

# 12th Project

Lecturer: Dr. Ayman Adel Abdelhamid

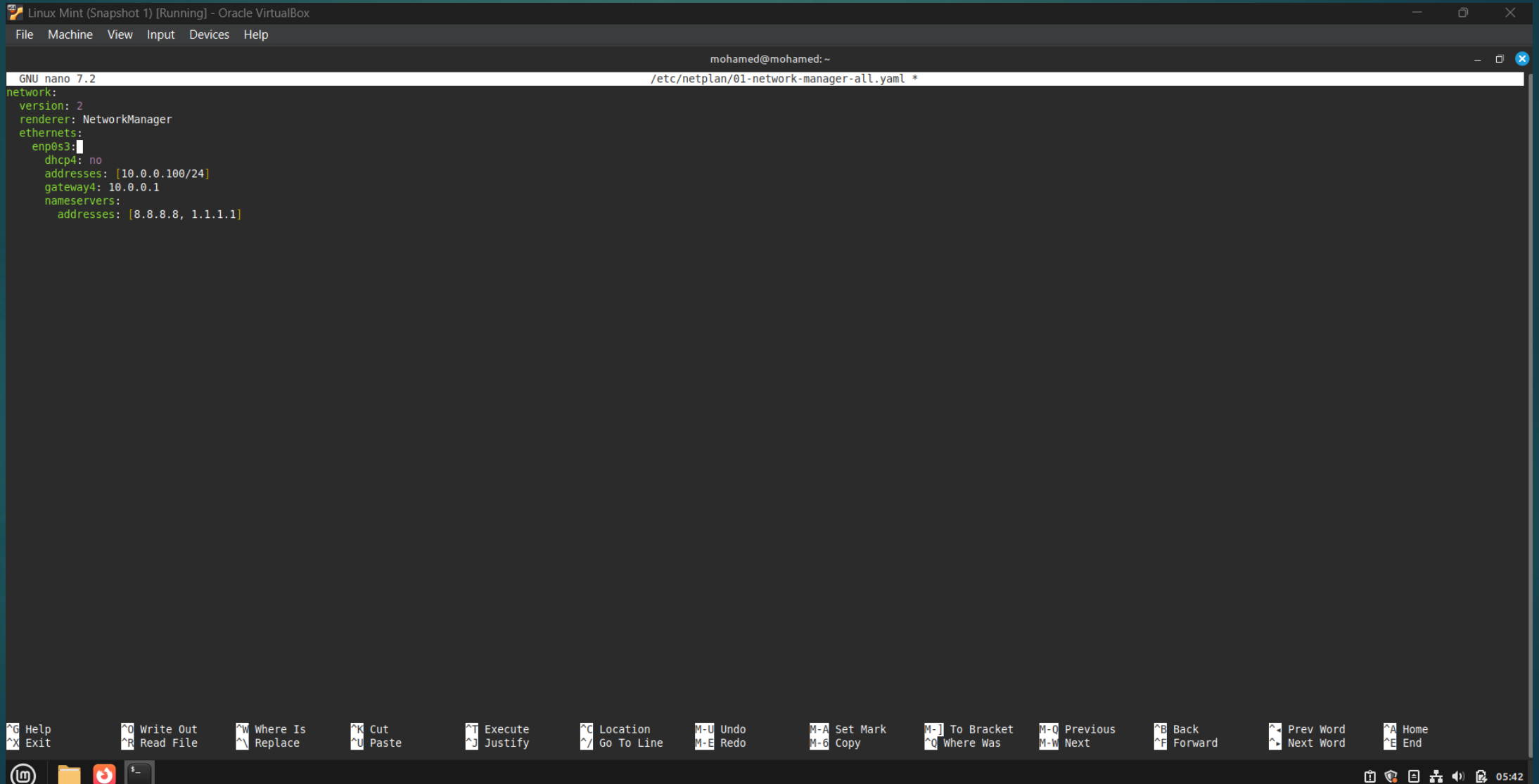
T.A: Abdelrhman Solyman

NAME:

MOHAMED ELSAYED MOHAMED 221010750

OMAR SHERIF HOSNY 221010339

# Configure the Network IP in Linux Min to 10.0.0.100



The screenshot shows a terminal window titled "Linux Mint (Snapshot 1) [Running] - Oracle VirtualBox". The terminal is running the GNU nano 7.2 text editor, editing the file `/etc/netplan/01-network-manager-all.yaml`. The user is logged in as `mohamed@mohamed:~`. The configuration file content is as follows:

```
network:
  version: 2
  renderer: NetworkManager
  ethernets:
    enp0s3:
      dhcp4: no
      addresses: [10.0.0.100/24]
      gateway4: 10.0.0.1
      nameservers:
        addresses: [8.8.8.8, 1.1.1.1]
```

The terminal window includes a menu bar with "File", "Machine", "View", "Input", "Devices", and "Help". At the bottom, there is a status bar with various keyboard shortcuts for nano, such as `^G Help`, `^O Write Out`, `^W Where Is`, `^K Cut`, `^T Execute`, `^C Location`, `M-U Undo`, `M-A Set Mark`, `M-J To Bracket`, `M-O Previous`, `^B Back`, `^P Prev Word`, `^A Home`, `^X Exit`, `^R Read File`, `^N Replace`, `^V Paste`, `^J Justify`, `^_ Go To Line`, `M-E Redo`, `M-C Copy`, `^O Where Was`, `M-W Next`, `^F Forward`, `^N Next Word`, and `^E End`. The system clock in the bottom right corner shows 05:42.

mohamed@mohamed: ~

```
mohamed@mohamed:~$ sudo nano /etc/netplan/01-network-manager-all.yaml
```

```
mohamed@mohamed:~$ sudo netplan apply
```

```
** (generate:9547): WARNING **: 05:42:21.692: Permissions for /etc/netplan/01-network-manager-all.yaml are too open. Netplan configuration should NOT be accessible by others.
```

```
** (generate:9547): WARNING **: 05:42:21.692: `gateway4` has been deprecated, use default routes instead.
```

```
See the 'Default routes' section of the documentation for more details.
```

```
** (process:9545): WARNING **: 05:42:22.126: Permissions for /etc/netplan/01-network-manager-all.yaml are too open. Netplan configuration should NOT be accessible by others.
```

```
** (process:9545): WARNING **: 05:42:22.127: `gateway4` has been deprecated, use default routes instead.
```

```
See the 'Default routes' section of the documentation for more details.
```

```
** (process:9545): WARNING **: 05:42:22.260: Permissions for /etc/netplan/01-network-manager-all.yaml are too open. Netplan configuration should NOT be accessible by others.
```

```
** (process:9545): WARNING **: 05:42:22.260: `gateway4` has been deprecated, use default routes instead.
```

