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.

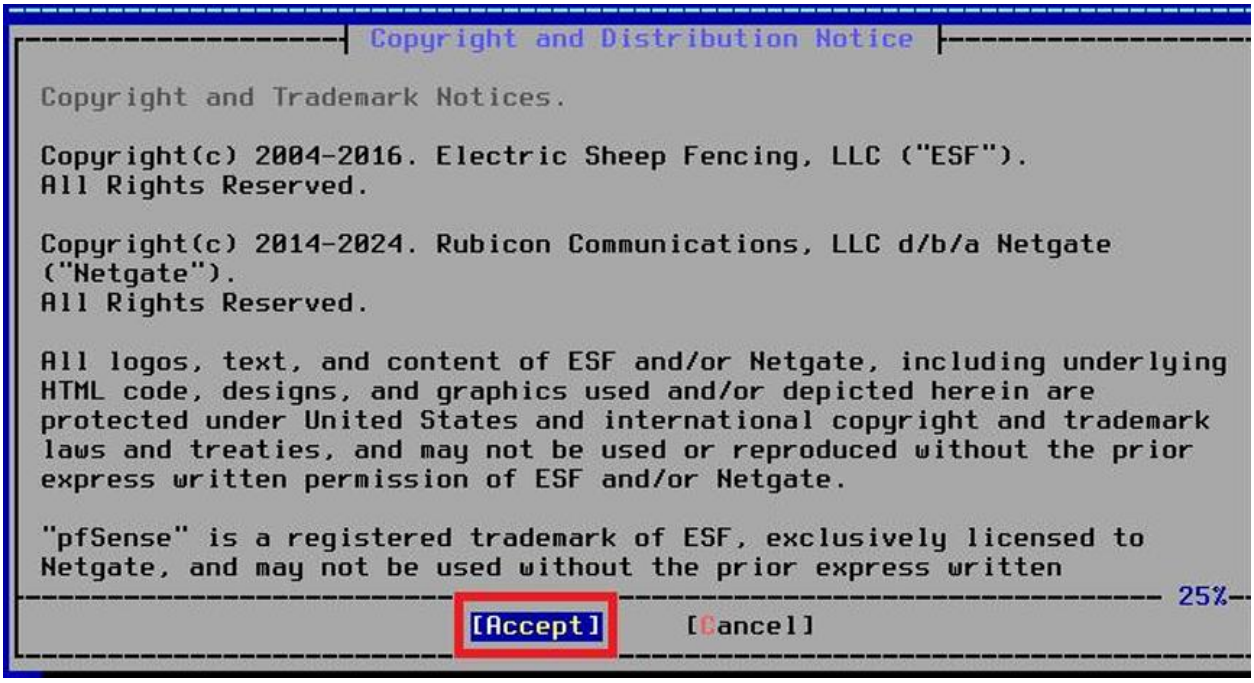
3. Install Suricata IDS on a separate Linux machine or within pfSense.

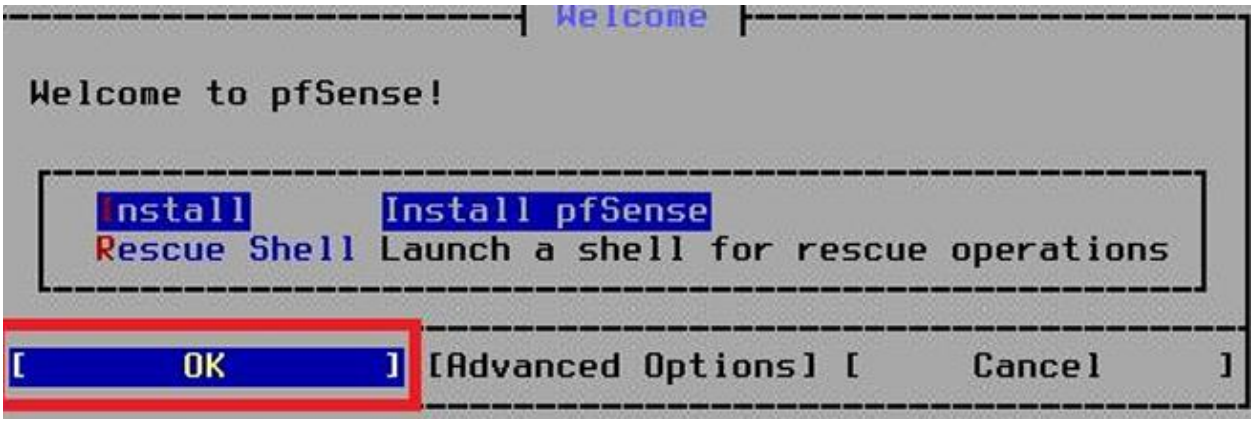
4. Configure Suricata to generate alerts and forward them to Wazuh.

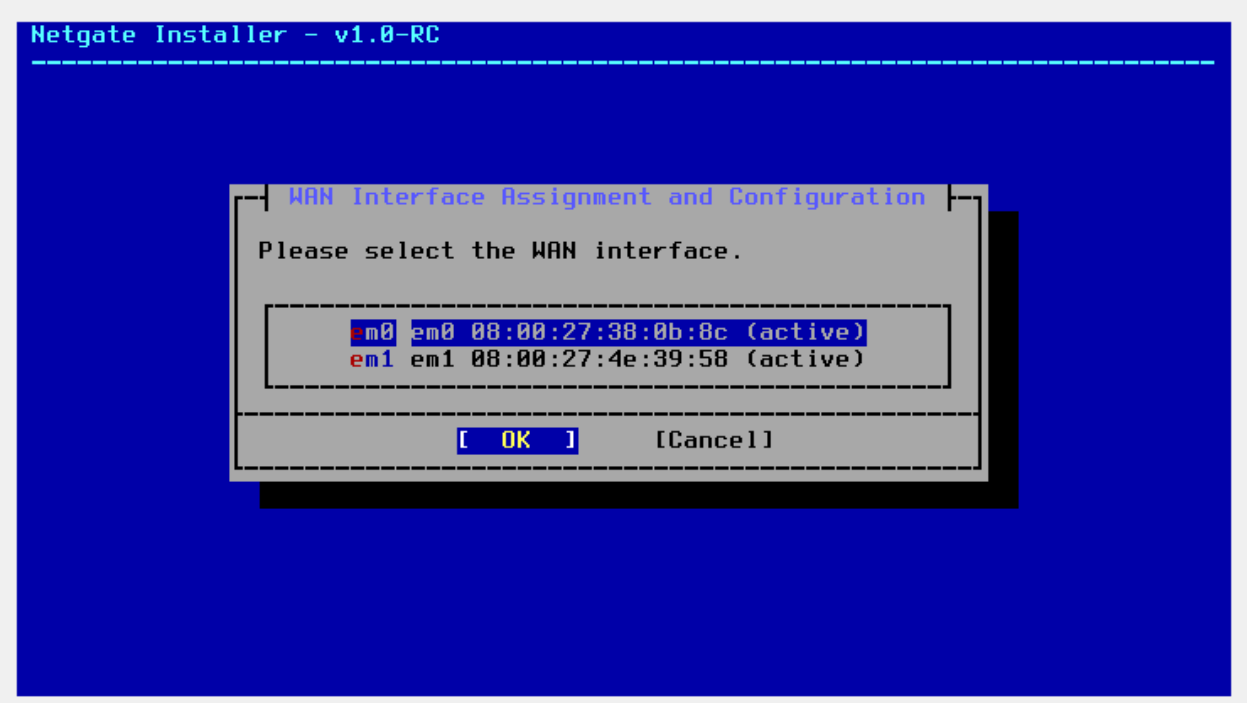
5. Simulate a port scan using nmap from one machine to another.

