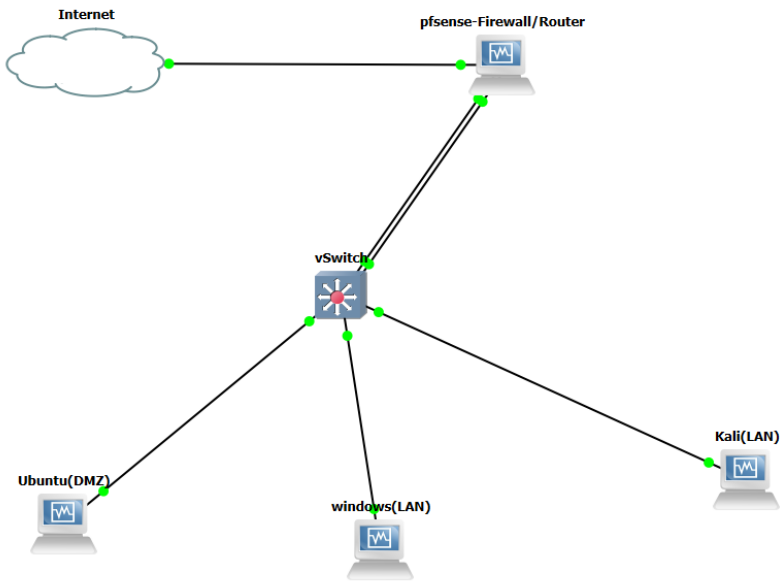
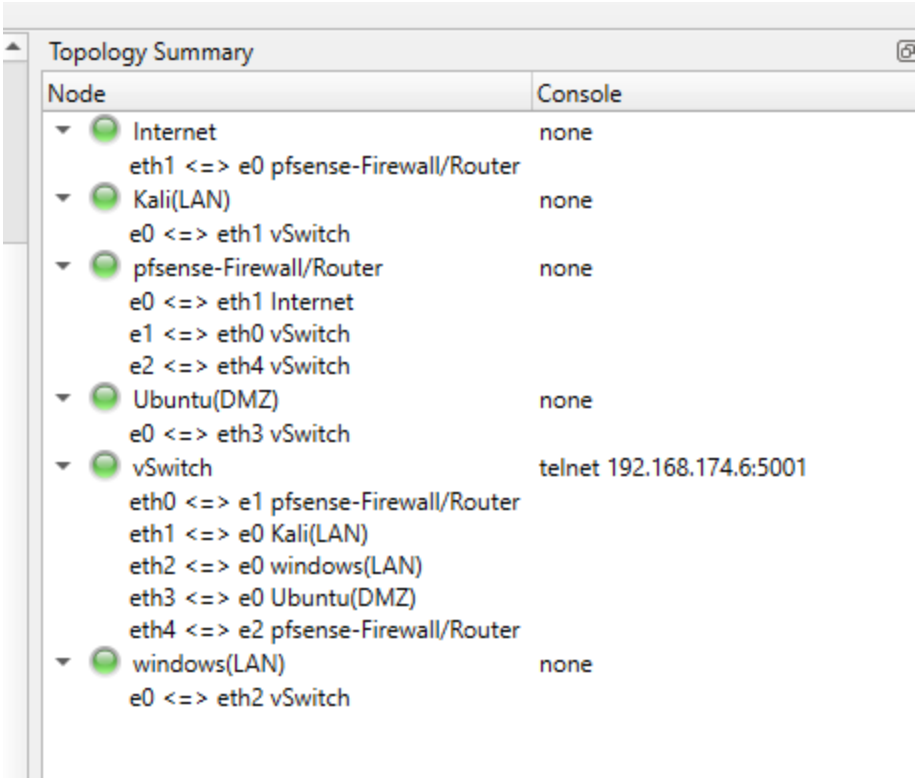
SECTION 1 — Network Environment Setup

GNS3 Topology Diagram

1. GNS3 Network Diagram

The GNS3 Network Diagram is an example of a properly designed lab topology used to simulate a small enterprise network comprising of a pfSense router/firewall at the centre of the topology with three separate interfaces; The WAN interface connects the pfSense router to the internet as well as private IP addresses located on the LAN segment, which contains all of the internal devices connected to the LAN segment, including two Kali Linux and Windows Workstations, and one of these is configured with a DMZ interface, which connects to an external user via an Internet WAN cloud. In addition, Virtual Switching provides connectivity between all devices within the topology and verifies that all interfaces are properly configured (i.e. eth0 → WAN, eth1 → LAN, and eth2 → DMZ) through the Topology Summary tab in GNS3. Furthermore, as reflected in this topology design, all public-facing services, Internal users and the Internet are clearly separated, providing the ideal basis for creating and testing a Secure





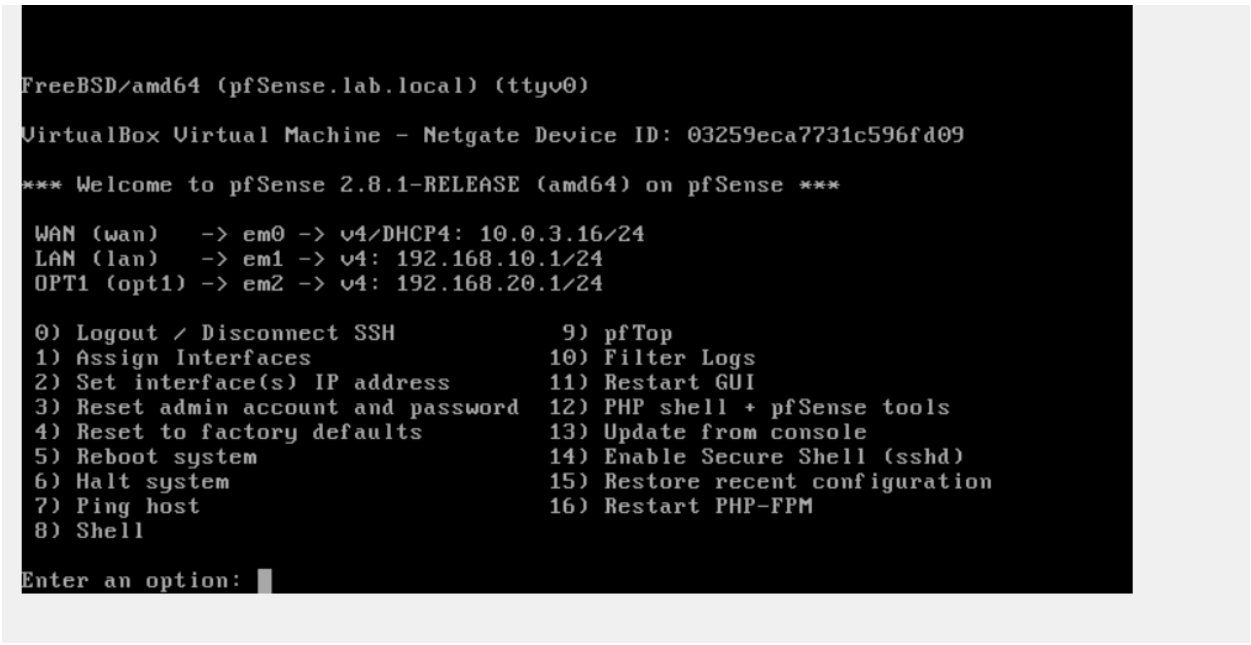
SECTION 2 — Network Design & Segmentation

The console menu of pfSense reflects a WAN interface connected to Internet using DHCP (em0), LAN interface using static ip of 192.168.10.0/24, and an Optional interface (em2) of 192.168.20.0/24. Later, Optional interface was named DMZ to represent fact that it is now holding devices with lower-trust levels devices connected to LAN. With three network interfaces, pfSense is able to enforce granular policies by segmenting trusted LANs, semi-trusted DMZs and untrusted WANS, which reflects best practices of network zoning.

In addition, the DMZ contains a terminal output of Ubuntu Server confirming it is receiving the static IP address of 192.168.20.10/24 and pfSense's DMZ Gateway is configured to default route of 192.168.20.1. indicates that either the static configuration or DHCP configuration completes within isolated DMZ.

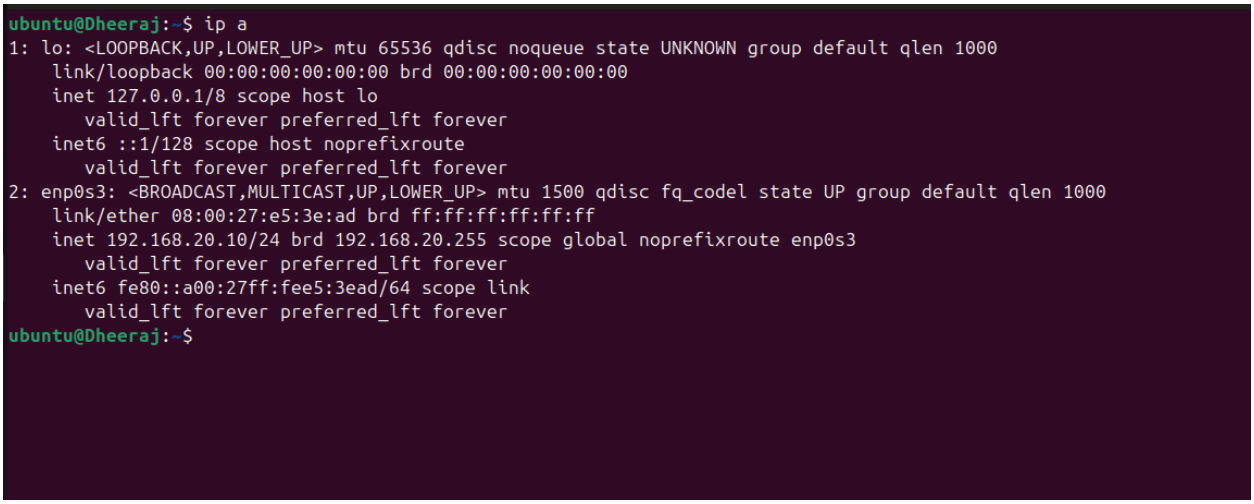
Lastly, Ubuntu Server in DMZ has achieved multiple successful Ping results across multiple segments and Internet connectivity by successfully pinging pfSense DMZ Gateway (192.168.20.1) and Google Public DNS (8.8.8.8). This confirms outbound Internet access from DMZ. This test confirms that IP reachability is working properly, NAT is working correctly, and that Kali system has successfully pinged a Windows host on the LAN.

pfSense Interface Assignments



Ubuntu DMZ IP (ip a)