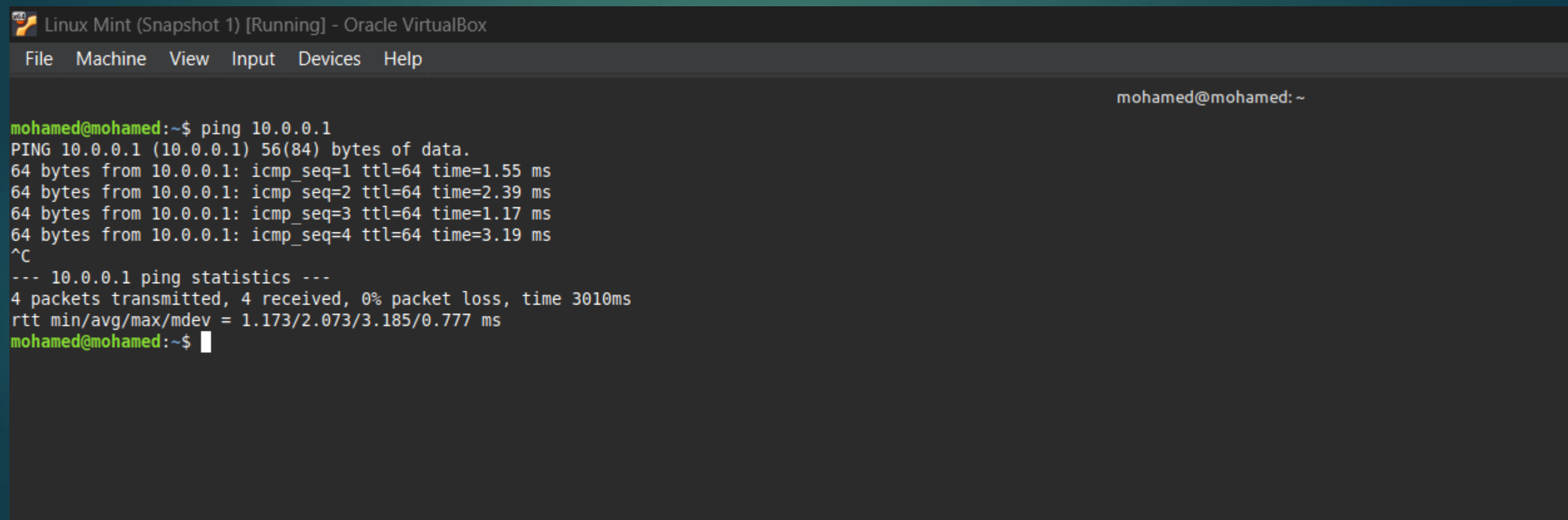
```
See the 'Default routes' section of the documentation for more details.
```

```
mohamed@mohamed:~$ ifconfig
```

```
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.0.100 netmask 255.255.255.0 broadcast 10.0.0.255
    inet6 fe80::a00:27ff:fe83:46c7 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:83:46:c7 txqueuelen 1000 (Ethernet)
    RX packets 203 bytes 42958 (42.9 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 363 bytes 57855 (57.8 KB)
    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 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 203 bytes 16327 (16.3 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 203 bytes 16327 (16.3 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Now Linux Mint in the same subnet as Pfsense and can see each other

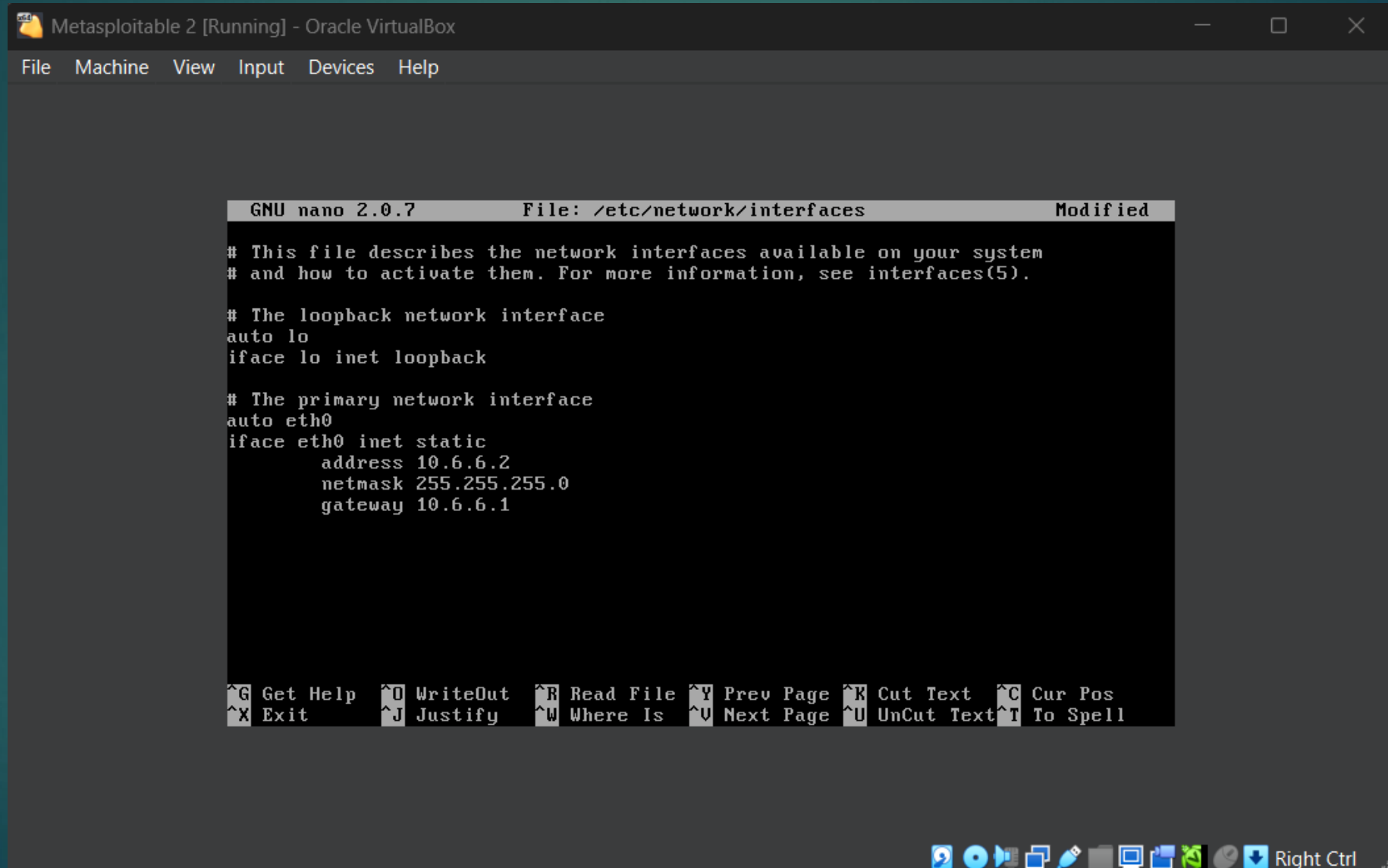


