XDR

wazuh.

The Open Source Security Platform

SIEM

pfsense®

Pfsense Intergated Wazuh

What is pfSense?

pfSense is an open-source firewall and router software distribution based on **FreeBSD**. It provides enterprise-level network security features and is widely used in small to large networks.

It can be installed on a physical machine or run as a **virtual machine**, acting as your network's **gateway** (between internal and external networks).

Why Use pfSense?

Feature	Description
Firewall	Powerful packet filtering with rules based on IP, port, protocol, etc.
Router	Acts as a full-featured router (NAT, DHCP, etc.).
VPN	Supports OpenVPN, IPsec, and WireGuard for secure remote access.
Traffic Shaping / QoS	Prioritize bandwidth for specific services or devices.
IDS/IPS	Integration with Snort or Suricata for intrusion detection/prevention.
Web Interface	Easy-to-use GUI for configuration—no command line needed.
Multi-WAN	Load balancing and failover with multiple Internet connections.
Captive Portal	Great for public Wi-Fi control (like hotels or cafes).
Logging s Monitoring	Full logs of traffic, system events, firewall alerts, etc.

How Does pfSense Work?

Network Interfaces:

- You configure **WAN** (external internet) and **LAN** (internal network) interfaces.
- Optionally, you can add **OPT** interfaces for things like DMZ or multiple LANs.

Firewall Rules:

- By default, it blocks all inbound WAN traffic.
- You set rules to allow/deny traffic between interfaces.

NAT (Network Address Translation):

- pfSense translates internal (private) IPs to a public IP (via WAN) to allow internet access.
- Also used for port forwarding from WAN to LAN services.

Services:

- **DHCP server** to assign IPs to LAN clients.
- **DNS resolver/forwarder** to speed up domain lookups.
- **VPN server/client** setup.

Logging s Monitoring:

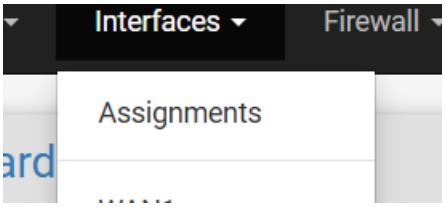
- Real-time traffic graphs, logs of blocked/allowed traffic, system messages.
- Can export logs to a SIEM or tools like **Wazuh**.

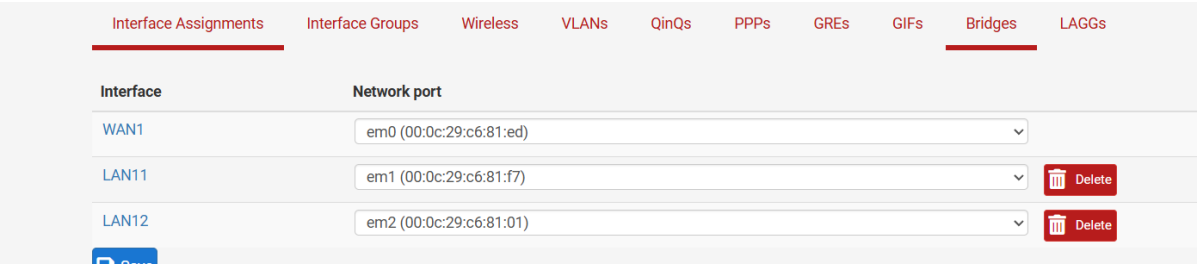
1. Installation and configuration

- Follow up two youtube channels (1) https://youtu.be/_AiJiS2gtFE?si=4waQzQItKApCD9n8)
- 2) https://youtu.be/eFzG44Ngulo?si=4AHu0tvYwZ33k-Er