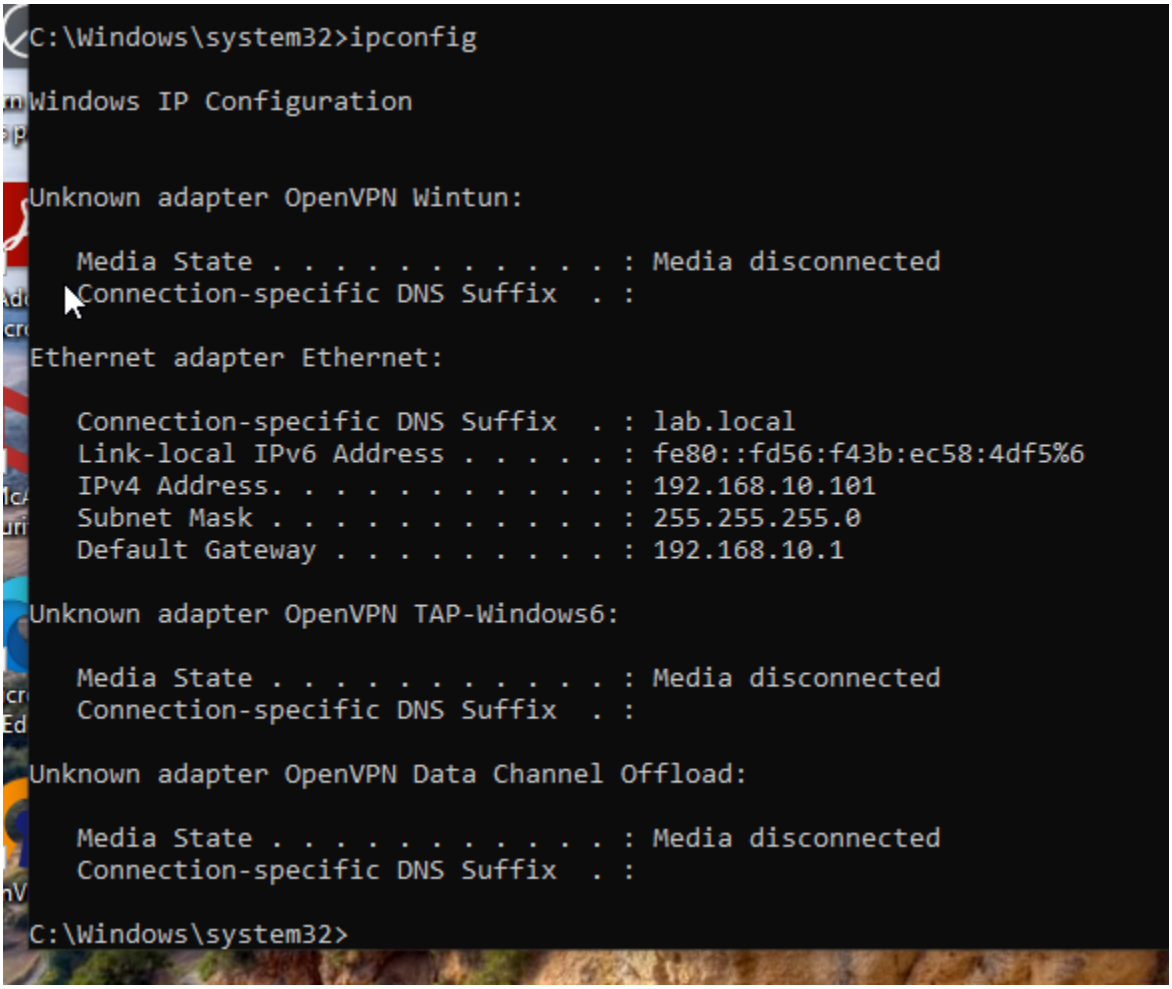
Showing: 192.168.20.10/24



Kali LAN

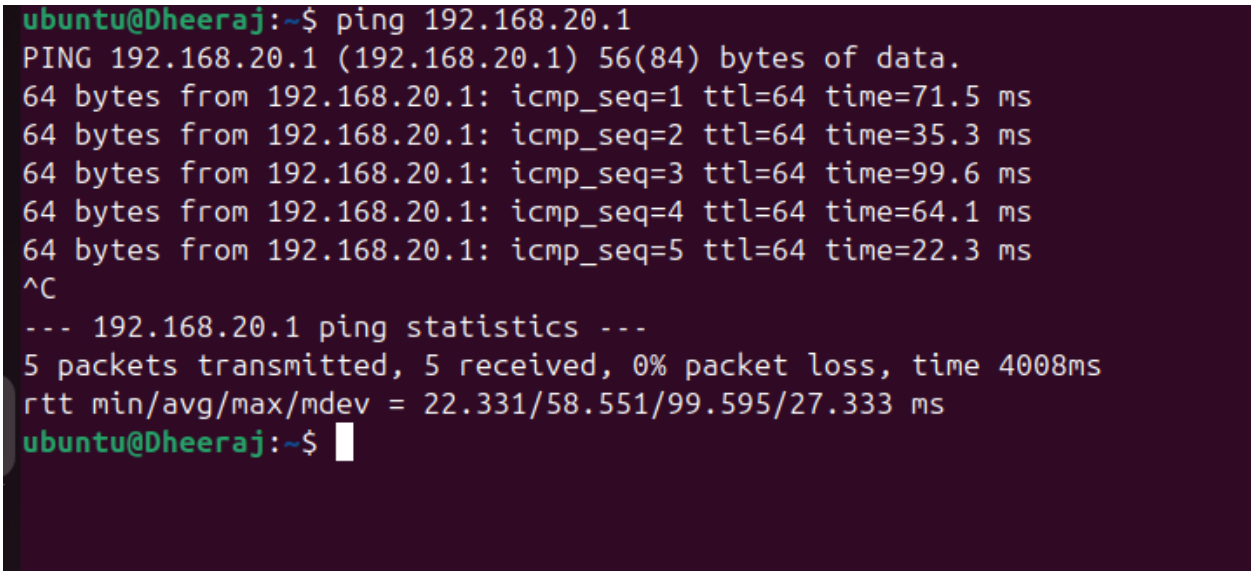
```
┌──(kali㉿Raj)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:1f:b7:23 brd ff:ff:ff:ff:ff:ff
    inet 192.168.10.100/24 brd 192.168.10.255 scope global dynamic noprefixroute eth0
       valid_lft 6715sec preferred_lft 6715sec
    inet6 fe80::dc08:831:24f:12cc/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

┌──(kali㉿Raj)-[~]
└─$
```

Windows LAN IP

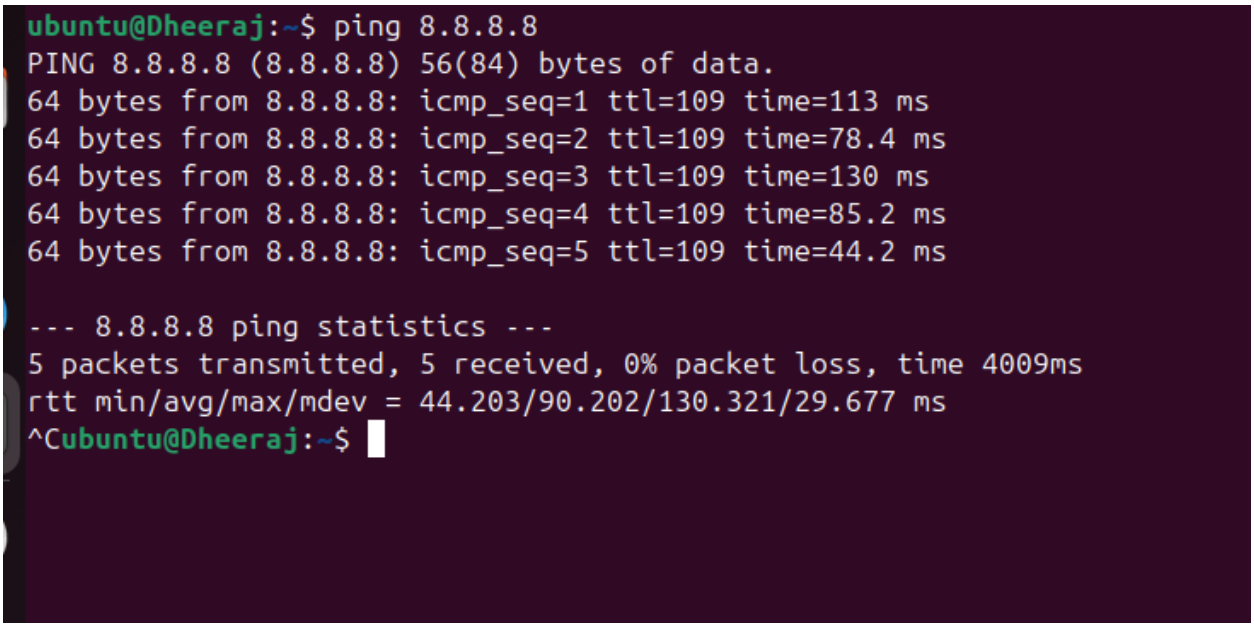


Ping tests between segments:

Ubuntu → pfSense DMZ (192.168.20.1)



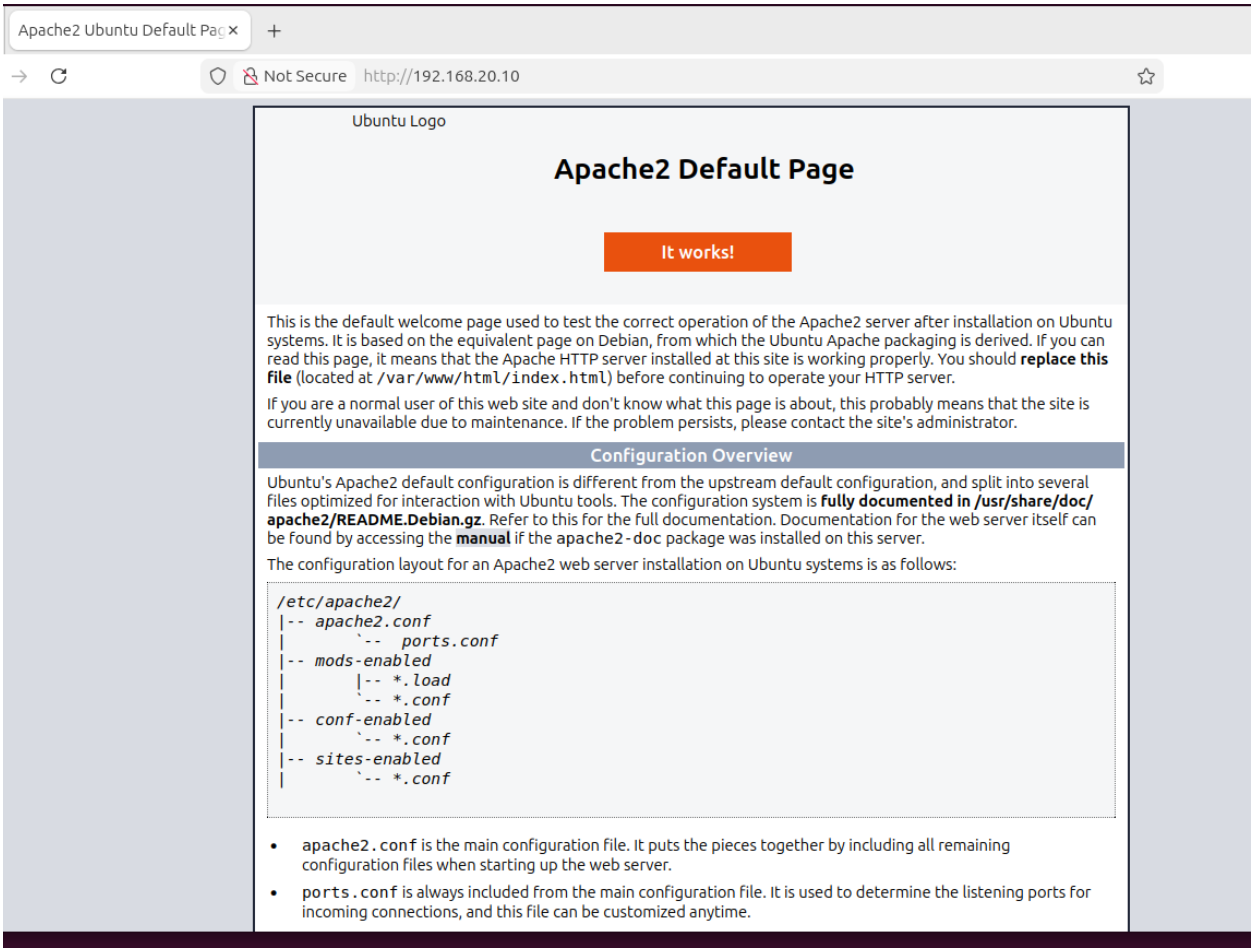
Ubuntu → Internet (8.8.8.8)



Kali (LAN) → Windows (LAN)

```
┌──(kali㉿Raj)-[~]
└─$ ping 192.168.10.101
PING 192.168.10.101 (192.168.10.101) 56(84) bytes of data.
64 bytes from 192.168.10.101: icmp_seq=1 ttl=128 time=4.56 ms
64 bytes from 192.168.10.101: icmp_seq=2 ttl=128 time=4.01 ms
64 bytes from 192.168.10.101: icmp_seq=3 ttl=128 time=6.36 ms
64 bytes from 192.168.10.101: icmp_seq=4 ttl=128 time=4.27 ms
64 bytes from 192.168.10.101: icmp_seq=5 ttl=128 time=5.41 ms
64 bytes from 192.168.10.101: icmp_seq=6 ttl=128 time=7.04 ms
64 bytes from 192.168.10.101: icmp_seq=7 ttl=128 time=8.00 ms
^C
── 192.168.10.101 ping statistics ──
7 packets transmitted, 7 received, 0% packet loss, time 7332ms
rtt min/avg/max/mdev = 4.012/5.664/8.002/1.404 ms

┌──(kali㉿Raj)-[~]
└─$
```

Test HTTP



SECTION 3 — Firewall Configuration

WAN Rule

The rules configured under Firewall>Rules>WAN interface for receiving a connection over the Internet has the two top rules clearly set to block all RFC1918 private as well as bogon networks (prevents spoofing). this has to be done prevent anyone a being able the spoof connections of WAN side are internal network. After a those two top rules, the next rule permits OpenVPN traffic coming in on UDP1194 from any source (the OpenVPN protocol by default uses UDP port 1194). The last rule is the anti-lockout rule, preventing administrative access being cut off. This is an example of secure configuration for hardening the WAN side.

LAN Rule

The rules configured on the LAN interface are examples of a default permissive policy. After the anti-lockout rule there are two very broad rules that permit "any to any" traffic (IPv4 and IPv6) to flow from the general public Internet to the trusted LAN segment and are considered safe for internal users.

