Security+ Lab Series

Lab 11: Configuring a Network Based Firewall

Document Version: 2020-12-10

Contents

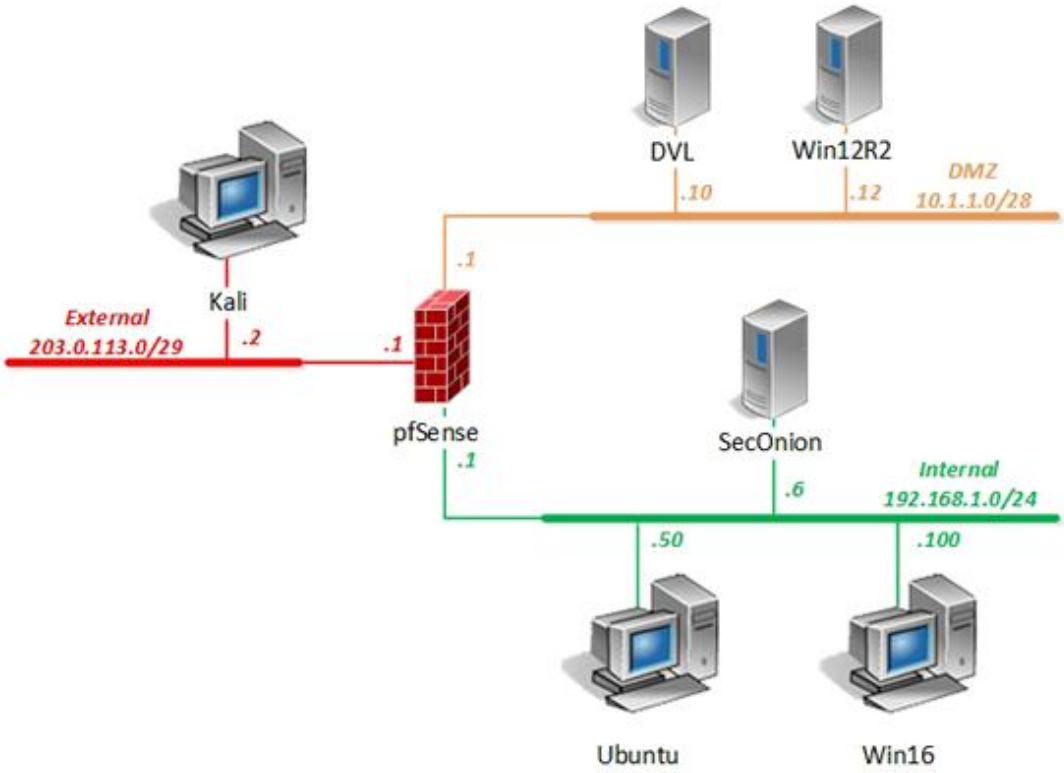
Introduction

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

Objectives

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

Lab Topology



Lab Settings

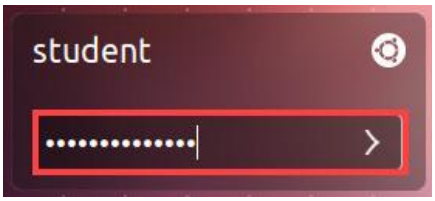
The information in the table below will be needed to complete the lab. The task sections below provide details on the use of this information.

Virtual Machine	IP Address	Account	Password
DVL	10.1.1.10 /28	root	toor
Kali	203.0.113.2 /29	root	toor
pfSense	eth0: 192.168.1.1 /24 eth1: 10.1.1.1 /28 eth2: 203.0.113.1 /29	admin	pfsense
SecOnion	eth0: 192.168.1.6 /24	soadmin	mypassword
		root	mypassword
Ubuntu	192.168.1.50 /24	student	securepassword
		root	securepassword
Win12R2	10.1.1.12 /28	administrator	Train1ng$
Win16	192.168.1.100 /24	lab-user	Train1ng$
		Administrator	Train1ng$

1 Configuring ICMP on the Firewall

1.1 Blocking ICMP Requests on pfSense

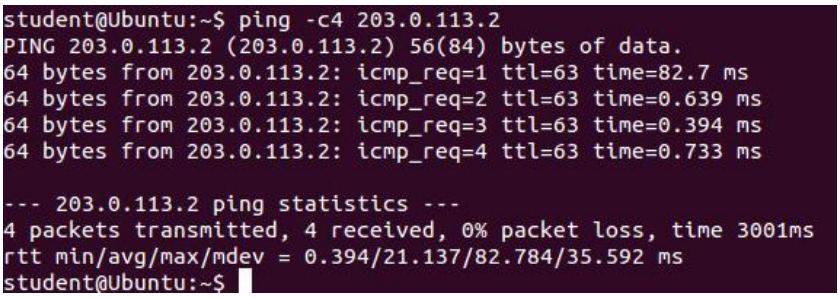
1. Launch the **Ubuntu** virtual machine to access the graphical login screen.
2. Log in as **`student`** with **`securepassword`** as the password.



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.

```
student@Ubuntu:~$ ping -c4 203.0.113.2
```



```
student@Ubuntu:~$ 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_req=1 ttl=63 time=82.7 ms
64 bytes from 203.0.113.2: icmp_req=2 ttl=63 time=0.639 ms
64 bytes from 203.0.113.2: icmp_req=3 ttl=63 time=0.394 ms
64 bytes from 203.0.113.2: icmp_req=4 ttl=63 time=0.733 ms

--- 203.0.113.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3001ms
rtt min/avg/max/mdev = 0.394/21.137/82.784/35.592 ms
student@Ubuntu:~$
```

5. After a successful ping, launch the **Kali** virtual machine to access the graphical login screen.
6. Log in as **`root`** with **`toor`** 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 **Ubuntu** system; **192.168.1.50**.

```
root@Kali-Attacker:~# ping -c4 192.168.1.50
```

```
root@Kali-Attacker:~# ping -c4 192.168.1.50
PING 192.168.1.50 (192.168.1.50) 56(84) bytes of data.
64 bytes from 192.168.1.50: icmp_req=1 ttl=63 time=0.433 ms
64 bytes from 192.168.1.50: icmp_req=2 ttl=63 time=0.507 ms
64 bytes from 192.168.1.50: icmp_req=3 ttl=63 time=0.725 ms
64 bytes from 192.168.1.50: icmp_req=4 ttl=63 time=0.535 ms

--- 192.168.1.50 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2998ms
rtt min/avg/max/mdev = 0.433/0.550/0.725/0.107 ms
root@Kali-Attacker:~#
```

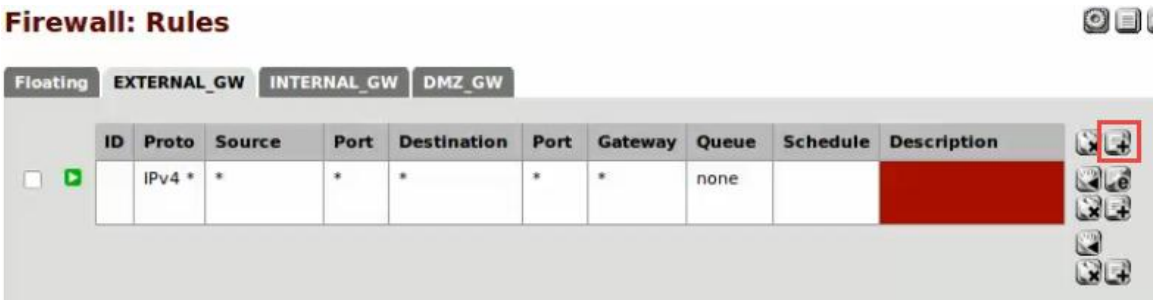
9. After the successful ping, change focus to the **Ubuntu** system and open the **Firefox** web browser.

