CySA+ Lab Series

Lab 16: Configuring a Firewall

Document Version: 2022-10-10

Material in this Lab Aligns to the Following	
CompTIA CySA+ (CS0-002) Exam Objectives	1.3 - Given a scenario, perform vulnerability management activities 2.1 - Explain software assurance best practices 3.1 - Given a scenario, analyze data as part of security monitoring activities 3.2 - Given a scenario, implement configuration changes to existing controls to improve security 3.3 - Explain the importance of proactive threat hunting
All-In-One CompTIA CySA+ Second Edition ISBN-13: 978-1260464306 Chapters	3: Vulnerability Management Activities 8: Security Solutions for Infrastructure Management 11: Data Analysis in Security Monitoring Activities 12: Implement Configuration Changes to Existing Controls to Improve Security 13: The Importance of Proactive Threat Hunting

Contents

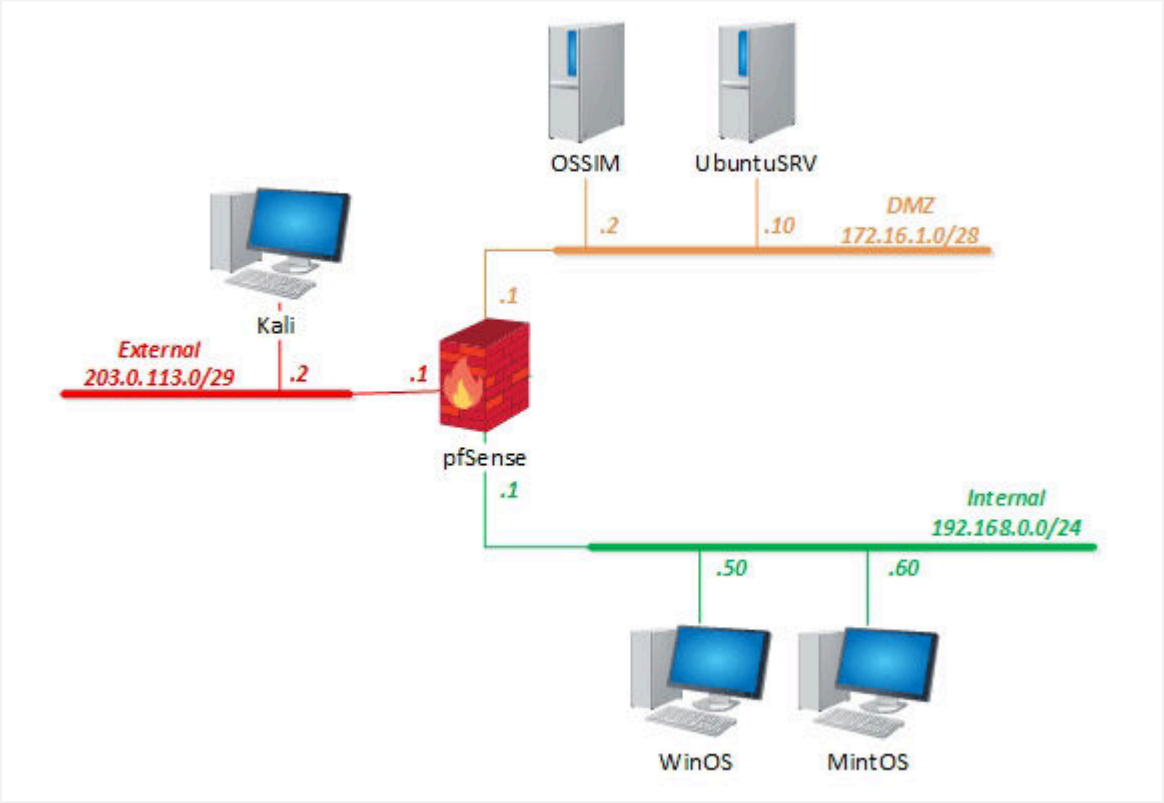
Introduction

In this lab, you will be configuring a firewall using an open source firewall, *pfSense*.

Objectives

- Implement security configuration parameters on a firewall
- Configuring ICMP on the Firewall
- Redirecting Traffic to Internal Hosts on the Network
- Configuring a VPN on the *pfSense* firewall

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.

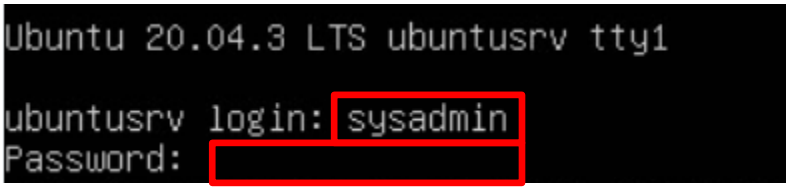
Virtual Machine	IP Address	Account	Password
WinOS (Server 2019)	192.168.0.50	Administrator	NDGlabpass123!
MintOS (Linux Mint)	192.168.0.60	sysadmin	NDGlabpass123!
OSSIM (AlienVault)	172.16.1.2	root	NDGlabpass123!
UbuntuSRV (Ubuntu Server)	172.16.1.10	sysadmin	NDGlabpass123!
Kali	203.0.113.2	sysadmin	NDGlabpass123!
pfSense	203.0.113.1 172.16.1.1 192.168.0.1	admin	NDGlabpass123!

1 Configuring ICMP on the Firewall

When a web server is placed in a DMZ for web access from inside the organization as well as from the internet, the web server is exposed. If traffic from the DMZ is allowed to access the Internal network, a bad actor can use the webserver to compromise the hosts and the data on the LAN. A security administrator needs to be aware of these backdoors and take corrective action to close them.

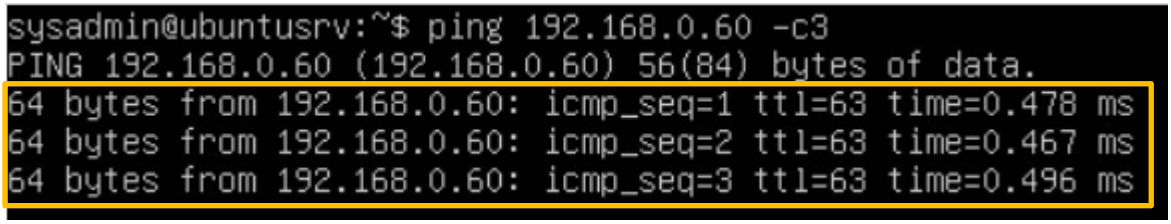
In this task, you will block ICMP (ping) packets from the DMZ from accessing hosts in the *Internal* network.

1. Set the focus on the **UbuntuSRV** computer.
2. Log in as `sysadmin` using the password: `NDGlabpass123!`



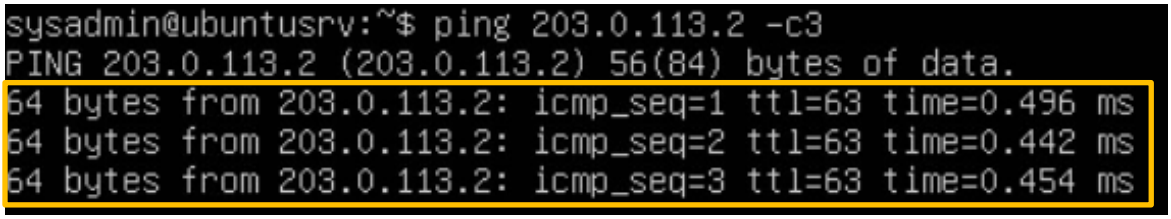
3. *Ping* the *MintOS* computer on the internal network by typing the following command:

```
ping 192.168.0.60 -c3
```

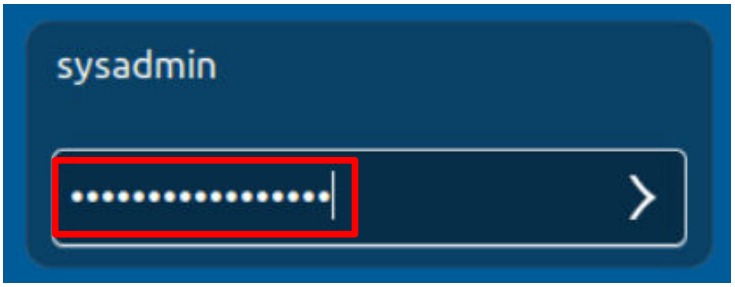


4. *Ping* the *Kali* computer on the external network by typing the following command:

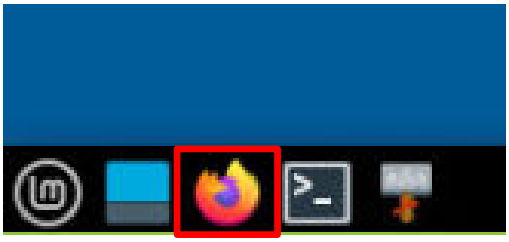
```
ping 203.0.113.2 -c3
```



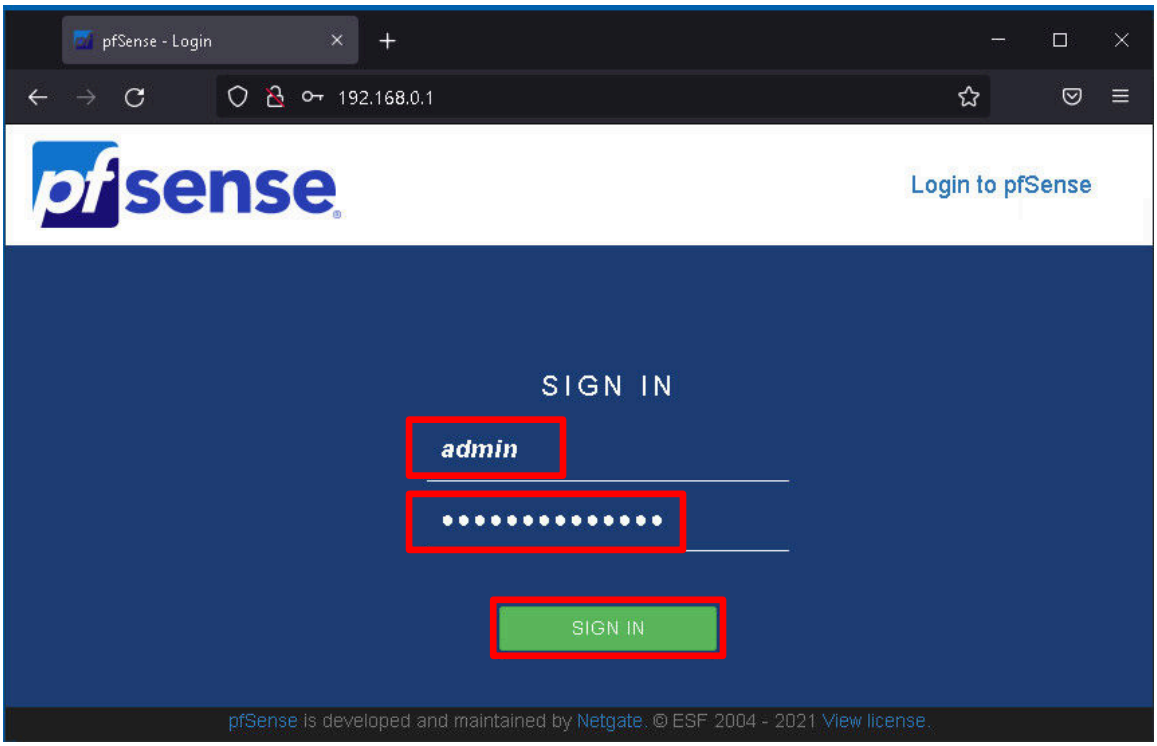
5. Set the focus to the **MintOS** computer.
6. Log in to the *sysadmin* account using the password: `NDGlabpass123!`



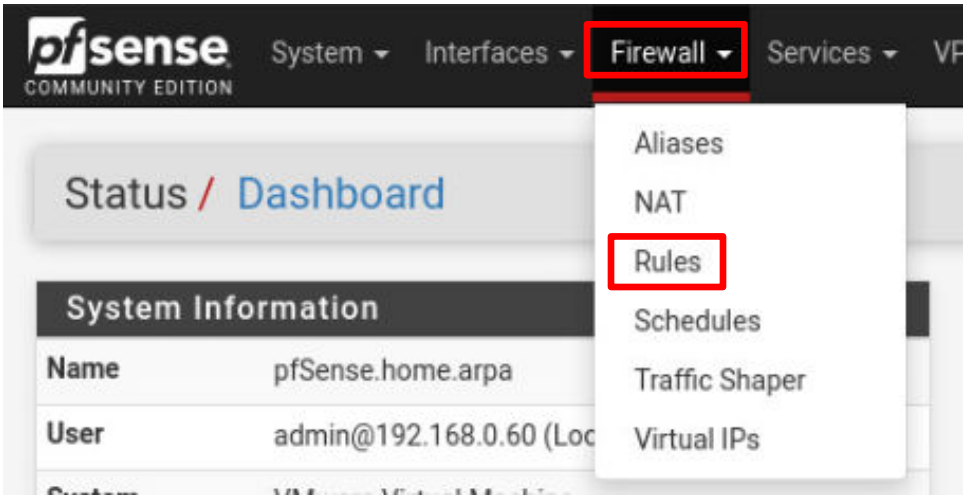
7. Open the browser by clicking on the **Firefox** icon in the toolbar at the bottom of the window.



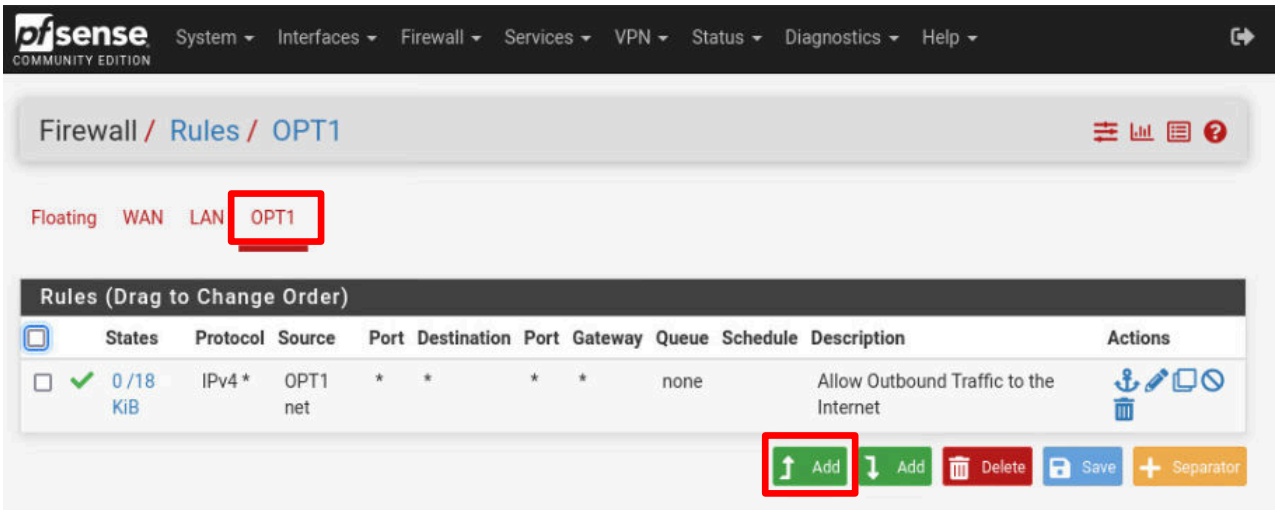
8. In the address bar of the browser, type `192.168.0.1`, which is the IP address of the **pfSense** server. Then log in as `admin` using the password `NDGlabpass123!` and click the **SIGN IN** button.



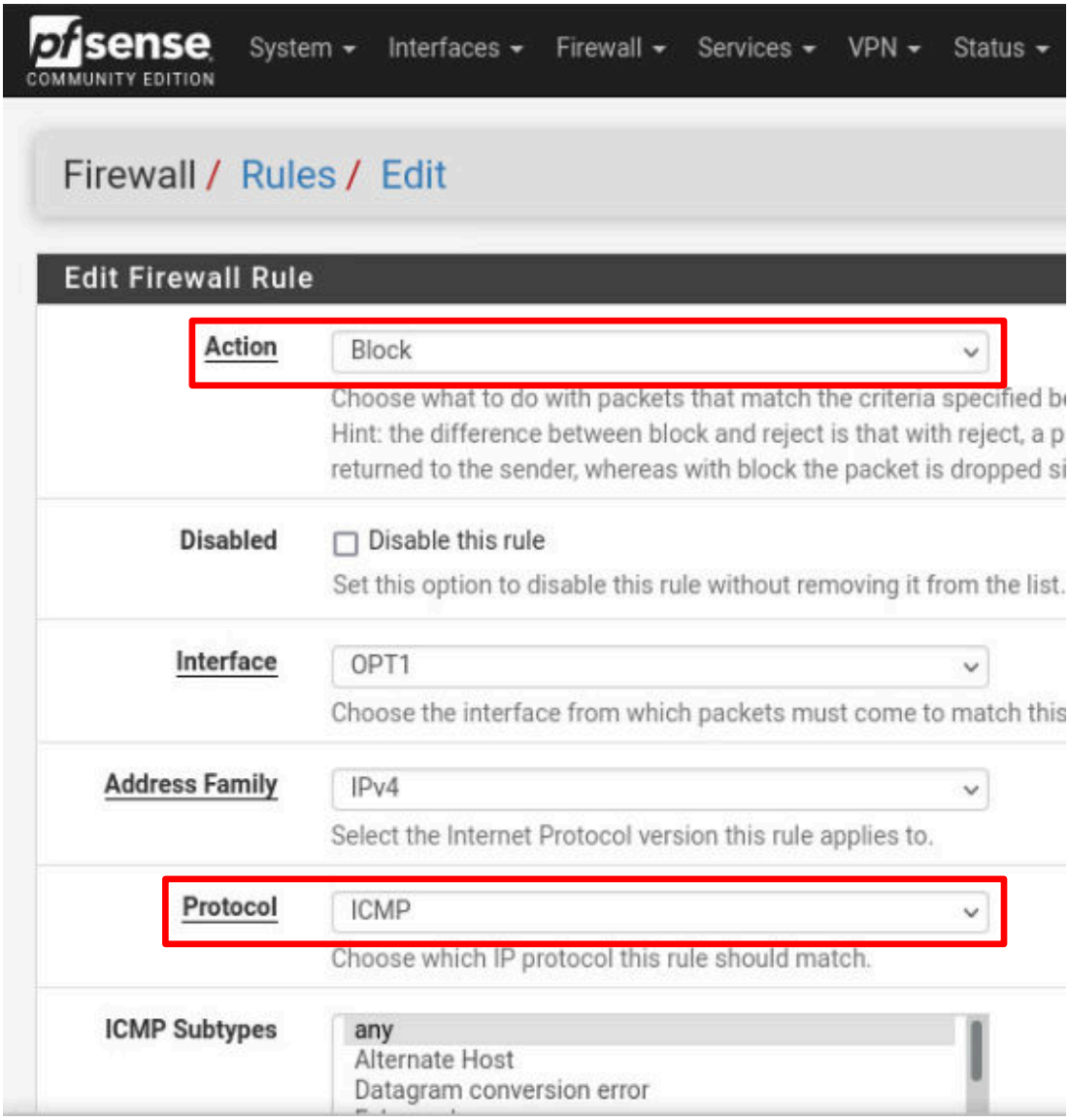
9. A rule will need to be added to block *ICMP* traffic from the *DMZ* to the internal network. Click on **Firewall**, then click on **Rules.**



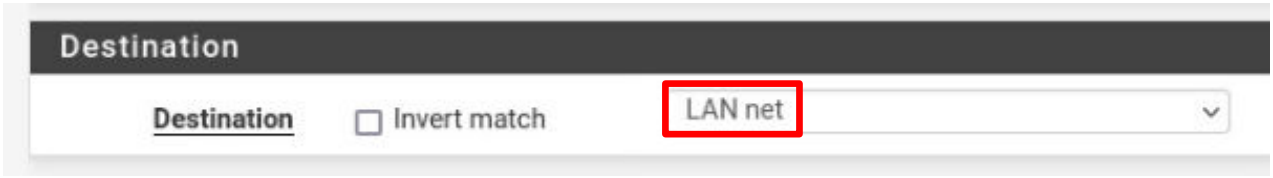
10. Click the **OPT1** interface option and click the **Add to Top** button.



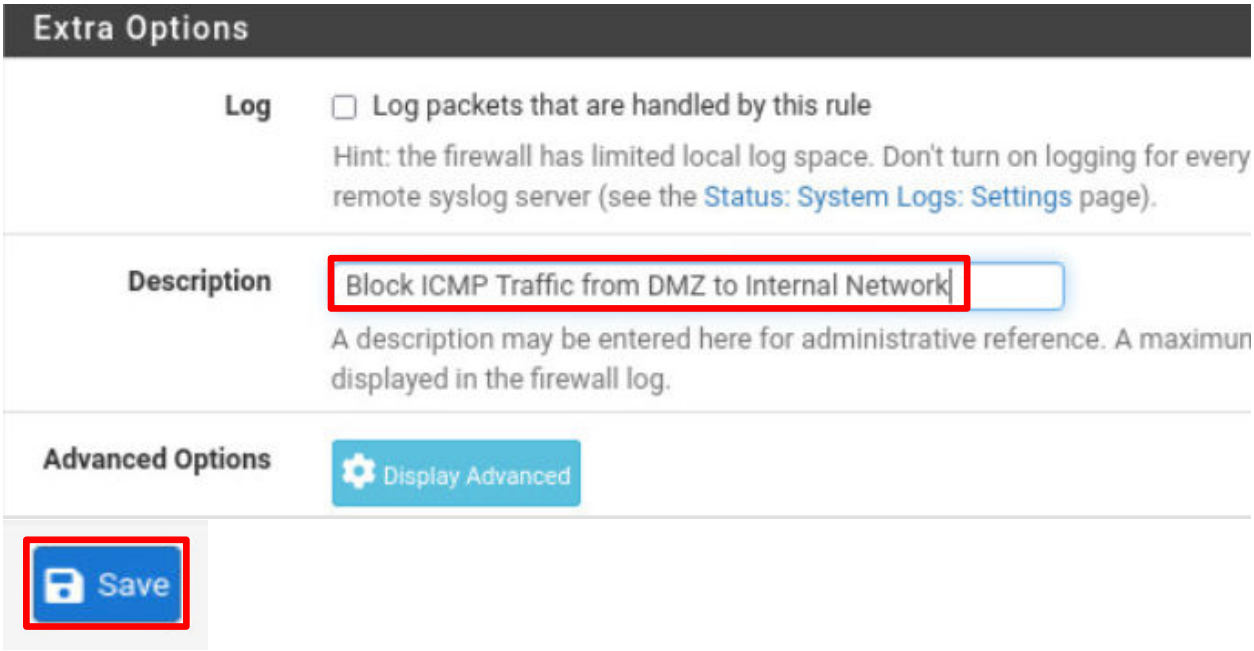
11. In the *Edit Firewall Rule* section, use the list arrow to change the *Action* to **Block** and then change the *Protocol* to **ICMP.**



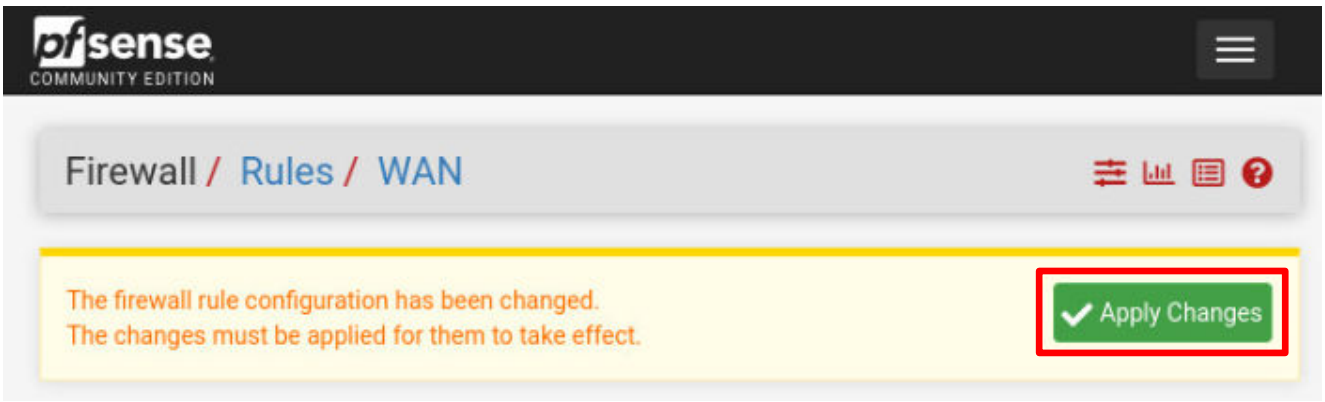
12. Scroll down to the lower half of the window. In the *Destination* section, use the list arrow to change the *Destination* to **LAN net**.



