



SECURITY+ V4 LAB SERIES

Lab 17: Configuring a Network-Based Firewall

Document Version: **2022-04-29**

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 © 2022 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	10
2.1 Configuring pfSense to Allow Port and Redirect Requests.....	10
2.2 Retargeted SSH Connection	11
3 Configuring VPN on pfSense	13
3.1 Configuring VPN Server.....	13
3.2 Exporting VPN Client Data.....	20
3.3 Configuring the VPN Client.....	22
3.4 Connecting the VPN Client	24
3.5 Managing VPN Connections.....	25

Introduction

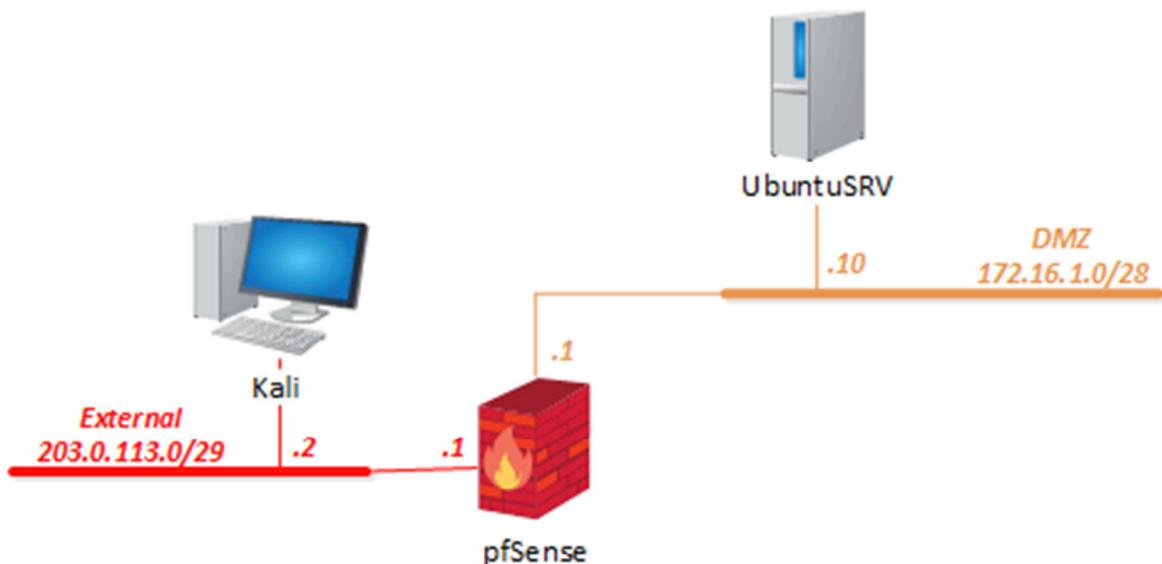
In this lab, you will be conducting network security practices using the pfSense VM.

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!

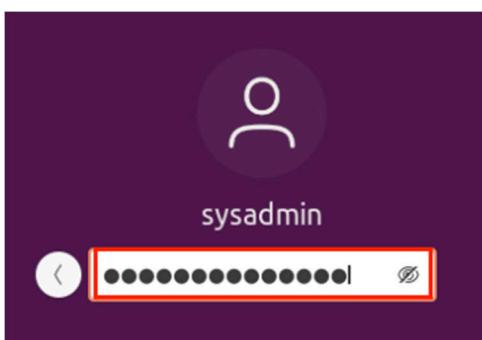
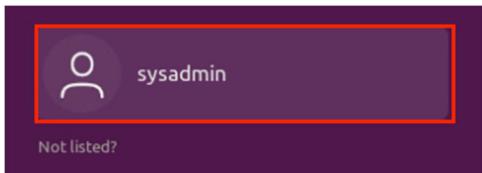
1 Configure ICMP on the Firewall

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.