10. In the *address space*, type **`http://192.168.1.1`**. Press **Enter**.

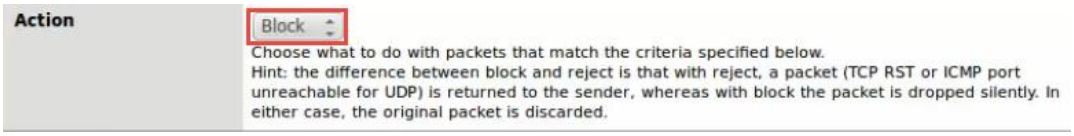
11. Type the username **`admin`** and password **`pfsense`**. Click the **Login** button.

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

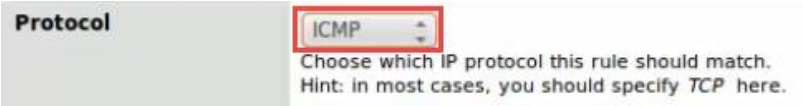
13. While viewing the **EXTERNAL_GW** tab, click the **+** icon on the top right to add a new rule.



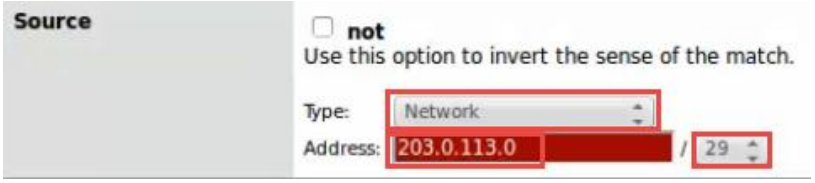
14. Click the drop-down box next to *Action* and select **Block**.



15. Select **ICMP** as the *Protocol* selection.



16. Select **Network** as the *Source Type* and enter **203.0.113.0** in the address space along with a **/29** mask.



17. Leave all other options as **defaults**.
18. Click the **Save** button located towards the bottom of the page.
19. When brought back to the *Firewall: Rules* page, notice the warning message. Select **Apply Changes**.

20. Select **Close** on the new warning message.

21. Verify that the firewall rules table represents exactly like the image below for the *EXTERNAL_GW* interface.

ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
	IPv4 ICMP	203.0.113.0/29	*	*	*	*	none		
	IPv4 *	*	*	*	*	*	none		

22. Change focus to the **Kali** system and navigate to the **terminal** window.

23. Attempt to **ping** the **Ubuntu** system.

```
root@Kali-Attacker:~# ping -c4 192.168.1.50
```

```
root@Kali-Attacker:~# ping -c4 192.168.1.50
PING 192.168.1.50 (192.168.1.50) 56(84) bytes of data.

--- 192.168.1.50 ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 3025ms

root@Kali-Attacker:~#
```

After 1-2 minutes, notice that 4 packets were transmitted and 0 were received, resulting in an unsuccessful ping attempt. The new firewall rule is effective.

24. Leave the *terminal* window open for the next task.

2 Redirecting Traffic to Internal Hosts on the Network

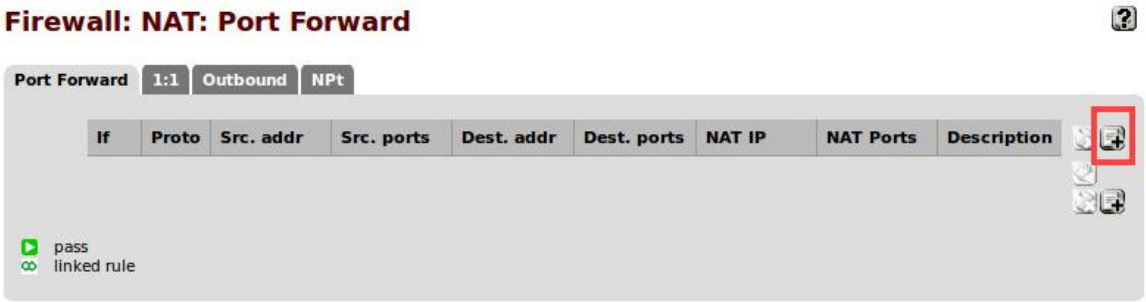
2.1 Configuring pfSense to Allow a Port and Redirect Requests

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

```
root@Kali-Attacker:~# nmap 203.0.113.1
```

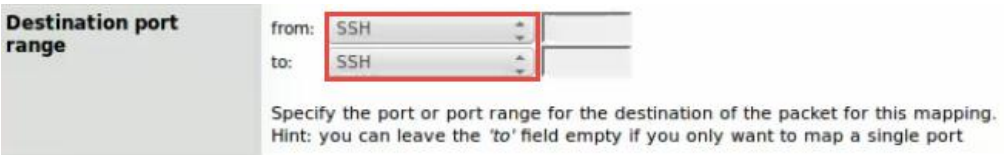
2. Change focus to the **Firefox** window on the **Ubuntu** system.
3. In the *pfSense* management interface, navigate to **Firewall > NAT**.

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



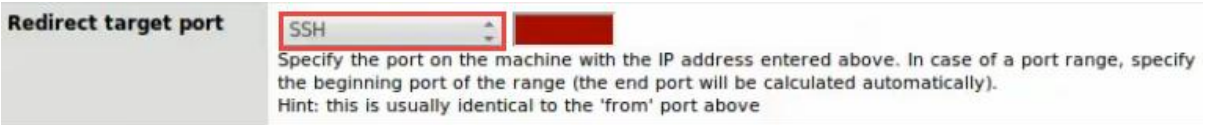
5. While on the *Firewall: NAT: Port Edit* interface, make the following changes:

   a. Change *Destination port range* to **SSH** for both "**from**" and "**to**" from the drop-down menu.



   b. Change *Redirect Target IP* to `192.168.1.50`.

   c. Change *Redirect Target Port* to **SSH** from the drop-down menu.



   d. Click the **Save** button located towards the bottom of the page.