```
Linux Mint (Snapshot 1) [Running] - Oracle VirtualBox
File Machine View Input Devices Help

mohamed@mohamed: ~

mohamed@mohamed:~$ ping 10.0.0.1
PING 10.0.0.1 (10.0.0.1) 56(84) bytes of data.
64 bytes from 10.0.0.1: icmp_seq=1 ttl=64 time=1.55 ms
64 bytes from 10.0.0.1: icmp_seq=2 ttl=64 time=2.39 ms
64 bytes from 10.0.0.1: icmp_seq=3 ttl=64 time=1.17 ms
64 bytes from 10.0.0.1: icmp_seq=4 ttl=64 time=3.19 ms
^C
--- 10.0.0.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3010ms
rtt min/avg/max/mdev = 1.173/2.073/3.185/0.777 ms
mohamed@mohamed:~$
```

## Configure the Network IP in Metasploitable2 to 10.6.6.2



```
Metasploitable 2 [Running] - Oracle VirtualBox
File Machine View Input Devices Help

GNU nano 2.0.7      File: /etc/network/interfaces      Modified

# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet static
    address 10.6.6.2
    netmask 255.255.255.0
    gateway 10.6.6.1

^G Get Help  ^O WriteOut  ^R Read File  ^Y Prev Page  ^K Cut Text   ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is   ^V Next Page  ^U UnCut Text ^T To Spell
```

```
msfadmin@metasploitable:~$ sudo /etc/init.d/networking restart
* Reconfiguring network interfaces... [ OK ]
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:83:d3:a1
          inet addr:10.6.6.2  Bcast:10.6.6.255  Mask:255.255.255.0
          inet6 addr: fdd4:6ba6:9191:fc00:a00:27ff:fe83:d3a1/64 Scope:Global
          inet6 addr: fe80::a00:27ff:fe83:d3a1/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:76 errors:0 dropped:0 overruns:0 frame:0
          TX packets:89 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:8125 (7.9 KB)  TX bytes:9202 (8.9 KB)
          Base address:0xd020  Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:129 errors:0 dropped:0 overruns:0 frame:0
          TX packets:129 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:37881 (36.9 KB)  TX bytes:37881 (36.9 KB)

msfadmin@metasploitable:~$
```

# Allow Traffic to Interface OPT1 to send and receive

pfSense.home.arpa - Firewall: Rules: OPT1 — Mozilla Firefox

10.0.0.1/firewall\_rules.php?if=opt1

pfSense COMMUNITY EDITION

System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

WARNING: The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

Firewall / Rules / OPT1

The changes have been applied successfully. The firewall rules are now reloading in the background. [Monitor the filter reload progress.](#)

Floating WAN LAN **OPT1** OPT2

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
No rules are currently defined for this interface All incoming connections on this interface will be blocked until pass rules are added. Click the button to add a new rule.											

Add Add Delete Toggle Copy Save Separator

pfSense is developed and maintained by Netgate. © ESF 2004 - 2025 [View license.](#)

06:39



System ▾

Interfaces ▾

Firewall ▾

Services ▾

VPN ▾

Status ▾

Diagnostics ▾

Help ▾



**WARNING:** The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

Firewall / Rules / Edit



## Edit Firewall Rule

**Action**

Pass ▾

Choose what to do with packets that match the criteria specified below.  
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

**Disabled**☐ Disable this rule

Set this option to disable this rule without removing it from the list.

**Interface**

OPT1 ▾

Choose the interface from which packets must come to match this rule.

**Address Family**

IPv4 ▾

Select the Internet Protocol version this rule applies to.

**Protocol**

ICMP ▾

Choose which IP protocol this rule should match.

**ICMP Subtypes**

any  
Alternate Host  
Datagram conversion error  
Echo reply

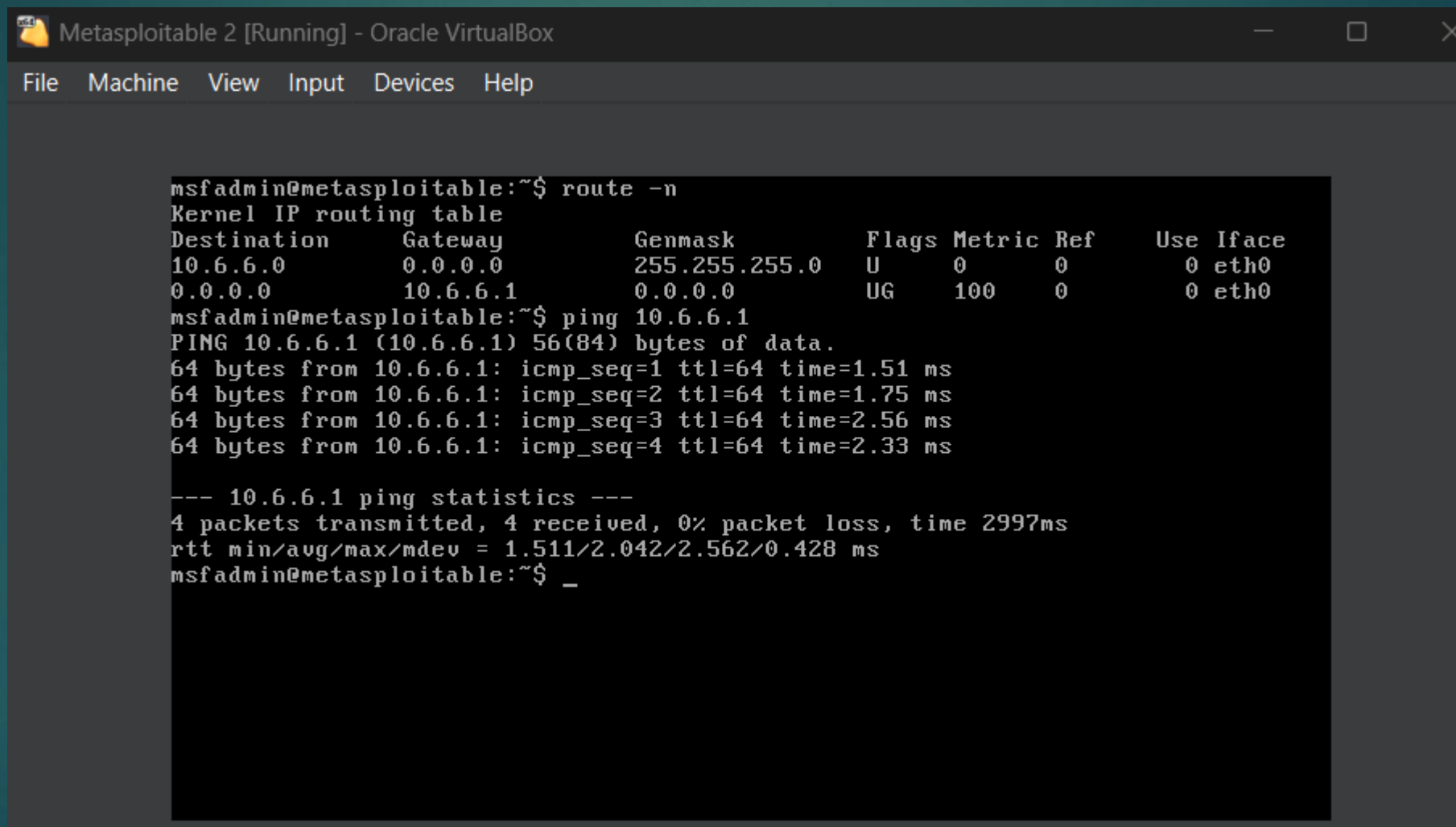
For ICMP rules on IPv4, one or more of these ICMP subtypes may be specified.

Source





Now Metasploitable2 in the same subnet as Pfense and can see each other



The screenshot shows a terminal window titled "Metasploitable 2 [Running] - Oracle VirtualBox". The terminal output displays the command `route -n` and its output, followed by a `ping 10.6.6.1` command and its results.

