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

Contents

Introduction

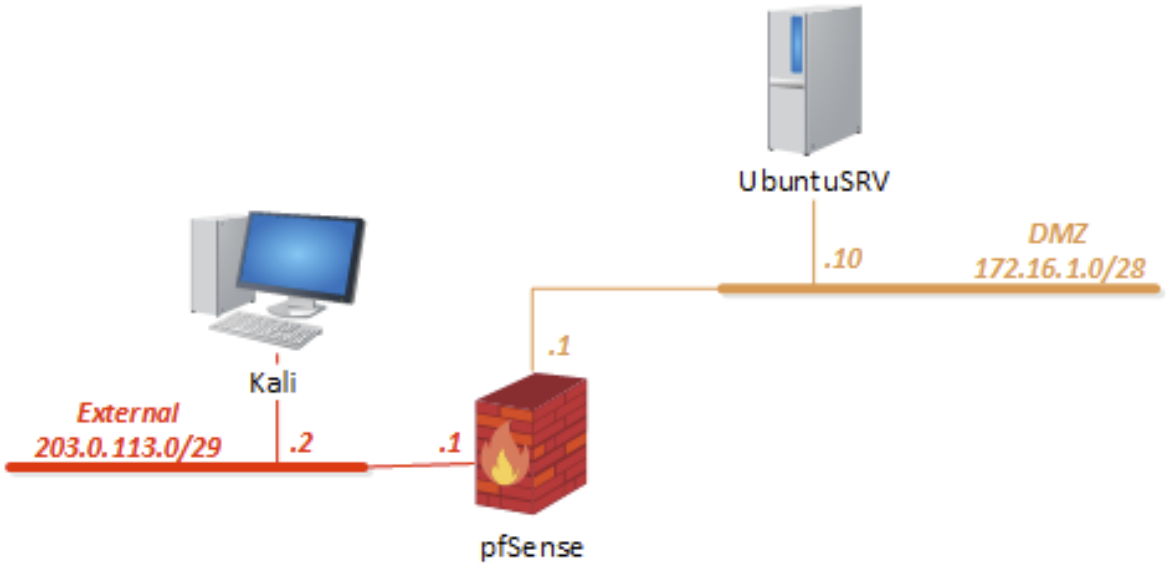
In this lab, you will be conducting network security practices using the pfSense VM.

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

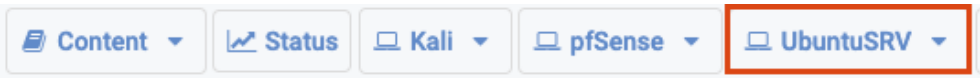
The information in the table below will be needed in order to complete the lab. The task sections below provide details on the use of this information.

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!`

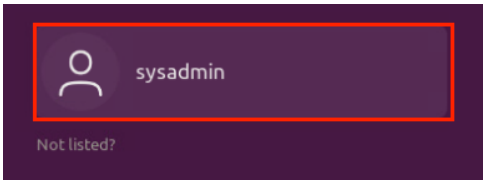
1 Configure ICMP on the Firewall

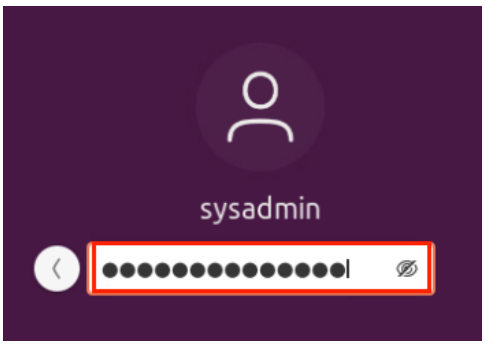
1.1 Blocking ICMP Requests on pfSense

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.

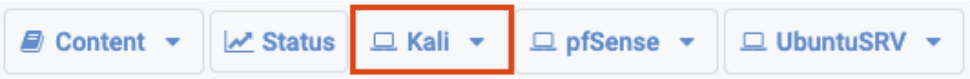
4. Send a ping request to the **Kali** system; **203.0.113.2**. Type the command below, followed by pressing the **Enter** key.

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

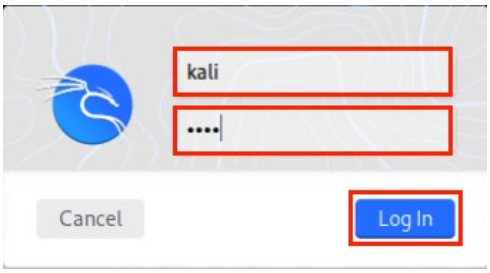
```
sysadmin@ubuntusrv:~$ ping -c4 203.0.113.2
PING 203.0.113.2 (203.0.113.2) 56(84) bytes of data.
64 bytes from 203.0.113.2: icmp_seq=1 ttl=63 time=1.10 ms
64 bytes from 203.0.113.2: icmp_seq=2 ttl=63 time=0.455 ms
64 bytes from 203.0.113.2: icmp_seq=3 ttl=63 time=0.550 ms
64 bytes from 203.0.113.2: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

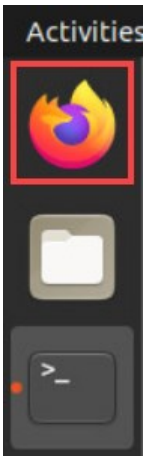
8. From the *Kali* terminal, send a ping request to the **UbuntuSRV** system: **172.16.1.10**.

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

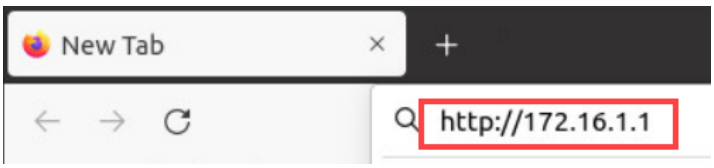
```
┌──(kali㉿kali)-[~]
└─$ ping -c4 172.16.1.10
PING 172.16.1.10 (172.16.1.10) 56(84) bytes of data.
64 bytes from 172.16.1.10: icmp_seq=1 ttl=63 time=0.568 ms
64 bytes from 172.16.1.10: icmp_seq=2 ttl=63 time=0.448 ms
64 bytes from 172.16.1.10: icmp_seq=3 ttl=63 time=0.458 ms
64 bytes from 172.16.1.10: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

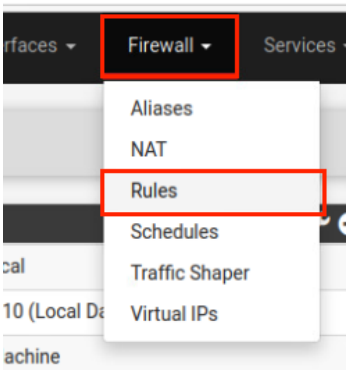


10. In the *address space*, type `http://172.16.1.1`. Press **Enter**.

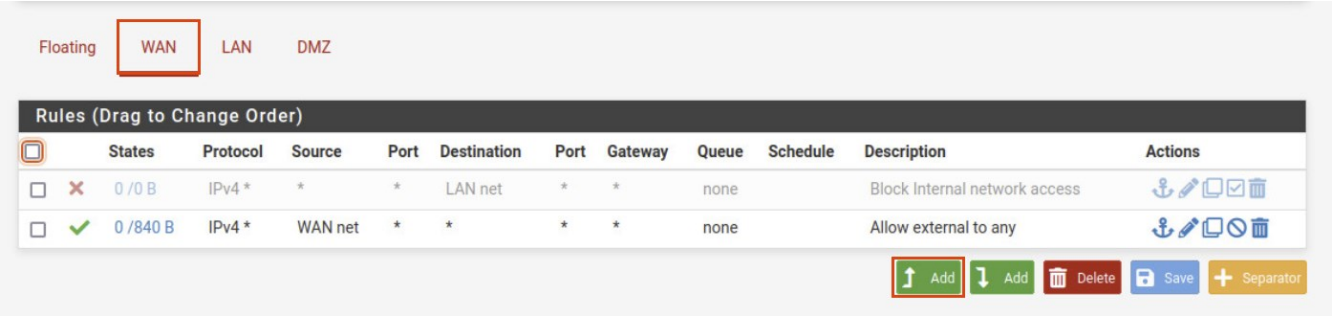


11. Type the username `sysadmin` and password `NDGlabpass123!`. Click the **SIGN IN** button.

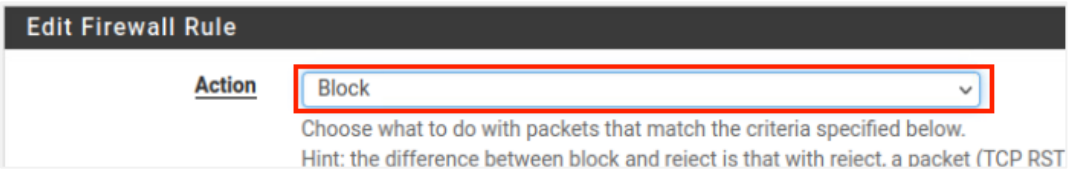
12. Once in the *pfSense* management graphical user interface, navigate to **Firewall > Rules.**