6. For the new configuration to take place, click the **Apply changes** button.

7. When the warning message appears, click the **Close** 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.

```
root@Kali-Attacker:~# nmap 203.0.113.1
```

```
root@Kali-Attacker:~# nmap 203.0.113.1

Starting Nmap 6.47 ( http://nmap.org ) at 2018-08-02 11:07 EDT
Nmap scan report for 203.0.113.1
Host is up (0.00031s latency).
Not shown: 997 filtered ports
PORT   STATE SERVICE
22/tcp open  ssh
53/tcp open  domain
80/tcp open  http
MAC Address: 00:50:56:9C:D3:F6 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 17.72 seconds
root@Kali-Attacker:~#
```

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. If prompted for a password, enter **securepassword**.

```
root@Kali-Attacker:~# ssh 203.0.113.1
```

```
root@Kali-Attacker:~# ssh 203.0.113.1
root@203.0.113.1's password:
Welcome to Ubuntu 12.04.5 LTS (GNU/Linux 3.13.0-32-generic i686)

 * Documentation:  https://help.ubuntu.com/

0 packages can be updated.
0 updates are security updates.

New release '14.04.1 LTS' available.
Run 'do-release-upgrade' to upgrade to it.


Your Hardware Enablement Stack (HWE) is supported until April 2017.

Last login: Sun Dec 17 12:30:57 2017 from 203.0.113.2
root@Ubuntu:~#
```


3. Confirm you are on the correct system by using the following command.

```
root@Ubuntu:~# ifconfig
```

```
root@Ubuntu:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:50:56:9c:59:78
          inet addr:192.168.1.50  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::250:56ff:fe9c:5978/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1577 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2260 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:893890 (893.8 KB)  TX bytes:213373 (213.3 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:599 errors:0 dropped:0 overruns:0 frame:0
          TX packets:599 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:40710 (40.7 KB)  TX bytes:40710 (40.7 KB)

root@Ubuntu:~#
```

4. Type the command below to determine the *default gateway*.

```
root@Ubuntu:~# route
```

```
root@Ubuntu:~# route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         192.168.1.1     0.0.0.0         UG    0      0        0 eth0
link-local      *               255.255.0.0     U     1000   0        0 eth0
192.168.1.0     *               255.255.255.0   U     1      0        0 eth0
root@Ubuntu:~#
```

5. Determine what ports are accessible on the internal network when attempting to scan the firewall appliance.

```
root@Ubuntu:~# nmap 192.168.1.1
```

```
root@Ubuntu:~# nmap 192.168.1.1

Starting Nmap 5.21 ( http://nmap.org ) at 2018-08-02 11:13 EDT
Nmap scan report for 192.168.1.1
Host is up (0.00026s latency).
Not shown: 997 filtered ports
PORT     STATE SERVICE
53/tcp   open  domain
80/tcp   open  http
3128/tcp open  squid-http
MAC Address: 00:50:56:9C:3F:57 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 17.52 seconds
root@Ubuntu:~#
```


3 Configuring VPN on a pfSense

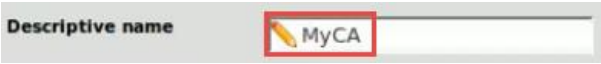
3.1 Configuring VPN Server

1. Change focus to the **Ubuntu** 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 **+** icon.

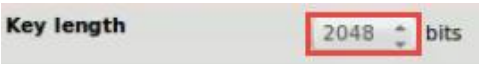
4. A new page should open; fill in the necessary fields.

   a. *Descriptive Name*: MyCA



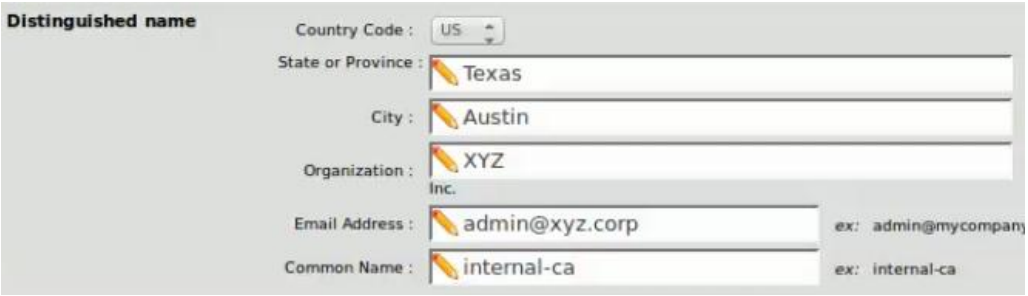
   b. *Method*: **Create an internal Certificate Authority**

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



d. *Lifetime*: **3650** days

e. *Distinguished name*:
   i. *Country Code*: **US**
   ii. *State or Province*: **Texas**
   iii. *City*: **Austin**
   iv. *Organization*: **XYZ**
   v. *Email Address*: **admin@xyz.corp**
   vi. *Common Name*: **internal-ca**



f. Click **Save**.

5. Add a server certificate this time by navigating to the **Certificates** tab.

6. To add a new certificate, click on the **+** icon.

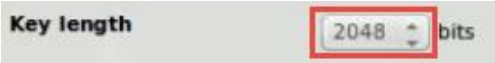
7. A new page should open; select the drop-down menu next to *Method* and select **Create an internal Certificate**.

8. Fill in the necessary fields:

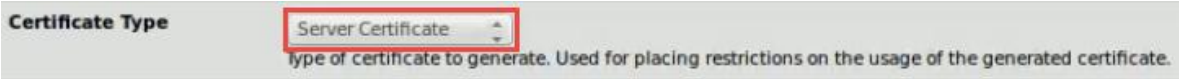
   a. *Descriptive Name*: `VPNServerCert`