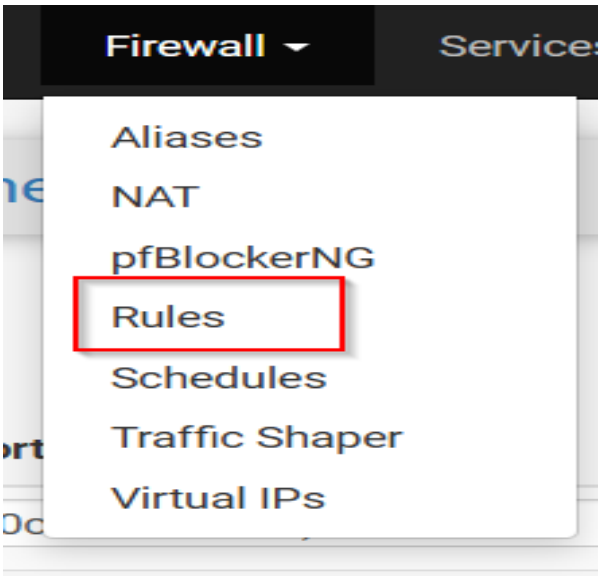
After installation done set your static Ip and login browser with your ip address and username pw (admin:pfsense)

Once login follow rest of the step in videos (Next lets assign interface of LAN11,12,Wan1)

