

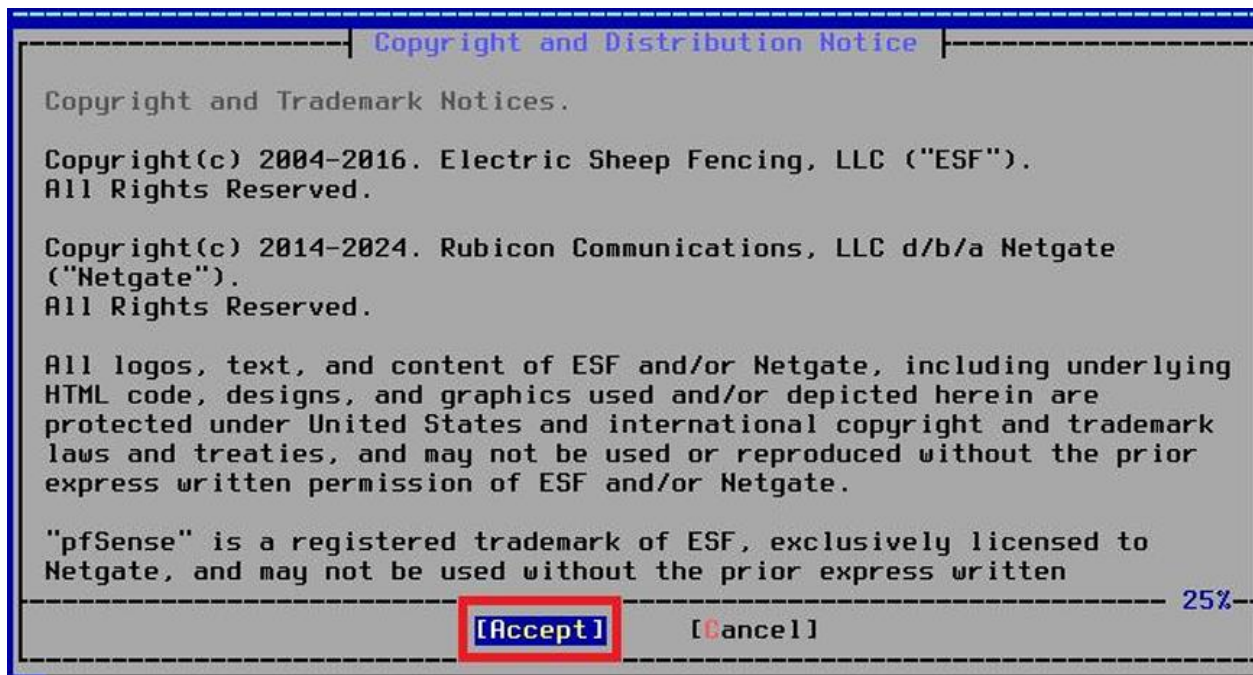
# Task 2 Submission

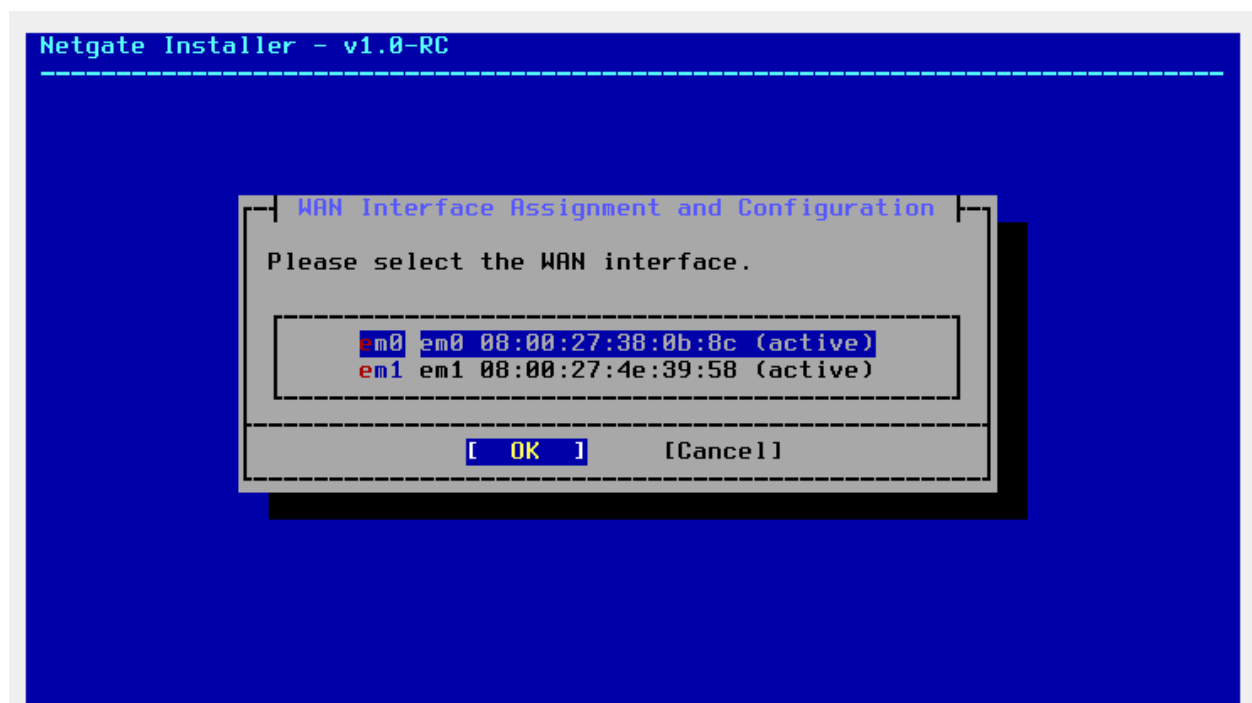
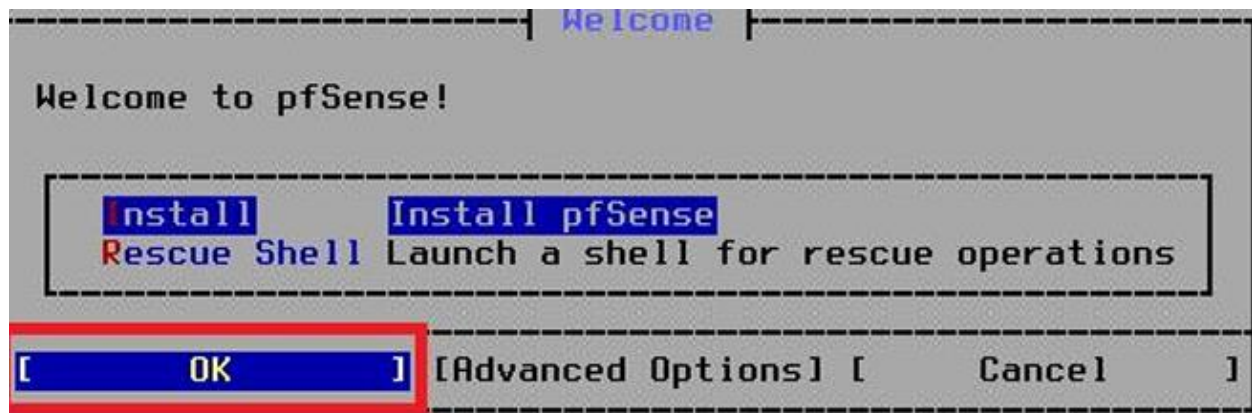
## Syed Hasa Raza Rizvi