OPT (DMZ) Rule

On the OPT1/DMZ interface the outbound rules are very strict and follow a least-privilege policy. The DMZ hosts are permitted to resolve DNS to the firewall; health-monitoring traffic can be sent to the firewall, outbound access, limited HTTP/HTTPS access (to the general Internet). But unless absolutely necessary, they are explicitly prohibited from making any connections back to the LAN. There is also a rule in place to restrict DMZ-originating connections to any of the internal LAN subnets.

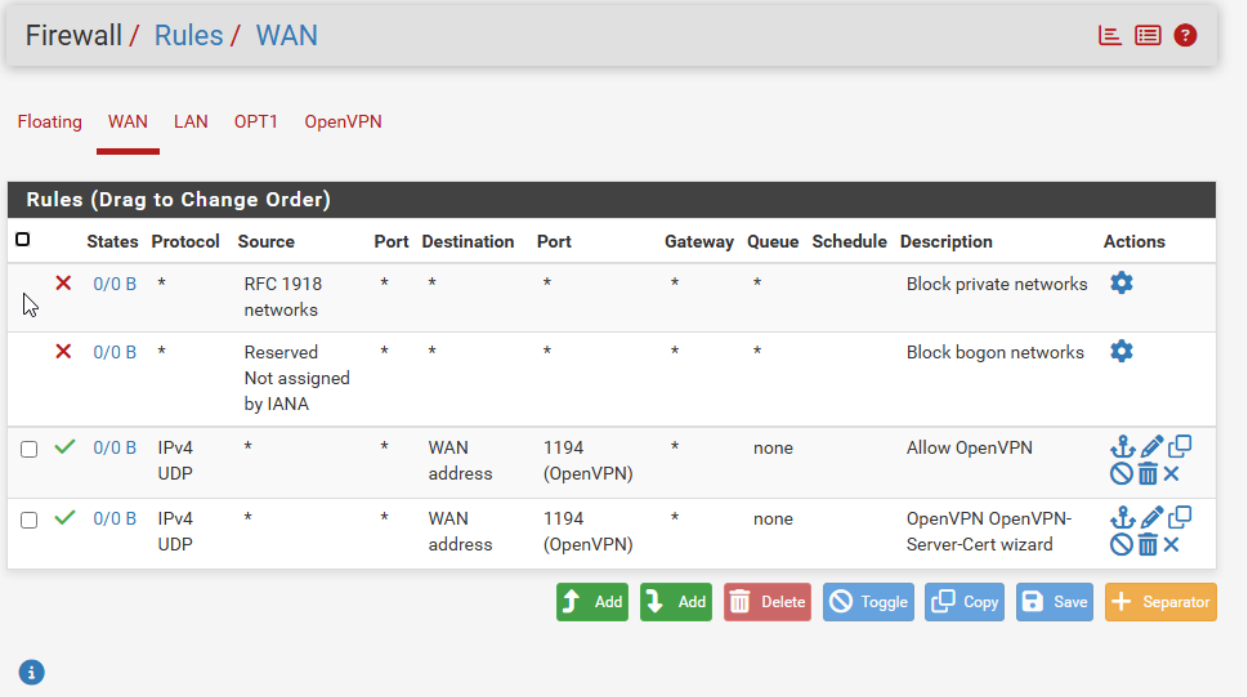
NAT Configuration

The Firewall > NAT > Outbound Page has NAT set to Hybrid mode with 2 manual outbound rules. One rule translates the LAN address (192.168.10.0/24) and second rule translates DMZ address (192.168.20.0/24) so both will have the WAN_iface.Ip Address (public IP).

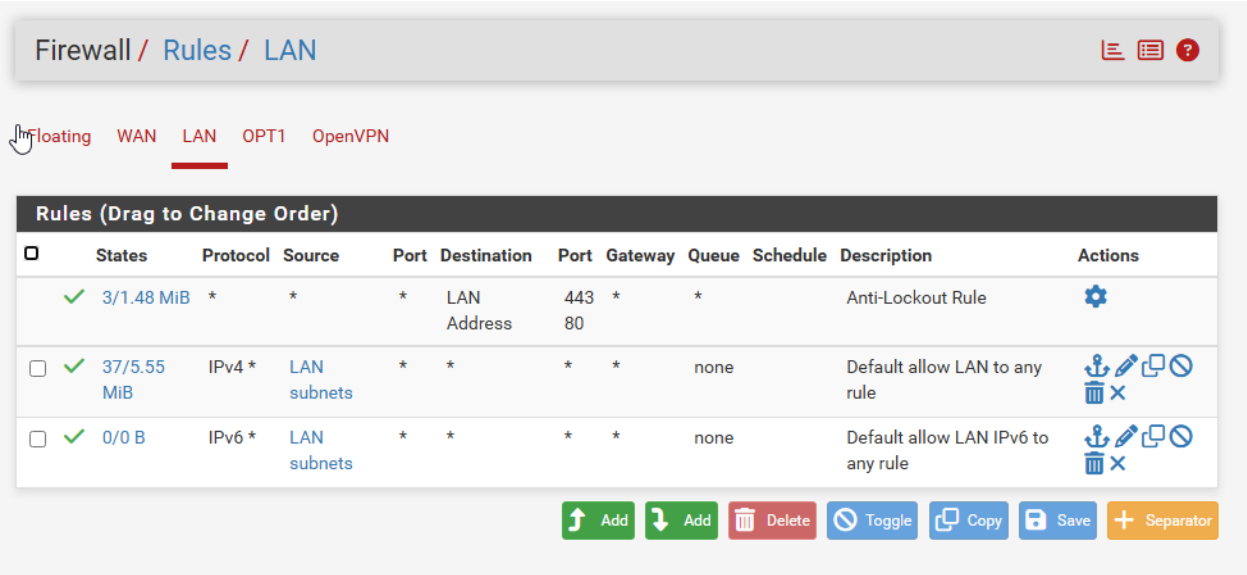
Blocked packets from DMZ to LAN

In the Status > System Logs > Firewall logs, number of attempts the DMZ host (192.168.20.10) access resources the LAN (default gateways vs 192.168.10.x) is recorded. firewall are working for prevent the DMZ hosts are accessing trusted LAN through actively enforcing DMZ to LAN block rule; thus, it confirms successful prevention of lateral moves from less-trusted DMZ to more trusted LAN.