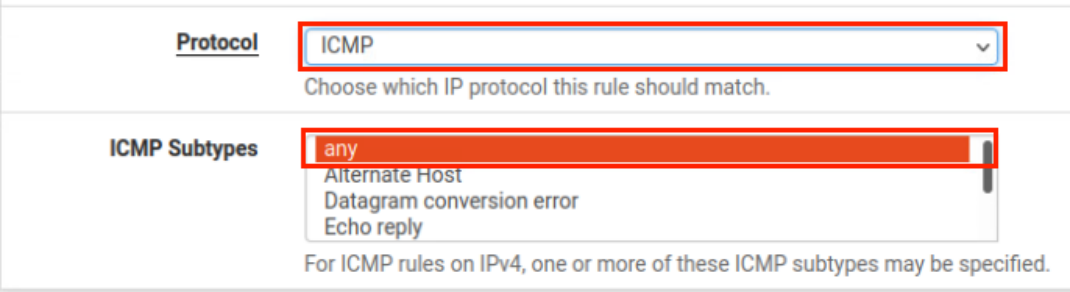
13. While viewing the *WAN* tab, click the **Add rule to the top of the list** icon on the bottom-right to add a new rule.



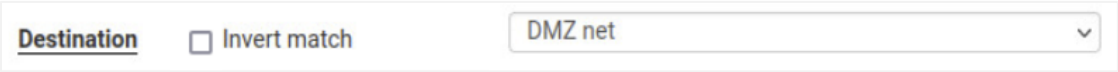
14. On the newly opened page, click the dropdown box next to *Action* and select **Block**.



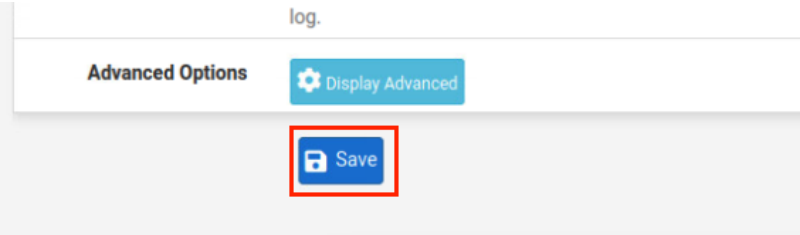
15. Select **ICMP** as the *Protocol* selection, and leave the *ICMP Subtypes* as is.



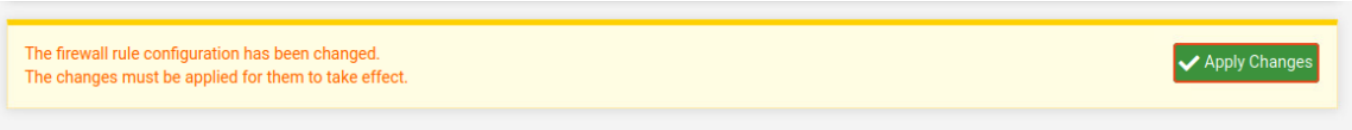
16. In the **Destination** section, set the network as the **DMZ net,** which is the **172.16.1.1/28** mask.



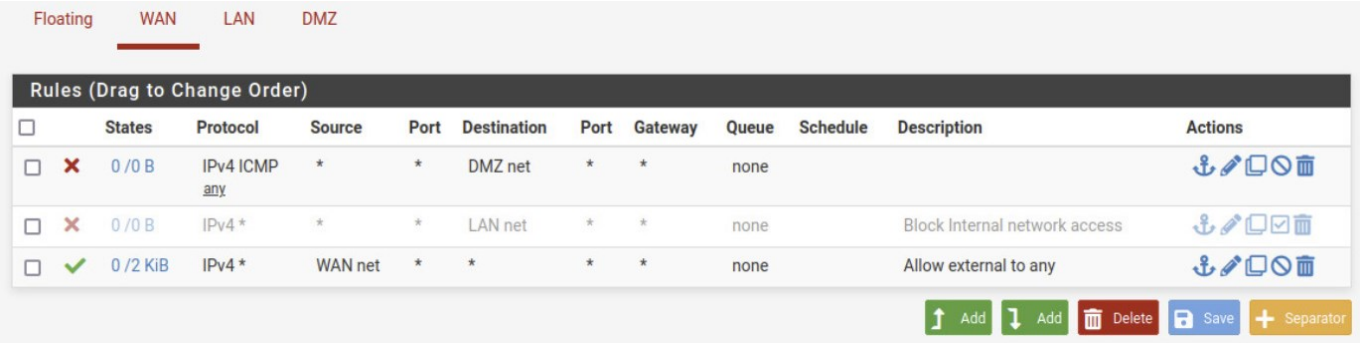
17. Leave all other options as **defaults.** Click the **Save** button located towards the bottom of the page.



