



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

Copyright © 2022 Network Development Group, Inc.
www.netdevgroup.com

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

Contents

Introduction	3
Objectives.....	3
Lab Topology	4
Lab Settings	5
1 Configuring ICMP on the Firewall	6
2 Redirecting Traffic Using Port Forwarding.....	12
3 Configuring a Virtual Private Network (VPN) on the Firewall	20
3.1 Setting up the Certificate for the VPN	20
3.2 Setup OpenVPN on the pfSense Firewall	29
3.3 Export VPN Client Configuration Data	34
3.4 Transfer, Configure and Run the VPN Client.....	36
3.5 Monitor the OpenVPN Log.....	48

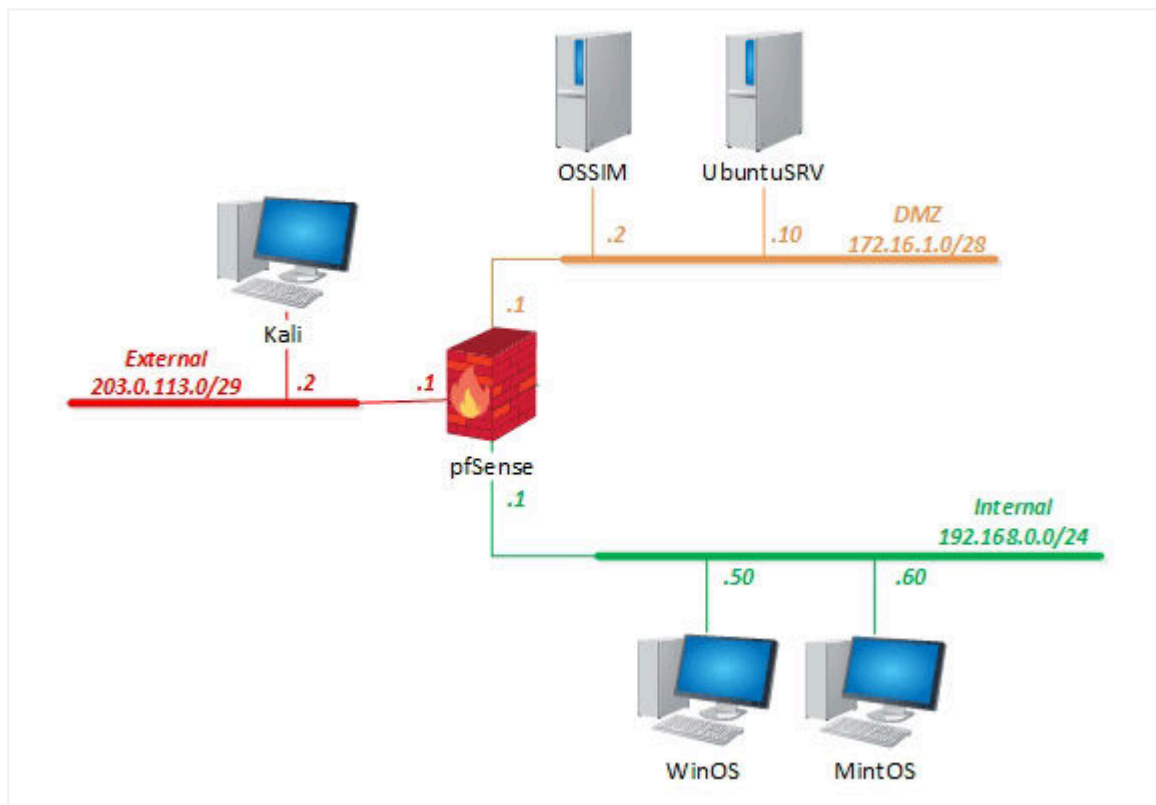
Introduction

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!

```
Ubuntu 20.04.3 LTS ubuntu:~$ ssh ubuntu:~$  
ubuntu login: sysadmin  
Password: [REDACTED]
```

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

```
ping 192.168.0.60 -c3
```

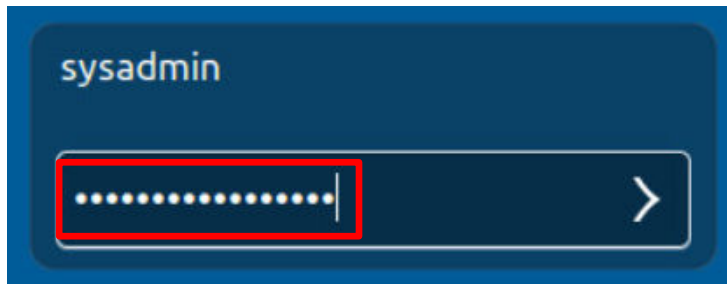
```
sysadmin@ubuntu:~$ ping 192.168.0.60 -c3  
PING 192.168.0.60 (192.168.0.60) 56(84) bytes of data:  
64 bytes from 192.168.0.60: icmp_seq=1 ttl=63 time=0.478 ms  
64 bytes from 192.168.0.60: icmp_seq=2 ttl=63 time=0.467 ms  
64 bytes from 192.168.0.60: icmp_seq=3 ttl=63 time=0.496 ms
```

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

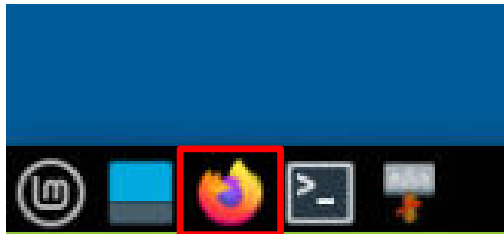
```
ping 203.0.113.2 -c3
```

```
sysadmin@ubuntu:~$ 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
```

5. Set the focus to the **MintOS** computer.
6. Log in to the *sysadmin* account using the password: NDGLabpass123!



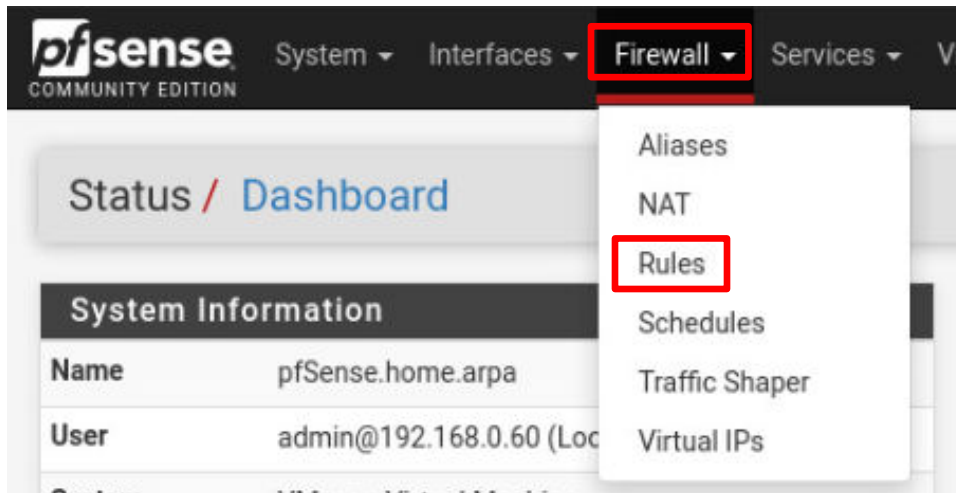
7. Open the browser by clicking on the **Firefox** icon in the toolbar at the bottom of the window.



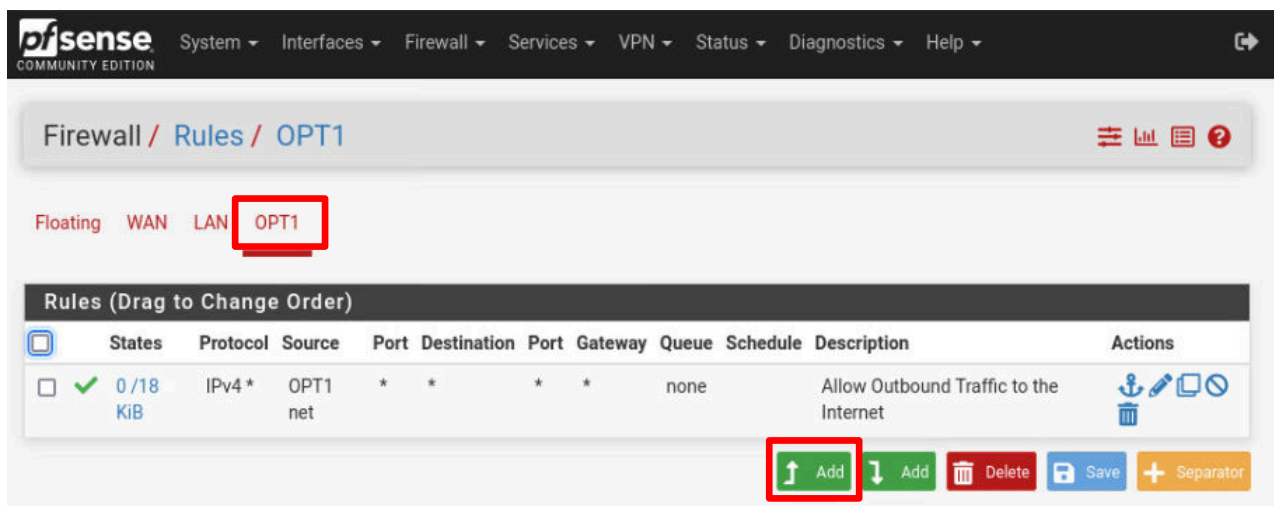
8. In the address bar of the browser, type 192.168.0.1, which is the IP address of the **pfSense** server. Then log in as **admin** using the password NDGLabpass123! and click the **SIGN IN** button.



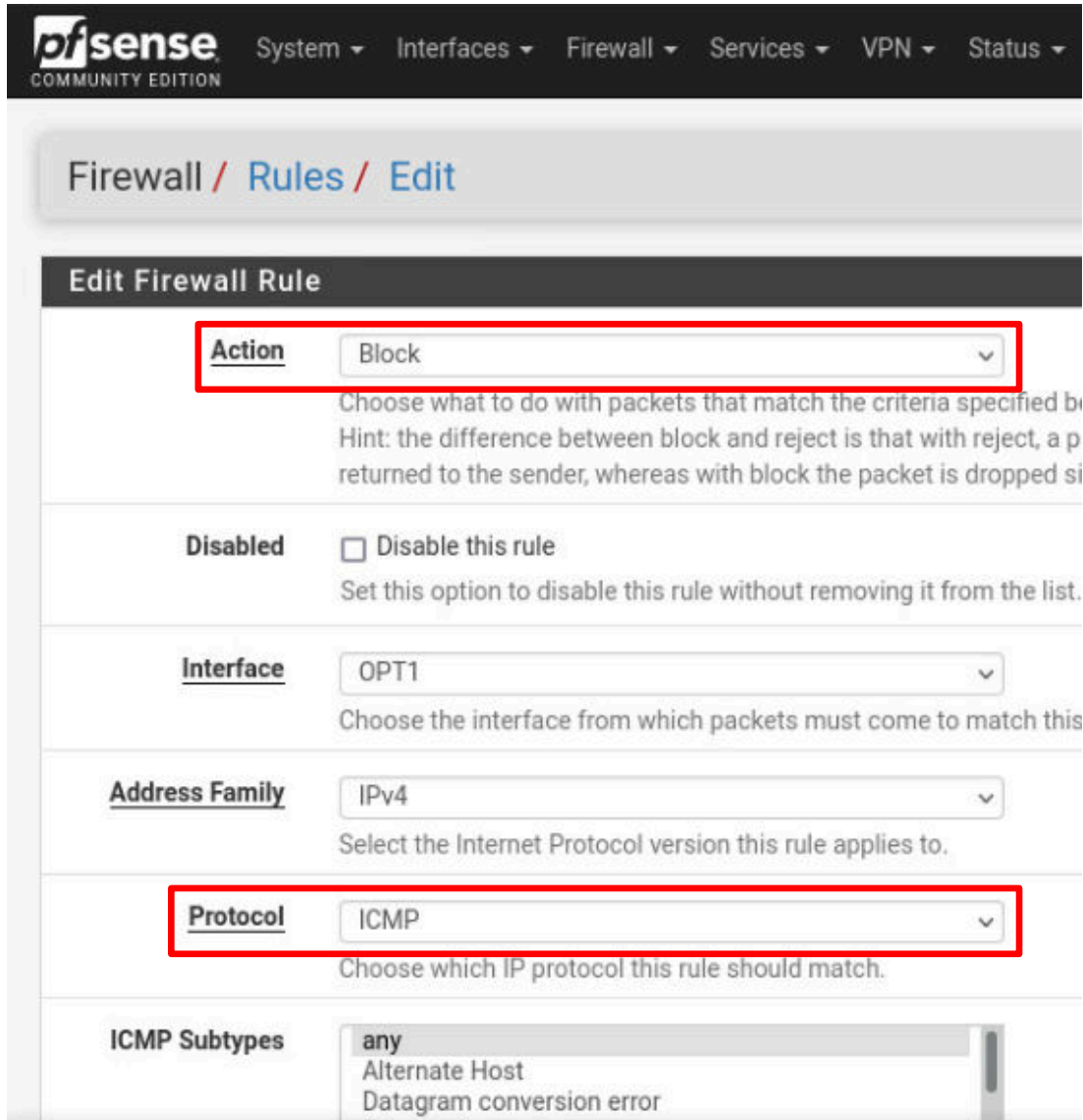
9. A rule will need to be added to block *ICMP* traffic from the *DMZ* to the internal network. Click on **Firewall**, then click on **Rules**.