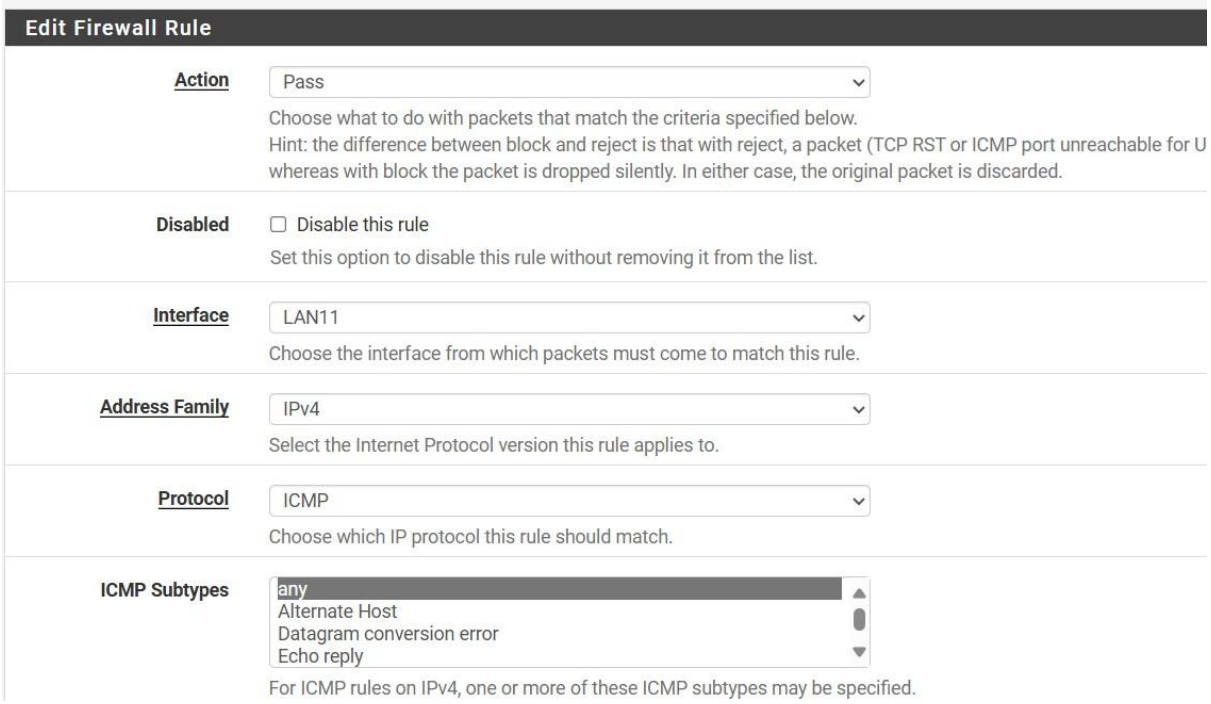


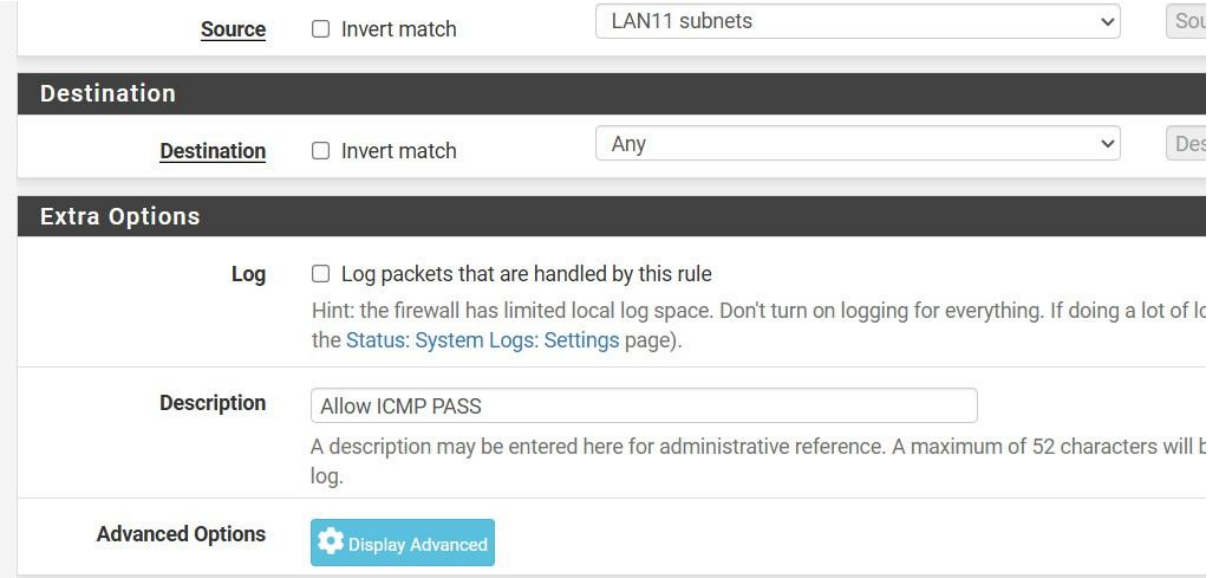


2. **Lets configure set the rules in firewall allow access to icmp and how to set the (FIREWALL-RULES-LAN11-ADD)**