### Tasks assigned:

1. Configure pfSense to forward logs to the Wazuh Manager using Syslog.
2. Verify pfSense logs are appearing in the Wazuh dashboard.
3. Install Suricata IDS on a separate Linux machine or within pfSense.
4. Configure Suricata to generate alerts and forward them to Wazuh.
5. Simulate a port scan using nmap from one machine to another.
6. Capture the Suricata alert triggered by the port scan in the Wazuh dashboard

Setting up and configuring pfsense:





Netgate Installer - v1.0-RC

---

WAN (em0) Network Mode Setup

Adjust the network operation mode for the WAN (em0) interface if necessary.

>>> Continue	Proceed with the installation
M Interface Mode	DHCP (client)
V VLAN Settings	VLAN Tagging disabled
U Use local resolver	false

[ OK ] [Cancel]

Continue with the displayed settings

Netgate Installer - v1.0-RC

---

LAN Interface Assignment and Configuration

Please select the LAN interface.

None	Do not assign the LAN interface
m1	em1 08:00:27:4e:39:58 (active)

[ OK ] [ Skip ] [Cancel]

## Netgate Installer - v1.0-RC

### LAN (em1) Network Mode Setup

Adjust the network operation mode for the LAN (em1) interface if necessary.

>>> Continue	Proceed with the installation
M Interface Mode	STATIC
V VLAN Settings	VLAN Tagging disabled
I IP Address	192.168.1.1/24
D DHCPD Enabled	true
S DHCPD Range Start	192.168.1.100
E DHCPD Range End	192.168.1.150

[ OK ]

[Cancel]

Continue with the displayed settings

### Interface Assignment and Configuration

Detected: VirtualBox Virtual Machine

Please confirm the interface assignment to continue with the installation.

LAN	em1 (active)
WAN	em0 (active)

[ Continue ]

[Assign/Configure]

[ Cancel ]

### Connectivity Check

Verifying the Internet connection...

Trying to reach the Netgate Servers, please wait (this can take a while)...

### Netgate Installer - v1.0-RC

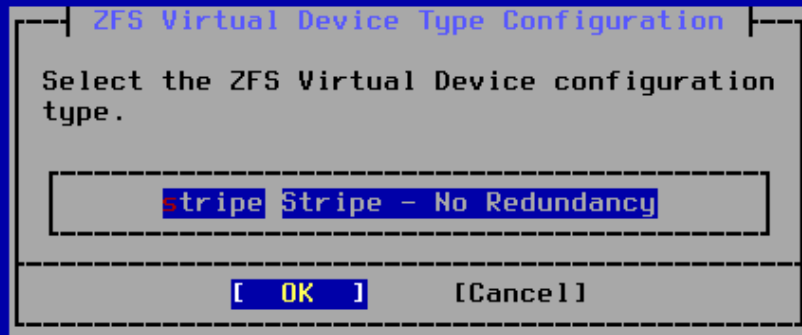
### Installation Options

Please select the File System type and the Partition Scheme.