13. In the *Extra Options* section, type the description `Block ICMP Traffic from DMZ to Internal Network`. At the bottom of the page, click the **Save** button.



14. Click the **Apply Changes** button.



15. Set the focus back to the *UbuntuSRV* computer.
16. *Ping* the *MintOS* computer again using the following command:

```
ping 192.168.0.60 -c3
```

```
sysadmin@ubuntusrv:~$ ping 192.168.0.60 -c3
PING 192.168.0.60 (192.168.0.60) 56(84) bytes of data.
^C
--- 192.168.0.60 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2033ms
```

There will be no response from the *MintOS* computer because the *ICMP* messages have been blocked.

17. To demonstrate that *ICMP* messages are blocked to all host addresses on the Internal network, ping the Internal network interface (**192.168.0.1**) on *pfSense* by using the following command:

```
ping 192.168.0.1 -c3
```

```
sysadmin@ubuntusrv:~$ ping 192.168.0.1 -c3
PING 192.168.0.1 (192.168.0.1) 56(84) bytes of data.
^C
--- 192.168.0.1 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2038ms
```

There will not be a response from the internal network interface on the *pfSense* computer.

If you try pinging the *WinOS* computer at **192.168.0.50**, you would not get a response because the Windows firewall is already blocking ICMP packets. If you wanted to test the rule on the *WinOS* computer, you would have to either change the firewall rules or turn off the firewall on the *WinOS* computer.

18. To confirm that *ICMP* packets can still be sent out, *ping* the *Kali* computer on the external network by typing the following command:

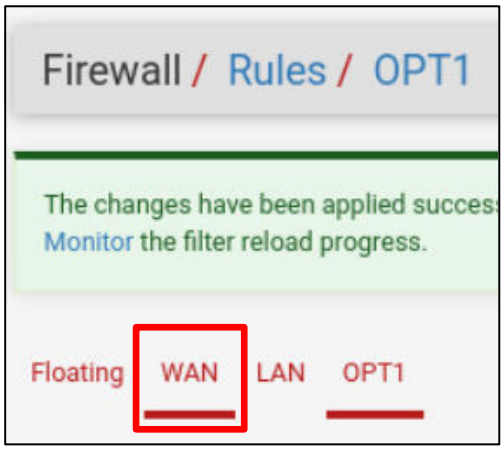
```
ping 203.0.113.2 -c3
```

```
sysadmin@ubuntusrv:~$ ping 203.0.113.2 -c3
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=0.496 ms
64 bytes from 203.0.113.2: icmp_seq=2 ttl=63 time=0.442 ms
64 bytes from 203.0.113.2: icmp_seq=3 ttl=63 time=0.454 ms
```

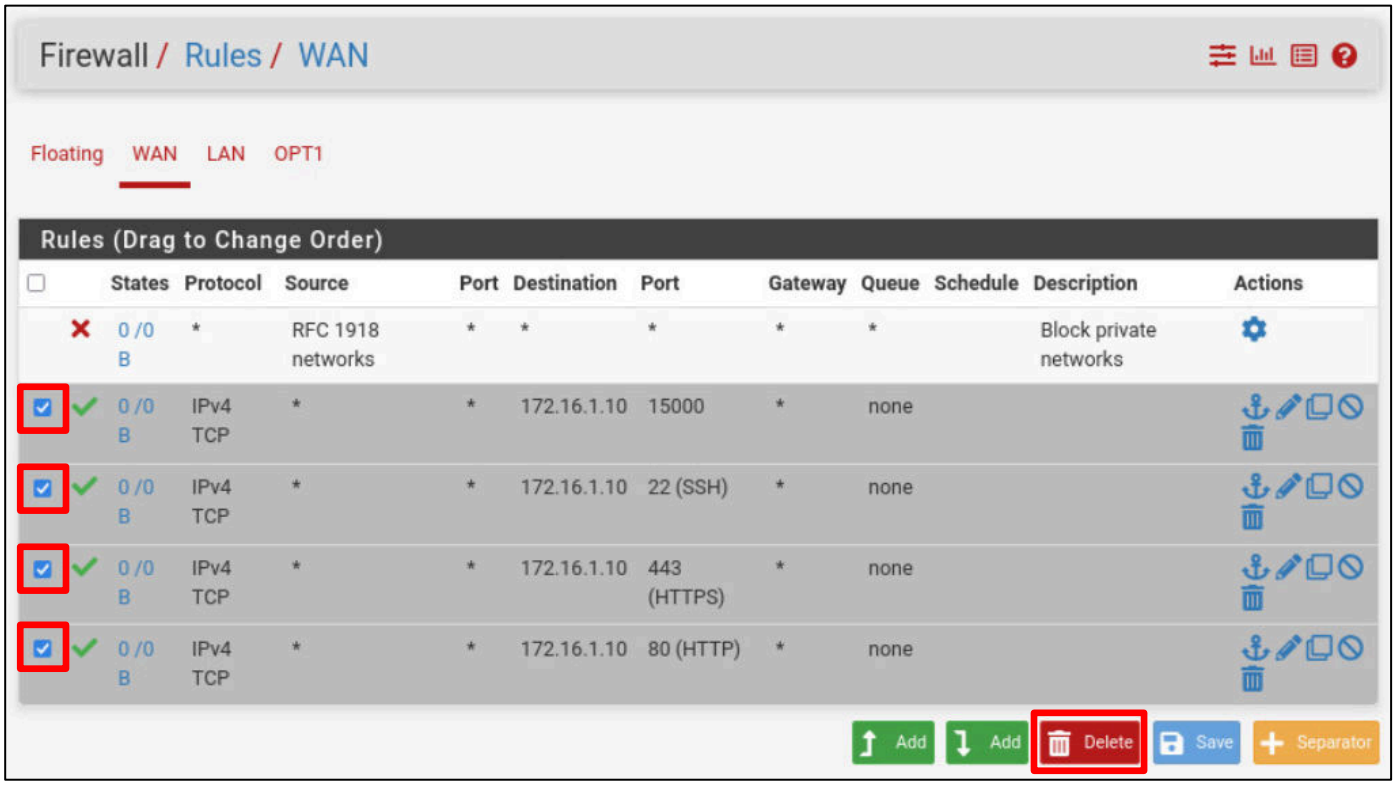
2 Redirecting Traffic Using Port Forwarding

Port Forwarding can be used to redirect traffic from external networks to hosts on private networks, such as 192.168.0.0 or 172.16.1.0, by using the *Network Address Translation* protocol or *NAT*.

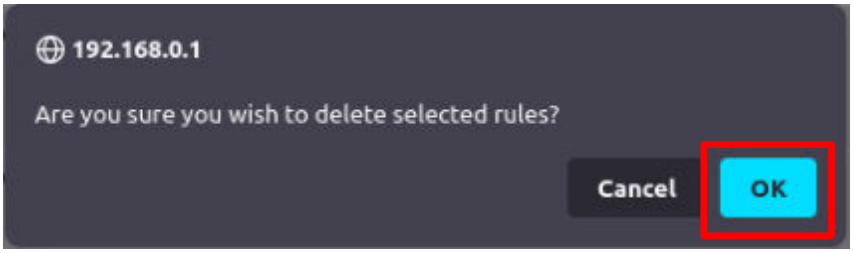
1. Return to the **MintOS** computer.
2. You should still be on the *Firewall/Rules/OPT1* page. Click on **WAN** in the menu bar.



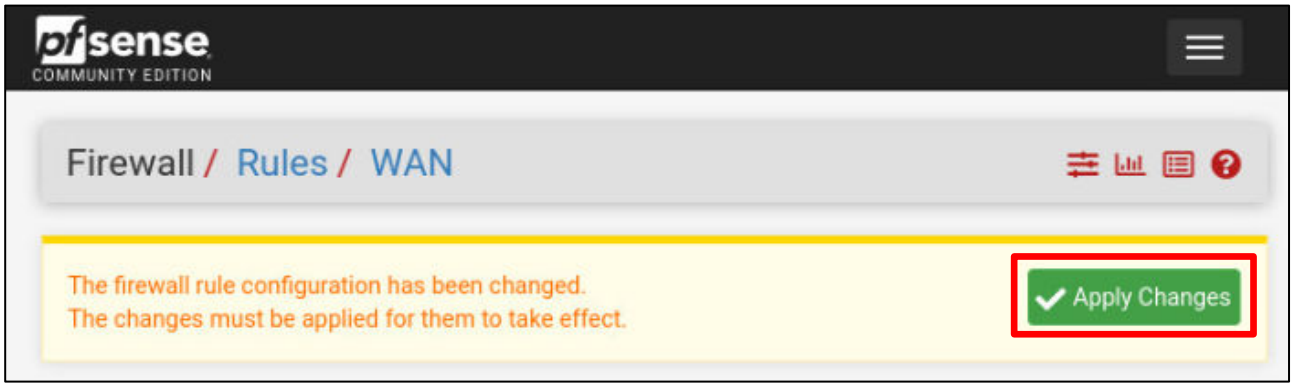
3. In the *Rules* box, click on the **checkbox** for all of the pass rules (the green checkmarks) for the IPv4 Protocol to destination 172.16.1.10 (the *UbuntuSRV* computer) and click the **Delete** button at the bottom of the window.



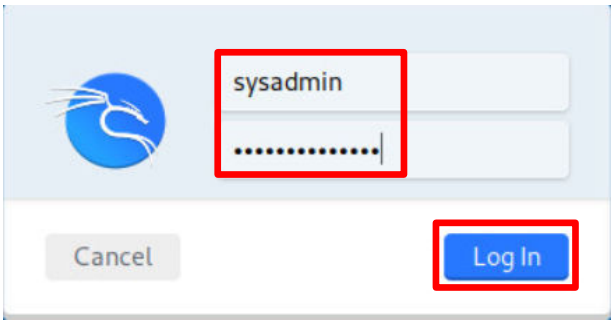
4. In the *Confirmation* window, when asked, *Are you sure you wish to delete the selected rules?* click the **OK** button.



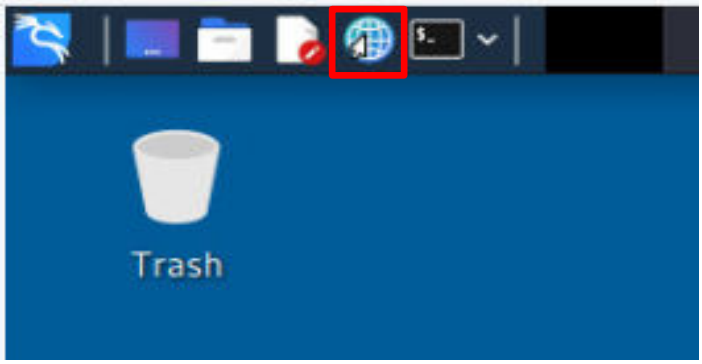
5. Click the **Apply Changes** button.



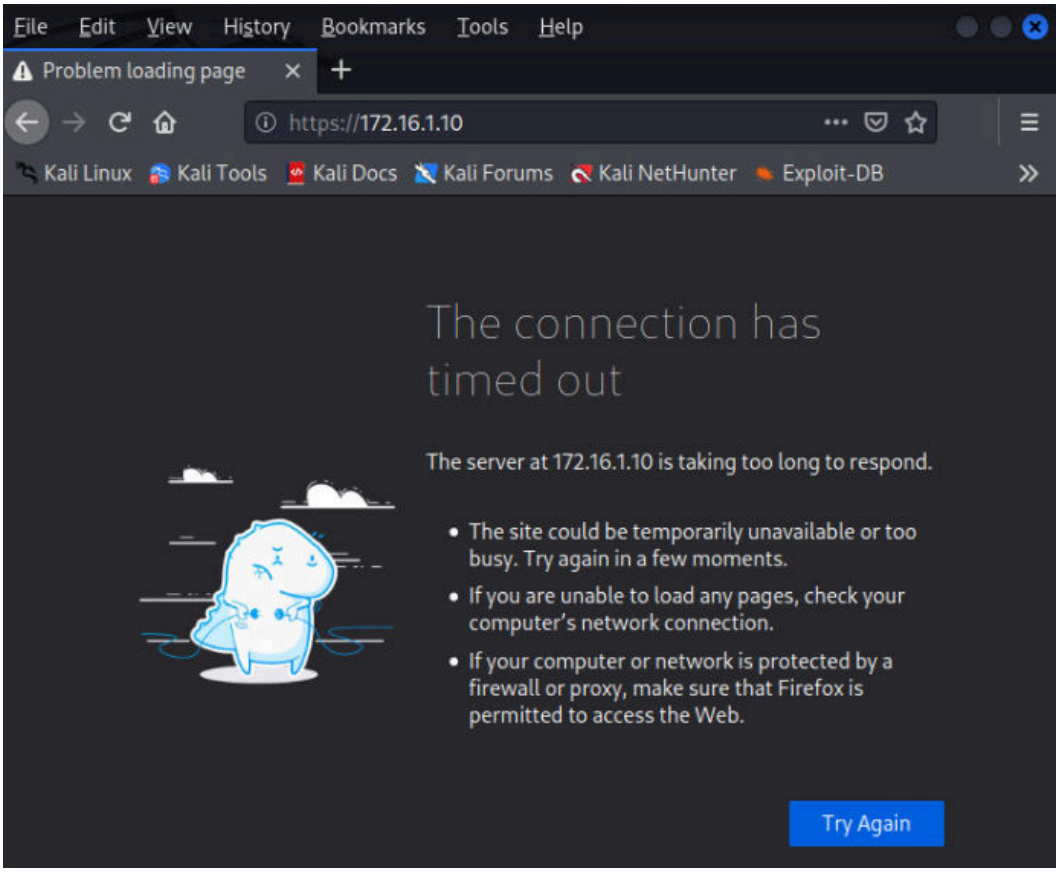
6. Set the focus to the **Kali** computer.
7. Log in as `sysadmin` using the password `NDGlabpass123!` and then click the **Log In** button.



8. Open the **Web Browser** application on the taskbar.



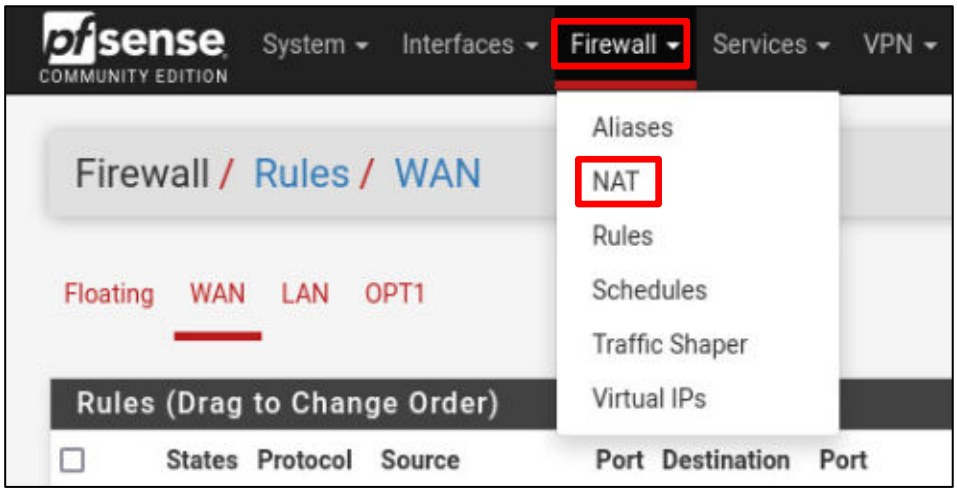
9. In the address bar, type `https://172.16.1.10`. After a couple of minutes, the browser should timeout, and you will see a window pop up, indicating that the website is not accessible.



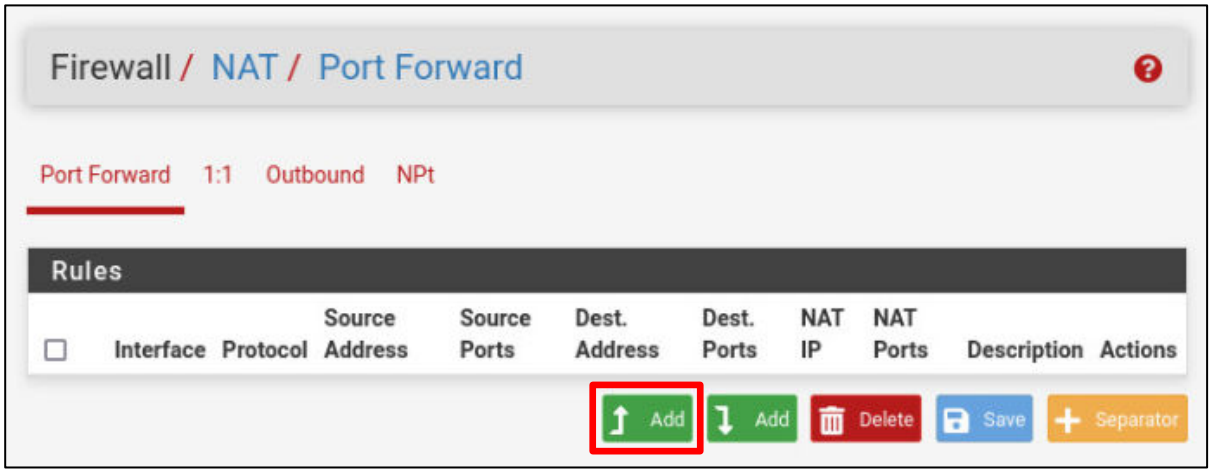
The connection from the external network to the web server on the *DMZ* network cannot be established because the *WAN*-based rules on the *pfSense* firewall were deleted, which effectively closed both *HTTP* and *HTTPS* access.

10. Close the **Firefox** browser window on the *Kali* computer.
11. Return to the **MintOS** computer. The *Firefox* browser should still be open to the *pfSense* management page.

12. Click on **Firewall** and click **NAT** from the dropdown menu.

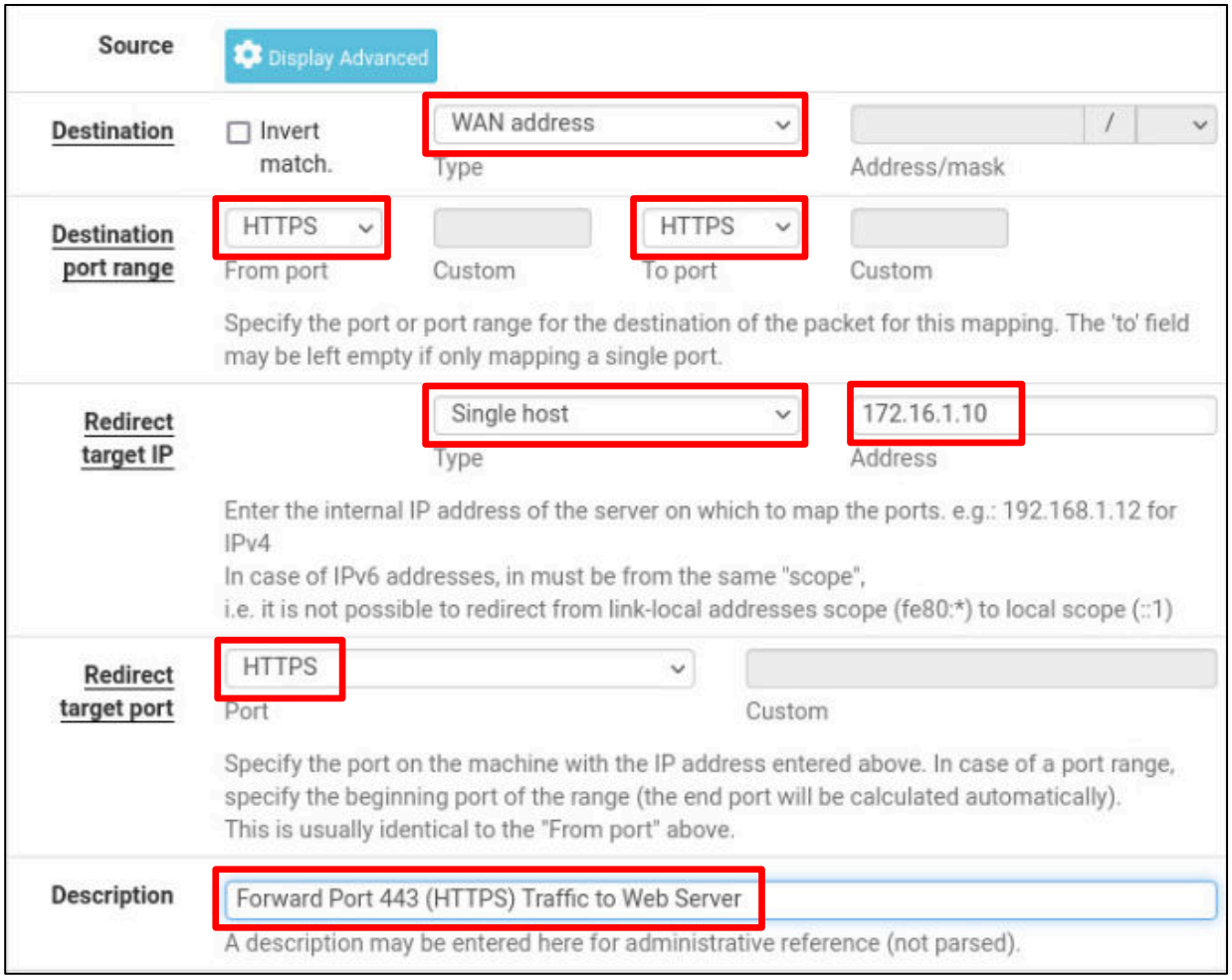


13. On the *Firewall/NAT/Port Forward* window, click on the **Add to Top** button.

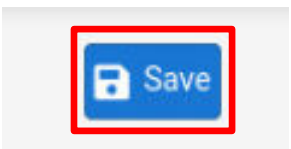


14. In the *Edit Redirect Entry* section, scroll down and make the following changes:

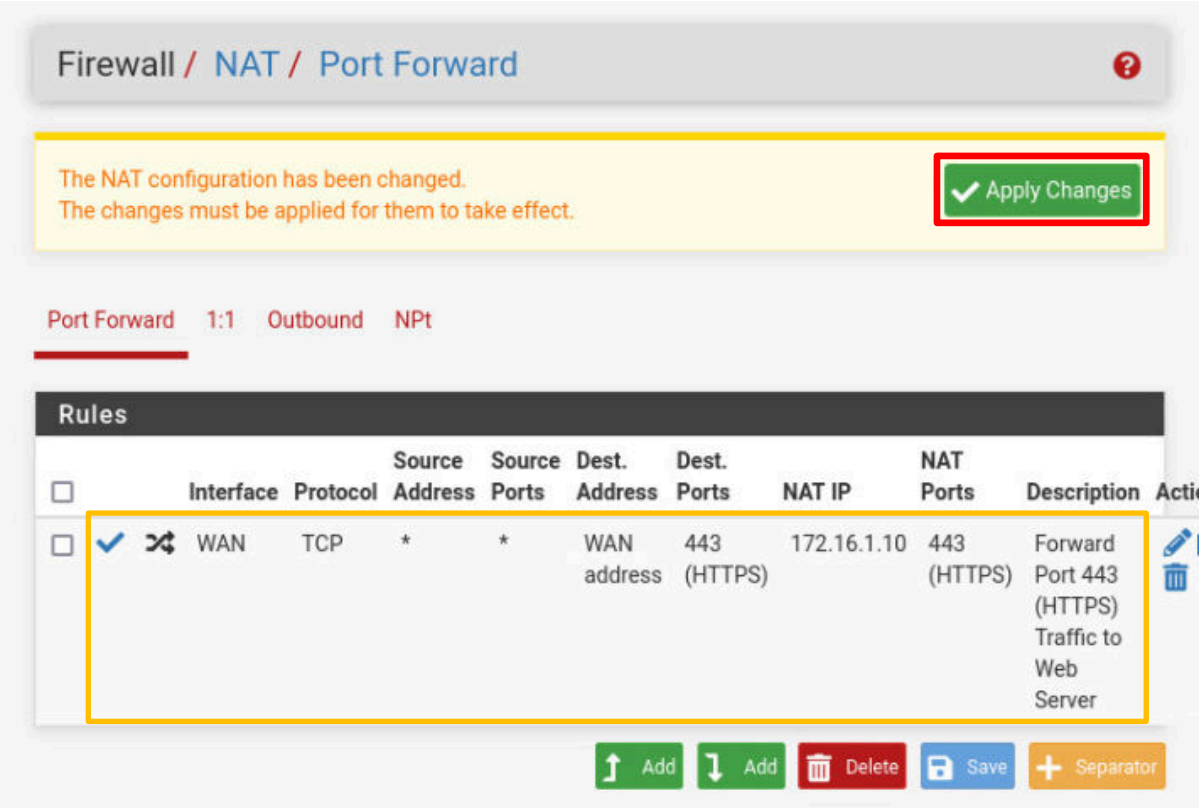
Destination	Use the list arrow and select **WAN Address** (if not already selected)
Destination Port Range:	Use the list arrow and select **HTTPS** for the **From Port** (the **To Port** should automatically select **HTTPS**)
Redirect Target IP	Use the list arrow and select **Single Host** as the *Type* and in the *Address* box, type `172.16.1.10`
Redirect Target Port	Use the list arrow and select **HTTPS**
Description	Type `Forward Port 443 (HTTPS) Traffic to the Web Server` in the box



