



SECURITY+ V4 LAB SERIES

Lab 17: Configuring a Network-Based Firewall

Document Version: **2024-01-29**

Material in this Lab Aligns to the Following	
CompTIA Security+ (SY0-601) Exam Objectives	3.3: Given a scenario, implement secure network designs 4.4: Given an incident, apply mitigation techniques or controls to secure an environment
All-In-One CompTIA Security+ Sixth Edition ISBN-13: 978-1260464009 Chapters	19: Secure Network Design 29: Mitigation Techniques and Controls

Copyright © 2024 Network Development Group, Inc.
www.netdevgroup.com

NETLAB+ is a registered trademark of Network Development Group, Inc.
KALI LINUX™ is a trademark of Offensive Security.
Microsoft®, Windows®, and Windows Server® are trademarks of the Microsoft group of companies.
VMware is a registered trademark of VMware, Inc.
SECURITY ONION is a trademark of Security Onion Solutions LLC.
Android is a trademark of Google LLC.
pfSense® is a registered mark owned by Electric Sheep Fencing LLC ("ESF").
All trademarks are property of their respective owners.

Contents

Introduction	3
Objective	3
Lab Topology	4
Lab Settings	5
1 Configure ICMP on the Firewall	6
1.1 Blocking ICMP Requests on pfSense	6
2 Redirecting Traffic to Internal Hosts on the Network	11
2.1 Configuring pfSense to Allow Port and Redirect Requests	11
2.2 Retargeted SSH Connection	12
3 Configuring VPN on pfSense	15
3.1 Configuring VPN Server	15
3.2 Exporting VPN Client Data	24
3.3 Configuring the VPN Client	25
3.4 Connecting the VPN Client	28
3.5 Managing VPN Connections	29

Introduction

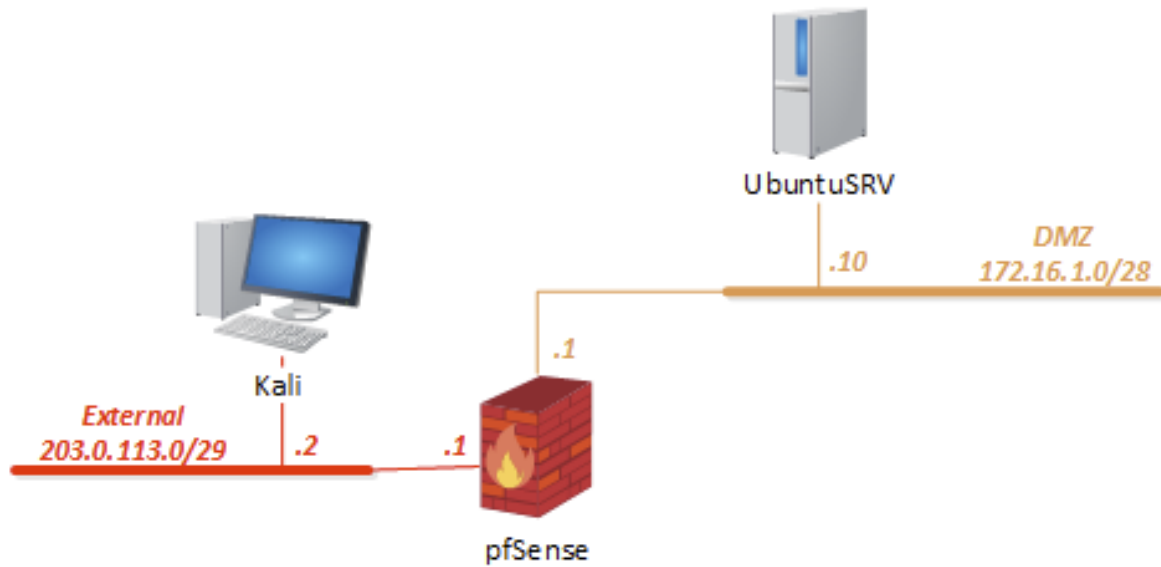
In this lab, you will be conducting network security practices using the pfSense VM.

Objective

In this lab, you will perform the following tasks:

- Install and configure network components to support organizational security
- Given a scenario, implement secure network architecture

Lab Topology



Lab Settings

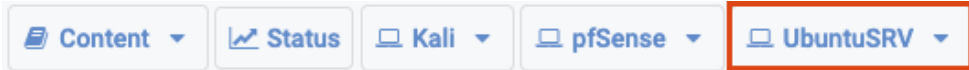
The information in the table below will be needed in order to complete the lab. The task sections below provide details on the use of this information.

Virtual Machine	IP Address	Account (if needed)	Password (if needed)
Kali	203.0.113.2	kali	kali
pfSense	192.168.0.1	sysadmin	NDGlabpass123!
UbuntuSRV	172.16.1.10	sysadmin	NDGlabpass123!

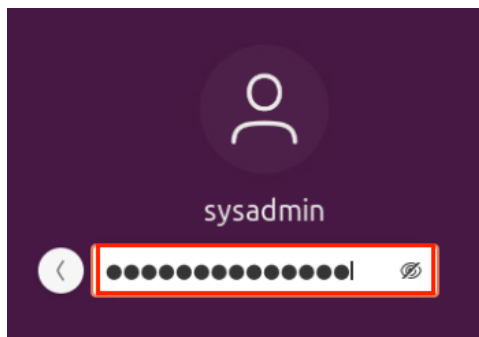
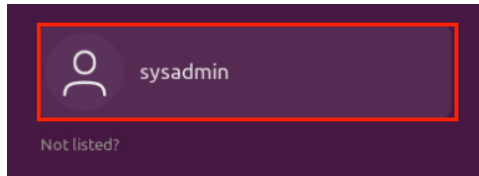
1 Configure ICMP on the Firewall

1.1 Blocking ICMP Requests on pfSense

1. Launch the **UbuntuSRV** virtual machine to access the graphical login screen.



2. Log in as **sysadmin** with **NDGlabpass123!** as the password.



3. Open a *Terminal* window by clicking on the **Terminal** icon located in the left menu pane.



4. Send a ping request to the **Kali** system; **203.0.113.2**. Type the command below, followed by pressing the **Enter** key.

```
sysadmin@ubuntusrv:~$ ping -c4 203.0.113.2
```

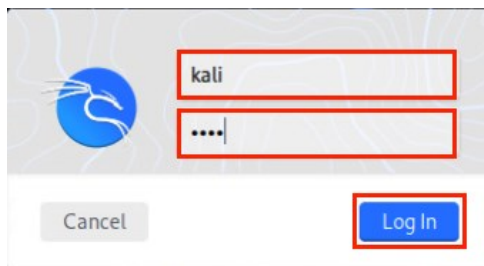
```
sysadmin@ubuntusrv:~$ ping -c4 203.0.113.2
PING 203.0.113.2 (203.0.113.2) 56(84) bytes of data.
64 bytes from 203.0.113.2: icmp_seq=1 ttl=63 time=1.10 ms
64 bytes from 203.0.113.2: icmp_seq=2 ttl=63 time=0.455 ms
64 bytes from 203.0.113.2: icmp_seq=3 ttl=63 time=0.550 ms
64 bytes from 203.0.113.2: icmp_seq=4 ttl=63 time=0.479 ms

--- 203.0.113.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3041ms
rtt min/avg/max/mdev = 0.455/0.646/1.102/0.265 ms
sysadmin@ubuntusrv:~$
```