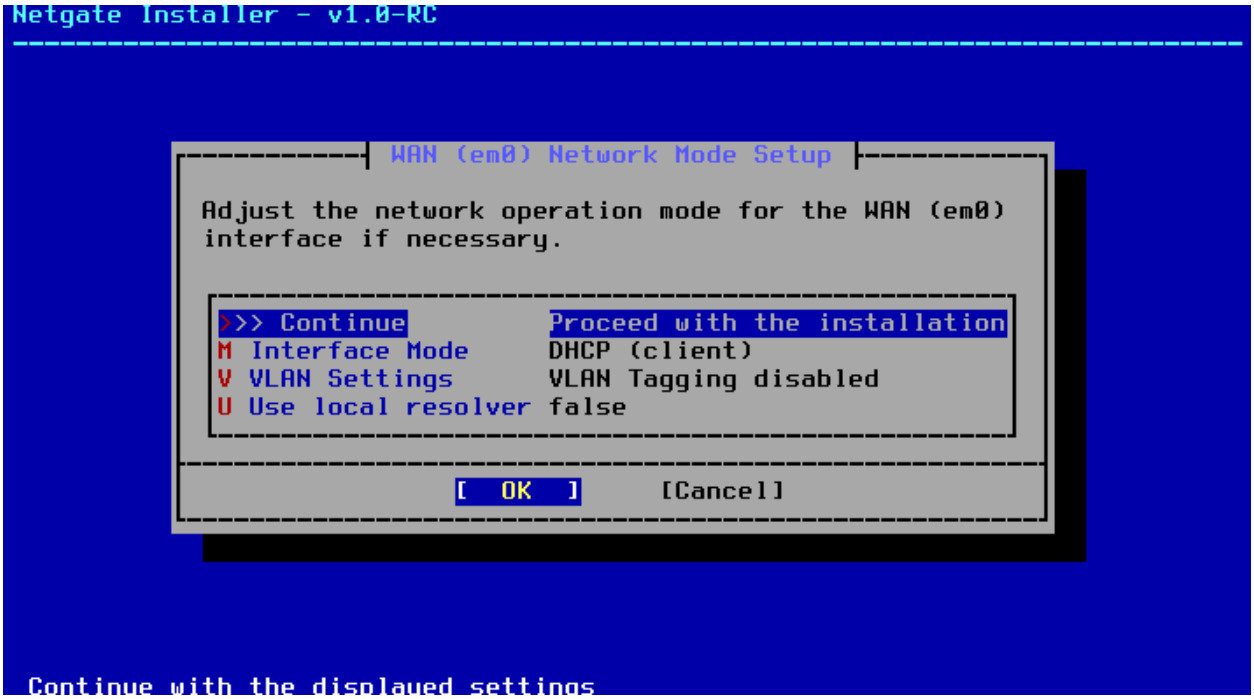
6. Capture the Suricata alert triggered by the port scan in the Wazuhdashboard

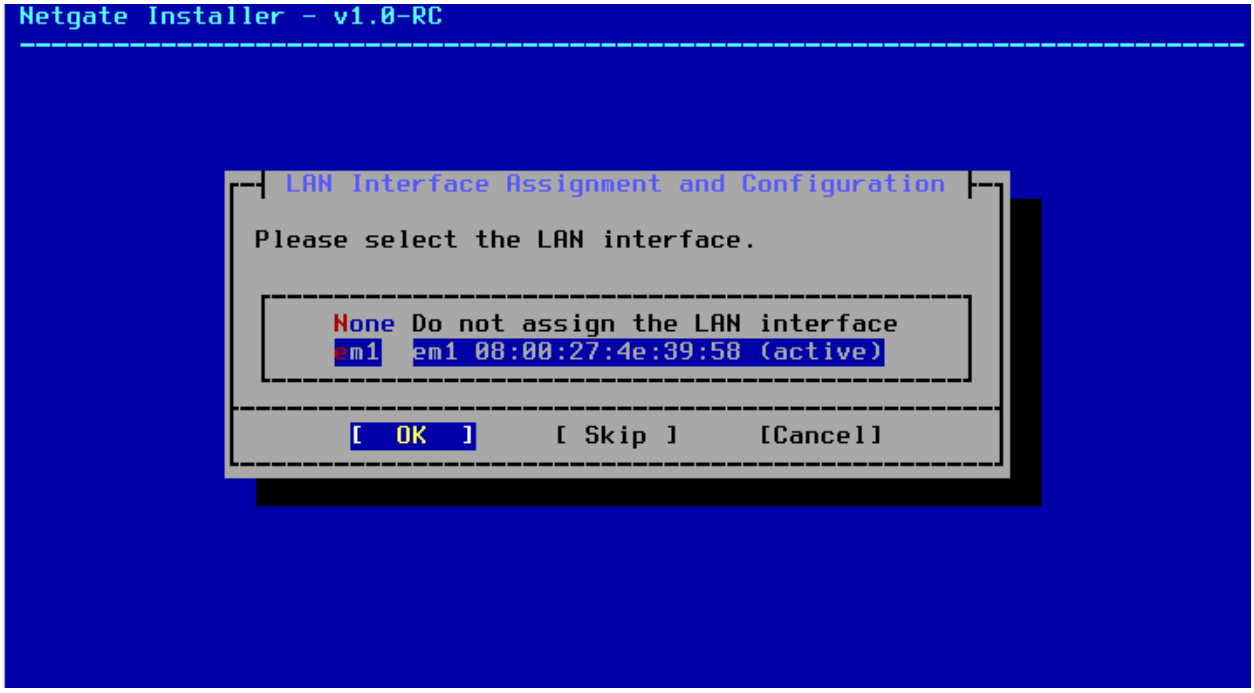
Setting up and configuring pfsense:

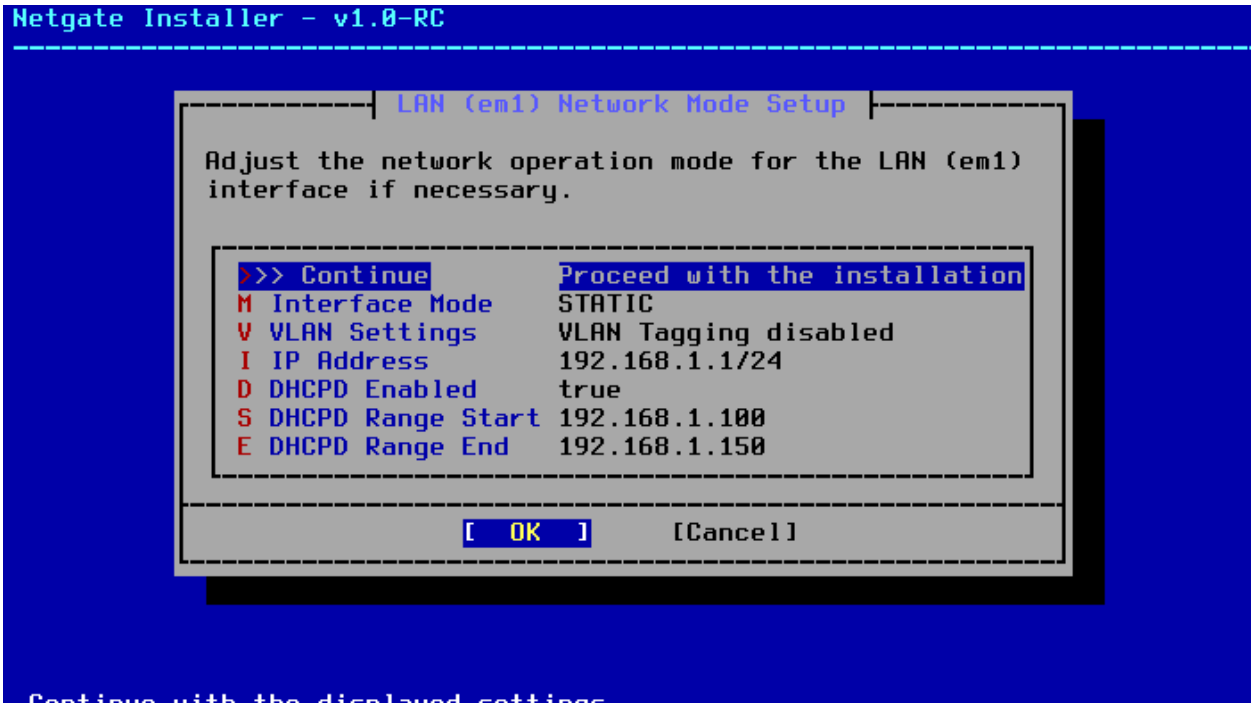


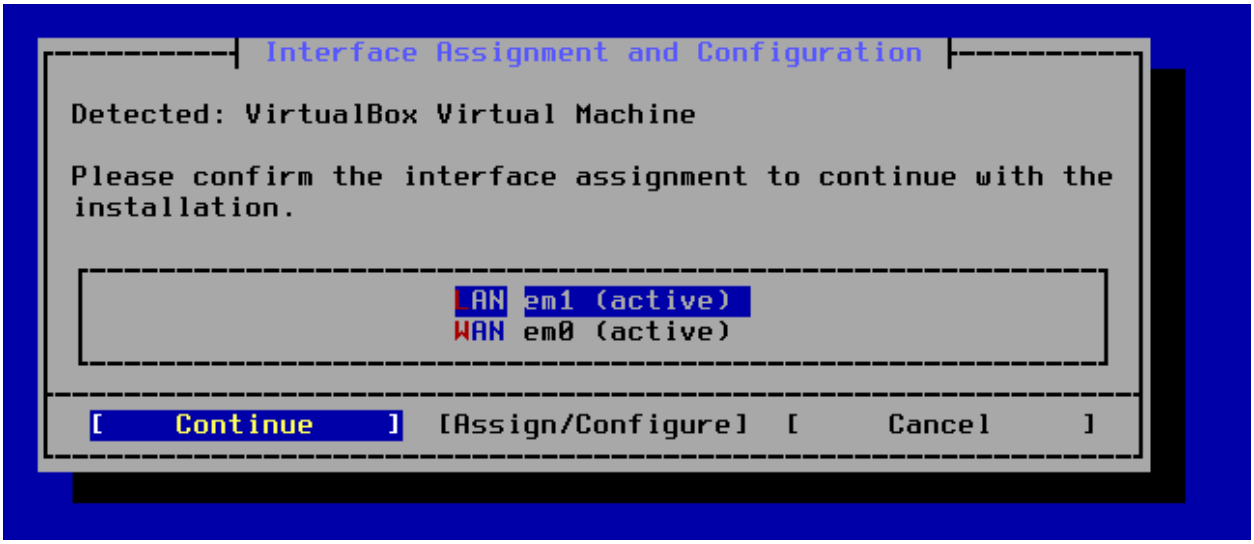

Welcome
Welcome to pfSense!
Install Install pfSense
Rescue Shell Launch a shell for rescue operations
[OK] [Advanced Options] [Cancel]

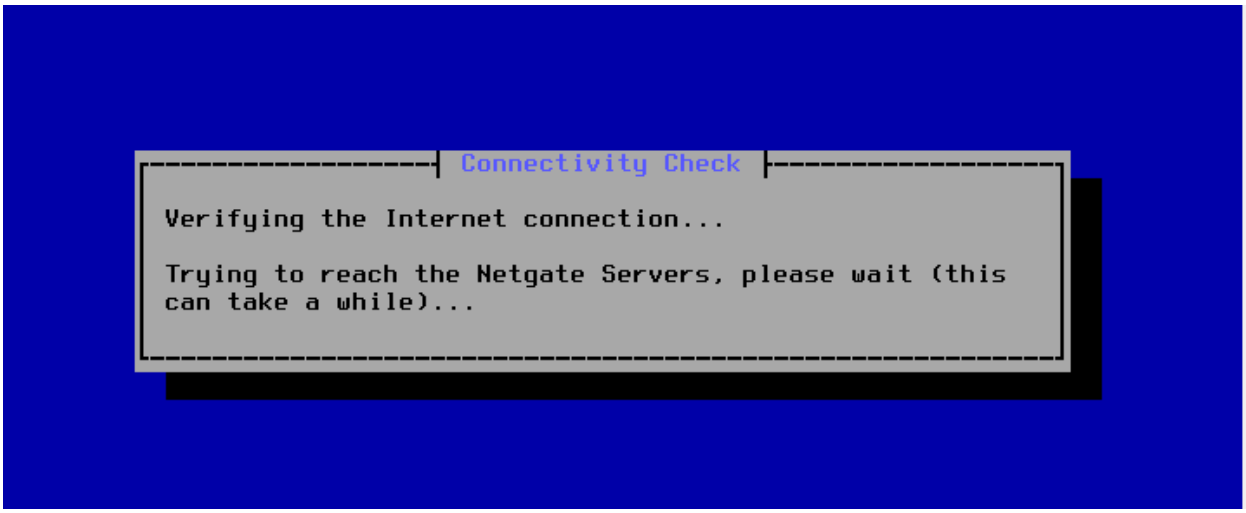

Netgate Installer - v1.0-RC
WAN Interface Assignment and Configuration
Please select the WAN interface.
em0 em0 08:00:27:38:0b:8c (active)
em1 em1 08:00:27:4e:39:58 (active)
[OK] [Cancel]

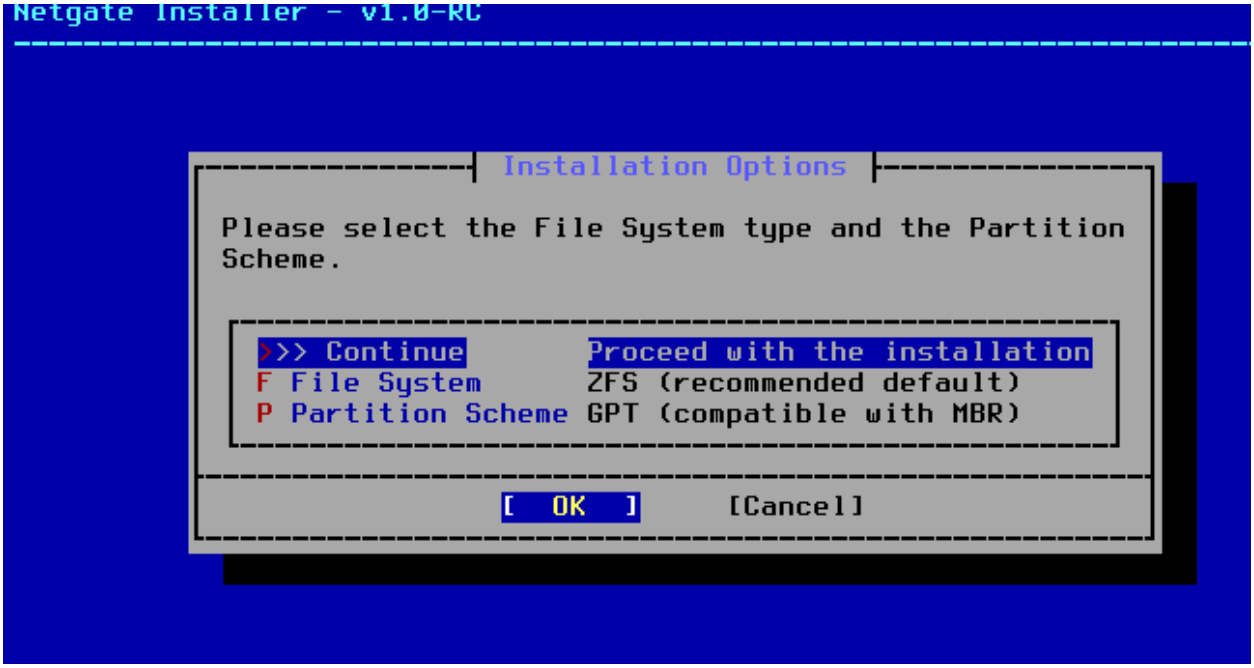

Netgate Installer - v1.0-RC
WAN (em0) Network Mode Setup
Adjust the network operation mode for the WAN (em0) interface if necessary.
>>> Continue Proceed with the installation
M Interface Mode DHCP (client)
V VLAN Settings VLAN Tagging disabled
U Use local resolver false
[OK]
[Cancel]
Continue with the displayed settings


Netgate Installer - v1.0-RC
LAN Interface Assignment and Configuration
Please select the LAN interface.
None Do not assign the LAN interface
em1 em1 08:00:27:4e:39:58 (active)
[OK]
[Skip]
[Cancel]