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**.



pfSense
COMMUNITY EDITION

System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾

Firewall / Rules / Edit

Edit Firewall Rule

Action Block ▾
Choose what to do with packets that match the criteria specified by this rule.
Hint: the difference between block and reject is that with reject, a packet is returned to the sender, whereas with block the packet is dropped silently.

Disabled ☐ Disable this rule
Set this option to disable this rule without removing it from the list.

Interface OPT1 ▾
Choose the interface from which packets must come to match this rule.

Address Family IPv4 ▾
Select the Internet Protocol version this rule applies to.

Protocol ICMP ▾
Choose which IP protocol this rule should match.

ICMP Subtypes
any
Alternate Host
Datagram conversion error

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**.



Destination

Destination ☐ Invert match 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.

Extra Options

Log
☐ Log packets that are handled by this rule
 Hint: the firewall has limited local log space. Don't turn on logging for every remote syslog server (see the [Status](#), [System Logs](#), [Settings](#) page).

Description

A description may be entered here for administrative reference. A maximum displayed in the firewall log.

Advanced Options

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

pfSense
COMMUNITY EDITION

Firewall / Rules / WAN

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

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:

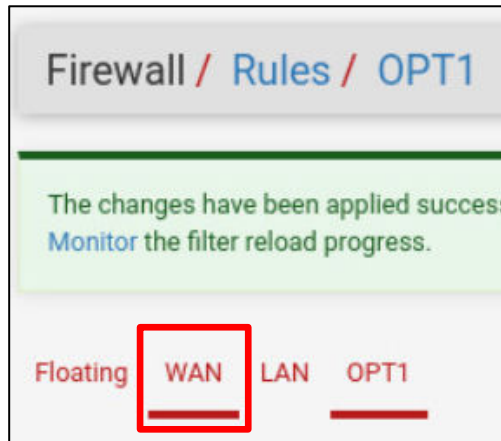
```
ping 203.0.113.2 -c3
```

```
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
```

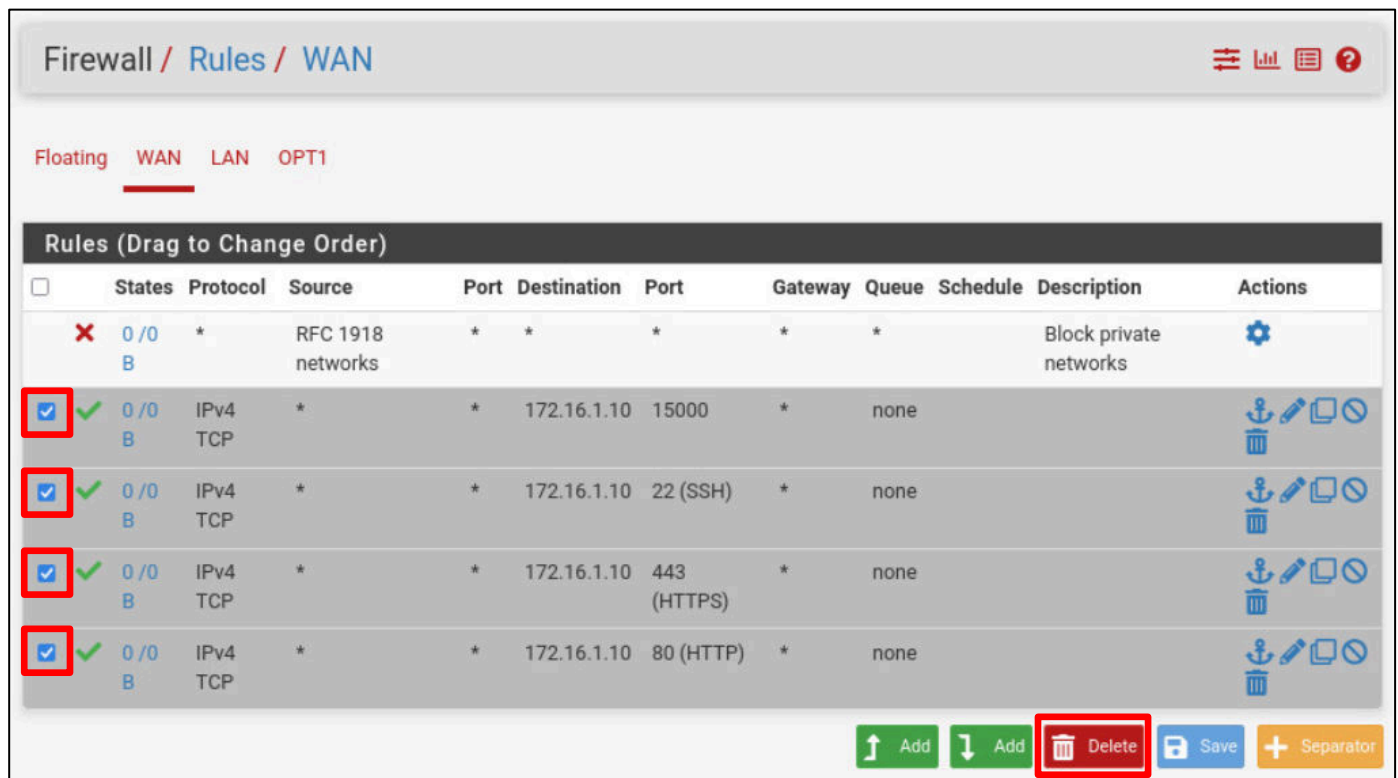
2 Redirecting Traffic Using Port Forwarding

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.

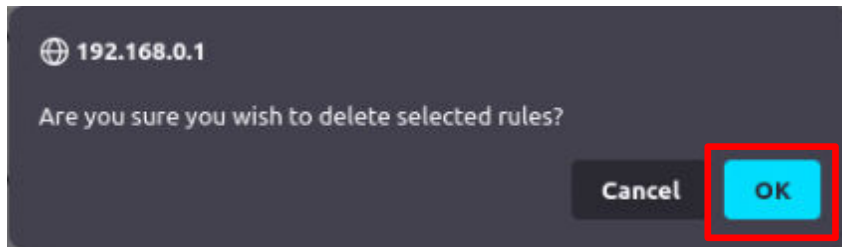
1. Return to the **MintOS** computer.
2. You should still be on the *Firewall/Rules/OPT1* page. Click on **WAN** in the menu bar.



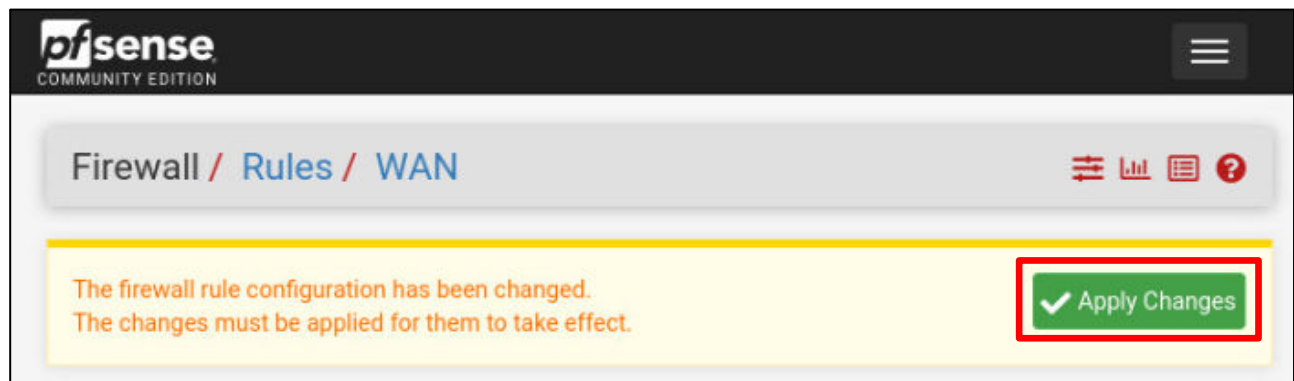
3. In the *Rules* box, click on the **checkbox** for all of the pass rules (the green checkmarks) for the IPv4 Protocol to destination 172.16.1.10 (the *UbuntuSRV* computer) and click the **Delete** button at the bottom of the window.



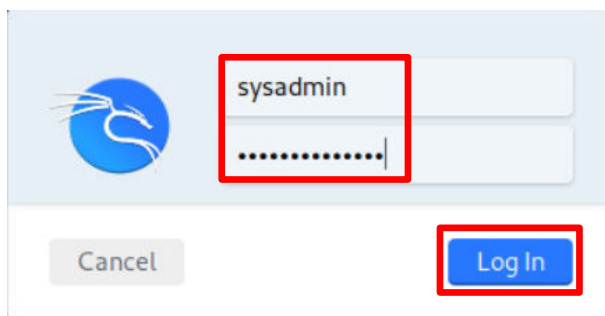
4. In the *Confirmation* window, when asked, *Are you sure you wish to delete the selected rules?* click the **OK** button.



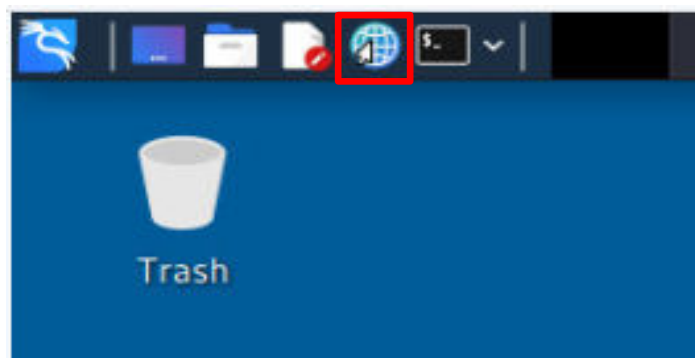
5. Click the **Apply Changes** button.



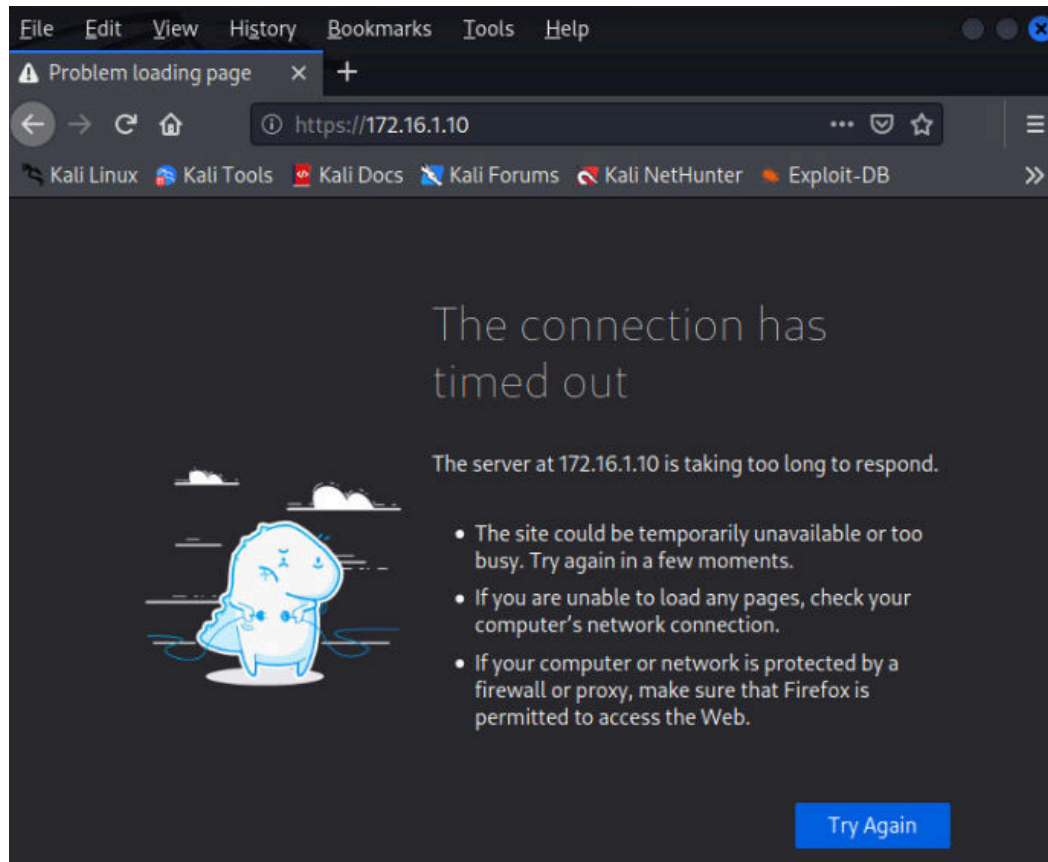
6. Set the focus to the **Kali** computer.
7. Log in as **sysadmin** using the password **NDGLabpass123!** and then click the **Log In** button.



