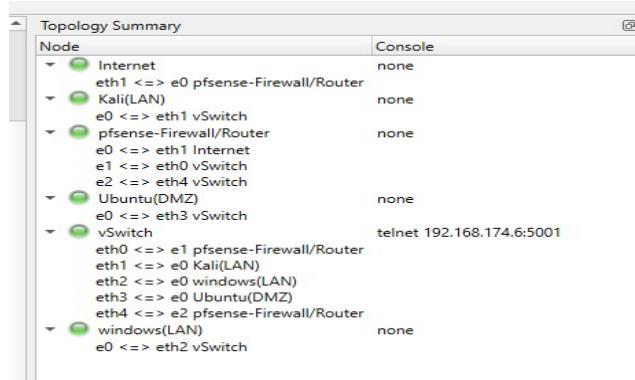
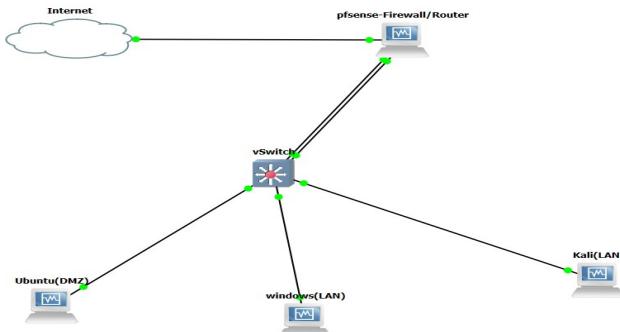


Network Environment Setup

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

```
FreeBSD/amd64 (pfSense.lab.local) (ttyv0)
VirtualBox Virtual Machine - Netgate Device ID: 03259eca7731c596fd09
*** Welcome to pfSense 2.8.1-RELEASE (amd64) on pfSense ***
WAN (wan)    -> em0    -> v4/DHCP4: 10.0.3.16/24
LAN (lan)    -> em1    -> v4: 192.168.10.1/24
OPT1 (opt1)  -> em2    -> v4: 192.168.20.1/24

0) Logout / Disconnect SSH      9) pfTop
1) Assign Interfaces           10) Filter Logs
2) Set interface(s) IP address 11) Restart GUI
3) Reset admin account and password 12) PHP shell + pfSense tools
4) Reset to factory defaults   13) Update from console
5) Reboot system               14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option: [
```

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.

The screenshot shows the Firewall > Rules > WAN page. At the top, there are tabs for Floating, WAN, LAN, OPT1, and OpenVPN. The WAN tab is selected. Below the tabs is a table titled "Rules (Drag to Change Order)". The table has columns for State, Protocol, Source, Port, Destination, Port, Gateway, Queue, Schedule, Description, and Actions. There are five rows in the table:

State	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
X 0/0 B *		RFC 1918 networks	*	*	*	*	*		Block private networks	
X 0/0 B *		Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	
<input type="checkbox"/> ✓ 0/0 B IPv4 UDP	*		*	WAN address	1194 (OpenVPN)	*	none		Allow OpenVPN	
<input type="checkbox"/> ✓ 0/0 B IPv4 UDP	*		*	WAN address	1194 (OpenVPN)	*	none		OpenVPN OpenVPN-Server-Cert wizard	

At the bottom of the table are buttons for Add, Delete, Toggle, Copy, Save, and Separator. A small information icon is located at the bottom left of the page.

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.

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/> 3/1.48 MiB	*	*	*	LAN Address	443 80	*	*	*	Anti-Lockout Rule	
<input type="checkbox"/> <input checked="" type="checkbox"/> 37/5.55 MiB	IPv4 *	LAN subnets	*	*	*	*	none		Default allow LAN to any rule	
<input type="checkbox"/> <input checked="" type="checkbox"/> 0/0 B	IPv6 *	LAN subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	

Buttons at the bottom: Add (up), Add (down), Delete, Toggle, Copy, Save, Separator.

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.

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/> <input checked="" type="checkbox"/> 0/0 B	IPv4 TCP	OPT1 subnets	*	This Firewall (self)	53 (DNS)	*	none		Permit DNS Queries from DMZ hosts to firewall resolver	
<input type="checkbox"/> <input checked="" type="checkbox"/> 0/1 KIB	IPv4 ICMP echoreq	OPT1 subnets	*	This Firewall (self)	*	*	none		Permit ICMP echo requests from DMZ for health Monitoring	
<input type="checkbox"/> <input checked="" type="checkbox"/> 79/1.43 MiB	IPv4 *	OPT1 subnets	*	*	*	*	none		Authorize general outbound traffic from DMZ to external networks	
<input type="checkbox"/> <input checked="" type="checkbox"/> 0/0 B	IPv4 *	OPT1 subnets	*	LAN subnets	*	*	none		Restrict all DMZ-origin traffic from reached LAN segment	
<input type="checkbox"/> <input checked="" type="checkbox"/> 0/0 B	IPv4 TCP	LAN subnets	*	192.168.10.10	80 (HTTP)	*	none		Allow LAN client to access DMZ web server over HTTP	

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.