```
msfadmin@metasploitable:~$ route -n
Kernel IP routing table
Destination      Gateway          Genmask          Flags Metric Ref    Use Iface
10.6.6.0          0.0.0.0          255.255.255.0    U        0      0        0 eth0
0.0.0.0           10.6.6.1         0.0.0.0          UG        100    0        0 eth0

msfadmin@metasploitable:~$ ping 10.6.6.1
PING 10.6.6.1 (10.6.6.1) 56(84) bytes of data:
64 bytes from 10.6.6.1: icmp_seq=1 ttl=64 time=1.51 ms
64 bytes from 10.6.6.1: icmp_seq=2 ttl=64 time=1.75 ms
64 bytes from 10.6.6.1: icmp_seq=3 ttl=64 time=2.56 ms
64 bytes from 10.6.6.1: icmp_seq=4 ttl=64 time=2.33 ms

--- 10.6.6.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2997ms
rtt min/avg/max/mdev = 1.511/2.042/2.562/0.428 ms
msfadmin@metasploitable:~$ _
```

# Make a Rules to make Linux Mint see and send traffic to Metasploitable2

pfSense.home.arpa - Firewall: Rules: LAN — Mozilla Firefox

10.0.0.1/firewall\_rules.php?if=lan

WARNING: The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

Firewall / Rules / LAN

Floating WAN LAN OPT1 OPT2

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	✓ 0/1.27 MiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	✓ 3/25.04 MiB	IPv4 *	LAN subnets	*	*	*	*	none		Default allow LAN to any rule	
<input type="checkbox"/>	✓ 0/0 B	IPv6 *	LAN subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	

Add Add Delete Toggle Copy Save Separator

pfSense is developed and maintained by Netgate. © ESF 2004 - 2025 View license.

06:41

Now Metasploitable2 and Linux Mint can send traffic to each other

The screenshot displays the pfSense web interface in a Mozilla Firefox browser. The browser's address bar shows the URL `10.0.0.1/firewall_rules.php?if=lan`. The pfSense interface includes a top navigation bar with the logo and menu items: System, Interfaces, Firewall, Services, VPN, Status, and Diagnostics. A sidebar on the left contains icons for various system functions. The main content area is titled "Firewall / Rules" and shows a "WARNING: The address is not valid" message. Below this, a green box indicates "The changes have been saved" and a link to "Monitor the filter rules". A table titled "Rules (Drag to)" lists firewall rules with columns for "States" and "Action". The first rule is "1/1.29 M" with a green checkmark in the "States" column. The second rule is "0/0 B" with a green checkmark in the "States" column. A terminal window is overlaid on the right side of the screen, showing a successful ping test from `mohamed@mohamed:~` to `10.6.6.2`. The terminal output shows five successful ping requests with varying times, followed by a summary of the ping statistics.