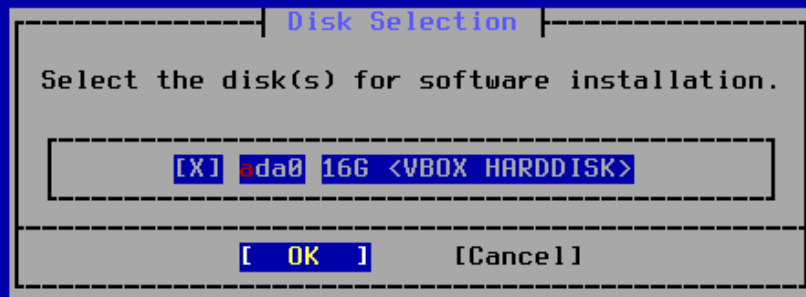
>>> Continue	Proceed with the installation
F File System	ZFS (recommended default)
P Partition Scheme	GPT (compatible with MBR)

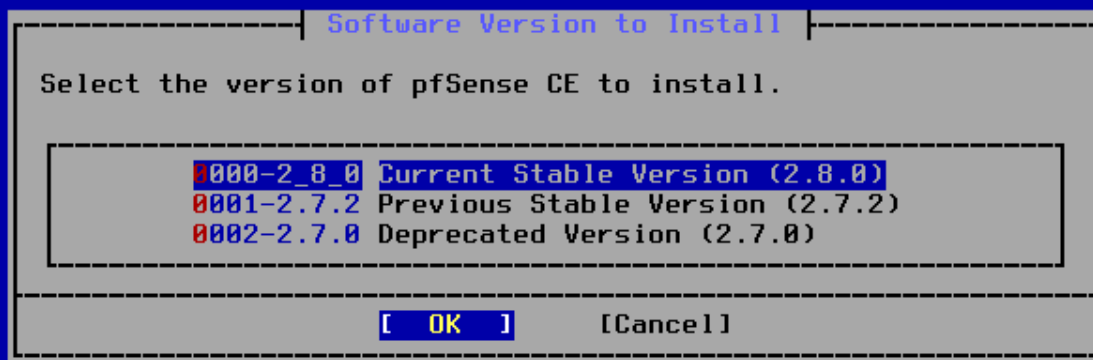
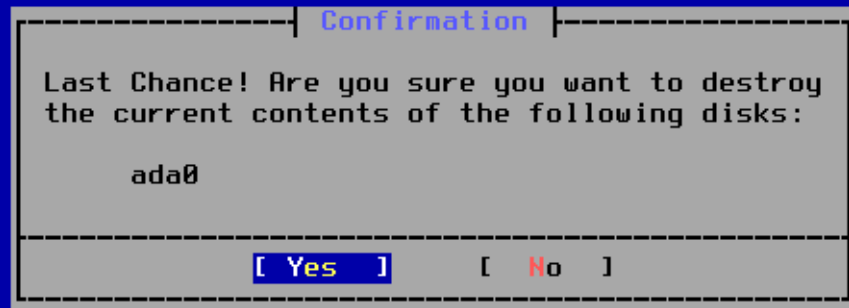
[ OK ]

[Cancel]



Netgate Installer - v1.0-RC





#### Installation Details

Installing Current Stable Version (2.8.0)

Selected configuration file: default (blank) configuration.

Installing pkg

Updating pfSense-core repository catalogue...



#### Installation Details

GPUs starting with the HD7000 series / Tahiti) or i915kms (for Intel APUs starting with HD3000 / Sandy Bridge) through kld\_list in /etc/rc.conf. radeonkms for older AMD GPUs can be loaded and there are some positive reports if EFI boot is NOT enabled.

For amdgpu: kld\_list="amdgpu"  
For Intel: kld\_list="i915kms"  
For radeonkms: kld\_list="radeonkms"

Please ensure that all users requiring graphics are members of the "video" group.

Please note that this package was built for FreeBSD 15.0.  
If this is not your current running version, please rebuild it from ports to prevent panics when loading the module.

pfSense Post Installation setup

pfSense Post Installation setup .. done.

< OK >

Netgate Installer - v1.0-RC

#### Complete

Installation of pfSense complete! Would you like to reboot into the installed system now?

[Reboot]