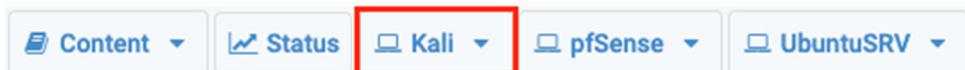
4. Send a ping request to the **Kali** system; **203.0.113.2**. Type the command below, followed by pressing the **Enter** key.

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

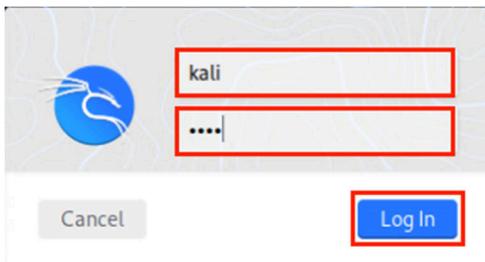
```
sysadmin@ubuntusrv:~$ ping -c4 203.0.113.2
PING 203.0.113.2 (203.0.113.2) 56(84) bytes of data.
64 bytes from 203.0.113.2: icmp_seq=1 ttl=63 time=1.10 ms
64 bytes from 203.0.113.2: icmp_seq=2 ttl=63 time=0.455 ms
64 bytes from 203.0.113.2: icmp_seq=3 ttl=63 time=0.550 ms
64 bytes from 203.0.113.2: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



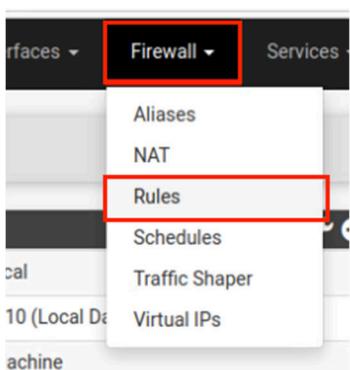
10. In the *address space*, type `http://192.168.0.1`. Press **Enter**.



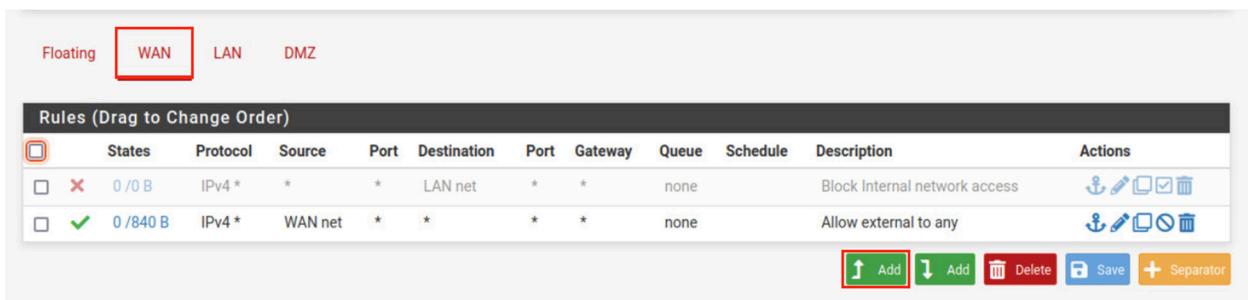
11. Type the username `sysadmin` and password `NDGLabpass123!`. Click the **SIGN IN** button.



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



13. While viewing the *WAN* tab, click the **Add** 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.

The screenshot shows a configuration page with two main sections. The first section is labeled "Protocol" with a dropdown menu set to "ICMP". Below it is a note: "Choose which IP protocol this rule should match.". The second section is labeled "ICMP Subtypes" with a dropdown menu set to "any". A list of options is visible: "Alternate Host", "Datagram conversion error", and "Echo reply". Below this list is a note: "For ICMP rules on IPv4, one or more of these ICMP subtypes may be specified."

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

The screenshot shows a configuration interface with a "Destination" field containing "DMZ net". There is also an "Invert match" checkbox and a dropdown menu.

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

The screenshot shows a configuration interface with an "Advanced Options" section containing a "Display Advanced" button. At the bottom, there is a "Save" button, which is highlighted with a red box.

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

The screenshot shows a yellow warning box with the text: "The firewall rule configuration has been changed. The changes must be applied for them to take effect." To the right of the box is a green "Apply Changes" button with a checkmark icon.

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

The screenshot shows a "Rules (Drag to Change Order)" table for the WAN interface. The table has columns: States, Protocol, Source, Port, Destination, Port, Gateway, Queue, Schedule, Description, and Actions. There are three rows:

- Row 1:** States: 0 / 0 B, Protocol: IPv4 ICMP any, Source: *, Destination: DMZ net, Port: *, Gateway: *, Queue: none, Description: none. Actions: edit, delete.
- Row 2:** States: 0 / 0 B, Protocol: IPv4 *, Source: *, Destination: LAN net, Port: *, Gateway: *, Queue: none, Description: Block Internal network access. Actions: edit, delete.
- Row 3:** States: 0 / 2 KiB, Protocol: IPv4 *, Source: WAN net, Destination: *, Port: *, Gateway: *, Queue: none, Description: Allow external to any. Actions: edit, delete.

At the bottom are buttons: Add (up/down), Delete, Save, and 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
```