5. After a successful ping, launch the **Kali** virtual machine to access the graphical login screen.



6. Log in as **kali** with **kali** as the password. Open the **Kali PC Viewer**.



7. Open a new terminal window by clicking on the **terminal** icon located in the top toolbar.



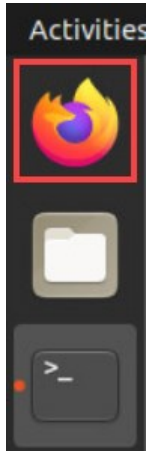
8. From the **Kali** terminal, send a ping request to the **UbuntuSRV** system: **172.16.1.10**.

```
kali@kali$ ping -c4 172.16.1.10
```

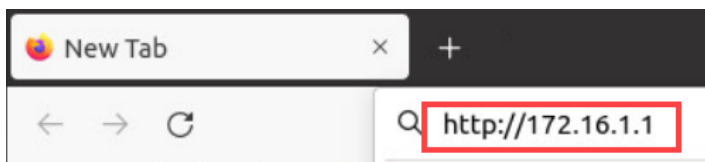
```
(kali@kali)-[~]
$ ping -c4 172.16.1.10
PING 172.16.1.10 (172.16.1.10) 56(84) bytes of data.
64 bytes from 172.16.1.10: icmp_seq=1 ttl=63 time=0.568 ms
64 bytes from 172.16.1.10: icmp_seq=2 ttl=63 time=0.448 ms
64 bytes from 172.16.1.10: icmp_seq=3 ttl=63 time=0.458 ms
64 bytes from 172.16.1.10: icmp_seq=4 ttl=63 time=0.520 ms

--- 172.16.1.10 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3057ms
rtt min/avg/max/mdev = 0.448/0.498/0.568/0.048 ms
```

9. After the successful ping, change focus to the **UbuntuSRV** system and open the **Firefox** web browser.



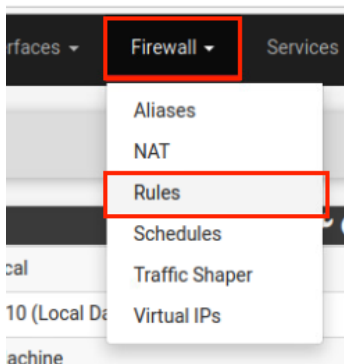
10. In the *address space*, type `http://172.16.1.1`. Press **Enter**.



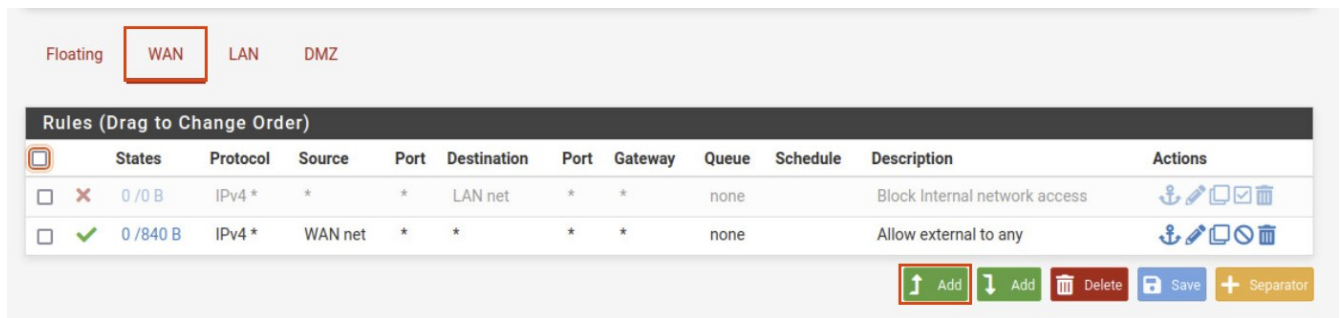
11. Type the username **sysadmin** and password **NDGlabpass123!**. Click the **SIGN IN** button.



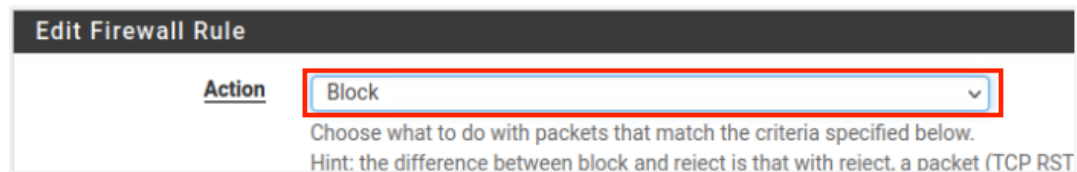
12. Once in the *pfSense* management graphical user interface, navigate to **Firewall > Rules**.



13. While viewing the *WAN* tab, click the **Add rule to the top of the list** icon on the bottom-right to add a new rule.



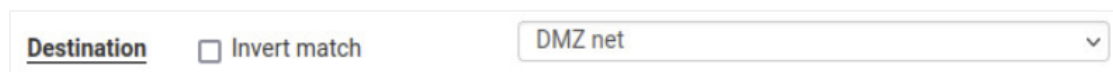
14. On the newly opened page, click the dropdown box next to *Action* and select **Block**.



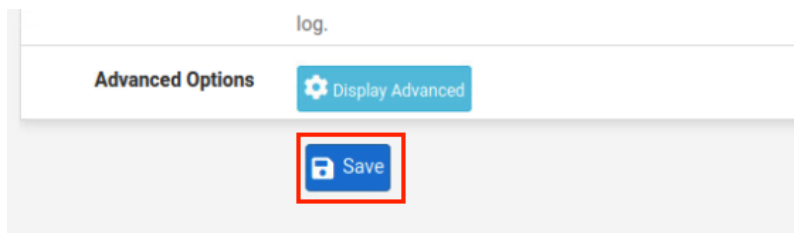
15. Select **ICMP** as the *Protocol* selection, and leave the *ICMP Subtypes* as is.



16. In the **Destination** section, set the network as the **DMZ net**, which is the **172.16.1.1/28** mask.



17. Leave all other options as **defaults**. Click the **Save** button located towards the bottom of the page.



18. When brought back to the *Firewall: Rules* page, notice the warning message. Select **Apply Changes**.

The firewall rule configuration has been changed.
The changes must be applied for them to take effect.