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



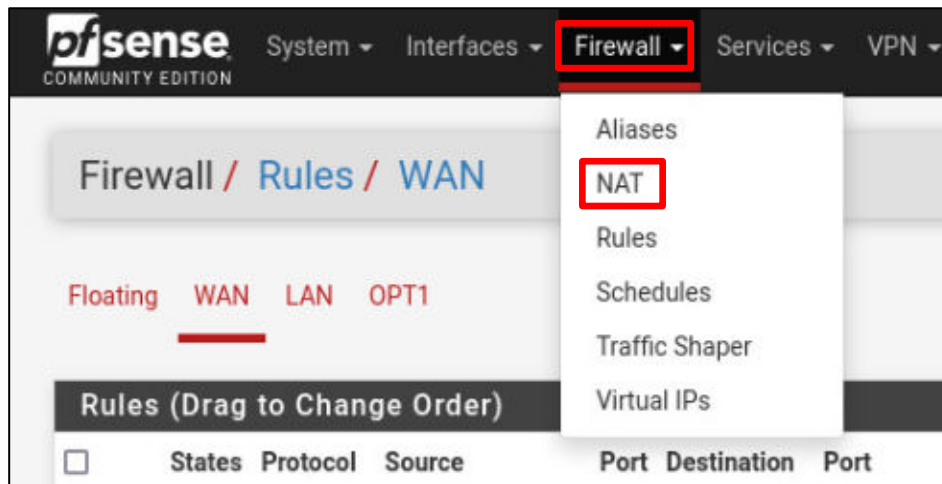
9. In the address bar, type `https://172.16.1.10`. After a couple of minutes, the browser should timeout, and you will see a window pop up, indicating that the website is not accessible.



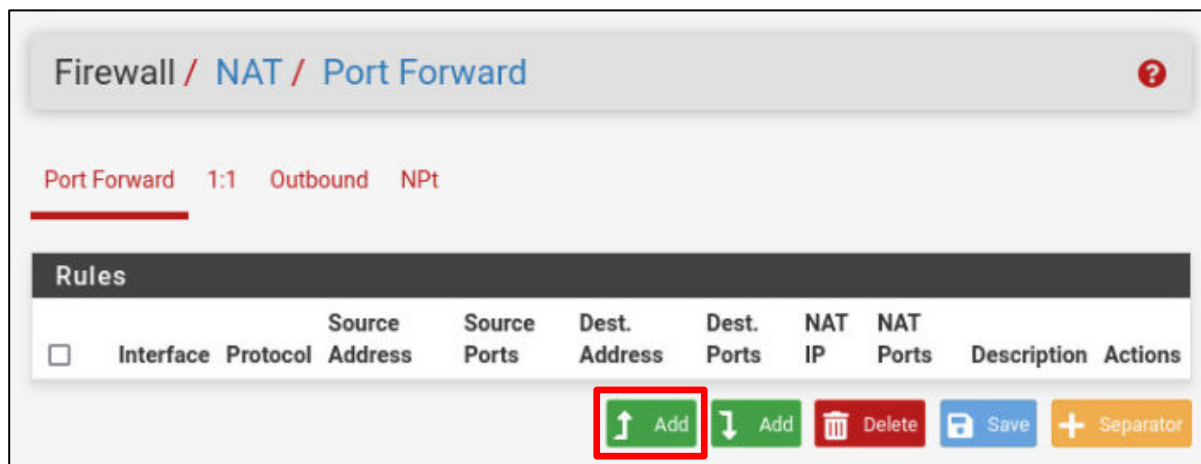
The connection from the external network to the web server on the *DMZ* network cannot be established because the *WAN*-based rules on the *pfSense* firewall were deleted, which effectively closed both *HTTP* and *HTTPS* access.

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.

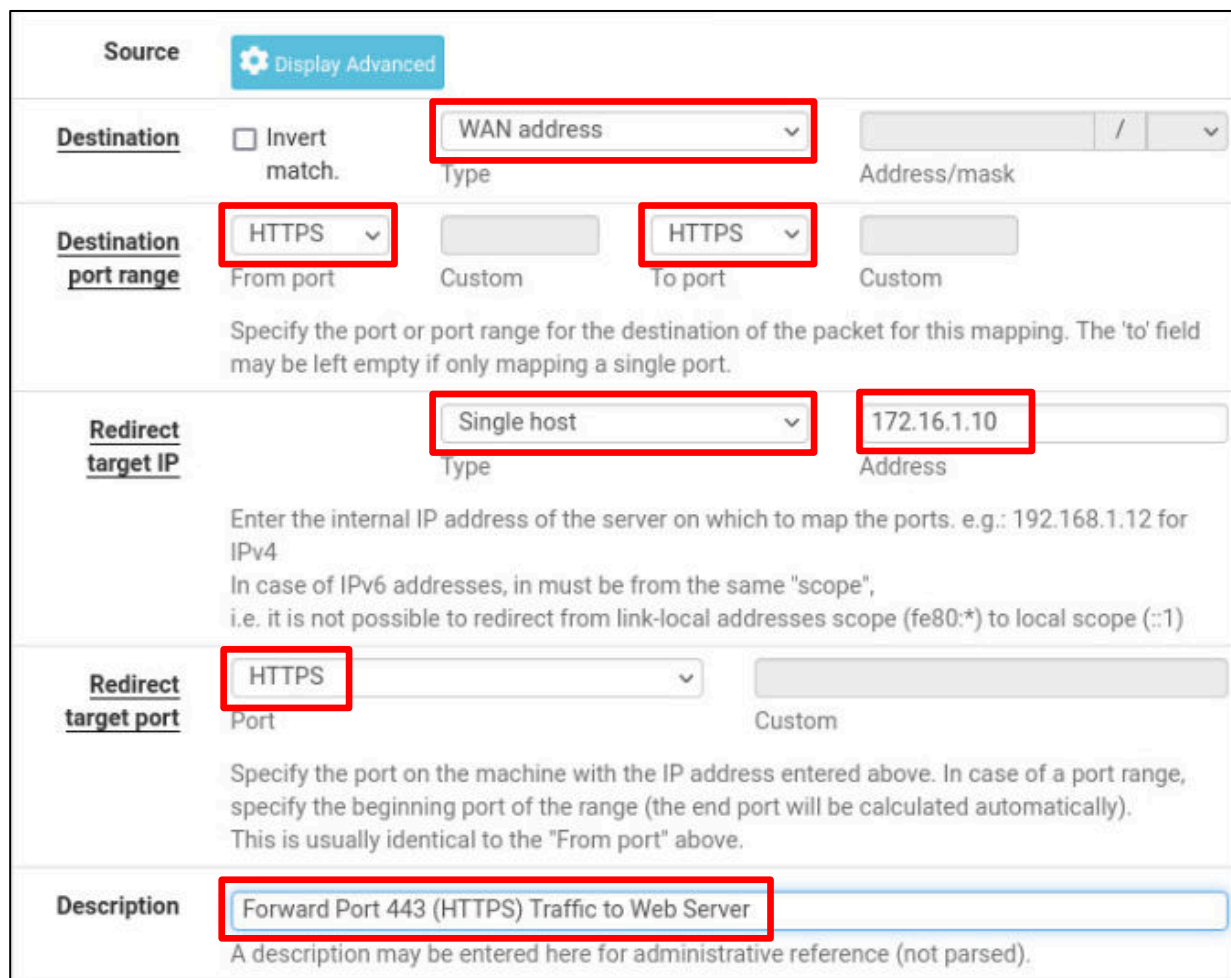


13. On the *Firewall/NAT/Port Forward* window, click on the **Add to Top** button.



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

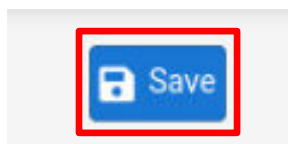
<i>Destination</i>	Use the list arrow and select WAN Address (if not already selected)
<i>Destination Port Range:</i>	Use the list arrow and select HTTPS for the From Port (the To Port should automatically select HTTPS)
<i>Redirect Target IP</i>	Use the list arrow and select Single Host as the <i>Type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



The screenshot shows the 'Edit Redirect Entry' configuration window. The following fields are highlighted with red boxes:

- Destination:** The dropdown menu is set to 'WAN address'.
- Destination port range:** The 'From port' dropdown is set to 'HTTPS'.
- Destination port range:** The 'To port' dropdown is set to 'HTTPS'.
- Redirect target IP:** The 'Type' dropdown is set to 'Single host'.
- Redirect target IP:** The 'Address' field contains '172.16.1.10'.
- Redirect target port:** The dropdown menu is set to 'HTTPS'.
- Description:** The text field contains 'Forward Port 443 (HTTPS) Traffic to Web Server'.

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.




Firewall / NAT / Port Forward ?






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

✓ Apply Changes

Port Forward 1:1 Outbound NPT

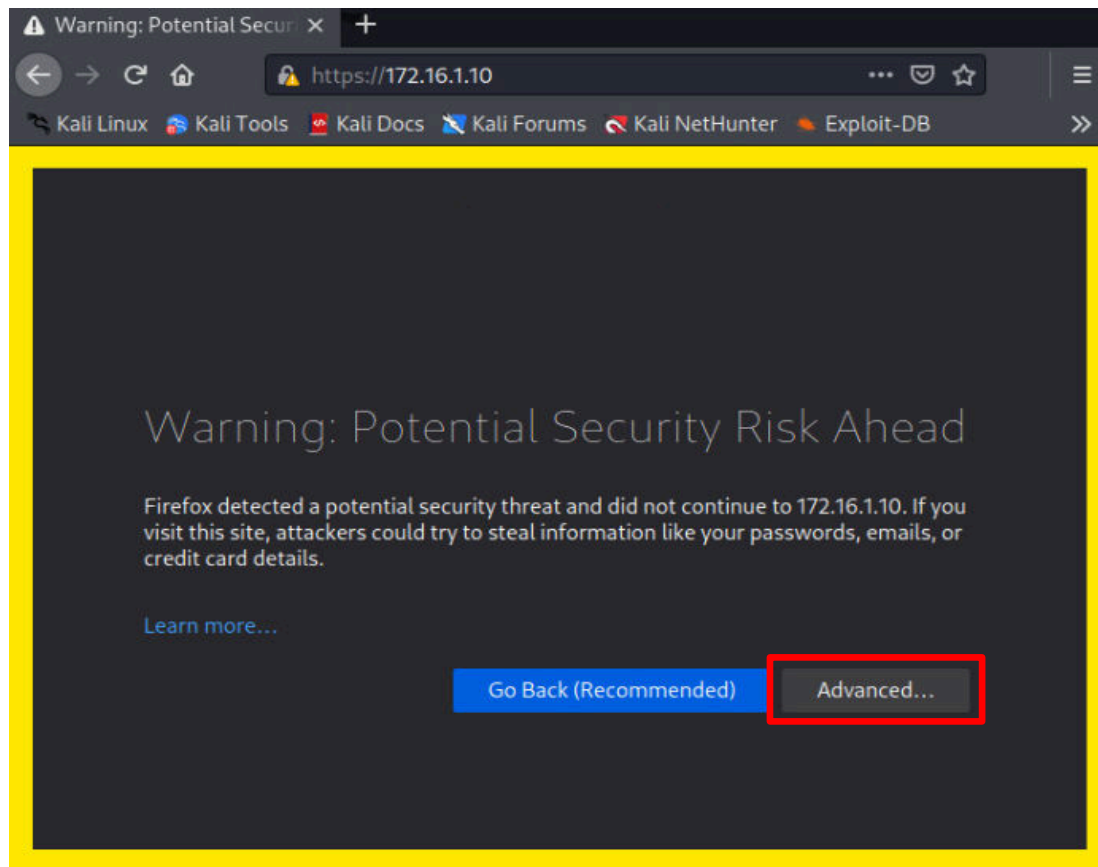
Rules

<input type="checkbox"/>		Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Action
<input type="checkbox"/>	<input checked="" type="checkbox"/> 	WAN	TCP	*	*	WAN address	443 (HTTPS)	172.16.1.10	443 (HTTPS)	Forward Port 443 (HTTPS) Traffic to Web Server	 

