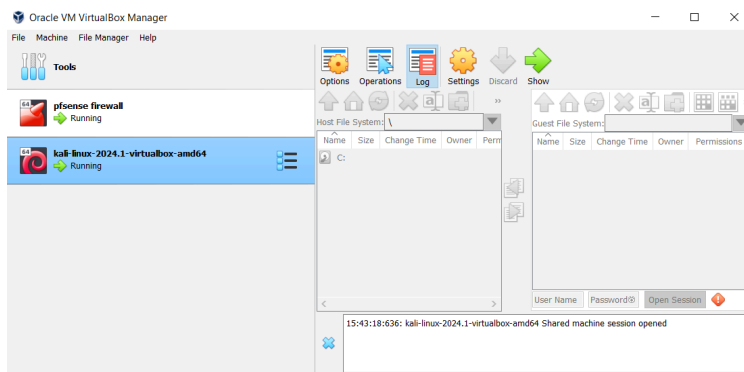
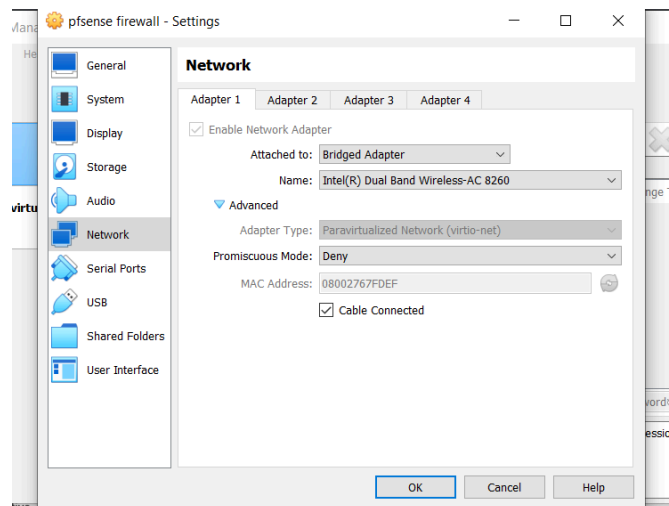


## 1. Install pfSense: OK, it's done

- Follow the steps outlined in the previous response "Installing pfSense on VirtualBox with DMZ Setup (Markdown Format)" to install pfSense on a VirtualBox VM.

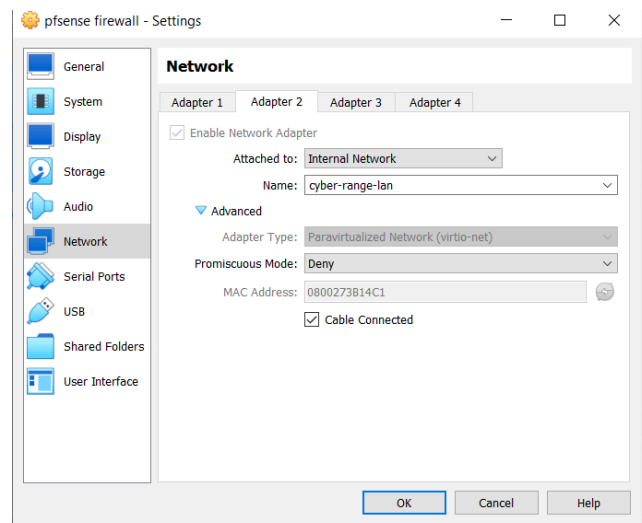


- During installation, select the following interface assignments:
- WAN (red): Bridged adapter connected to your internet modem.



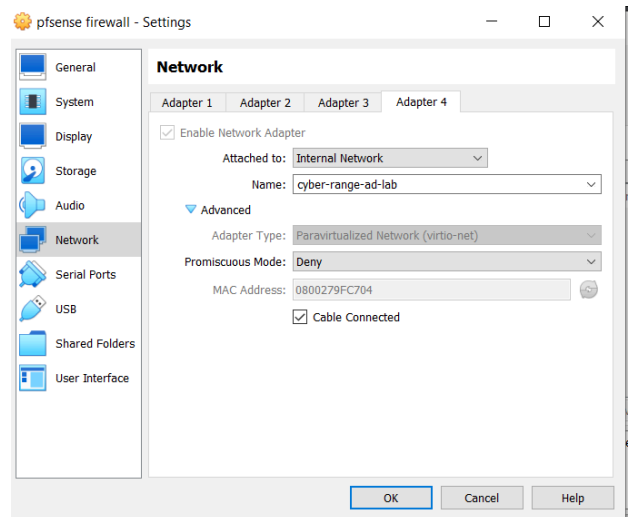
- LAN (green): Internal network adapter (created within VirtualBox).

○



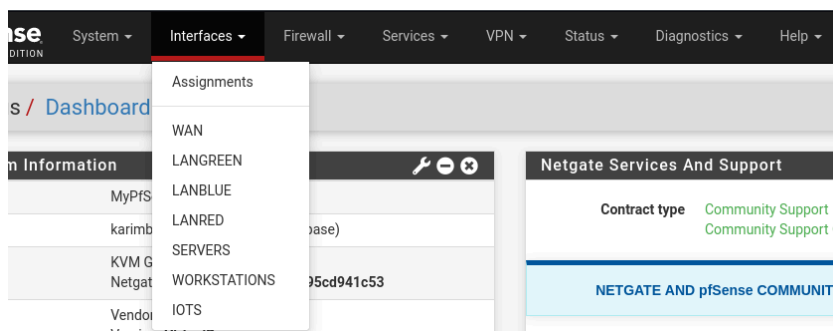
○

- **DMZ (red):** Separate internal network adapter (created within VirtualBox)



## 2. Configure VLANs:

- In the pfSense web GUI, go to **Interfaces > Assignments**.