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

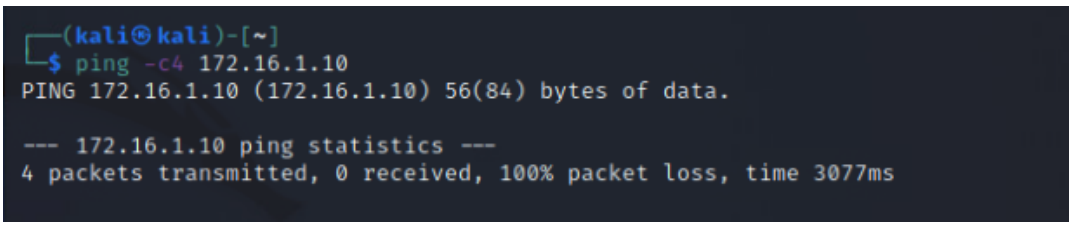


19. Verify that the firewall rules table looks like the image below for the *WAN* interface.



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
```

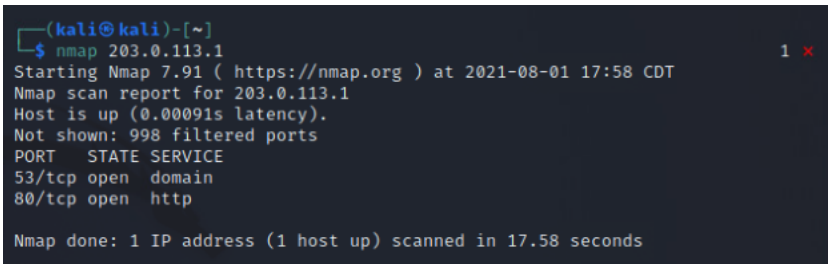


2 Redirecting Traffic to Internal Hosts on the Network

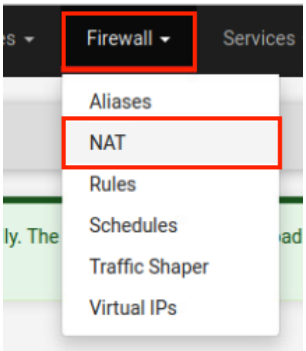
2.1 Configuring pfSense to Allow Port and Redirect Requests

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

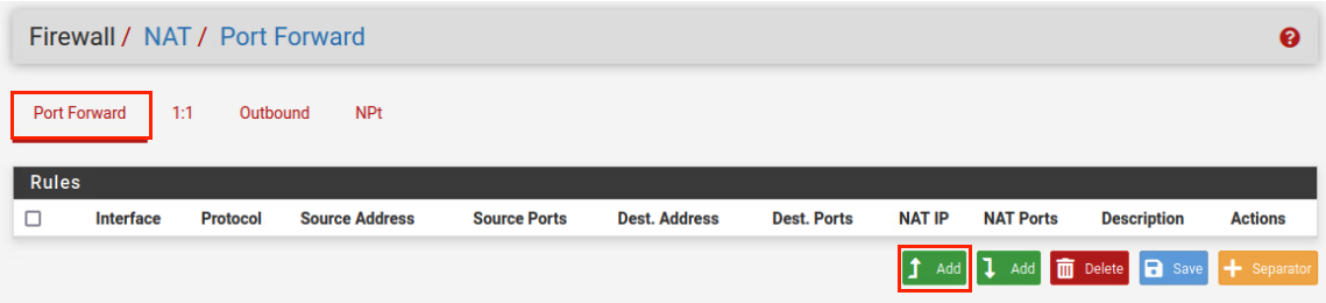
```
kali@kali$ nmap 203.0.113.1
```



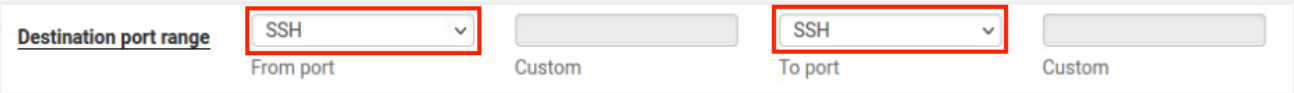
2. Change focus to the **Firefox** window on the **UbuntuSRV** system. In the *pfSense* management interface, navigate to **Firewall > NAT.**



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

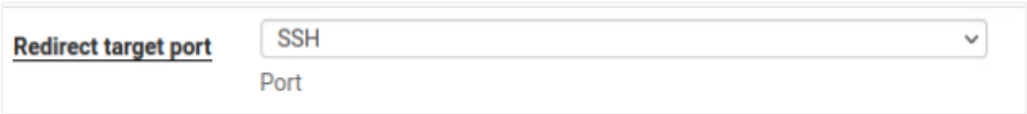


4. While on the *Firewall* / *NAT* / *Port Forward* / *Edit* interface, make the following changes:
   a. Change *Destination port range* to **SSH** for both *From port* and *To port* from the dropdown menu.

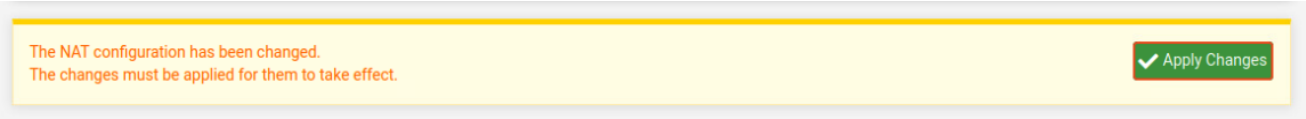


   b. Change *Redirect target IP* to `172.16.1.10`.

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



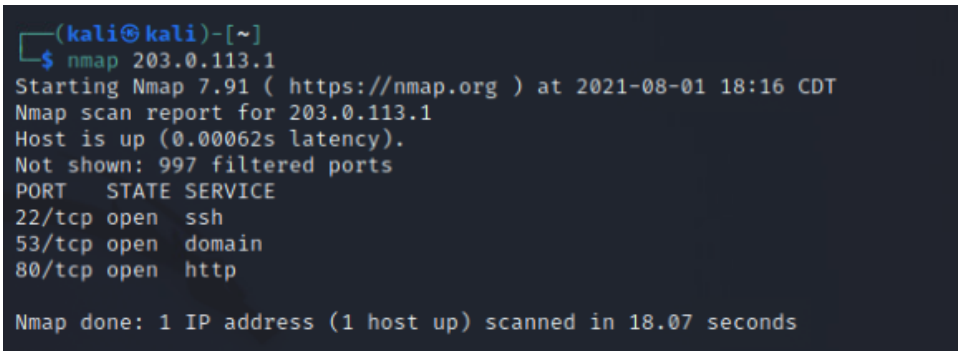
   d. Click the **Save** button located towards the bottom of the page
5. For the new configuration to take place, click the **Apply changes** button.



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
```

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
        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
```

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
```

5. Type the command `exit` to leave the active SSH connection.

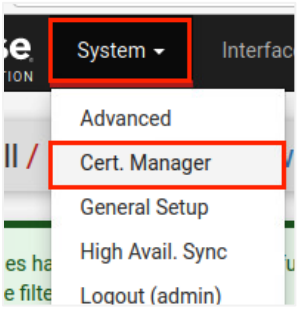
```
sysadmin@ubuntusrv:~$ exit
logout
Connection to 203.0.113.1 closed.

┌──(kali㉿kali)-[~]
└─$
```

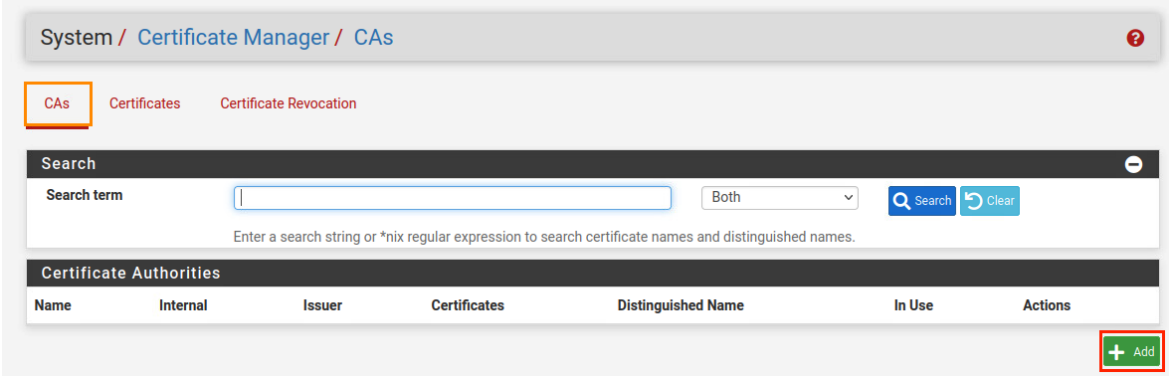
3 Configuring VPN on pfSense

3.1 Configuring VPN Server

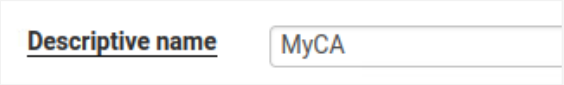
1. Change focus to the **UbuntuSRV** system and focus on the **Firefox** web browser. If you are not already logged into the *pfSense firewall management interface*, do so now.
2. While logged in, navigate to **System > Cert Manager**.



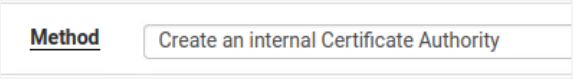
3. On the *System / Certificate Manager / CAs* page, while on the *CAs* tab, click on the **+ Add** button.