✓ Apply Changes

19. Verify that the firewall rules table looks like the image below for the *WAN* interface.

FloatingWANLANDMZ

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 ICMP any	*	*	DMZ net	*	*	none			
<input type="checkbox"/>	0/0 B	IPv4 *	*	*	LAN net	*	*	none		Block Internal network access	
<input type="checkbox"/>	0/2 KiB	IPv4 *	WAN net	*	*	*	*	none		Allow external to any	

Add

Add

Delete

Save

Separator

20. Change focus to the **Kali** system and navigate to the **Terminal** window. Attempt to **ping** the **UbuntuSRV** system once again. The ping should not succeed.

```
kali@kali$ ping -c4 172.16.1.10
```

```
(kali@kali)-[~]
$ ping -c4 172.16.1.10
PING 172.16.1.10 (172.16.1.10) 56(84) bytes of data.

--- 172.16.1.10 ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 3077ms
```

2 Redirecting Traffic to Internal Hosts on the Network

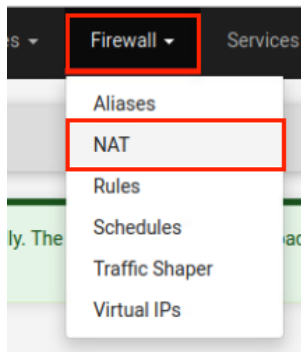
2.1 Configuring pfSense to Allow Port and Redirect Requests

1. While on the *Kali* system, enter the command below to scan for open ports on the firewall appliance.

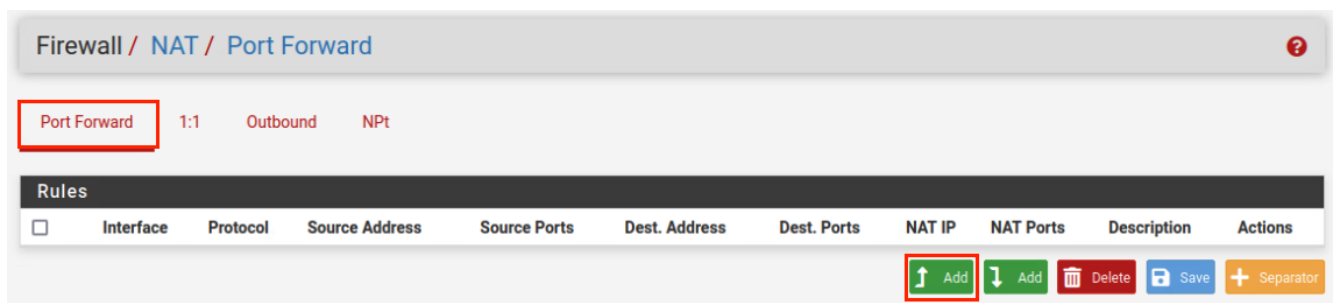
```
kali@kali$ nmap 203.0.113.1
```

```
(kali@kali)-[~]  
$ nmap 203.0.113.1  
Starting Nmap 7.91 ( https://nmap.org ) at 2021-08-01 17:58 CDT  
Nmap scan report for 203.0.113.1  
Host is up (0.00091s latency).  
Not shown: 998 filtered ports  
PORT      STATE SERVICE  
53/tcp    open  domain  
80/tcp    open  http  
  
Nmap done: 1 IP address (1 host up) scanned in 17.58 seconds
```

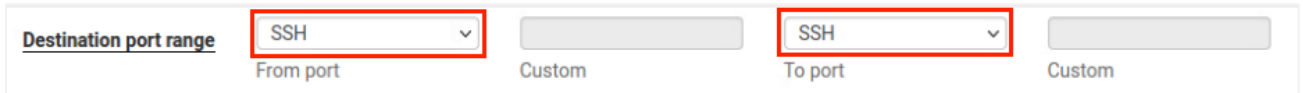
2. Change focus to the **Firefox** window on the **UbuntuSRV** system. In the *pfSense* management interface, navigate to **Firewall > NAT**.



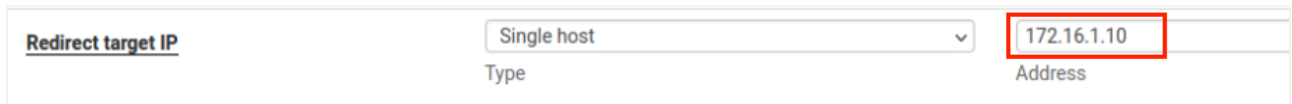
3. On the *Firewall / NAT / Port Forward* interface, click the **Add rule to the top of the list** button to add a new rule.



4. While on the *Firewall / NAT / Port Forward / Edit* interface, make the following changes:
 - a. Change *Destination port range* to **SSH** for both *From port* and *To port* from the dropdown menu.



- b. Change *Redirect target IP* to **172.16.1.10**.



- c. Change *Redirect target port* to **SSH** from the dropdown menu.



- d. Click the **Save** button located towards the bottom of the page
5. For the new configuration to take place, click the **Apply changes** button.

The NAT configuration has been changed.
The changes must be applied for them to take effect.

✓ Apply Changes

2.2 Retargeted SSH Connection

1. Change focus to the **Kali** system and initiate a quick scan against the firewall appliance using the terminal.

```
kali@kali$ nmap 203.0.113.1
```

```
(kali@kali)-[~]
$ nmap 203.0.113.1
Starting Nmap 7.91 ( https://nmap.org ) at 2021-08-01 18:16 CDT
Nmap scan report for 203.0.113.1
Host is up (0.00062s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain
80/tcp    open  http
Nmap done: 1 IP address (1 host up) scanned in 18.07 seconds
```



Notice the change of open ports on the system; *SSH* is now open.

2. Verify the *SSH* configuration made on the firewall by typing the following command. Answer **yes** to accept the fingerprint. If prompted for a password, enter **NDGLabpass123!**.

```
kali@kali$ ssh sysadmin@203.0.113.1
```

```
(kali@kali)-[~]
$ ssh sysadmin@203.0.113.1
The authenticity of host '203.0.113.1 (203.0.113.1)' can't be established.
ECDSA key fingerprint is SHA256:Q/tBtXJLxJyOgvr6JheGkrFVSAUoEYYubMgwCPGDhW0.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '203.0.113.1' (ECDSA) to the list of known hosts.
sysadmin@203.0.113.1's password:
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.4.0-80-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Fri 24 Feb 2023 02:36:27 AM UTC

System load:  0.16               Processes:           371
Usage of /:   34.2% of 38.26GB   Users logged in:    1
Memory usage: 40%               IPv4 address for docker0: 172.17.0.1
Swap usage:   0%                IPv4 address for ens160: 172.16.1.10

 * Super-optimized for small spaces - read how we shrank the memory
   footprint of MicroK8s to make it the smallest full K8s around.

   https://ubuntu.com/blog/microk8s-memory-optimisation

0 updates can be applied immediately.

The list of available updates is more than a week old.
To check for new updates run: sudo apt update
```

- Notice the *Secure Shell* prompt says you are on the **sysadmin@ubuntu** machine. To confirm you are on the correct system, use the **ifconfig** command.

```
sysadmin@ubuntu:~$ ifconfig
docker0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    inet 172.17.0.1 netmask 255.255.0.0 broadcast 172.17.255.255
    ether 02:42:8a:10:81:ad txqueuelen 0 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    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

ens160: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 172.16.1.10 netmask 255.255.255.240 broadcast 172.16.1.15
    inet6 fe80::250:56ff:fe16:110 prefixlen 64 scopeid 0x20<link>
    ether 00:50:56:16:01:10 txqueuelen 1000 (Ethernet)
    RX packets 3233 bytes 1666957 (1.6 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4075 bytes 389930 (389.9 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 11967 bytes 1023597 (1.0 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 11967 bytes 1023597 (1.0 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

- Type the command **route** to examine the *default gateway*.