15. At the bottom of the window, click on the **Save** button.

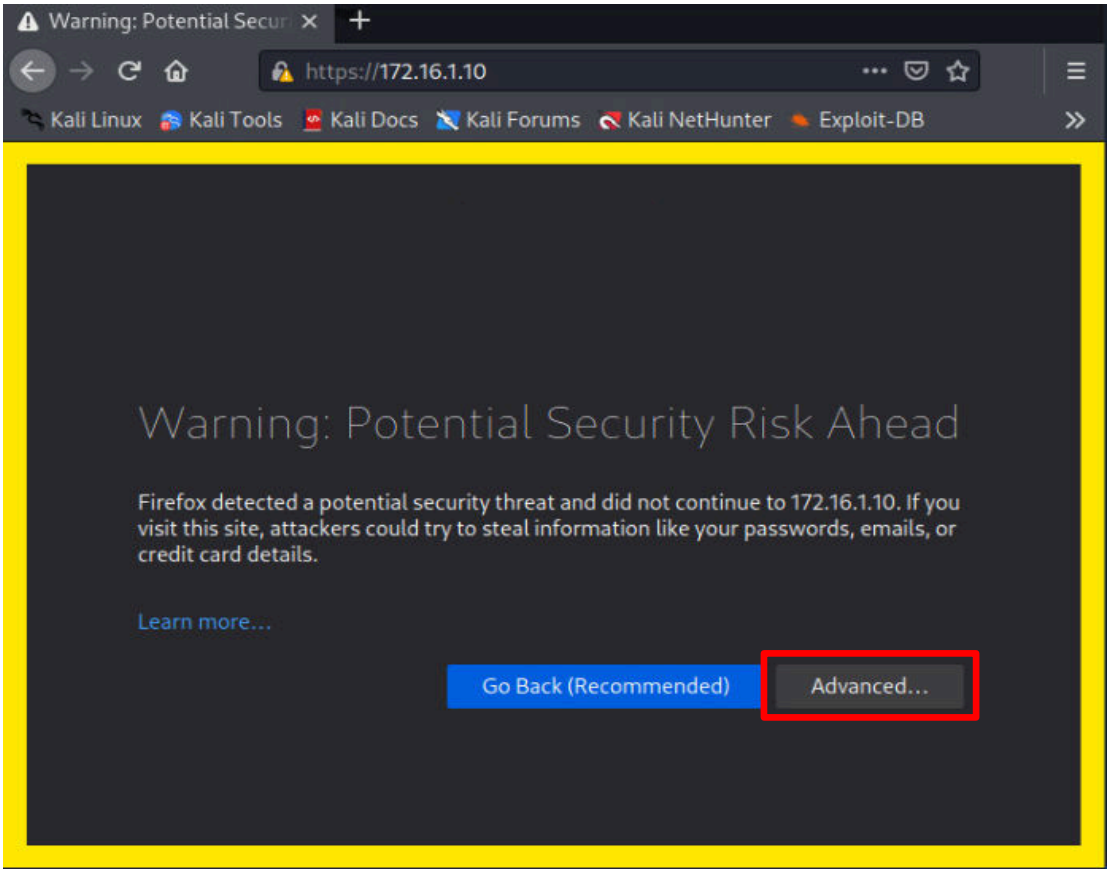


16. Confirm that the redirect is correct and click on the **Apply Changes** button.

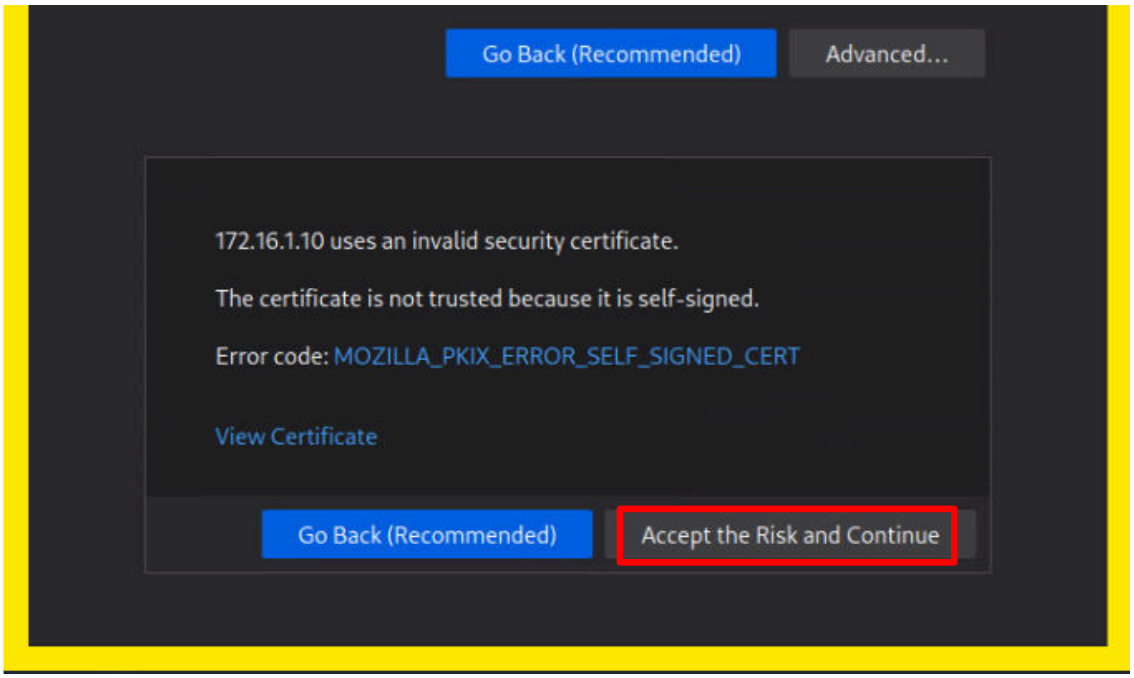


17. Return to the *Kali* computer.

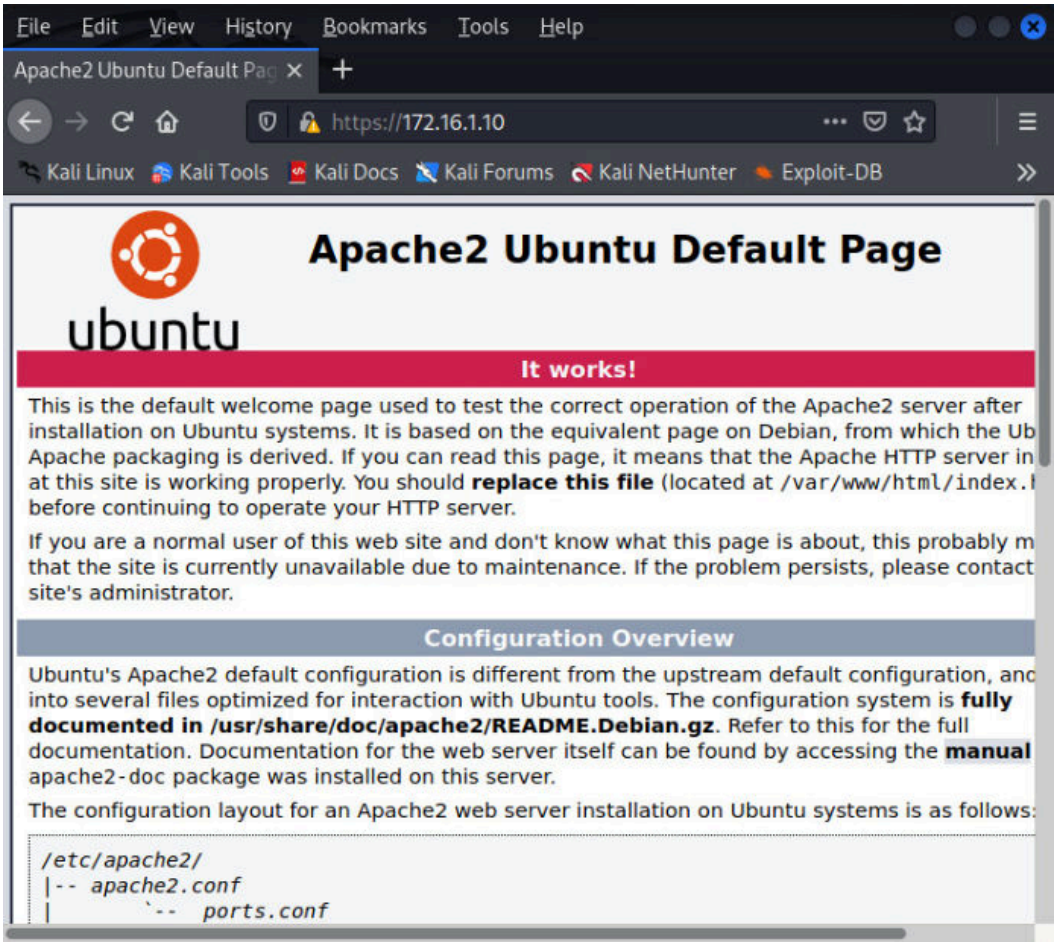
18. Open the Firefox browser and type in the IP address of the *UbuntuSRV* computer (`https://172.16.1.10`). You should get a security risk warning. Click the **Advanced** button.



19. Scroll down to the bottom of the window and click **Accept the Risk and Continue** button.



You should now see the *Apache2 Ubuntu Default Page* in a successful attempt to communicate with the *UbuntuSRV* web service via HTTPS.



20. Close the **Firefox** browser window.

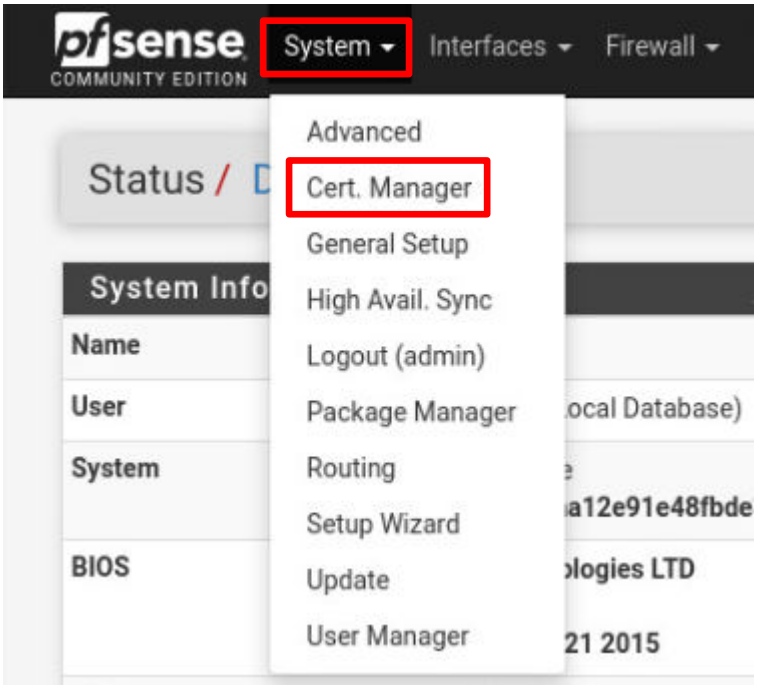
3 Configuring a Virtual Private Network (VPN) on the Firewall

Another tool that allows devices out on the internet to access resources on the inside network is a Virtual Private Network or VPN. A VPN effectively extends an organization's private network across and through public networks. A host connected through a VPN appears as though connected directly to the organization's local network.

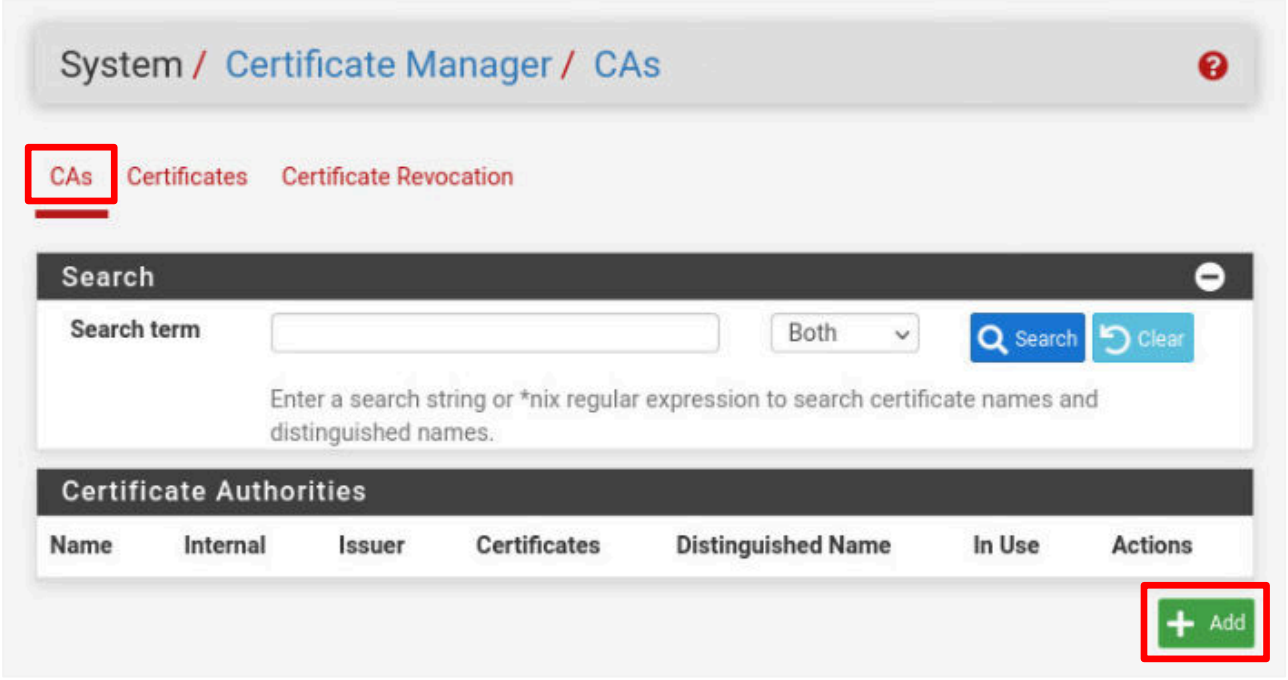
A security analyst could be tasked with securely setting up the organization's VPN and monitoring the activity to ensure that it is being used only by authorized users.

3.1 Setting up the Certificate for the VPN

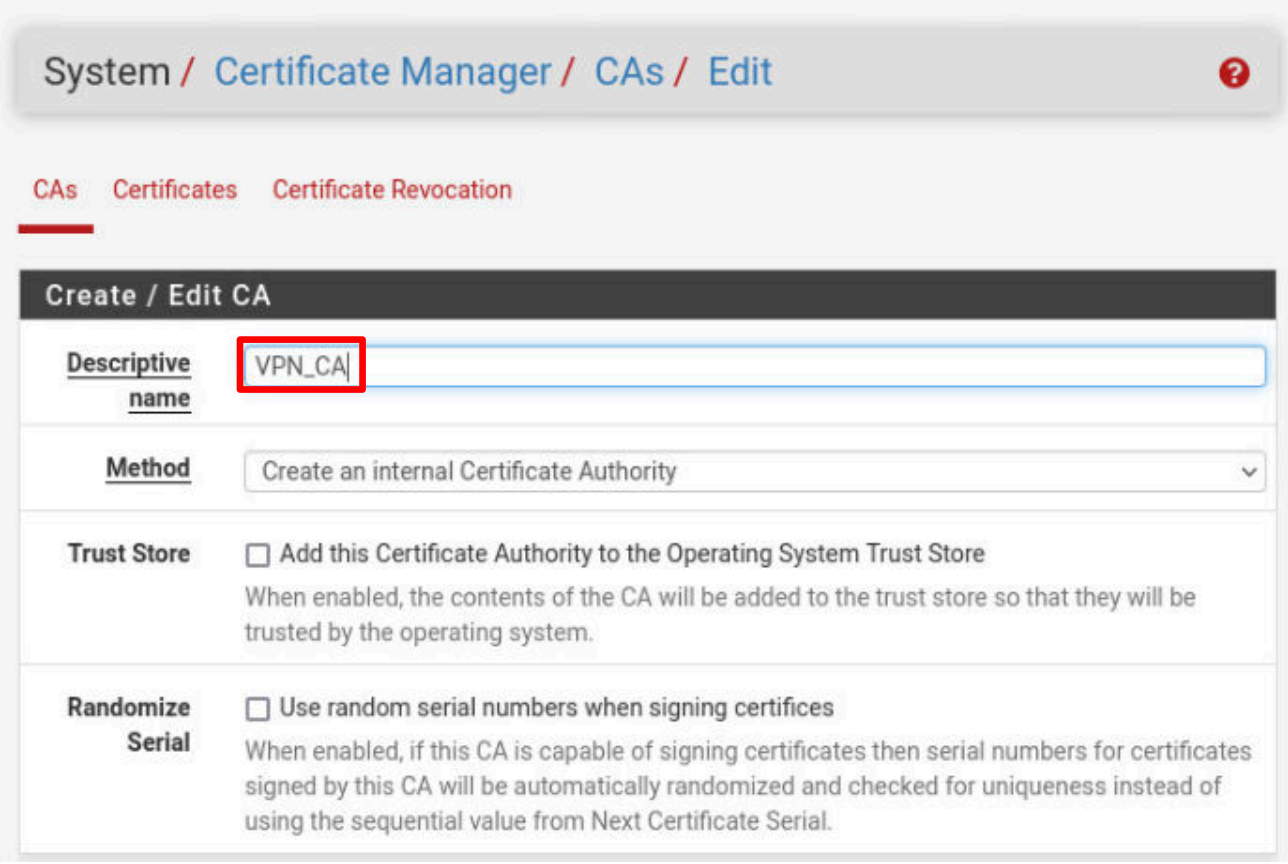
1. Change the focus to the **MintOS** computer.
2. From the *pfSense Dashboard*, click on **System** and then click on the **Cert Manager** from the dropdown menu.



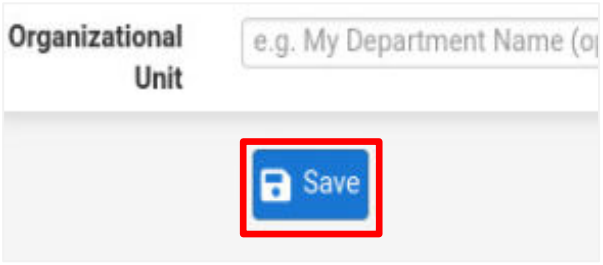
3. On the *System/Certificate Manager/CAs* page, the **CAs** tab should be selected, and then click the **+Add** button at the bottom of the window.



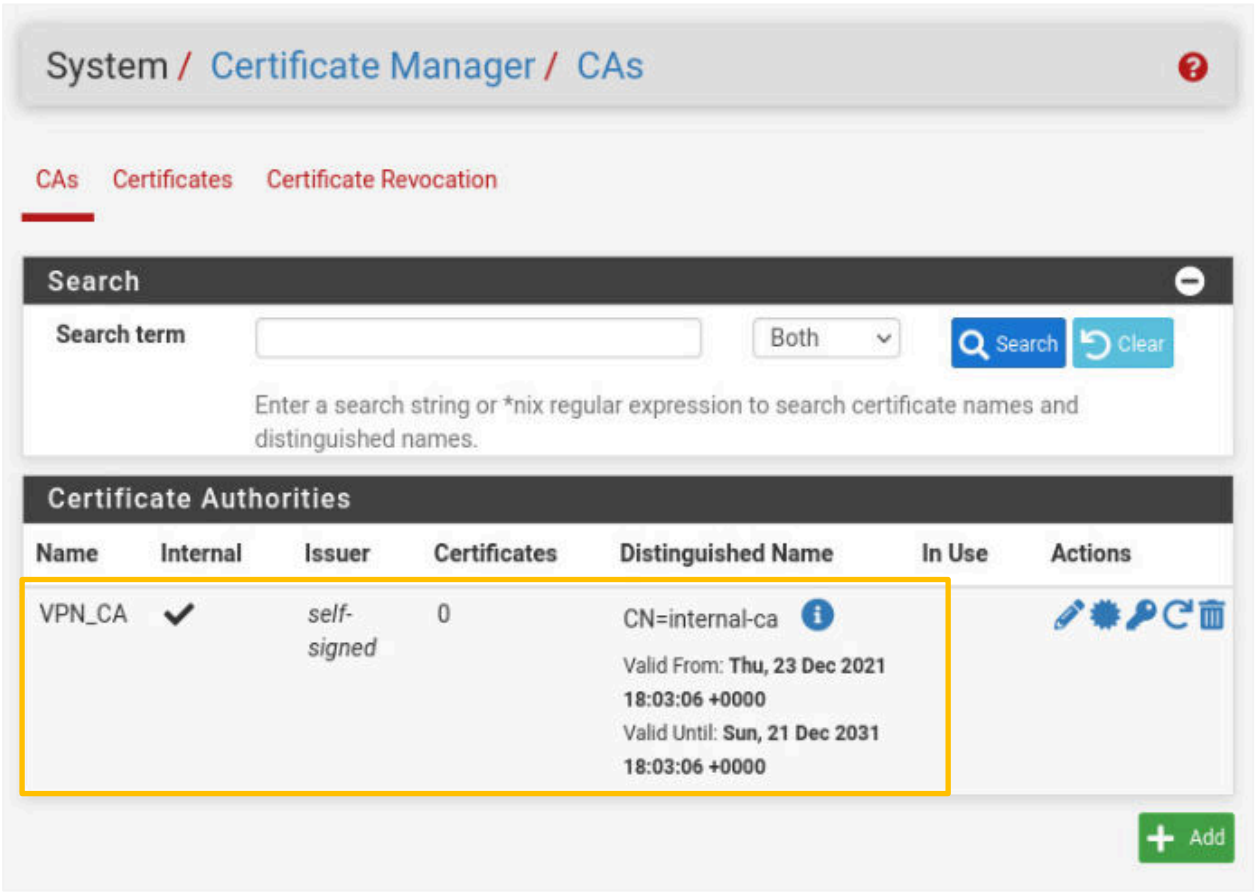
4. On the *System/Certificate Manager/CAs/Edit* page in the *Create/Edit CA* section, type `VPN_CA` for the *Descriptive Name.*



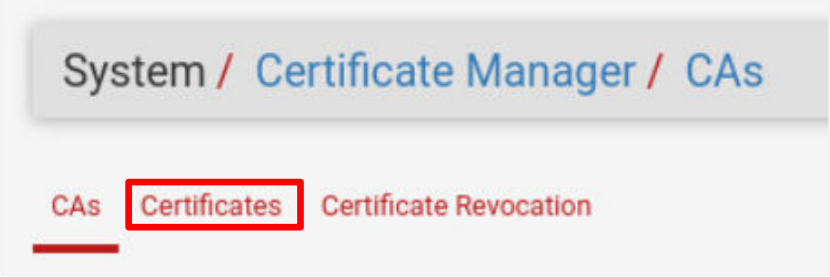
5. The remaining fields can be left at their default values. Scroll to the bottom of the window and click on the **Save** button.