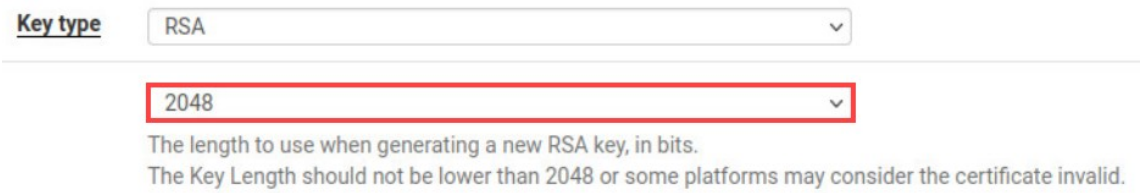
4. A new page should open; fill in the necessary fields.
   a. *Descriptive Name*: `MyCA`



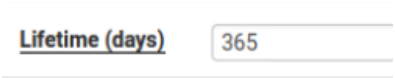
   b. *Method*: **Create an internal Certificate Authority**



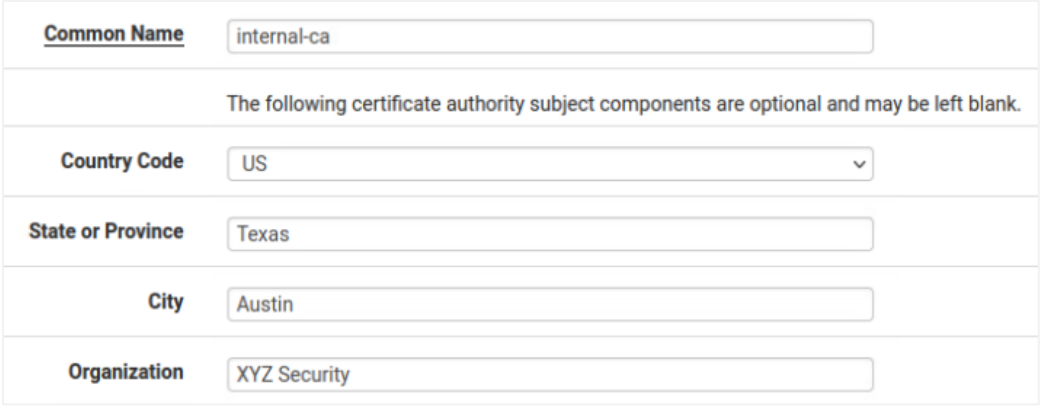
c. *Key Length*: **2048** bits



d. *Lifetime*: `365` days

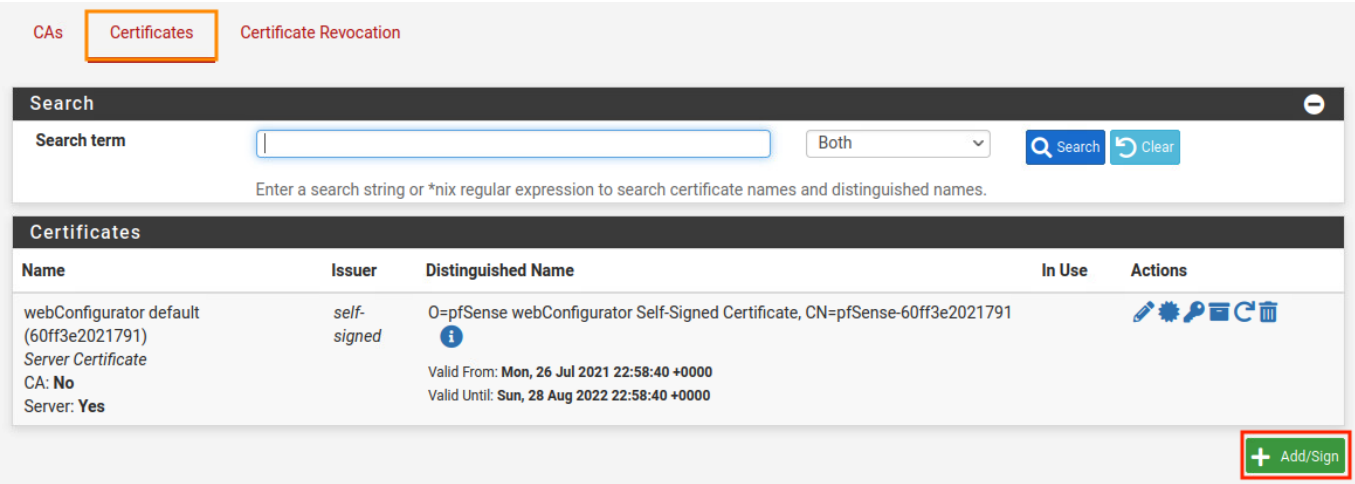


e. *Distinguished Name*:
   i. *Common Name*: `internal-ca`
   ii. *Country Code*: `US`
   iii. *State or Province*: `Texas`
   iv. *City*: `Austin`
   v. *Organization*: `XYZ Security`

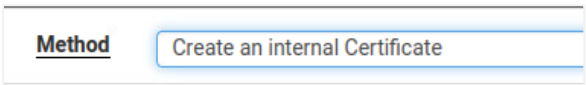


f. Click **Save**.

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

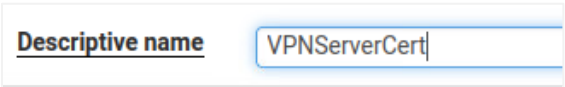


6. A new page should open; select the dropdown menu next to *Method* and select **Create an internal Certificate.**

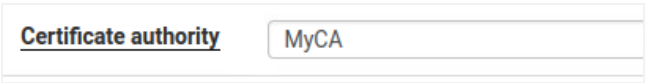


7. Fill in the necessary fields.

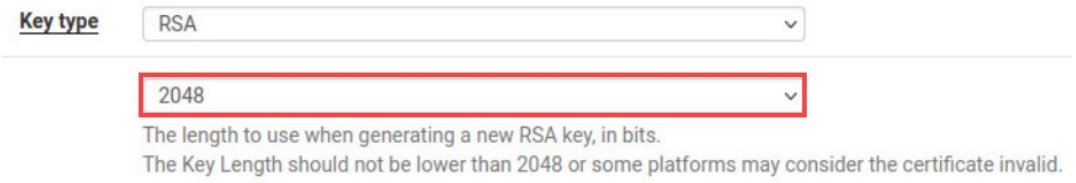
   a. *Descriptive Name*: `VPNServerCert`