```
sysadmin@ubuntu:~$ route
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
default 172.16.1.1 0.0.0.0 UG 0 0 0 ens160
172.16.1.0 0.0.0.0 255.255.255.240 U 0 0 0 ens160
172.17.0.0 0.0.0.0 255.255.0.0 U 0 0 0 docker0
```

- Type the command **exit** to leave the active SSH connection.

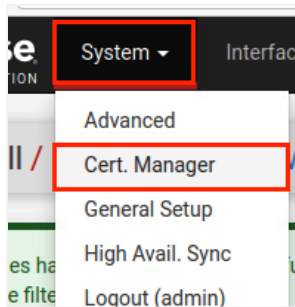
```
sysadmin@ubuntu:~$ exit
logout
Connection to 203.0.113.1 closed.

(kali@kali)-[~]
$
```

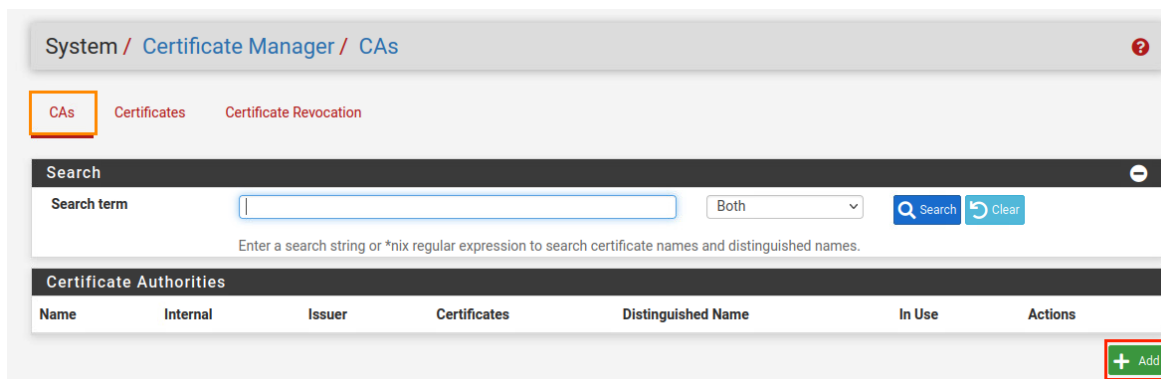
3 Configuring VPN on pfSense

3.1 Configuring VPN Server

1. Change focus to the **UbuntuSRV** system and focus on the **Firefox** web browser. If you are not already logged into the *pfSense firewall management interface*, do so now.
2. While logged in, navigate to **System > Cert Manager**.



3. On the *System / Certificate Manager / CAs* page, while on the **CAs** tab, click on the **+ Add** button.



4. A new page should open; fill in the necessary fields.
 - a. *Descriptive Name*: MyCA

Descriptive name	MyCA
-------------------------	------

- b. *Method*: **Create an internal Certificate Authority**

Method	Create an internal Certificate Authority
---------------	--

c. *Key Length*: **2048** bits

Key type RSA

2048

The length to use when generating a new RSA key, in bits.
The Key Length should not be lower than 2048 or some platforms may consider the certificate invalid.

d. *Lifetime*: 365 days

Lifetime (days) 365

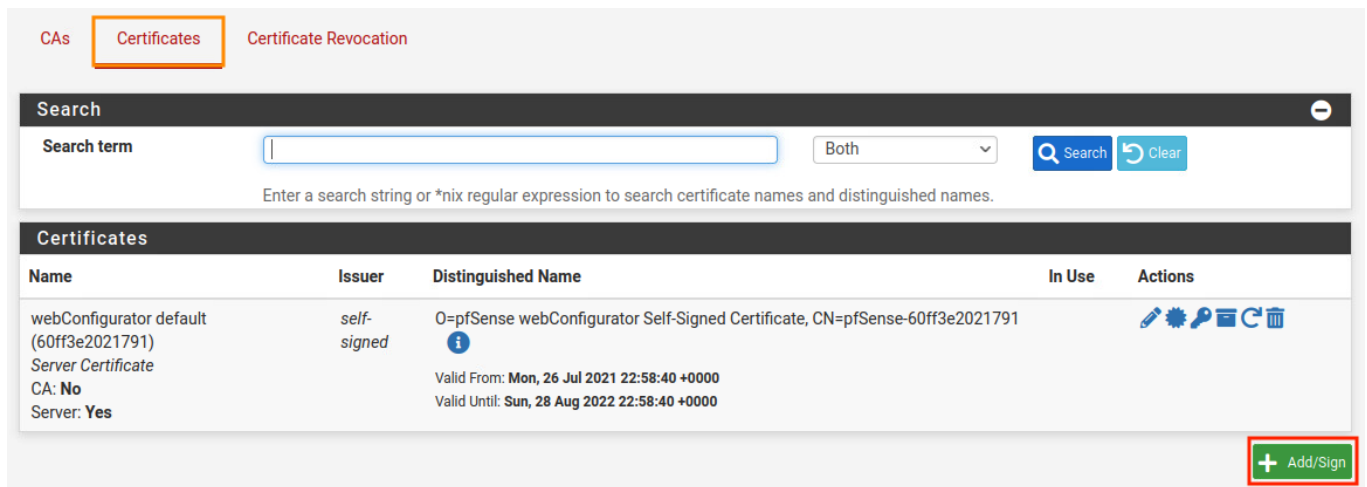
e. *Distinguished Name*:

- i. *Common Name*: internal-ca
- ii. *Country Code*: US
- iii. *State or Province*: Texas
- iv. *City*: Austin
- v. *Organization*: XYZ Security

<u>Common Name</u>	internal-ca
The following certificate authority subject components are optional and may be left blank.	
<u>Country Code</u>	US
<u>State or Province</u>	Texas
<u>City</u>	Austin
<u>Organization</u>	XYZ Security

f. Click **Save**.

5. Add a server certificate this time by navigating to the **Certificates** tab. To add a new certificate, click on the **+ Add/Sign** button.








CA's **Certificates** Certificate Revocation

Search

Search term Both

Enter a search string or *nix regular expression to search certificate names and distinguished names.

Certificates

Name	Issuer	Distinguished Name	In Use	Actions
webConfigurator default (60ff3e2021791) Server Certificate CA: No Server: Yes	self-signed	O=pfSense webConfigurator Self-Signed Certificate, CN=pfSense-60ff3e2021791 Valid From: Mon, 26 Jul 2021 22:58:40 +0000 Valid Until: Sun, 28 Aug 2022 22:58:40 +0000		    

+ Add/Sign

6. A new page should open; select the dropdown menu next to *Method* and select **Create an internal Certificate**.

Method

7. Fill in the necessary fields.

- a. *Descriptive Name*: **VPNServerCert**

Descriptive name

- b. *Certificate authority*: **MyCA**

Certificate authority

- c. *Key Length*: **2048** bits

Key type

The length to use when generating a new RSA key, in bits.
The Key Length should not be lower than 2048 or some platforms may consider the certificate invalid.

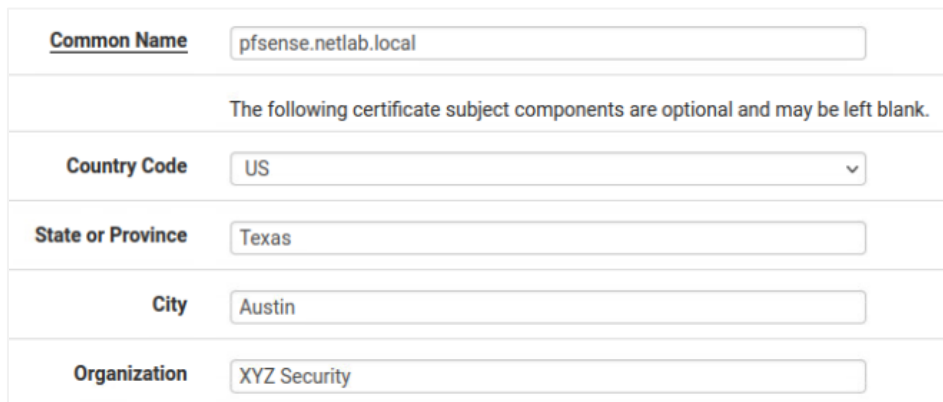
d. *Lifetime*: **365** days



Lifetime (days) 365

e. Distinguished Name:

- i. *Common Name*: **pfsense.netlab.local**
- ii. *Country Code*: **US**
- iii. *State or Province*: **Texas**
- iv. *City*: **Austin**
- v. *Organization*: **XYZ Security**



Common Name pfsense.netlab.local

The following certificate subject components are optional and may be left blank.

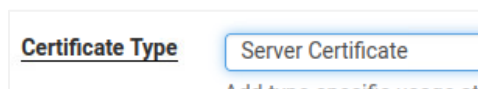
Country Code US

State or Province Texas

City Austin

Organization XYZ Security

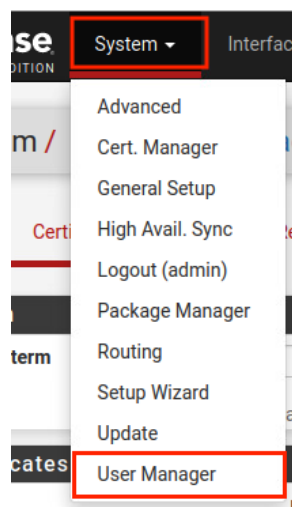
f. *Certificate Type*: **Server Certificate**



Certificate Type Server Certificate

g. Click **Save**.

8. Navigate to **System > User Manager**.



9. On the *System: User Manager* page, click the **+Add** icon to create a new user.

System / User Manager / Users ?

Users Groups Settings Authentication Servers

Users					
	Username	Full name	Status	Groups	Actions
<input type="checkbox"/>	admin	System Administrator	✓	admins	
<input type="checkbox"/>	sysadmin	Netlab Sysadmin	✓	admins	

+ Add
Delete

10. Fill in the necessary fields.

a. *Username*: vpnuser

Username

b. *Password*: vpnpassword

Password

c. *Full name*: VPN User

Full name
User's full name, for admin

d. Check the box next to **Click to create a user certificate** (more options will appear). Then verify the following information.

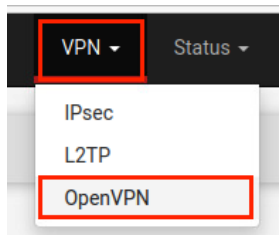
Certificate ☒ Click to create a user certificate

- i. *Descriptive name:* VPNUser_Cert
- ii. *Certificate Authority:* **MyCA**
- iii. *Key Length:* **2048** bits
- iv. *Lifetime:* **365** days

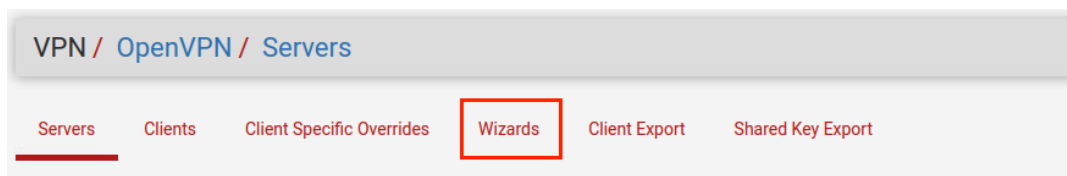
Descriptive name	VPNUser_Cert
Certificate authority	MyCA
Key type	RSA
	2048
	The length to use when generating a new RSA key, in bits. The Key Length should not be lower than 2048 or some platforms may consid
Digest Algorithm	sha256
	The digest method used when the certificate is signed. The best practice is to use an algorithm stronger than SHA1. Some platforms
Lifetime	365

e. Click **Save**.

11. Navigate to **VPN > OpenVPN**.



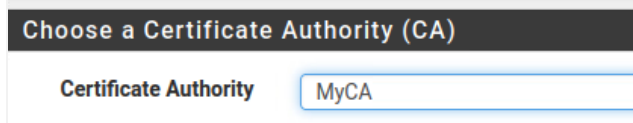
12. While on the *OpenVPN: Server* page, click on the **Wizards** tab.



13. A new page appears; select **Local User Access** for *Type of Server*. Click **Next**.

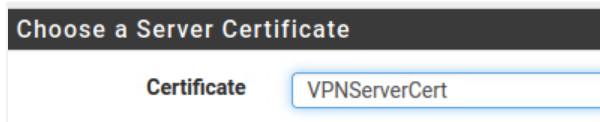
Select an Authentication Backend Type	
Type of Server	Local User Access
NOTE: If unsure, leave this set to "Local User Access."	

14. On the next page, select **MyCA** as the *Certificate Authority*. Click **Next**.



The screenshot shows a form titled "Choose a Certificate Authority (CA)". It has a label "Certificate Authority" and a dropdown menu with "MyCA" selected.


15. Next, select **VPNServerCert** as the *Certificate*. Click **Next**.



The screenshot shows a form titled "Choose a Server Certificate". It has a label "Certificate" and a dropdown menu with "VPNServerCert" selected.

16. On the next page, fill in all necessary fields as mentioned below (if the field is not mentioned, leave its default setting):

a. *Interface*: WAN