- Go to lan11 add

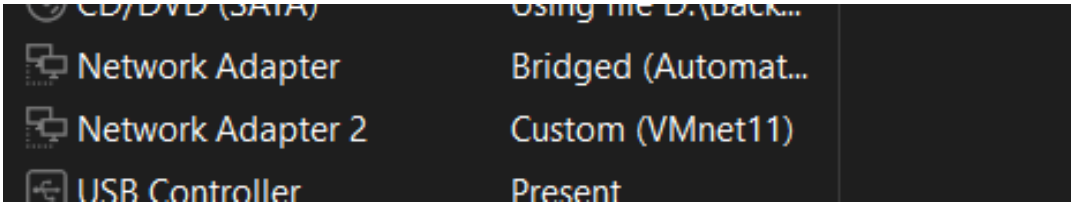




- Next lets ping ip address local machine and vmware machine side also
- Ping 192.168.11.1

```
PS C:\Users\admin> ping 192.168.11.1

Pinging 192.168.11.1 with 32 bytes of data:
Reply from 192.168.11.1: bytes=32 time<1ms TTL=64
Reply from 192.168.11.1: bytes=32 time<1ms TTL=64
Reply from 192.168.11.1: bytes=32 time<1ms TTL=64
Reply from 192.168.11.1: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.11.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

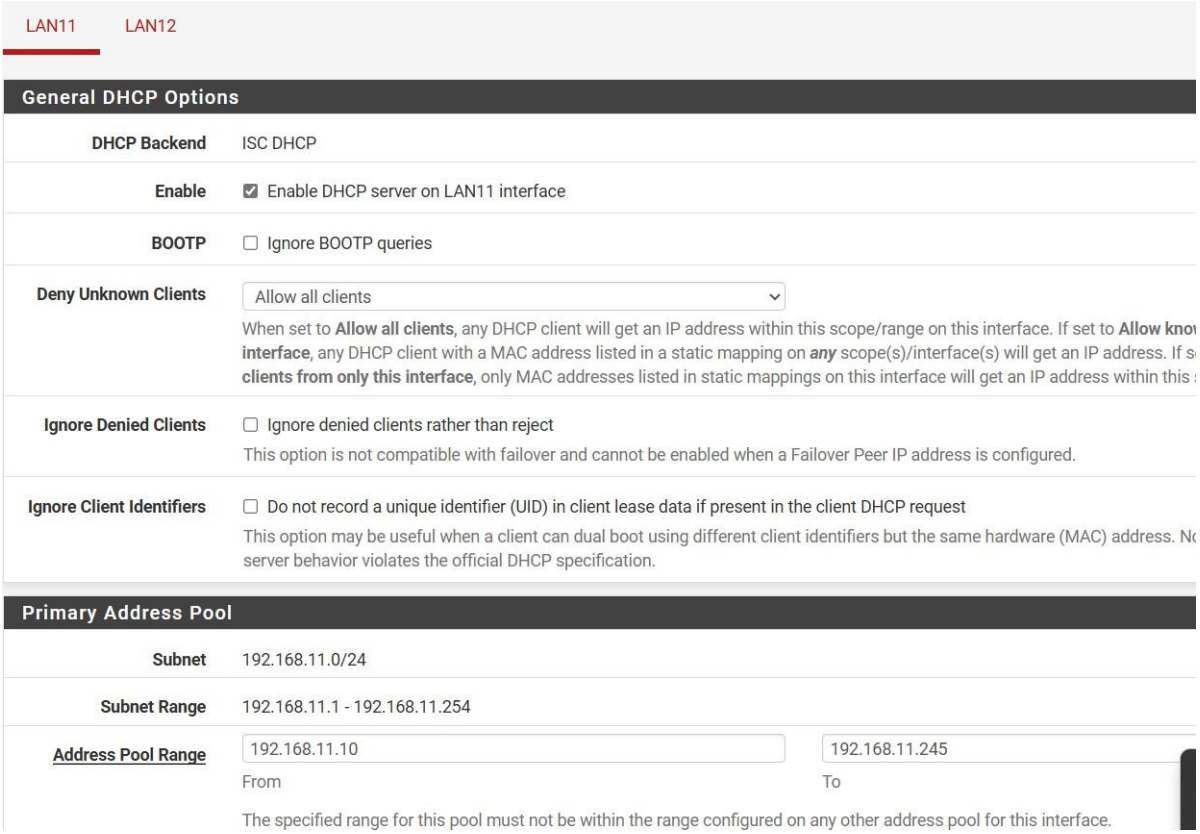
Above the image ip able to ping both local and vmware machine and notes (While pinging the form vmware other machine to firewall make sure enable two network bridge and custom vmet11, are which you save the virtual machine network adaptor

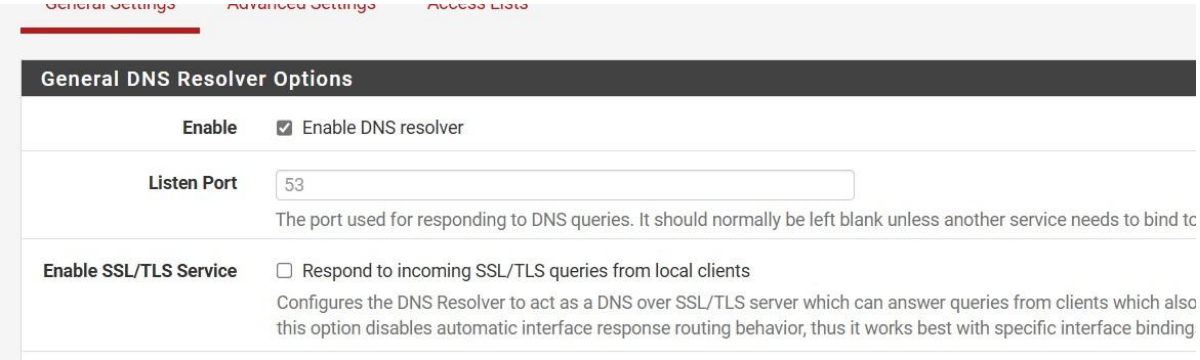


3. And make sure enable ssh of firewall (https://youtu.be/oakOE2iDkhU?si=3S20Gn_NQ7Wf4Ufl) - Follow the videos to access ssh to local machine