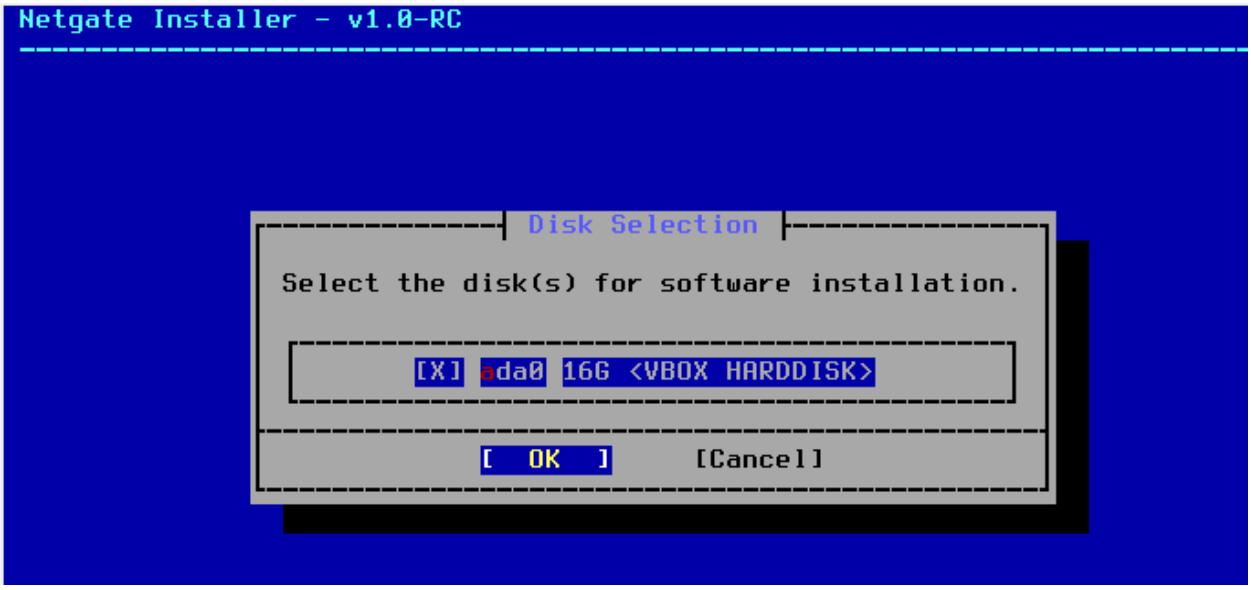

Netgate Installer - v1.0-RC
LAN (em1) Network Mode Setup
Adjust the network operation mode for the LAN (em1) interface if necessary.
>>> Continue Proceed with the installation
M Interface Mode STATIC
V VLAN Settings VLAN Tagging disabled
I IP Address 192.168.1.1/24
D DHCPD Enabled true
S DHCPD Range Start 192.168.1.100
E DHCPD Range End 192.168.1.150
[OK] [Cancel]

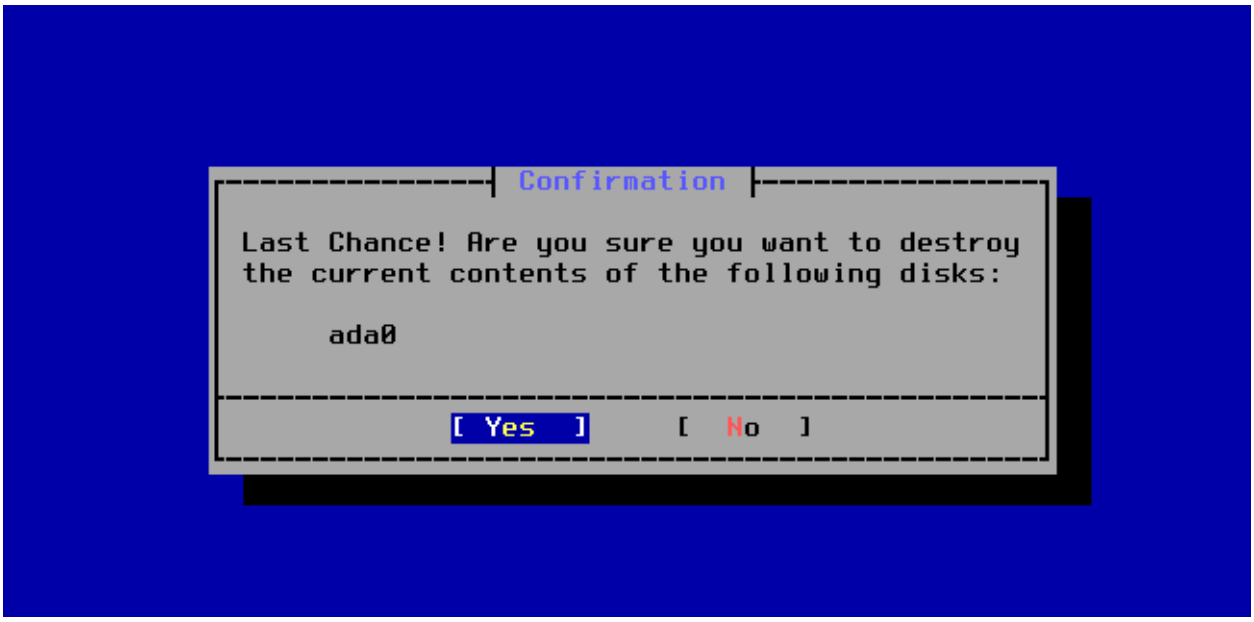

Interface Assignment and Configuration
Detected: VirtualBox Virtual Machine
Please confirm the interface assignment to continue with the installation.
LAN em1 (active)
WAN em0 (active)
[Continue] [Assign/Configure] [Cancel]

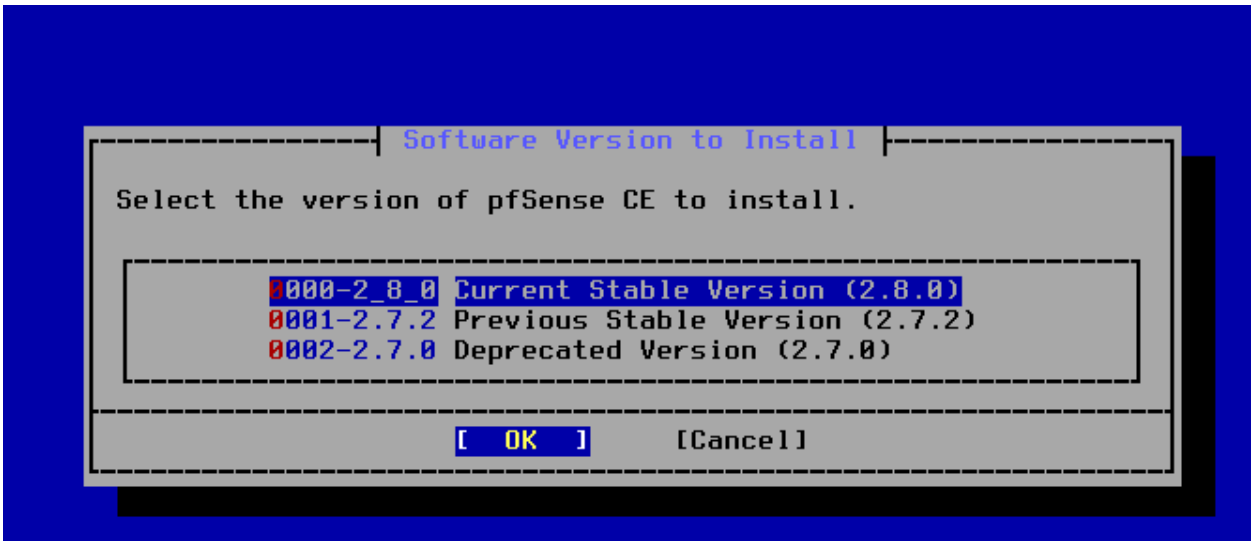

Connectivity Check
Verifying the Internet connection...
Trying to reach the Netgate Servers, please wait (this can take a while)...


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]