The screenshot shows a form with a label "Interface" and a dropdown menu with "WAN" selected. Below the dropdown, there is a small text label "The interface where OpenVPN".

b. *Protocol*: UDP on IPv4 Only



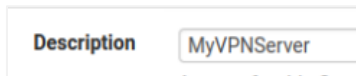
The screenshot shows a form with a label "Protocol" and a dropdown menu with "UDP on IPv4 only" selected.

c. *Local Port*: 1194



The screenshot shows a form with a label "Local Port" and a text input field containing "1194". Below the input field, there is a small text label "Local port used".

d. *Description*: MyVPNServer



The screenshot shows a form with a label "Description" and a text input field containing "MyVPNServer".

e. *Cryptographic Settings:*

- i. *TLS Authentication:* **Checked**
- ii. *Generate TLS Key:* **Checked**
- iii. *DH Parameters Length:* **2048 bit**
- iv. *Fallback Data Encryption Algorithm:* **AES-128-CBC (128-bit)**
- v. *Hardware Crypto:* **No Hardware Crypto Acceleration**

TLS Authentication	<input checked="" type="checkbox"/>	Enable authentication of TLS packets.
Generate TLS Key	<input checked="" type="checkbox"/>	Automatically generate a shared TLS authentication key.
DH Parameters Length	<input type="text" value="2048 bit"/>	Length of Diffie-Hellman (DH) key exchange parameters, used for establishing a secure connection. The length of the key is determined by the key size, but as with other such settings, the larger the key, the more secure the connection. As of 2016, 2048 bit is a common and typical selection.
Data Encryption Negotiation	<input checked="" type="checkbox"/>	Enable negotiation of Data Encryption Algorithms between client and server. The client and server negotiate the best algorithm to use.
Data Encryption Algorithms	<div>AES-256-GCM AES-128-GCM CHACHA20-POLY1305</div>	List of algorithms clients can negotiate to encrypt traffic between endpoints. The client and server negotiate the best algorithm to use. Certain algorithms will perform better on different hardware, depending on the hardware capabilities. After finishing the wizard for additional choices.
Fallback Data Encryption Algorithm	<input type="text" value="AES-128-CBC (128 bit key, 128 bit block)"/>	The algorithm used to encrypt traffic between endpoints when data encryption negotiation fails.
Auth Digest Algorithm	<input type="text" value="SHA256 (256-bit)"/>	The method used to authenticate traffic between endpoints. This setting must be compatible with the chosen encryption algorithm.
Hardware Crypto	<input type="text" value="No Hardware Crypto Acceleration"/>	Whether to use hardware acceleration for cryptographic operations.

- f. *Tunnel Settings:*
- i. *Tunnel Network:* 10.1.1.0/24
 - ii. *Redirect Gateway:* **Checked**
 - iii. *Local Network:* 172.16.1.0/28
 - iv. *Concurrent Connections:* 10
 - v. *Compression:* **Disable Compression**

Tunnel Network	<input type="text" value="10.1.1.0/24"/>
This is the virtual network used for private communications between this server and client hosts expressed using CIDR notation (eg. 10.0.8.0/24). The first network address will be assigned to the server virtual interface. The remaining network addresses will be assigned to connecting clients.	
Redirect Gateway	<input checked="" type="checkbox"/>
Force all client generated traffic through the tunnel.	
Local Network	<input type="text" value="172.16.1.0/28"/>
This is the network that will be accessible from the remote endpoint, expressed as a CIDR range. This may be left blank if not adding a route to the local network through this tunnel on the remote machine. This is generally set to the LAN network.	
Concurrent Connections	<input type="text" value="10"/>
Specify the maximum number of clients allowed to concurrently connect to this server.	
Allow Compression	<input type="text" value="Refuse any non-stub compression (Most secure)"/>
Allow compression to be used with this VPN instance, which is potentially insecure.	
Compression	<input type="text" value="Disable Compression [Omit Preference]"/>
Compress tunnel packets using the chosen option. Can save bandwidth, but is potentially insecure and may expose data. This setting has no effect if compression is not allowed. Adaptive compression will dynamically disable compression for a period of time if OpenVPN detects that the data in the packets is not being compressed efficiently.	

- g. *Client Settings:*
- i. *Dynamic IP:* **Checked**

Dynamic IP	<input checked="" type="checkbox"/>
Allow connected client	

- h. Click **Next**.

17. On the *Firewall Rule Configuration* page, fill in the necessary fields:

- a. *Firewall Rule:* **Checked**
- b. *OpenVPN rule:* **Checked**
- c. Click **Next**.

Traffic from clients to server	
Firewall Rule	<input checked="" type="checkbox"/>
Add a rule to per	
Traffic from clients through VPN	
OpenVPN rule	<input checked="" type="checkbox"/>
Add a rule to allo	

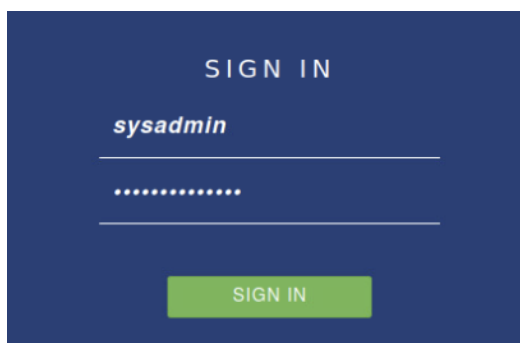
18. On the final configuration page, select **Finish**.

3.2 Exporting VPN Client Data

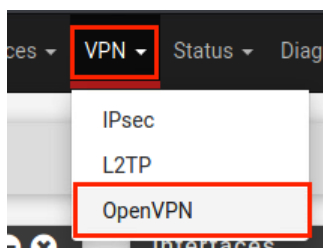
1. Switch to the **kali** machine, and start a *Firefox* browser.



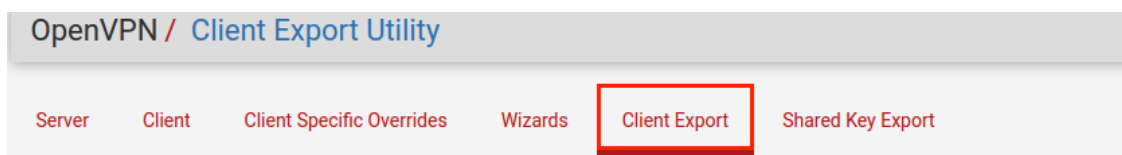
2. Go to <http://203.0.113.1> and log in as username **sysadmin** and password **NDGlabpass123!**.



3. Under **VPN**, click to go to the **OpenVPN** page.



4. Click on the **Client Export** tab.



5. Scroll down towards the bottom where the *OpenVPN Clients* is presented. Underneath the *Export* column, click on the **Archive** link to download the bundled configurations.

OpenVPN Clients		
User	Certificate Name	Export
vpnuser	VPNUser_Cert	<p>- Inline Configurations:</p> <p> Most Clients Android </p> <p> OpenVPN Connect (iOS/Android) </p> <p>- Bundled Configurations:</p> <p> Archive Config File Only </p> <p>- Current windows Installers (2.5.2-lx01):</p> <p> 64-bit 32-bit </p> <p>- Legacy Windows Installers (2.4.11-lx01):</p> <p> 10/2016/2019 7/8.1/2012r2 </p> <p>- Viscosity (Mac OS X and Windows):</p> <p> Viscosity Bundle Viscosity Inline Config </p>

6. Notice that the file download is complete.

3.3 Configuring the VPN Client

1. While on the **Kali** system, open a **terminal** and type the command below to change to the **Downloads** directory.