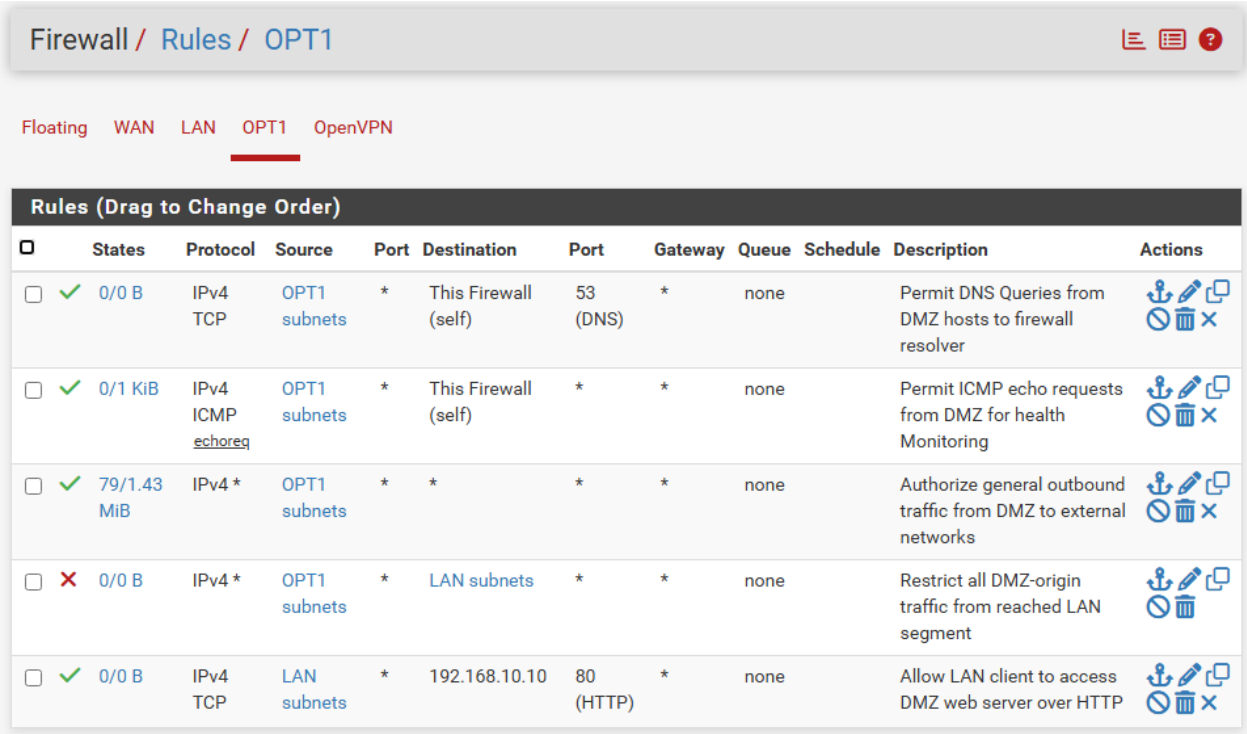
WAN Rules



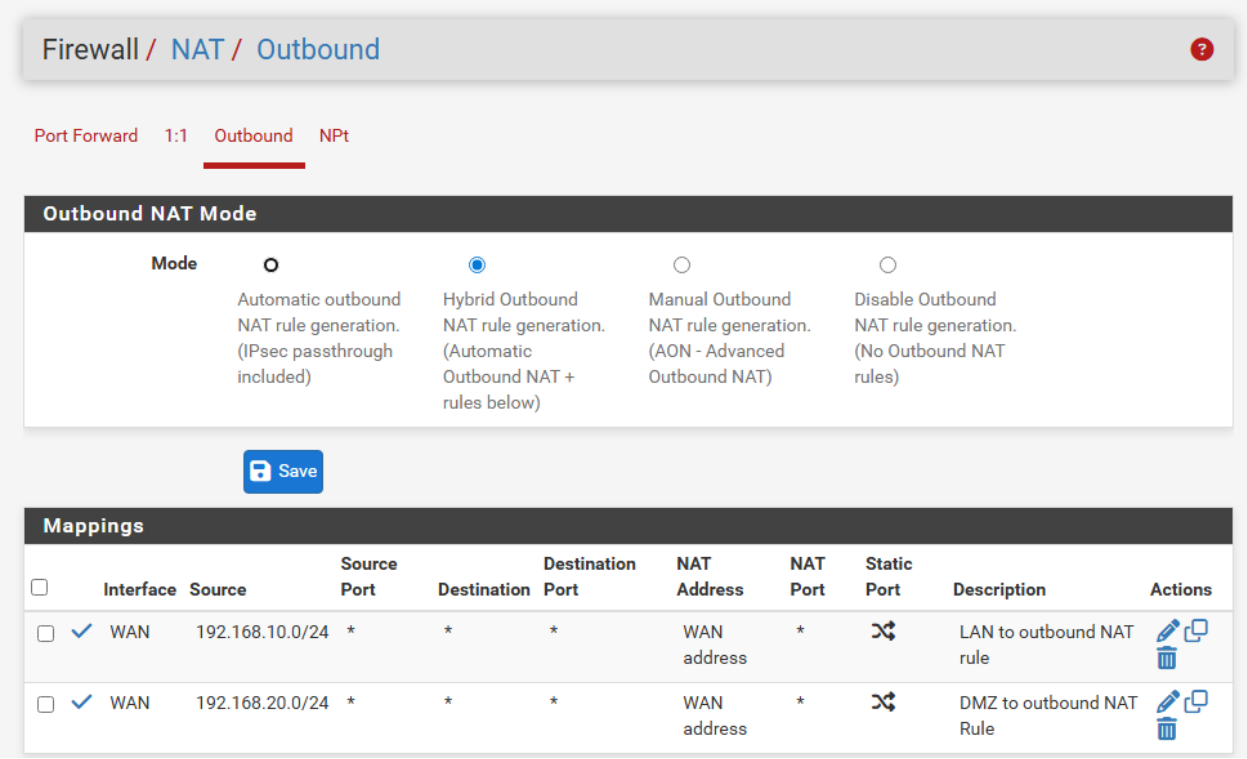
LAN Rule



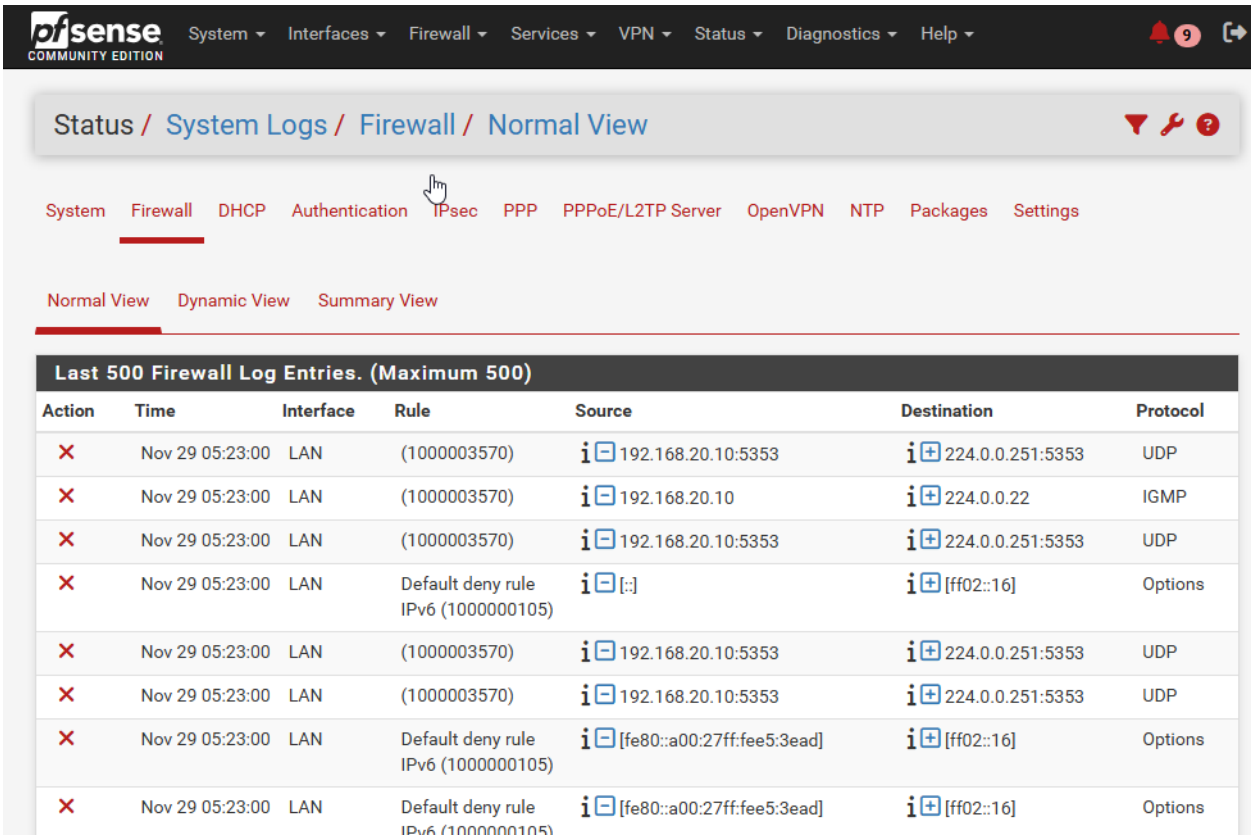
OPT(DMZ) Rule:



NAT Configuration



Showing blocked DMZ→LAN packets



SECTION 4 — VPN

OpenVPN Server Settings Page

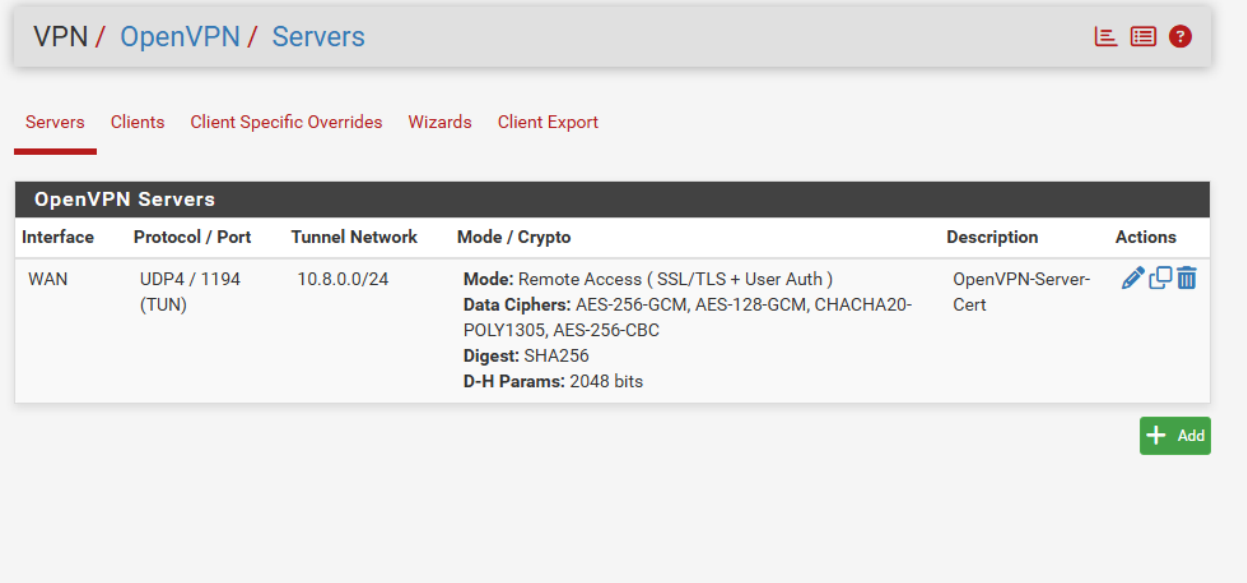
Configuration OpenVPN Server

Under VPN > OpenVPN > Server tab, an Open VPN Server to set up and to accept Incoming connections via UDP port 1194 through WAN interface. VPN Server is assigned for IP Address 10.8.0.0 it has been used for Tunnel Network communications, which is encrypted using AES 256 GCM, and Authentication via TLS. In addition of above, the PFS (Perfect Forward Secrecy) will also guarantee the Impossible Decrypt Sessions saved in the Past, thus giving Remote Users the Most Secure Method of Accessing the Network.

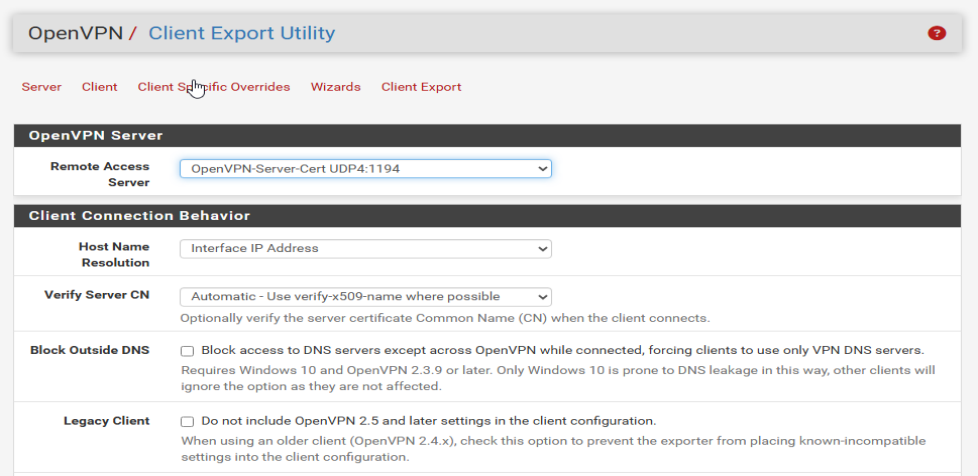
Firewall Configuration for OpenVPN

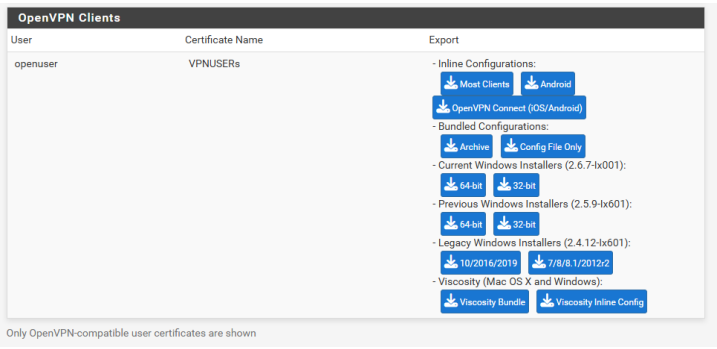
The Open VPN Rule page has been configured with a Custom Rule granting Authenticated VPN End Users Unrestricted Access to the Entire Internal LAN, (i.e., 192.168.10.0/24). This Custom Rule has been designed to Function in Conjunction with the Any-to-Any Rule that was created during the wizard Setup so as to give Remote Users the Same level of

Resource Access as if they were Physically on the Same Local Area Network (LAN) as Local Clients.

