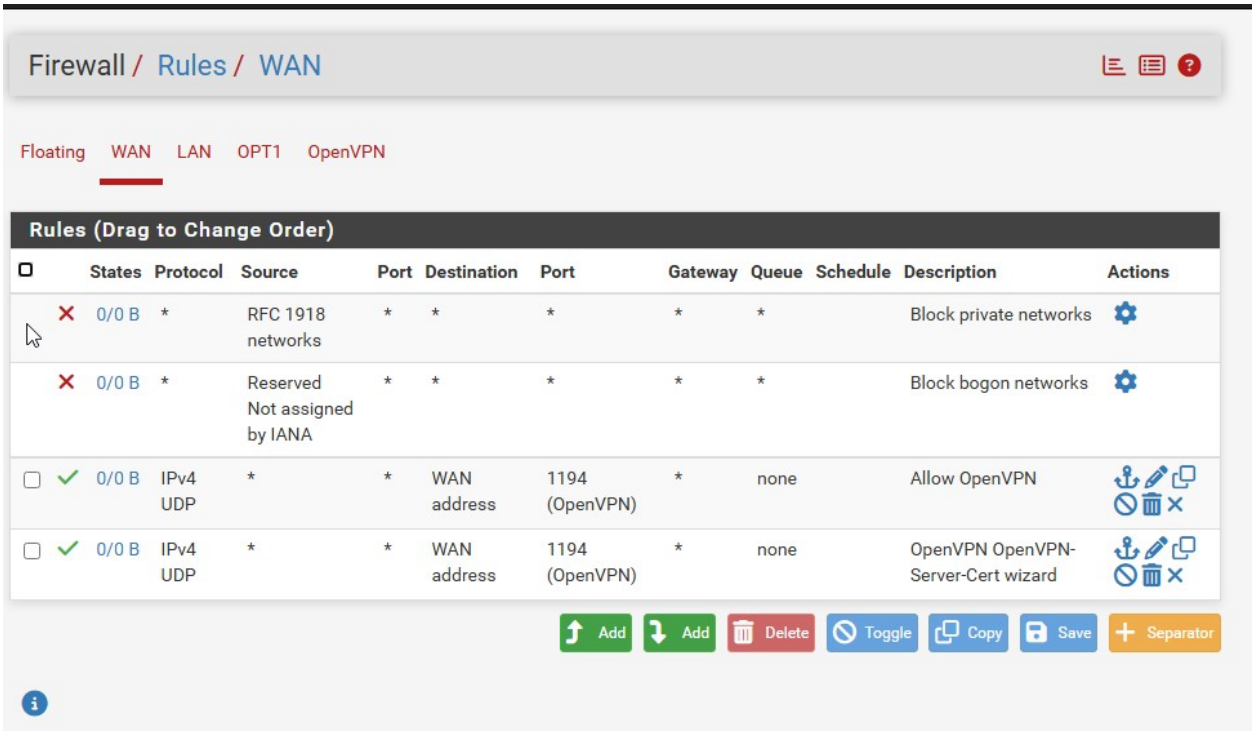


Network Design & Segmentation pfSense Interface Assignments

Firewall Configuration

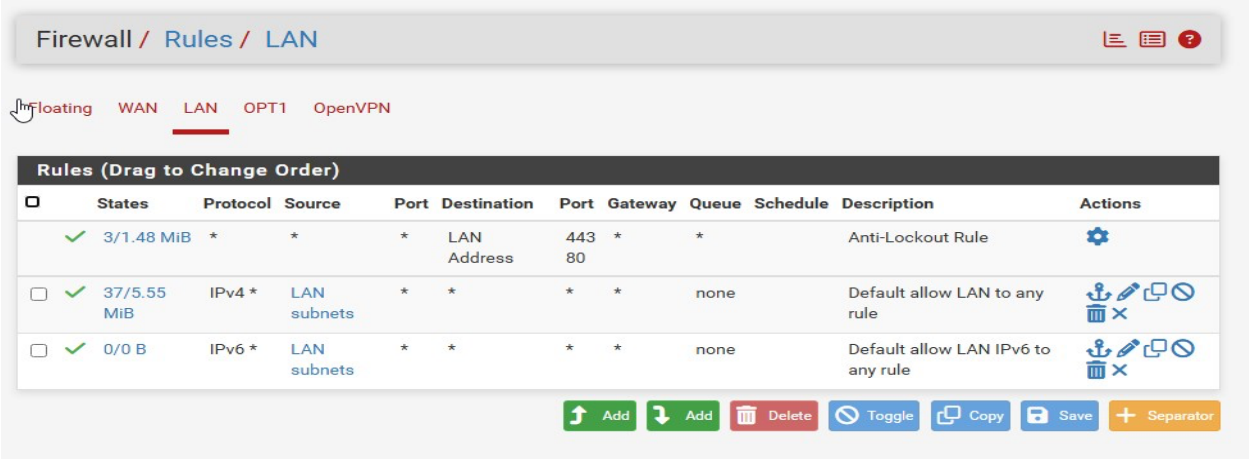
WAN Rule

WAN Rule: The top of the Firewall > Rules > WAN section of pfSense displays 2 specifically defined block rules to block access to the WAN interface by any private RFC1918 or bogon network. Underneath those 2 rules is a rule that allows all OpenVPN traffic over UDP port 1194 and the