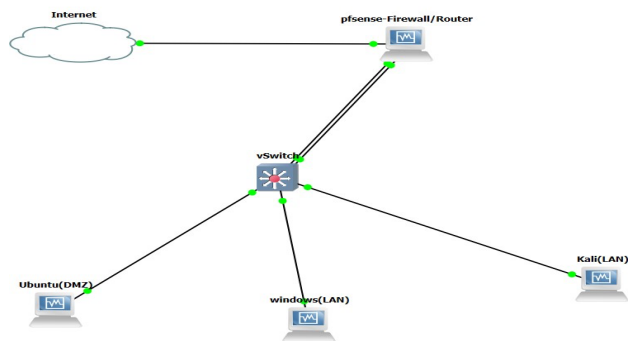


Network Environment Setup

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 DMZ (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.



Topology Summary	
Node	Console
Internet	none
eth1 <=> e0 pfSense-Firewall/Router	
Kali(LAN)	none
e0 <=> eth1 vSwitch	
pfSense-Firewall/Router	none
e0 <=> eth1 Internet	
e1 <=> eth0 vSwitch	
e2 <=> eth4 vSwitch	
Ubuntu(DMZ)	none
e0 <=> eth3 vSwitch	
vSwitch	telnet 192.168.174.6:5001
eth0 <=> e1 pfSense-Firewall/Router	
eth1 <=> e0 Kali(LAN)	
eth2 <=> e0 windows(LAN)	
eth3 <=> e0 Ubuntu(DMZ)	
eth4 <=> e2 pfSense-Firewall/Router	
windows(LAN)	none
e0 <=> eth2 vSwitch	

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.

Firewall / Rules / WAN

Floating **WAN** LAN OPT1 OpenVPN

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	0/0 B	*	RFC 1918 networks	*	*	*	*	*		Block private networks	
<input checked="" type="checkbox"/>	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	

Add Add Delete Toggle Copy Save Separator

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.

Firewall / Rules / LAN											
Floating WAN LAN OPT1 OpenVPN											
Rules (Drag to Change Order)											
<input type="checkbox"/>	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"/>	37/5.55 MiB	IPv4 *	LAN subnets	*	*	*	*	none		Default allow LAN to any rule	
<input type="checkbox"/>	0/0 B	IPv6 *	LAN subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	
Add Add 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.

Firewall / Rules / OPT1											
Floating WAN LAN OPT1 OpenVPN											
Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input 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"/>	0/1 KiB	IPv4 ICMP echo req	OPT1 subnets	*	This Firewall (self)	*	*	none		Permit ICMP echo requests from DMZ for health Monitoring	
<input type="checkbox"/>	79/1.43 MiB	IPv4 *	OPT1 subnets	*	*	*	*	none		Authorize general outbound traffic from DMZ to external networks	
<input type="checkbox"/>	0/0 B	IPv4 *	OPT1 subnets	*	LAN subnets	*	*	none		Restrict all DMZ-origin traffic from reached LAN segment	
<input 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.

Firewall / NAT / Outbound

Port Forward 1:1 Outbound NPT

Outbound NAT Mode

Mode

- ☐ Automatic outbound NAT rule generation. (IPsec passthrough included)
- ☒ Hybrid Outbound NAT rule generation. (Automatic Outbound NAT + rules below)
- ☐ Manual Outbound NAT rule generation. (AON - Advanced Outbound NAT)
- ☐ Disable Outbound NAT rule generation. (No Outbound NAT rules)

[Save](#)

Mappings

<input type="checkbox"/>	Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description	Actions
<input type="checkbox"/>	<input checked="" type="checkbox"/> WAN	192.168.10.0/24	*	*	*	WAN address	*	<input checked="" type="checkbox"/>	LAN to outbound NAT rule	Edit Delete
<input type="checkbox"/>	<input checked="" type="checkbox"/> WAN	192.168.20.0/24	*	*	*	WAN address	*	<input checked="" type="checkbox"/>	DMZ to outbound NAT Rule	Edit Delete

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.

Pfsense COMMUNITY EDITION

System Interfaces Firewall Services VPN Status Diagnostics Help

Status / System Logs / Firewall / Normal View

System Firewall DHCP Authentication IPsec PPP PPPoE/L2TP Server OpenVPN NTP Packages Settings

Normal View Dynamic View Summary View

Last 500 Firewall Log Entries. (Maximum 500)

Action	Time	Interface	Rule	Source	Destination	Protocol
×	Nov 29 05:23:00	LAN	(1000003570)	192.168.20.10:5353	224.0.0.251:5353	UDP
×	Nov 29 05:23:00	LAN	(1000003570)	192.168.20.10	224.0.0.22	IGMP
×	Nov 29 05:23:00	LAN	(1000003570)	192.168.20.10:5353	224.0.0.251:5353	UDP
×	Nov 29 05:23:00	LAN	Default deny rule IPv6 (1000000105)	[::]	[:::16]	Options
×	Nov 29 05:23:00	LAN	(1000003570)	192.168.20.10:5353	224.0.0.251:5353	UDP
×	Nov 29 05:23:00	LAN	(1000003570)	192.168.20.10:5353	224.0.0.251:5353	UDP
×	Nov 29 05:23:00	LAN	Default deny rule IPv6 (1000000105)	[fe80::a00:27ff:fee5:3ead]	[:::16]	Options
×	Nov 29 05:23:00	LAN	Default deny rule IPv6 (1000000105)	[fe80::a00:27ff:fee5:3ead]	[:::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.

[VPN](#) / [OpenVPN](#) / [Servers](#)

[Servers](#) [Clients](#) [Client Specific Overrides](#) [Wizards](#) [Client Export](#)

OpenVPN Servers

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	  

 Add










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.

[Firewall](#) / [Rules](#) / [OpenVPN](#)

[Floating](#) [WAN](#) [LAN](#) [OPT1](#) [OpenVPN](#)

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓	0/0 B	IPv4 TCP	*	*	LAN subnets	*	*	none	Allows VPN to LAN Network	    
<input type="checkbox"/>	✓	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.

Services / Suricata

Interfaces

Global Settings

Updates

Alerts

Blocks

Files

Pass Lists

Suppress

Logs View

Logs Mgmt

SID Mgmt

Sync

IP Lists

Interface Settings Overview

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

+ 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.

LAN Settings

LAN Categories

LAN Rules

LAN Flow/Stream

LAN App Parsers

LAN Variables

LAN IP Rep

Available Rule Categories

Category

app-layer-events.rules

Select the rule category to view and manage.

View All

Rule Signature ID (SID) Enable/Disable Overrides

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
<div></div>	<div></div>	1	2260000	ip	any	any	any	any	SURICATA Applayer Mismatch protocol both directions
<div></div>	<div></div>	1	2260001	ip	any	any	any	any	SURICATA Applayer Wrong direction first Data
<div></div>	<div></div>	1	2260002	ip	any	any	any	any	SURICATA Applayer Detect protocol only one direction
<div></div>	<div></div>	1	2260003	ip	any	any	any	any	SURICATA Applayer Protocol detection skipped
<div></div>	<div></div>	1	2260004	tcp	any	any	any	any	SURICATA Applayer No TLS after STARTTLS
<div></div>	<div></div>	1	2260005	tcp	any	any	any	any	SURICATA Applayer Unexpected protocol

Category Rules Summary

Total Rules: 6

Default Enabled: 6

Default Disabled: 0

User Enabled: 0

User Disabled: 0

Auto-Managed: 0