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

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

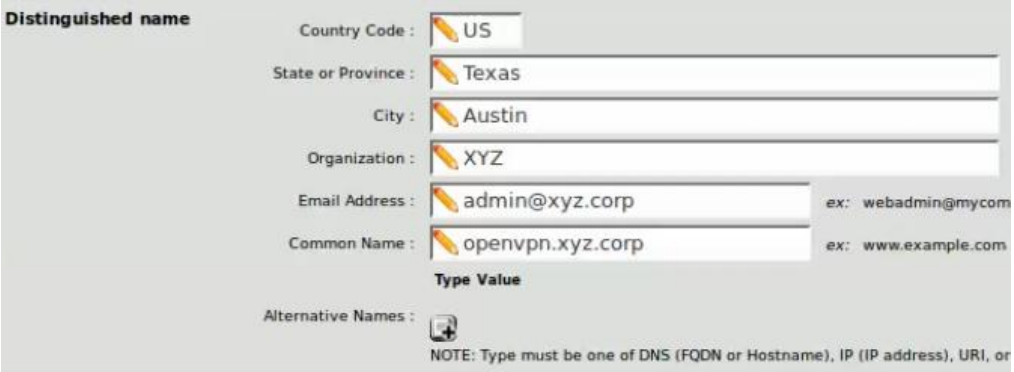


   d. *Certificate Type*: **Server Certificate**



   e. *Lifetime*: `3650` days

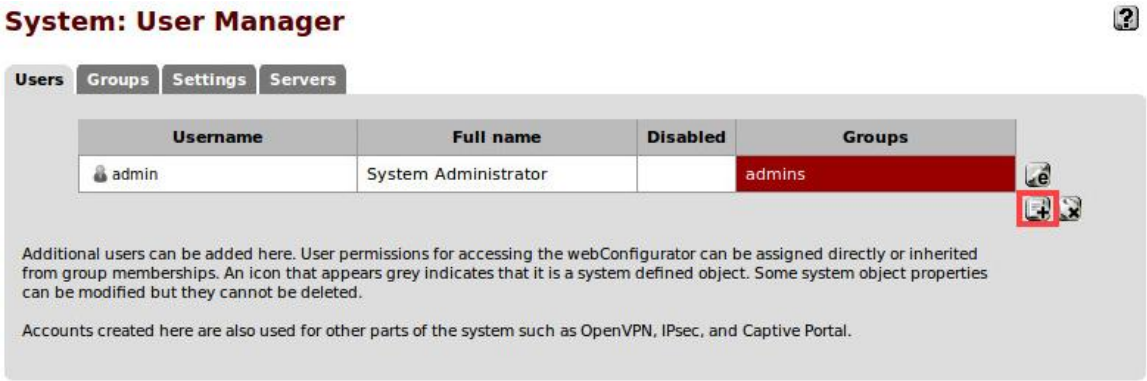
   f. Distinguished Name:
      i. *Country Code*: **US**
      ii. *State or Province*: `Texas`
      iii. *City*: `Austin`
      iv. *Organization*: `XYZ`
      v. *Email Address*: `admin@xyz.corp`
      vi. *Common Name*: `openvpn.xyz.corp`



g. Click **Save**.

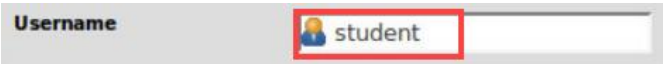
9. Navigate to **System > User Manager**.

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



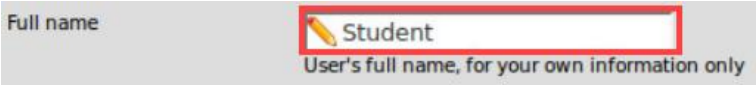
11. Fill in the necessary fields:

a. *Username*: **`student`**



b. *Password*: **bpassx**

c. *Full name*: **Student**



d. Check the box next to **Click to create a user certificate** (more options will appear):

i. *Descriptive name*: **student_cert**
ii. *Certificate Authority*: **MyCa**
iii. *Key Length*: **2048** bits
iv. *Lifetime*: **3650** days

e. Click **Save**.

12. Navigate to **VPN > OpenVPN**.

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

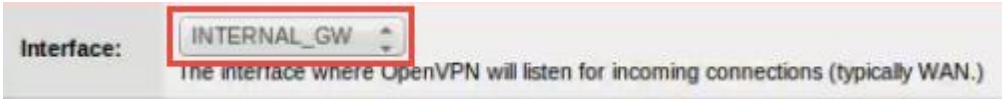
14. A new page appears; select **Local User Access** for *Type of Server*. Click **Next**.