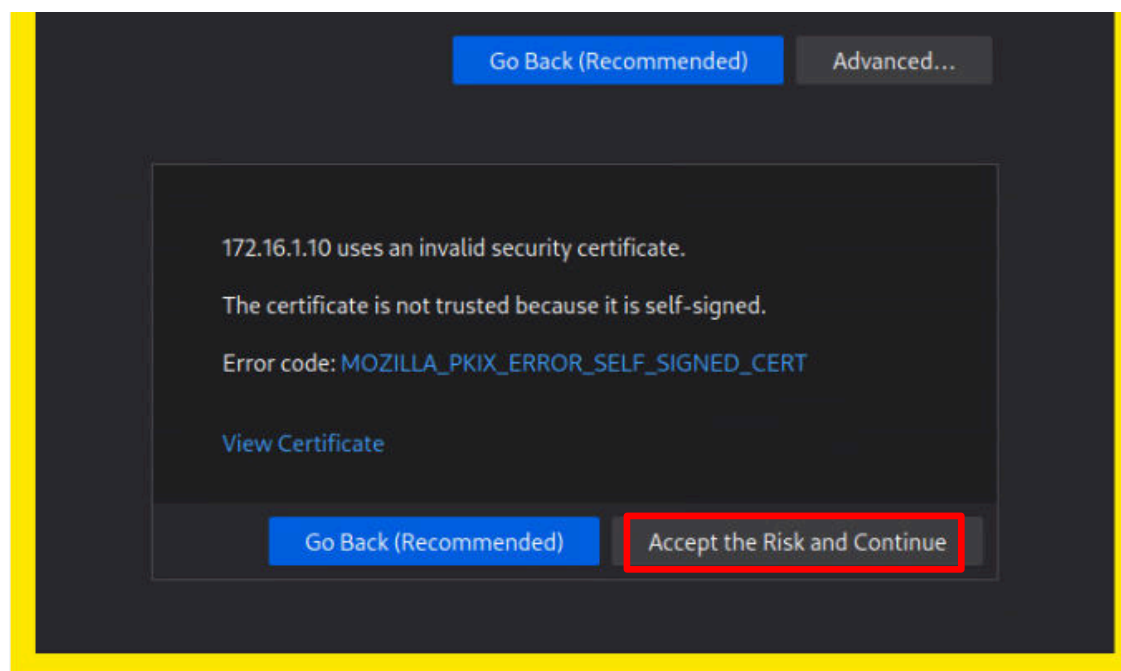
 Add  Add  Delete  Save  Separator

17. Return to the *Kali* computer.

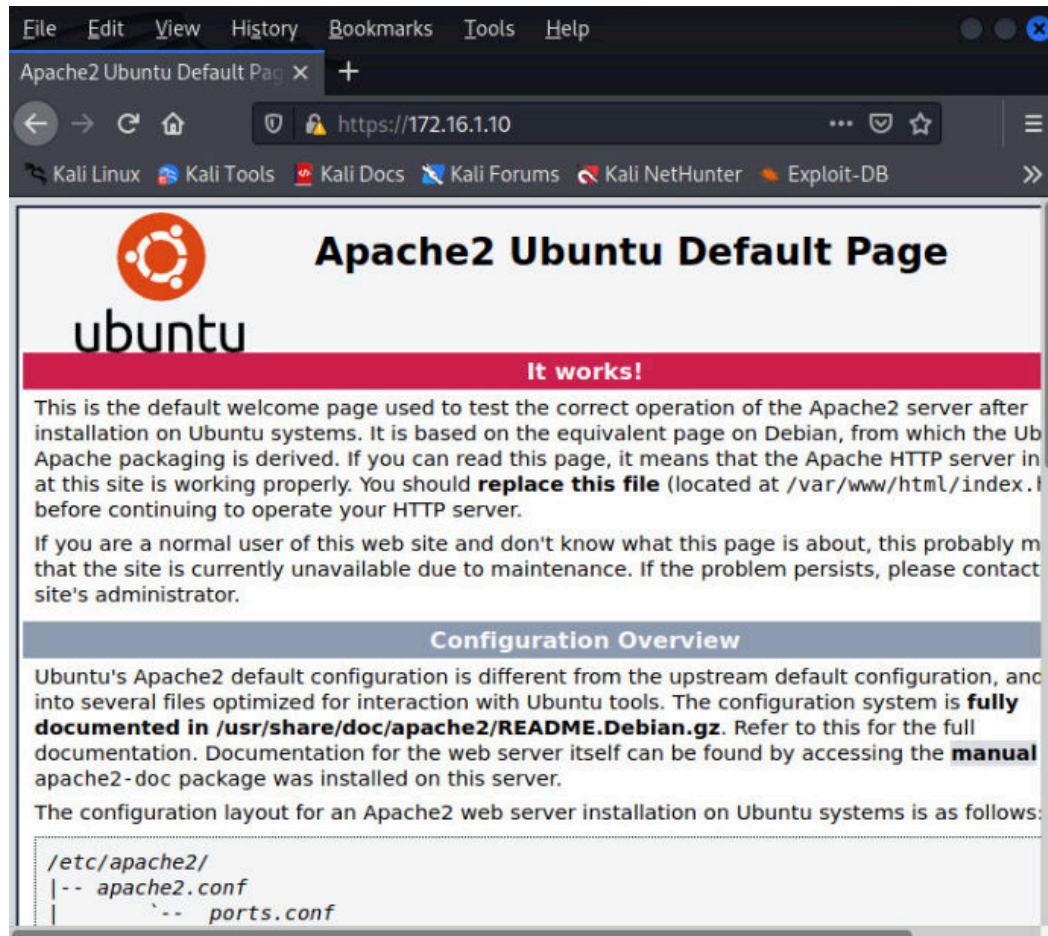
18. Open the Firefox browser and type in the IP address of the *UbuntuSRV* computer (<https://172.16.1.10>). You should get a security risk warning. Click the **Advanced** button.



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.

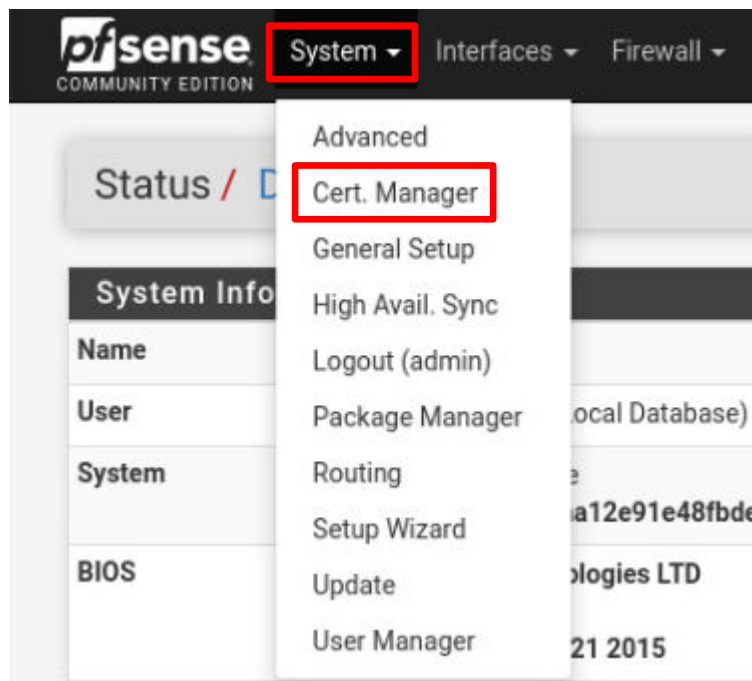
3 Configuring a Virtual Private Network (VPN) on the Firewall

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.

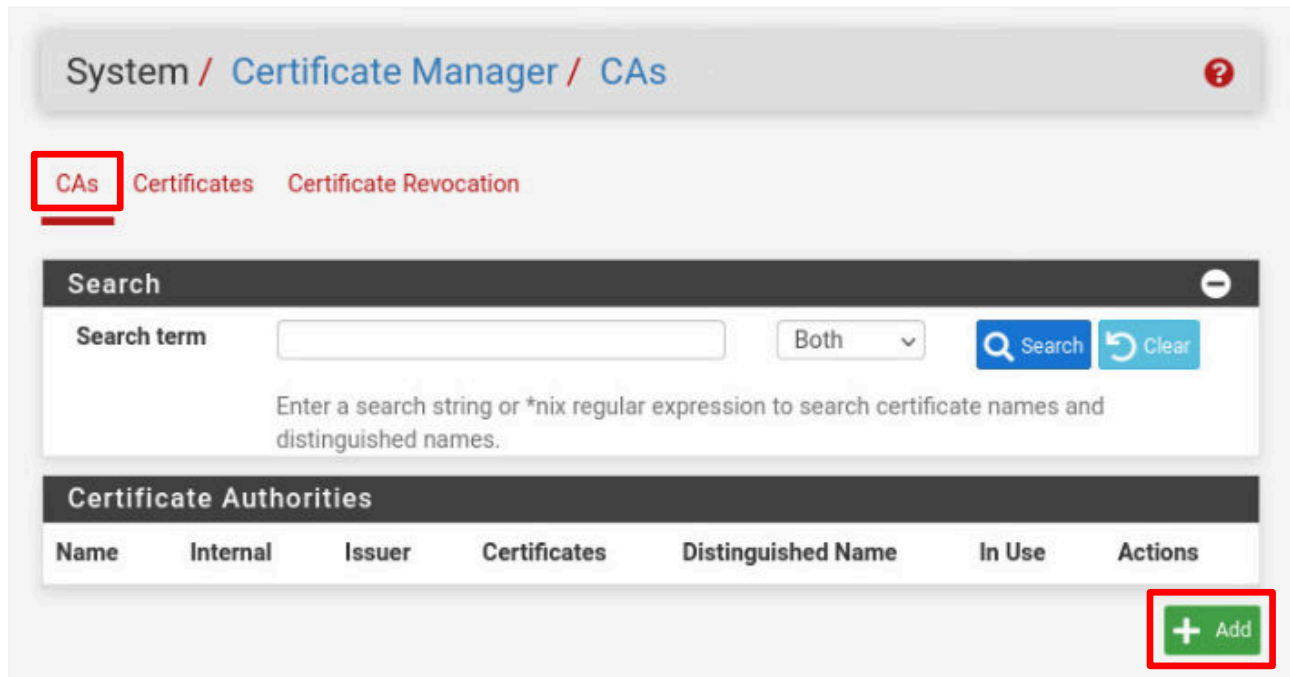
A security analyst could be tasked with securely setting up the organization's VPN and monitoring the activity to ensure that it is being used only by authorized users.

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.



- 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.



System / Certificate Manager / CAs

CAs Certificates Certificate Revocation

Search

Search term Both

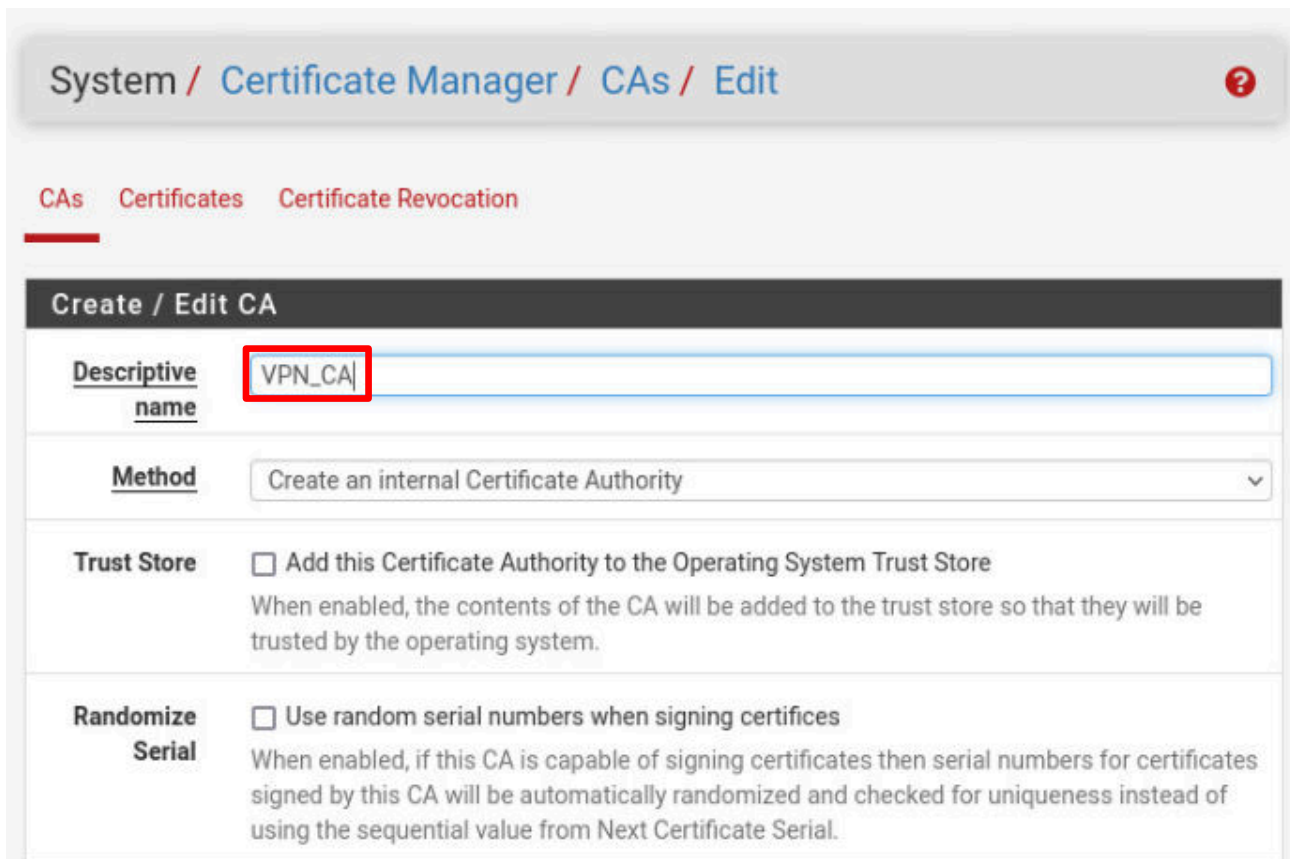
Enter a search string or *nix regular expression to search certificate names and distinguished names.

Certificate Authorities

Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions
------	----------	--------	--------------	--------------------	--------	---------

+ Add

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



System / Certificate Manager / CAs / Edit

CAs Certificates Certificate Revocation

Create / Edit CA

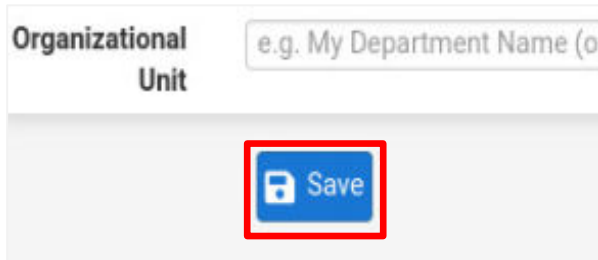
Descriptive name

Method

Trust Store ☐ Add this Certificate Authority to the Operating System Trust Store
When enabled, the contents of the CA will be added to the trust store so that they will be trusted by the operating system.