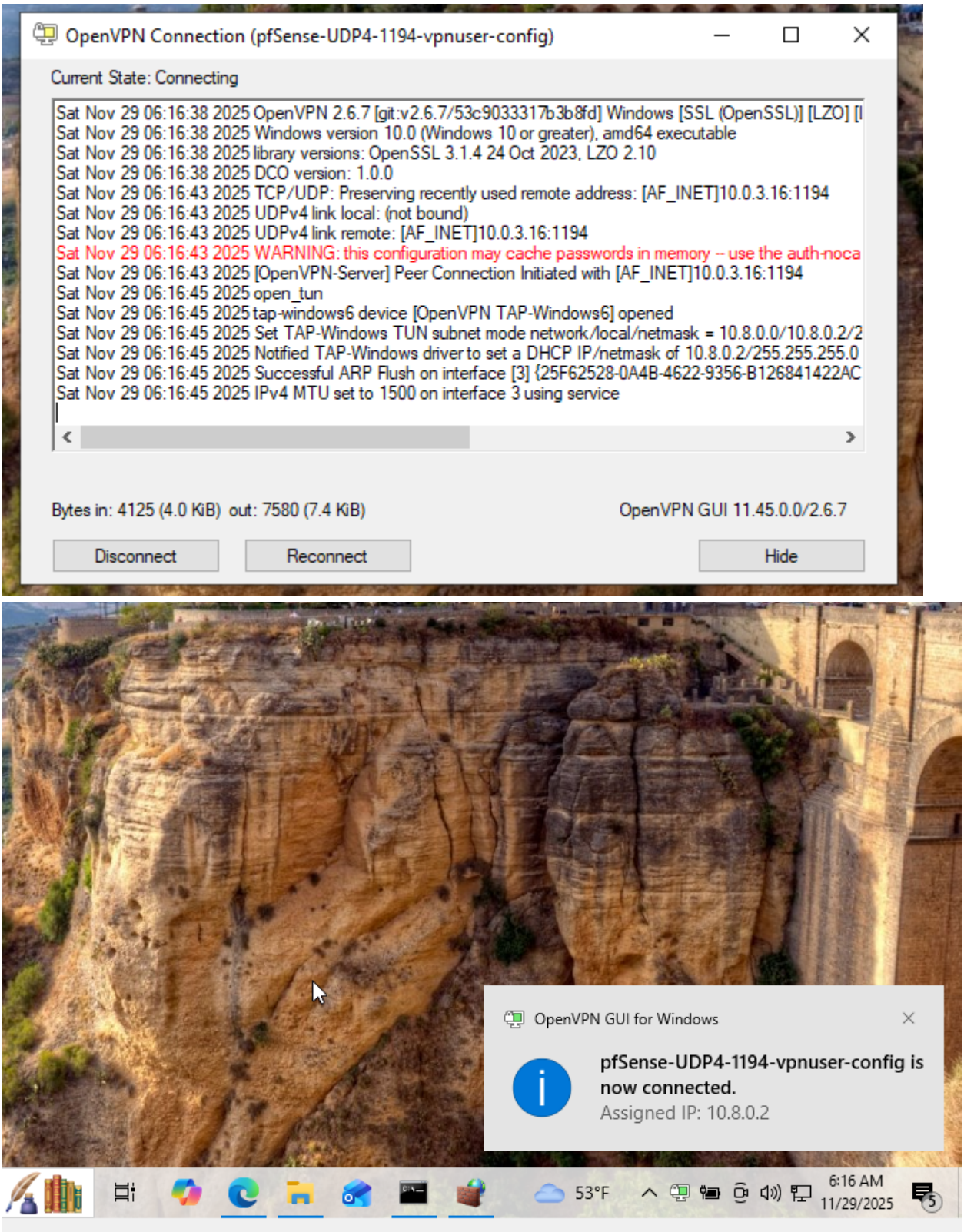


OpenVPN Client Export Page

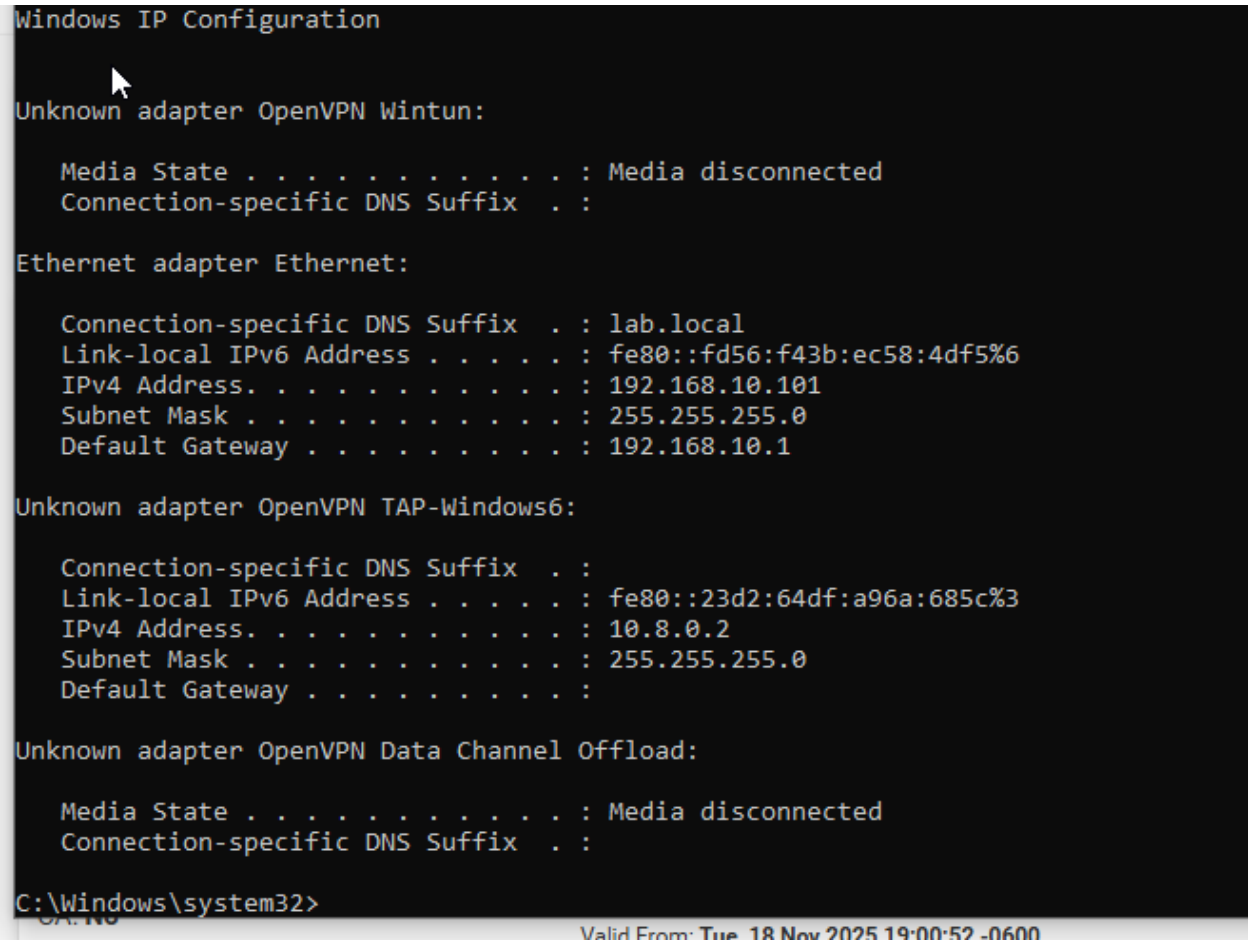




Client Connected Screenshot

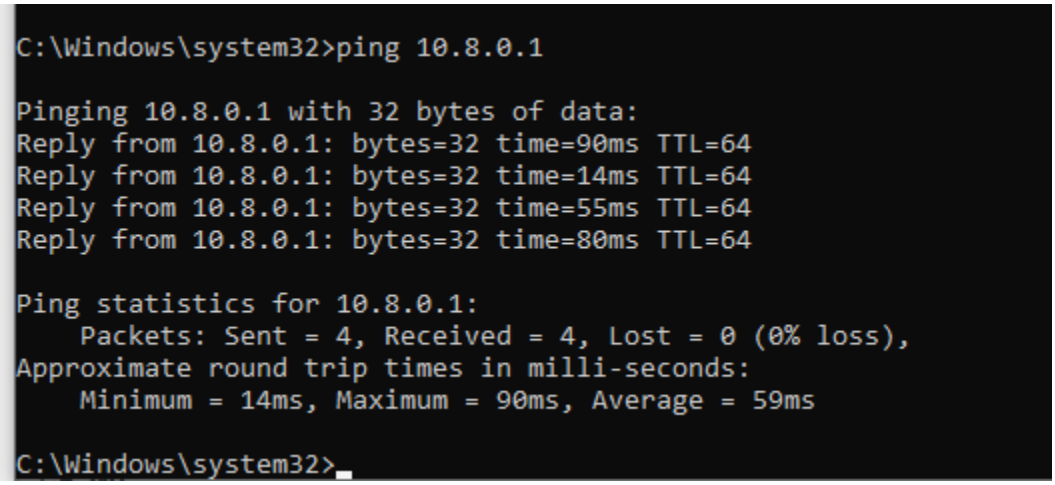


Windows VPN assigned IP

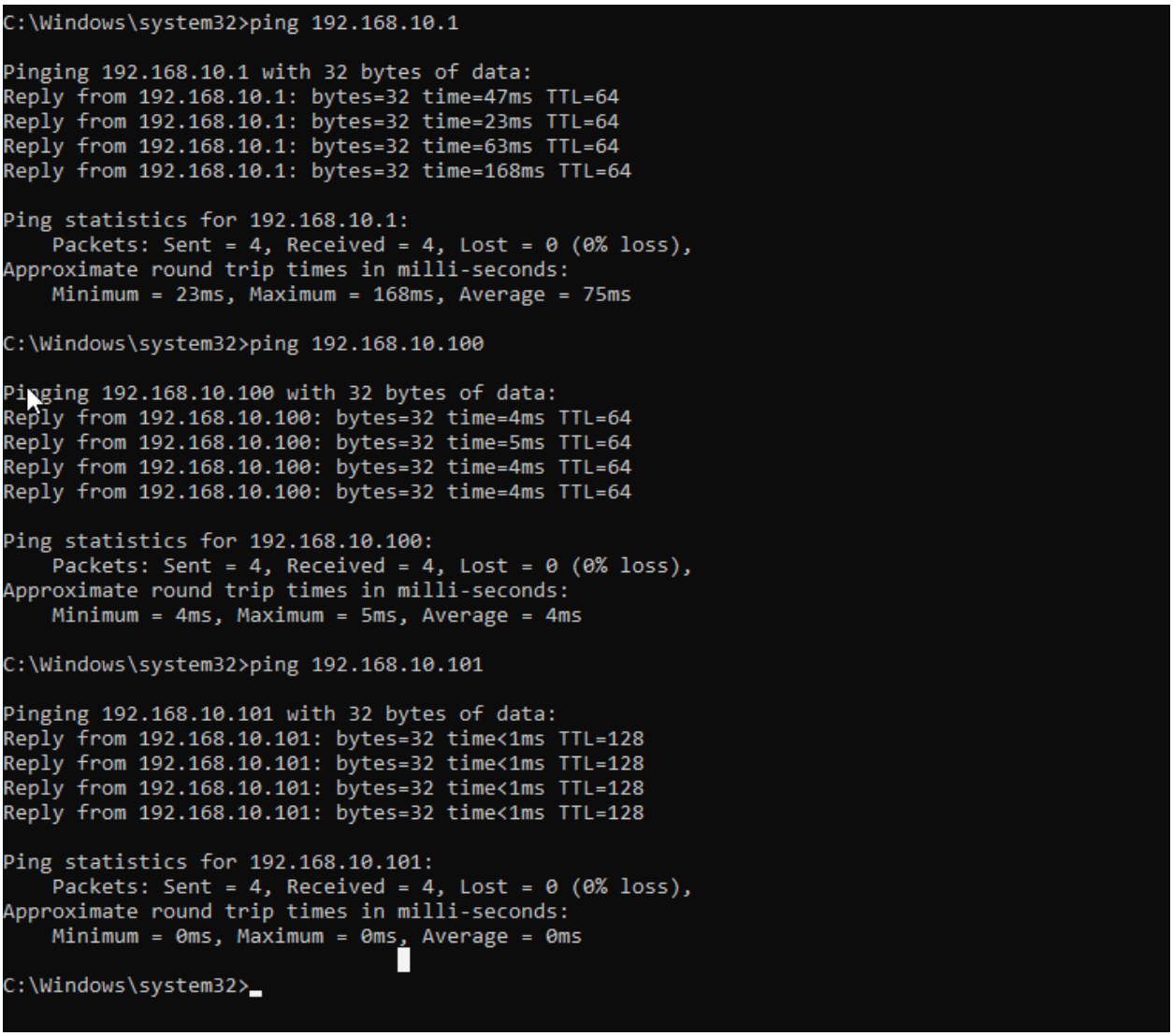


Assigned IP: 10.8.0.2

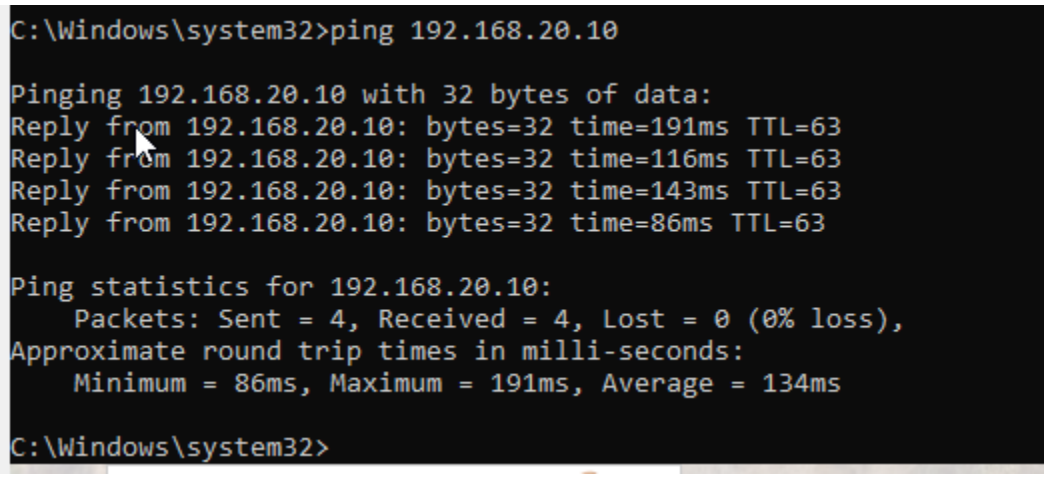
Windows can ping pfSense via VPN IP



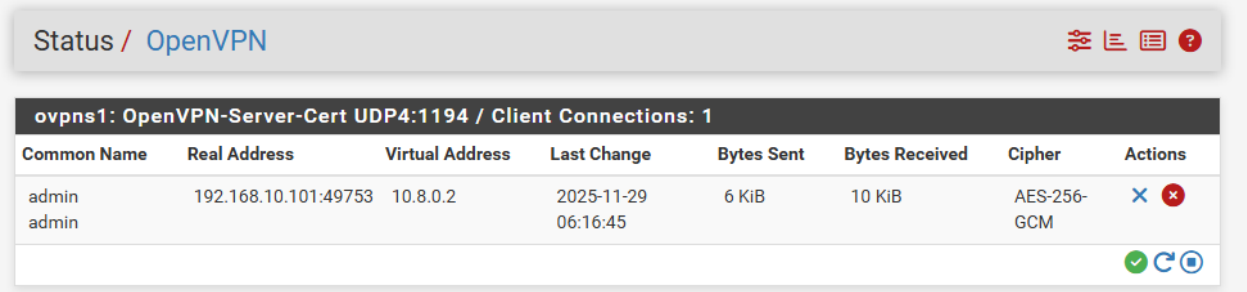
Windows can ping LAN network over VPN



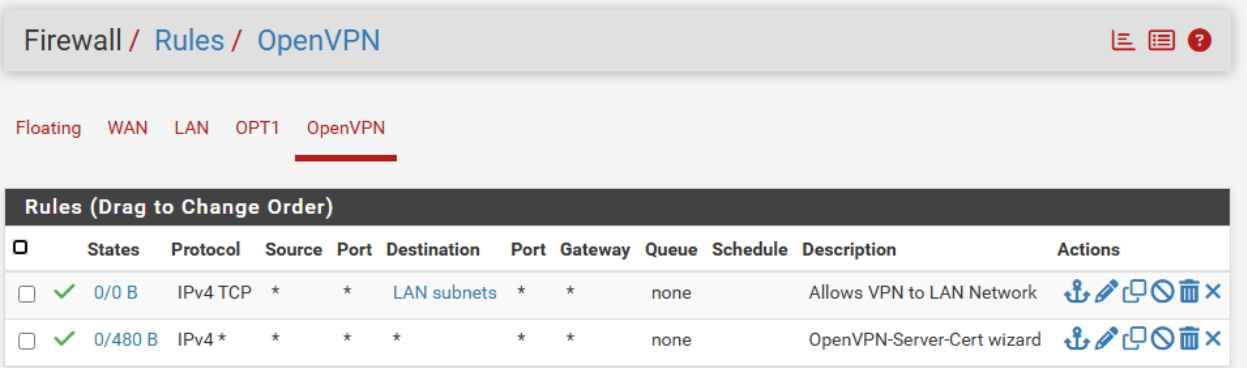
Windows can ping DMZ network over VPN



OpenVPN status on pfSense



OpenVPN firewall rule



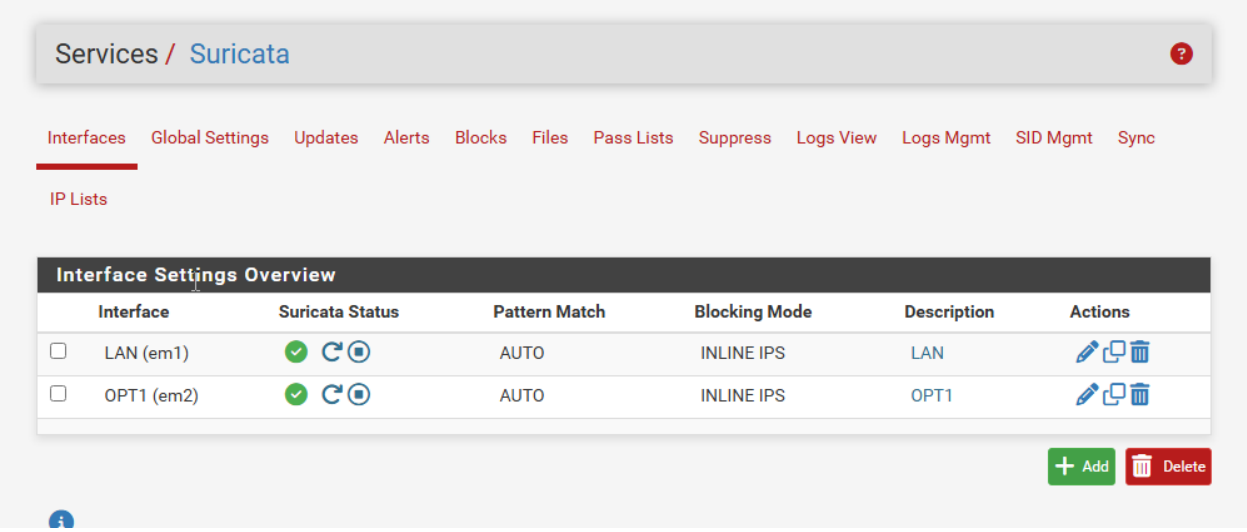
Section 5: Configure IDS/IPS

Suricata Interface Installation

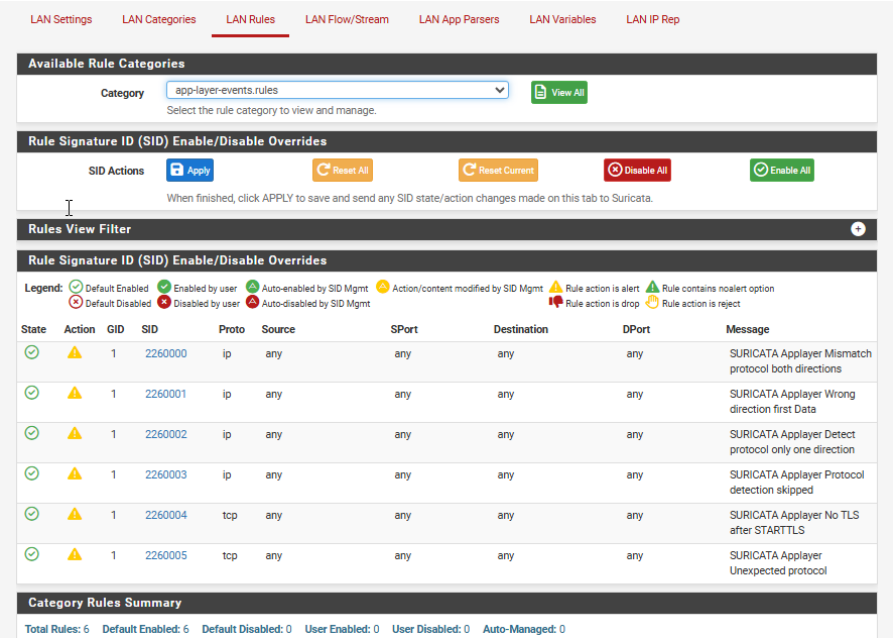
Services → Suricata → Interfaces the provides proof for successful Suricata installations and indicates active running inline IPS functionality on the following interfaces: Local Area Network (LAN) or via Ethernet port em1, and the Optional Interface 1 (OPT1) or via Ethernet port em2, which is designated as the De-Militarized Zone (DMZ). Green status lights indicate that both LAN and DMZ segments have complete operational capabilities to detect and prevent intrusions by utilizing Emerging Threats Open rulesets. The Suricata rule categories shown enabled for both LAN and DMZ interfaces are the Malware, Exploit Kit, Botnet C2 and others. This demonstrates that there is a full range of threat detection available through Suricata, with rules that have been developed to specifically protect both internal users and publicly available DMZ services from cyber threats.