```
PS C:\Users\admin> ssh admin@192.168.11.1
The authenticity of host '192.168.11.1 (192.168.11.1)' can't be established.
ED25519 key fingerprint is SHA256:zYohDDludgsfUiDwlWOgNzQZUehxGXtzjlKGrt6+0Xk.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.11.1' (ED25519) to the list of known hosts.
(admin@192.168.11.1) Password for admin@pfSense.blackweb.local:
VMware Virtual Machine - Netgate Device ID: 410e5509dffe45609aee

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

 WAN1 (wan)       -> em0        -> v4/DHCP4: 111.111.111.123/28
 LAN11 (lan)      -> em1        -> v4: 192.168.11.1/24
 LAN12 (opt1)     -> em2        -> v4: 192.168.12.1/24

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

- Before that enable the DHCP server and DNS Resolver





PFSENSE INTERGATED WAZUH:


```
PS C:\Users\admin> ssh admin@192.168.11.1
The authenticity of host '192.168.11.1 (192.168.11.1)' can't be established.
ED25519 key fingerprint is SHA256:zYohDDludgsfUiDwlWOgNzQZUehxGXtzjlKGrt6+0Xk.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.11.1' (ED25519) to the list of known hosts.
(admin@192.168.11.1) Password for admin@pfSense.blackweb.local:
VMware Virtual Machine - Netgate Device ID: 410e5509dffe45609aee

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

 WAN1 (wan)       -> em0        -> v4/DHCP4: 111.111.111.123/28
 LAN11 (lan)      -> em1        -> v4: 192.168.11.1/24
 LAN12 (opt1)     -> em2        -> v4: 192.168.12.1/24

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

- In PFSENSE MACHINE OF SSH press (8) shell will open

- In pfsesne don't have nano and vim editor and we need to install manually which editor your comfortable download the packages
- Pkg install nano or vim (noted : I have the packages in NANO editor)

```
[2.7.2-RELEASE][admin@pfSense.blackweb.local]/root: pkg install nano or vim
```

- Open directories nano /usr/local/etc/pkg/repos/pfSense.conf

```
/usr/local/etc/pkg/repos/pfSense.conf
```

```
FreeBSD: { enabled: yes }

pfSense-core: {
    url: "pkg+https://pkg.pfsense.org/pfSense_v2_7_2_amd64-core",
    mirror_type: "srv",
    signature_type: "fingerprints",
    fingerprints: "/usr/local/share/pfSense/keys/pkg",
    enabled: yes
}

pfSense: {
```

- Next open /usr/local/etc/pkg/repos/FreeBSD.conf

```
/usr/local/etc/pkg/repos/FreeBSD.conf
```

```
  GNU nano 7.2
FreeBSD: { enabled: yes  }
```

- Lets search wazuh-agent (pkg search wazuh-agent)
- The package will like wazuh-agent-4.11.2.1 and download packages (pkg install wazuh-agent) copy version number from machine and install it
- Next once we download the wazuh-agent package and lets update the fressbsd (pkg update -f)