```
mohamed@mohamed:~$ ping 10.6.6.2
PING 10.6.6.2 (10.6.6.2) 56(84) bytes of data:
64 bytes from 10.6.6.2: icmp_seq=1 ttl=63 time=1.83 ms
64 bytes from 10.6.6.2: icmp_seq=2 ttl=63 time=2.40 ms
64 bytes from 10.6.6.2: icmp_seq=3 ttl=63 time=2.45 ms
64 bytes from 10.6.6.2: icmp_seq=4 ttl=63 time=2.12 ms
64 bytes from 10.6.6.2: icmp_seq=5 ttl=63 time=4.38 ms
--- 10.6.6.2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4032ms
rtt min/avg/max/mdev = 1.827/2.633/4.375/0.898 ms
^Cmohamed@mohamed:~$
```

# Install Snort to detect unusual traffic

The screenshot displays the pfSense web interface in a Mozilla Firefox browser window. The browser's address bar shows the URL `10.0.0.1/pkg_mgr_installed.php`. The pfSense header includes the logo and navigation tabs: System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. The 'System' tab is selected, and its dropdown menu is open, listing options: Advanced, Certificates, General Setup, High Availability, Package Manager, Register, Routing, Setup Wizard, Update, User Manager, and Logout (admin). The main content area features a warning message about the default password, a breadcrumb trail 'System / Installed Packages', and a section titled 'Installed Packages' which currently displays 'There are no packages installed'. The footer of the interface states 'pfSense is developed and maintained by Netgate. © ESF 2004 - 2025 View license.' The desktop taskbar at the bottom shows various application icons and the system clock at 07:23.



System ▾

Interfaces ▾

Firewall ▾

Services ▾

VPN ▾

Status ▾

Diagnostics ▾

Help ▾



**WARNING:** The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

System / Package Manager / Available Packages ?

Installed Packages

Available Packages

## Search

Search term

snort

Both ▾

Search

Clear

Enter a search string or \*nix regular expression to search package names and descriptions.

## Packages

Name	Version	Description
------	---------	-------------

snort	4.1.6_17	Snort is an open source network intrusion prevention and detection system (IDS/IPS). Combining the benefits of signature, protocol, and anomaly-based inspection.
-------	----------	---

[+ Install](#)

Package Dependencies:

[snort-2.9.20\\_8](#)



System

Interfaces

Firewall

Services

VPN

Status

Diagnostics

Help



**WARNING:** The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

System / [Package Manager](#) / [Package Installer](#)



Installed Packages

Available Packages

Package Installer

Confirmation Required to install package pfSense-pkg-snort.

☒ Confirm



System ▾

Interfaces ▾

Firewall ▾

Services ▾

VPN ▾

Status ▾

Diagnostics ▾

Help ▾



**WARNING:** The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

System / Package Manager / Package Installer



Please wait while the installation of **pfSense-pkg-snort** completes.  
This may take several minutes. Do not leave or refresh the page!

Installed Packages

Available Packages

Package Installer

### Package Installation