pfSense anti-lockout rule that allows access to the pfSense web) GUI and SSH from the LAN interface.

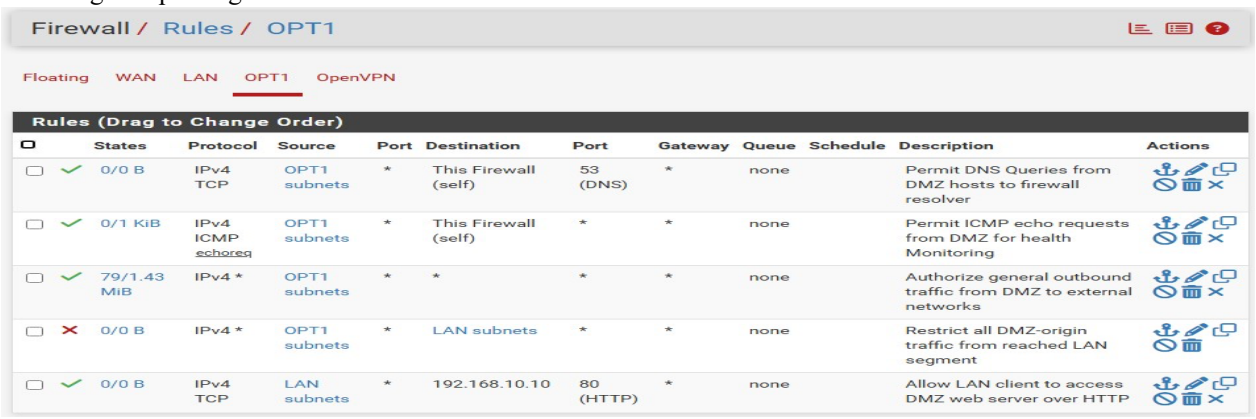


LAN Rule

LAN Rule: The Firewall > Rules > LAN interface shows the default permissive rules for the LAN segment. The top rule is the anti-lockout rule, followed by two default allow rules permitting any IPv4 and IPv6 traffic from LAN subnets to any destination, ensuring internal users have full outbound Internet access.

