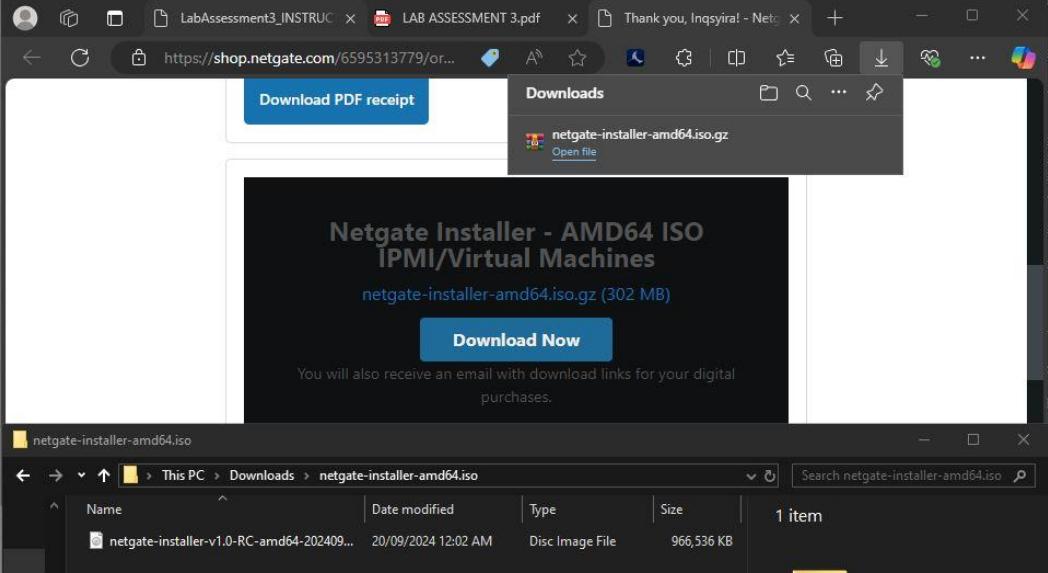


## SNORT AND FIREWALL PROVISIONING

host address for LAN in the virtual box: **192.168.6.0**

TOOL DETAILS	RESULTS
pfSense Installation (successful/Fail)	

Network  
Requirement  
Setup

```
Fadhilah_Inqsyira [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Configure IPv6 address LAN interface via DHCP6? (y/n) n
Enter the new LAN IPv6 address. Press <ENTER> for none:
>

Do you want to enable the DHCP server on LAN? (y/n) y
Enter the start address of the IPv4 client address range: 192.168.6.20
Enter the end address of the IPv4 client address range: 192.168.6.250
Disabling IPv6 DHCPD...

Please wait while the changes are saved to LAN...
Reloading filter...
Reloading routing configuration...
DHCPD...

The IPv4 LAN address has been set to 192.168.6.1/24
You can now access the webConfigurator by opening the following URL in your web
browser:
http://192.168.6.1/
Press <ENTER> to continue. █
```

```
Fadhilah_Inqsyira [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Available interfaces:
1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em1 - static)

Enter the number of the interface you wish to configure: 2
Configure IPv4 address LAN interface via DHCP? (y/n) n
Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.6.1

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0 = 16
     255.0.0.0 = 8

Enter the new LAN IPv4 subnet bit count (1 to 32):
> 24

For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Configure IPv6 address LAN interface via DHCP6? (y/n) n
```

```
Fadhilah_Inqsyira [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
The IPv4 LAN address has been set to 192.168.6.1/24
You can now access the webConfigurator by opening the following URL in your web
browser:
http://192.168.6.1/
Press <ENTER> to continue.
KVM Guest - Netgate Device ID: 0bf49de7e9f2dfd6bb24

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

WAN (wan)      -> em0          -> v4/DHCP4: 10.0.2.15/24
LAN (lan)      -> em1          -> v4: 192.168.6.1/24

 8) 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) Enable Secure Shell (sshd)
 6) Halt system                 15) Restore recent configuration
 7) Ping host                   16) Restart PHP-FPM

Enter an option: █
```

Kali Linux Reboot (Successful/Fail)

```

ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    ether 08:00:27:16:b5:64 txqueuelen 1000 (Ethernet)
      RX packets 10 bytes 1138 (1.1 KiB)
      RX errors 0 dropped 0 overruns 0 frame 0
      TX packets 0 bytes 0 (0.0 B)
      TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.6.22 netmask 255.255.255.0 broadcast 192.168.6.25
      inet6 fe80::a00:27ff:fe02:6a57 prefixlen 64 scopid 0x20<link>
        ether 08:00:27:92:6a:57 txqueuelen 1000 (Ethernet)
          RX packets 5 bytes 866 (866.0 B)
          RX errors 0 dropped 0 overruns 0 frame 0
          TX packets 26 bytes 3540 (3.4 KiB)
          TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
      inet6 ::1 prefixlen 128 scopid 0x10<host>
        loop txqueuelen 1000 (Local Loopback)
          RX packets 206 bytes 12300 (12.0 KiB)
          RX errors 0 dropped 0 overruns 0 frame 0
          TX packets 206 bytes 12300 (12.0 KiB)

FreeBSD/and64 (pfSense.home.arpa) (tty0)
KVM Guest - Netgate Device ID: 0bf49de7e9f2fd6bb24
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***
HAN (wan)      -> em0      -> v4/DHCP4: 10.0.2.15/24
LHN (lan)      -> en1      -> v4: 192.168.6.1/24
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) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