The screenshot shows a terminal window with the following output:

```
(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

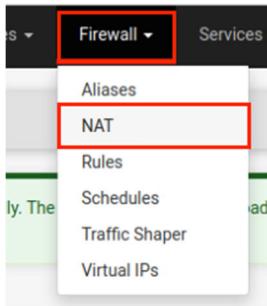
- While on the *Kali* system, enter the command below to scan for open ports on the firewall appliance.

```
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
```

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



- On the *Firewall: NAT: Port Forward* interface, click the **+** icon on the top-right to add a new rule.

	Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions

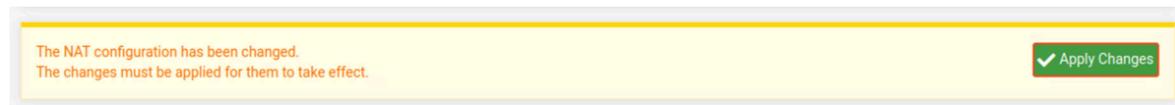
- While on the *Firewall / NAT / Port / Edit* interface, make the following changes:
 - Change *Destination port range* to **SSH** for both *From port* and *To port* from the dropdown menu.

Destination port range	SSH	From port	Custom	To port	SSH	Custom
------------------------	-----	-----------	--------	---------	-----	--------

- 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.



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/tBtXJLxJyOgyr6JheGkrFVSAUoEYYubMgwCPGDhW0.
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 Sun 01 Aug 2021 11:30:02 PM UTC

System load: 0.07      Processes:            309
Usage of /: 60.3% of 19.56GB  Users logged in:        1
Memory usage: 29%
Swap usage:  0%          IPv4 address for docker0: 172.17.0.1
                           IPv4 address for ens160: 172.16.1.10

0 updates can be applied immediately.

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

Last login: Sun Aug  1 23:28:44 2021 from 203.0.113.2
sysadmin@ubuntusrv:~$
```

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

```
sysadmin@ubuntusrv:~$ 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
        ether fe80::2e0:5bff:fe16:10 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
```

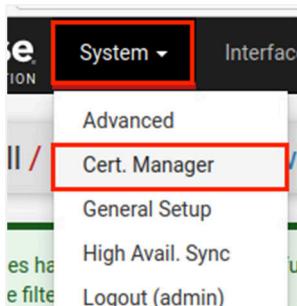
4. Type the command **route** to examine the *default gateway*.

```
sysadmin@ubuntusrv:~$ 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
```

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 Authority Manager* page, while on the **CAs** tab, click on the **+Add** button.

A screenshot of the 'System / Certificate Manager / CAs' page. The 'CAs' tab is selected, indicated by an orange border. The page includes a search bar with fields for 'Search term' and 'Both'. Below the search bar is a table titled 'Certificate Authorities' with columns: Name, Internal, Issuer, Certificates, Distinguished Name, In Use, and Actions. A red box highlights the '+ Add' button in the 'Actions' column of the first row.