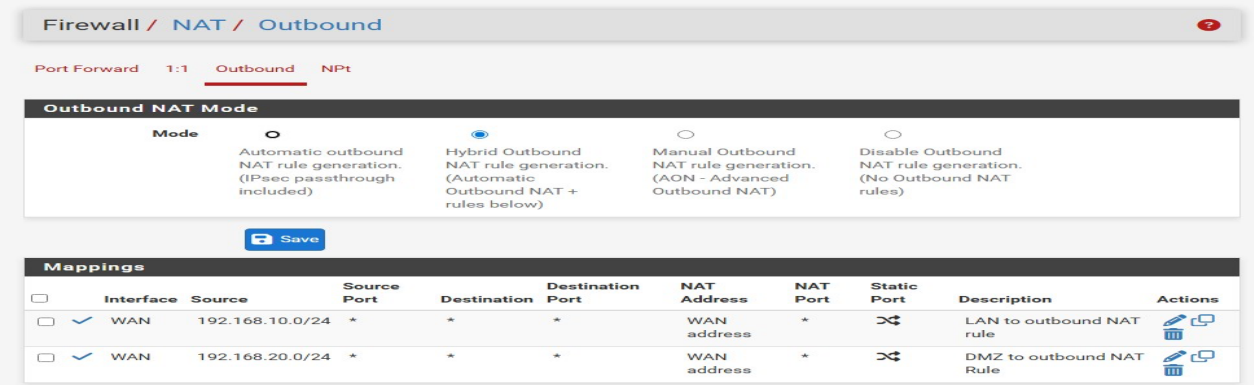


OPT(DMZ) Rule: The interface for Outbound Rules for OPT (DMZ) has many restrictive rules governing the services allowed from the OPT1 (DMZ) interface. Only DNS queries (port 53) sent to the Firewall itself are permitted, as well as health monitoring requests to external servers, outbound traffic from the DMZ to other networks, limited access to resources on the internal (LAN) network, and web access over HTTP and HTTPS – thus, enforcing leastprivilege for hosts located within a DMZ.



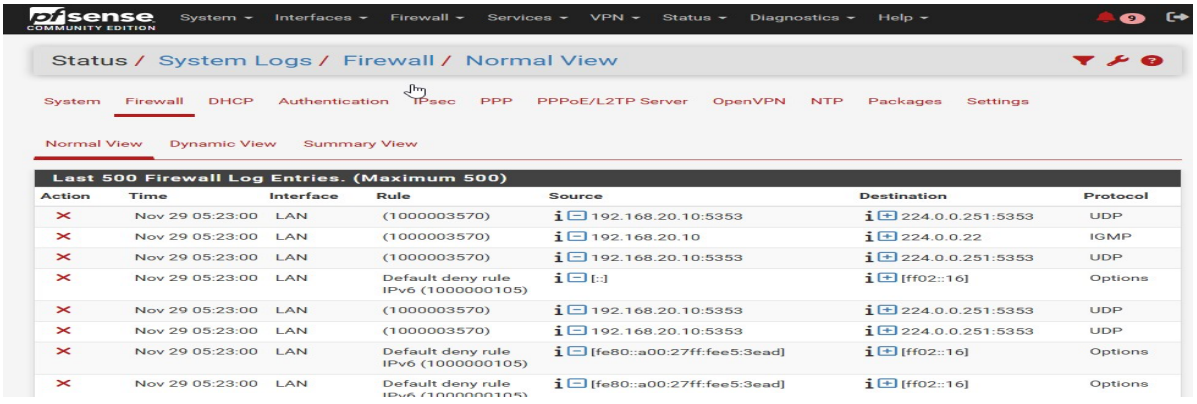
NAT Configuration

On the NAT Configuration page (Firewall > NAT > Outbound), the NAT Mode is set to Hybrid. There are two Manual Outbound NAT Rules created. The LAN Subnet (192.168.10.0/24) translates to a WAN Interface Address as do the DMZ Subnet (192.168.20.0/24) so that hosts on either the LAN or DMZ can access the Internet properly using Source Address Translation.