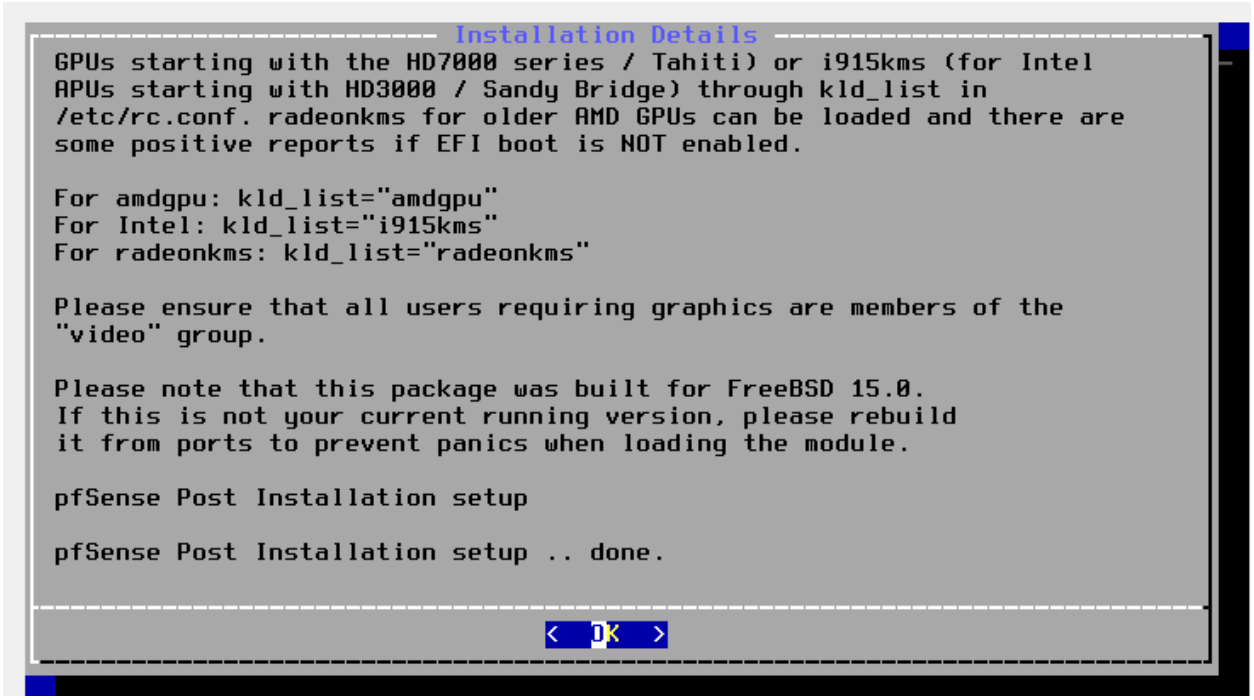

ZFS Virtual Device Type Configuration
Select the ZFS Virtual Device configuration type.
stripe Stripe - No Redundancy
[OK]
[Cancel]

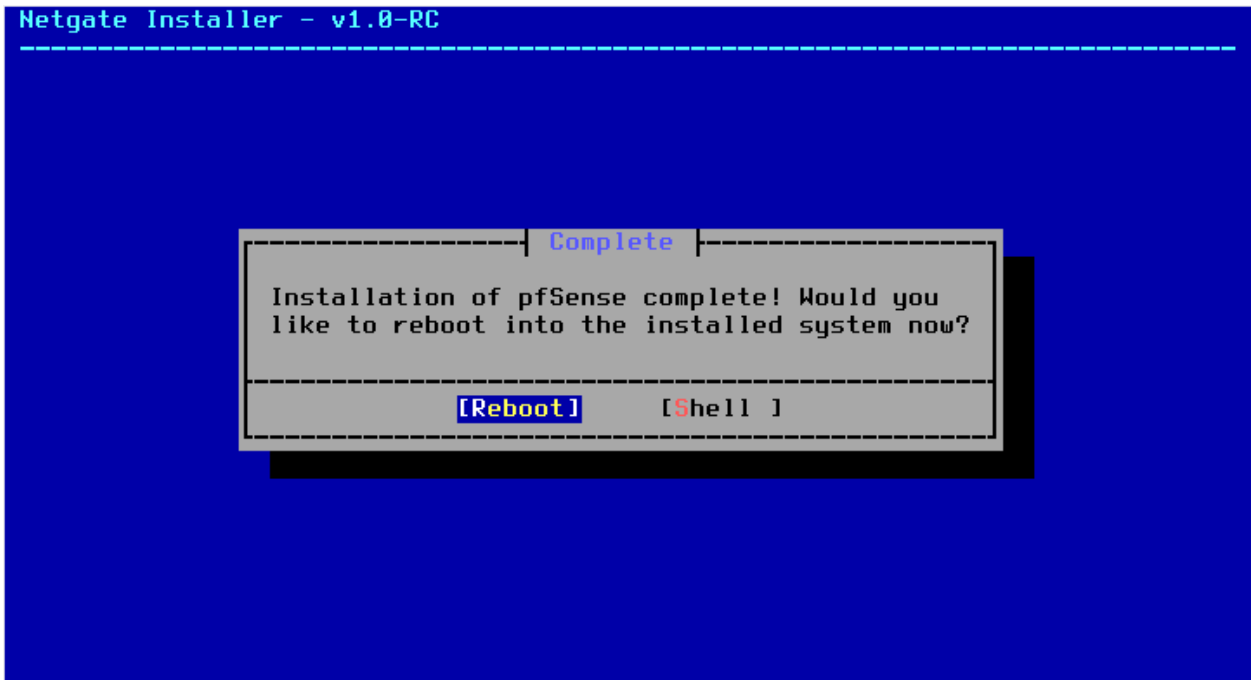

Netgate Installer - v1.0-RC
Disk Selection
Select the disk(s) for software installation.
[X] ada0 16G <VBOX HARDDISK>
[OK]
[Cancel]


Confirmation
Last Chance! Are you sure you want to destroy
the current contents of the following disks:
ada0
[Yes]
[No]


Software Version to Install
Select the version of pfSense CE to install.
0000-2_8_0 Current Stable Version (2.8.0)
0001-2.7.2 Previous Stable Version (2.7.2)
0002-2.7.0 Deprecated Version (2.7.0)
[OK]
[Cancel]

```
------------------------- Installation Details -------------------------

 Installing Current Stable Version (2.8.0)

 Selected configuration file: default (blank) configuration.

 Installing pkg

 Updating pfSense-core repository catalogue...

------------------------------------------------------------------------
```

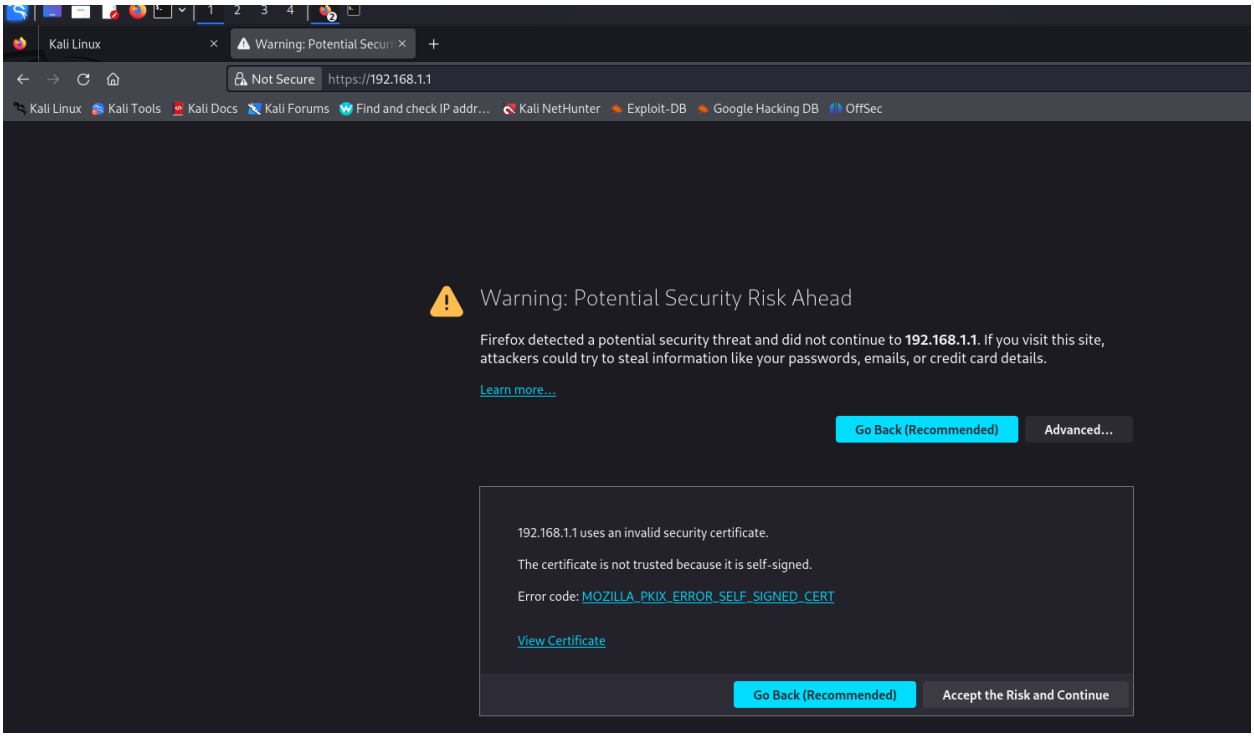

Installation Details
GPUs starting with the HD7000 series / Tahiti) or i915kms (for Intel
APUs starting with HD3000 / Sandy Bridge) through kld_list in
/etc/rc.conf. radeonkms for older AMD GPUs can be loaded and there are
some positive reports if EFI boot is NOT enabled.
For amdgpu: kld_list="amdgpu"
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 >