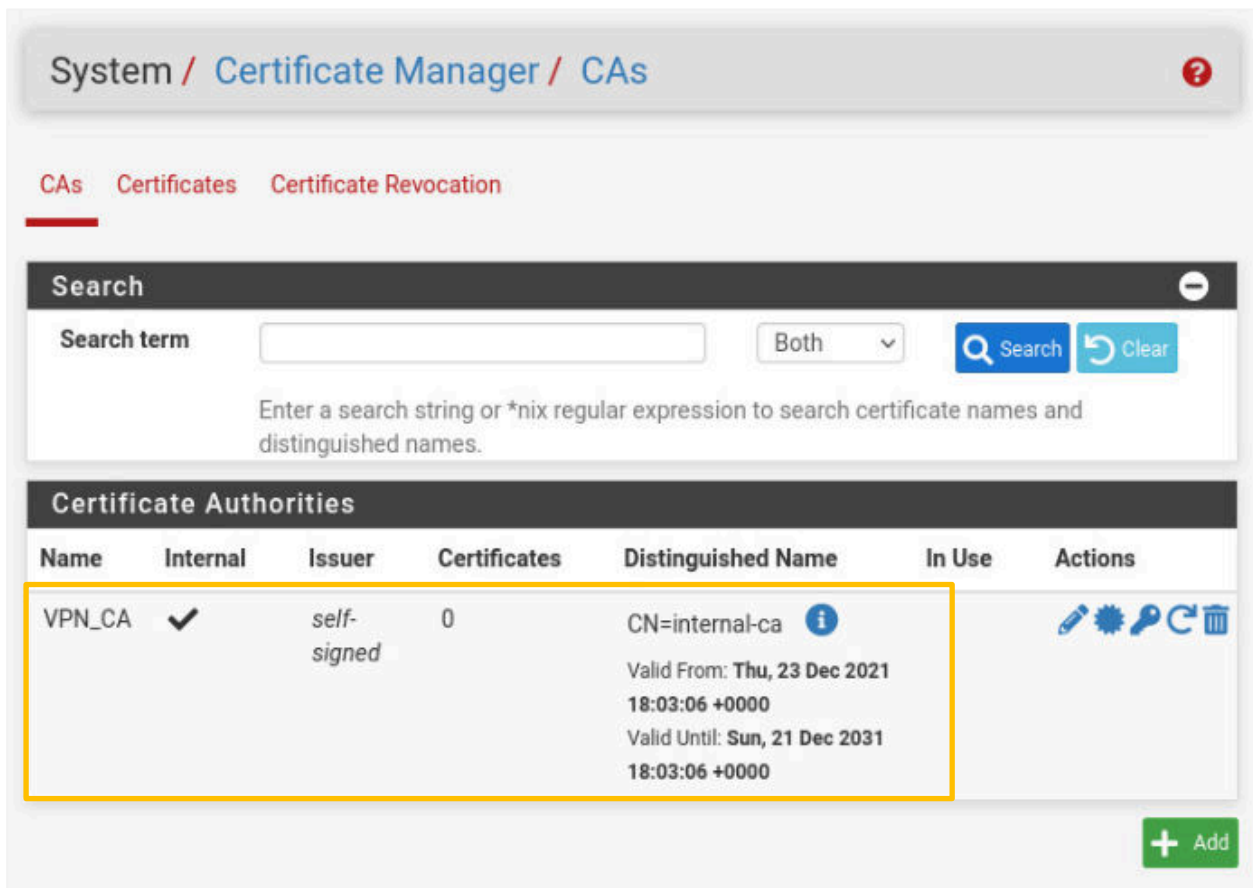
Randomize Serial ☐ Use random serial numbers when signing certifies
When enabled, if this CA is capable of signing certificates then serial numbers for certificates signed by this CA will be automatically randomized and checked for uniqueness instead of using the sequential value from Next Certificate Serial.

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








The screenshot shows a form with a label 'Organizational Unit' and a text input field containing 'e.g. My Department Name (o)'. Below the input field is a blue button with a white floppy disk icon and the text 'Save'. The button is highlighted with a red rectangular border.

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**.

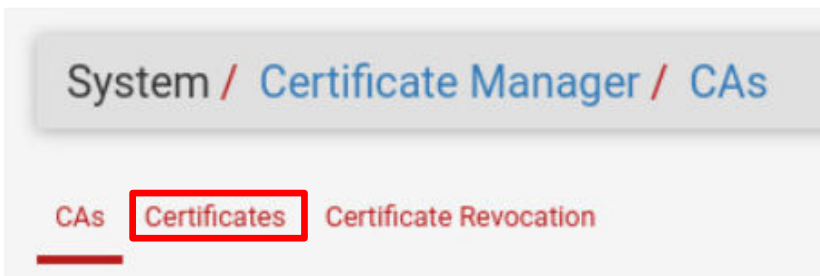


The screenshot shows the 'System / Certificate Manager / CAs' interface. At the top, there are tabs for 'CAs', 'Certificates', and 'Certificate Revocation'. Below the tabs is a search bar with a 'Search term' input field, a 'Both' dropdown, and 'Search' and 'Clear' buttons. Below the search bar is a table titled 'Certificate Authorities'.

Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions
VPN_CA	✓	self-signed	0	CN=internal-ca Valid From: Thu, 23 Dec 2021 18:03:06 +0000 Valid Until: Sun, 21 Dec 2031 18:03:06 +0000		    

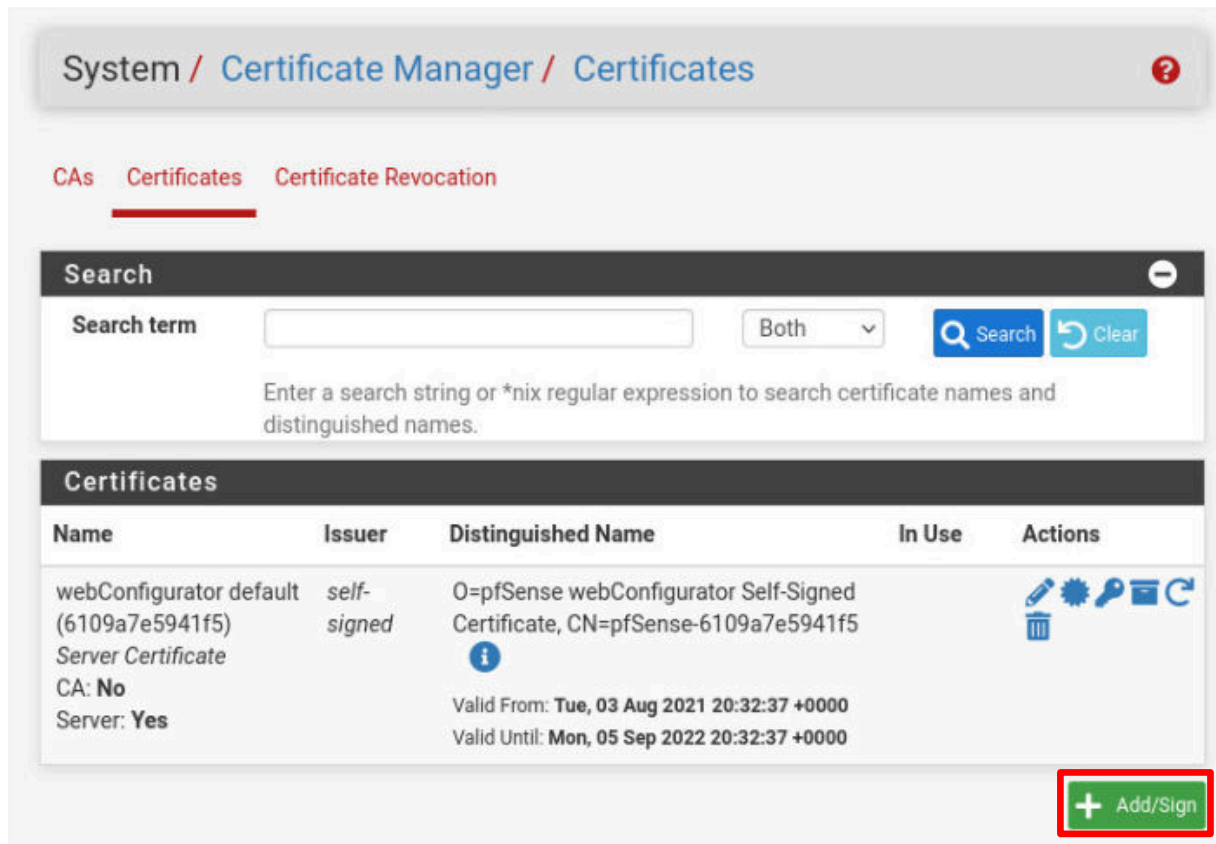
At the bottom right of the table is a green '+ Add' button.

7. Click on **Certificates**.



The screenshot shows the 'System / Certificate Manager / CAs' interface. At the top, there are tabs for 'CAs', 'Certificates', and 'Certificate Revocation'. The 'Certificates' tab is highlighted with a red rectangular border.

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



System / Certificate Manager / Certificates





CA's Certificates Certificate Revocation

Search

Search term Both

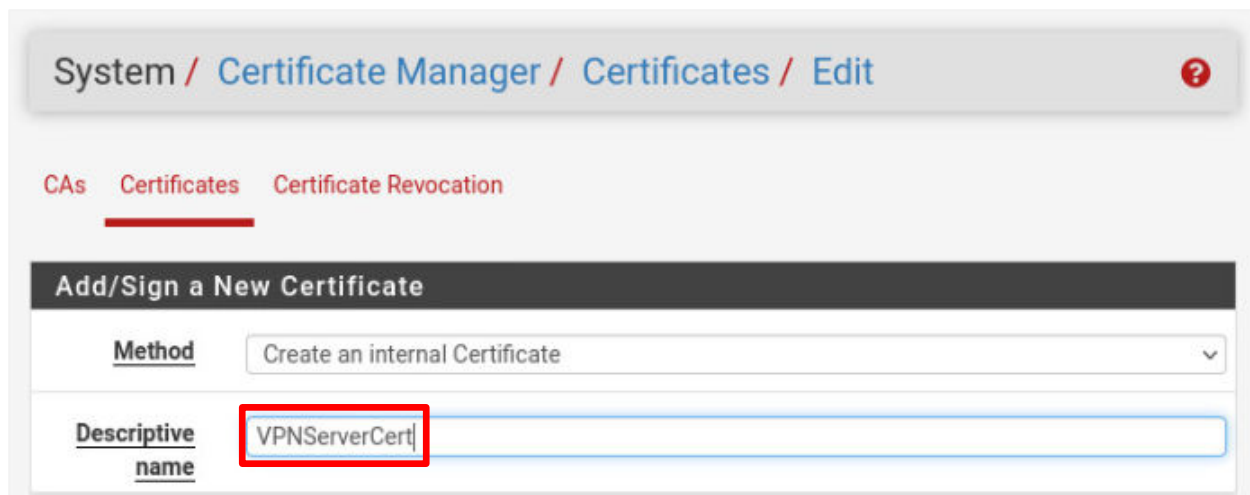
Enter a search string or *nix regular expression to search certificate names and distinguished names.

Certificates

Name	Issuer	Distinguished Name	In Use	Actions
webConfigurator default (6109a7e5941f5) Server Certificate CA: No Server: Yes	self-signed	O=pfSense webConfigurator Self-Signed Certificate, CN=pfSense-6109a7e5941f5 Valid From: Tue, 03 Aug 2021 20:32:37 +0000 Valid Until: Mon, 05 Sep 2022 20:32:37 +0000		   

+ Add/Sign

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



System / Certificate Manager / Certificates / Edit

CA's Certificates Certificate Revocation

Add/Sign a New Certificate

Method Create an internal Certificate

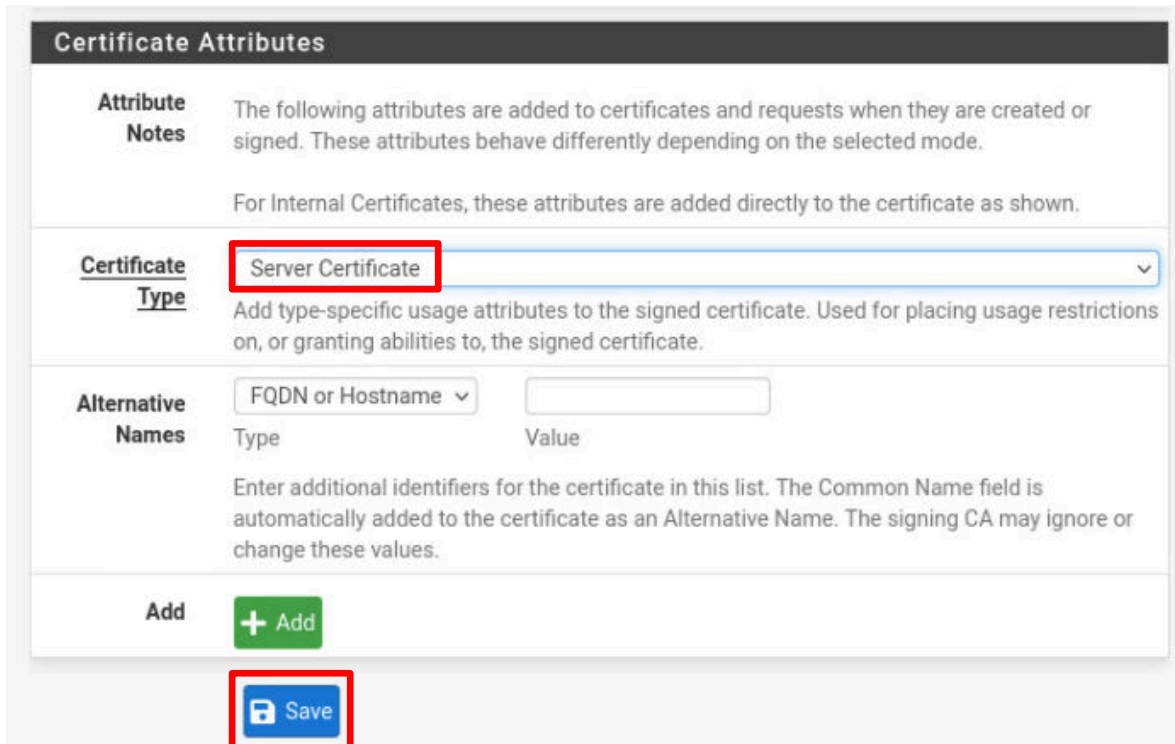
Descriptive name

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

Internal Certificate

Certificate authority	VPN_CA
Key type	RSA
	2048 The length to use when generating a new RSA key, in bits. The Key Length should not be lower than 2048 or some platforms may consider the certificate invalid.
Digest Algorithm	sha256 The digest method used when the certificate is signed. The best practice is to use an algorithm stronger than SHA1. Some platforms may consider weaker digest algorithms invalid
Lifetime (days)	3650 The length of time the signed certificate will be valid, in days. Server certificates should not have a lifetime over 398 days or some platforms may consider the certificate invalid.
Common Name	openvpn.mycompany.org

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.