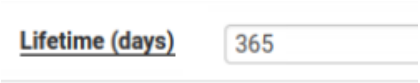
   b. *Certificate authority*: **MyCA**



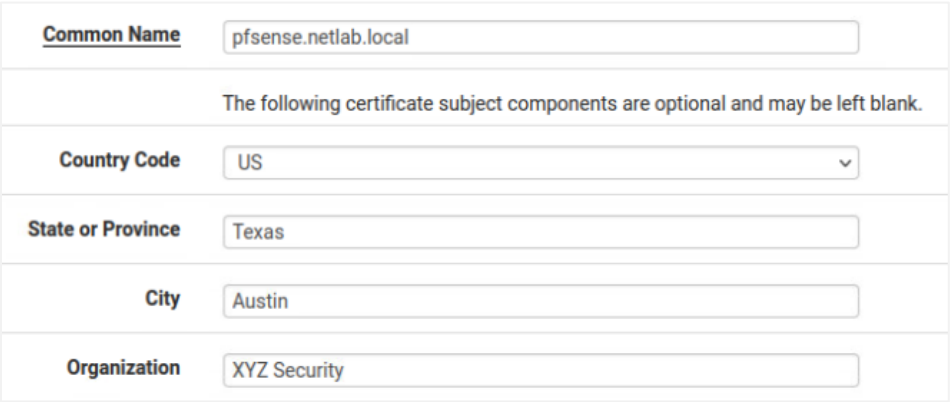
   c. *Key Length*: **2048** bits



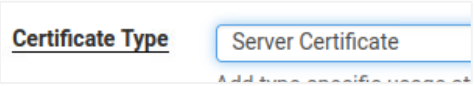
d. *Lifetime*: **365** days



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`

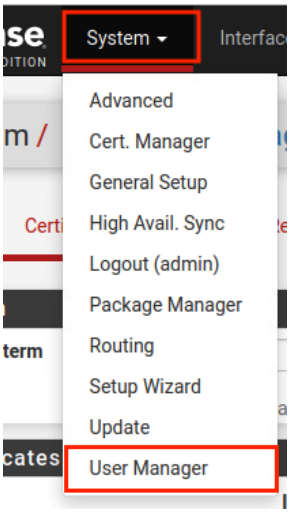


f. *Certificate Type*: **Server Certificate**

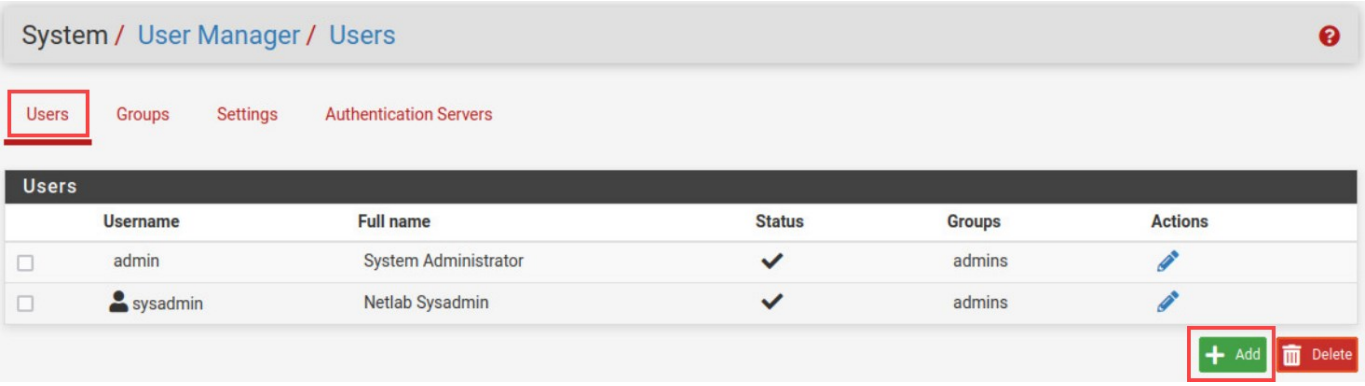


g. Click **Save**.

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

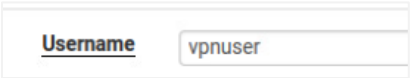


9. On the *System: User Manager* page, click the **+Add** icon to create a new user.



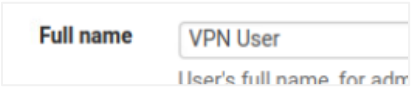
10. Fill in the necessary fields.

    a. *Username*: `vpnuser`

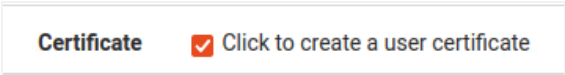


    b. *Password*: `vpnpassword`

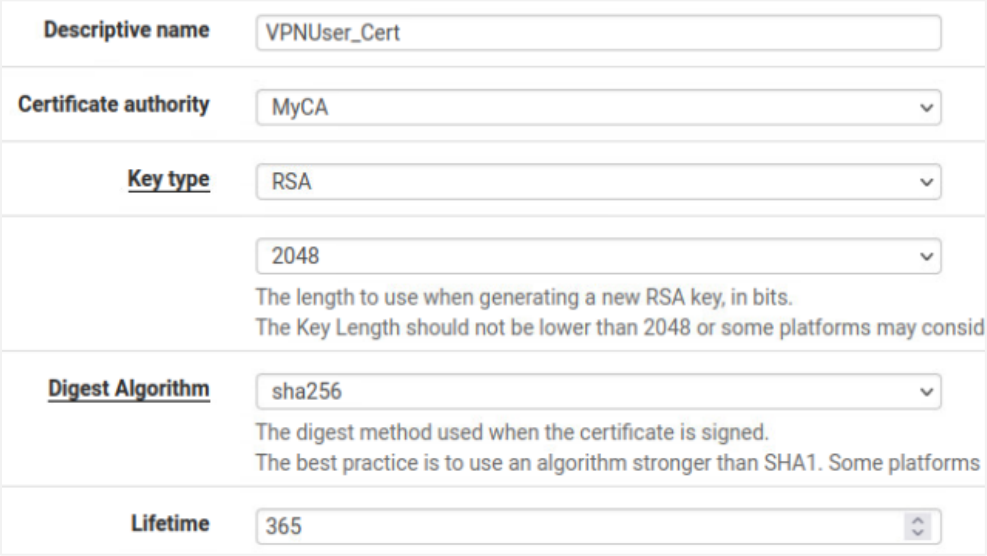
    c. *Full name*: `VPN User`



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

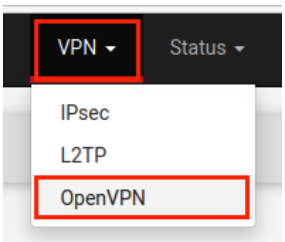


i. *Descriptive name*: `VPNUser_Cert`
ii. *Certificate Authority*: **MyCA**
iii. *Key Length*: **2048** bits
iv. *Lifetime*: **365** days

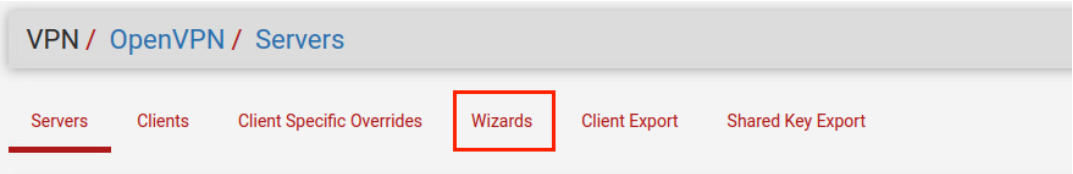


e. Click **Save**.

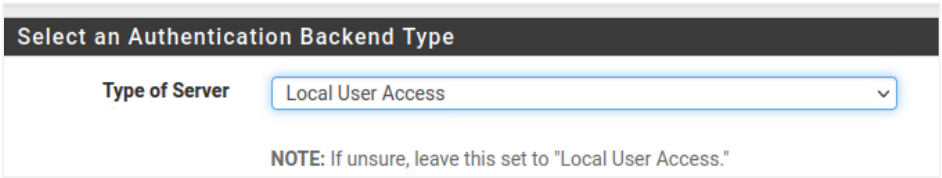
11. Navigate to **VPN > OpenVPN.**



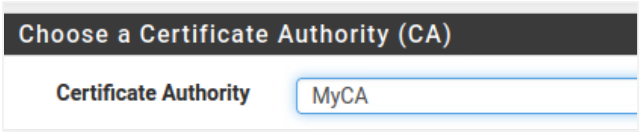
12. While on the *OpenVPN: Server* page, click on the **Wizards** tab.



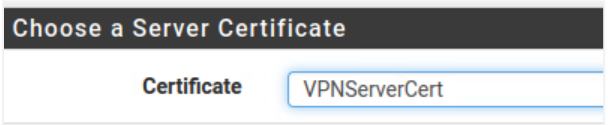
13. A new page appears; select **Local User Access** for *Type of Server*. Click **Next.**



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



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

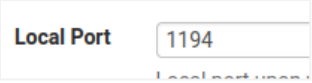


16. On the next page, fill in all necessary fields as mentioned below (if the field is not mentioned, leave its default setting):