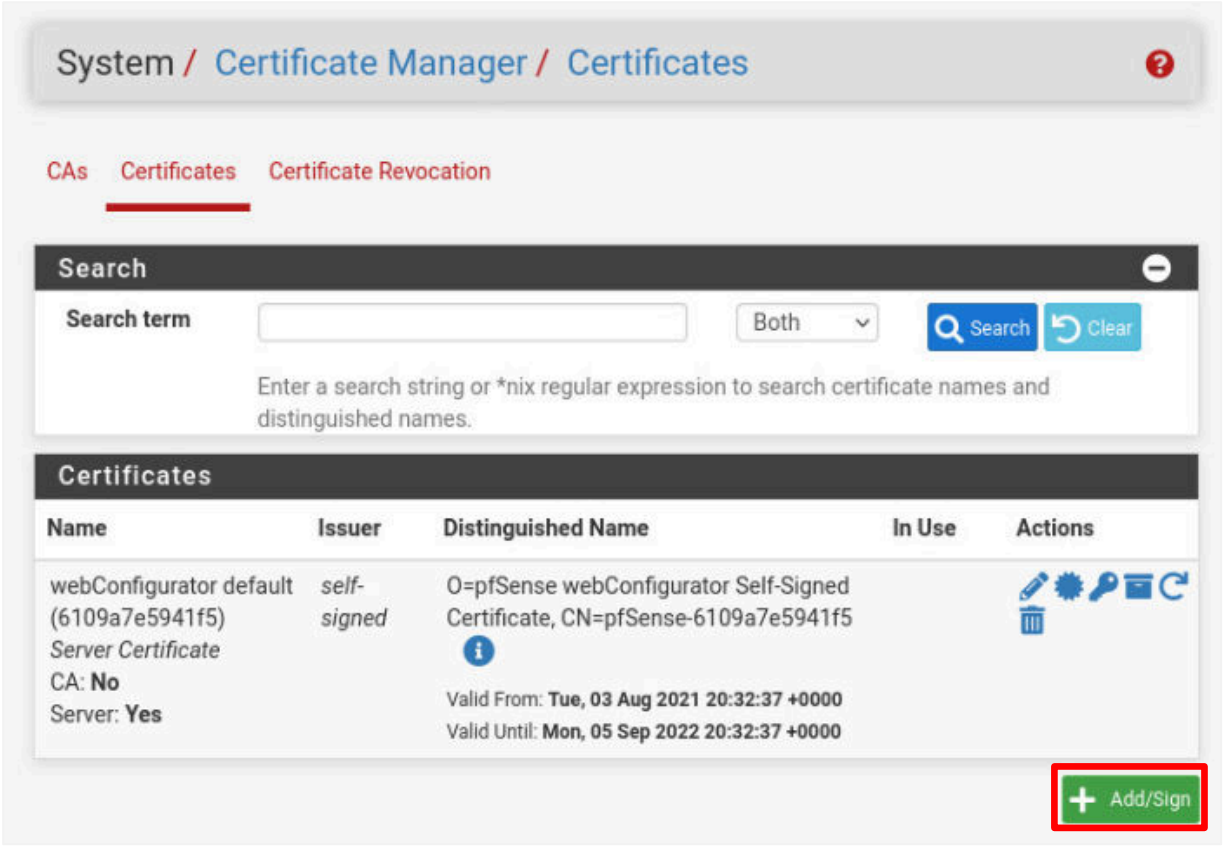
6. You should see the **Certificate Authorities** entry in the CA list. Now, you will create the server certificate to go with the **Certificate Authority.**



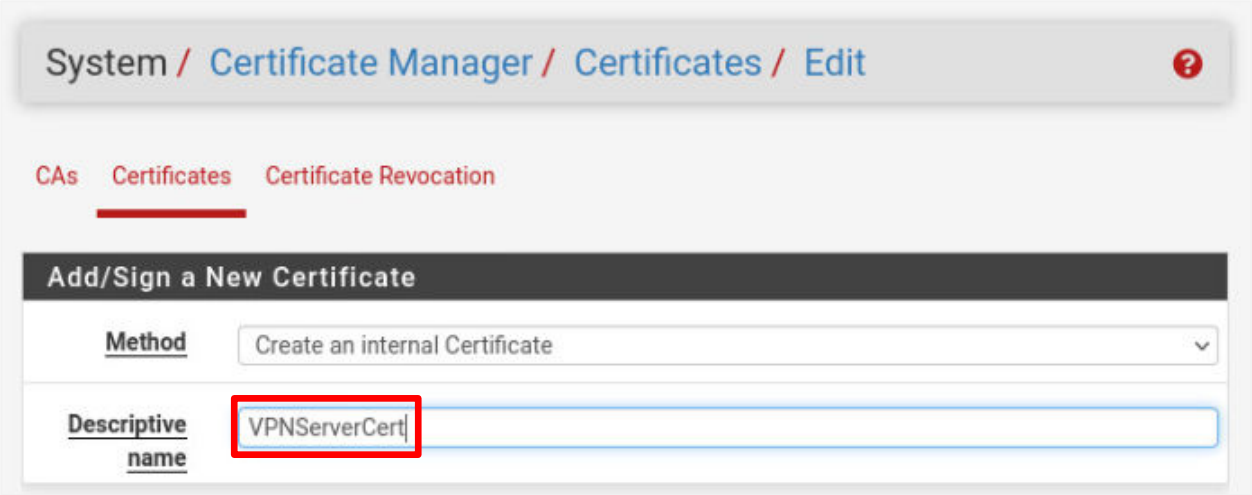
7. Click on **Certificates.**



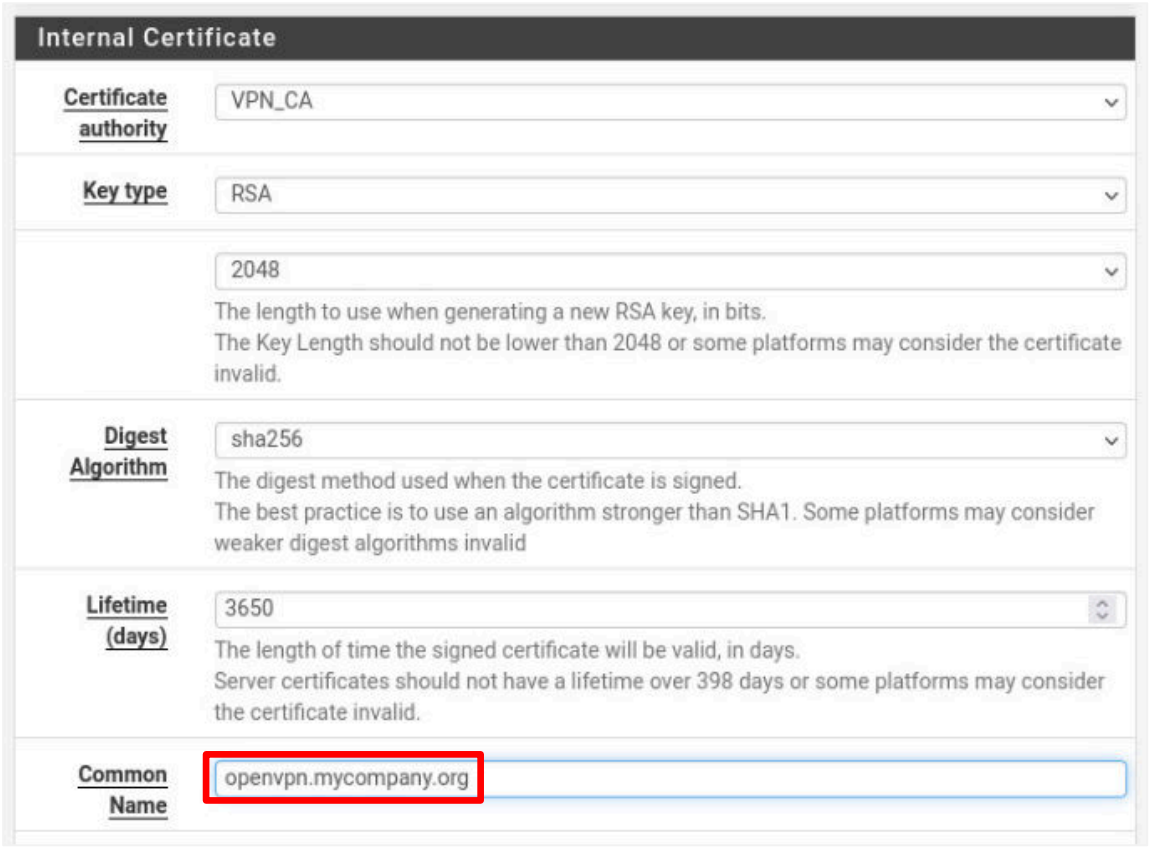
8. Click the **+Add/Sign** button.



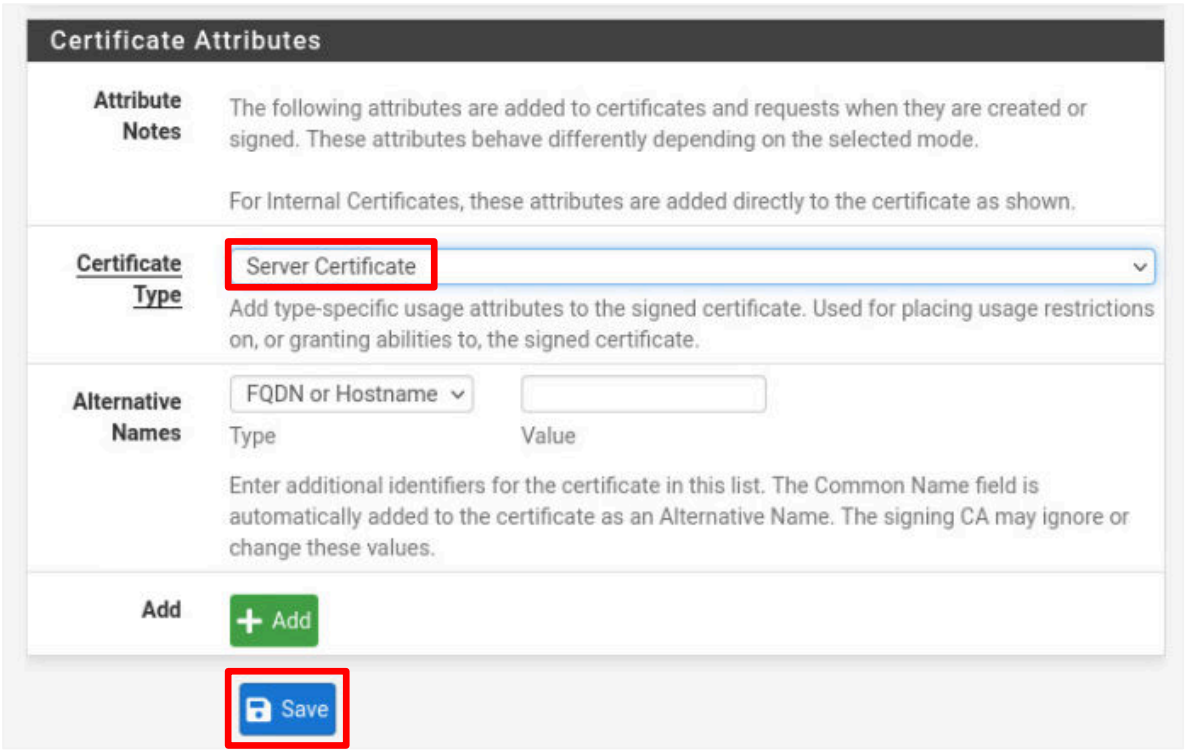
9. Under the *Add/Sign a New Certificate* section, type `VPNServerCert` as the *Descriptive Name*.



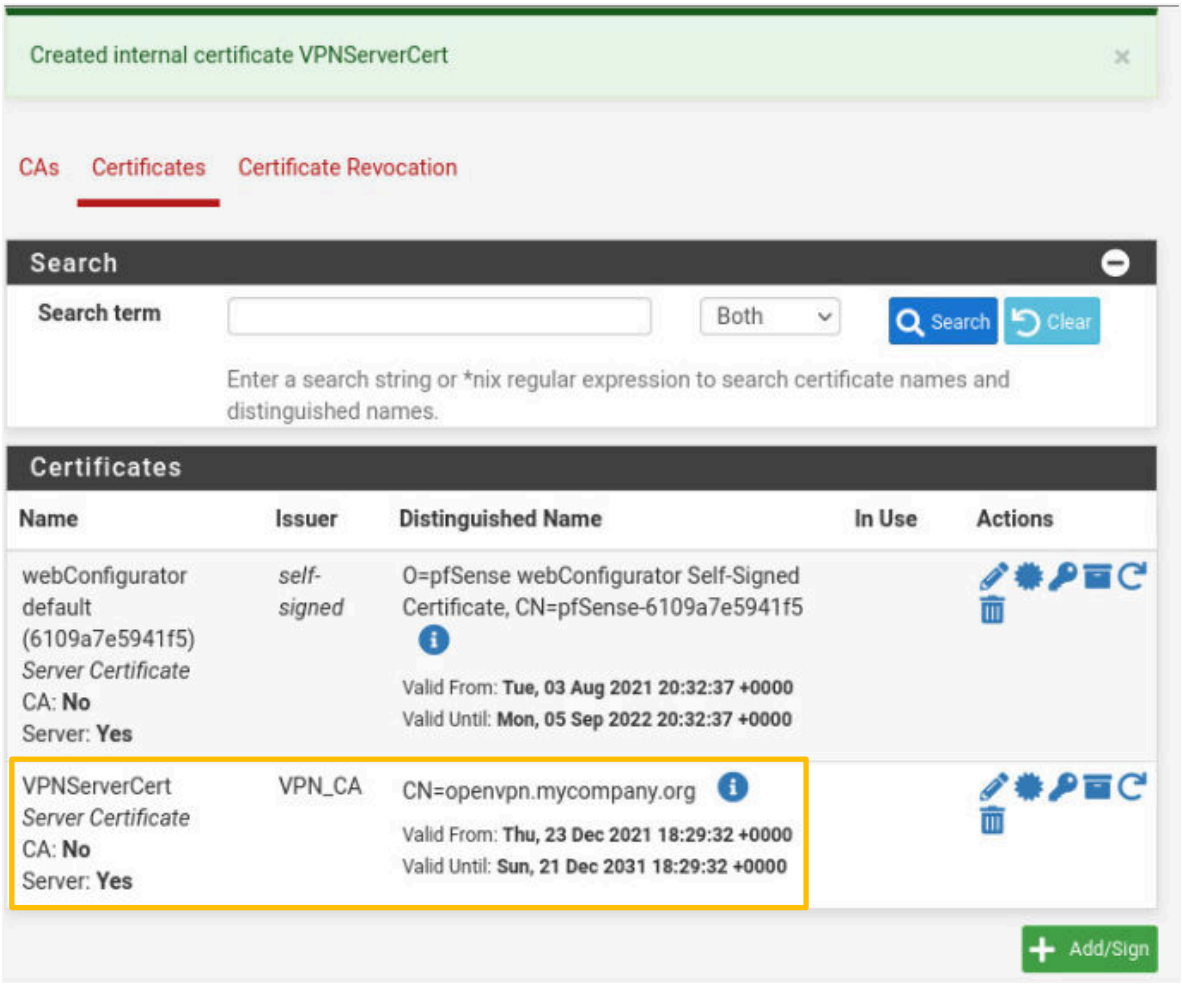
10. Scroll down the page to the *Internal Certificate* section, and type `openvpn.mycompany.org` in the *Common Name* section.



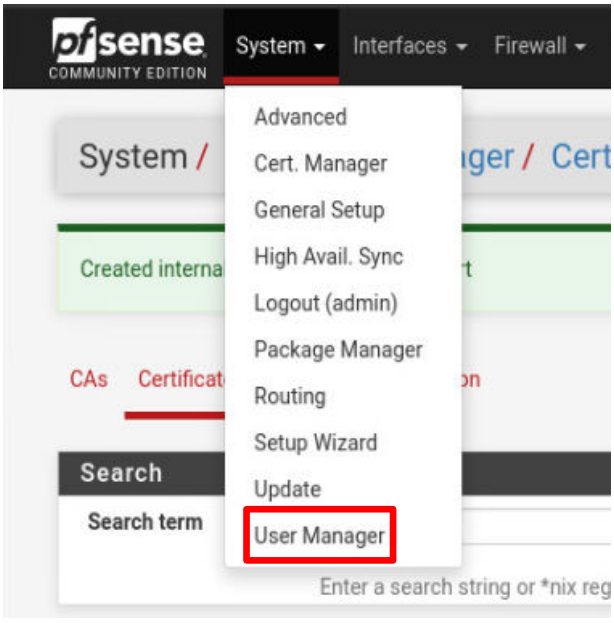
11. The remaining *Internal Certificate* fields can be left at their default values. Scroll down to the lower part of the window. In the *Certificate Attributes* section, in the *Certificate Type* field, use the list arrow to select **Server Certificate**. Then, click the **Save** button at the bottom of the window.



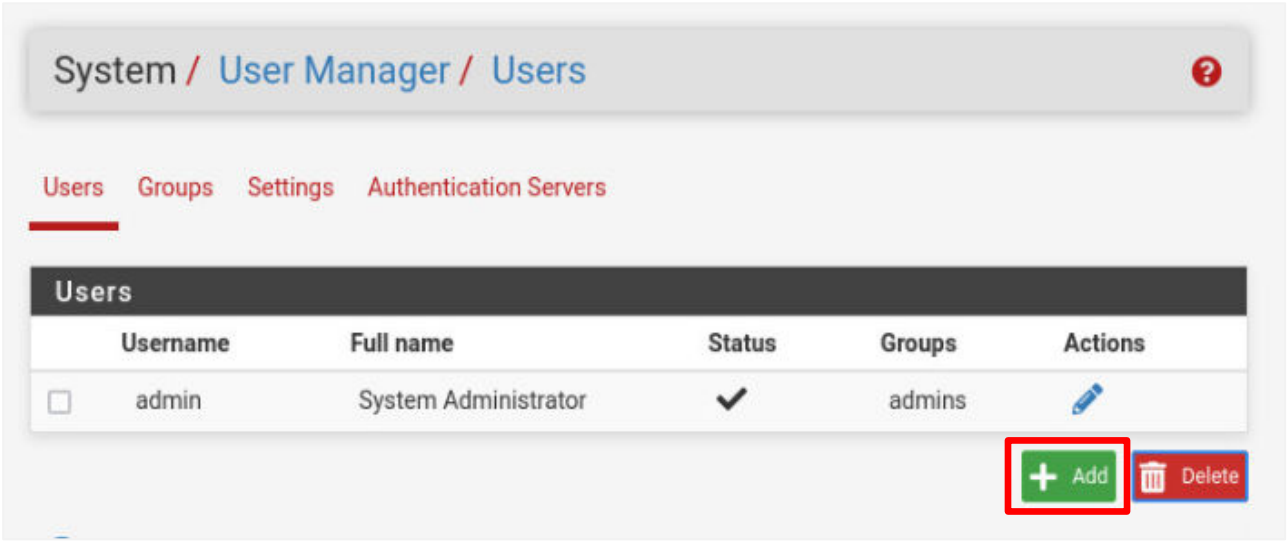
You should now see that the server certificate *VPNServerCert* has been created.



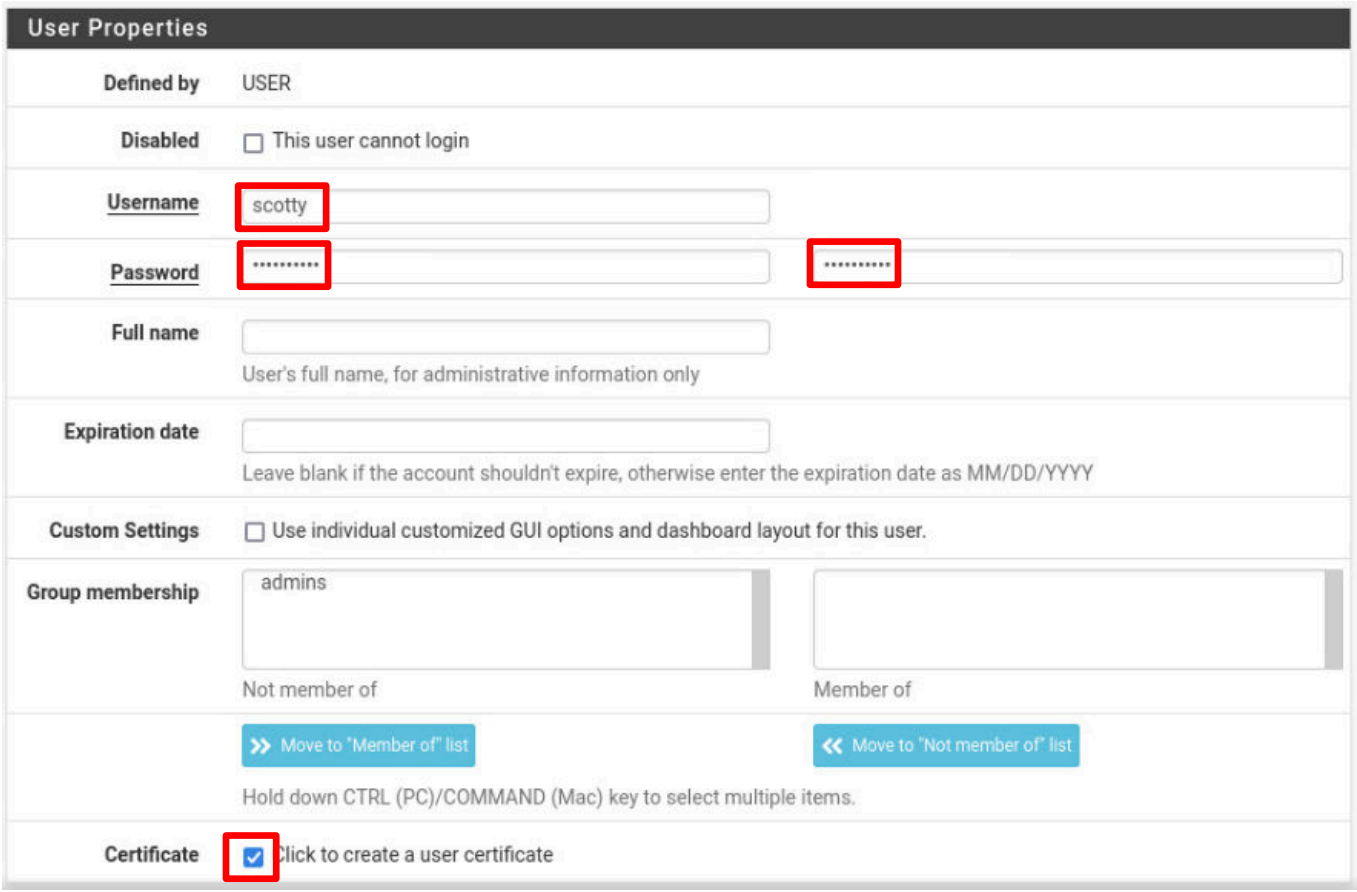
12. Finally, you'll create the User Certificate that will be installed on the remote device. At the top of the *pfSense* window, click on **System** and then click on **User Manager**.



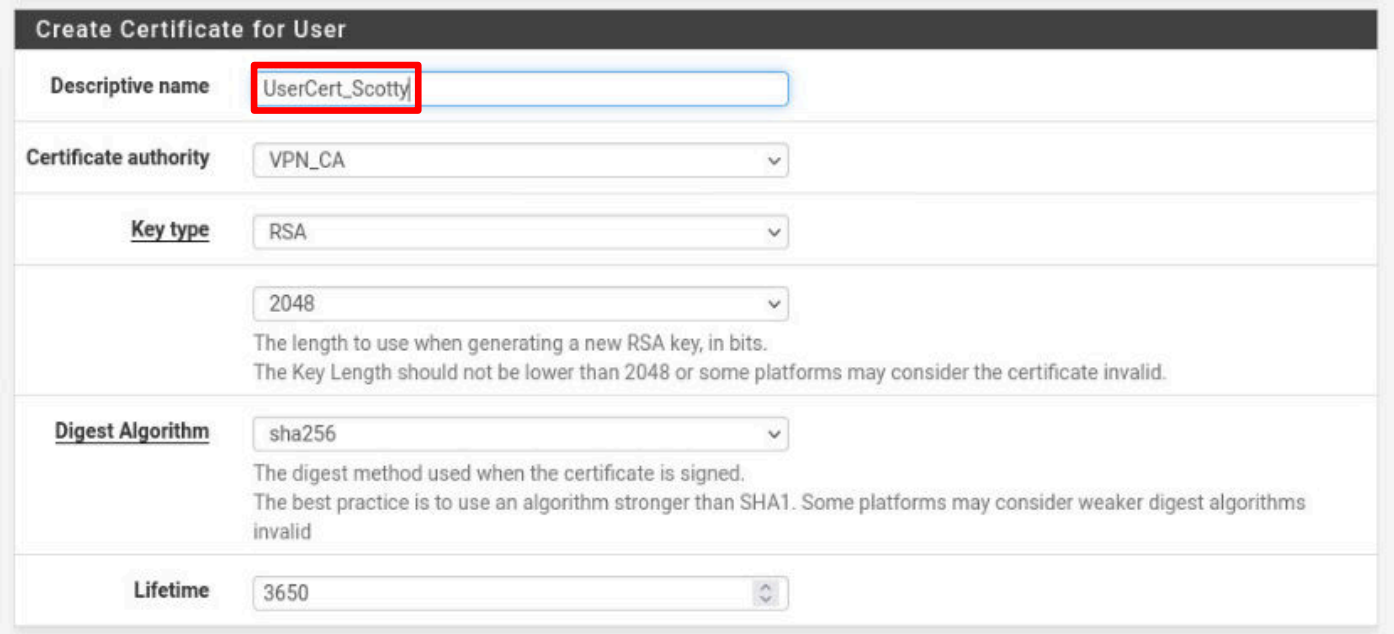
13. On the *System/User Manager/Users* page, click on the **+Add** button to create a new user who will be allowed access to the VPN.