[Shell]

```
Starting CRON... done.
pfSense 2.8.0-RELEASE amd64 20250521-2312
Bootup complete

FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)

VirtualBox Virtual Machine - Netgate Device ID: ca766483530783f286aa

*** Welcome to pfSense 2.8.0-RELEASE (amd64) on pfSense ***

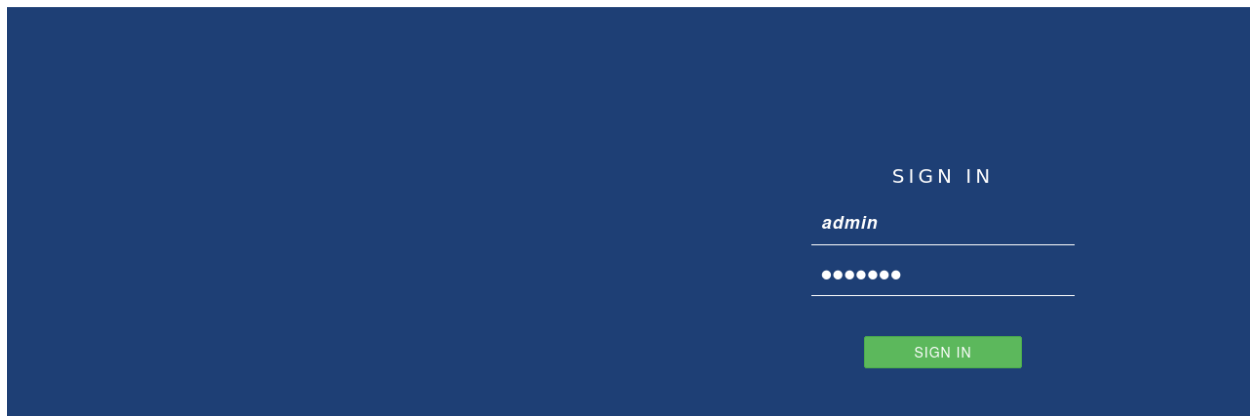
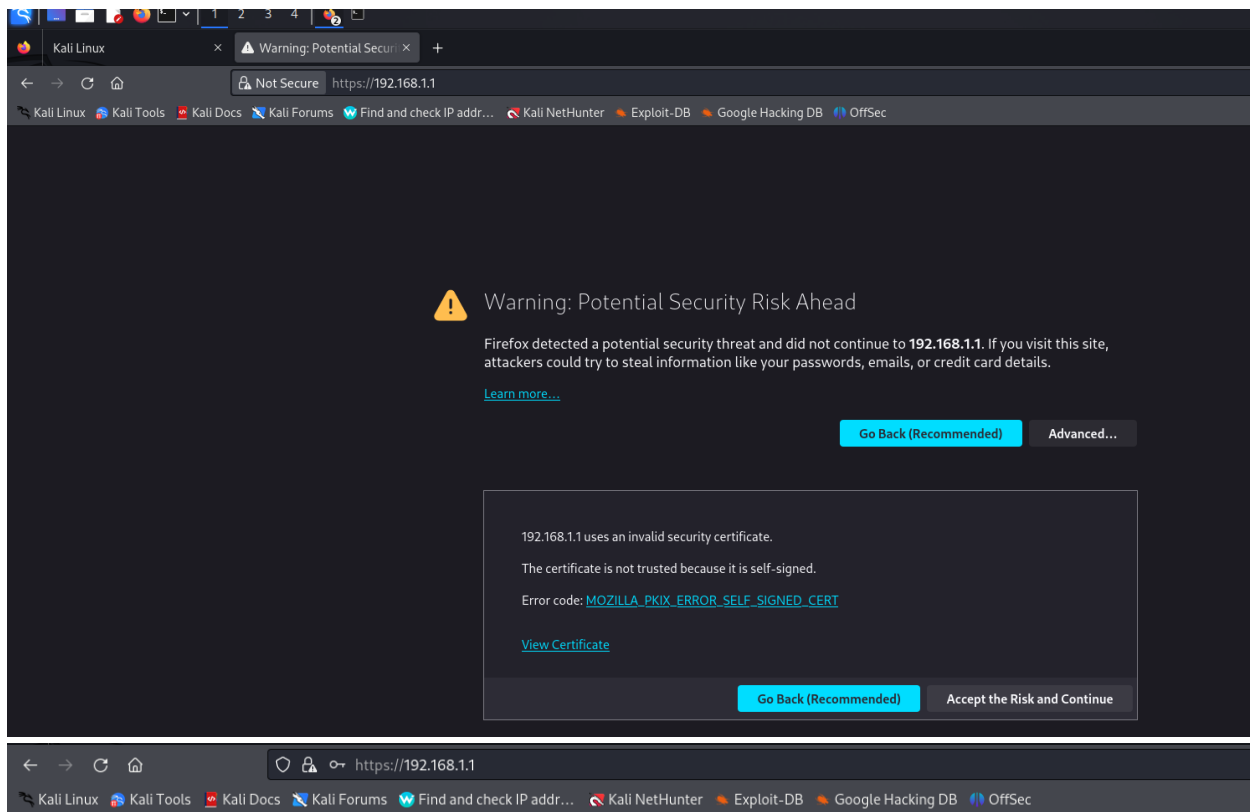
WAN (wan) -> em0 -> v4/DHCP4: 10.0.2.15/24
                        v6/DHCP6: fd00::a00:27ff:fe38:b8c/64
LAN (lan) -> em1 -> v4: 192.168.1.1/24

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: █
```

This is the ip of pfsense: 192.168.1.1

Turned on kali and search this ip on the browser





[» Next](#)

[» Next](#)

Activate

**WARNING:**

The password for this account is insecure. Password is currently set to the default value (pfsense).  
Change the password as soon as possible.

## Wizard / pfSense Setup / Configure LAN Interface

Step 5 of 9

## Configure LAN Interface

On this screen the Local Area Network information will be configured.

LAN IP Address

Type dhcp if this interface uses DHCP to obtain its IP address.