4. A new page should open; fill in the necessary fields.

- a. *Descriptive Name:* MyCA

<u>Descriptive name</u>	MyCA
-------------------------	------

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

<u>Method</u>	Create an internal Certificate Authority
---------------	--

- c. *Key Length:* 2048 bits

2048
The length to use when generating a new RSA key, in bits.

- d. *Lifetime:* 365 days

<u>Lifetime (days)</u>	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** button.

CA	Certificates	Certificate Revocation										
Search Search term <input type="text"/> Both <input type="button" value="Search"/> <input type="button" value="Clear"/> Enter a search string or *nix regular expression to search certificate names and distinguished names.												
Certificates <table border="1"> <thead> <tr> <th>Name</th> <th>Issuer</th> <th>Distinguished Name</th> <th>In Use</th> <th>Actions</th> </tr> </thead> <tbody> <tr> <td>webConfigurator default (60ff3e2021791) Server Certificate CA: No Server: Yes</td> <td>self-signed</td> <td>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</td> <td></td> <td> </td> </tr> </tbody> </table>			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		
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										
<input style="border: 2px solid red; padding: 2px 10px; margin-right: 10px;" type="button" value="+"/> Add/Sign												

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

<u>Method</u>	Create an internal Certificate
---------------	---------------------------------------

7. Fill in the necessary fields.

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

<u>Descriptive name</u>	VPNServerCert
-------------------------	---------------

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

<u>Certificate authority</u>	MyCA
------------------------------	------

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

2048
The length to use when generating a new RSA key, in bits.

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

<u>Lifetime (days)</u>	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**

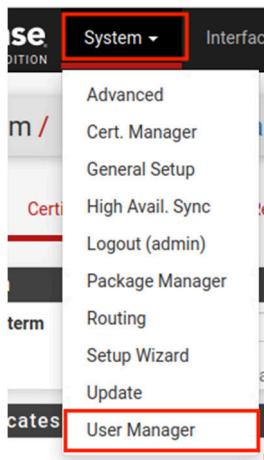
<u>Common Name</u>	pfsense.netlab.local
The following certificate subject components are optional and may be left blank.	
<u>Country Code</u>	US
<u>State or Province</u>	Texas
<u>City</u>	Austin
<u>Organization</u>	XYZ Security

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

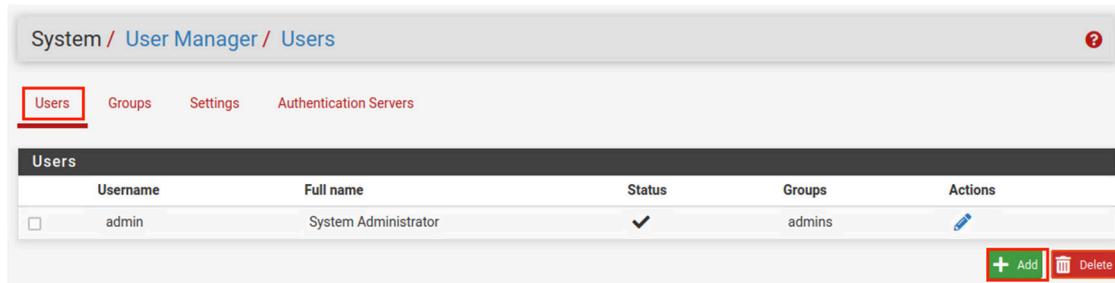
<u>Certificate Type</u>	Server Certificate
Add type specific usage at	

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.



10. Fill in the necessary fields.

a. Username: vpnuser

<u>Username</u>	vpnuser
-----------------	---------

b. Password: vpnpassword

<u>Password</u>	*****	*****
-----------------	-------	-------

c. Full name: VPN User

<u>Full name</u>	VPN User
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.