```

Accessing pfSense GUI

The screenshot shows the pfSense Community Edition web interface. The main navigation bar includes links for Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, and OffSec.

The current page is "Interfaces / LAN (em1)". A warning message at the top states: "WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager."

The "General Configuration" section contains the following fields:

- Enable:** checked
- Description:** LAN
- IPv4 Configuration Type:** Static IPv4
- IPv6 Configuration Type:** None
- MAC Address:** XX:XXXX:XX:XX:XX:XX
- MTU:** (dropdown menu)
- MSS:** (dropdown menu)
- Speed and Duplex:** Default (no preference, typically autoselect)

The "Static IPv4 Configuration" section contains:

- IPv4 Address:** 192.168.6.1
- IPv4 Upstream gateway:** None
- Add a new gateway:** button

Below these sections, there is a note: "If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button. On local area network interfaces the upstream gateway should be "none". Selecting an upstream gateway causes the firewall to treat this interface as a WAN type interface. Gateways can be managed by clicking here."

The "Reserved Networks" section has a checkbox: "Block private networks".

## Interface Added into pfSense

The screenshot shows the pfSense web interface with the URL `192.168.6.1/snort/snort_interfaces.php`. The title bar says "Kali Linux VM [Running] - Oracle VM VirtualBox". The main content area is titled "Services / Snort / Interfaces". A table titled "Interface Settings Overview" lists one interface:

Interface	Snort Status	Pattern Match	Blocking Mode	Description	Actions
LAN (em1)	<span style="color:red">X</span> <span style="color:green">P</span>	AC-BNFA	DISABLED	LAN	<span style="color:blue">Edit</span> <span style="color:orange">Delete</span>

At the bottom of the page, there is a note: "pfSense is developed and maintained by Netgate. © ESF 2004 - 2025 View license."

## IDS Rules Applied (Successful/Fail)

The screenshot shows the pfSense web interface with the URL `192.168.6.1/snort/snort_rules.php`. The title bar says "Kali Linux VM [Running] - Oracle VM VirtualBox". The main content area is titled "Services / Snort / Interface Settings / LAN - Rules". A message box says "Custom rules validated successfully and any active Snort process on this interface has been signaled to live-load the new rules." Below it, a table shows the rule categories:

Category Selection:	custom.rules
Select the rule category to view and manage.	

The "Defined Custom Rules" section contains the following rule:

```
alert icmp $HOME_NET any -> $EXTERNAL_NET any (msg:"ping found!";sid:10000010;)
```

Host Triggered  
in Kali Linux -  
Ping 8.8.8.8  
(Successful/Fail)

```
File Actions Edit View Help
(inqsyirazamri@inq) ~
$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=58 time=252 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=58 time=56.3 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=58 time=15.6 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=58 time=69.0 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=58 time=209 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=58 time=13.9 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=58 time=19.8 ms
64 bytes from 8.8.8.8: icmp_seq=8 ttl=58 time=18.5 ms
64 bytes from 8.8.8.8: icmp_seq=9 ttl=58 time=17.0 ms
64 bytes from 8.8.8.8: icmp_seq=10 ttl=58 time=475 ms
64 bytes from 8.8.8.8: icmp_seq=11 ttl=58 time=304 ms
64 bytes from 8.8.8.8: icmp_seq=12 ttl=58 time=82.5 ms
64 bytes from 8.8.8.8: icmp_seq=13 ttl=58 time=108 ms
64 bytes from 8.8.8.8: icmp_seq=14 ttl=58 time=407 ms
64 bytes from 8.8.8.8: icmp_seq=15 ttl=58 time=893 ms
64 bytes from 8.8.8.8: icmp_seq=16 ttl=58 time=191 ms
64 bytes from 8.8.8.8: icmp_seq=17 ttl=58 time=219 ms
64 bytes from 8.8.8.8: icmp_seq=18 ttl=58 time=142 ms
64 bytes from 8.8.8.8: icmp_seq=19 ttl=58 time=257 ms
64 bytes from 8.8.8.8: icmp_seq=20 ttl=58 time=54.7 ms
64 bytes from 8.8.8.8: icmp_seq=21 ttl=58 time=12.4 ms
64 bytes from 8.8.8.8: icmp_seq=22 ttl=58 time=67.3 ms
64 bytes from 8.8.8.8: icmp_seq=23 ttl=58 time=24.9 ms
64 bytes from 8.8.8.8: icmp_seq=24 ttl=58 time=19.9 ms
64 bytes from 8.8.8.8: icmp_seq=25 ttl=58 time=23.4 ms
64 bytes from 8.8.8.8: icmp_seq=26 ttl=58 time=13.7 ms
^C
--- 8.8.8.8 ping statistics ---
26 packets transmitted, 26 received, 0% packet loss, time 25020ms
rtt min/avg/max/mdev = 12.396/152.523/892.714/195.206 ms

(inqsyirazamri@inq) ~
$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
^C
--- 8.8.8.8 ping statistics ---
83 packets transmitted, 0 received, 100% packet loss, time 83925ms

(inqsyirazamri@inq) ~
$
```