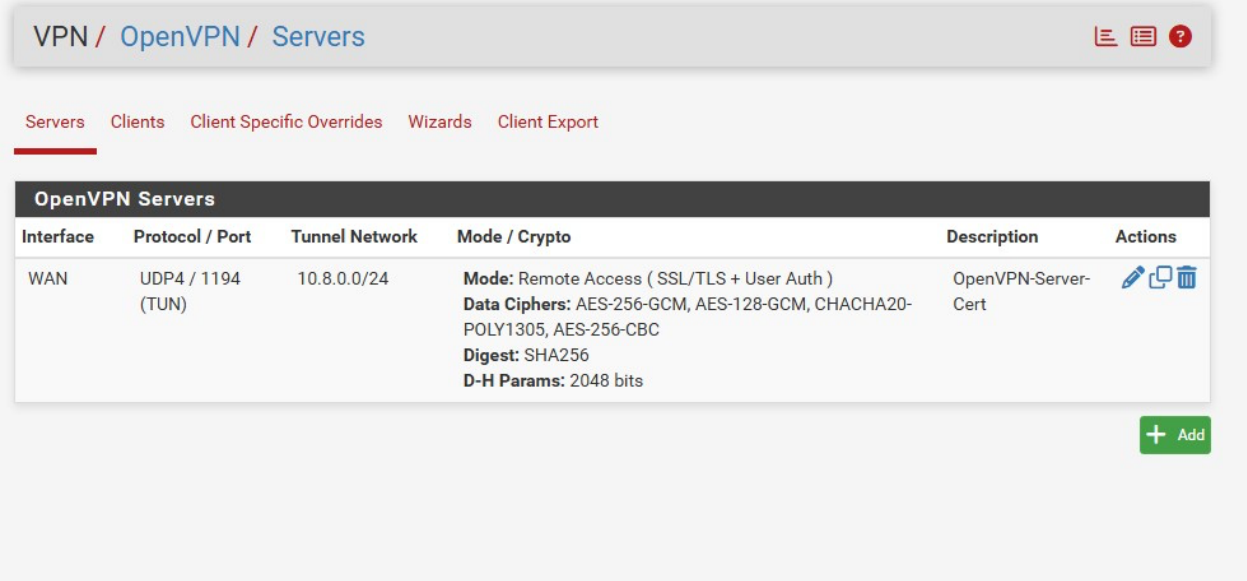
Showing blocked DMZ→LAN packets

VPN Applications Page: The Application > VPN > OpenVPN page displays a list of all configured VPN servers. The OpenVPN configuration specified by the provider will be automatically populated in this application after you have logged into your VPN provider (you must log into your VPN provider at least once) and created your OpenVPN account. Once you have created your OpenVPN account, you can then connect to your OpenVPN VPN server using an OpenVPN compliant client application or OpenVPN compatible router.