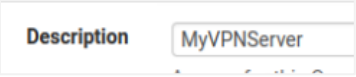
    a. *Interface*: `WAN`

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

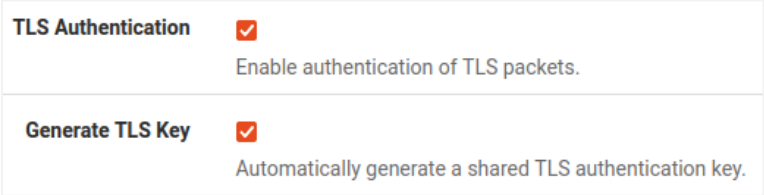
    c. *Local Port*: `1194`

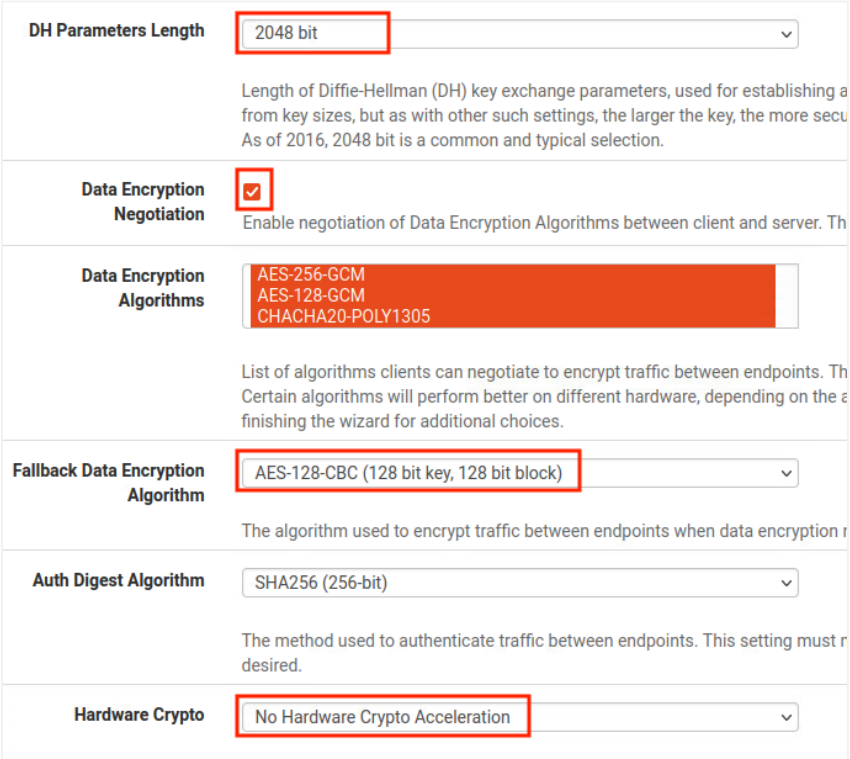


    d. *Description*: `MyVPNServer`

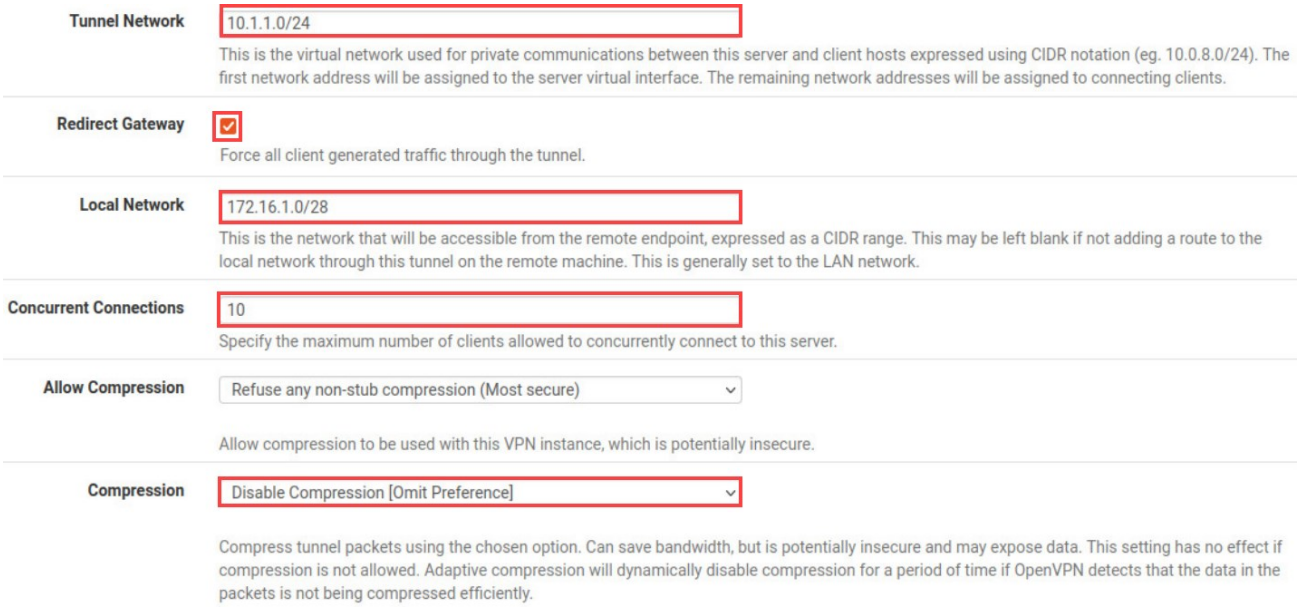


e. *Cryptographic Settings*:
   i. *TLS Authentication*: **Checked**
   ii. *Generate TLS Key*: **Checked**
   iii. *DH Parameters Length*: **2048 bit**
   iv. *Fallback Data Encryption Algorithm*: **AES-128-CBC (128-bit)**
   v. *Hardware Crypto*: **No Hardware Crypto Acceleration**



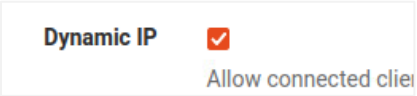


f. *Tunnel Settings*:
   i. *Tunnel Network*: `10.1.1.0/24`
   ii. *Redirect Gateway*: **Checked**
   iii. *Local Network*: `172.16.1.0/28`
   iv. *Concurrent Connections*: `10`
   v. *Compression*: **Disable Compression**



g. Client Settings:

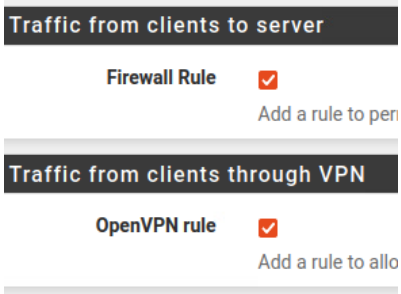
   i. *Dynamic IP*: **Checked**



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**.



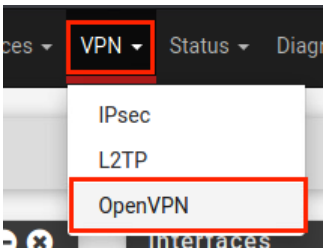
18. On the final configuration page, select **Finish.**

3.2 Exporting VPN Client Data

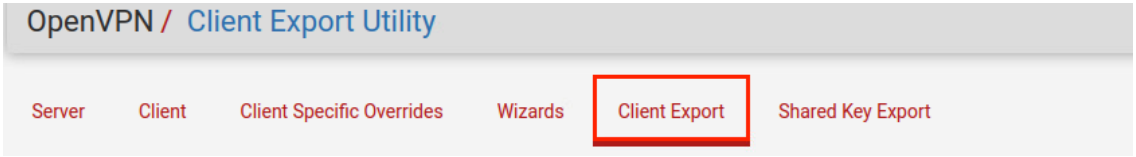
1. Switch to the **kali** machine, and start a *Firefox* browser.

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

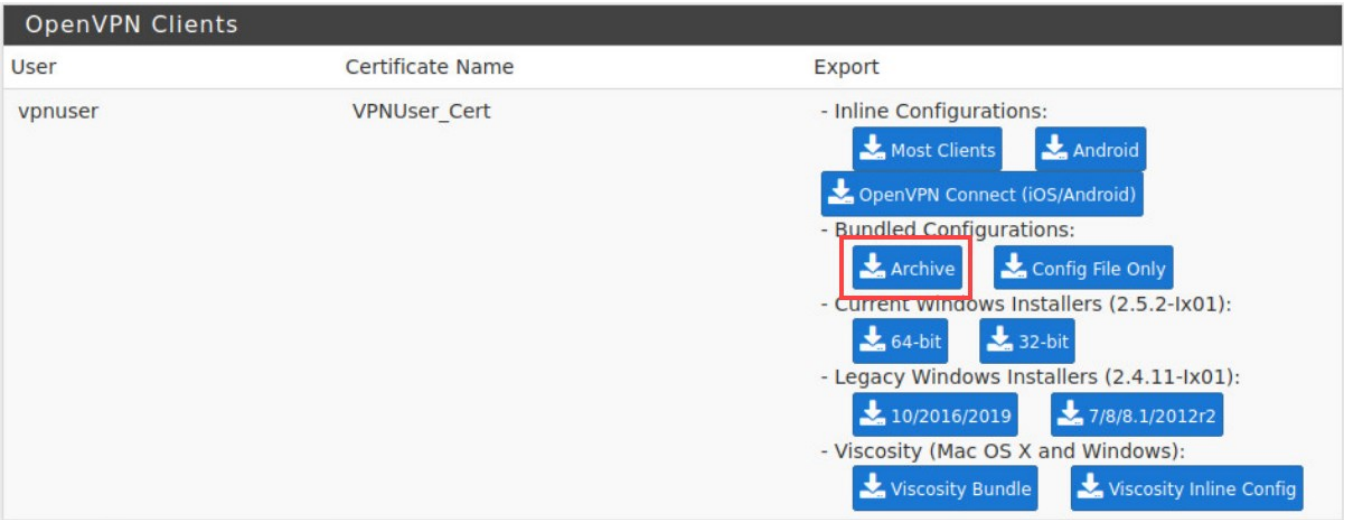
3. Under **VPN**, click to go to the **OpenVPN** page.