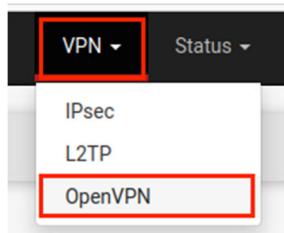
<u>Certificate</u>	<input checked="" type="checkbox"/> Click to create a user certificate
--------------------	--

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

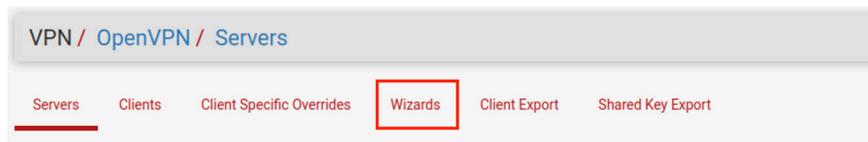
Descriptive name	VPNUser_Cert
Certificate authority	MyCA
Key type	RSA
<input type="button" value="2048"/> <small>The length to use when generating a new RSA key, in bits. The Key Length should not be lower than 2048 or some platforms may consider it too weak.</small>	
Digest Algorithm	sha256
<small>The digest method used when the certificate is signed. The best practice is to use an algorithm stronger than SHA1. Some platforms may not support stronger algorithms.</small>	
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
<small>NOTE: If unsure, leave this set to "Local User Access."</small>	

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

Choose a Certificate Authority (CA)

Certificate Authority MyCA

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

Choose a Server Certificate

Certificate VPNServerCert

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**

Interface WAN

The interface where OpenVPN...

b. *Protocol*: **UDP on IPv4 Only**

Protocol UDP on IPv4 only

c. *Local Port*: **1194**

Local Port 1194

Local port number

d. *Description*: **myVPNServer**

Description 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"/>	(Red box)
<p>Length of Diffie-Hellman (DH) key exchange parameters, used for establishing a secure connection. Larger key sizes are more secure, but also require more processing power.</p> <p>As of 2016, 2048 bit is a common and typical selection.</p>		
Data Encryption Negotiation	<input checked="" type="checkbox"/>	Enable negotiation of Data Encryption Algorithms between client and server. This is recommended.
Data Encryption Algorithms	<input type="checkbox"/> AES-256-GCM <input type="checkbox"/> AES-128-GCM <input type="checkbox"/> CHACHA20-POLY1305	
<p>List of algorithms clients can negotiate to encrypt traffic between endpoints. The choice depends on the specific hardware and performance requirements.</p> <p>Certain algorithms will perform better on different hardware, depending on the architecture and finishing the wizard for additional choices.</p>		
Fallback Data Encryption Algorithm	<input type="text" value="AES-128-CBC (128 bit key, 128 bit block)"/>	
<p>The algorithm used to encrypt traffic between endpoints when data encryption negotiation fails.</p>		
Auth Digest Algorithm	<input type="text" value="SHA256 (256-bit)"/>	
<p>The method used to authenticate traffic between endpoints. This setting must match the client configuration if authentication is desired.</p>		
Hardware Crypto	<input type="text" value="No Hardware Crypto Acceleration"/>	

f. *Tunnel Settings:*

- i. *Tunnel Network: 10.1.1.0/24*
- ii. *Redirect Gateway: Checked*
- iii. *Local Network: 192.168.0.0/28*
- iv. *Concurrent Connections: 10*
- v. *Compression: Disable Compression*

Tunnel Network	<input type="text" value="10.1.1.0/24"/>	(Red box)	
<p>This is the virtual network used for private communication. The first network address will be assigned to the server virtual interface.</p>			
Redirect Gateway	<input checked="" type="checkbox"/>	Force all client generated traffic through the tunnel.	
Local Network	<input type="text" value="192.168.0.0/24"/>	(Red box)	
<p>This is the network that will be accessible from the remote machine through the local network on the remote machine.</p>			
Concurrent Connections	<input type="text" value="10"/>	(Red box)	
<p>Specify the maximum number of clients allowed to connect simultaneously.</p>			
Allow Compression	<input type="text" value="Refuse any non-stub compression (Most secure)"/>		
<p>Allow compression to be used with this VPN instance, while maintaining security.</p>			
Compression	<input type="text" value="Disable Compression [Omit Preference]"/>		(Red box)

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



- 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**.