Subnet Mask

&gt;&gt; Next

## Step-by-Step Integration

### Step 1: Enable Remote Logging in pfSense

The screenshot shows the pfSense web interface in a browser. The address bar displays `https://192.168.1.1/wizard.php?xml=setup_wizard.xml&stepid=9`. The browser's tab bar includes links to Kali Linux, Kali Tools, Kali Docs, Kali Forums, Find and check IP address, Kali NetHunter, Exploit-DB, Google Hacking DB, and OffSec. The pfSense header shows the 'Community Edition' logo and navigation menus for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. The main content area is titled 'Wizard / pfSense Setup / Wizard completed.' and features a green progress bar for 'Step 9 of 9'. Below this, a dark banner reads 'Wizard completed.' The main text area contains the following information:

- Congratulations! pfSense is now configured.**  
We recommend that you check to see if there are any software updates available. Keeping your software up to date is one of the most important things you can do to maintain the security of your network.  
[Check for updates](#)
- Remember, we're here to help.**  
[Click here](#) to learn about Netgate 24/7/365 support services.
- User survey**  
Please help all the people involved in improving and expanding pfSense software by taking a moment to answer this short survey (all answers are anonymous)  
[Anonymous User Survey](#)
- Useful resources.**
  - Learn more about Netgate's product line, services, and pfSense software from our [website](#)
  - To learn about Netgate appliances and other offers, [visit our store](#)
  - Become part of the pfSense community. Visit our [forum](#)
  - Subscribe to our [newsletter](#) for ongoing product information, software announcements and special offers.

At the bottom left is a blue 'Finish' button. On the right side, there is a partially visible 'Activate W' button and a 'Go to Setting:' link.

← → ↻ 🏠 [https://192.168.1.1/status\\_logs\\_settings.php](https://192.168.1.1/status_logs_settings.php)

Kali Linux Kali Tools Kali Docs Kali Forums Find and check IP addr... Kali NetHunter Exploit-DB Google Hacking DB OffSec

**Enable Remote Logging**

☒ Send log messages to remote syslog server

Source Address

LAN

This option will allow the logging daemon to bind to a single IP address, rather than all IP addresses. If a single IP is picked, remote syslog servers must all be of that IP type. To mix IPv4 and IPv6 remote syslog servers, bind to all interfaces.

NOTE: If an IP address cannot be located on the chosen interface, the daemon will bind to all addresses.

IP Protocol

IPv4

This option is only used when a non-default address is chosen as the source above. This option only expresses a preference; If an IP address of the selected type is not found on the chosen interface, the other type will be tried.

Remote log servers

192.168.1.20:514

IP[port]

IP[port]

Remote Syslog Contents

☒ Everything

☐ System Events

☐ Firewall Events

☐ DNS Events (Resolver/unbound, Forwarder/dnsmasq, filterdns)

☐ DHCP Events (DHCP Daemon, DHCP Relay, DHCP Client)

☐ PPP Events (PPPoE WAN Client, LZTP WAN Client, PPTP WAN Client)

☐ General Authentication Events

☐ Captive Portal Events

☐ VPN Events (IPsec, OpenVPN, LZTP, PPPoE Server)

☐ Gateway Monitor Events

☐ Routing Daemon Events (RADVD, UPnP, RIP, OSPF, BGP)

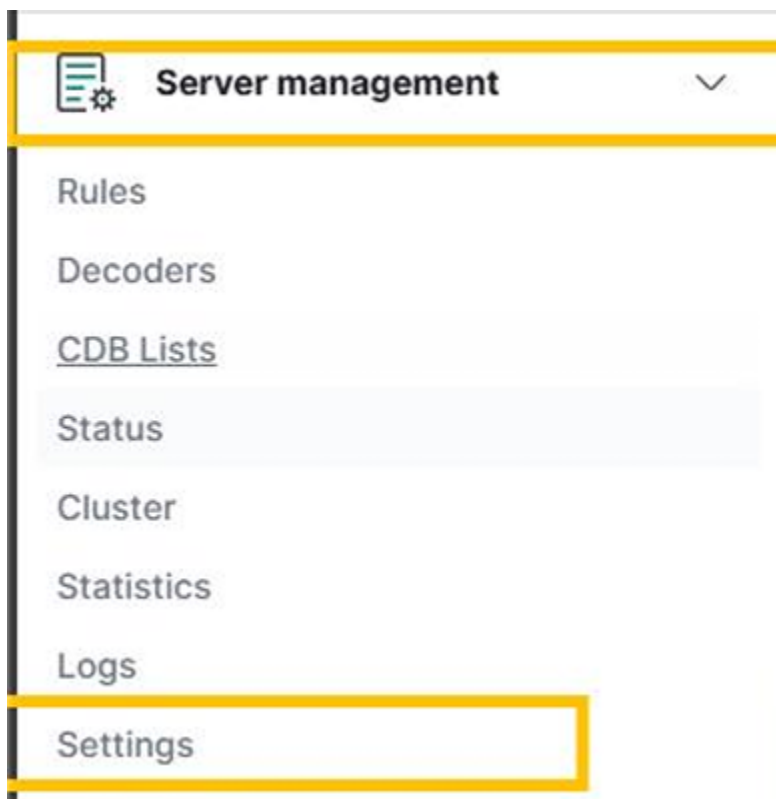
☐ Network Time Protocol Events (NTP Daemon, NTP Client)

☐ Wireless Events (hostapd)

Syslog sends UDP datagrams to port 514 on the specified remote syslog server, unless another port is specified. Be sure to set syslogd on the remote server to accept syslog messages from pfSense.