Certificate Attributes

Attribute Notes
The following attributes are added to certificates and requests when they are created or signed. These attributes behave differently depending on the selected mode.

For Internal Certificates, these attributes are added directly to the certificate as shown.

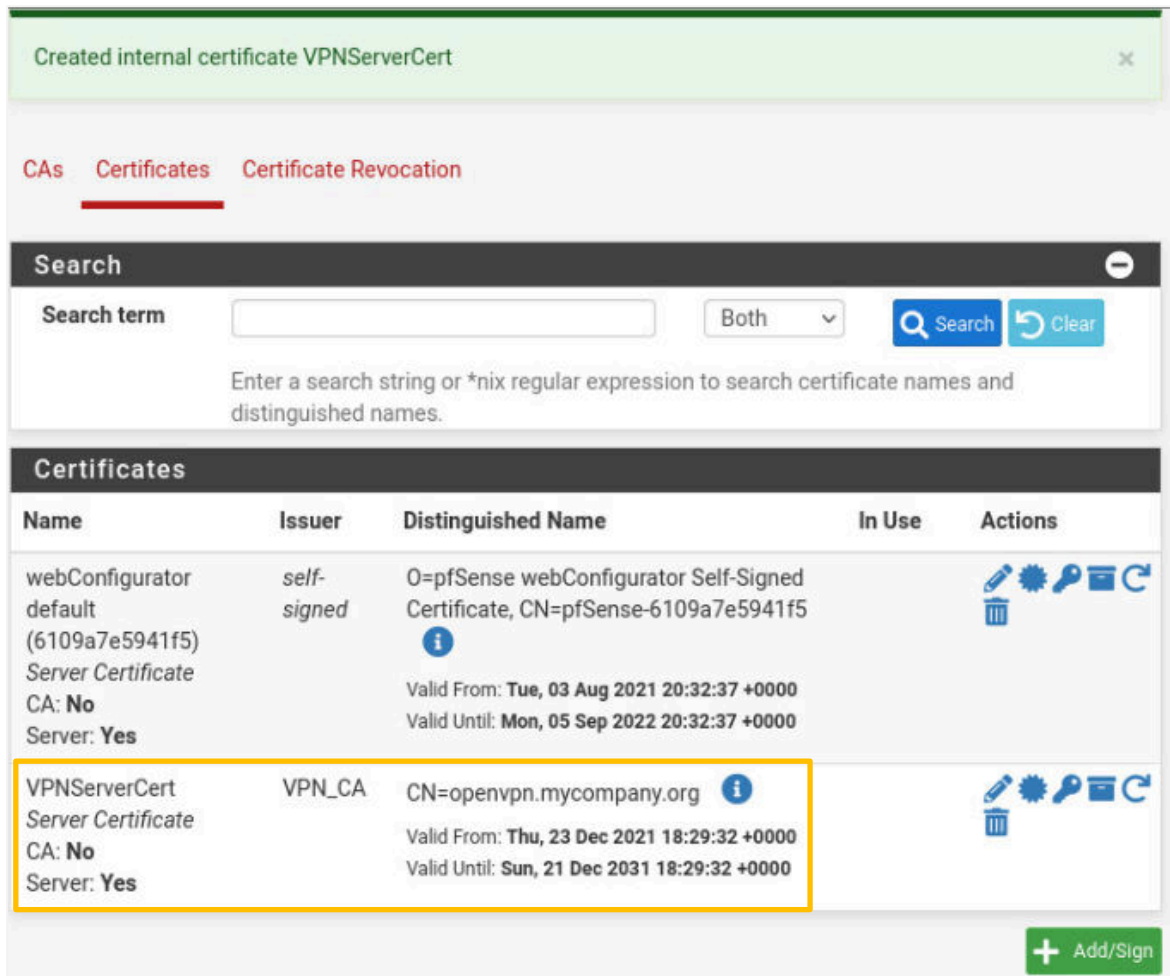
Certificate Type
Server Certificate
Add type-specific usage attributes to the signed certificate. Used for placing usage restrictions on, or granting abilities to, the signed certificate.

Alternative Names
FQDN or Hostname
Type Value
Enter additional identifiers for the certificate in this list. The Common Name field is automatically added to the certificate as an Alternative Name. The signing CA may ignore or change these values.









Add + Add

Save

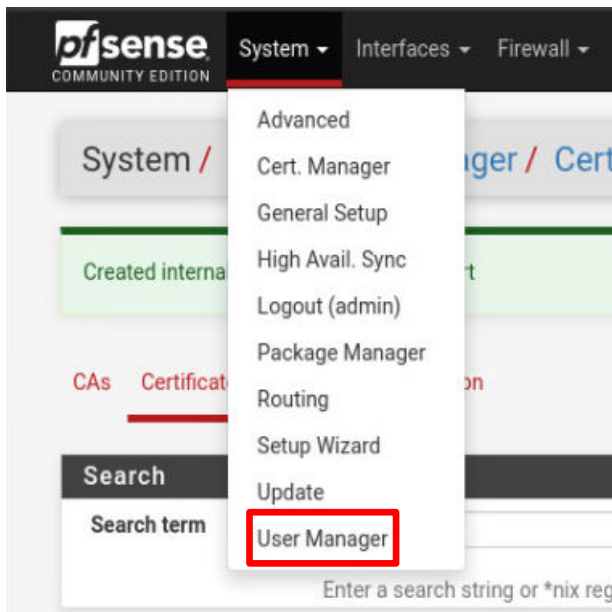
You should now see that the server certificate *VPNServerCert* has been created.



The screenshot shows the pfSense web interface with the 'Certificates' tab selected. A green notification banner at the top states 'Created internal certificate VPNServerCert'. Below the navigation tabs (CAs, Certificates, Certificate Revocation), there is a search bar and a table of certificates. The table has columns for Name, Issuer, Distinguished Name, In Use, and Actions. Two certificates are listed: 'webConfigurator default' and 'VPNServerCert'. The 'VPNServerCert' row is highlighted with an orange border. It is issued by 'VPN_CA' and has a distinguished name of 'CN=openvpn.mycompany.org'. Its validity period is from 'Thu, 23 Dec 2021 18:29:32 +0000' to 'Sun, 21 Dec 2031 18:29:32 +0000'. The 'In Use' column shows a green checkmark, and the 'Actions' column contains icons for editing, deleting, and refreshing.

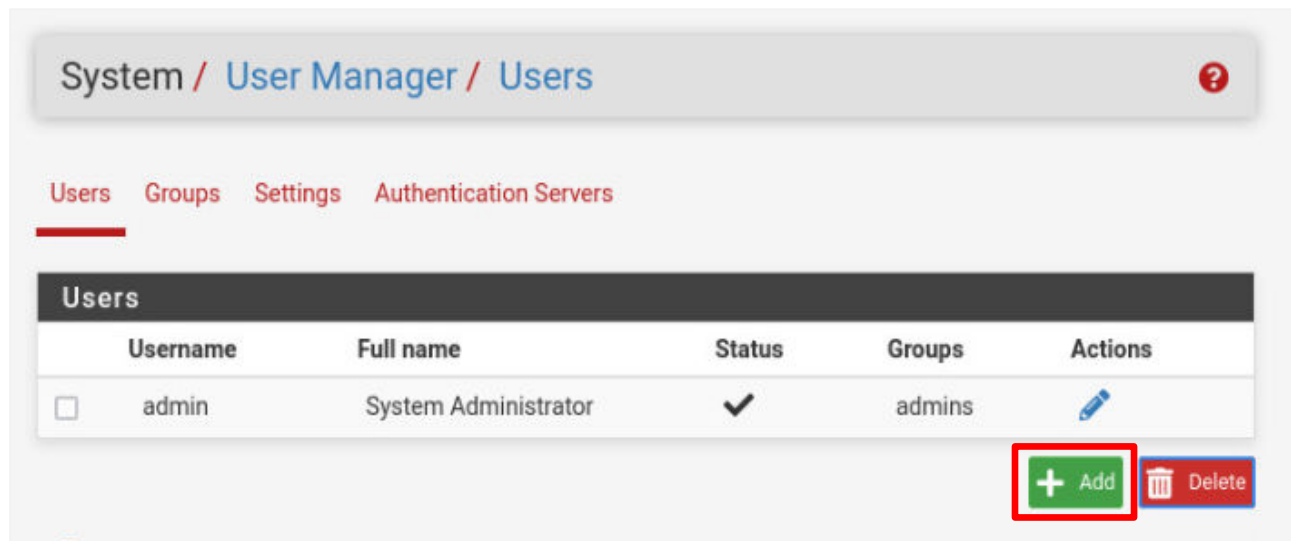
Name	Issuer	Distinguished Name	In Use	Actions
webConfigurator default (6109a7e5941f5) Server Certificate CA: No Server: Yes	self-signed	O=pfSense webConfigurator Self-Signed Certificate, CN=pfSense-6109a7e5941f5 Valid From: Tue, 03 Aug 2021 20:32:37 +0000 Valid Until: Mon, 05 Sep 2022 20:32:37 +0000		  
VPNServerCert Server Certificate CA: No Server: Yes	VPN_CA	CN=openvpn.mycompany.org Valid From: Thu, 23 Dec 2021 18:29:32 +0000 Valid Until: Sun, 21 Dec 2031 18:29:32 +0000		  

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**.

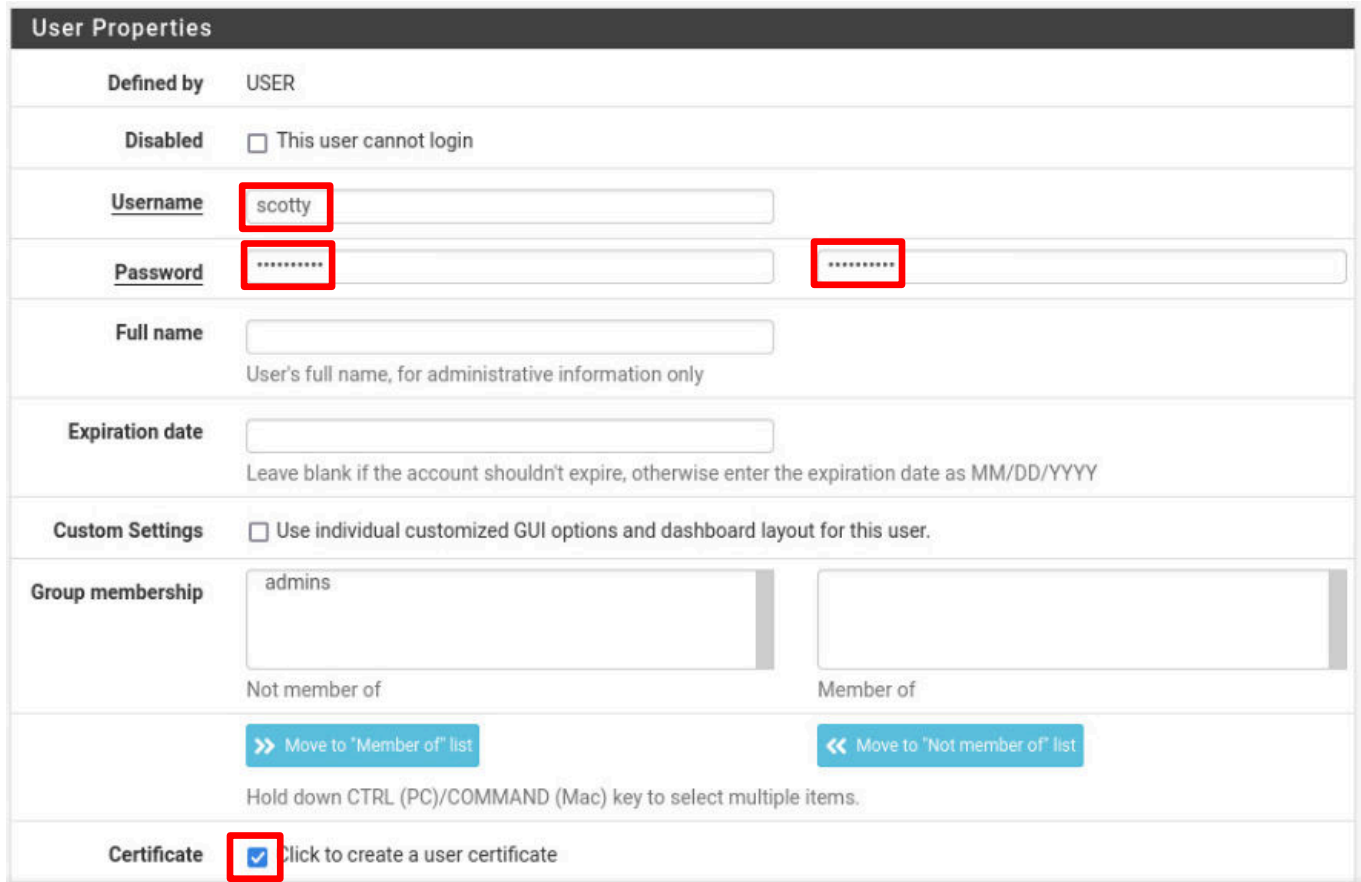


The screenshot shows the pfSense web interface with the 'System' menu open. The 'User Manager' option is highlighted with a red rectangle. The menu includes options like Advanced, Cert. Manager, General Setup, High Avail. Sync, Logout (admin), Package Manager, Routing, Setup Wizard, Update, and User Manager. The background shows the same 'Certificates' page as the previous screenshot.