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



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



6. Notice that the file download is complete**.**

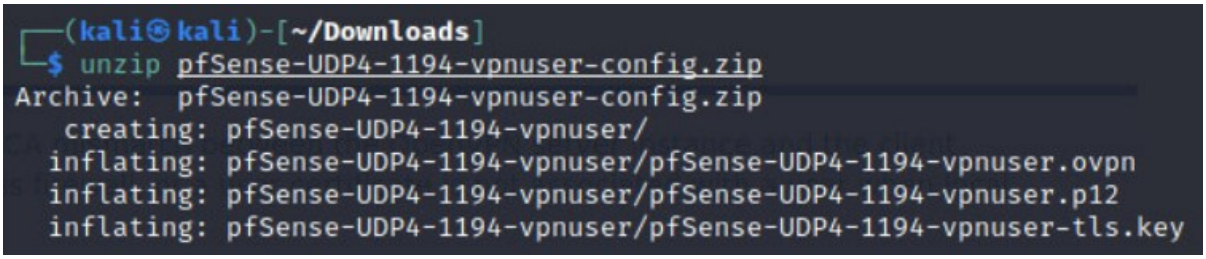
3.3 Configuring the VPN Client

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

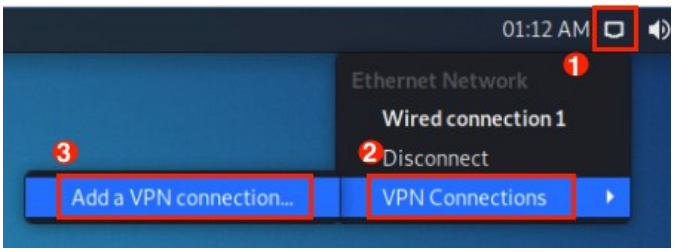
```
kali@kali$ cd ~/Downloads
```

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

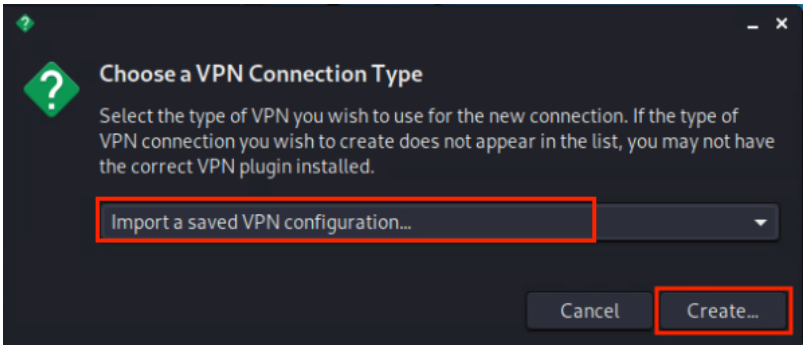
```
kali@kali$ unzip pfSense-UDP4-1194-vpnuser-config.zip
```



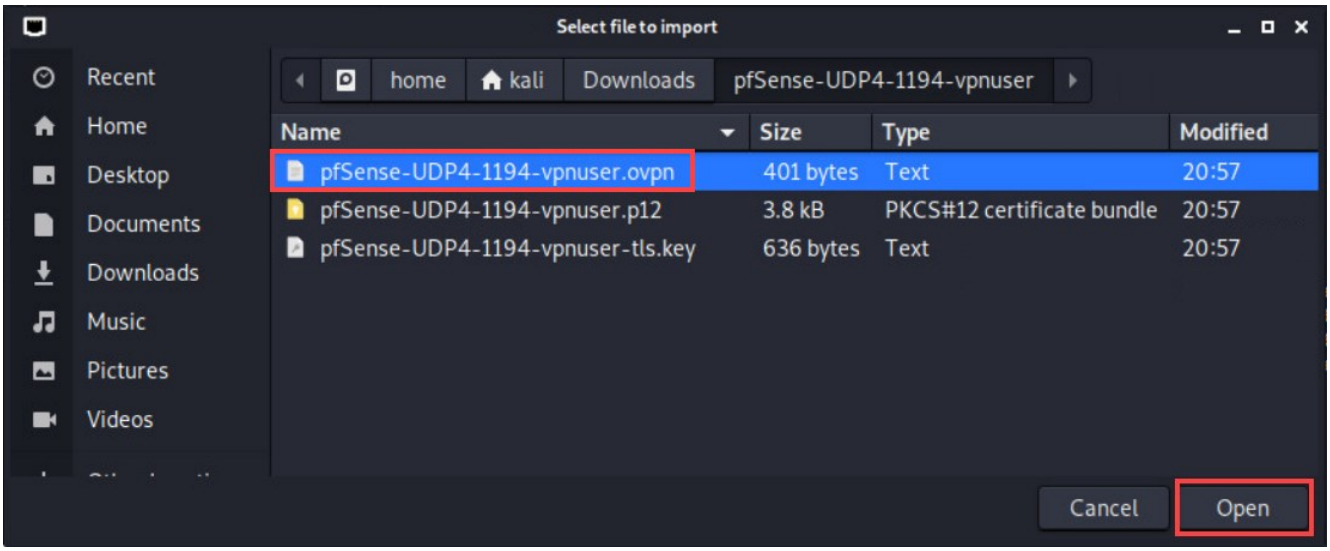
3. Open the **Network Manager** by clicking on the **network** icon located on the top pane and navigate to **VPN Connections > Add a VPN Connection**.



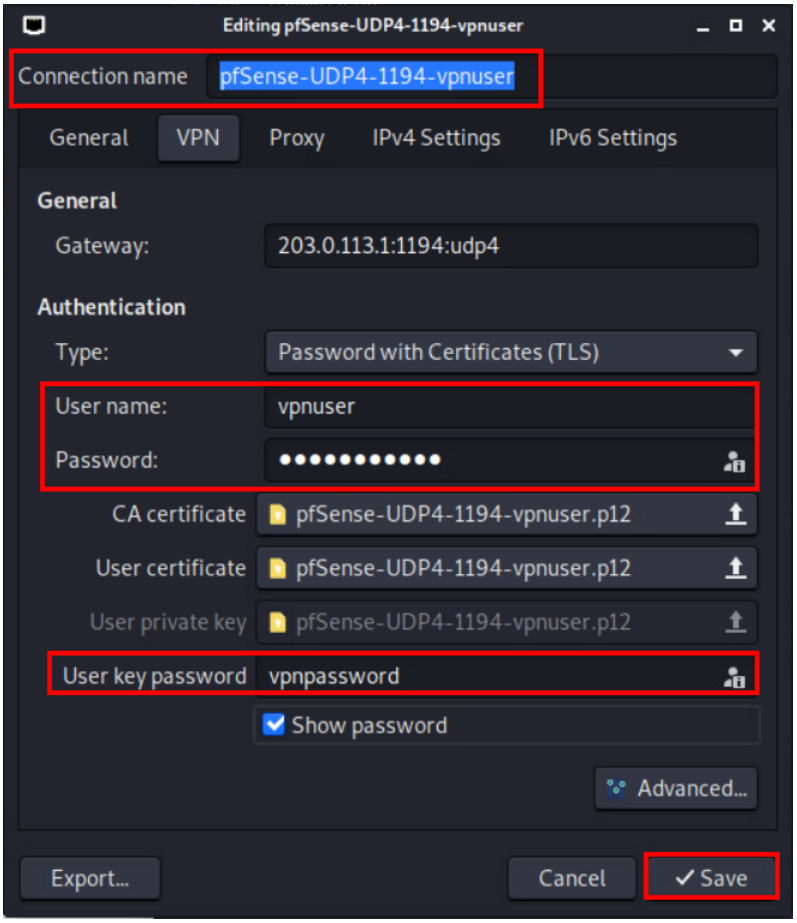
4. On the *Choose a VPN connection Type* window, select **Import a saved VPN configuration** option and click **Create**.