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

3.2 Exporting VPN Client Data

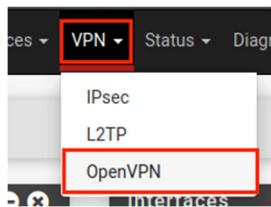
1. Switch to the **kali** machine, and start a *Firefox* browser.



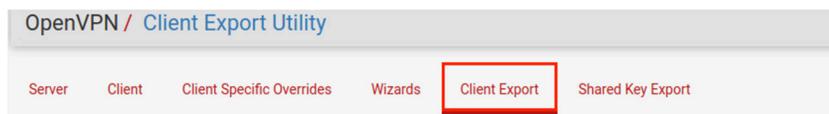
2. Go to <http://203.0.113.1> and log in as username **sysadmin** and password **NDGLabpass123!**.



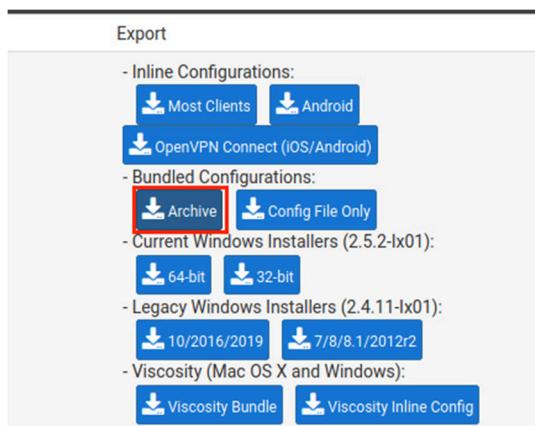
3. Under **VPN**, click to go to the **OpenVPN** page.



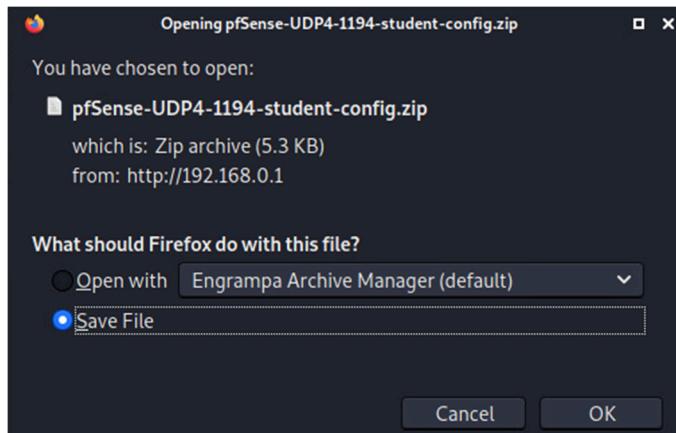
4. Click on the **Client Export** tab.



5. Scroll down towards the bottom where the *Client Install Packages* table is presented. Underneath the *Export* column, click on the **Archive** link to download the configurations.



6. A download message appears. Select **Save File** and click **OK**.



3.3 Configuring the VPN Client

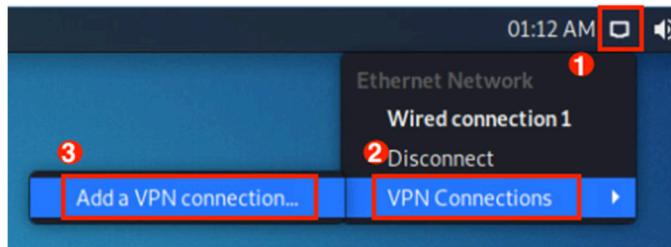
1. While on the **Kali** system, open a **terminal** and type the command below to change to the **Downloads** directory.

```
kali㉿kali$ cd ~/Downloads
```