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.



User Properties

Defined by: USER

Disabled: ☐ This user cannot login

Username:

Password:

Full name:

Expiration date:

Custom Settings: ☐ Use individual customized GUI options and dashboard layout for this user.

Group membership:

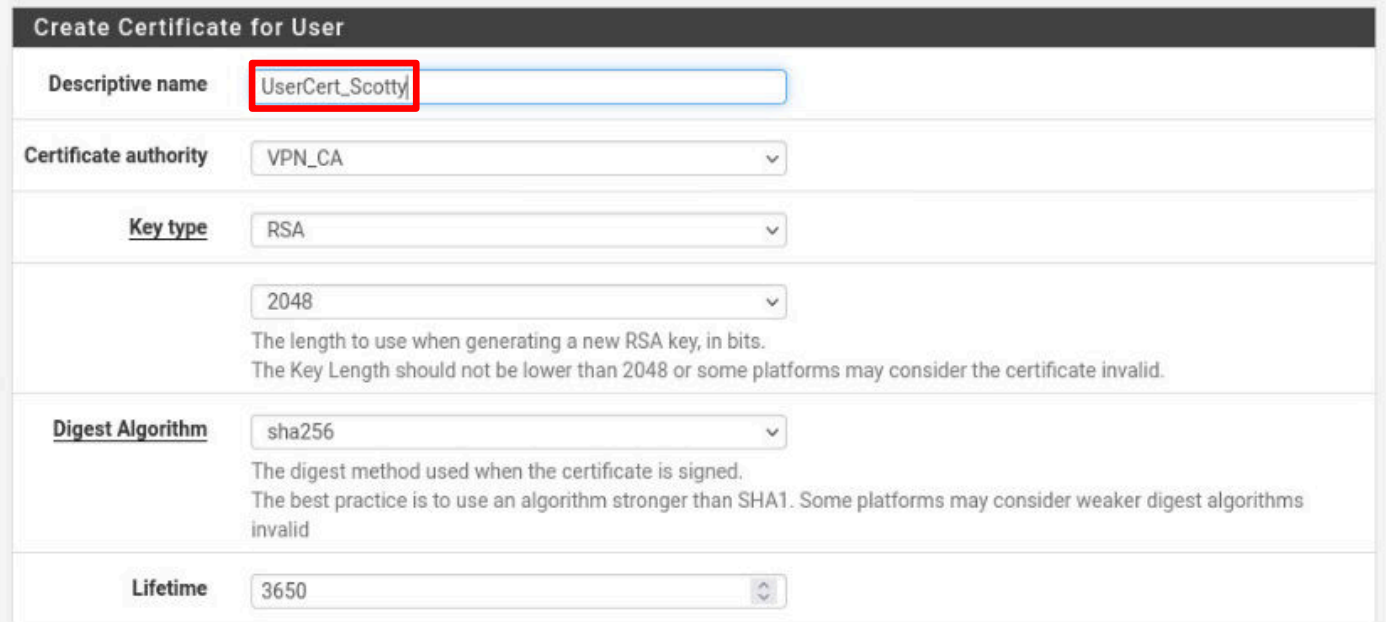
Not member of: Member of:

>> Move to "Member of" list << Move to "Not member of" list

Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.

Certificate: ☒ Click 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.



Create Certificate for User

Descriptive name

Certificate authority

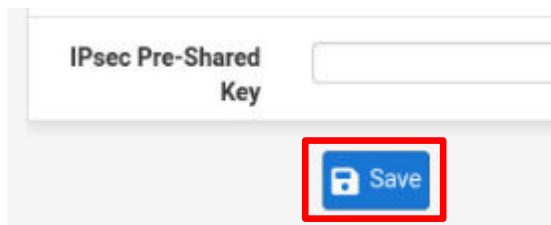
Key type

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


Digest Algorithm
The digest method used when the certificate is signed.
The best practice is to use an algorithm stronger than SHA1. Some platforms may consider weaker digest algorithms invalid

Lifetime

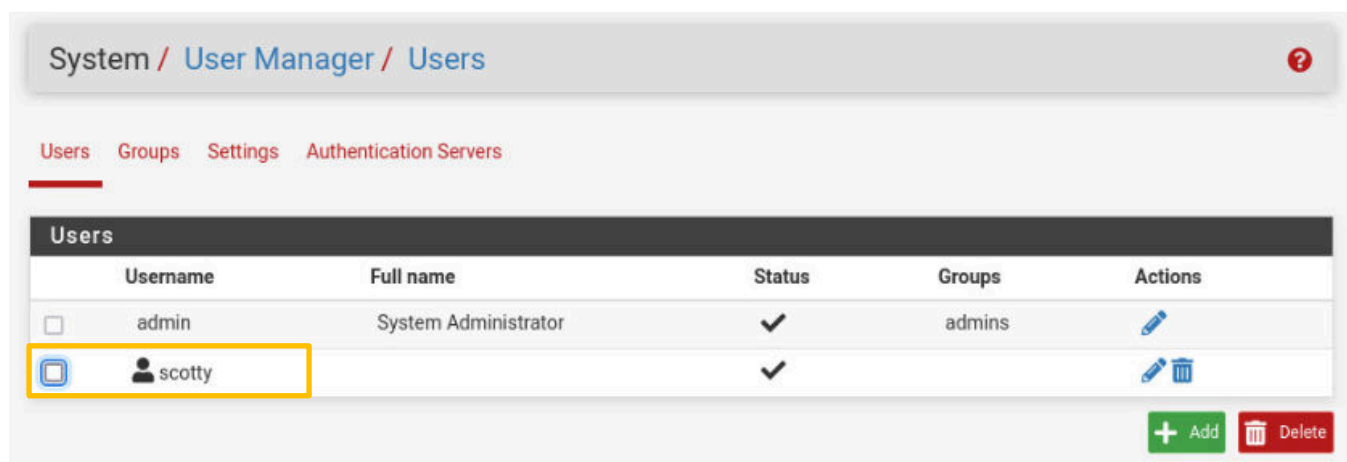
16. Scroll to the bottom of the page and click the **Save** button.



IPsec Pre-Shared Key

 Save

You will see the new user added to the list.



System / User Manager / Users

Users Groups Settings Authentication Servers

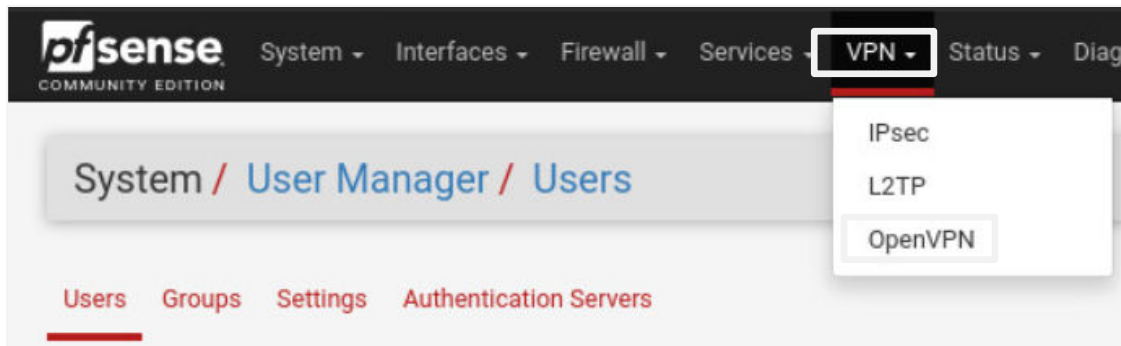
Users					
	Username	Full name	Status	Groups	Actions
<input type="checkbox"/>	admin	System Administrator	✓	admins	
<input checked="" type="checkbox"/>	scotty		✓		

Add Delete

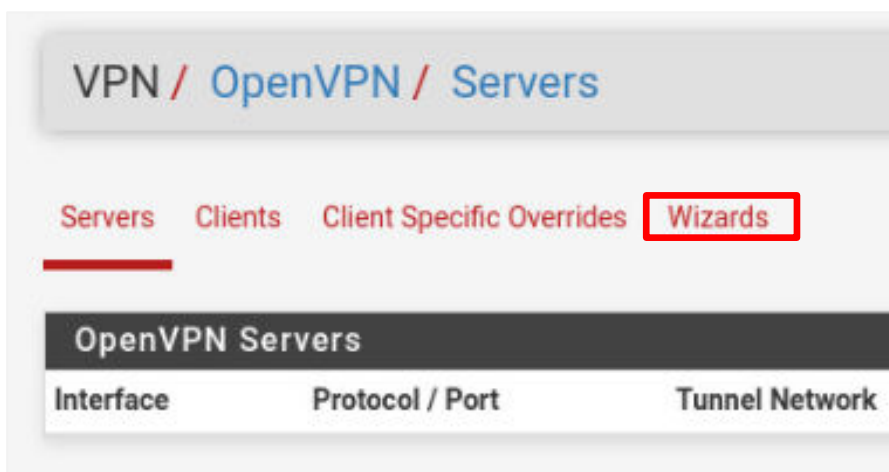
17. Remain on the *MintOS* computer and continue to the next task.

3.2 Setup OpenVPN on the pfSense Firewall

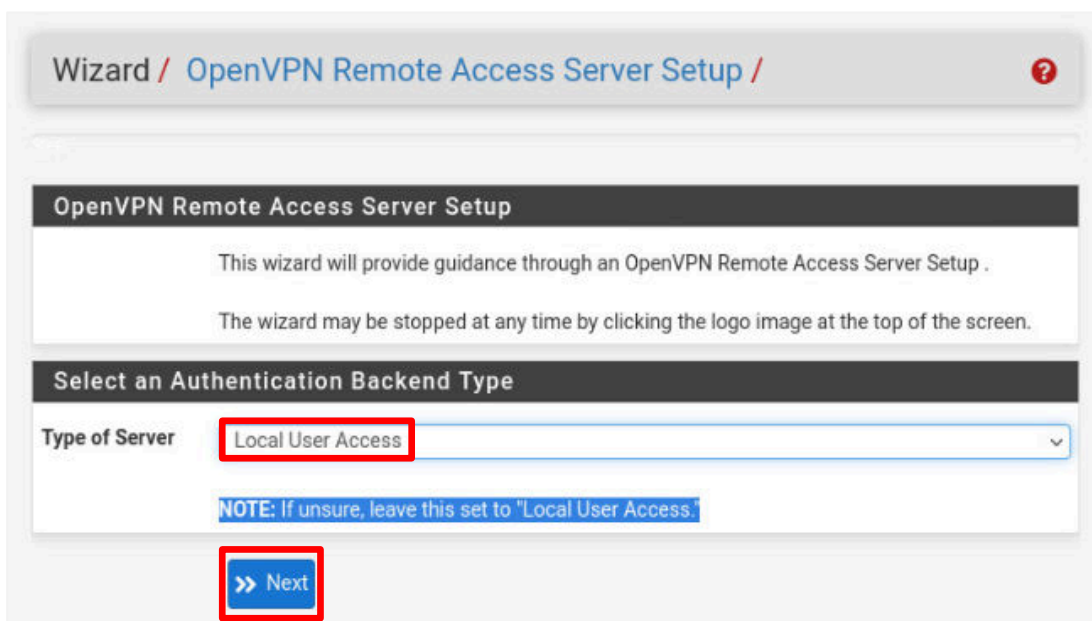
1. Click **VPN** on the top menu and then click on **OpenVPN** in the dropdown list.