```
[2/6] Fetching snort-2.9.20_8.pkg: ..... done
[3/6] Fetching daq-2.2.2_3.pkg: ..... done
[4/6] Fetching libpcap-1.10.4.pkg: ..... done
[5/6] Fetching pfSense-pkg-snort-4.1.6_17.pkg: ..... done
[6/6] Fetching libpfctl-0.8.pkg: . done
Checking integrity... done (0 conflicting)
[1/6] Installing libdnet-1.13_4...
[1/6] Extracting libdnet-1.13_4: ..... done
[2/6] Installing libpcap-1.10.4...
[2/6] Extracting libpcap-1.10.4: ..... done
[3/6] Installing daq-2.2.2_3...
[3/6] Extracting daq-2.2.2_3: ..... done
[4/6] Installing libpfctl-0.8...
[4/6] Extracting libpfctl-0.8: ..... done
```





COMMUNITY EDITION

System ▾

Interfaces ▾

Firewall ▾

Services ▾

VPN ▾

Status ▾

Diagnostics ▾

Help ▾



**WARNING:** The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

System / [Package Manager](#) / [Package Installer](#)



pfSense-pkg-snort installation successfully completed.

[Installed Packages](#)[Available Packages](#)[Package Installer](#)

### Package Installation

Please note that, by default, snort will truncate packets larger than the default snaplen of 15158 bytes. Additionally, LRO may cause issues with Stream5 target-based reassembly. It is recommended to disable LRO, if your card supports it.

This can be done by appending '-lro' to your ifconfig\_ line in rc.conf.

=====

Message from pfSense-pkg-snort-4.1.6\_17:

--

Please visit Services - Snort - Interfaces tab first to add an interface, then select your desired rules packages at the Services - Snort - Global tab. Afterwards visit the Updates tab to download your configured rulesets.

>>> Cleaning up cache... done.

Success





System ▾

Interfaces ▾

Firewall ▾

Services ▾

VPN ▾

Status ▾

Diagnostics ▾

Help ▾



**WARNING:** The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

Services / [Snort](#) / Global Settings[Snort Interfaces](#)[Global Settings](#)[Updates](#)[Alerts](#)[Blocked](#)[Pass Lists](#)[Suppress](#)[IP Lists](#)[SID Mgmt](#)[Log Mgmt](#)[Sync](#)

### Snort Subscriber Rules

**Enable Snort VRT**☐ Click to enable download of Snort free Registered User or paid Subscriber rules

[Sign Up for a free Registered User Rules Account](#)  
[Sign Up for paid Snort Subscriber Rule Set \(by Talos\)](#)

### Snort GPLv2 Community Rules

**Enable Snort GPLv2**☒ Click to enable download of Snort GPLv2 Community rules

The Snort Community Ruleset is a GPLv2 Talos certified ruleset that is distributed free of charge without any Snort Subscriber License restrictions. This ruleset is updated daily and is a subset of the subscriber ruleset.

### Emerging Threats (ET) Rules

**Enable ET Open**☒ Click to enable download of Emerging Threats Open rules

ETOpen is an open source set of Snort rules whose coverage is more limited than ETPro.

**Enable ET Pro**☐ Click to enable download of Emerging Threats Pro rules

[Sign Up for an ETPro Account](#)  
ETPro for Snort offers daily updates and extensive coverage of current malware threats.

**WARNING:** The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

[Services](#) / [Snort](#) / [Updates](#)

Snort Interfaces    Global Settings    Updates    Alerts

### Installed Rule Set MD5 Signature

Rule Set Name/Publisher
Snort Subscriber Ruleset
Snort GPLv2 Community Rules
Emerging Threats Open Rules
Snort OpenAppID Detectors
Snort AppID Open Text Rules
Feodo Tracker Botnet C2 IP Rules

MD5 Signature Date
Not Enabled
Not Downloaded
Not Downloaded
Not Enabled
Not Enabled
Not Enabled

## Update Your Rule Set

Last Update	Unknown	Result: Unknown
-------------	---------	-----------------

Update Rules ☒ Update Rules

Click **UPDATE RULES** to check for and automatically apply any new posted updates for selected rules packages. Clicking **FORCE UPDATE** will zero out the MD5 hashes and force the download and application of the latest versions of the enabled rules packages.

## Manage Rule Set Log

 View Log

 Clear Log

The log file is limited to 1024K in size and is automatically cleared when that limit is exceeded.

### Rules Update Task

Updating rule sets may take a while ... please wait for the process to complete.

This dialog will auto-close when the update is finished.



Close



System

Interfaces

Firewall

Services

VPN

Status

Diagnostics

Help

**WARNING:** The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

Services / Snort / Interfaces

Snort Interfaces

Global Settings

Updates

Alerts

Blocked

Pass Lists

Suppress

IP Lists

SID Mgmt

Log Mgmt

Sync

### Interface Settings Overview

Interface	Snort Status	Pattern Match	Blocking Mode	Description	Actions
-----------	--------------	---------------	---------------	-------------	---------

+ Add





System ▾

Interfaces ▾

Firewall ▾

Services ▾

VPN ▾

Status ▾

Diagnostics ▾

Help ▾



**WARNING:** The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

Services / [Snort](#) / WAN - Interface Settings



[Snort Interfaces](#)

[Global Settings](#)

[Updates](#)

[Alerts](#)

[Blocked](#)

[Pass Lists](#)

[Suppress](#)

[IP Lists](#)

[SID Mgmt](#)

[Log Mgmt](#)

[Sync](#)

[WAN Settings](#)

General Settings

**Enable** ☒ Enable interface

**Interface**   
Choose the interface where this Snort instance will inspect traffic.

**Description**   
Enter a meaningful description here for your reference.

**Snap Length**   
Enter the desired interface snaplen value in bytes. Default is 1518 and is suitable for most applications.

Alert Settings