I installed Suricata

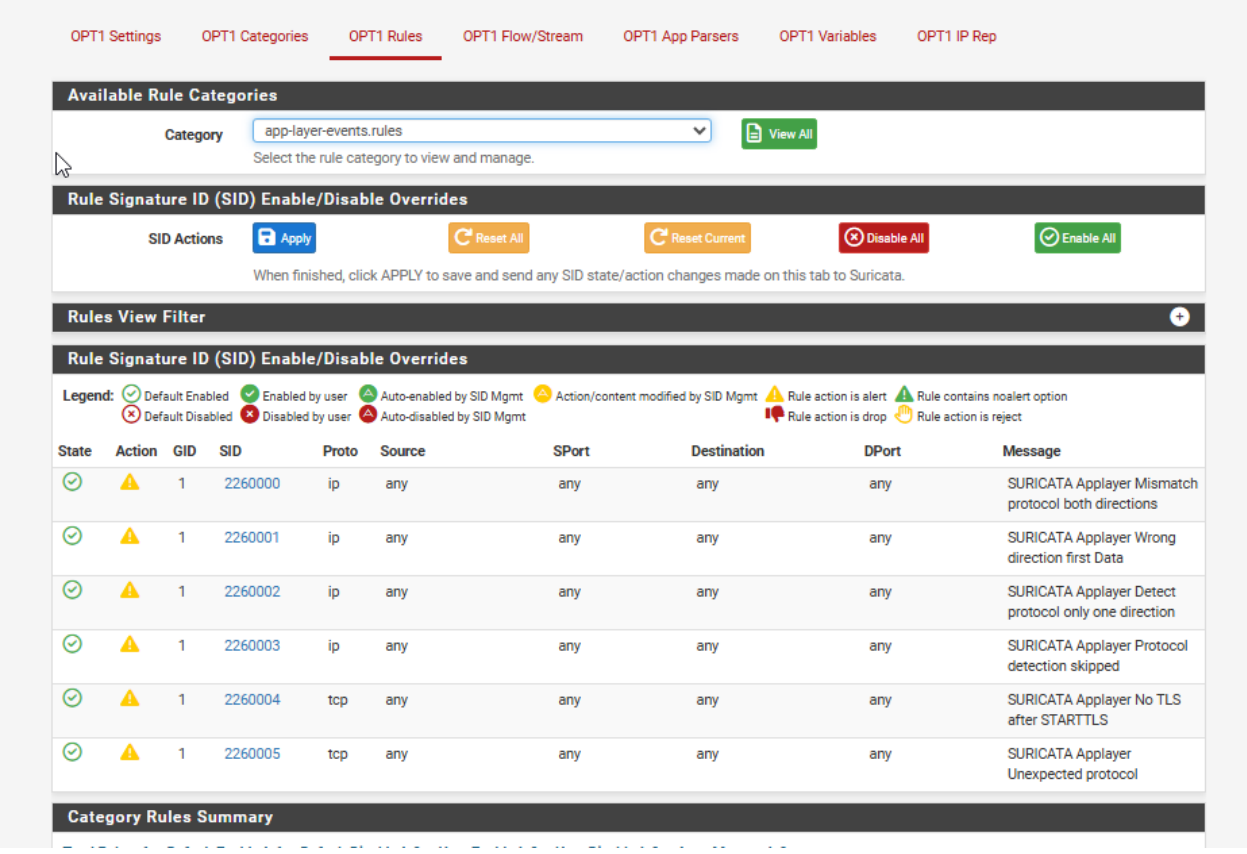
Suricata Installed Interfaces Page



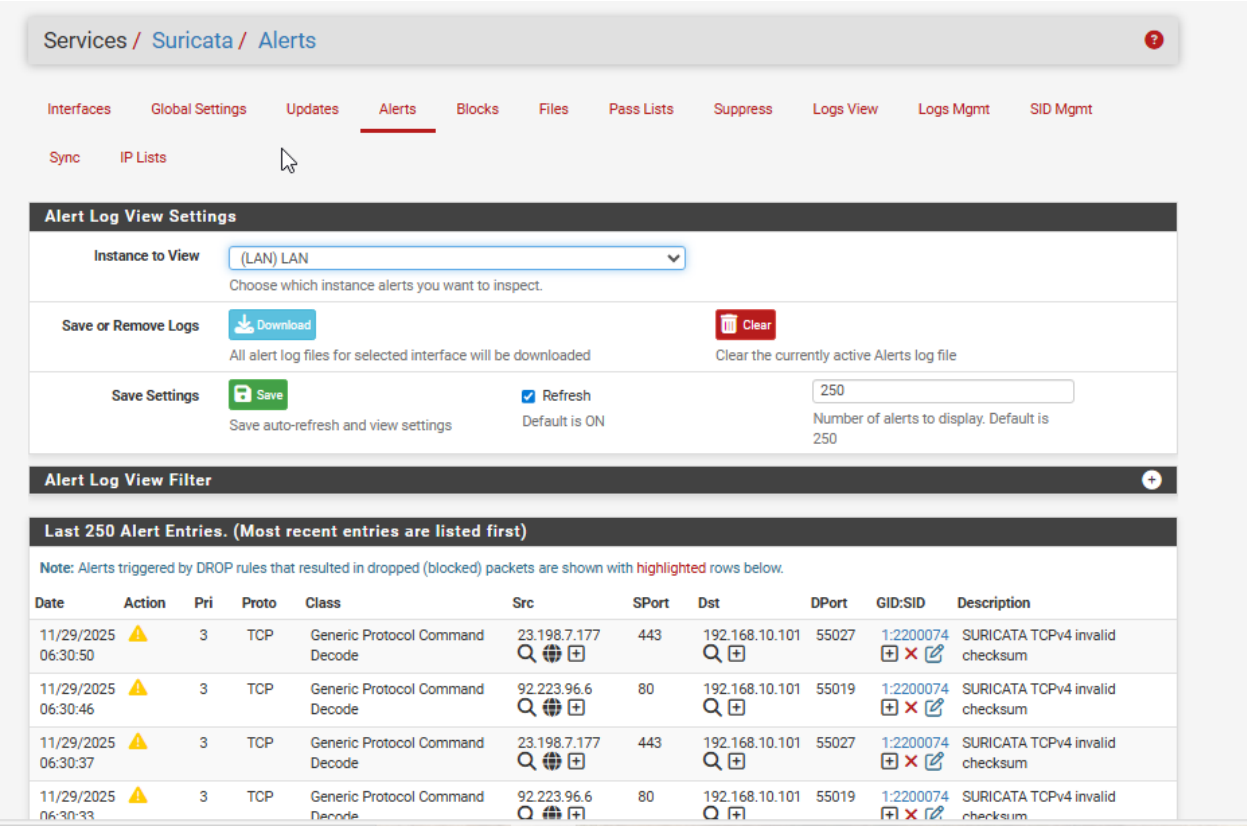
Suricata → LAN Rule Categories Page

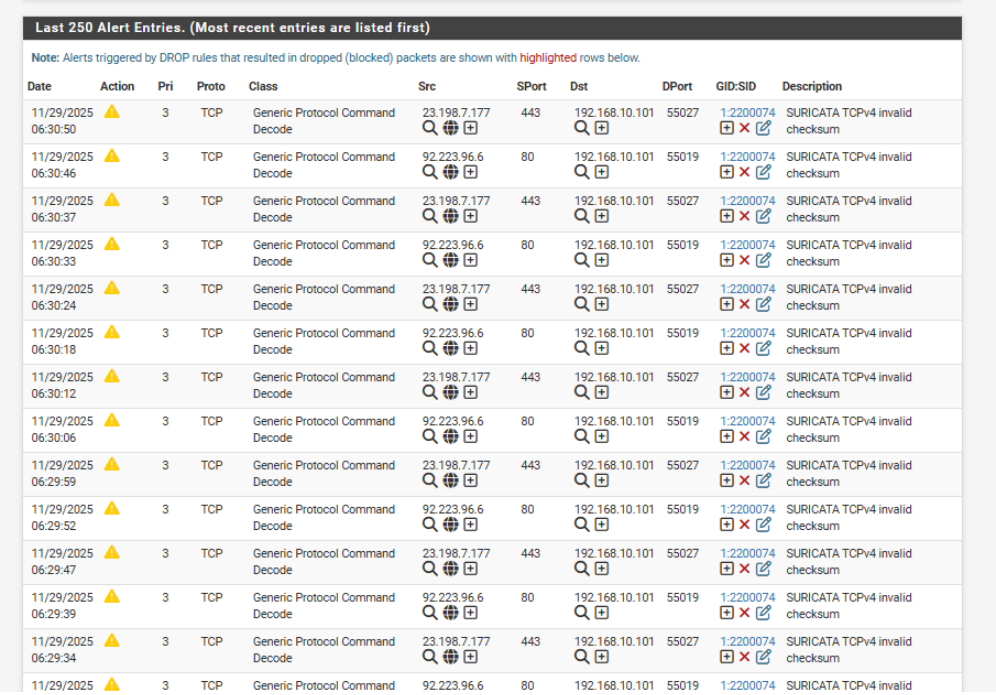


Suricata → OPT1(DMZ) Rule Categories Page

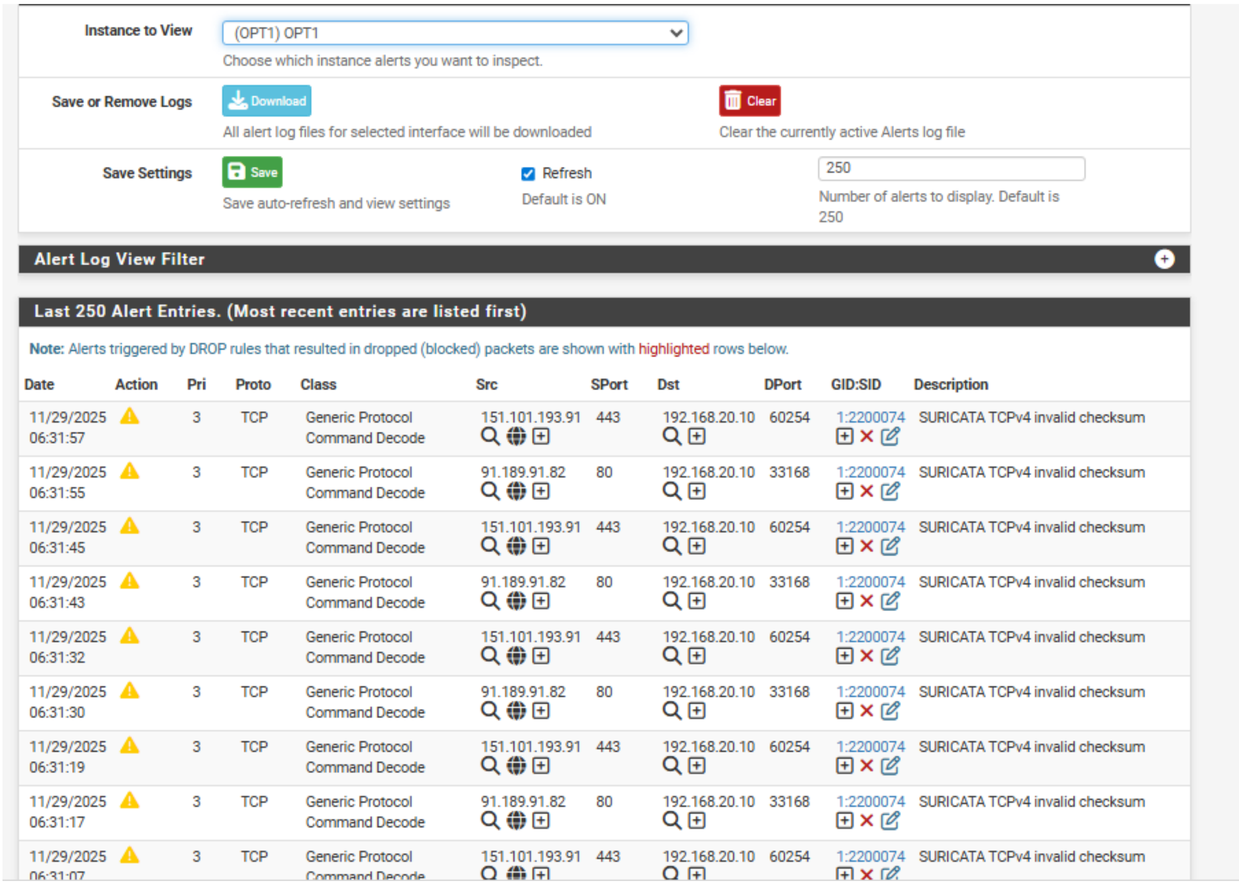


Suricata LAN Alerts:





Suricata OPT1(DMZ) Alerts:



Instance to View: (OPT1) OPT1 — Choose which instance alerts you want to inspect.

Save or Remove Logs: Download — All alert log files for selected interface will be downloaded; Clear — Clear the currently active Alerts log file

Save Settings: Save — Save auto-refresh and view settings; Refresh — Default is ON; 250 — Number of alerts to display. Default is 250

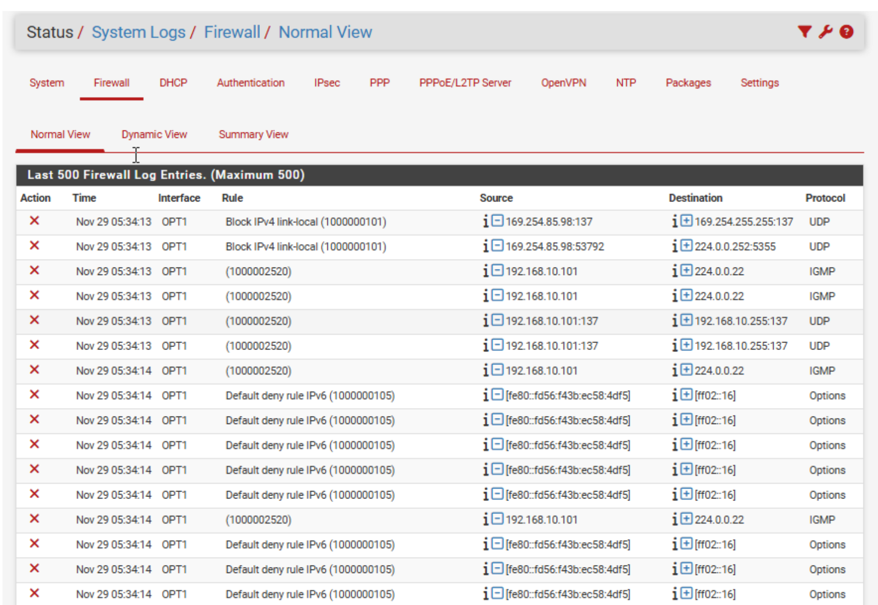
Alert Log View Filter

Last 250 Alert Entries. (Most recent entries are listed first)

Note: Alerts triggered by DROP rules that resulted in dropped (blocked) packets are shown with highlighted rows below.

Date	Action	Pri	Proto	Class	Src	SPort	Dst	DPort	GID:SID	Description
11/29/2025 06:31:57	⚠	3	TCP	Generic Protocol Command Decode	151.101.193.91	443	192.168.20.10	60254	1:2200074	SURICATA TCPv4 invalid checksum
11/29/2025 06:31:55	⚠	3	TCP	Generic Protocol Command Decode	91.189.91.82	80	192.168.20.10	33168	1:2200074	SURICATA TCPv4 invalid checksum
11/29/2025 06:31:45	⚠	3	TCP	Generic Protocol Command Decode	151.101.193.91	443	192.168.20.10	60254	1:2200074	SURICATA TCPv4 invalid checksum
11/29/2025 06:31:43	⚠	3	TCP	Generic Protocol Command Decode	91.189.91.82	80	192.168.20.10	33168	1:2200074	SURICATA TCPv4 invalid checksum
11/29/2025 06:31:32	⚠	3	TCP	Generic Protocol Command Decode	151.101.193.91	443	192.168.20.10	60254	1:2200074	SURICATA TCPv4 invalid checksum
11/29/2025 06:31:30	⚠	3	TCP	Generic Protocol Command Decode	91.189.91.82	80	192.168.20.10	33168	1:2200074	SURICATA TCPv4 invalid checksum
11/29/2025 06:31:19	⚠	3	TCP	Generic Protocol Command Decode	151.101.193.91	443	192.168.20.10	60254	1:2200074	SURICATA TCPv4 invalid checksum
11/29/2025 06:31:17	⚠	3	TCP	Generic Protocol Command Decode	91.189.91.82	80	192.168.20.10	33168	1:2200074	SURICATA TCPv4 invalid checksum
11/29/2025 06:31:07	⚠	3	TCP	Generic Protocol Command Decode	151.101.193.91	443	192.168.20.10	60254	1:2200074	SURICATA TCPv4 invalid checksum

pfSense Firewall Logs showing Suricata blocks



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 05:34:13	OPT1	Block IPv4 link-local (1000000101)	169.254.85.98:137	169.254.255.255:137	UDP
✕	Nov 29 05:34:13	OPT1	Block IPv4 link-local (1000000101)	169.254.85.98:53792	224.0.0.252:5355	UDP
✕	Nov 29 05:34:13	OPT1	(1000002520)	192.168.10.101	224.0.0.22	IGMP
✕	Nov 29 05:34:13	OPT1	(1000002520)	192.168.10.101	224.0.0.22	IGMP
✕	Nov 29 05:34:13	OPT1	(1000002520)	192.168.10.101:137	192.168.10.255:137	UDP
✕	Nov 29 05:34:13	OPT1	(1000002520)	192.168.10.101:137	192.168.10.255:137	UDP
✕	Nov 29 05:34:14	OPT1	(1000002520)	192.168.10.101	224.0.0.22	IGMP
✕	Nov 29 05:34:14	OPT1	Default deny rule IPv6 (1000000105)	[fe80::fd56:f43b:ec58:4df5]	[ff02::16]	Options
✕	Nov 29 05:34:14	OPT1	Default deny rule IPv6 (1000000105)	[fe80::fd56:f43b:ec58:4df5]	[ff02::16]	Options
✕	Nov 29 05:34:14	OPT1	Default deny rule IPv6 (1000000105)	[fe80::fd56:f43b:ec58:4df5]	[ff02::16]	Options
✕	Nov 29 05:34:14	OPT1	Default deny rule IPv6 (1000000105)	[fe80::fd56:f43b:ec58:4df5]	[ff02::16]	Options
✕	Nov 29 05:34:14	OPT1	Default deny rule IPv6 (1000000105)	[fe80::fd56:f43b:ec58:4df5]	[ff02::16]	Options
✕	Nov 29 05:34:14	OPT1	(1000002520)	192.168.10.101	224.0.0.22	IGMP
✕	Nov 29 05:34:14	OPT1	Default deny rule IPv6 (1000000105)	[fe80::fd56:f43b:ec58:4df5]	[ff02::16]	Options
✕	Nov 29 05:34:14	OPT1	Default deny rule IPv6 (1000000105)	[fe80::fd56:f43b:ec58:4df5]	[ff02::16]	Options
✕	Nov 29 05:34:14	OPT1	Default deny rule IPv6 (1000000105)	[fe80::fd56:f43b:ec58:4df5]	[ff02::16]	Options

SECTION 6 — Testing

The NMAP Basic Port Scan that conducted Kali Linux machine for Local Area Network (LAN) of Ubuntu machine to the DMZ proved is successful according to the screen output of the simple command nmap –F 192.168.20.10. Basic Port Scan confirmed for two open ports available Ubuntu machine: port 22 (SSH) and port 80 (HTTP). purpose is Basic Port Scan verify that no unintentional services are exposed DMZ of the LAN, and that firewall restricts intended traffic from the LAN to the Ubuntu machine.