The screenshot shows the 'Outbound NAT Mode' section with four options: Automatic outbound NAT rule generation (selected), Hybrid Outbound NAT rule generation, Manual Outbound NAT rule generation, and Disable Outbound NAT rule generation. Below this is the 'Mappings' table:

Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description	Actions
WAN	192.168.10.0/24	*	*	*	WAN address	*	iox	LAN to outbound NAT rule	
WAN	192.168.20.0/24	*	*	*	WAN address	*	iox	DMZ to outbound NAT Rule	

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.

The screenshot shows the 'Normal View' of the Firewall Log. The table displays the last 500 log entries:

Action	Time	Interface	Rule	Source	Destination	Protocol
✗	Nov 29 05:23:00	LAN	(1000003570)	i [192.168.20.10:5353]	i [224.0.0.251:5353]	UDP
✗	Nov 29 05:23:00	LAN	(1000003570)	i [192.168.20.10]	i [224.0.0.22]	IGMP
✗	Nov 29 05:23:00	LAN	(1000003570)	i [192.168.20.10:5353]	i [224.0.0.251:5353]	UDP
✗	Nov 29 05:23:00	LAN	Default deny rule IPv6 (1000000105)	i [:]	i [ff02::16]	Options
✗	Nov 29 05:23:00	LAN	(1000003570)	i [192.168.20.10:5353]	i [224.0.0.251:5353]	UDP
✗	Nov 29 05:23:00	LAN	(1000003570)	i [192.168.20.10:5353]	i [224.0.0.251:5353]	UDP
✗	Nov 29 05:23:00	LAN	Default deny rule IPv6 (1000000105)	i [fe80::a0:27ff:fee5:3ead]	i [ff02::16]	Options
✗	Nov 29 05:23:00	LAN	Default deny rule IPv6 (1000000105)	i [fe80::a0:27ff:fee5:3ead]	i [ff02::16]	Options

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.

The screenshot shows the 'OpenVPN / Servers' page. At the top, there are tabs for 'Servers' (which is selected), 'Clients', 'Client Specific Overrides', 'Wizards', and 'Client Export'. Below the tabs is a table titled 'OpenVPN Servers' with the following data:

Interface	Protocol / Port	Tunnel Network	Mode / Crypto	Description	Actions
WAN	UDP4 / 1194 (TUN)	10.8.0.0/24	Mode: Remote Access (SSL/TLS + User Auth) Data Ciphers: AES-256-GCM, AES-128-GCM, CHACHA20-POLY1305, AES-256-CBC Digest: SHA256 D-H Params: 2048 bits	OpenVPN-Server-Cert	

At the bottom right of the table area is a green 'Add' button with a plus sign.

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.

The screenshot shows the 'Firewall / Rules / OpenVPN' page. At the top, there are tabs for 'Floating', 'WAN', 'LAN', 'OPT1', and 'OpenVPN' (which is selected). Below the tabs is a table titled 'Rules (Drag to Change Order)' with the following data:

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
0/0 B	IPv4 TCP	*	*	LAN subnets	*	*	none		Allows VPN to LAN Network	
0/480 B	IPv4 *	*	*	*	*	*	none		OpenVPN-Server-Cert wizard	

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.

Interface	Suricata Status	Pattern Match	Blocking Mode	Description	Actions
<input type="checkbox"/> LAN (em1)	✓	AUTO	INLINE IPS	LAN	
<input type="checkbox"/> OPT1 (em2)	✓	AUTO	INLINE IPS	OPT1	

Add Delete

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.

Category	app-layer-events.rules	View All							
Select the rule category to view and manage.									
SID Actions	Apply	Reset All	Reset Current	Disable All	Enable All				
When finished, click APPLY to save and send any SID state/action changes made on this tab to Suricata.									
Rules View Filter									
Rule Signature ID (SID) Enable/Disable Overrides									
Legend: ✓ Default Enabled ✓ Enabled by user ✓ Auto-enabled by SID Mgmt ⚠ Action/content modified by SID Mgmt ⚠ Rule action is alert ✓ Rule contains noalert option ✗ Default Disabled ✗ Disabled by user ✗ Auto-disabled by SID Mgmt ✗ Rule action is drop ✗ Rule action is reject									
State	Action	GID	SID	Proto	Source	SPort	Destination	DPort	Message
✓	⚠	1	2260000	ip	any	any	any	any	SURICATA Applayer Mismatch protocol both directions
✓	⚠	1	2260001	ip	any	any	any	any	SURICATA Applayer Wrong direction first Data
✓	⚠	1	2260002	ip	any	any	any	any	SURICATA Applayer Detect protocol only one direction
✓	⚠	1	2260003	ip	any	any	any	any	SURICATA Applayer Protocol detection skipped
✓	⚠	1	2260004	tcp	any	any	any	any	SURICATA Applayer No TLS after STARTTLS
✓	⚠	1	2260005	tcp	any	any	any	any	SURICATA Applayer Unexpected protocol

Total Rules: 6 Default Enabled: 6 Default Disabled: 0 User Enabled: 0 User Disabled: 0 Auto-Managed: 0