**Send Alerts to System Log** ☐ Snort will send Alerts to the firewall's system log. Default is Not Checked.

**Enable Packet Captures** ☐ Checking this option will automatically capture packets that generate a Snort alert into a tcpdump compatible file



1518

Enter the desired interface snaplen value in bytes. Default is 1518 and is suitable for most applications.

## Alert Settings

☐ Snort will send Alerts to the firewall's system log. Default is Not Checked.

☐ Checking this option will automatically capture packets that generate a Snort alert into a tcpdump compatible file

☐ Checking this option will cause Snort to simultaneously log alerts to a unified2 binary format log file in the logging subdirectory for this interface.  
Default is Not Checked.

Log size and retention limits for the Unified2 log should be configured on the LOG MGMT tab when this option is enabled.

## Block Settings

☒ Checking this option will automatically block hosts that generate a Snort alert. Default is Not Checked.

Legacy Mode 

Select blocking mode operation. Legacy Mode inspects copies of packets while Inline Mode inserts the Snort inspection engine into the network stack between the NIC and the OS. Default is Legacy Mode.

Legacy Mode uses the PCAP engine to generate copies of packets for inspection as they traverse the interface. Some "leakage" of packets will occur before Snort can determine if the traffic matches a rule and should be blocked. Inline mode instead intercepts and inspects packets before they are handed off to the host network stack for further processing. Packets matching DROP rules are simply discarded (dropped) and not passed to the host network stack. No leakage of packets occurs with Inline Mode. **WARNING: Inline Mode only works with NIC drivers which properly support Netmap!** Supported drivers: `bnxt`, `cc`, `cxgbe`, `cxl`, `em`, `ena`, `ice`, `igb`, `igc`, `ix`, `ixgbe`, `ixl`, `lem`, `re`, `vmx`, `vtnet`. If problems are experienced with Inline Mode, switch to Legacy Mode instead.

☒ Checking this option will kill firewall established states for the blocked IP. Default is checked.

BOTH

Select which IP extracted from the packet you wish to block. Default is BOTH.

## Detection Performance Settings

AC-BNEA

Snort is 'live-reloading' the new rule set.

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

OPT1 Settings OPT1 Categories OPT1 Rules OPT1 Variables OPT1 Preprocs OPT1 IP Rep OPT1 Logs

Available Rule Categories

Category Selection: GPLv2\_community.rules

Select the rule category to view and manage.

Rule Signature ID (SID) Enable/Disable Overrides

SID Actions

Apply

Reset All

Reset Current

Disable All

Enable All

When finished, click APPLY to save and send any SID enable/disable changes made on this tab to Snort.

Rules View Filter

Selected Category's Rules

Legend: Default Enabled Enabled by user Auto-enabled by SID Mgmt Action/content modified by SID Mgmt Rule action is alert  
 Default Disabled Disabled by user Auto-disabled by SID Mgmt

State	Action	GID	SID	Proto	Source	SPort	Destination	DPort	Message
		1	105	tcp	\$HOME_NET	2589	\$EXTERNAL_NET	any	MALWARE-BACKDOOR - Dagger_1.4.0
		1	108	tcp	\$EXTERNAL_NET	any	\$HOME_NET	7597	MALWARE-BACKDOOR QAZ Worm Client Login access
		1	110	tcp	\$EXTERNAL_NET	any	\$HOME_NET	12345:12346	MALWARE-BACKDOOR netbus getinfo
		1	115	tcp	\$HOME_NET	20034	\$EXTERNAL_NET	any	MALWARE-BACKDOOR

## Services / Snort / Interface Settings / OPT1 - Categories

Snort Interfaces

Global Settings

Updates

Alerts

Blocked

Pass Lists

Suppress

IP Lists

SID Mgmt

Log Mgmt

Sync

OPT1 Settings

OPT1 Categories

OPT1 Rules

OPT1 Variables

OPT1 Preprocs

OPT1 IP Rep

OPT1 Logs



## Automatic Flowbit Resolution

## Resolve Flowbits

☒ If checked, Snort will auto-enable rules required for checked flowbits. Default is Checked.

Snort will examine the enabled rules in your chosen rule categories for checked flowbits. Any rules that set these dependent flowbits will be automatically enabled and added to the list of files in the interface rules directory.

## Select the rulesets (Categories) Snort will load at startup

 - Category is auto-enabled by SID Mgmt conf files - Category is auto-disabled by SID Mgmt conf files

Select All

Unselect All

 Save

Enable

Ruleset: Snort GPLv2 Community Rules



Snort GPLv2 Community Rules (Talos certified)

Enable

Ruleset: FEODO Tracker Botnet C2 IP Rules



Feodo Tracker Botnet C2 IP Rules

Enable

Ruleset: ET Open Rules

Snort Subscriber rules are not enabled.

Snort OPENAPPID rules are not enabled.



emerging-activex.rules



emerging-attack\_response.rules



emerging-botcc.portgrouped.rules



emerging-botcc.rules



emerging-chat.rules





**WARNING:** The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

## Services / Snort / Alerts

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

### Alert Log View Settings

Interface to Inspect

OPT1 (vtnet2)

☐ Auto-refresh view

250

Choose interface..

Alert lines to display.



Alert Log Actions



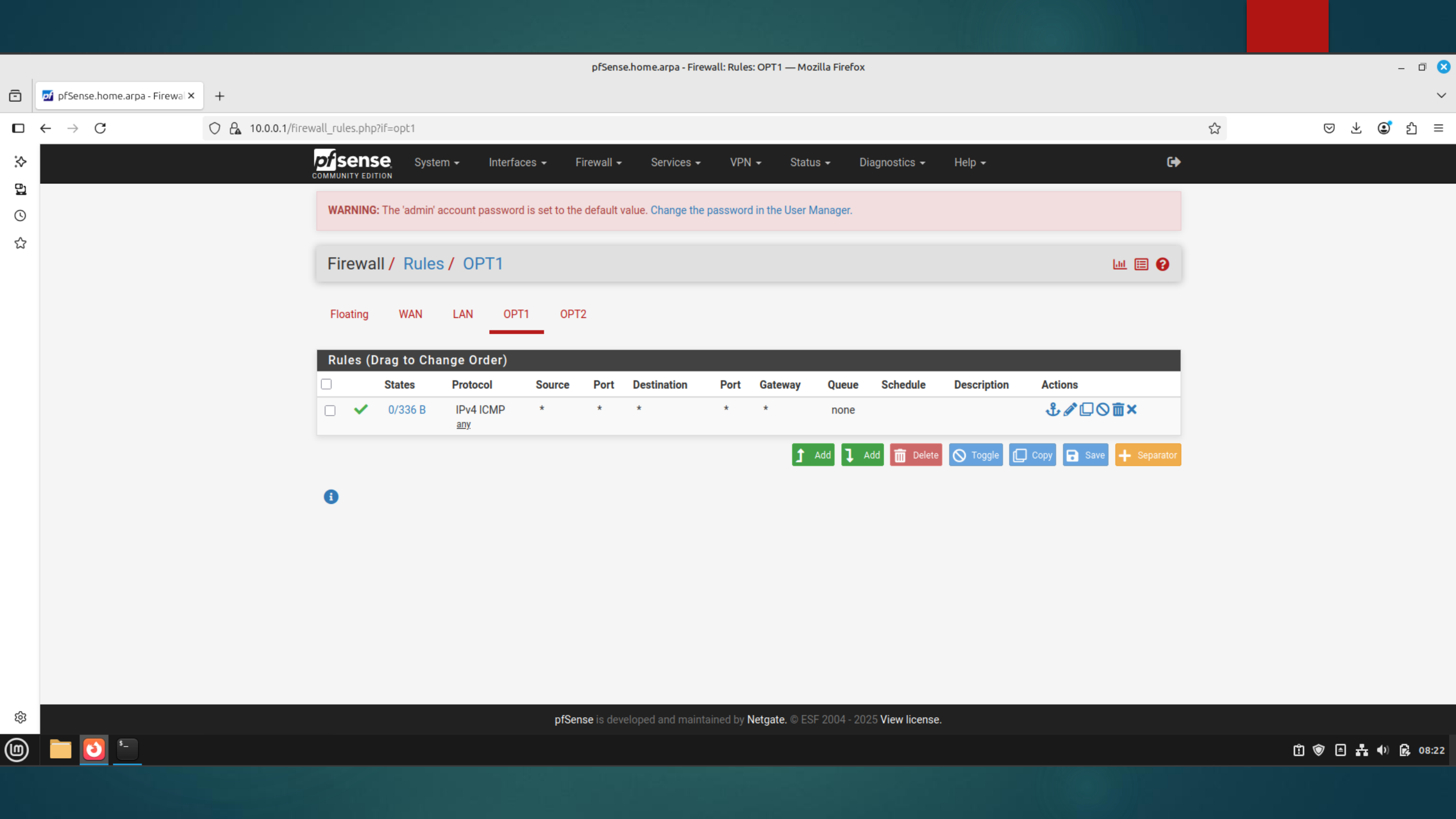
### Alert Log View Filter

### 2 Entries in Active Log

Date	Action	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	GID:SID	Description
2025-06-03 04:58:06		3	TCP	Unknown Traffic	10.6.6.2	80	10.0.0.100	48260	120:3	(http_inspect) NO CONTENT-LENGTH OR TRANSFER-ENCODING IN HTTP RESPONSE
2025-06-03 04:58:06		3	TCP	Unknown Traffic	10.0.0.100	48260	10.6.6.2	80	120:8	(http_inspect) INVALID CONTENT-LENGTH OR CHUNK SIZE