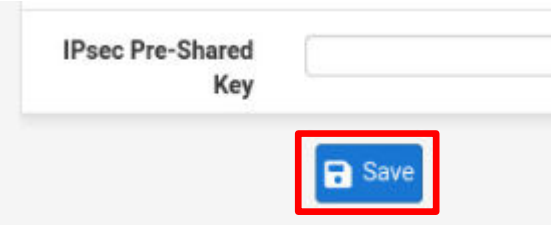
14. On the *System/User Manager/Users/Edit* page, type `scotty` as the *Username*, `Password1` for the *Password,* and again to confirm. Then, click the **Certificate** checkbox to create a user certificate.



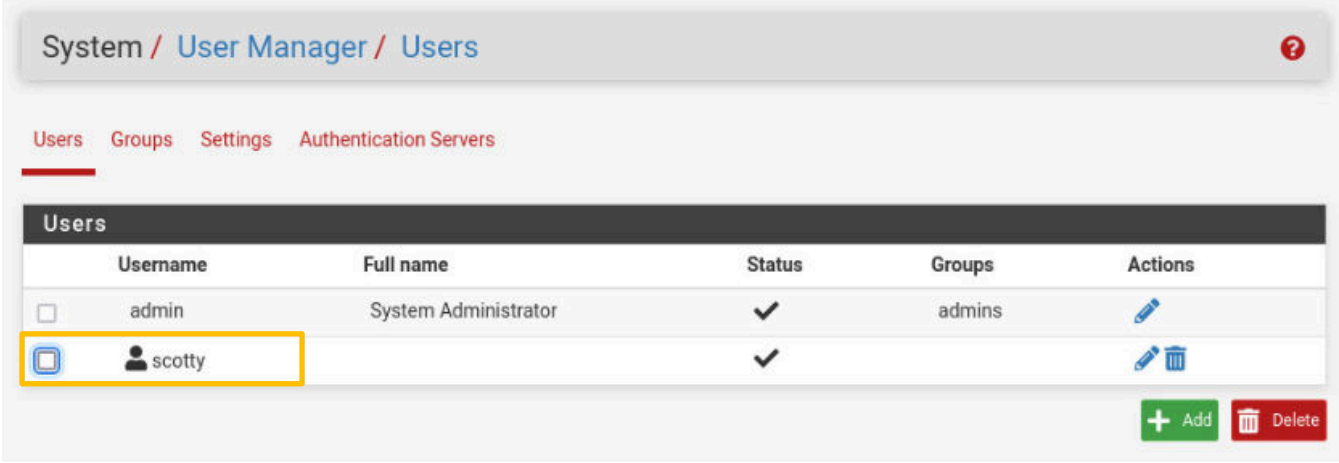
15. Scroll down the window to the *Create Certificate for User* section and type `UserCert_Scotty` as the *Descriptive Name*. Leave all of the other fields at their defaults.



16. Scroll to the bottom of the page and click the **Save** button.



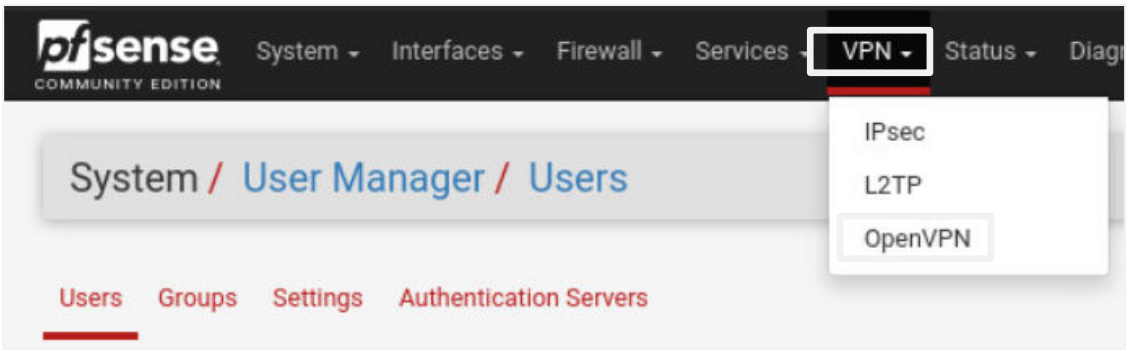
You will see the new user added to the list.



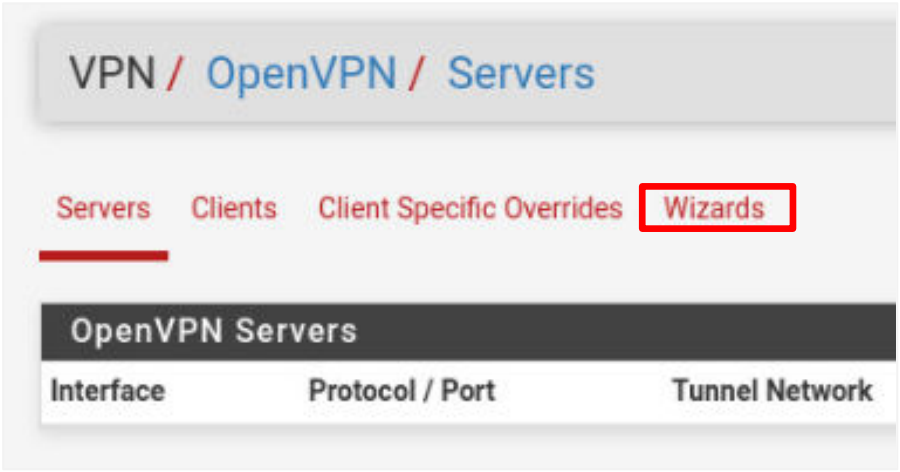
17. Remain on the *MintOS* computer and continue to the next task.

3.2 Setup OpenVPN on the pfSense Firewall

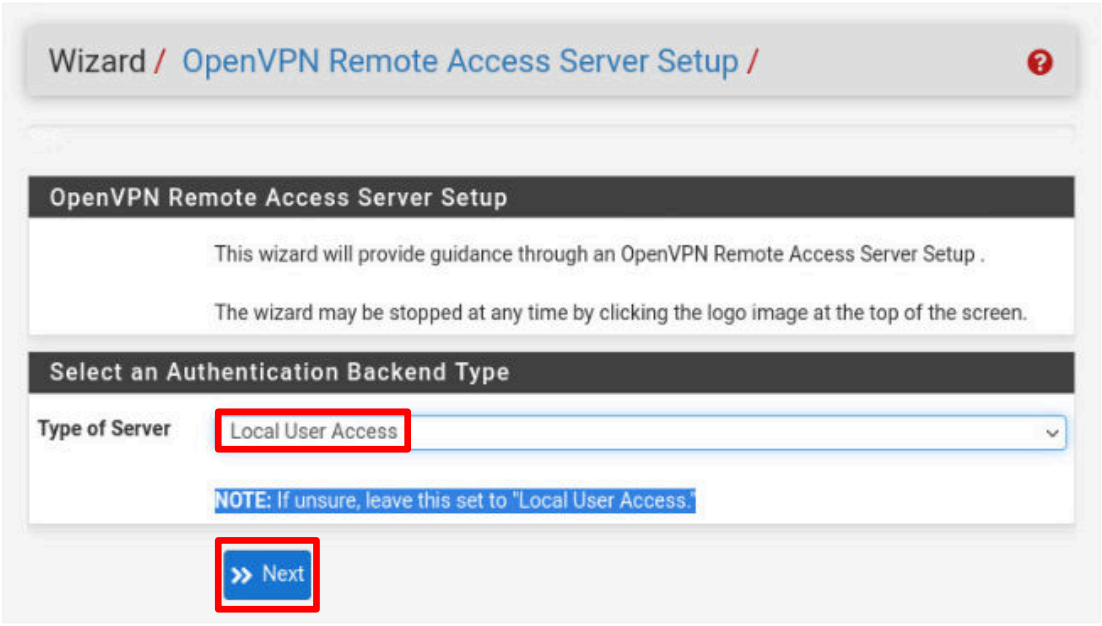
1. Click **VPN** on the top menu and then click on **OpenVPN** in the dropdown list.



2. On the *VPN/OpenVPN/Servers* page, click **Wizards** to set up the *OpenVPN* server.

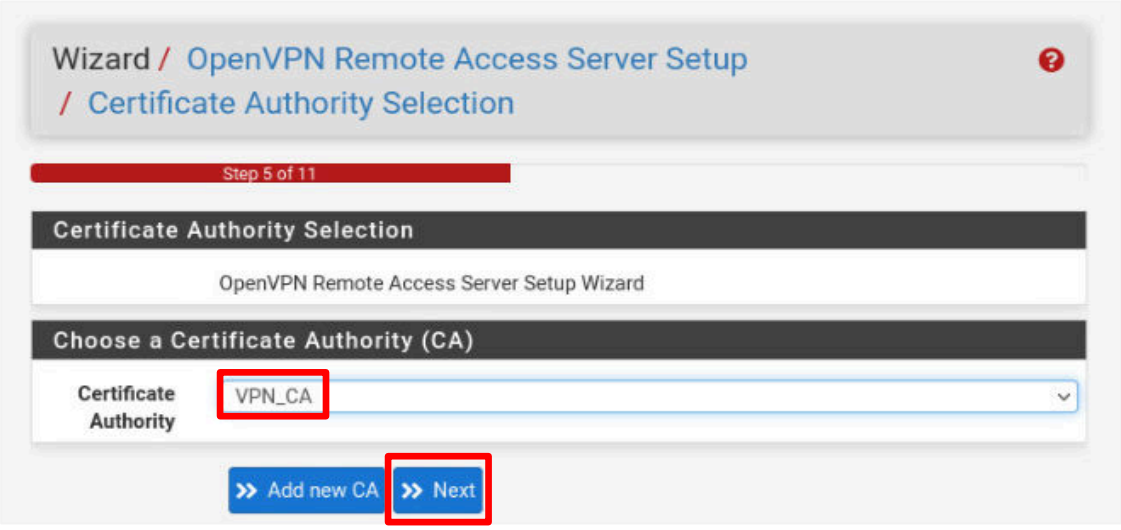


3. Make sure **Local User Access** is selected and click **Next**.



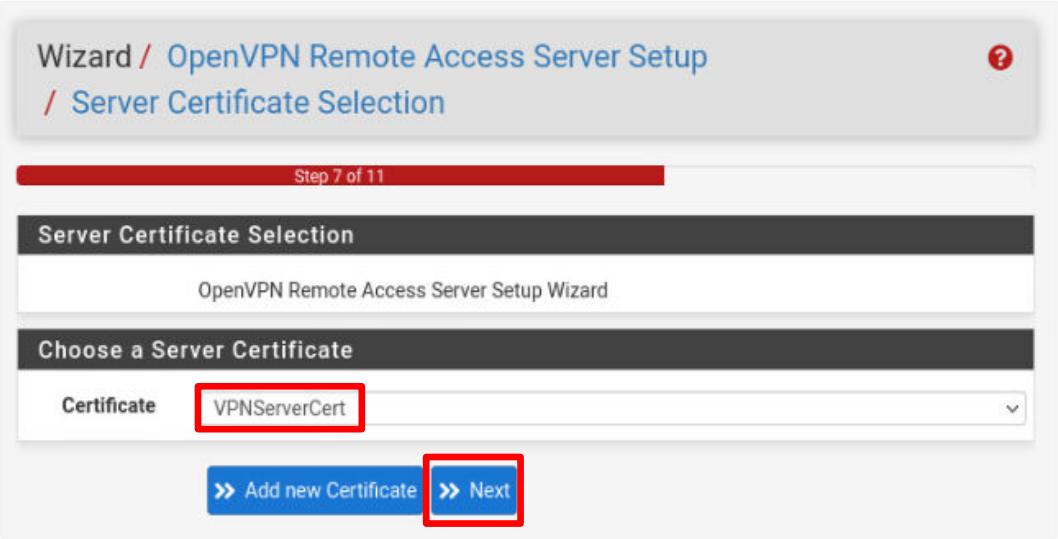
The above selection is for the type of authentication service to allow access to the VPN. By selecting **Local User Access** authentication will use the local database of users on the *OpenVPN* server, where you have already created one user in the previous task. You could select **RADIUS** or **LDAP** (which can be used for **Active Directory**) for more consolidated authentication.

4. Make sure **VPN_CA** is selected, then click **Next**.



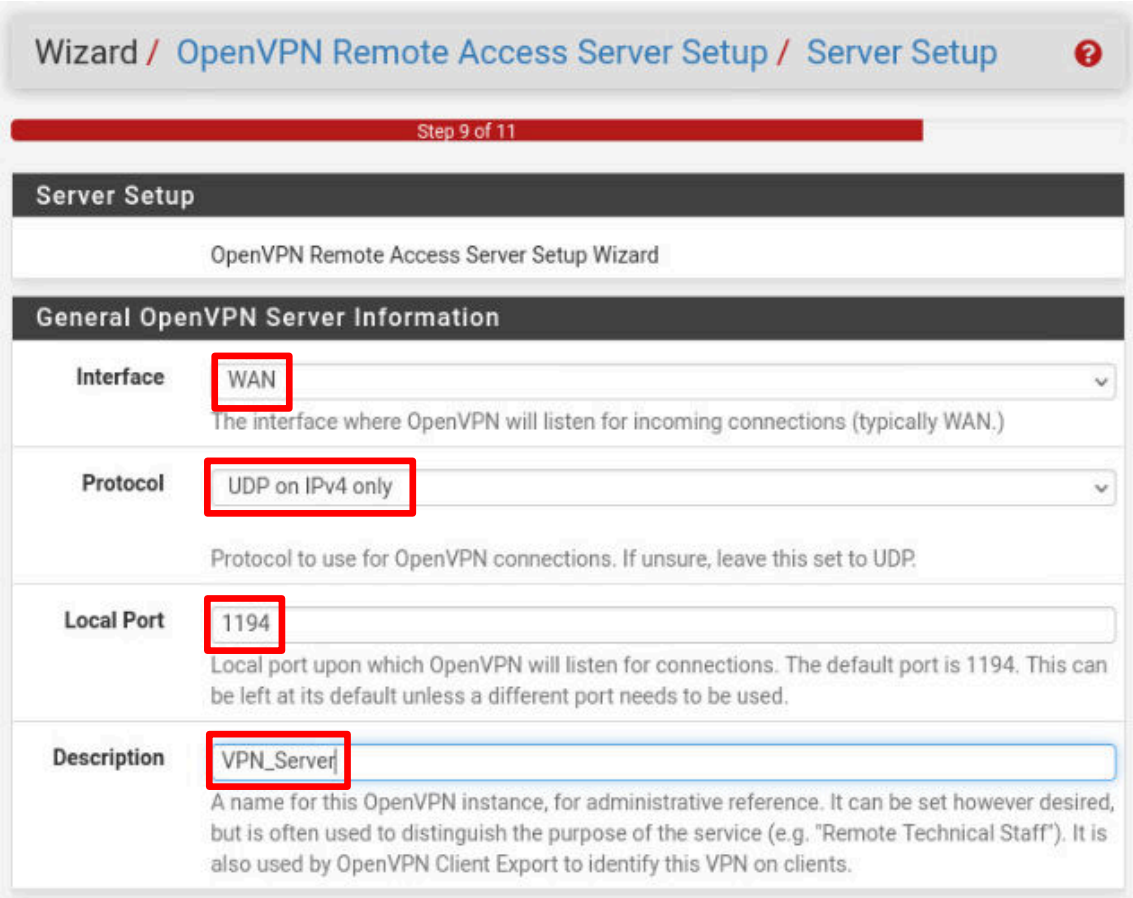
If it does not show **VPN_CA**, use the list arrow on the right to show a list of all of the CAs that were created and then select it from there. If **VPN_CA** is not in that list, you will have to go back to the previous task and recreate the CA.

5. Make sure **VPNServerCert** is selected, then click **Next**.



6. The next page has several sections that will need to be filled in. In the *General OpenVPN Server Information* section, configure the following:

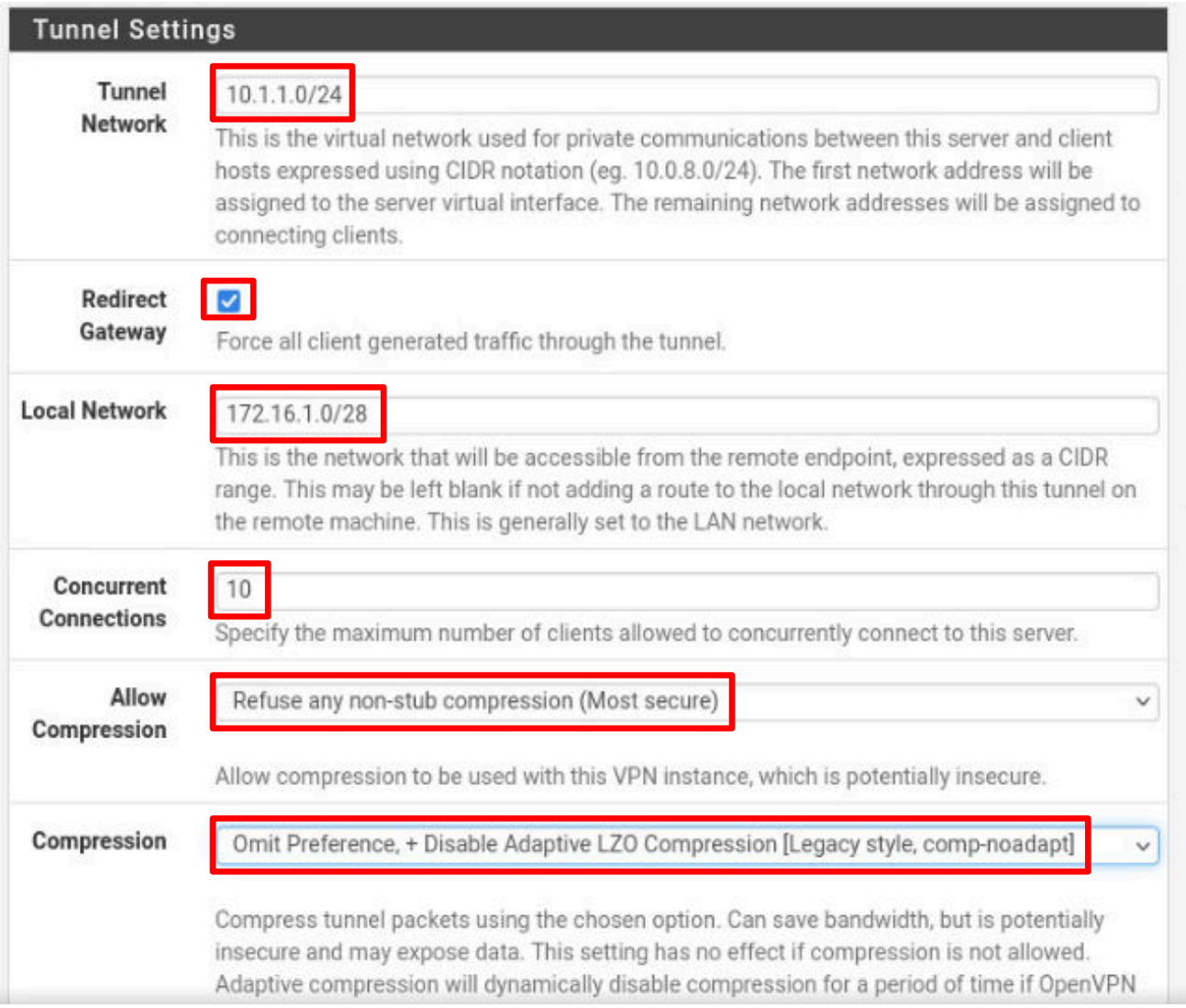
Interface	**WAN** (should already be selected)
Protocol	**UDP on IPv4 only** (should already be selected)
Local Port	1194 (should already be selected)
Description	VPN_Server



7. Scroll down to the *Tunnel Settings* section and type the following in the indicated fields:

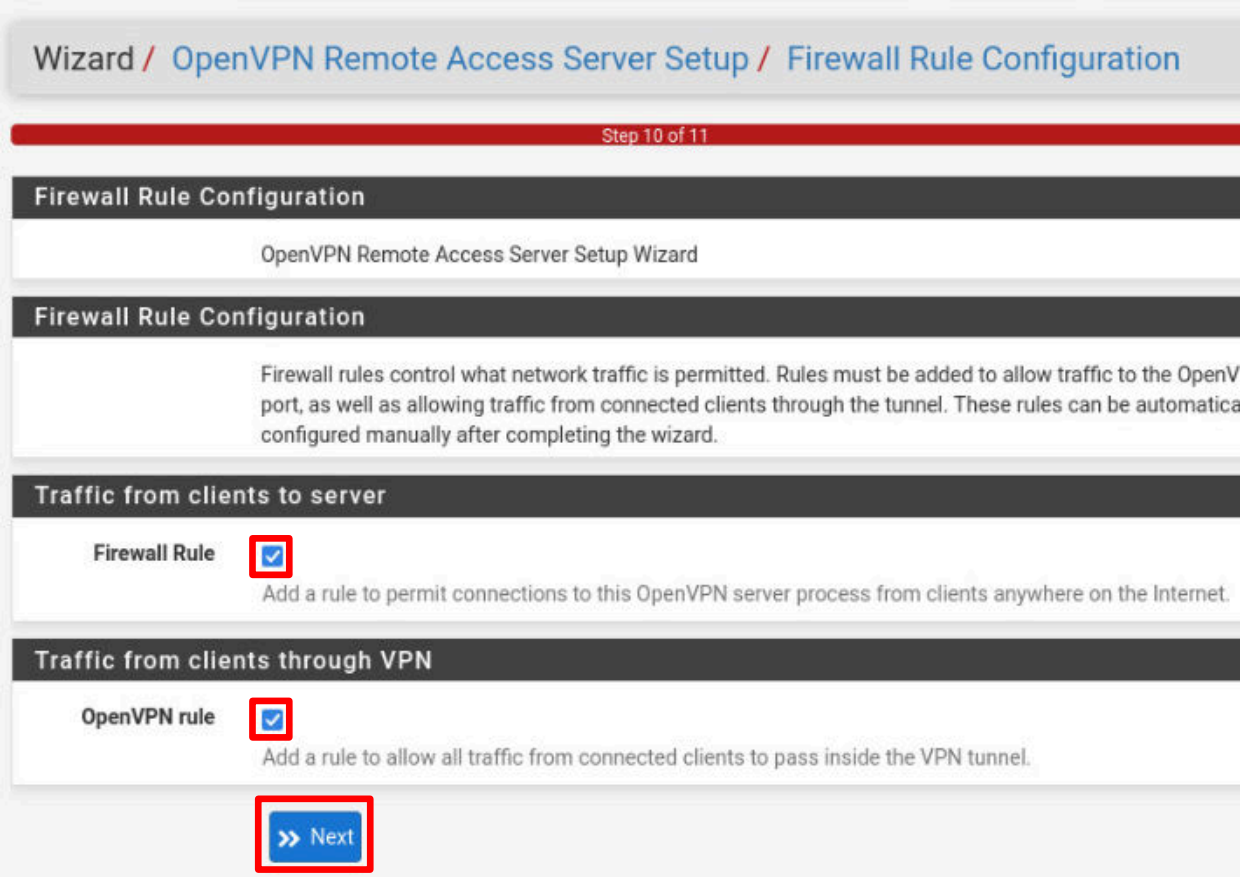
Tunnel Network	`10.1.1.0/24`
Redirect Gateway	**Checked**
Local Network	`172.16.1.0/28` (VPN clients will only be able to access the **DMZ)**
Concurrent Connections	`10`
Allow Compression	**Refuse any non-stub compression (Most secure)** (should already be selected)
Compression	**Omit Preference, + Disable Adaptive LZO Compression**

Leave the rest of the entries in the section at their default values.