Save

## Step 2: Custom Syslog Configuration (for UI Logs)



## Main configurations

Name	Description
Global Configuration	Global and remote settings
Cluster	Master node configuration
Registration Service	Automatic agent registration service


Edit `/var/ossec/etc/ossec.conf` on the Wazuh Manager.


Add the following in the `<remote>` section:

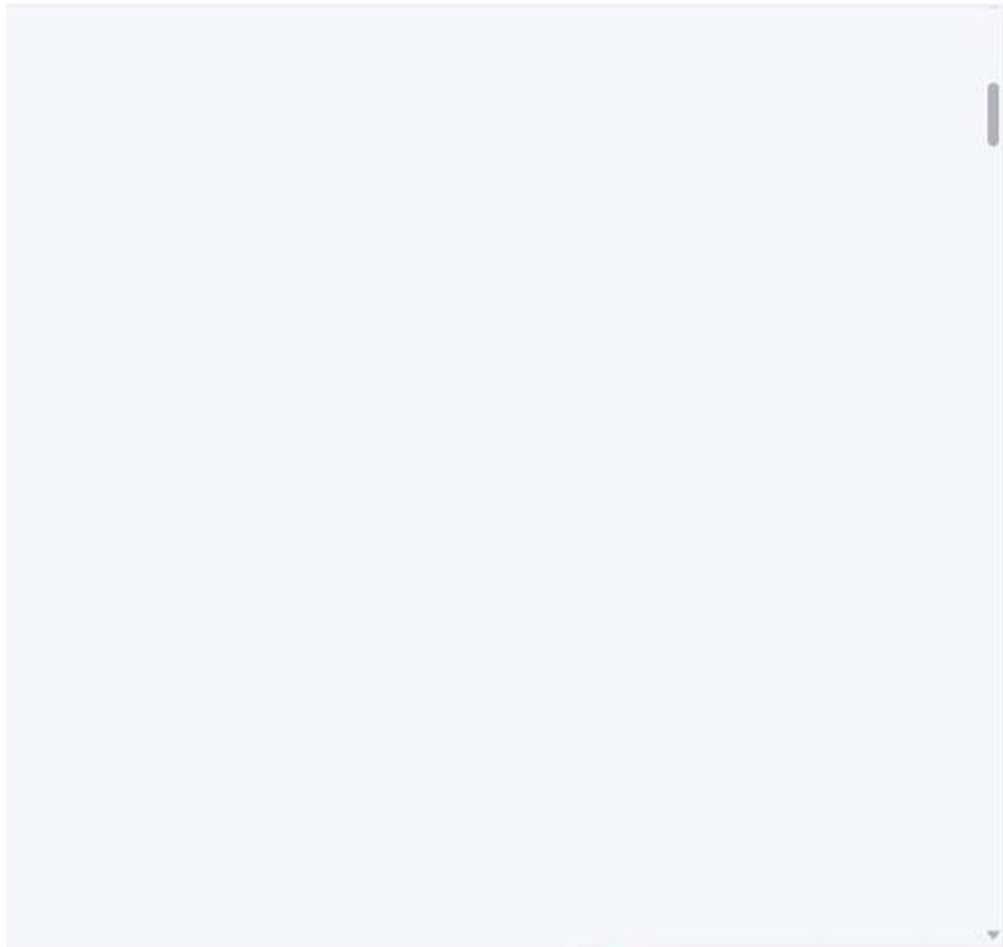
```
<!-- pfSense Firewall Integration -->
<remote>
<connection>syslog</connection>
<port>514</port>
<protocol>udp</protocol>
<allowed-ips>Pfsense WAN IP/24</allowed-ips>
<local_ip>Wazuh IP</local_ip>
</remote>
```

Replace `Pfsense_WAN_IP/24` and `Wazuh_Server_IP` with actual IP addresses.

 Refresh

 Save

 Restart Manager



Manager was restarted

### Step 3: Add Custom Decoders & Rules (for UI Event Parsing)

#### Decoders (3)

 Manage decoders files

 Add new decoders file

 Refresh

 Export formatted

From here you can manage your decoders.

relative\_dirname=etc/decoders

WQL

Custom decoders

Name	Program name	Order	File ↑	Path
------	--------------	-------	--------	------

Custom Decoder: `/var/ossec/etc/decoders/`. Create `pfsense-custom-decoder.xml` in `/var/ossec/etc/decoders/`.



```
<!-- add new decoder for pfsense "Filename: pfsense-custom-  
decoder.xml"-->
```

```
<decoder name="pfsense-custom">
```

```
  <prematch>filterlog</prematch>
```

```
</decoder>
```

```
<decoder name="pfsense-fields">
```

```
  <parent>pfsense-custom</parent>
```

```
  <regex>^(\w+)[\d]:  
  \S*,\S*,\S*,(\S*),\S*,\S*,(\S*),\S*,\S*,\S*,\S*,\S*,\S*,\S*,\S*,(\S*),\  
  \S*,(\S*),(\S*),(\d*),(\d*),\S*</regex>
```

```
  <order>logsource,id,action,protocol,srcip,dstip,srcport,dstport</order>
```

```
</decoder>
```



```
<pfsense-custom-decoder.xml  
Decoders Test Save  
1 <decoder name="pfsense-custom">  
2   <prematch>filterlog</prematch>  
3 </decoder>  
4  
5 <decoder name="pfsense-fields">  
6   <parent>pfsense-custom</parent>  
7   <regex>^(\w+)[\d]: \S*,\S*,\S*,(\S*),\S*,\S*,(\S*),\S*,\S*,\S*,\S*,\S*,\S*,\S*,\S*,(\S*),  
8   \S*,(\S*),(\S*),(\d*),(\d*),\S*</regex>  
9   <order>logsource,id,action,protocol,srcip,dstip,srcport,dstport</order>  
10 </decoder>
```

Custom Rules: Create pfsense-custom-rules.xml in /var/ossec/etc/rules/.