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

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

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

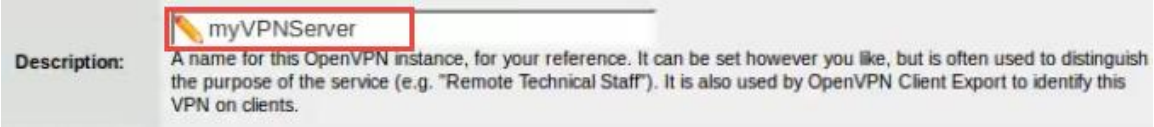
    a. *Interface*: **INTERNAL_GW**



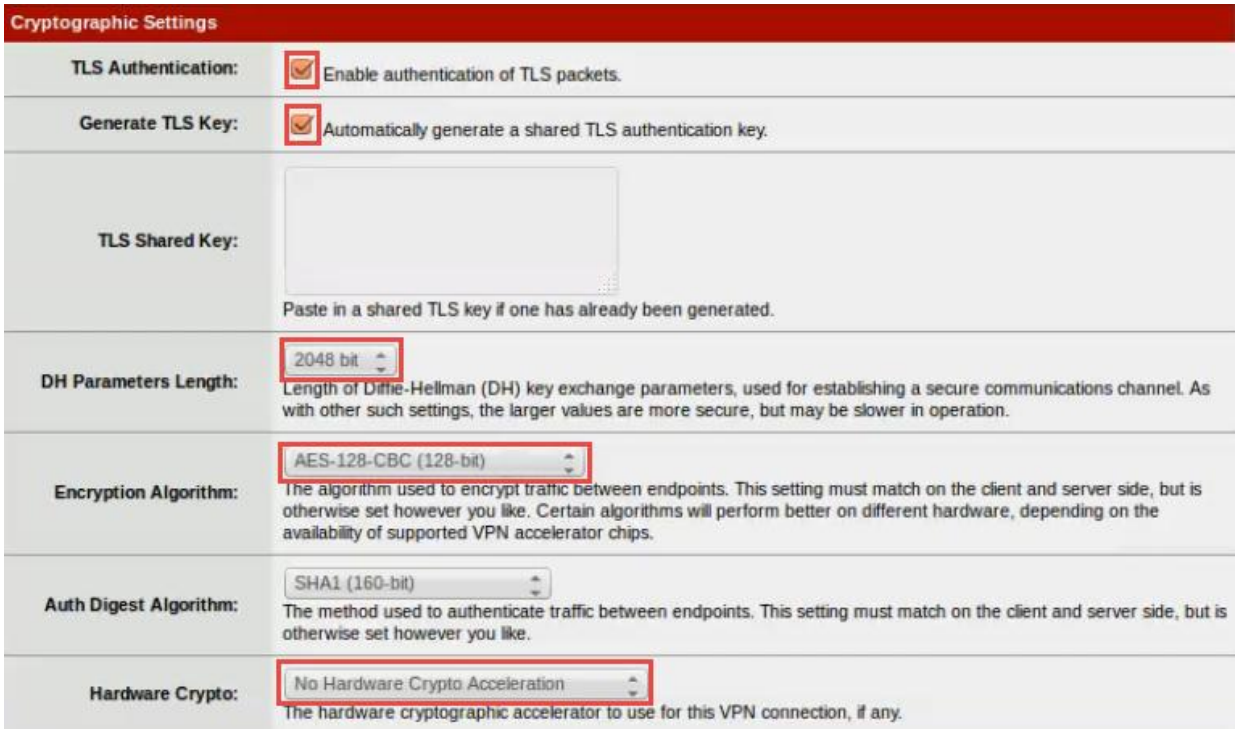
    b. *Protocol*: **UDP**

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

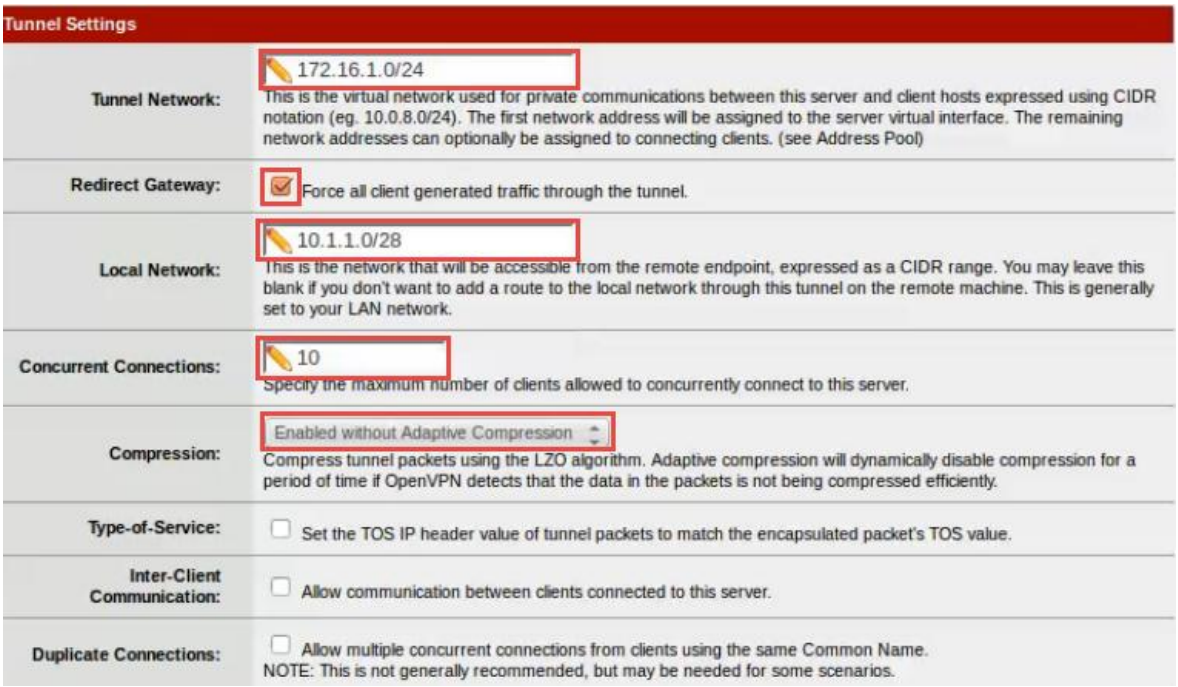
d. *Description*: **myVPNServer**



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

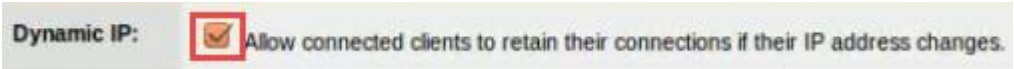


f. *Tunnel Settings*:
   i. *Tunnel Network*: **172.16.1.0/24**
   ii. *Redirect Gateway*: **Checked**
   iii. *Local Network*: **10.1.1.0/28**
   iv. *Concurrent Connections*: **10**
   v. *Compression*: **Enabled without Adaptive Compression**

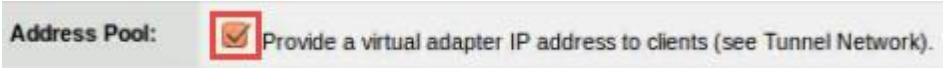


g. Client Settings:

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



ii. *Address Pool*: **Checked**



h. Click **Next**.

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

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

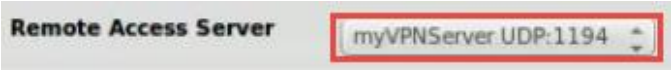
19. On the final configuration page, select **Finish**.

3.2 Exporting VPN Client Data

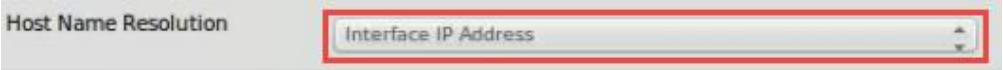
1. While logged in the *pfSense webConfigurator*, navigate to **VPN > OpenVPN** if not already.
2. Click on the **Client Export** tab.

3. Verify the configurations:

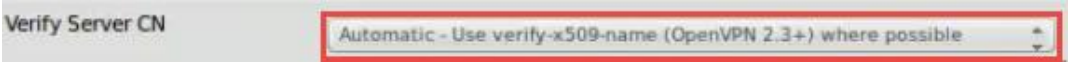
   a. *Remote Access Server*: **myVPN_Server UDP:1194**



   b. *Host Name Resolution*: **Interface IP Address**



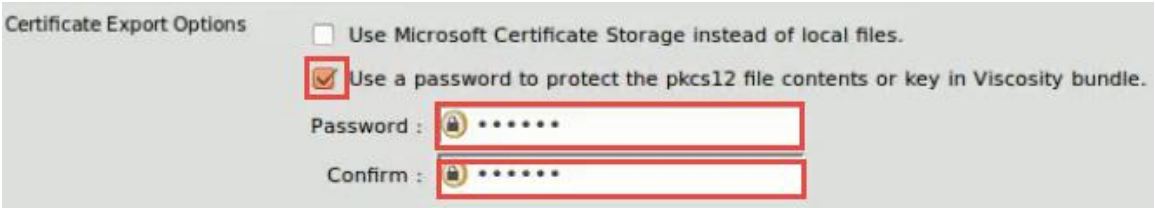
   c. *Very Server CN*: **Automatic …**



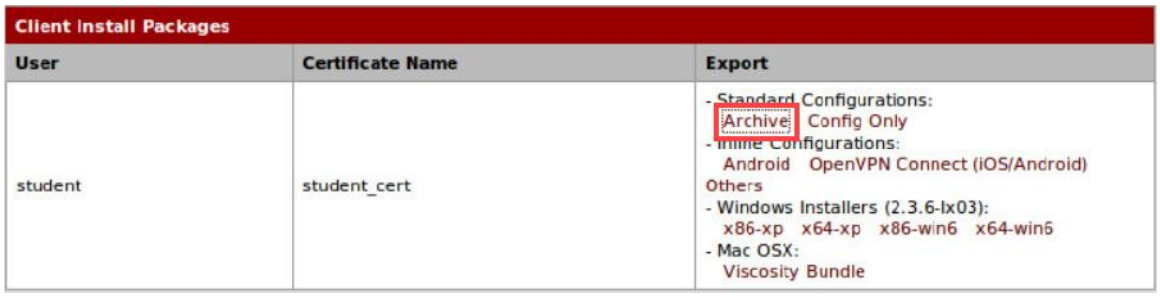
   d. U*se Random Local Port*: **Checked**

e. *Certificate Export Options*: Check the box to **Use a password to protect the pkcs12 file.**

i. Type **bpassx** in both fields.