```
[2.7.2-RELEASE][admin@pfSense.blackweb.local]/root:  pkg update -f
```

```
[2.7.2-RELEASE][admin@pfSense.blackweb.local]/root: service wazuh-agent status
wazuh-modulesd is running...
wazuh-logcollector is running...
wazuh-syscheckd is running...
wazuh-agentd is running...
wazuh-execd is running...
[2.7.2-RELEASE][admin@pfSense.blackweb.local]/root:
```

- Next lets edit ossec.conf to add the wazuh-server ip address (nano /var/ossec/etc/ossec.conf)
-

```
    <server>
      <address>192.168.31.84</address>
      <port>1514</port>
      <protocol>tcp</protocol>
    </server>
```

Add wazuh-server Ip address and next change the protocol (udp to tcp) and next save exit and restart wazsuh-agent (service wazuh-agent restart) and next lets check the status in wazuh-server dashboard the pfsense connected or not..

```
[2.7.2-RELEASE][admin@pfSense.blackweb.local]/root: service wazuh-agent status
wazuh-modulesd is running...
wazuh-logcollector is running...
wazuh-syscheckd is running...
wazuh-agentd is running...
wazuh-execd is running...
[2.7.2-RELEASE][admin@pfSense.blackweb.local]/root:
```

ID	Name	IP address	Group(s)	Operating system	Cluster node	Version
003	Backbox1	192.168.31.180	default	Ubuntu 24.04.1 LTS	node01	v4.11.2
004	pfSense.blackweb.local	111.111.111.123	default	BSD 14.0	node01	v4.11.2

Rows per page: 10

Above the images pfsense successfully connected

Wazuh-Server Endpoints Machine

Let's set the rules in wazuh-server to monitoring the pfsense logs and alert message of logs

- Create the new directories in /var/ossec/ruleset

```
# nano /var/ossec/ruleset/decoders/pfsense_custom_decoders.xml
```

```
  GNU nano 6.2                    /var/ossec/ruleset/decoders/pfsense_custom_decoders.xml
<decoder name="pfsense-filterlog">
    <prematch>^filterlog</prematch>
    <regex offset="after_prematch">\s*,\s*,\s*,(\s*),\s*,\s*,(\s*),
(\s*),\s*,\s*,\s*,\s*,\s*,\s*,\s*,\s*,(\s*),\s*,(\s*),(\s*),(\s*),(\s*)</regex>
<order>logid,action,direction,protocol,srcip,dstip,srcport,dstport</order>
</decoder>

<!-- Monitoring Web Ui Confgiuration -->

<!-- PFSENSE PHP-FPM EVENTS -->
<decoder name="pfsense-php">
  <program_name>php-fpm</program_name> </decoder>

<!-- Rule Successful login for user  -->
<decoder name="pfsense-php">
  <parent>pfsense-php</parent>
  <regex type="pcre2">(.*\.php): Successful login for user '(\S+)' from: ([0-9]{1,3}\.[09]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}) \((.*)\)</regex>
  <order>loginpage,username,fromip,authdatabase</order>
  </decoder>

 <!-- Rule Configuration Change: wizard subsystem. -->
 <decoder name="pfsense-php">
   <parent>pfsense-php</parent>
   <regex type="pcre2">(.*\.php): Configuration Change: (\S+)@([0-9]{1,3}\.[0-9]{1,3}\.[09]{1,3}\.[0-9]{1,3}) \((.*)\): (.*)</regex>
   <order>changepage,username,fromip,authdatabase,message</order>
  </decoder>
```

```
root@ubuntu: /home/ubuntu
/var/ossec/ruleset/rules/pfsense_custom_rules.xml
```

```
<group name="pfsense,">
<rule id="87703" level="10" >
        <decoded_as>pfsense-php</decoded_as>
        <match>Successful login for user</match>-->
        <description>A new login was detected in pfSense webGui.</description>
    </rule>
</group>