Rules (4,498)

[Manage rules files](#) [Add new rules file](#) [Refresh](#) [Export formatted](#)

From here you can manage your rules.

Search							WQL	Custom rules
ID ↑	Description	Groups	Regulatory compliance	Level	File	Path		
1	Generic template for all syslog rules.	syslog		0	0010-rules_config.xml	ruleset/rules		
2	Generic template for all firewall rules.	firewall		0	0010-rules_config.xml	ruleset/rules		
3	Generic template for all ids rules.	ids		0	0010-rules_config.xml	ruleset/rules		
4	Generic template for all web rules.	web-log		0	0010-rules_config.xml	ruleset/rules		
5	Generic template for all web proxy rules.	squid		0	0010-rules_config.xml	ruleset/rules		

< pfSense-custom-rules.xml

[Ruleset Test](#) [Save](#)

```
1 <group name="pfSense, custom, ">
2 <rule id="100900" level="0">
3   <decoded_as>pfSense-custom</decoded_as>
4   <field name="logsource">filterlog</field>
5   <description>pfSense firewall rules grouped.</description>
6 </rule>
7
8 <rule id="100901" level="4">
9   <if_sid>100900</if_sid>
10  <action>pass</action>
11  <options>no_full_log</options>
12  <description>pfSense firewall allow event.</description>
13  <group>firewall_allow,pci_dss_1.4,gpg13_4.12,hipaa_164.312.a.1,nist_800_53_SC.7,tsc_CC6.7,tsc_CC6.8,</group>
14 </rule>
15
16 <rule id="100902" level="5">
17   <if_sid>100900</if_sid>
18   <action>block</action>
19   <options>no_full_log</options>
20   <description>pfSense firewall drop event.</description>
21   <group>firewall_block,pci_dss_1.4,gpg13_4.12,hipaa_164.312.a.1,nist_800_53_SC.7,tsc_CC6.7,tsc_CC6.8,</group>
22 </rule>
23
24 <rule id="100903" level="10" frequency="10" timeframe="45" ignore="240">
25   <if_matched_sid>100902</if_matched_sid>
26   <same_source_ip />
27   <description>Multiple pfSense firewall blocks events from same source.</description>
28   <mitre>
29     <ids>T1110</ids>
```

Restart the Wazuh Manager to apply changes.

## Step 4: Configure Wazuh Manager

Add a custom log collection rule in Wazuh to parse pfSense logs. Use decoders and rules to categorize events (e.g., firewall denials, port scans, login attempts)

2. Verify pfSense logs are appearing in the Wazuh dashboard.

## Step 5: Monitor Logs

Logs from pfSense are forwarded to Wazuh Manager for analysis

rule.description	rule.level	rule.id
pfSense firewall drop event.	5	100902
pfSense firewall drop event.	5	100902
pfSense firewall drop event.	5	100902
pfSense firewall drop event.	5	100902
pfSense firewall drop event.	5	100902
pfSense firewall drop event.	5	100902
pfSense firewall drop event.	5	100902
pfSense firewall drop event.	5	100902
pfSense firewall drop event.	5	100902
pfSense firewall drop event.	5	100902
pfSense firewall drop event.	5	100902
pfSense firewall drop event.	5	100902
pfSense firewall drop event.	5	100902
pfSense firewall drop event.	5	100902
pfSense firewall drop event.	5	100902
pfSense firewall drop event.	5	100902

### 3. Install Suricata IDS on a separate Linux machine

#### Step-by-Step Setup Instructions Step 1: Set Up kali-NIDS and Install Suricata

```
sudo apt update
```

```
sudo apt install suricata-y
```

#### Step 2: Download and Install Suricata Rules

```
wget https://rules.emergingthreats.net/open/suricata/emerging.rules.tar.gz
```

```
sudo tar-xvzf emerging.rules.tar.gz
```

```
sudo mv rules/*.rules /etc/suricata/rules/
```

```
sudo chmod-R 644 /etc/suricata/rules/*
```

### 4. Configure Suricata to generate alerts and forward them to Wazuh.

#### Step 3: Configure Suricata Edit Suricata config:

```
sudo nano /etc/suricata/suricata.yaml
```

Update network variables:

```
HOME_NET: "[192.168.1.1/24]"
```

```
EXTERNAL_NET: " !$HOME_NET"
```

Set network interface (replace enp0s3 with yours):

af-packet:

- interface: enp0s3

```
# Linux high speed capture support
af-packet:
- interface: eth0
  # Number of receive threads. "auto"
  #threads: auto
  # Default clusterid. AF_PACKET will
```