Alerts Showing  
in the Snort  
(Showing/Not  
Showing)

Services / Snort / Alerts

Snort Interfaces Global Settings Updates Alerts Blocked Pass Lists Suppress IP Lists SID Mgmt Log Mgmt Sync

Alert Log View Settings

Interface to Inspect: LAN (em1) Auto-refresh: 250 Save

Alert Log Actions: Download Clear

Alert Log View Filter

83 Entries in Active Log

Date	Action	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	GID:SID	Description
2025-01-03 21:34:25	⚠️	0	ICMP		192.168.6.22	Q ↗	8.8.8.8	Q ↗	1:10000010	ping found!
2025-01-03 21:34:24	⚠️	0	ICMP		192.168.6.22	Q ↗	8.8.8.8	Q ↗	1:10000010	ping found!
2025-01-03 21:34:23	⚠️	0	ICMP		192.168.6.22	Q ↗	8.8.8.8	Q ↗	1:10000010	ping found!
2025-01-03 21:34:22	⚠️	0	ICMP		192.168.6.22	Q ↗	8.8.8.8	Q ↗	1:10000010	ping found!
2025-01-03 21:34:21	⚠️	0	ICMP		192.168.6.22	Q ↗	8.8.8.8	Q ↗	1:10000010	ping found!
2025-01-03 21:34:20	⚠️	0	ICMP		192.168.6.22	Q ↗	8.8.8.8	Q ↗	1:10000010	ping found!
2025-01-03 21:34:19	⚠️	0	ICMP		192.168.6.22	Q ↗	8.8.8.8	Q ↗	1:10000010	ping found!
2025-01-03 21:34:18	⚠️	0	ICMP		192.168.6.22	Q ↗	8.8.8.8	Q ↗	1:10000010	ping found!

## Alerts showing for IPS Blocked Host in Snort (Showing/Not Showing)

The screenshot shows the pfSense web interface with the URL `192.168.6.1/snort/snort_alerts.php`. The page title is "Services / Snort / Alerts". The "Alerts" tab is selected. A warning message at the top states: "WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager." Below this, there is an "Alert Log View Settings" section with a dropdown for "Interface to Inspect" set to "LAN (em1)". There are buttons for "Save" and "Clear". An "Alert Log Actions" section includes "Download" and "Clear" buttons. The main area displays a table titled "106 Entries in Active Log" with the following columns: Date, Action, Pri, Proto, Class, Source IP, SPort, Destination IP, DPort, GID:SID, and Description. The table lists 106 entries, all of which are ICMP ping requests from 192.168.6.22 to 8.8.8.8, with descriptions like "ping found!" and GID:SID values ranging from 1:10000010 to 1:10000010.

## IPS Blocked Host showing in the Blocked Section in Snort (Showing/Not Showing)

The screenshot shows the pfSense web interface with the URL `192.168.6.1/snort/snort_blocked.php`. The page title is "Services / Snort / Blocked Hosts". The "Blocked" tab is selected. A warning message at the top states: "WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager." Below this, there is a "Blocked Hosts and Log View Settings" section with tabs for "Blocked Hosts" and "Log View". It includes buttons for "Download" and "Clear", and checkboxes for "Save" and "Refresh". A setting for "Number of blocked entries to view. Default is 500" is shown. The main area displays a table titled "Last 500 Hosts Blocked by Snort (only applicable to Legacy Blocking Mode interfaces)" with columns: #, IP, Alert Descriptions and Event Times, and Remove. One entry is listed: "# 1 IP 8.8.8.8 Alert Descriptions and Event Times ping found! - 2025-01-03 21:45:10 Remove". A note at the bottom states: "1 host IP address is currently being blocked Snort on Legacy Blocking Mode interfaces." At the bottom of the page, a footer notes: "pfSense is developed and maintained by Netgate. © ESF 2004 - 2025 View license."