```
mohamed@mohamed: ~
mohamed@mohamed:~$ nmap -sV 10.6.6.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-06-03 07:58 EEST
mohamed@mohamed:~$
```





**WARNING:** The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

Firewall / Rules / OPT1

📊 📄 ?

Floating

WAN

LAN

**OPT1**

OPT2

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓	0/336 B	IPv4 ICMP any	*	*	*	*	none			🔗 ✎ 📄 ⏏️ 🗑️ ✕

⬆️ Add ⬇️ Add 🗑️ Delete ⏏️ Toggle 📄 Copy 💾 Save ➕ Separator





System

Interfaces

Firewall

Services

VPN

Status

Diagnostics

Help



**WARNING:** The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

Firewall / Rules / Edit



### Edit Firewall Rule

**Action**

Block

Choose what to do with packets that match the criteria specified below.  
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

**Disabled**

☐ Disable this rule

Set this option to disable this rule without removing it from the list.

**Interface**

OPT1

Choose the interface from which packets must come to match this rule.

**Address Family**

IPv4

Select the Internet Protocol version this rule applies to.

**Protocol**

TCP

Choose which IP protocol this rule should match.

### Source

**Source**

☐ Invert match

Any

Source Address /

Display Advanced

The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value.



## Source

Source☐ Invert match

Any

Source Address

 Display Advanced

The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, **any**.

## Destination

Destination☐ Invert match

Network

10.6.6.2

/ 24

Destination Port Range

FTP (21)

From

Custom

FTP (21)

To

Custom

Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

## Extra Options

Log☐ Log packets that are handled by this rule

Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the [Status: System Logs: Settings](#) page).

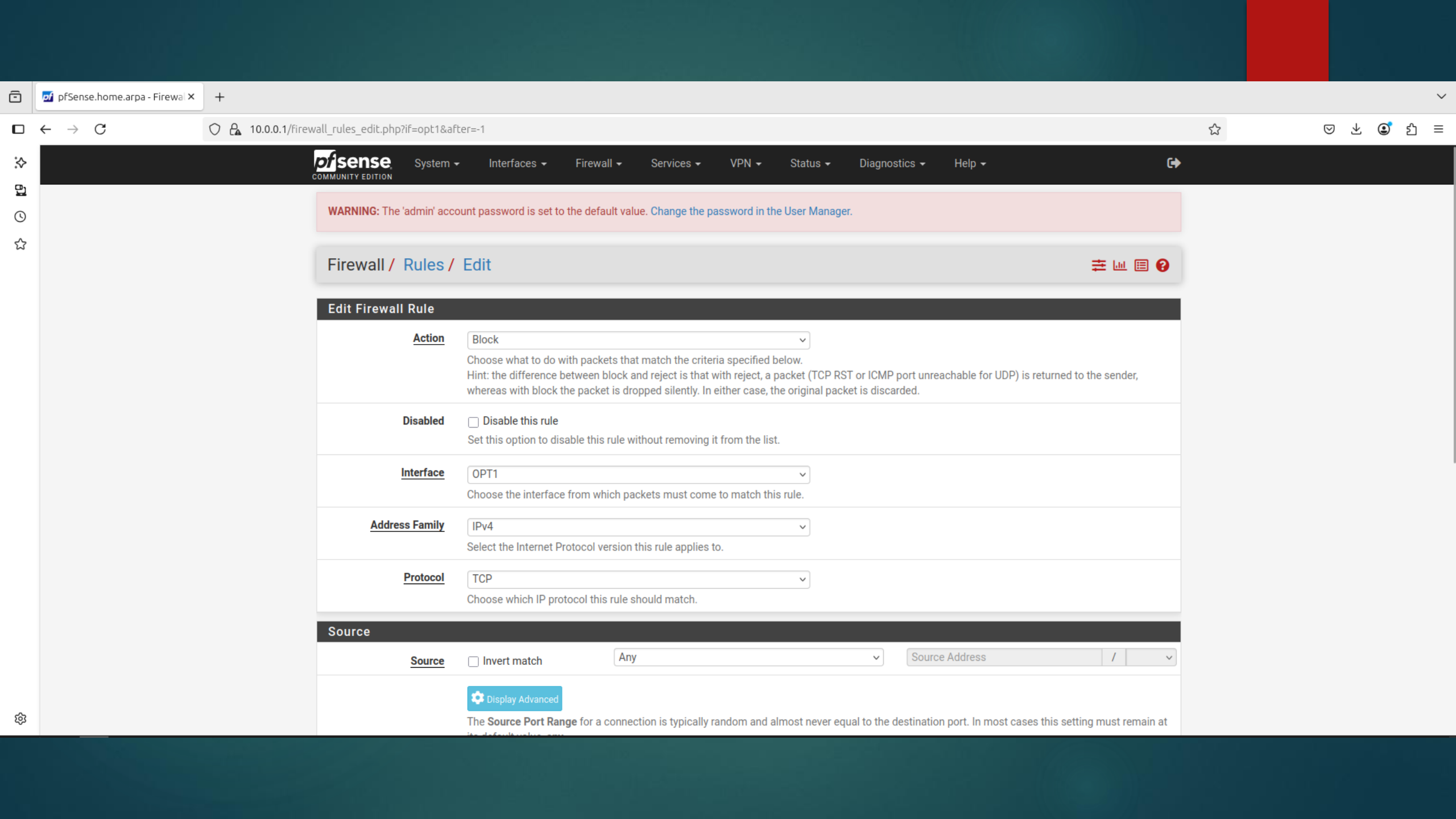
Description

Block FTP attacks

A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

Advanced Options

 Display Advanced Save



System ▾

Interfaces ▾

Firewall ▾

Services ▾

VPN ▾

Status ▾

Diagnostics ▾

Help ▾



**WARNING:** The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

Firewall / Rules / Edit



### Edit Firewall Rule

**Action**

Block ▾

Choose what to do with packets that match the criteria specified below.  
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

**Disabled**

☐ Disable this rule

Set this option to disable this rule without removing it from the list.

**Interface**

OPT1 ▾

Choose the interface from which packets must come to match this rule.

**Address Family**

IPv4 ▾

Select the Internet Protocol version this rule applies to.

**Protocol**

TCP ▾

Choose which IP protocol this rule should match.

### Source

**Source**

☐ Invert match

Any ▾

Source Address / ▾

Display Advanced

The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value.

**Source**

Source

☐ Invert match

Any

Source Address

Display Advanced

The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, **any**.

**Destination**

Destination

☐ Invert match

Network

10.6.6.2

**Destination Port Range**

Telnet (23)

From

Custom

To

Telnet (23)

Custom

Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

**Extra Options**

**Log**

☐ Log packets that are handled by this rule

Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the [Status: System Logs: Settings](#) page).

**Description**

A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

**Advanced Options**

Display Advanced

Save



WARNING: The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

Firewall / Rules / OPT1



The changes have been applied successfully. The firewall rules are now reloading in the background. [Monitor the filter reload progress.](#)

Floating WAN LAN OPT1 OPT2

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✗ 0/0 B	IPv4 TCP	*	*	10.6.6.2/24	23 (Telnet)	*	none			
<input type="checkbox"/>	✗ 0/0 B	IPv4 TCP	*	*	10.6.6.2/24	21 (FTP)	*	none		Block FTP attacks	
<input type="checkbox"/>	✓ 0/336 B	IPv4 ICMP any.	*	*	*	*	*	none			

Add Add Delete Toggle Copy Save Separator



(kali㉿kali)-[~]

\$ ping 192.168.179.136

PING 192.168.179.136 (192.168.179.136) 56(84) bytes of data.

64 bytes from 192.168.179.136: icmp\_seq=1 ttl=63 time=1.80 ms

64 bytes from 192.168.179.136: icmp\_seq=2 ttl=63 time=0.921 ms

64 bytes from 192.168.179.136: icmp\_seq=3 ttl=63 time=1.09 ms

^C

— 192.168.179.136 ping statistics —

3 packets transmitted, 3 received, 0% packet loss, time 2003ms

rtt min/avg/max/mdev = 0.921/1.269/1.795/0.378 ms

(kali㉿kali)-[~]

\$ nmap -A 192.168.179.136

Starting Nmap 7.95 ( <https://nmap.org> ) at 2025-05-22 13:05 EDT

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

WAN (em0)

Choose interface..

☒ Auto-refresh view

250

Alert lines to display.

Save

Alert Log Actions

Download

Clear

Alert Log View Filter

2 Entries in Active Log

Date	Action	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	GID:SID	Description
2025-05-22 21:01:38	⚠	3	TCP	Misc activity	192.168.179.136	6667	192.168.179.149	59939	1:2000355	ET CHAT IRC authorization message
2025-05-22 20:06:06	⚠	3	TCP	Misc activity	192.168.179.136	6667	192.168.179.149	51308	1:2000355	ET CHAT IRC authorization message