```
kali@kali$ cd ~/Downloads
```

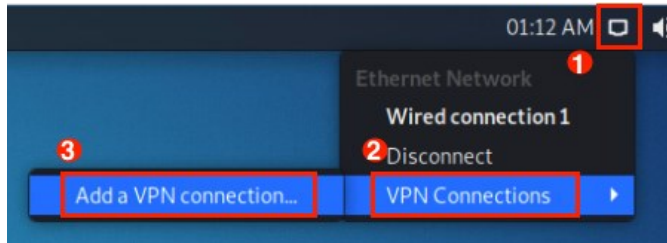
```
(kali@kali)-[~]
$ cd ~/Downloads
```

2. **Unzip** the downloaded zip file.

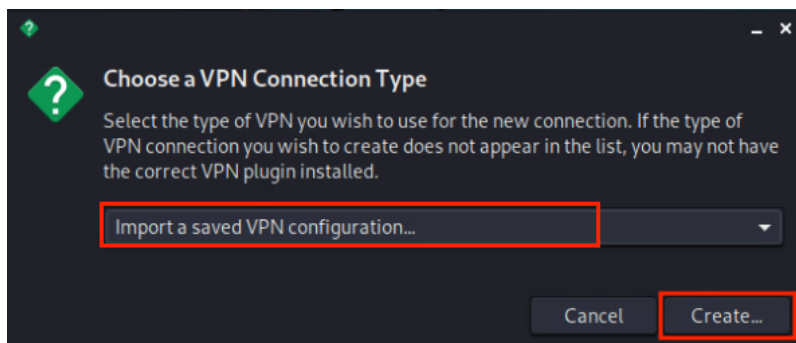
```
kali@kali$ unzip pfSense-UDP4-1194-vpnuser-config.zip
```