<group name="pfsense,">
<rule id="87704" level="10">
        <decoded_as>pfsense-php</decoded_as>
        <match>Configuration Change</match>-->
        <description>A configuration change was detected in pfSense firewall.</description>
    </rule>
</group>
```

- Next save the file and exit restart wazuh-server(systemctl restart wazuh-manager)

- **Next open the attack machine (BACKBOX OR KALI,PARROT,ETC)**

  Nc -zv 192.168.1.1 22

Breakdown of the Options:

- nc: Netcat — a network utility for reading/writing data across TCP/UDP.
- -z: "Zero I/O mode" - tells netcat not to send any data, just scan/check.
- -v: Verbose mode - prints the result (e.g., open/closed port).
- 192.168.15.181: The target IP address.
- 22: The port number to check (port 22 is standard for **SSH**).

```
File  Edit  View  Terminal  Tabs  Help
root@Backbox1:/home/backbox# nc -zv 192.168.11.1 22
Connection to 192.168.11.1 22 port [tcp/ssh] succeeded!
root@Backbox1:/home/backbox#
```

4563	error: Fssh_kex_exchange_identification: Connection closed by remote host
30889	Received disconnect from 192.168.11.11 port 48496:11: Bye Bye [preauth]

Next the brute force attack with hydra attack machine (Backbox) ip 1G2.168.11.11 target machine (PFSENSE) 1G2.168.11.1

```
root@Backbox1:/home/backbox# hydra -l admin -P pass.txt 192.168.11.1 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or f
inding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-05-05 12:21:37
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 10 tasks per 1 server, overall 10 tasks, 10 login tries (l:1/p:10), ~1 try per task
[DATA] attacking ssh://192.168.11.1:22/
```

17118	Blocking "192.168.11.11/32" for 240 secs (4 attacks in 0 secs, after 2 abuses over 570 secs.)
39931	Failed password for admin from 192.168.11.11 port 40452 ssh2
39633	Failed password for admin from 192.168.11.11 port 40430 ssh2
40058	Failed password for admin from 192.168.11.11 port 40462 ssh2
40340	Failed password for admin from 192.168.11.11 port 40482 ssh2
39826	Failed password for admin from 192.168.11.11 port 40438 ssh2
39826	fatal: userauth_finish: send failure packet: Permission denied [preauth]

.235	pfSense.blackweb.local	sshd: authentication failed.
.232	pfSense.blackweb.local	sshd: authentication failed.
.229	pfSense.blackweb.local	sshd: authentication failed.
.227	pfSense.blackweb.local	sshd: authentication failed.
.224	pfSense.blackweb.local	sshd: authentication failed.

	@timestamp	May 5, 2025 @ 12:21:38.235
t	_index	wazuh-alerts-4.x-2025.05.05
t	agent.id	004
t	agent.ip	111.111.111.123
t	agent.name	pfSense.blackweb.local
t	data.dstuser	admin
t	data.srcip	192.168.11.11
t	data.srcport	40438
t	decoder.name	sshd

t	rule.description	sshd: authentication failed.
#	rule.firedtimes	3
t	rule.gdpr	IV_35.7.d, IV_32.2
t	rule.gpg13	7.1
t	rule.groups	syslog, sshd, authentication_failed
t	rule.hipaa	164.312.b
t	rule.id	5760
#	rule.level	5

t	rule.mitre.tactic	Credential Access, Lateral Movement
t	rule.mitre.technique	Password Guessing, SSH
t	rule.nist_800_53	AU.14, AC.7

Refer:

https://youtu.be/eFzG44Ngulo?si=vFGz0LADblCrwxTG

https://youtu.be/_AiJiS2gtFE?si=jMu450-xneva-r1Z

https://github.com/StevenBlack/hosts

https://youtu.be/ebPnF74RgFw?si=m6foYM5B9Y8mlylI (ICMP) VIEDOS ALLOW PORT

AT END OPEN PFSENSE SHELL nano /usr/local/etc/pkg/repos/pfSense.conf change to enable (No)

Nano /usr/local/etc/pkg/repos/FreeBSD.conf – changed enable yes to NO

Next save and exit (pkg update -f)