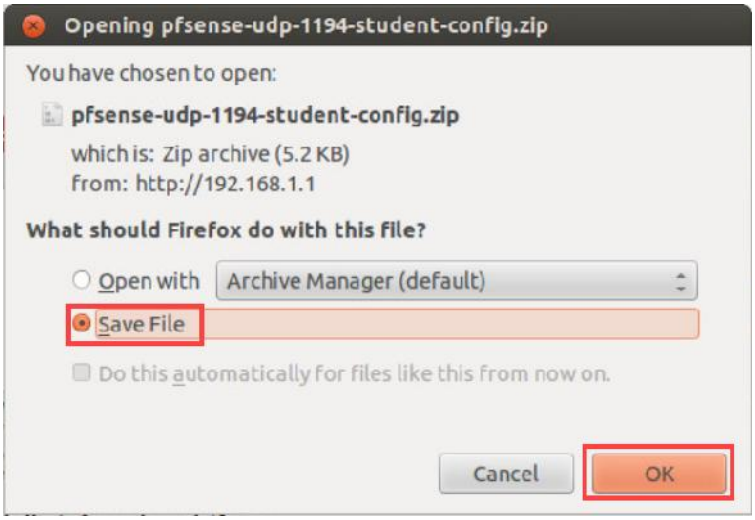


4. Scroll down towards the bottom where the *Client Install Packages* table is presented. Underneath the *Export* column, click on the **Archive** link for **Standard Configurations**.



Client Install Packages		
User	**Certificate Name**	**Export**
student	student_cert	- Standard Configurations: Archive Config Only - Inline Configurations: Android OpenVPN Connect (iOS/Android) Others - Windows Installers (2.3.6-Ix03): x86-xp x64-xp x86-win6 x64-win6 - Mac OSX: Viscosity Bundle

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



The file will be saved in the **/home/student/Downloads** directory by default.

3.3 Configuring the VPN Client

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

```
student@Ubuntu:~$ cd /home/student/Downloads
```

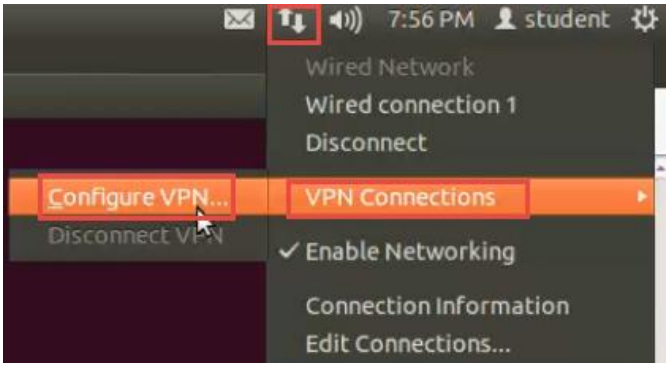
```
student@Ubuntu:~$ cd /home/student/Downloads
student@Ubuntu:~/Downloads$
```

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

```
student@Ubuntu:~/Downloads$ unzip pfsense-udp-1194-student-config.zip
```

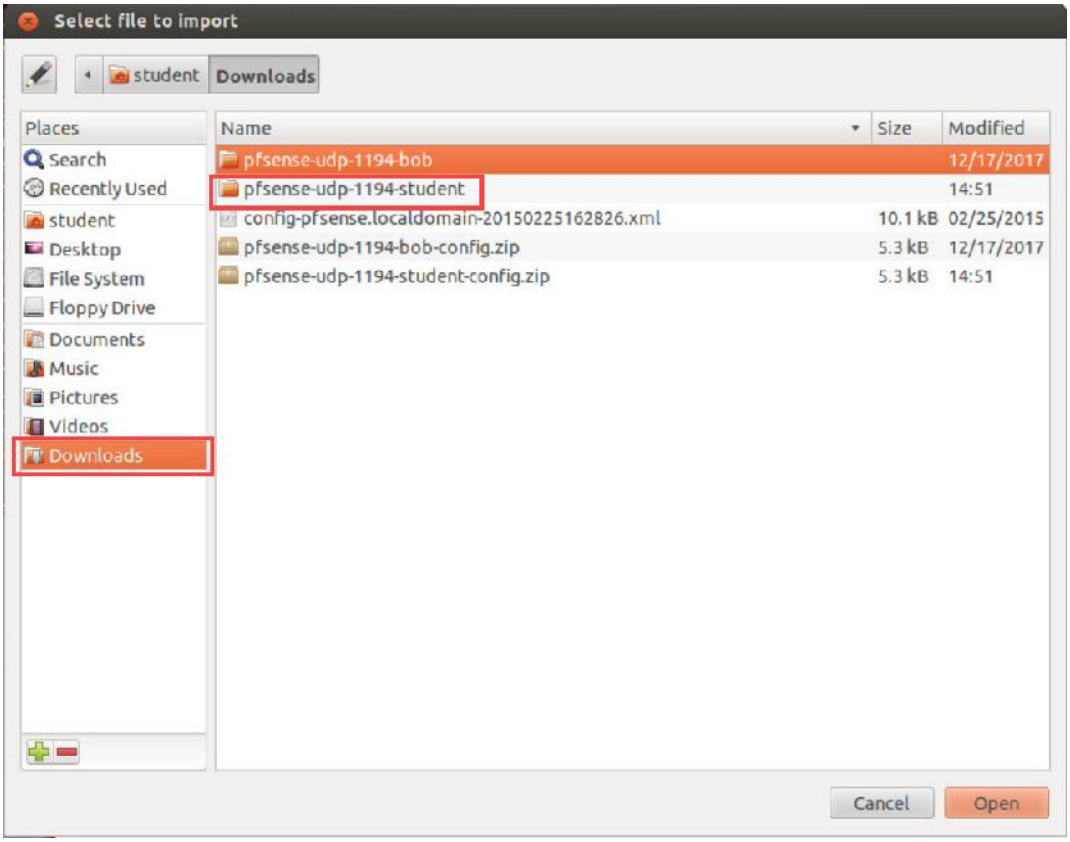
```
student@Ubuntu:~/Downloads$ unzip pfsense-udp-1194-student-config.zip
Archive:  pfsense-udp-1194-student-config.zip
   creating: pfsense-udp-1194-student/
  inflating: pfsense-udp-1194-student/pfsense-udp-1194-student.ovpn
  inflating: pfsense-udp-1194-student/pfsense-udp-1194-student-tls.key
 extracting: pfsense-udp-1194-student/pfsense-udp-1194-student.p12
student@Ubuntu:~/Downloads$
```