```
(kali@kali)-[~/Downloads]
$ unzip pfSense-UDP4-1194-vpnuser-config.zip
Archive:  pfSense-UDP4-1194-vpnuser-config.zip
  creating: pfSense-UDP4-1194-vpnuser/
  inflating: pfSense-UDP4-1194-vpnuser/pfSense-UDP4-1194-vpnuser.ovpn
  inflating: pfSense-UDP4-1194-vpnuser/pfSense-UDP4-1194-vpnuser.p12
  inflating: pfSense-UDP4-1194-vpnuser/pfSense-UDP4-1194-vpnuser-tls.key
```

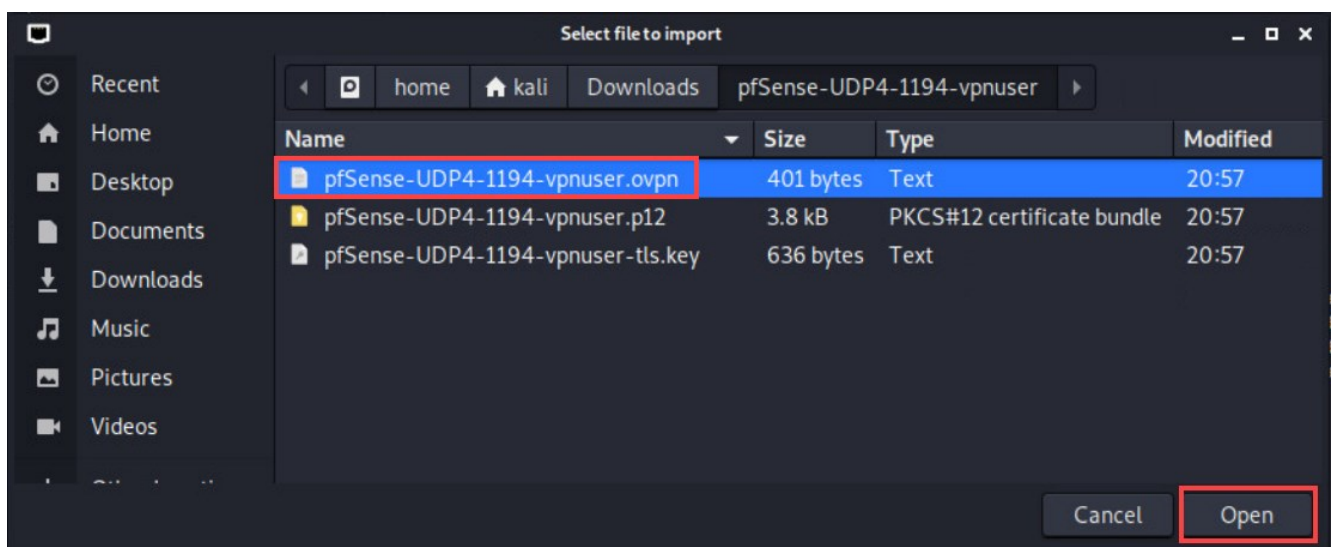
- Open the **Network Manager** by clicking on the **network** icon located on the top pane and navigate to **VPN Connections > Add a VPN Connection**.



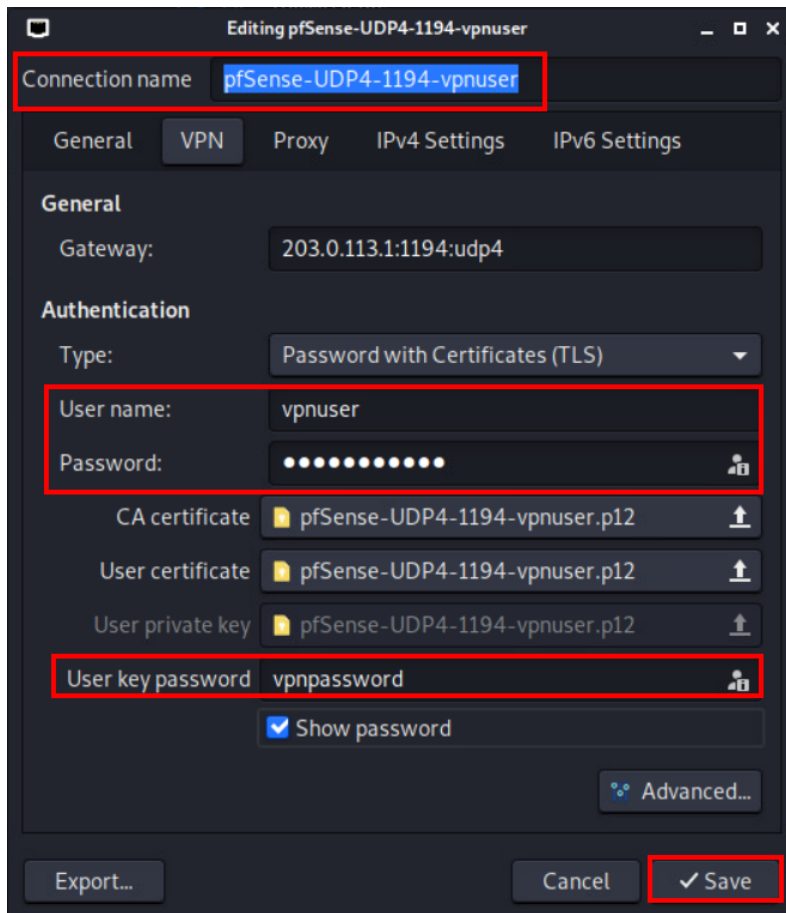
- On the *Choose a VPN connection Type* window, select **Import a saved VPN configuration** option and click **Create**.



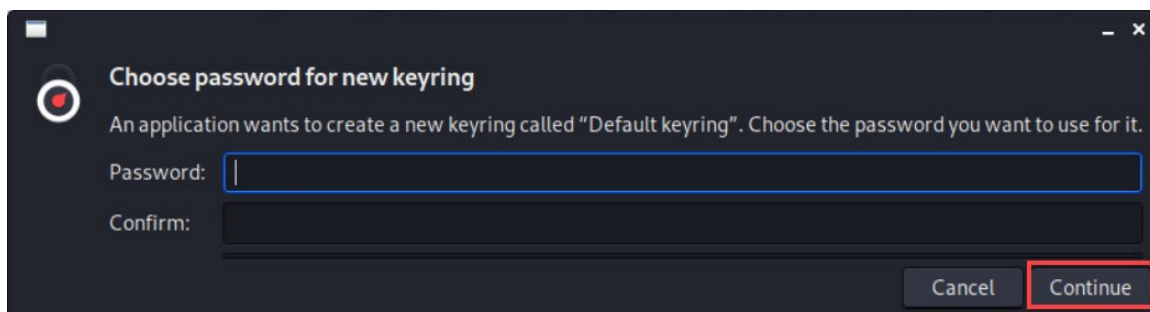
- In the *File Manager* window, select **Downloads** from the menu on the left. Double-click on the **pfSense-udp-1194-vpnuser** folder. Select the **pfSense-UDP4-1194-vpnuser.ovpn** file and click the **Open** button.



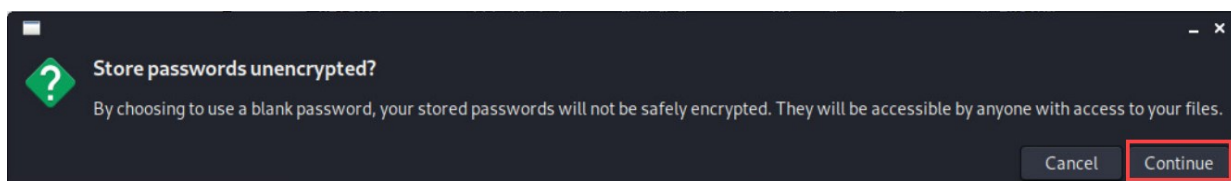
6. In the new pop-up window, leave the *Connection name* as is. Type `vpnuser` in the *User name* field, and type `vpnpassword` in the *Password* field. Then, type the `vpnpassword` again in the *User key password* field. Then, click the **Save** button.



7. If prompted to create a password for the new key ring, leave the two fields empty and click **Continue**.

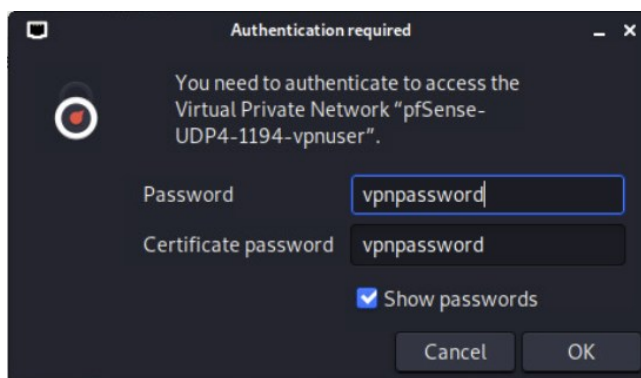
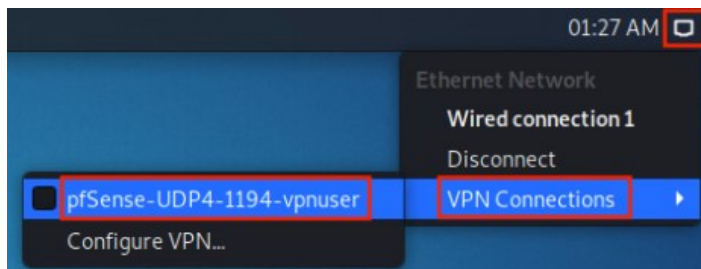


8. If prompted to store passwords unencrypted, click **Continue**.

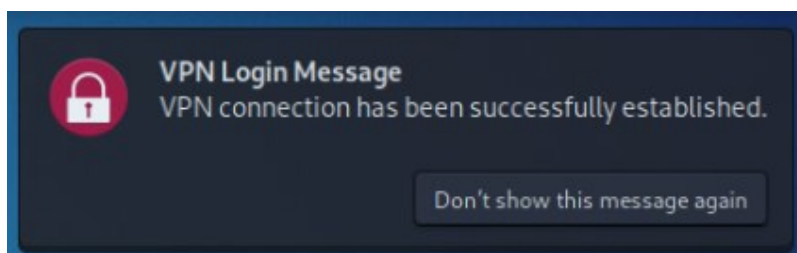


3.4 Connecting the VPN Client

1. Connect using the *VPN* settings by clicking on the **Network Manager** icon on the top pane and navigating to **VPN Connection > pfSense-UDP4-1194-vpnuser**. If prompted for a password, enter `vpnpassword`. Click **OK**.



2. Once the connection is established, a message will pop up like so:



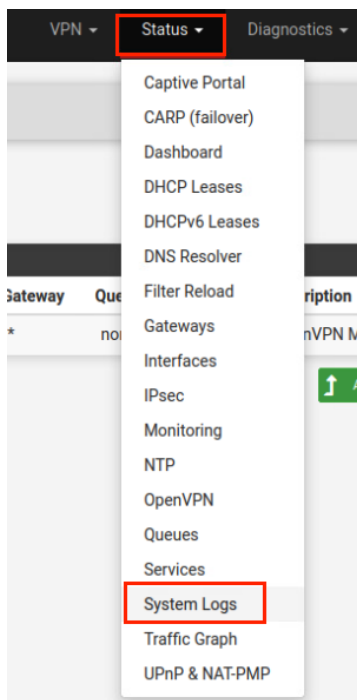
3. Verify the *VPN* tunnel and the IP address given by entering the command below in a *Terminal*.