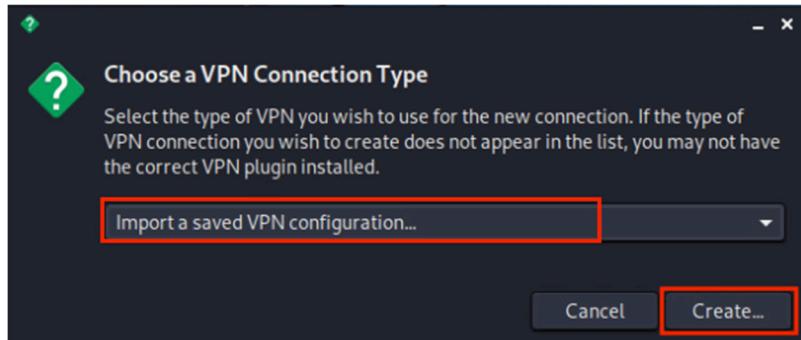
2. **Unzip** the downloaded zip file.

```
kali㉿kali$ unzip pfSense-UDP4-1194-student-config.zip
```

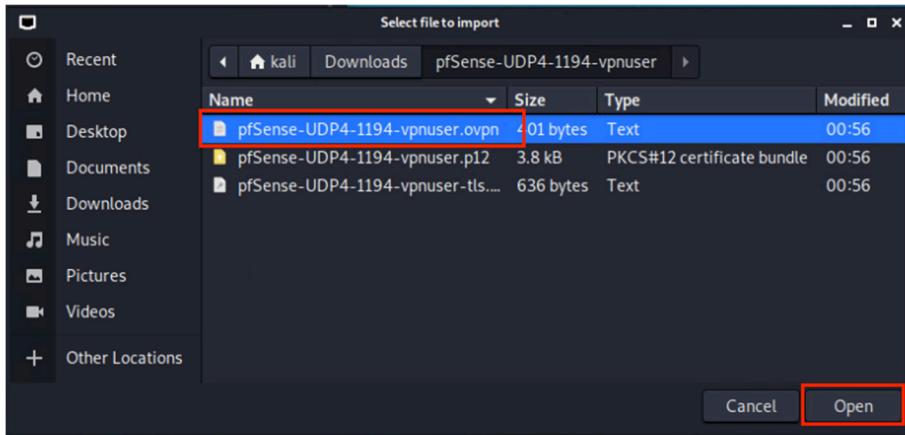
3. Open the **Network Manager** by clicking on the **network** icon located on the top pane and navigating to **VPN Connections > Add a VPN Connection...**



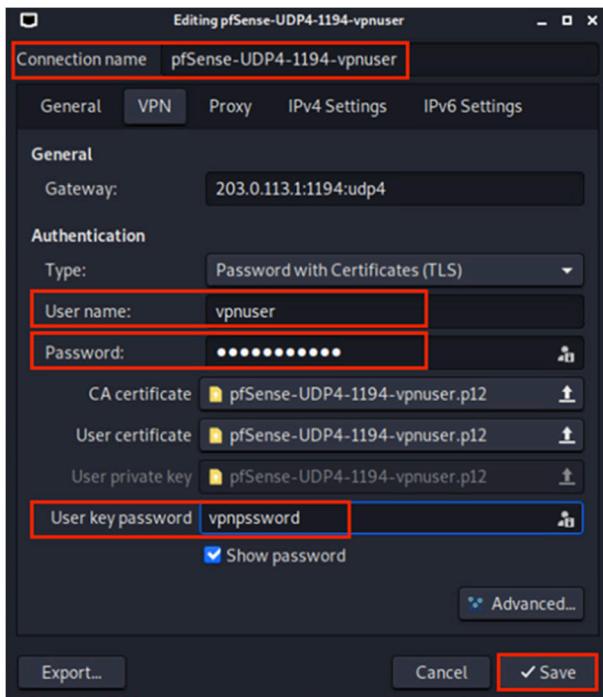
4. On the *Choose a VPN connection Type* window, select **Import a saved VPN configuration...** option and click **Create....**