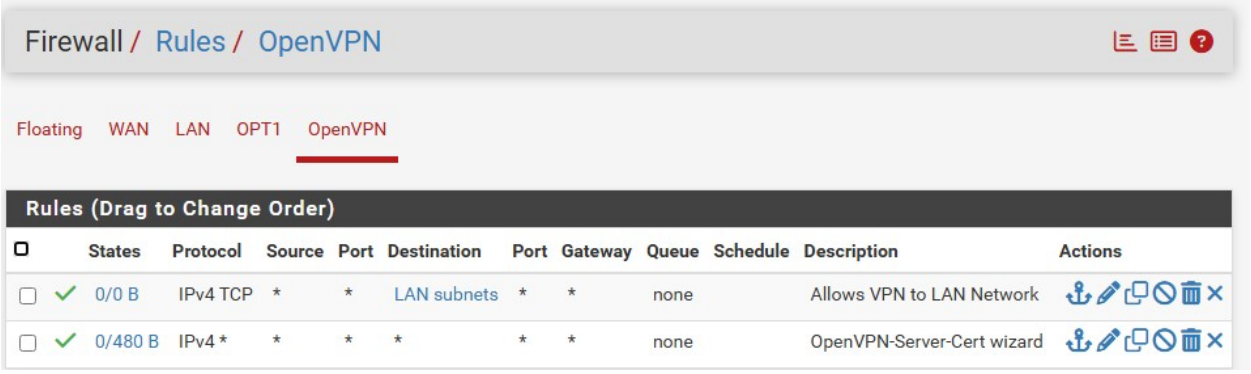
OpenVPN Server Settings Page

VPN Applications Page: The Application > VPN > OpenVPN page displays a list of all configured VPN servers. The OpenVPN configuration specified by the provider will be automatically populated in this application after you have logged into your VPN provider (you must log into your VPN provider at least once) and created your OpenVPN account. Once you have created your OpenVPN account, you can then connect to your OpenVPN VPN server using an OpenVPN compliant client application or OpenVPN compatible router.



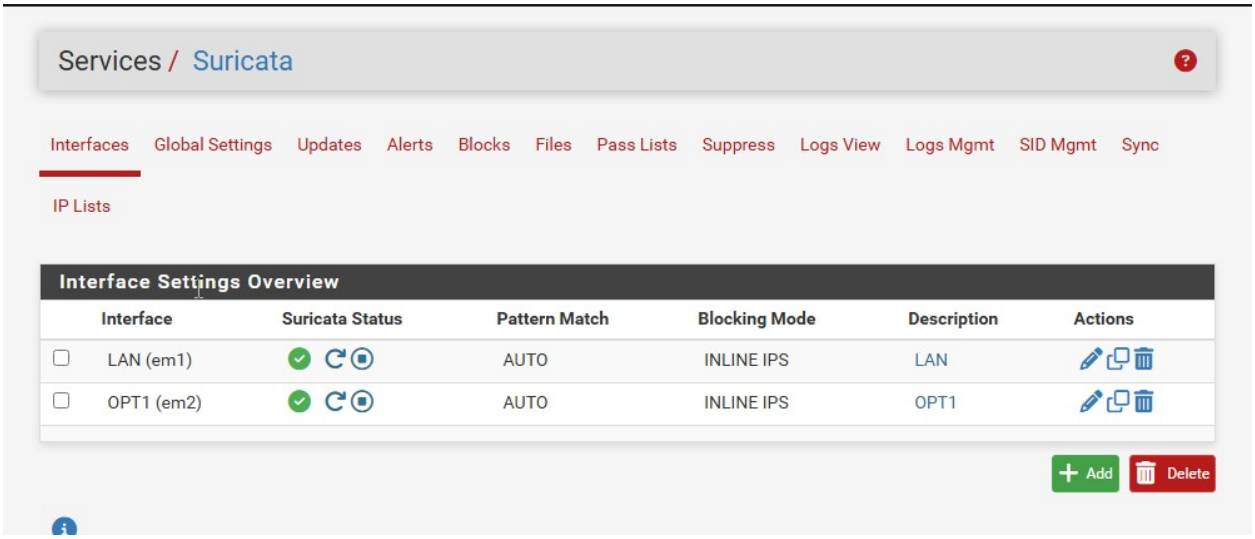
OpenVPN firewall rule

OpenVPN Firewall Configuration : You can use the Firewall page of the OpenVPN application to create a firewall rule that allows authenticated users to connect to your LAN from an OpenVPN connection. The default firewall rules created by the OpenVPN wizard will allow these users access to your LAN, along with the same privileges as users connected directly to your LAN.



Configure IDS/IPS I installed Suricata 11Suricata Installed Interfaces Page

Confirming Suricata Installation on Interfaces: Suricata has been installed and activated on both LAN (em1) and OPT1/DMZ (em2) networks in IPS Mode via the Inline IPS blocking method and will download the Emerging Threats Open ruleset automatically for the system's operation.



Suricata → LAN Rule Categories Page

Supported Rule Types by Suricata on the LAN Network: The image is only partially visible but indicates that there are many high-priority types of rules enabled, including rules related to malware, exploit kits, and Botnet C2 traffic, among others, which will provide excellent levels of threat detection and protection from attacks on the LAN segment of your computer systems.