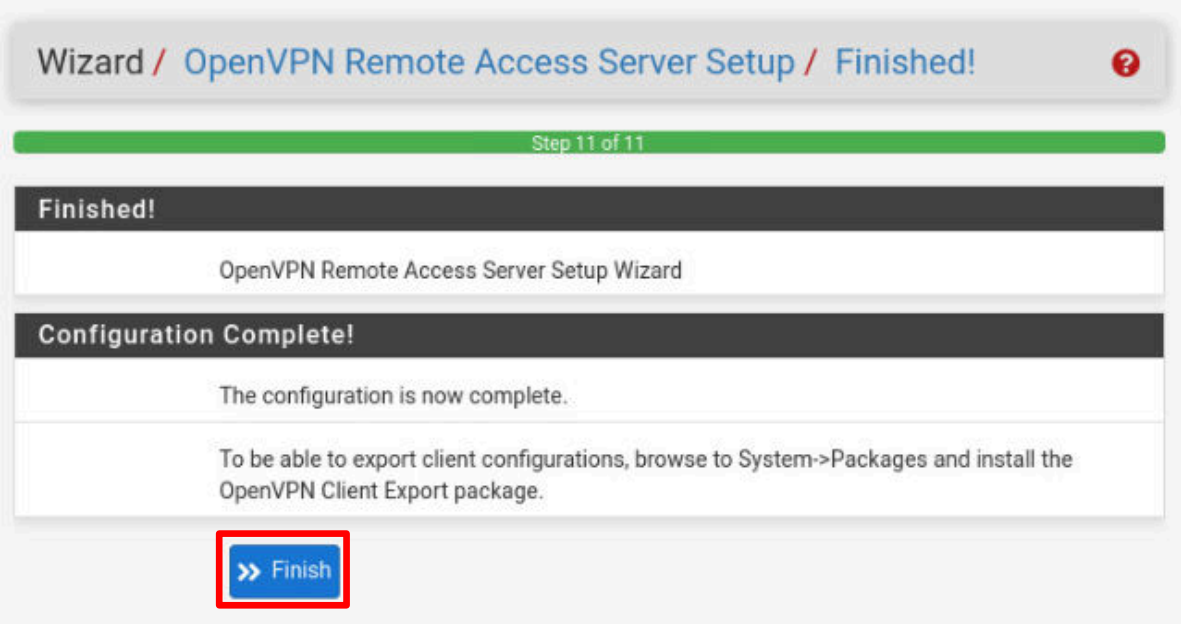


8. Scroll to the bottom of the page and click **Next.**

9. On the *Firewall Rule Configuration* page, confirm the **Firewall Rule** and **OpenVPN rule** checkboxes are checked. Then, click **Next**.



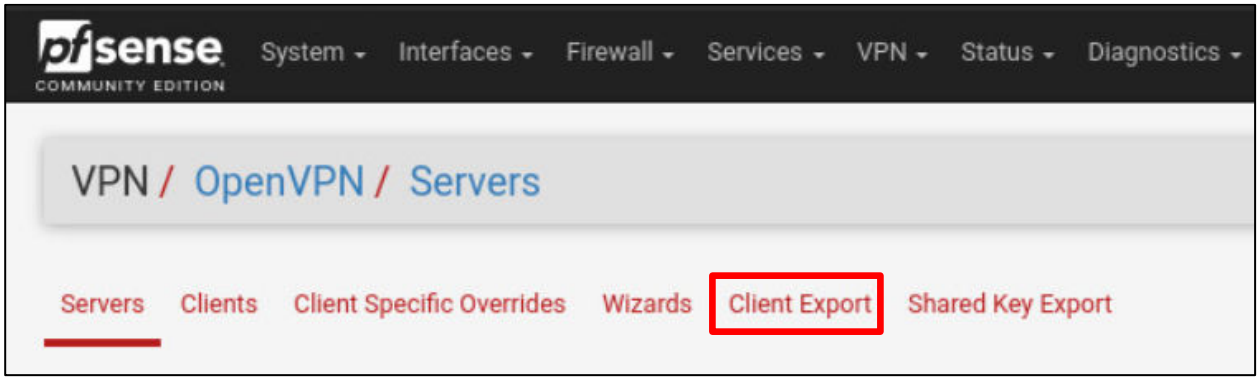
10. On the final page of the wizard, click the **Finish** button.



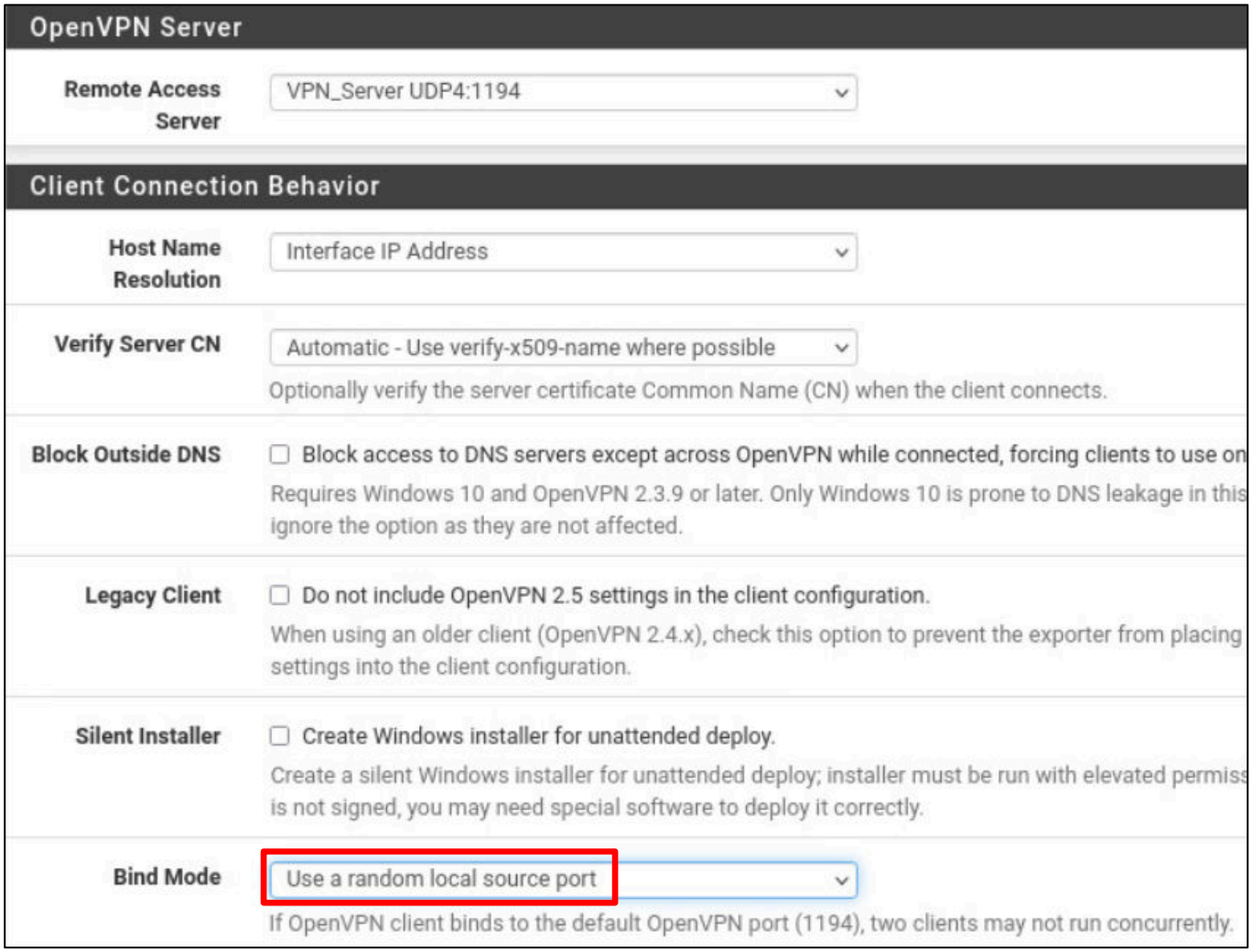
11. Remain in the *MintOS* tab and leave the *pfSense* web page open and proceed to the next task.

3.3 Export VPN Client Configuration Data

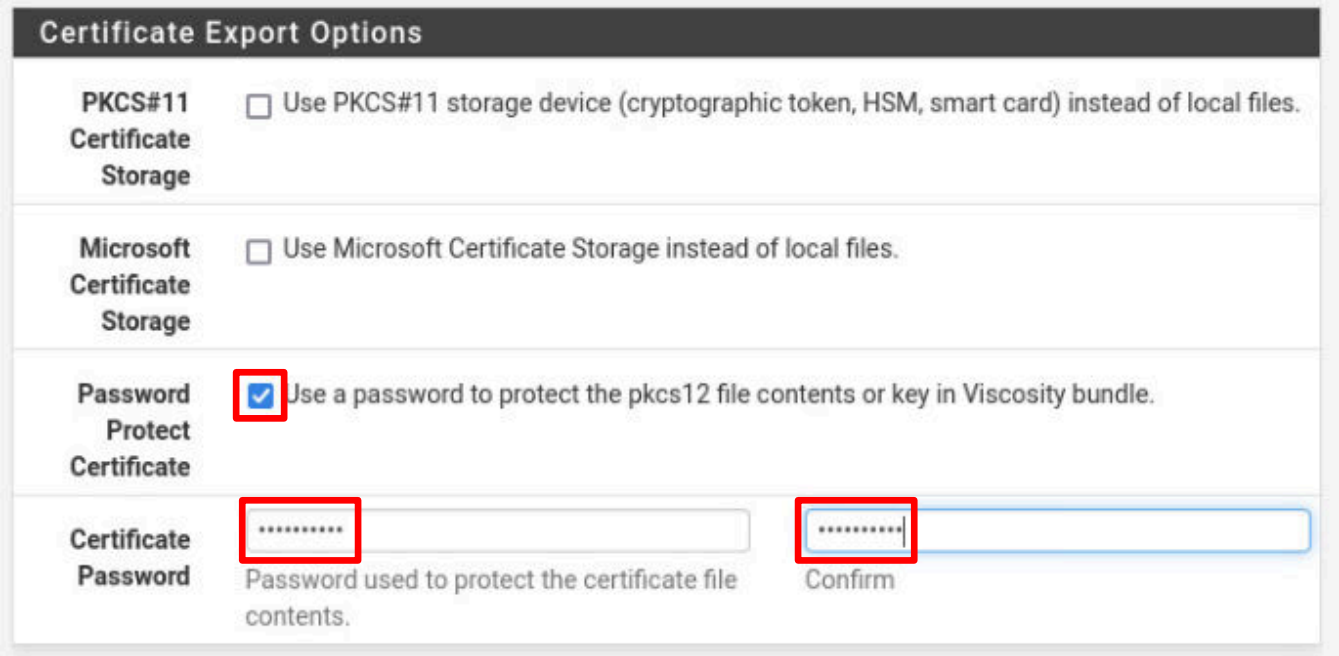
1. On the *VPN/OpenVPN/Servers* page, click on **Client Export**.



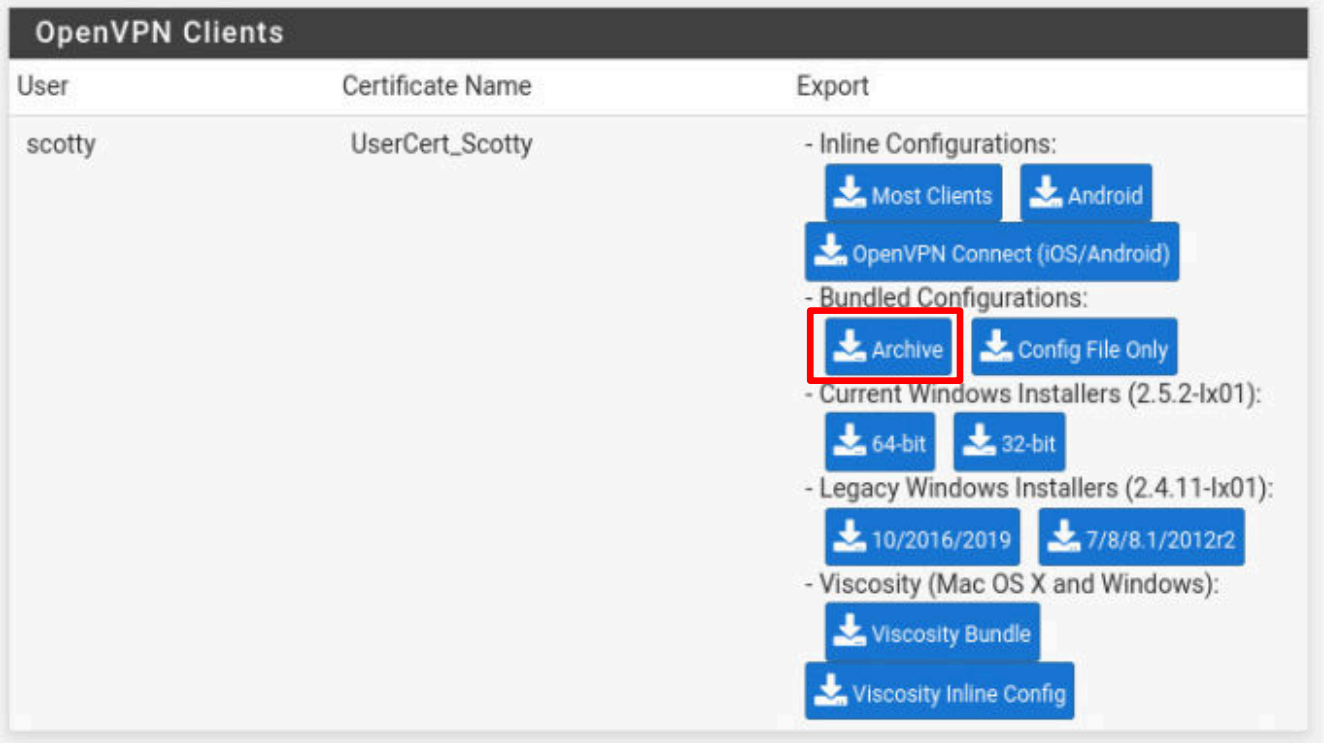
2. In the *Client Connection Behavior* section, click the list arrow for *Bind Mode* and select **Use a random local source port.**



3. In the *Certificate Export Options* section, click the **Password Protect Certificate** checkbox. Type `Password1` for the *Certificate Password* and then type `Password1` again to confirm.



4. Scroll down towards the bottom to the *OpenVPN Clients* section. Underneath the *Export* column, click on the **Archive** button for *Bundled Configurations*.



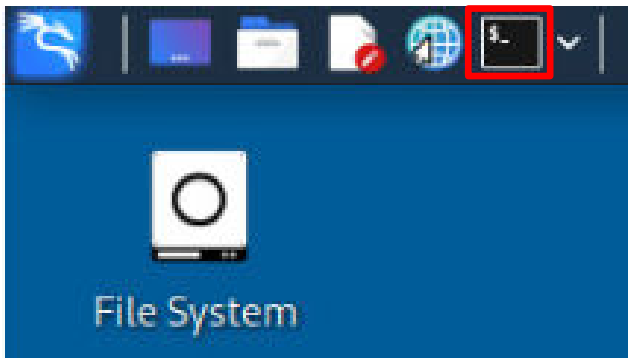
The *OpenVPN* client file will be saved in the directory **/home/sysadmin/Downloads.**

5. Minimize the **Firefox** browser window.

3.4 Transfer, Configure and Run the VPN Client

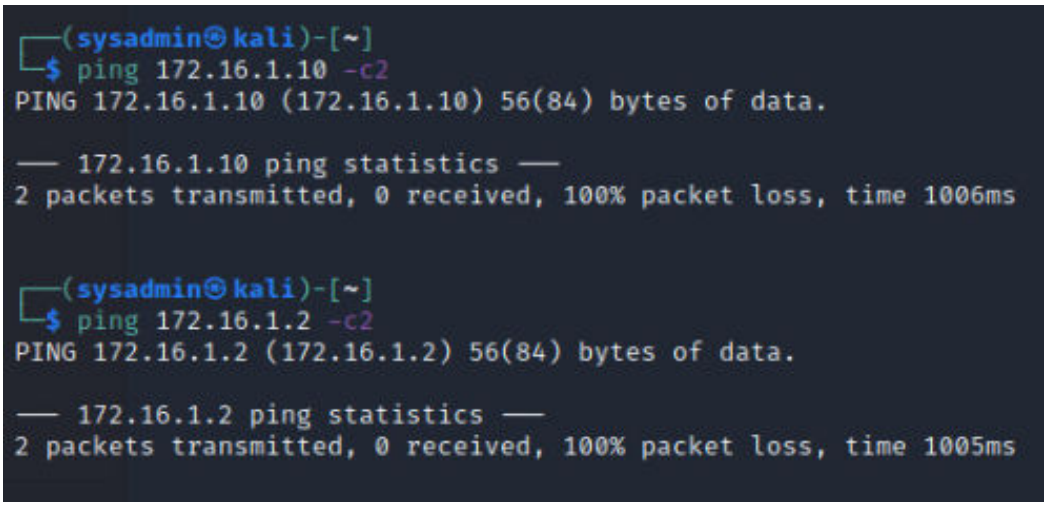
You will need to transfer the *OpenVPN* configuration from the previous task to the *Kali* computer. Normally the file would be copied either by removable media or a secure transfer. The *NETLAB+* environment does not have a removable media option, so the easiest way to accomplish the transfer is an **SMB** file share using *Samba*. The **SMB** configuration has already been set up in the **LabFiles** folder on the desktop and has been shared with the name **xfer**.

1. Set the focus to the **Kali** tab and click on the **Terminal** icon in the taskbar to start a terminal session.



2. Before we set up and use the *OpenVPN* client, make sure that you cannot access the services on the **DMZ** network. From the terminal session, try to ping the *UbuntuSRV* and *OSSIM* hosts by typing the following commands:

```
ping 172.16.1.10 -c2
ping 172.16.1.2 -c2
```

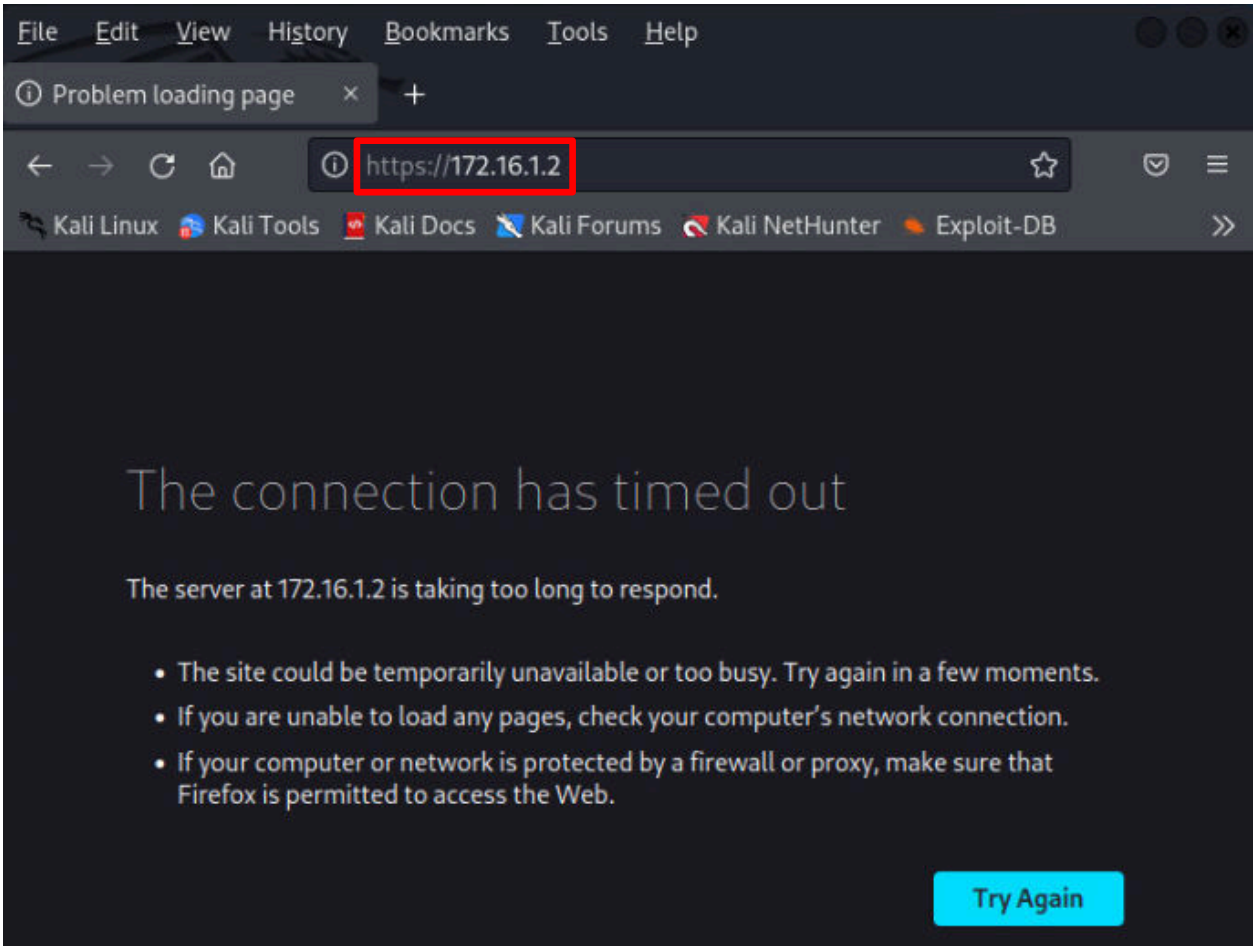


3. From the terminal, try to SSH to the *UbuntuSRV* by typing the following command:

```
ssh 172.16.1.10
```

After a couple of minutes, the SSH connection attempt will time out.

4. For one last test, open the **Firefox** web browser and try connecting to the *OSSIM Web Manager* by typing the address `https://172.16.1.2`.

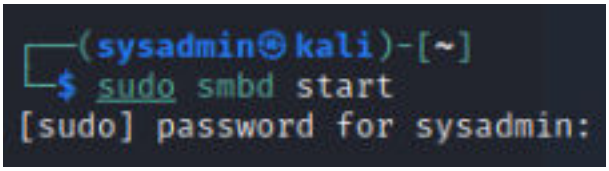


After a couple of minutes, the connection will time out.

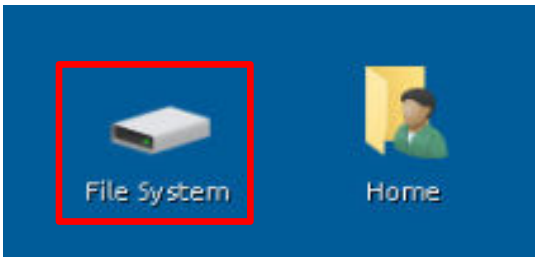
5. Close the browser window.