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



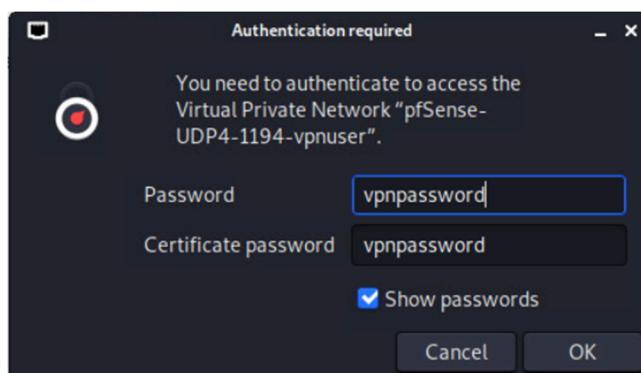
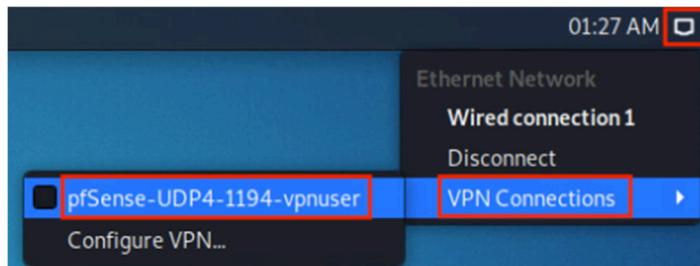
6. In the new pop-up window, leave the *Connection name* as is. Type **vpnuser** in the *User name* field, and type **vpnpassword** in the *Password* field. Then, type the **vpnpassword** again in the *User key password* field. Then, click the **Save** button.



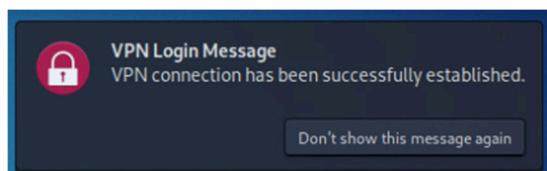
7. When prompted to create a password for the new key ring, leave the two fields empty and click **Create**. In the new window, click **Continue**.

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**.



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



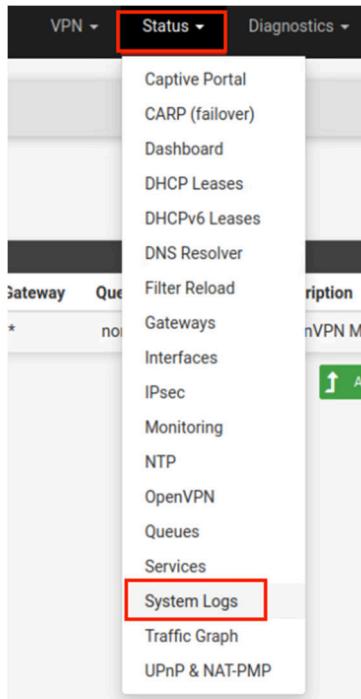
3. Verify the VPN tunnel and the IP address given by entering the command below in a *Terminal*.

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

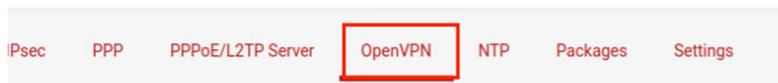
```
(kali㉿kali)-[~/Downloads]
$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
        inet6 ::1/128 scope 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

- Once connected to the **VPN server**, switch to the **UbuntuSRV**, **Firefox** web browser, and navigate back to the **pfSense Web Configurator**.
- 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 'vpnuser' authenticated
Aug 2 05:57:15	openvpn	16992	vpnuser/203.0.113.2:40404 MULTI_sva: pool returned IPv4=10.1.1.2, IPv6=(Not enabled)
Aug 2 06:09:56	openvpn	16992	vpnuser/203.0.113.2:40404 [vpnuser] 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
vpnuser	203.0.113.2:43848	10.1.1.2	2021-08-02 06:25:13	11 Kib	13 Kib	AES-256-GCM
vpnuser						X
Status: <input checked="" type="checkbox"/> Actions: C R						

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