Enable promiscuous mode:

sudo ip link set eth0 promisc on

Restart Suricata:

sudo systemctl restart suricata

sudo systemctl enable suricata

Step 4: Already Installed Wazuh Agent on kali-NIDS

Configure Wazuh Agent:

sudo nano /var/ossec/etc/ossec.conf

Set manager IP:

<client>

<server>

<address>" your address" </address>

</server>

</client>

Step 5: Configure Wazuh to Monitor Suricata Logs

Suricata logs live here: /var/log/suricata/eve.json

Edit agent config again:

```
sudo nano /var/ossec/etc/ossec.conf
```

Add:

```
<localfile>
```

```
<log_format>json </log_format>
```

```
<location> /var/log/suricata/eve.json</location>
```

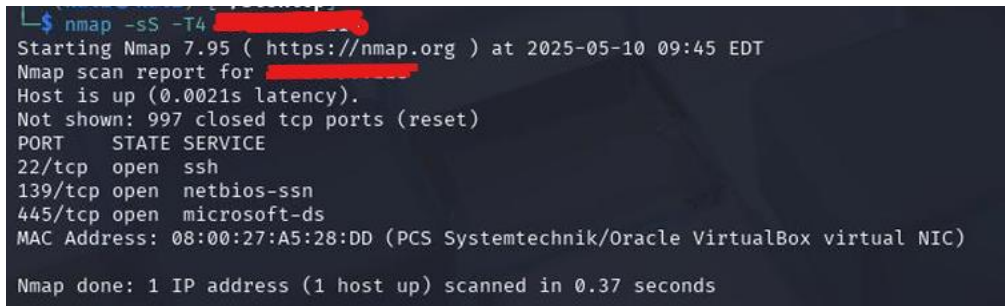
```
</localfile>
```

Restart Wazuh Agent:

```
sudo systemctl restart wazuh-agent
```

5. Simulate a port scan using nmap from one machine to another.

Step 6: Trigger and Detect an Intrusion:

A terminal window showing the output of an nmap scan. The command executed is 'nmap -sS -T4 [redacted]'. The output indicates the host is up with a latency of 0.0021s. It lists three open ports: 22/tcp (ssh), 139/tcp (netbios-ssn), and 445/tcp (microsoft-ds). The MAC address is 08:00:27:A5:28:DD, identified as a virtual NIC. The scan completed in 0.37 seconds.

```
$ nmap -sS -T4 [redacted]
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-10 09:45 EDT
Nmap scan report for [redacted]
Host is up (0.0021s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
MAC Address: 08:00:27:A5:28:DD (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

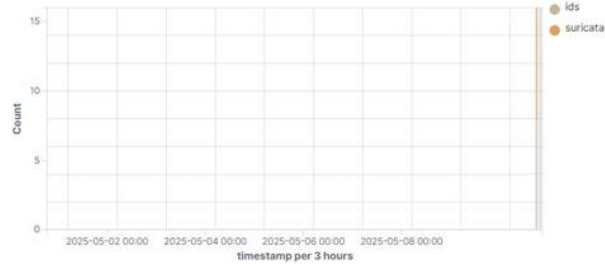
Nmap done: 1 IP address (1 host up) scanned in 0.37 seconds
```

Then, log into Wazuh Dashboard > Modules > Security Events or NIDS

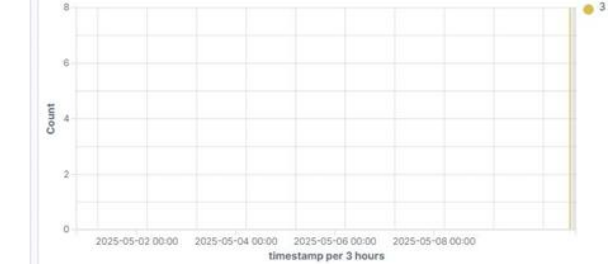
Look for Suricata alerts (e.g., Nmap scan detection).

6. Capture the Suricata alert triggered by the port scan in the Wazuh dashboard

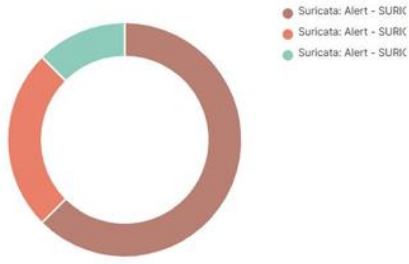
Top 10 Alert groups evolution



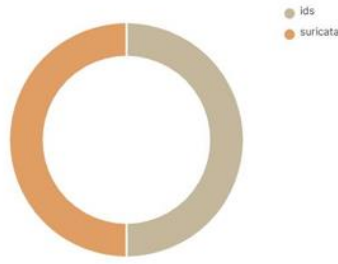
Alerts



Top 5 alerts



Top 5 rule groups



Top 5 PCI DSS Requirements

No results found

Suricata: Alert - SURICATA HTTP invalid content length field in request

Suricata: Alert - SURICATA SMB malformed request dialects

Suricata: Alert - SURICATA SMB malformed request dialects

Suricata: Alert - SURICATA SMB malformed request dialects

Suricata: Alert - SURICATA SMB malformed request dialects

Suricata: Alert - SURICATA SMB malformed request dialects

Suricata: Alert - SURICATA ICMPv4 unknown code

Suricata: Alert - SURICATA ICMPv4 unknown code