6. In the terminal window, type the following command to start the *Samba* service on the *Kali* computer. If asked for the **[sudo] password for sysadmin**, type: `NDGlabpass123!`

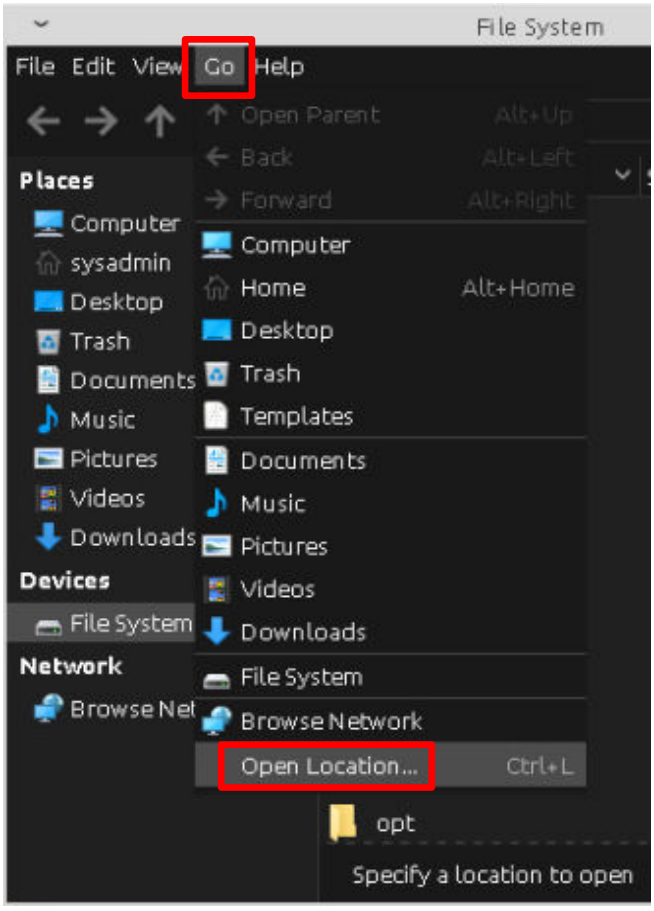
```
sudo smbd start
```



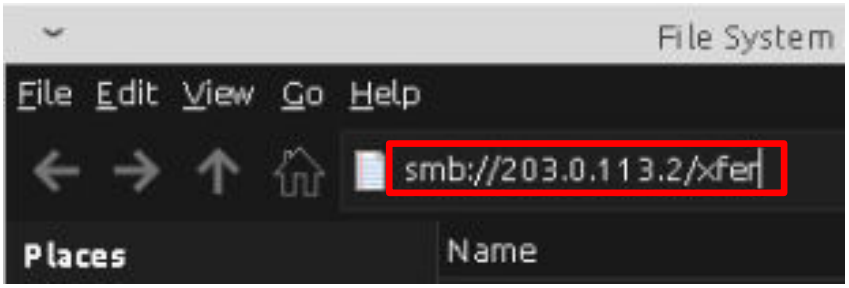
7. Set the focus on the **MintOS** computer and then double-click on the **File System** icon on the desktop:



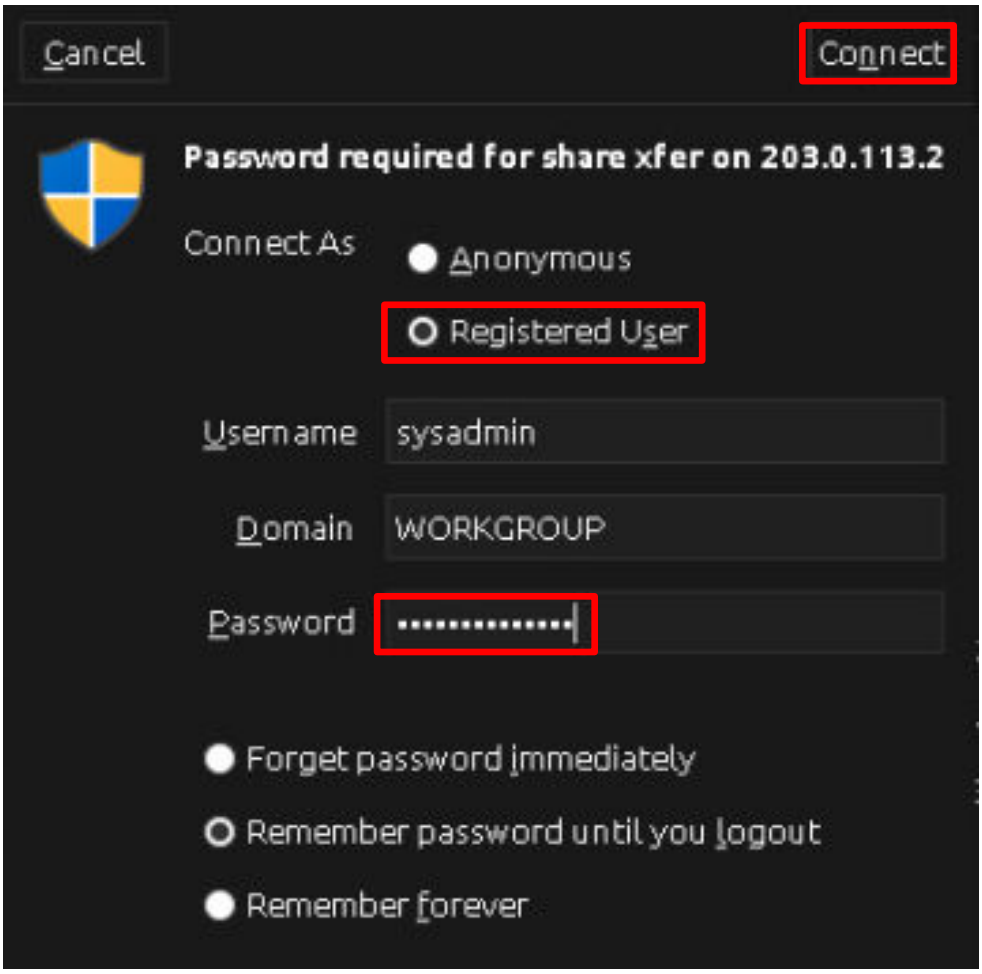
8. On the *File System* window, click on the **Go** menu item, and click on **Open Location** on the dropdown menu.



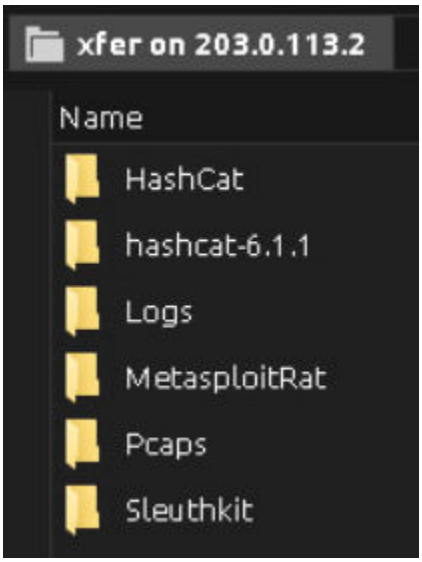
9. In the address bar, type in the location `smb://203.0.113.2/xfer` and press **Enter**.



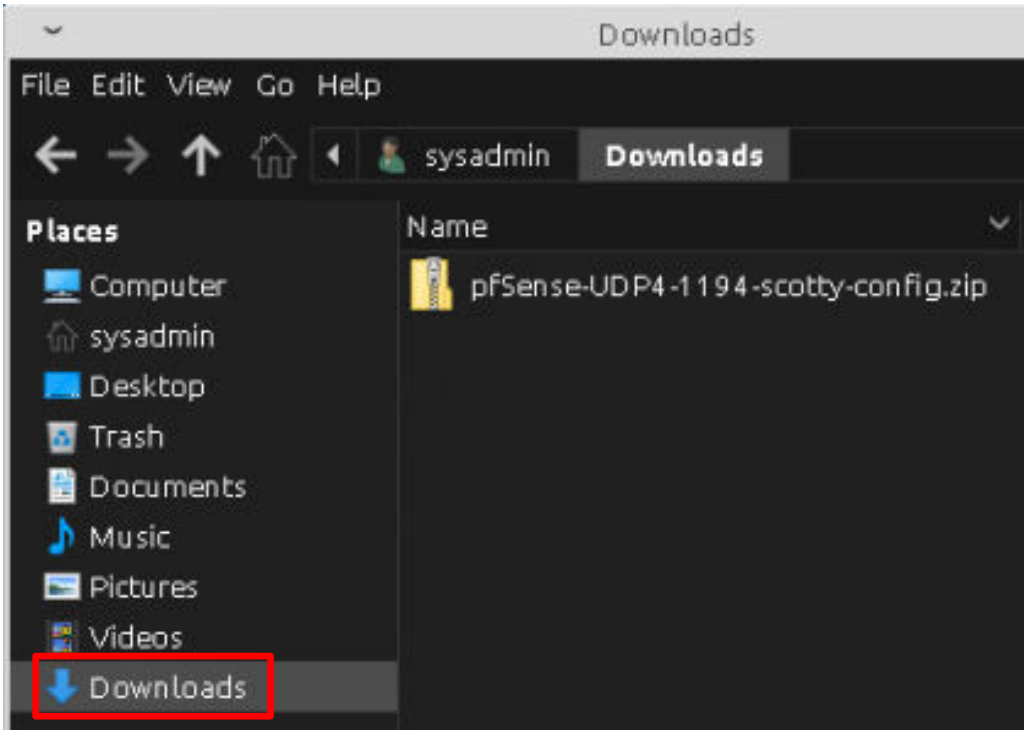
10. On the *Authentication* window, asking for the share password, click on the **Registered User** radio button, confirm the *Username* is `sysadmin` and the *Domain* is `WORKGROUP`. In the *Password* field, type `NDGlabpass123!` and then click **Connect** in the upper-right of the window.



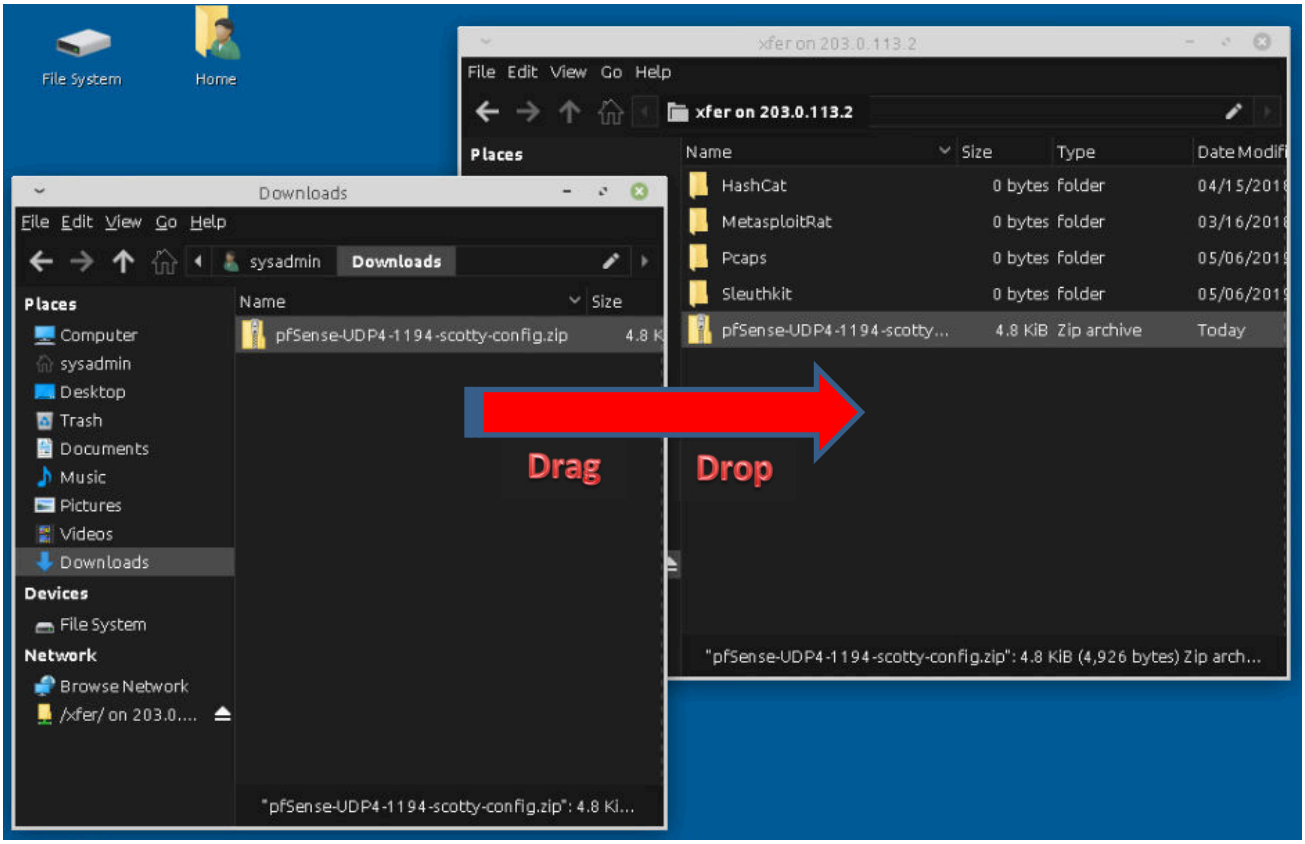
You should see the window with the six folders that are in the *LabFiles* directory.



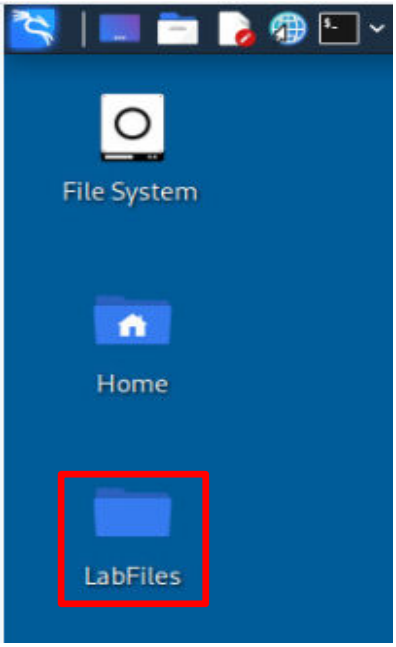
11. Double-click on the **File System** icon on the desktop again to open another *File System* instance.
12. Under **Places** on the left side of the window, click on **Downloads**.



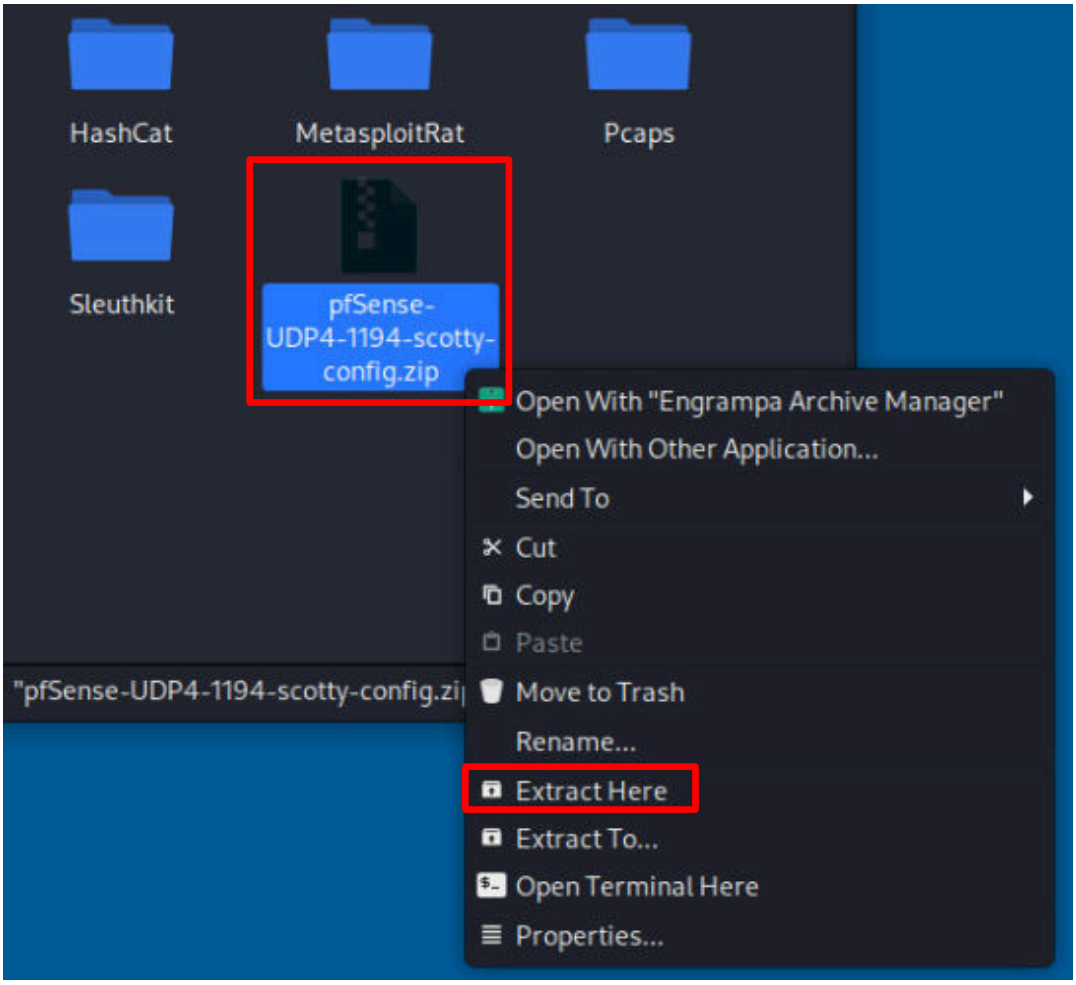
13. Drag and drop the **pfSense-UDP4-1194-scotty-config.zip** file in the *Downloads* folder to the *xfer on 203.0.113.2* folder (which is on the *Kali* computer).



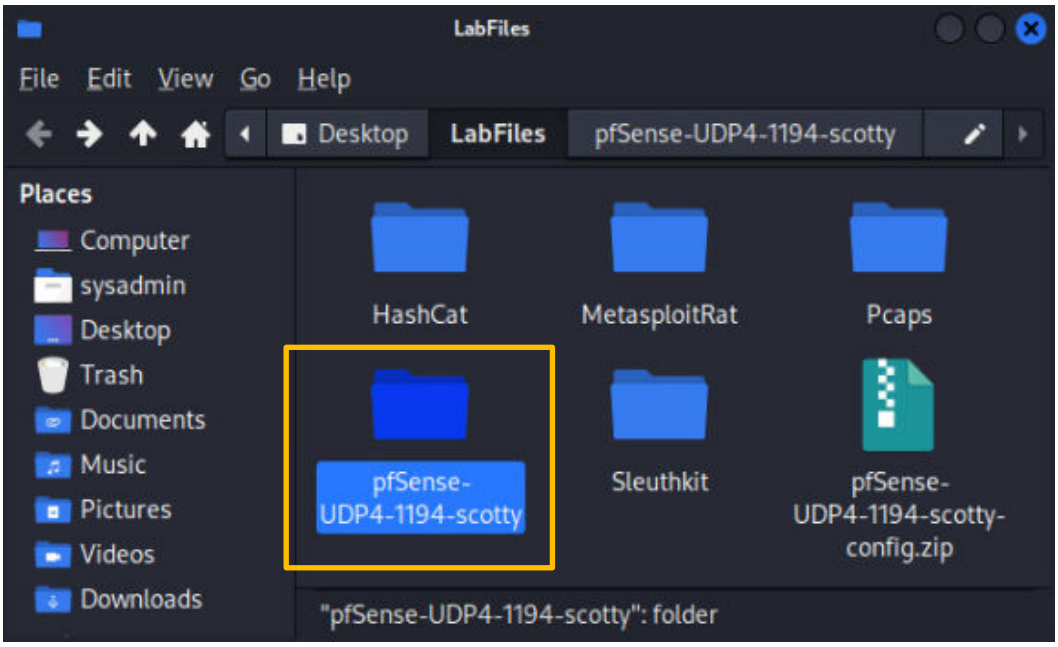
14. Close the two **File System** windows.
15. Return to the **Kali** computer. On the desktop, double-click to open the **LabFiles** folder.



16. Right-click on the **pfSense-UDP4-1194-scotty-config.zip** file and click on **Extract Here** to unzip the *OpenVPN* user configuration files.

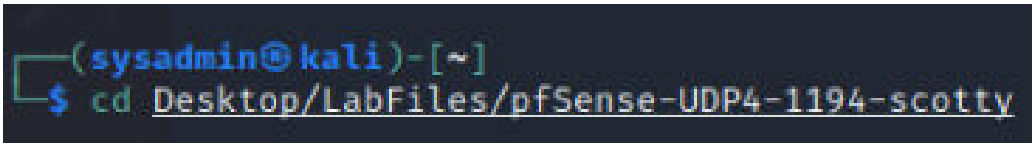


You should now see the **pfSense-UDP4-1194-scotty** folder.



17. In the terminal window, type the following command to change to the **pfSense-UDP4-1194-scotty** directory:

```
cd Desktop/LabFiles/pfSense-UDP4-1194-scotty
```

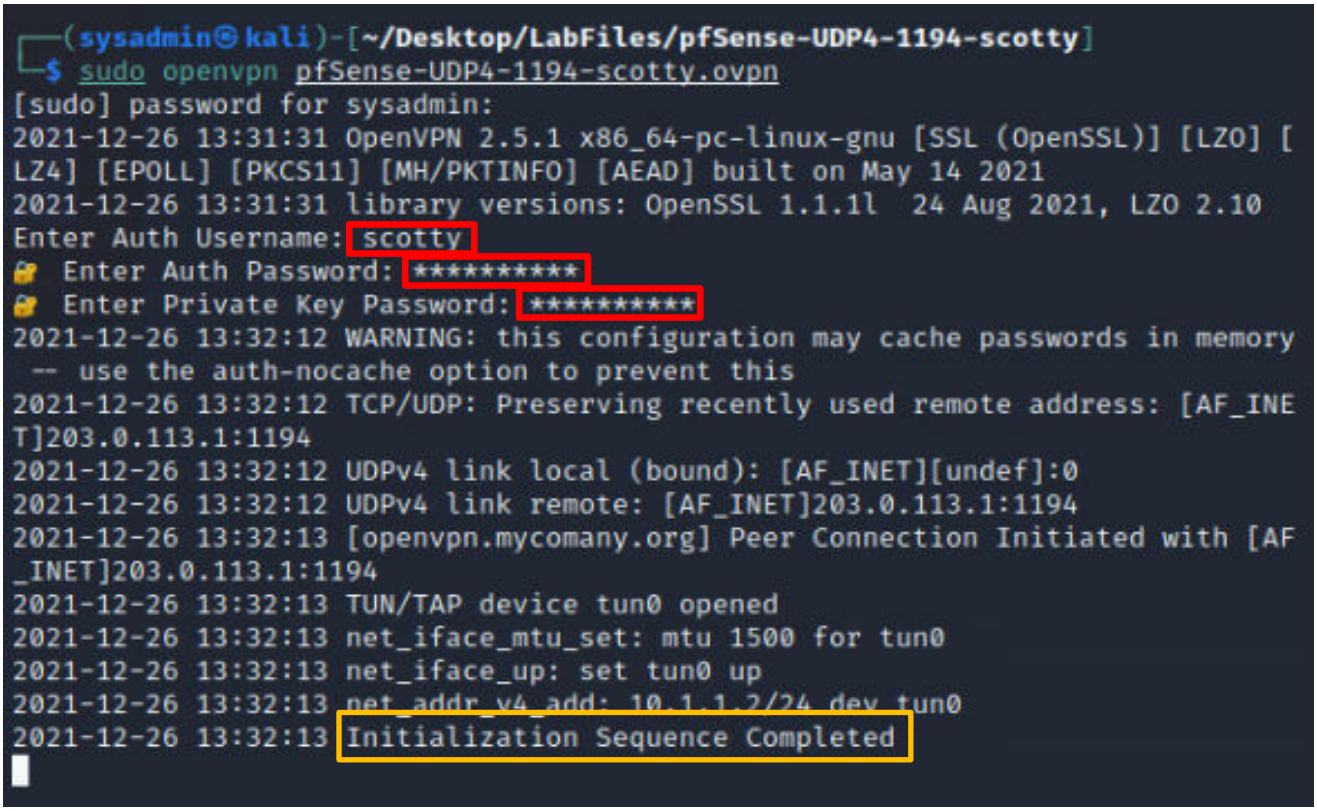


18. Type the following command to start the *OpenVPN* client. If asked for the **[sudo] password for sysadmin**, type: `NDGlabpass123!`

```
sudo openvpn pfSense-UDP4-1194-scotty.ovpn
```

19. When prompted, type the following:

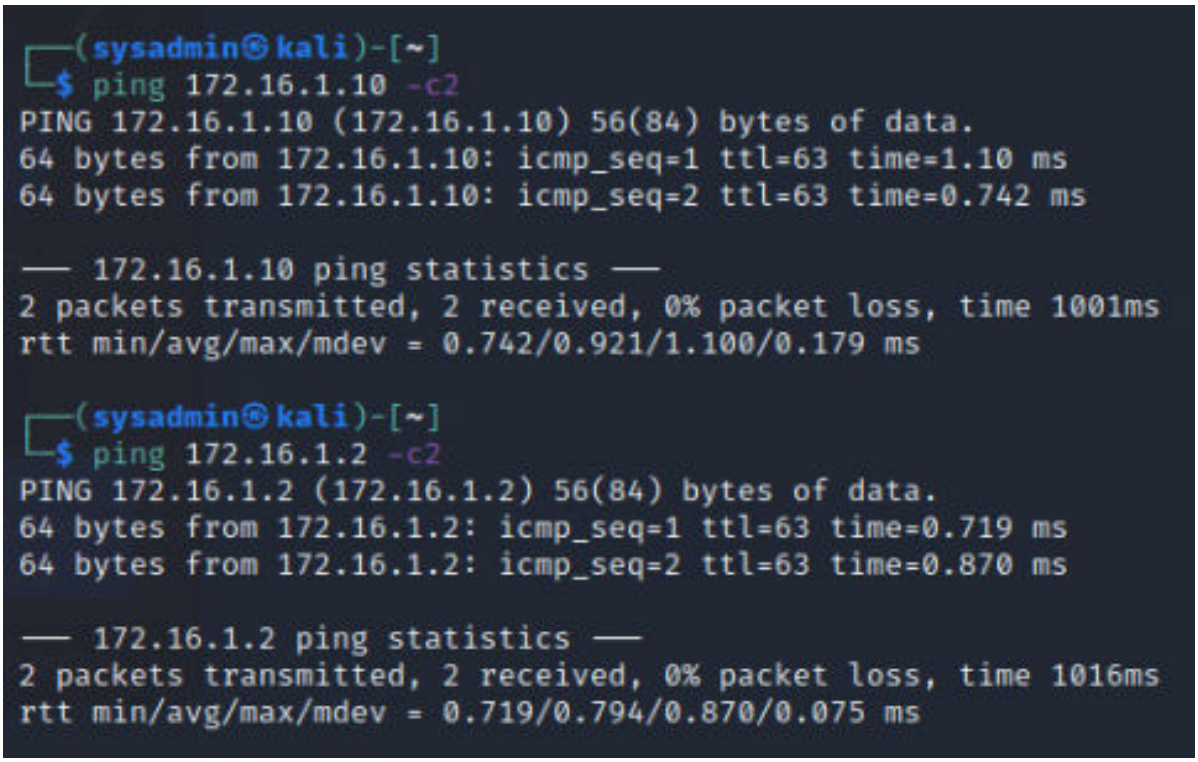
Enter Auth Username	`scotty`
Enter Auth Password	`Password1`
Enter Private Key Password	`Password1`



When the VPN is connected, you should see the message **Initialization Sequence Completed**. The *OpenVPN* client is running in the Terminal session, and it will seem that the program is hung up, but it is not. Minimize the terminal window.