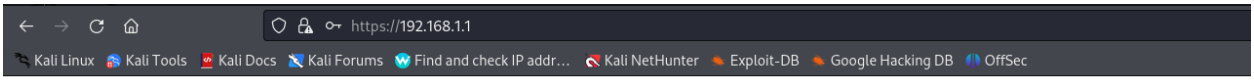

Netgate Installer - v1.0-RC
Complete
Installation of pfSense complete! Would you
like to reboot into the installed system now?
[Reboot]
[Shell]

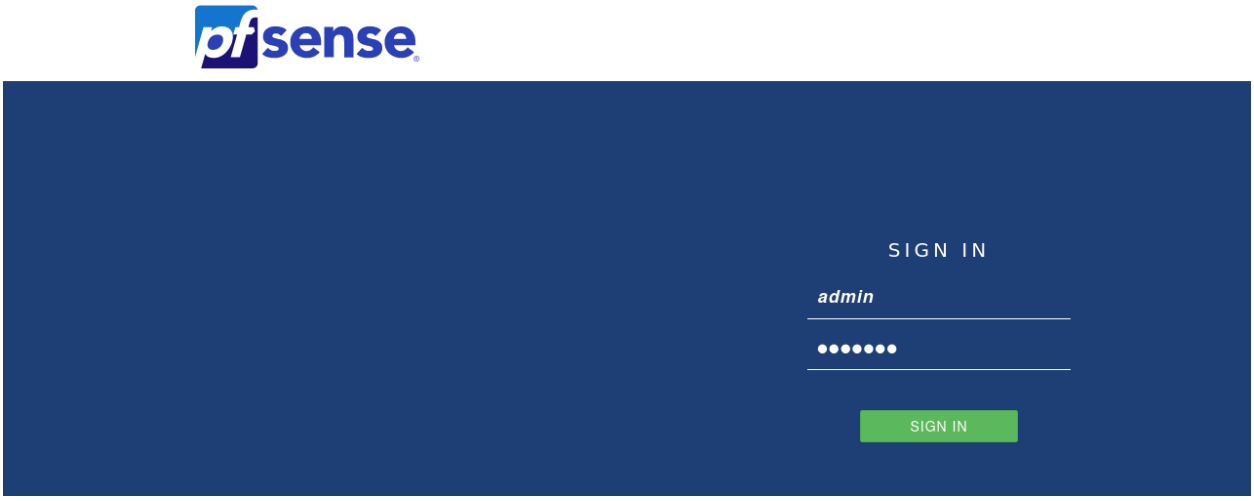
```
Starting CRON... done.
pfSense 2.8.0-RELEASE amd64 20250521-2312
Bootup complete

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


Kali Linux
Warning: Potential Securi
Not Secure
https://192.168.1.1
Kali Linux Kali Tools Kali Docs Kali Forums Find and check IP addr... Kali NetHunter Exploit-DB Google Hacking DB OffSec
Warning: Potential Security Risk Ahead
Firefox detected a potential security threat and did not continue to 192.168.1.1. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.
Learn more...
Go Back (Recommended)
Advanced...
192.168.1.1 uses an invalid security certificate.
The certificate is not trusted because it is self-signed.
Error code: MOZILLA_PKIX_ERROR_SELF_SIGNED_CERT
View Certificate
Go Back (Recommended)
Accept the Risk and Continue


https://192.168.1.1
Kali Linux Kali Tools Kali Docs Kali Forums Find and check IP addr... Kali NetHunter Exploit-DB Google Hacking DB OffSec


pfsense
SIGN IN
admin
SIGN IN

pfsense COMMUNITY EDITION | System | Interfaces | Firewall | Services | VPN | Status | Diagnostics | Help

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 /

pfSense Setup

Welcome to pfSense® software!

This wizard will provide guidance through the initial configuration of pfSense.

The wizard may be stopped at any time by clicking the logo image at the top of the screen.

pfSense® software is developed and maintained by Netgate®

Learn more

Next

Step 2 of 9

General Information

On this screen the general pfSense parameters will be set.