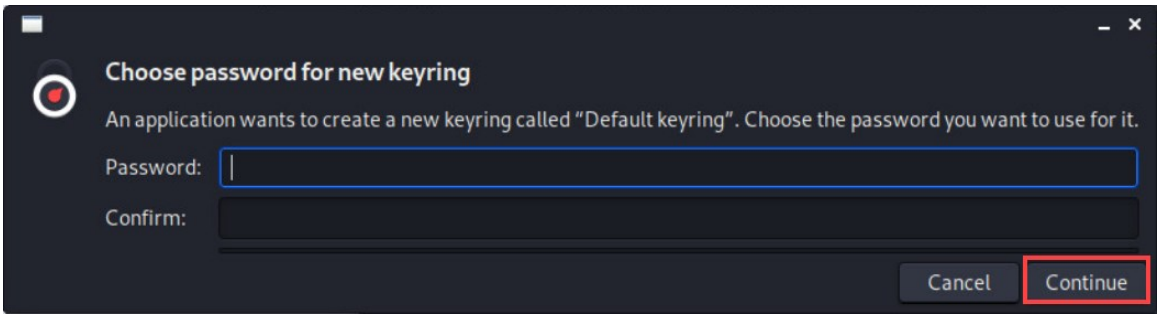
5. In the *File Manager* window, select **Downloads** from the menu on the left. Double-click on the **pfsense-udp-1194-vpnuser** folder. Select the **pfSense-UDP4-1194-vpnuser.ovpn** file and click the **Open** button.



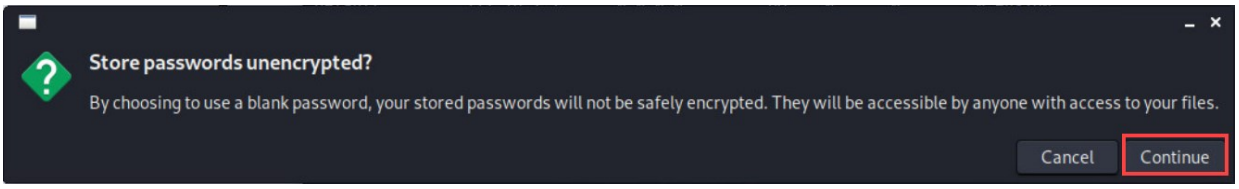
6. In the new pop-up window, leave the *Connection name* as is. Type `vpnuser` in the *User name* field, and type `vpnpassword` in the *Password* field. Then, type the `vpnpassword` again in the *User key password* field. Then, click the **Save** button.



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

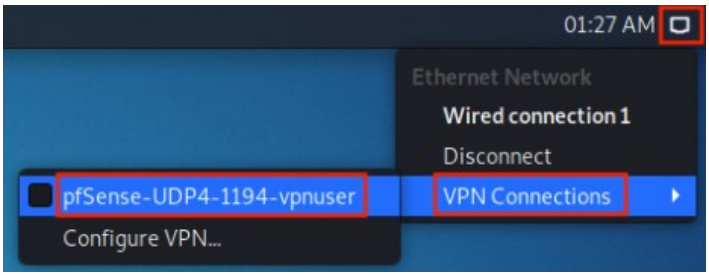


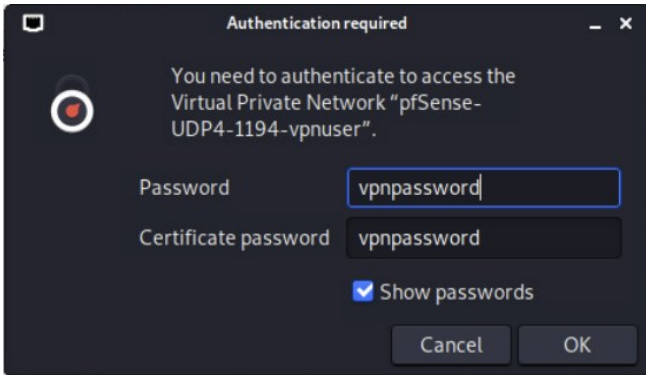
8. If prompted to store passwords unencrypted, click **Continue**.



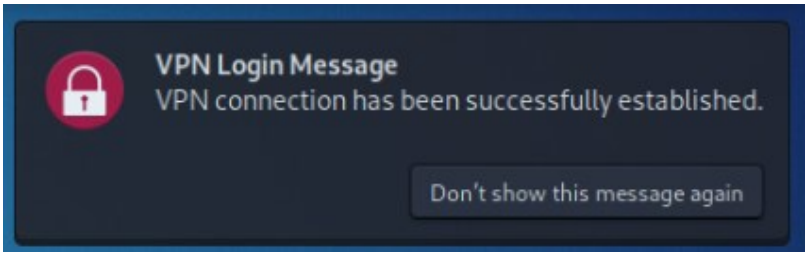
3.4 Connecting the VPN Client

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:



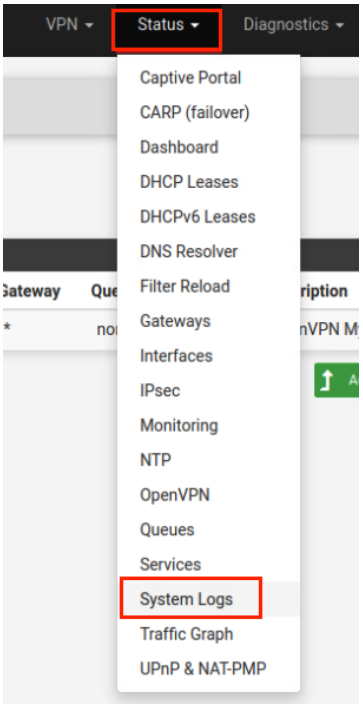
3. Verify the *VPN* tunnel and the IP address given by entering the command below in a *Terminal.*

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

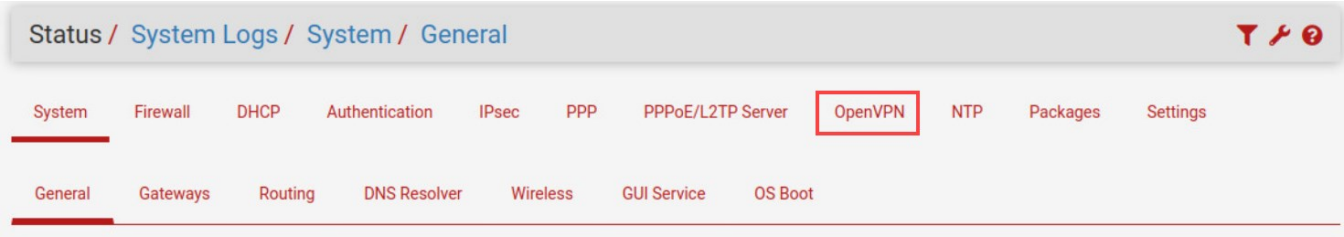
```
┌──(kali㉿kali)-[~/Downloads]
└─$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group def
ault qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope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



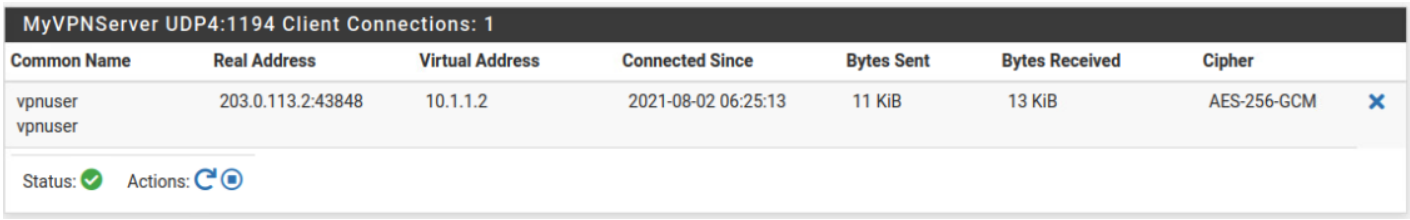
3. On the new page, select the **OpenVPN** tab.



4. 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

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



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