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

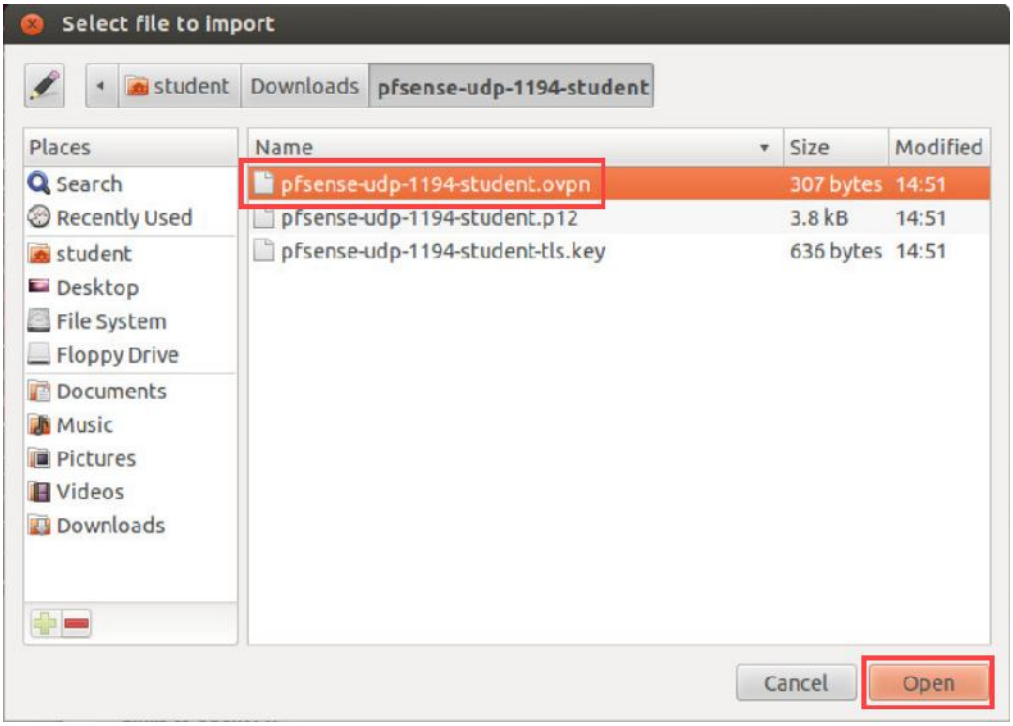


4. On the *Network Connections* window, confirm you are on the **VPN** tab. Click on the **Import** button.

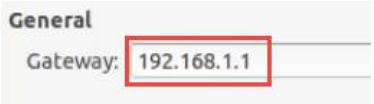
5. In the *File Manager* window, select **Downloads** from the menu on the left. Double-click on the **pfsense-udp-1194-student** folder.



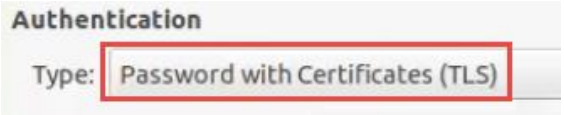
6. Select the **pfsense-udp-1194-student.ovpn** file and click the **Open** button.



7. In the new pop-up window, set the *Gateway* to **192.168.1.1**.



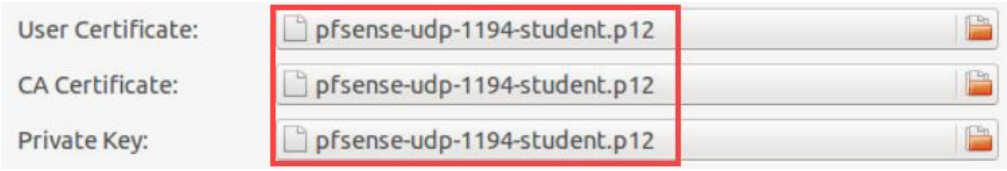
8. Confirm that the *Authentication Type* is configured to **Password with Certificate (TLS)**.



9. Type **student** in the *User name* field.

10. Type **bpassx** in the *Password* field.

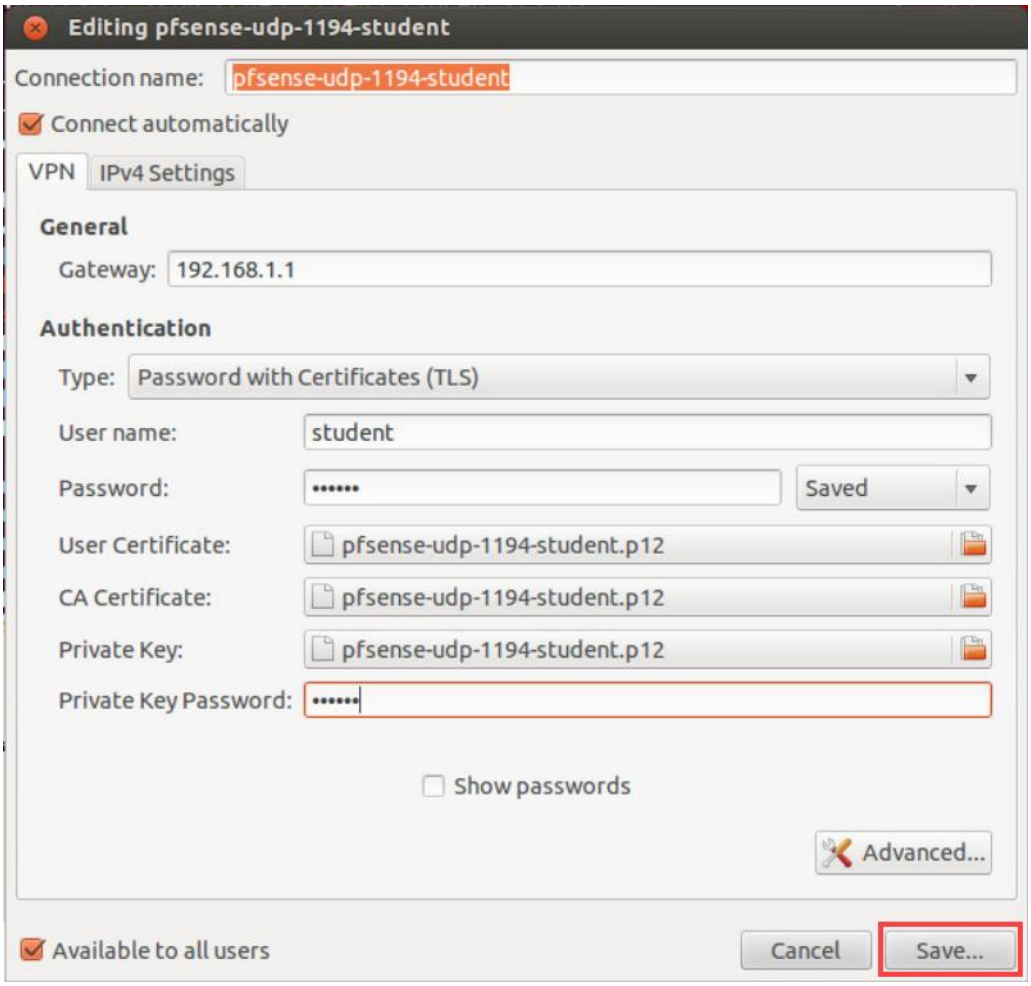
11. Confirm that the file **pfsense-udp-1194-student.p12** occupies the entry for *User Certificate*, *CA Certificate,* and *Private Key*.