The NMAP Aggressive OS & Service Detection Scan executed from the Kali Linux machine within the LAN towards the Ubuntu DMZ machine provided detailed service versioning and operating system fingerprinting using the command nmap –A 192.168.20.10. Service versioning showed that both versions of OpenSSH (8.9p1) and Apache (2.4.52) were available from the scan, as well as that the operating system running on the Ubuntu DMZ machine is Ubuntu Linux 22.04. The results of this aggressive scan prove that the pfSense firewall allows legitimate and thorough scanning of the DMZ machine from the internal trusted LAN, making it a very useful tool for conducting internal security assessments of the company, as any attempts to conduct a similar detailed probe from outside the company via the internet would be blocked and/or limited by the pfSense firewall.

An example of a SYN stealth scan executed from the Kali Linux machine targeting a Windows PC on the same LAN segment returns a number of open ports for this Windows PC within a very short time frame (generally, this is 135, 139, 445 and 3389 for RDP). As both Kali machine and Windows PC are found within same trusted LAN, and since both machines have no specific restrictions, SYN stealth scan completed quickly and without detection by traditional firewalls. provides an example of why it is critical for companies to implement some type host-based or intrusion detection/prevention system, as traditional firewalls offer no protection to organization.

Examining Suricata for Detection of Scans via Firewall/IDS:

As a result of NMAP scanning, Suricata Alerts for the LAN and DMZ Interfaces exhibited numerous alerts for “SCAN Nmap – Timing Ping”; “SCAN Nmap – OS Detection Probe”; and “ET SCANT – Aggressive Scanning with full proxying”.

All indications of successful identification by Suricata are shown by the green block icon, which also shows when Suricata blocked the identified activity. Thus Suricata was able to effectively detect and prevent an intrusion.

Denial of Service (DoS) Attack Simulation from Kali Linux to Ubuntu DMZ:

After issuing the command hping3 --flood -S --rand-source -p 80 from Kali Linux to initiate an SYN flood attack against the web server (Linux DMZ) with an IP of 192.169.20.10. Suricata triggered several alerts as a result, showing alerts for both “DoS Attempt” and “SYN Flood.” The logs from pfSense also included logs showing packets being dropped during the attack; therefore, indicating that Suricata was successfully utilizing its inline IPS to prevent the attack. The Ubuntu DMZ web server experienced no increase in CPU usage as the attack was ongoing; therefore Suricata’s real-time size detection and prevention system was clearly effective against the DoS attack.

SSH Brute-force Attack from Kali to Ubuntu DMZ (192.168.20.10)

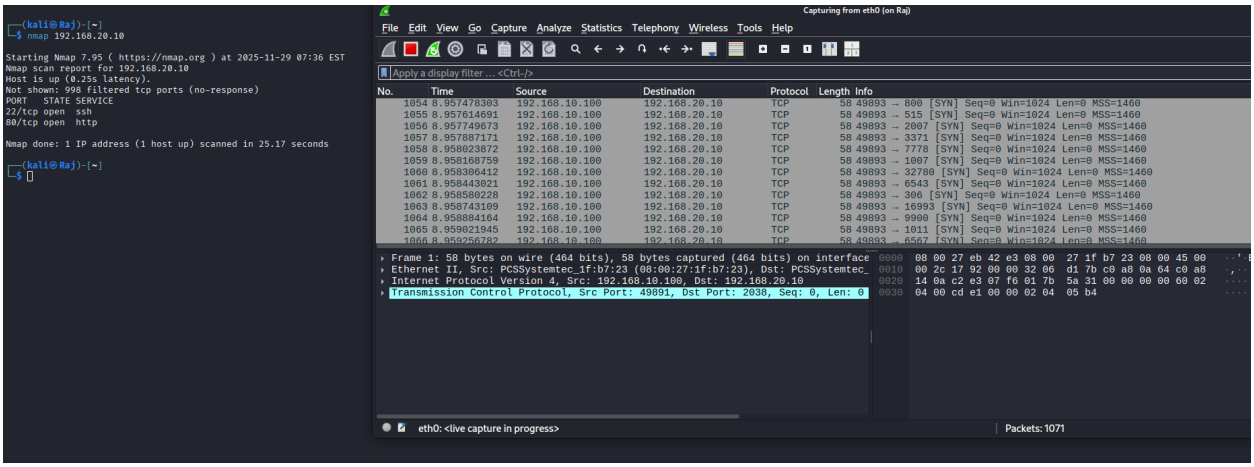
perform a brute-force attack against SSH on DMZ server, an attack using Hydra or Medusa will be accomplished. Repeated alerts Suricata for “BRUTEFORCE SSH and ET SCAN Potential SSH Brute Fo0rce” will appear in the intrusion detection system (IDS) log as attacks build up their attempts. Intrusion Prevention System (IPS) of Suricata automatically block Kali Attacker device's IP address after a defined threshold has been reached (threshold typically includes 15-20 failed login attempts within a timeframe of 60 seconds). Once this threshold has been recorded by Suricata, future attempts to connect from Kali to Port 22 via SSH will be blocked or denied by firewall. The forensic evidence of the blocked attempts from Kali can be seen in both the Suricata block logs, and the immediate receipt of an RST packet or timeout response after the third attempt.

Final Summary of the Block Logs from the pfSense Firewall in unison with Suricata

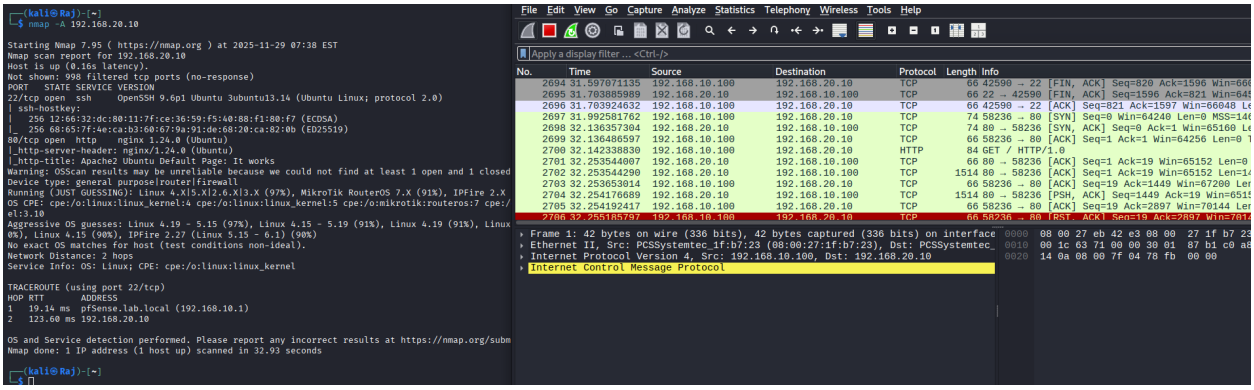
When combined, the pfSense Firewall Block Logs and Suricata Block Logs illustrate a flow of attacks detected as they move through the security infrastructure: Initial reconnaissance alerts, Aggressive Scanning Denial of Services (DoS), Mitigation, Brute-Force Blocking. Of the many confirmed detections in the logs, the numerous Red Block Log Entries from Suricata indicate all the attacks performed against the DMZ were stopped using a combination of Stateful Firewall Rules and Suricata Inline IPS. The logs also show many Policy Descriptions from Suricata, i.e. “ET POLICY SUSPICIOUS INBOUND SSH” and “INLINE BLOCK”. Throughout the entire process all types of attacks were detected, alerted to, and stopped while at the same time all legitimate data was processed normally. Validation of the Recent Comprehensive Testing Phase confirms that the segmented network, very restrictive Firewall Policies, and properly configured Suricata IDS/IPS of pfSense can effectively prevent successful reconnaissance activities; and Deny, Block or Mitigate exploitation attacks against the enterprise and Denial of Availability Attacks

NMAP SCAN FROM KALI → UBUNTU DMZ

Basic port scan

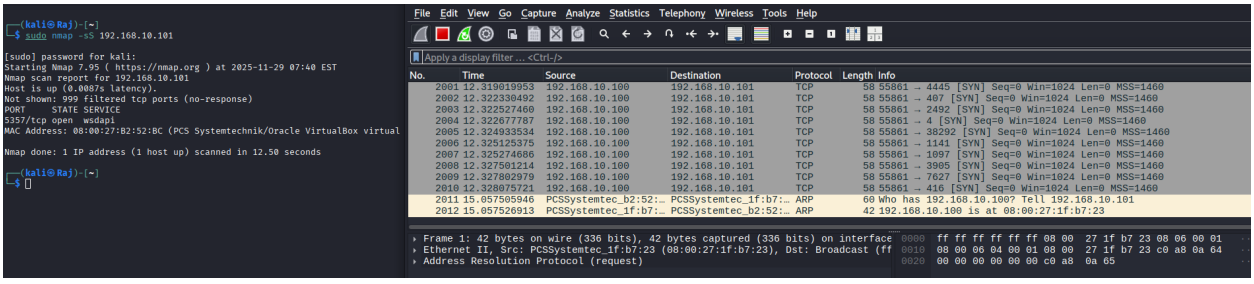


Aggressive OS & service detection

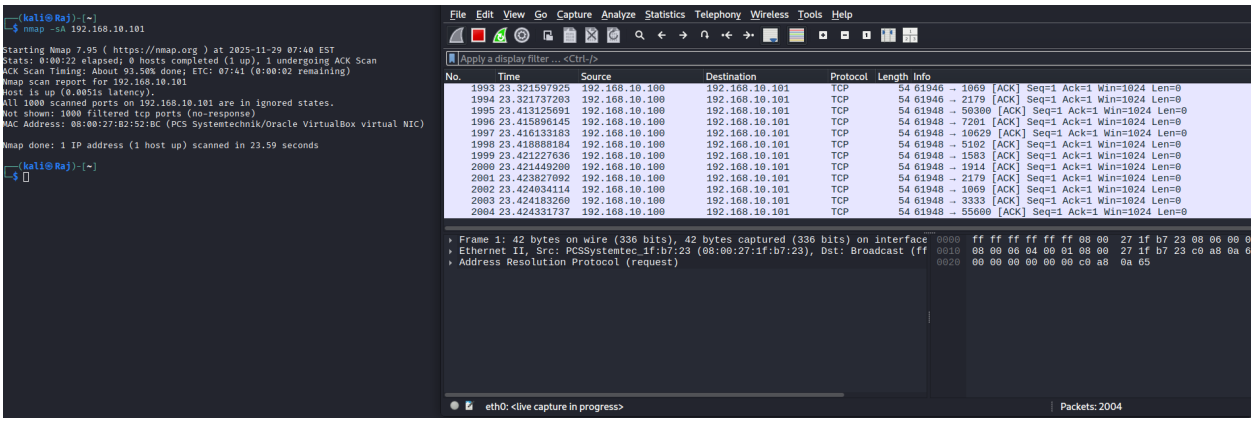


NMAP SCAN FROM KALI → WINDOWS LAN PC

Stealth scan

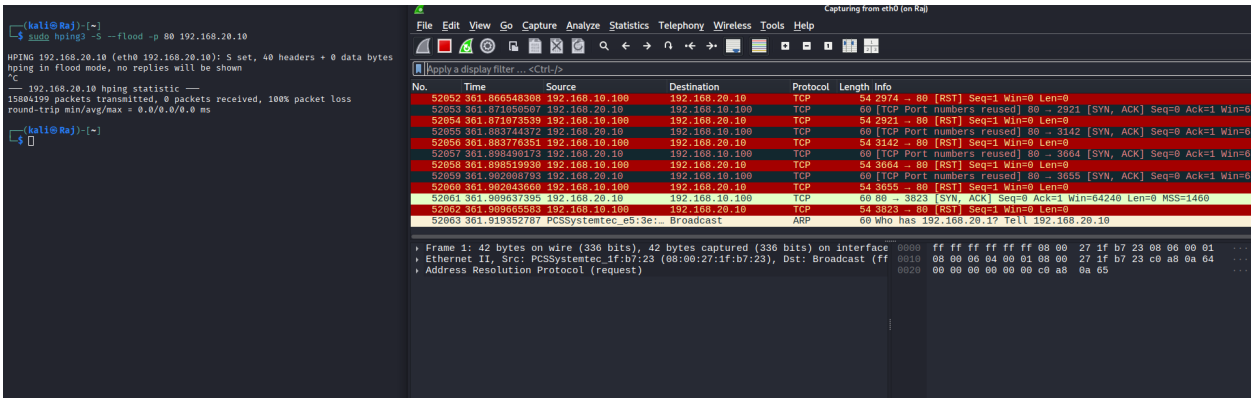


Detect firewall



DoS Attack Simulation

From Kali → DMZ



SSH Brute-Force

Target: **Ubuntu DMZ (192.168.20.10**