Hostname: pfSense

Name of the firewall host, without domain part.

Examples: pfsense, firewall, edgefw

Domain: home.arpa

Domain name for the firewall.

Examples: home.arpa, example.com

Do not end the domain name with '.local' as the final part (Top Level Domain, TLD). The 'local' TLD is widely used by mDNS (e.g. Avahi, Bonjour, Rendezvous, Airprint, Airplay) and some Windows systems and networked devices. These will not network correctly if the router uses 'local' as its TLD. Alternatives such as 'home.arpa', 'local.lan', or 'mylocal' are safe.

The default behavior of the DNS Resolver will ignore manually configured DNS servers for client queries and query root DNS servers directly. To use the manually configured DNS servers below for client queries, visit Services > DNS Resolver and enable DNS Query Forwarding after completing the wizard.

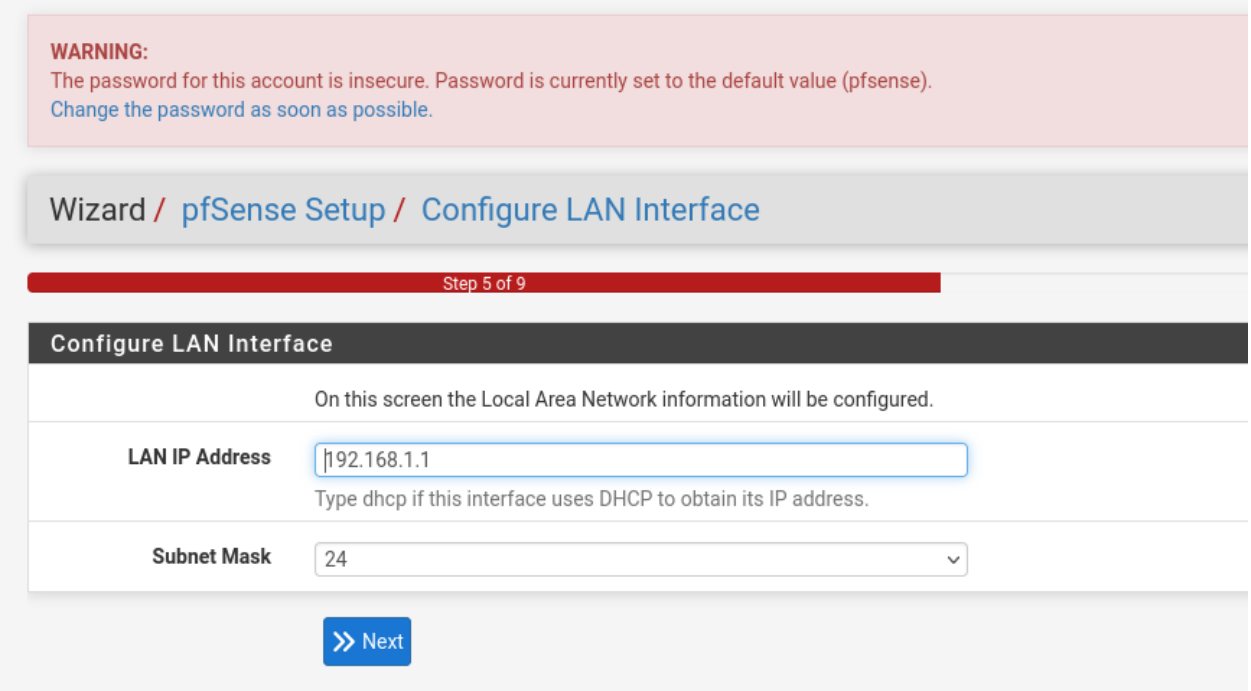
Primary DNS Server:

Secondary DNS Server:

Override DNS: ☑

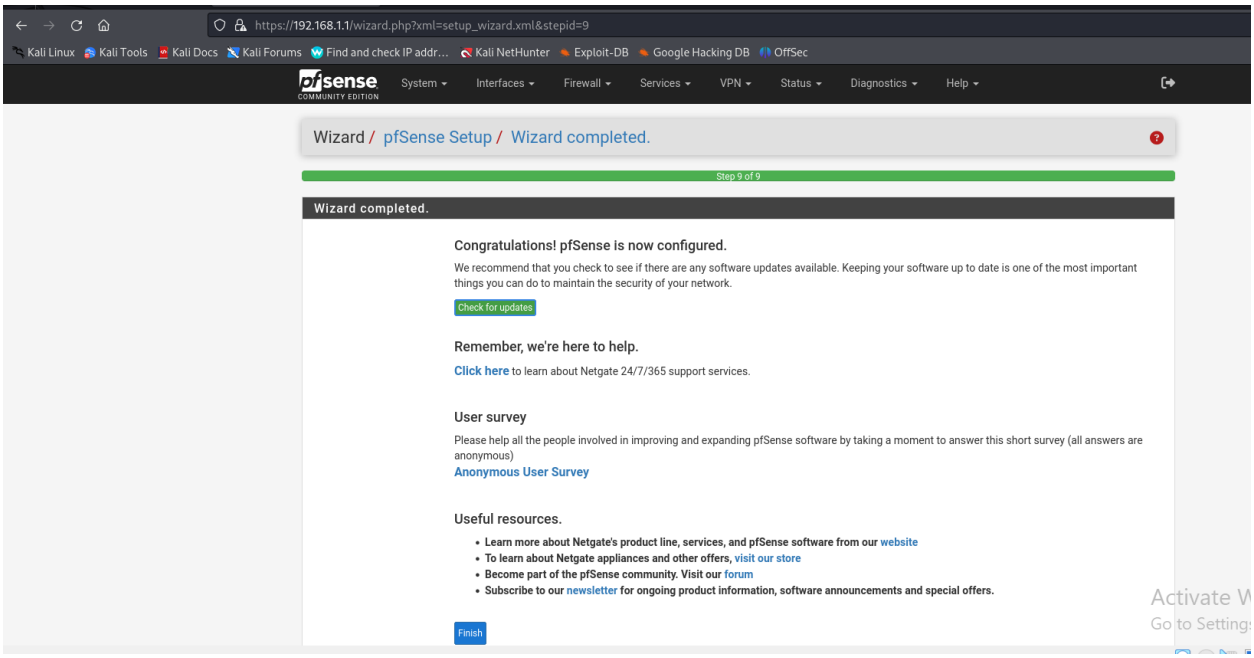
Allow DNS servers to be overridden by DHCP/PPP on WAN

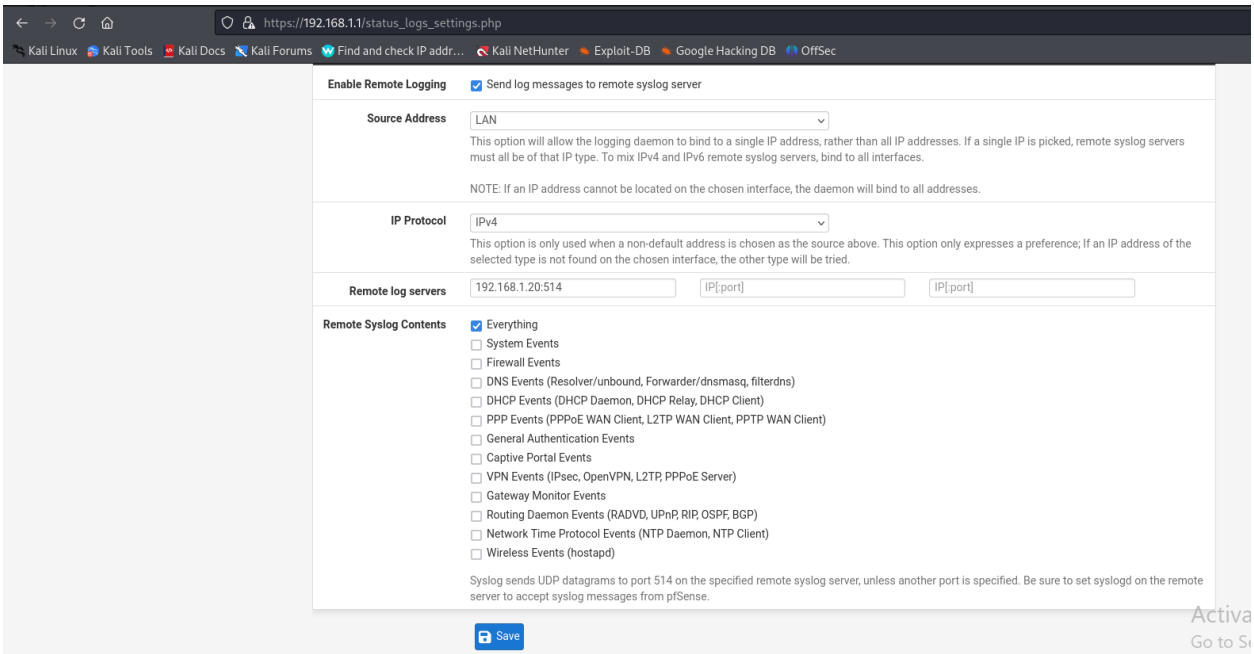
Next



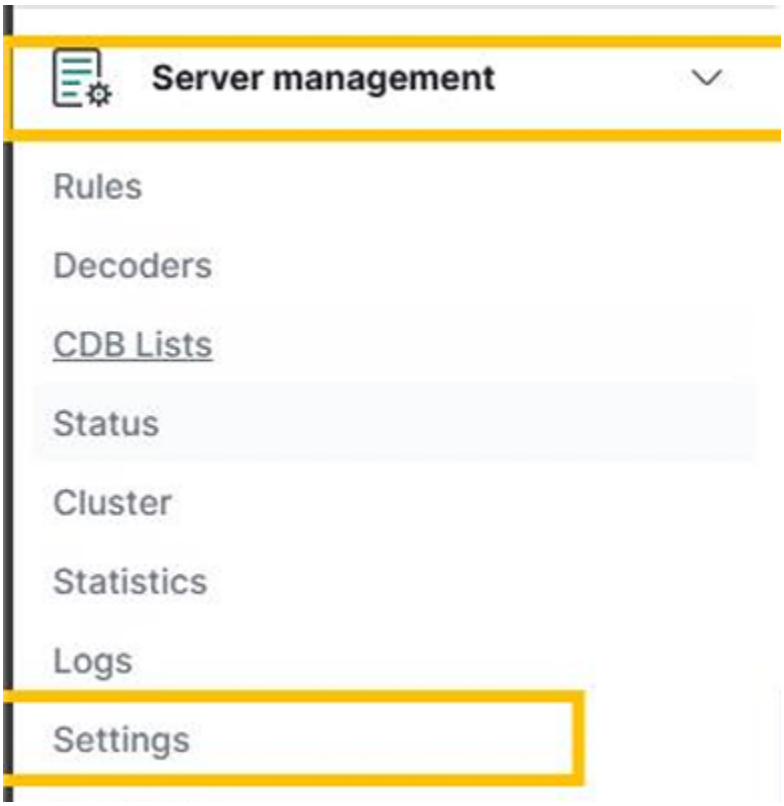
Step-by-Step Integration

Step 1: Enable Remote Logging in pfSense





Step 2: Custom Syslog Configuration (for UI Logs)

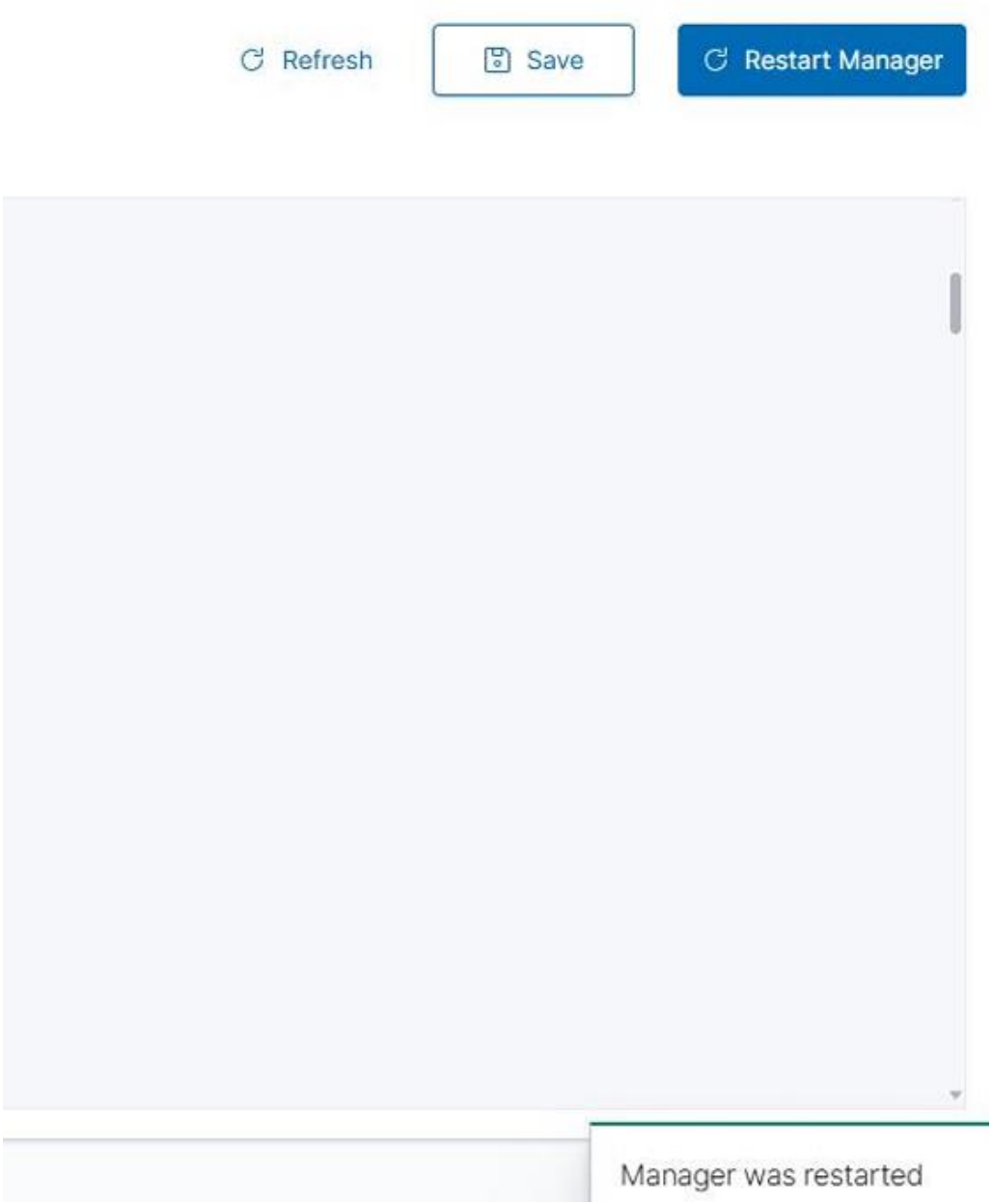


Edit /var/ossec/etc/ossec.conf on the Wazuh Manager.

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.

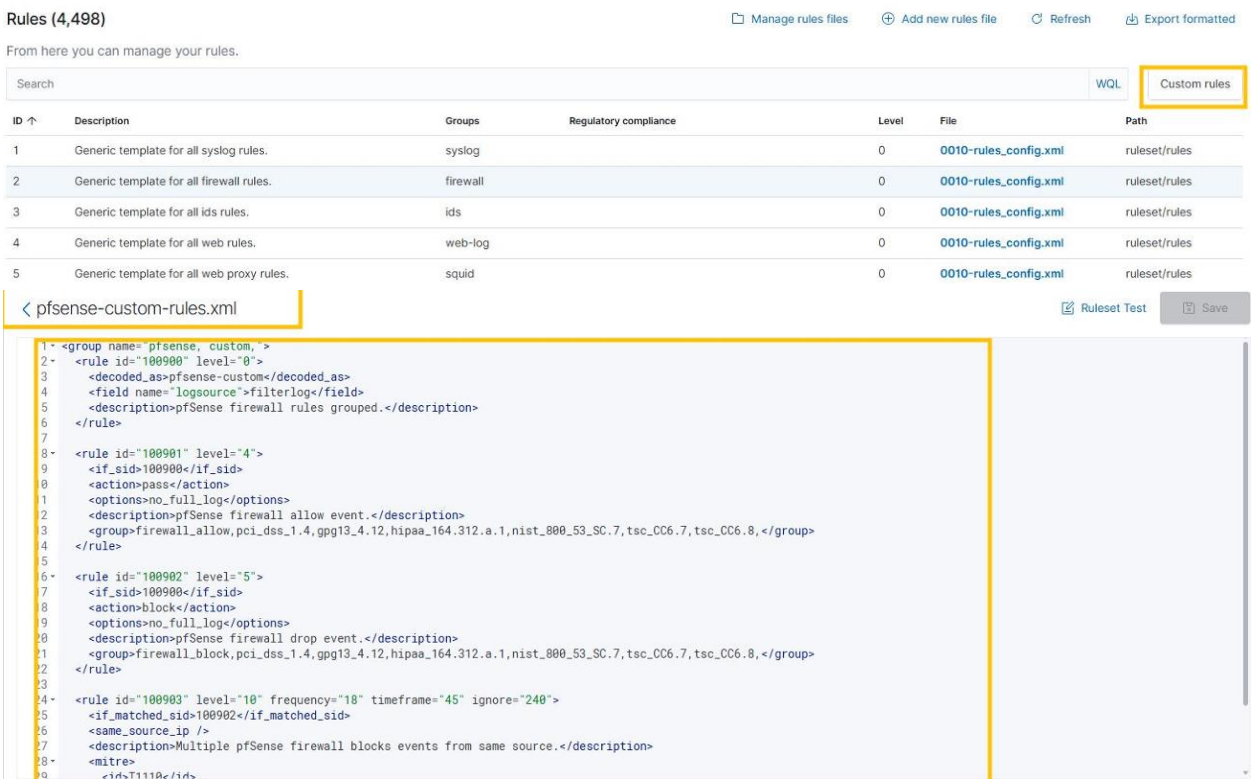


Step 3: Add Custom Decoders & Rules (for UI Event Parsing)

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*),(\S*),(\d*),(\d*),\S*</regex>

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

</decoder>
```