```
kali@kali$ ip addr
```

```
(kali@kali) - [~/Downloads]
$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group def
  aut qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP
  group default qlen 1000
    link/ether 00:50:56:03:13:02 brd ff:ff:ff:ff:ff:ff
    inet 203.0.113.2/29 brd 203.0.113.7 scope global noprefixroute eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::250:56ff:fe03:1302/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
5: tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast
  state UNKNOWN group default qlen 500
    link/none
    inet 10.1.1.2/24 brd 10.1.1.255 scope global noprefixroute tun0
        valid_lft forever preferred_lft forever
    inet6 fe80::b8b5:79b9:8953:a736/64 scope link stable-privacy
        valid_lft forever preferred_lft forever
```

3.5 Managing VPN Connections

1. Once connected to the *VPN server*, switch to the **UbuntuSRV**, **Firefox** web browser, and navigate back to the **pfSense Web Configurator**.
2. When logged in as *admin*, navigate to **Status > System Logs** from the top menu pane.






- On the new page, select the **OpenVPN** tab.



- Notice the authentication to the *VPN server*. You may have to scroll down to find it.

Aug 2 05:57:15	openvpn	41845	user 'vpuser' authenticated
Aug 2 05:57:15	openvpn	16992	vpuser/203.0.113.2:40404 MULTI_sva: pool returned IPv4=10.1.1.2, IPv6=(Not enabled)
Aug 2 06:09:56	openvpn	16992	vpuser/203.0.113.2:40404 [vpuser] Inactivity timeout (-ping-restart), restarting

- Navigate to **Status > OpenVPN**.
- Notice how the current active *VPN connections* are listed here.

MyVPNServer UDP4:1194 Client Connections: 1						
Common Name	Real Address	Virtual Address	Connected Since	Bytes Sent	Bytes Received	Cipher
vpuser vpuser	203.0.113.2:43848	10.1.1.2	2021-08-02 06:25:13	11 KiB	13 KiB	AES-256-GCM
Status:  Actions:  						

- The lab is now complete; you may end the reservation.