20. Test the VPN connection by repeating the tests we performed at the beginning of the task. Open a second terminal session and try to ping the *UbuntuSRV* and *OSSIM* hosts by typing the following commands:

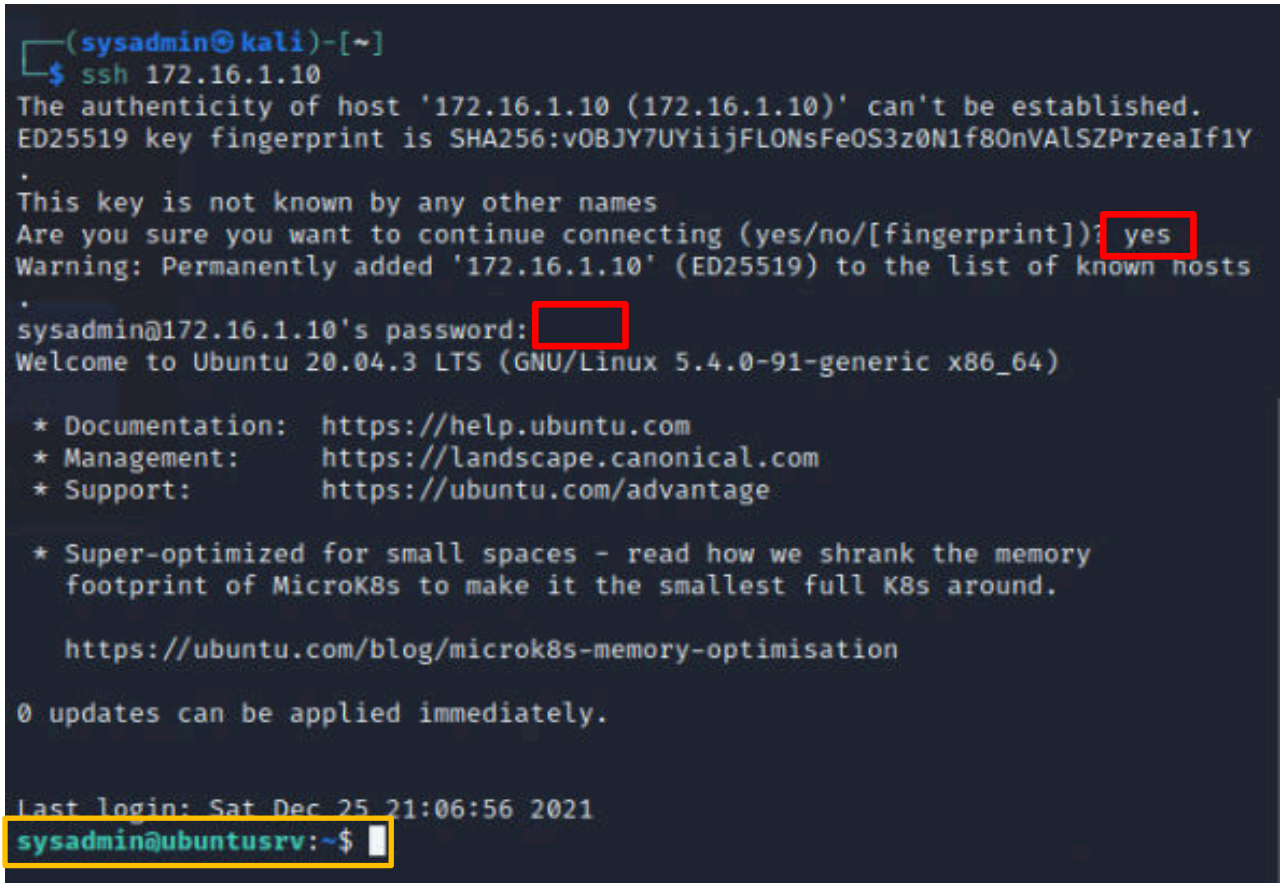
```
ping 172.16.1.10 -c2
ping 172.16.1.2 -c2
```



21. From the terminal, try to SSH to the *UbuntuSRV* by typing the following command:

```
ssh 172.16.1.10
```

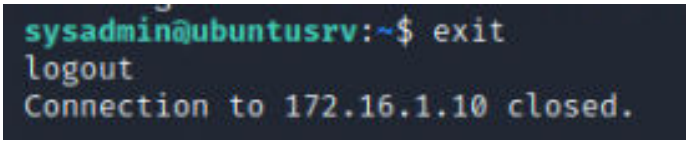

22. When warned that the **key** is not known and asked if you want to continue the connection, type `yes`. When asked for the **sysadmin@172.16.1.10 password,** type: `NDGlabpass123!`



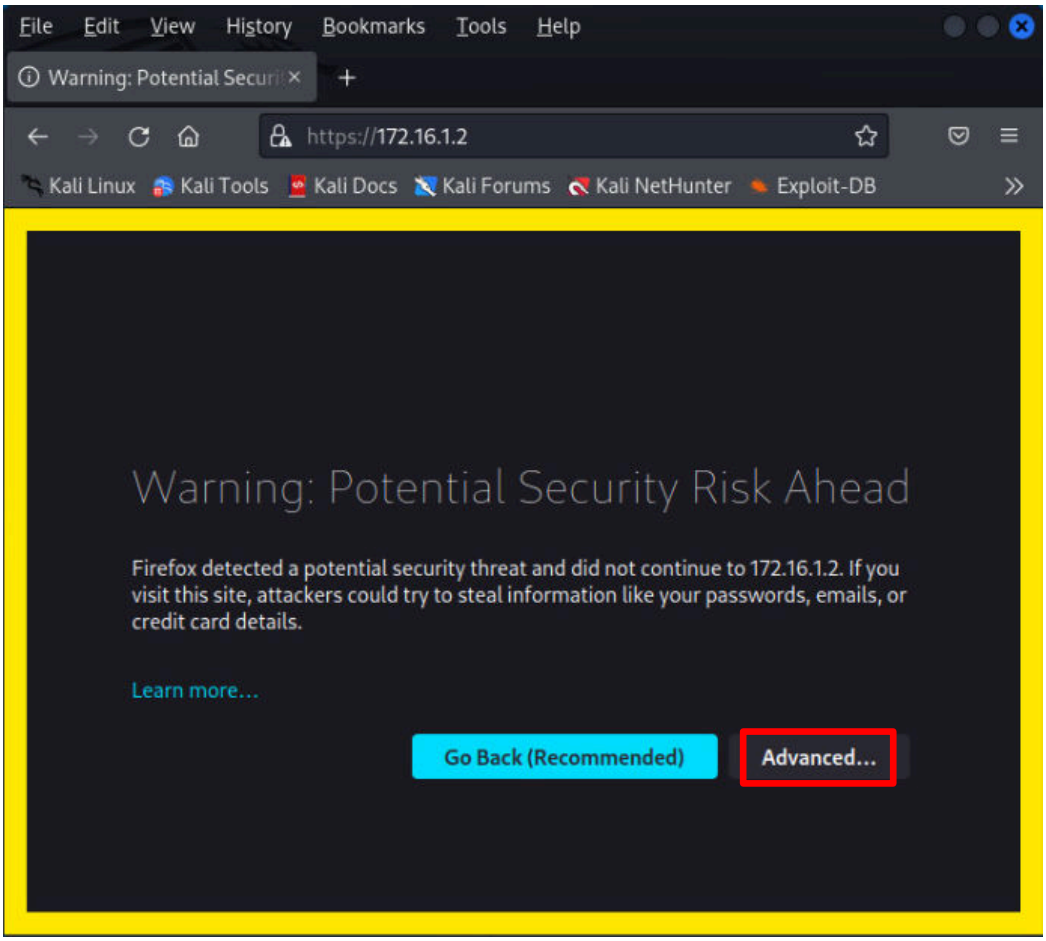
You should see the **sysadmin@ubuntusrv:~$** prompt.

23. Leave the SSH session by typing the following:

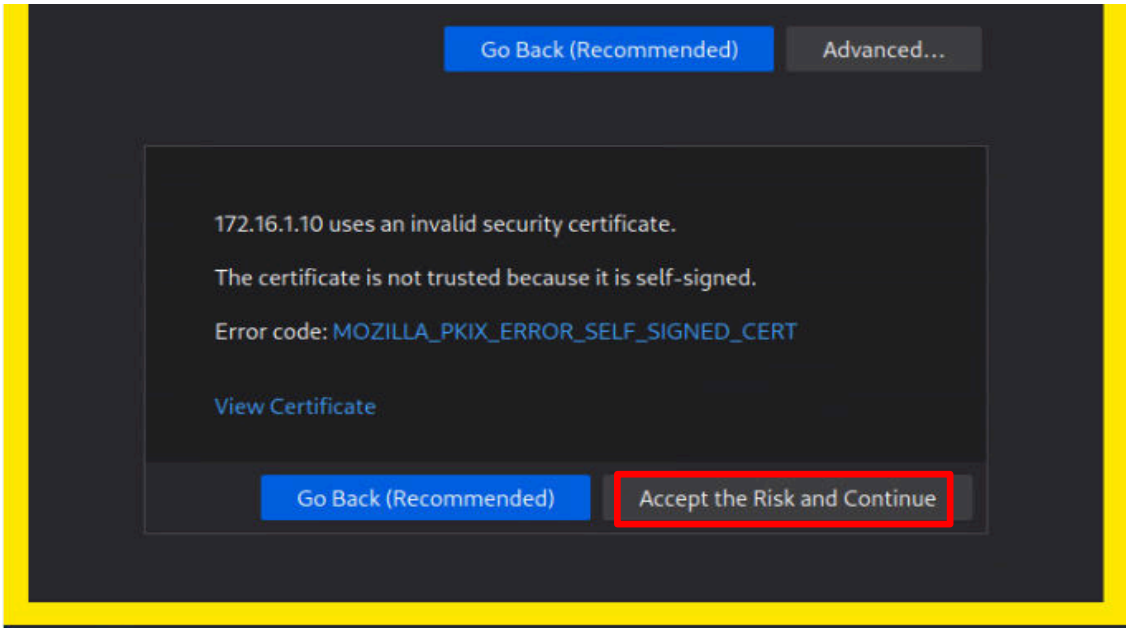
```
exit
```



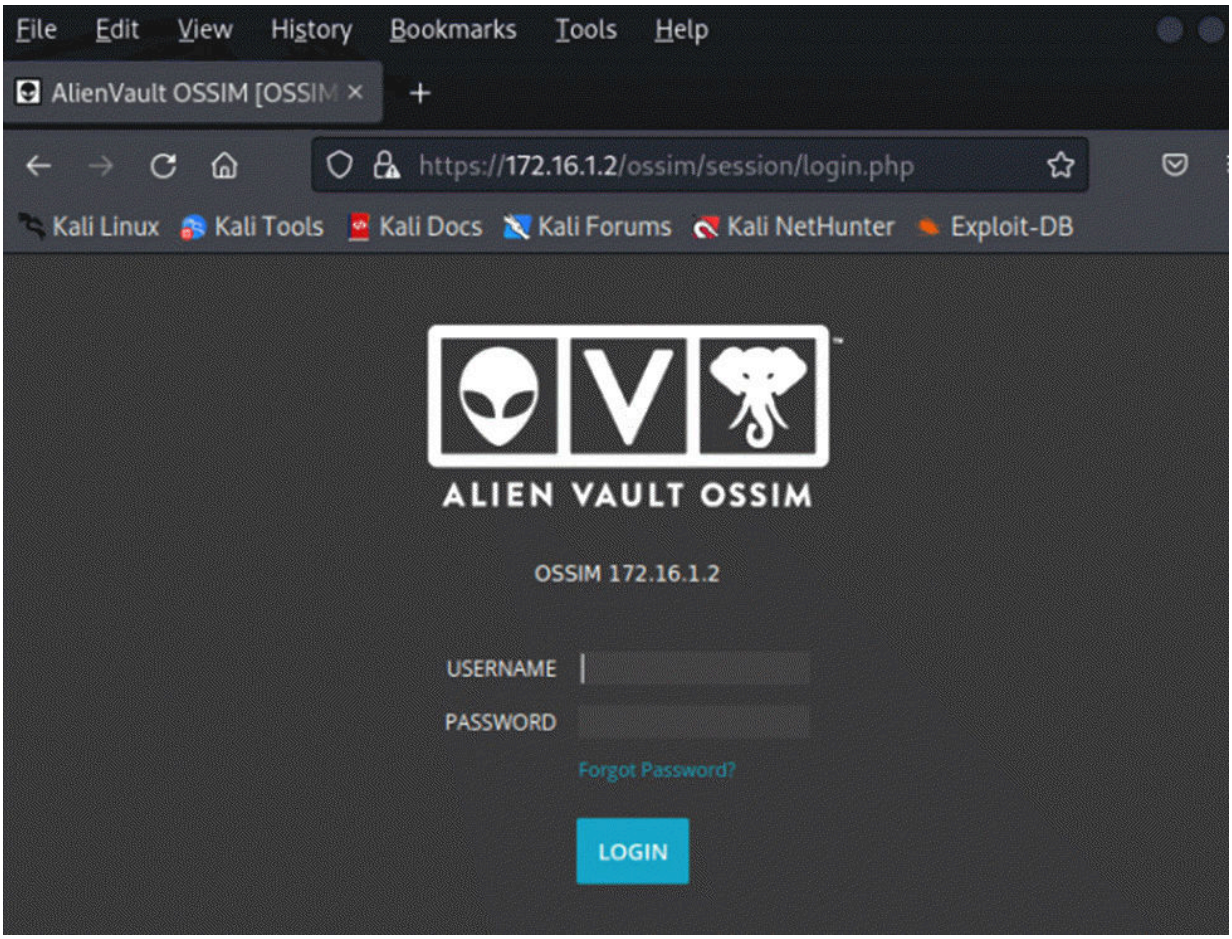
24. Open the *Firefox* web browser and try connecting to the *OSSIM Web Manager* by typing the address `https://172.16.1.2`. You should receive a security risk warning. Click the **Advanced** button.



25. Scroll down to the bottom of the window and click **Accept the Risk and Continue** button.



26. You should see the *Alien Vault OSSIM* login page. Close the **Firefox** browser window.

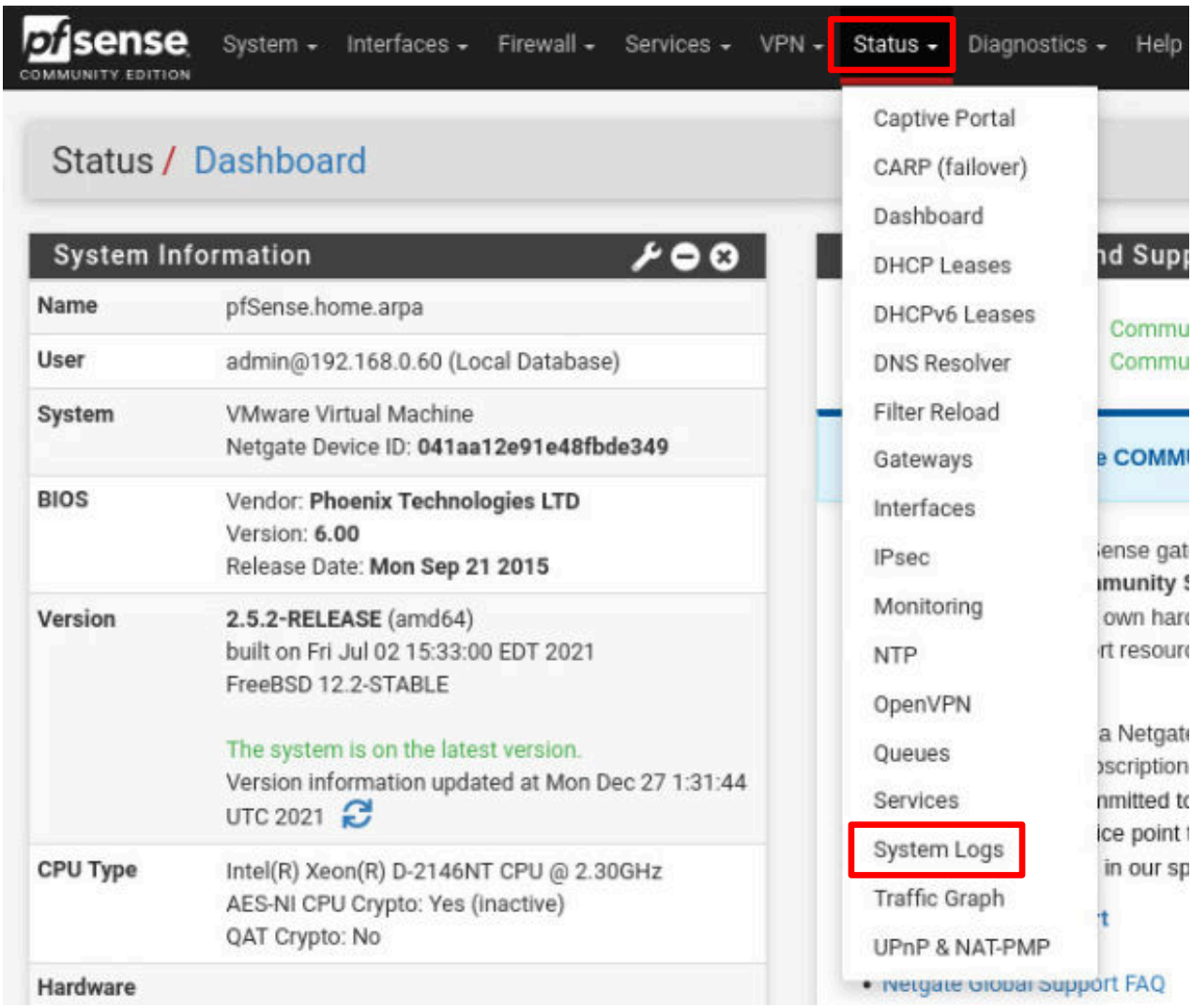


27. Restore the terminal session window where the *OpenVPN* client is running and press **Ctrl+C** to end the *OpenVPN* session.
28. Close all open windows.

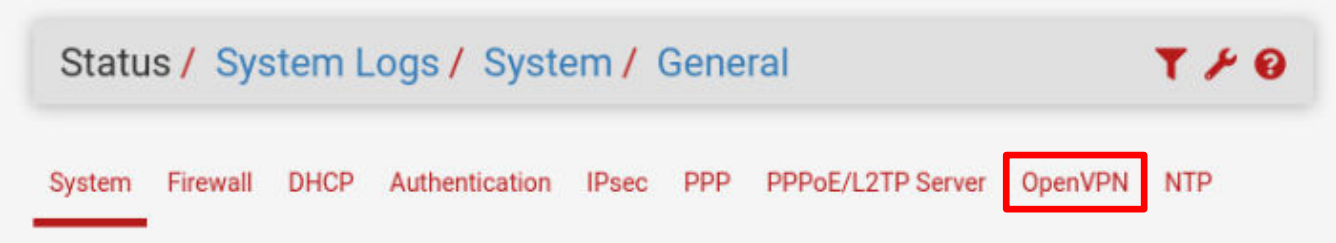
3.5 Monitor the OpenVPN Log

One of the activities a security analyst needs to do is to monitor the logs of the traffic that goes through the *pfSense* firewall. In the case of the *OpenVPN* service, this means monitoring who connects to the VPN and when they connect. Using information, such as **date and time**, **IP address** from where the request is coming from and the **user's name**, a security analyst can determine if the VPN may have been compromised.

1. Set the focus to the **MintOS** computer.
2. Restore the **pfSense** page.
3. Click on the **Status** menu item, then click on **System Logs** in the dropdown menu.



4. On the *Status/System Logs/System/General* page, click on **OpenVPN**.



5. In the log entries, you can see all of the connection actions. In particular, look for the following entries:

   - **[scotty] Peer Connection Initiated**
   - **User 'scotty' authenticated**
   - **scotty/203.0.113.2:43429 … returned IPv4=10.1.1.2**

Last 14 OpenVPN Log Entries. (Maximum 500)

Time	Process	PID	Message
Dec 26 21:43:18	openvpn	28631	203.0.113.2:43429 peer info: IV_VER=2.5.1
Dec 26 21:43:18	openvpn	28631	203.0.113.2:43429 peer info: IV_PLAT=linux
Dec 26 21:43:18	openvpn	28631	203.0.113.2:43429 peer info: IV_PROTO=6
Dec 26 21:43:18	openvpn	28631	203.0.113.2:43429 peer info: IV_NCP=2
Dec 26 21:43:18	openvpn	28631	203.0.113.2:43429 peer info: IV_CIPHERS=AES-256-GCM:AES-128-GCM:CHACHA20-POLY
Dec 26 21:43:18	openvpn	28631	203.0.113.2:43429 peer info: IV_LZ4=1
Dec 26 21:43:18	openvpn	28631	203.0.113.2:43429 peer info: IV_LZ4v2=1
Dec 26 21:43:18	openvpn	28631	203.0.113.2:43429 peer info: IV_LZO=1
Dec 26 21:43:18	openvpn	28631	203.0.113.2:43429 peer info: IV_COMP_STUB=1
Dec 26 21:43:18	openvpn	28631	203.0.113.2:43429 peer info: IV_COMP_STUBv2=1
Dec 26 21:43:18	openvpn	28631	203.0.113.2:43429 peer info: IV_TCPNL=1
Dec 26 21:43:18	openvpn	28631	203.0.113.2:43429 [scotty] Peer Connection Initiated with [AF_INET]203.0.113.2:43429
Dec 26 21:43:18	openvpn	97711	user 'scotty' authenticated
Dec 26 21:43:18	openvpn	28631	scotty/203.0.113.2:43429 MULTI_sva: pool returned IPv4=10.1.1.2, IPv6=(Not enabled)

6. The lab is completed. You may now end the reservation.