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



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 denies, 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

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 Instaled 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.

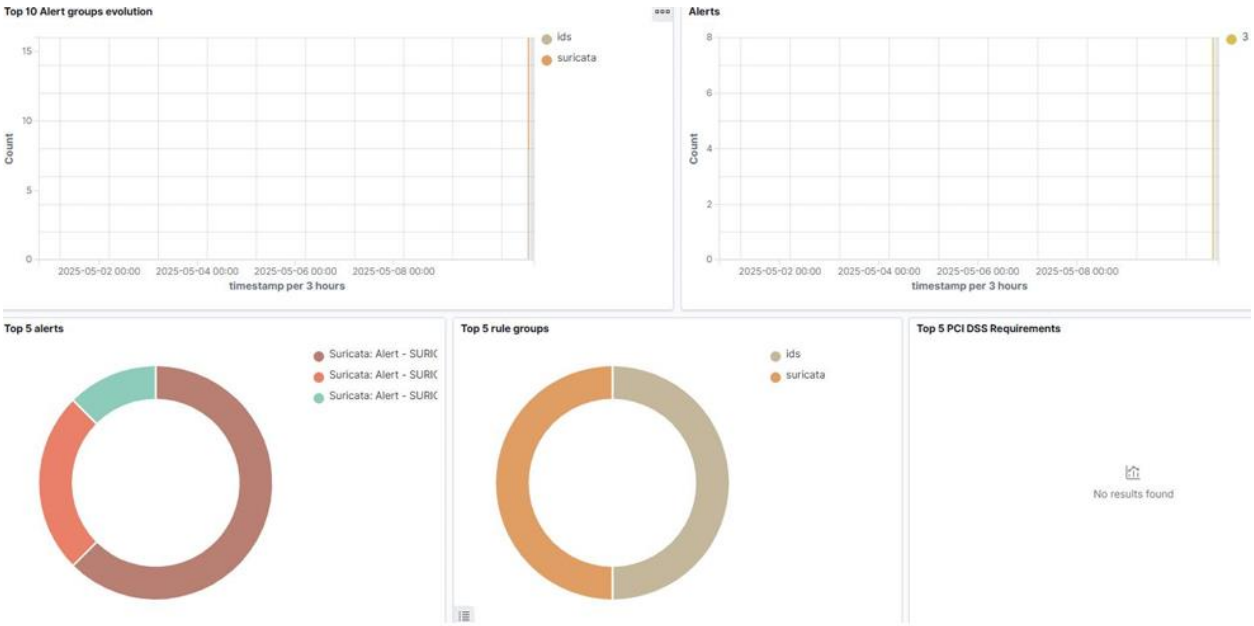
Step 6: Trigger and Detect an Intrusion:

```
└$ 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



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