- Create two new VLAN interfaces:
  - **Guest (Blue):** Tag it with a unique VLAN ID .
  - **DMZ (Red):** Tag it with a different VLAN ID .

Interface	Network port
WAN	vtnet0 (08:00:27:07:a4:f4)
LANGREEN	vtnet1 (08:00:27:a8:dc:92) <span>Delete</span>
LANBLUE	vtnet2 (08:00:27:4a:38:b2) <span>Delete</span>
LANRED	vtnet3 (08:00:27:1c:27:30) <span>Delete</span>
Servers	VLAN 10 on vtnet1 - lan (servers) <span>Delete</span>
Workstations	VLAN 20 on vtnet0 - wan (Workstations) <span>Delete</span>
IoT	VLAN 30 on vtnet0 - wan (IoT) <span>Delete</span>

Save

- Assign the Guest VLAN interface to the internal network adapter dedicated for guest devices.
- Assign the DMZ VLAN interface to the separate internal network adapter dedicated for the DMZ.

LANGREEN	LANBLUE	LANRED	SERVERS	WORKSTATIONS	IOT5
<b>General DHCP Options</b>					
DHCP Backend		Kea DHCP			
Enable		<input checked="" type="checkbox"/> Enable DHCP server on LANGREEN interface			
Deny Unknown Clients		<div>Allow all clients</div> <p>When set to <b>Allow all clients</b>, any DHCP client will get an IP address within this scope/range on this interface. If set to <b>Allow known clients from any interface</b>, any DHCP client with a MAC address listed in a static mapping on <b>any</b> scope(s)/interface(s) will get an IP address. If set to <b>Allow known clients from only this interface</b>, only MAC addresses listed in static mappings on this interface will get an IP address within this scope/range.</p>			
Ignore Client Identifiers		<input type="checkbox"/> Do not record a unique identifier (UID) in client lease data if present in the client DHCP request This option may be useful when a client can dual boot using different client identifiers but the same hardware (MAC) address. Note that the resulting server behavior violates the official DHCP specification.			
<b>Primary Address Pool</b>					
Subnet		10.0.0.0/24			
Subnet Range		10.0.0.1 - 10.0.0.254			
Address Pool Range		<div>10.0.0.10</div> <div>10.0.0.245</div> <div>From</div> <div>To</div> <p>The specified range for this pool must not be within the range configured on any other address pool for this interface.</p>			
Additional Pools		<div>+ Add Address Pool</div> <p>If additional pools of addresses are needed inside of this subnet outside the above range, they may be specified here.</p>			
<b>Server Options</b>					

### 3. Configure Firewall Rules:

- Go to **Firewall > Rules**.

- Create the following rules:
  - **Deny all traffic:** Block all traffic between any interface by default.
  - **Allow specific traffic:** Create specific rules to allow:
    - LAN to Guest: Only necessary traffic (e.g., web browsing, limited internet access).
    - Guest to LAN: Only allow specific outbound traffic (e.g., DNS lookups).
    - LAN to DMZ (optional): Only necessary traffic for exposed services.
    - DMZ to WAN (optional): Only allowed outbound traffic for the exposed services.
    - WAN to any: Block all incoming traffic by default.

Firewall / Rules / LANGREEN

Floating WAN **LANGREEN** LANBLUE LANRED SERVERS WORKSTATIONS IOTS

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	1/2.13 MB	*	*	*	LANGREEN Address	443	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	0/0 B	IPv4+6 *	*	*	WAN subnets	*	*	none			
<input checked="" type="checkbox"/>	14/235.23 MB	IPv4 *	LANGREEN subnets	*	*	*	*	none		Default allow LAN to any rule	
<input checked="" type="checkbox"/>	0/0 B	IPv6 *	LANGREEN subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	

Add Add Delete Toggle Copy Save Separator

Firewall / Rules / LANRED

Floating WAN LANGREEN LANBLUE **LANRED** SERVERS WORKSTATIONS IOTS

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	0/0 B	IPv4 *	LANRED subnets	*	LANRED address	*	*	none		Allow packets to default gateway	
<input checked="" type="checkbox"/>	0/0 B	IPv4 *	LANRED subnets	*	kali	*	*	none		Allow packets to Kali VM	
<input checked="" type="checkbox"/>	0/0 B	IPv4 *	LANRED subnets	*	!RFC1918	*	*	none		Allow packets to any non-private address	
<input type="checkbox"/>	0/0 B	IPv4+6 *	*	*	*	*	*	none		Block everything else	

Add Add Delete Toggle Copy Save Separator

Firewall / Rules / LANBLUE

Floating WAN LANGREEN **LANBLUE** LANRED SERVERS WORKSTATIONS IOTS

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	0/0 B	IPv4 *	LANBLUE subnets	*	kali	*	*	none		Allow packets to Kali VM	
<input type="checkbox"/>	0/0 B	IPv4+6 *	*	*	*	*	*	none		Block access to everything	

Add Add Delete Toggle Copy Save Separator