12. Type **bpassx** in the *Private Key Password* field.

13. Leave everything else in their **default** settings.

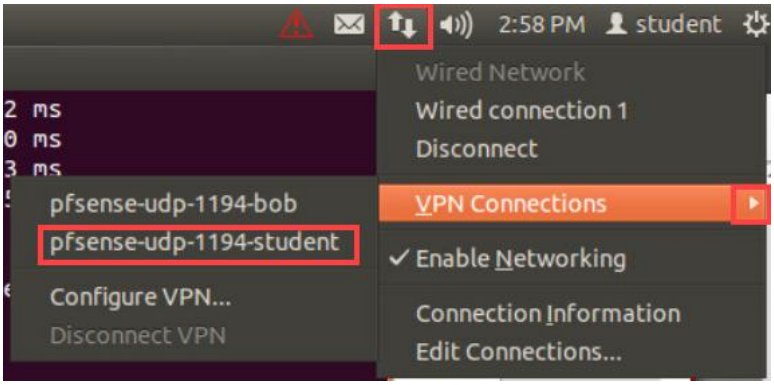
14. Verify that the configurations reflect the image below. Click the **Save** button.



15. **Close** the *Network Connections* window.

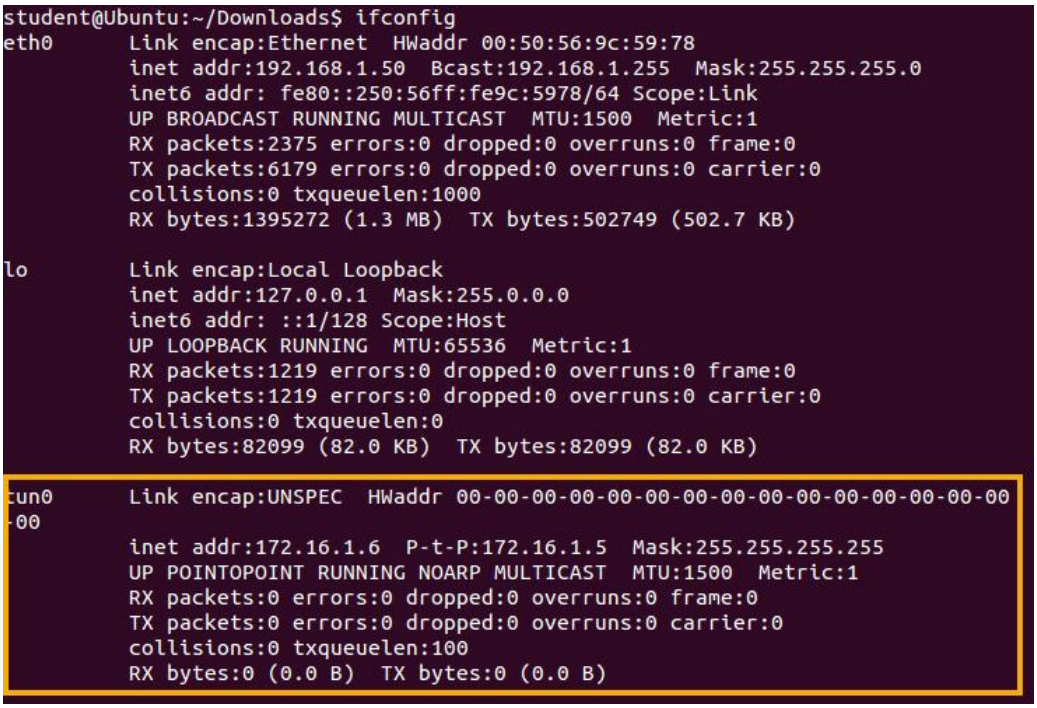
3.4 Connecting the VPN Client

1. Connect using the *VPN* settings by clicking on the **Network Manager** icon on the top pane and navigate to **VPN Connection > pfsense-udp-1194-student**.



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

```
student@Ubuntu:~/Downloads$ ifconfig
```



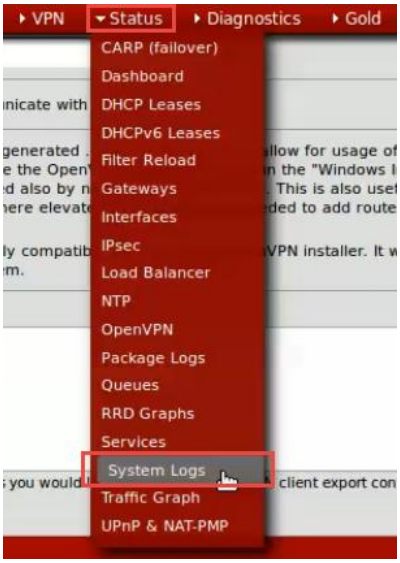
```
student@Ubuntu:~/Downloads$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:50:56:9c:59:78
          inet addr:192.168.1.50  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::250:56ff:fe9c:5978/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2375 errors:0 dropped:0 overruns:0 frame:0
          TX packets:6179 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1395272 (1.3 MB)  TX bytes:502749 (502.7 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:1219 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1219 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:82099 (82.0 KB)  TX bytes:82099 (82.0 KB)

tun0      Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
-00
          inet addr:172.16.1.6  P-t-P:172.16.1.5  Mask:255.255.255.255
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

3.5 Managing VPN Connections

1. Once connected to the *VPN server*, switch to the **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.

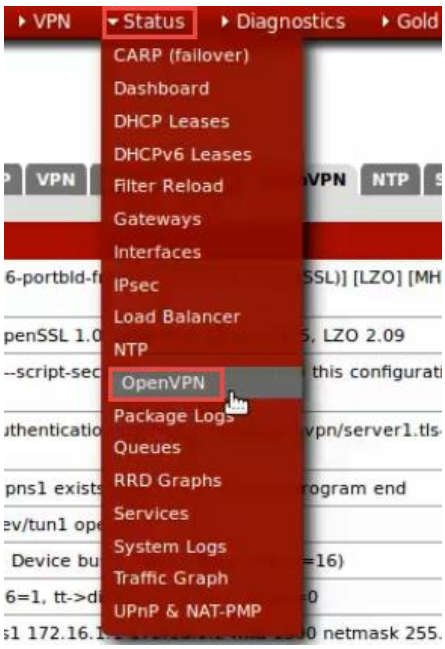


3. On the new page, select the **OpenVPN** tab.

4. Notice the steps per *student's* authentication to the *VPN server*.

Dec 14 19:59:10	openvpn: user 'student' authenticated
Dec 14 19:59:10	openvpn[53298]: 192.168.1.50:55297 [student] Peer Connection Initiated with [AF_INET]192.168.1.50:55297
Dec 14 19:59:10	openvpn[53298]: student/192.168.1.50:55297 MULTI_sva: pool returned IPv4=172.16.1.6, IPv6=(Not enabled)
Dec 14 19:59:12	openvpn[53298]: student/192.168.1.50:55297 send_push_reply(): safe_cap=940

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.