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



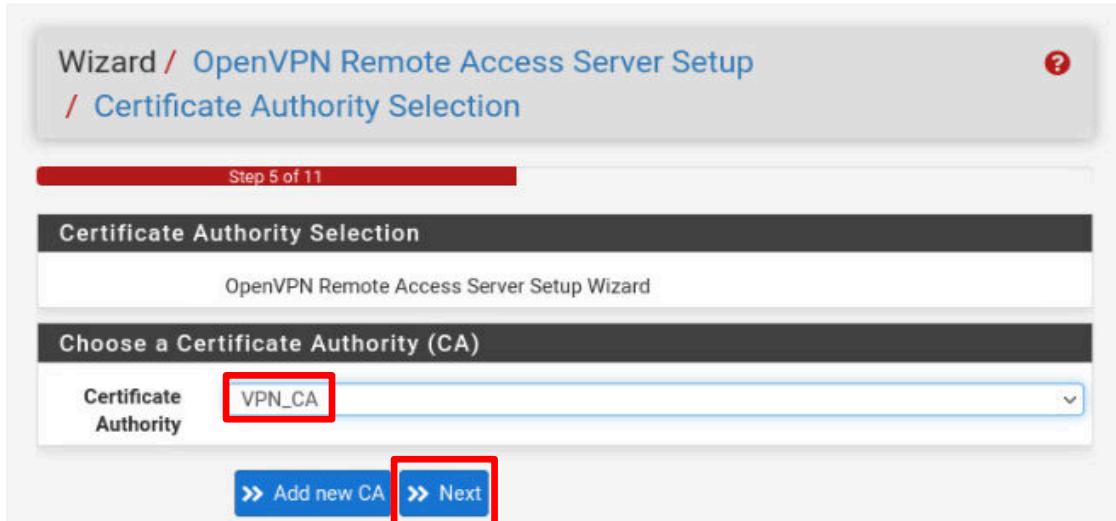
3. Make sure **Local User Access** is selected and click **Next**.





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**.

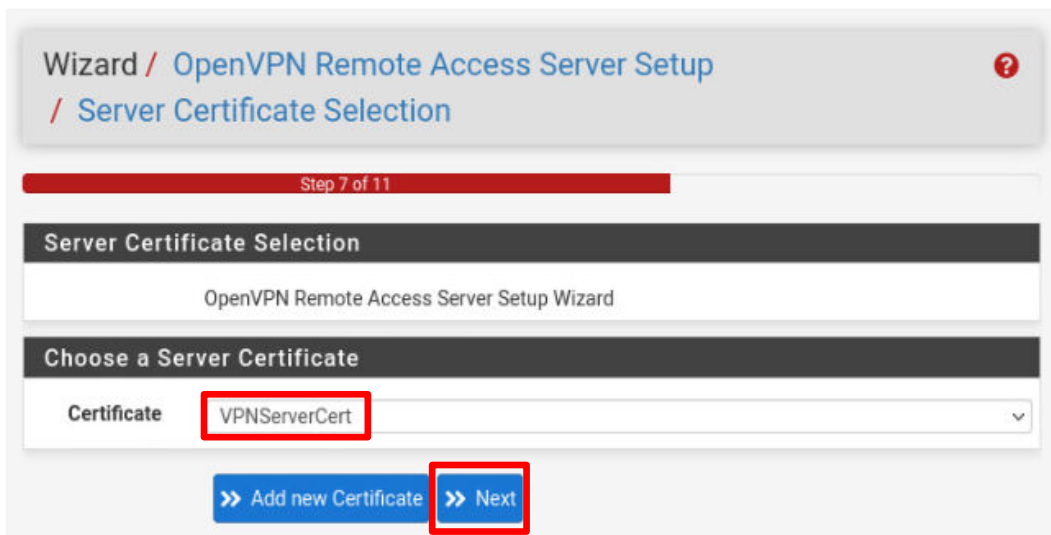


The screenshot shows the 'Certificate Authority Selection' step of the wizard. The breadcrumb trail is 'Wizard / OpenVPN Remote Access Server Setup / Certificate Authority Selection'. A progress bar indicates 'Step 5 of 11'. The title is 'Certificate Authority Selection'. Below it, the text 'OpenVPN Remote Access Server Setup Wizard' is displayed. The main section is 'Choose a Certificate Authority (CA)'. It features a dropdown menu labeled 'Certificate Authority' with 'VPN_CA' selected. At the bottom, there are two buttons: '>> Add new CA' and '>> Next'. The 'Next' button is highlighted with a red box.



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**.



The screenshot shows the 'Server Certificate Selection' step of the wizard. The breadcrumb trail is 'Wizard / OpenVPN Remote Access Server Setup / Server Certificate Selection'. A progress bar indicates 'Step 7 of 11'. The title is 'Server Certificate Selection'. Below it, the text 'OpenVPN Remote Access Server Setup Wizard' is displayed. The main section is 'Choose a Server Certificate'. It features a dropdown menu labeled 'Certificate' with 'VPNServerCert' selected. At the bottom, there are two buttons: '>> Add new Certificate' and '>> Next'. The 'Next' button is highlighted with a red box.

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

<i>Interface</i>	WAN (should already be selected)
<i>Protocol</i>	UDP on IPv4 only (should already be selected)
<i>Local Port</i>	1194 (should already be selected)
<i>Description</i>	VPN_Server

Wizard / OpenVPN Remote Access Server Setup / Server Setup ?

Step 9 of 11

Server Setup

OpenVPN Remote Access Server Setup Wizard

General OpenVPN Server Information

Interface WAN ▼
 The interface where OpenVPN will listen for incoming connections (typically WAN.)

Protocol UDP on IPv4 only ▼
 Protocol to use for OpenVPN connections. If unsure, leave this set to UDP.

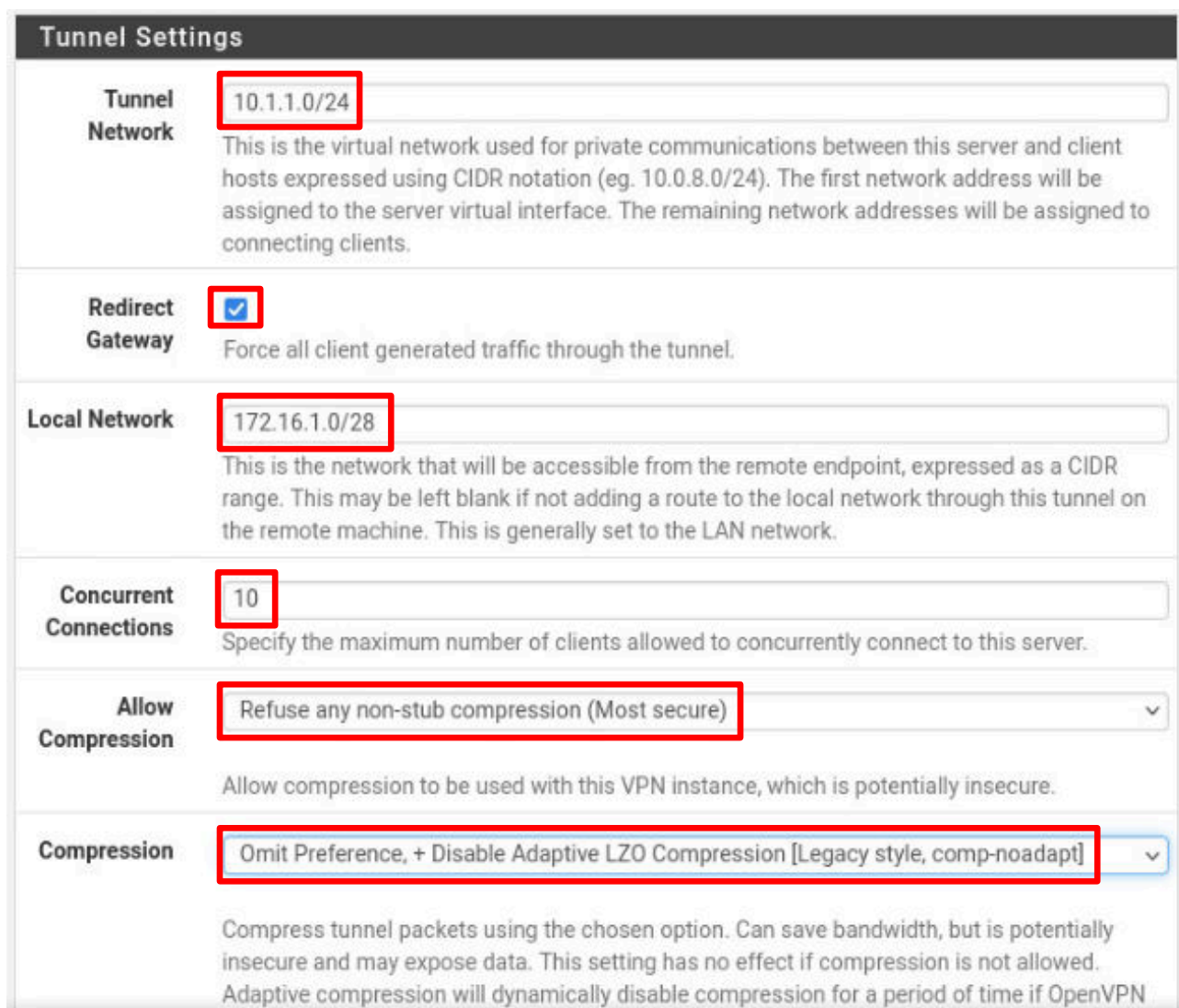
Local Port 1194
 Local port upon which OpenVPN will listen for connections. The default port is 1194. This can be left at its default unless a different port needs to be used.

Description VPN_Server
 A name for this OpenVPN instance, for administrative reference. It can be set however desired, but is often used to distinguish the purpose of the service (e.g. "Remote Technical Staff"). It is also used by OpenVPN Client Export to identify this VPN on clients.

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

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

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



Tunnel Settings

Tunnel Network 10.1.1.0/24
This is the virtual network used for private communications between this server and client hosts expressed using CIDR notation (eg. 10.0.8.0/24). The first network address will be assigned to the server virtual interface. The remaining network addresses will be assigned to connecting clients.

Redirect Gateway ☒
Force all client generated traffic through the tunnel.

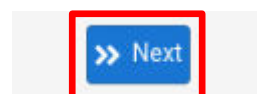
Local Network 172.16.1.0/28
This is the network that will be accessible from the remote endpoint, expressed as a CIDR range. This may be left blank if not adding a route to the local network through this tunnel on the remote machine. This is generally set to the LAN network.

Concurrent Connections 10
Specify the maximum number of clients allowed to concurrently connect to this server.

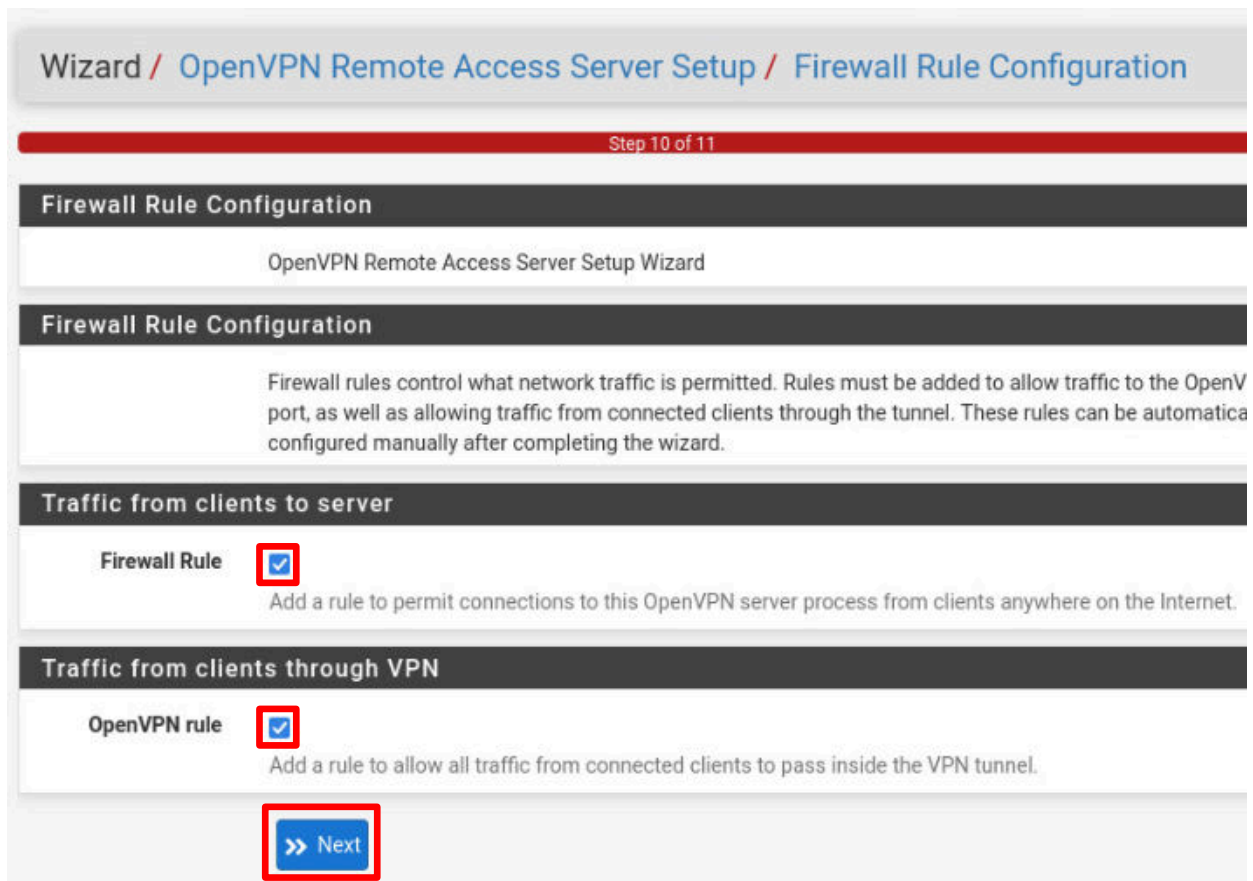
Allow Compression Refuse any non-stub compression (Most secure) ▾
Allow compression to be used with this VPN instance, which is potentially insecure.

Compression Omit Preference, + Disable Adaptive LZO Compression [Legacy style, comp-noadapt] ▾
Compress tunnel packets using the chosen option. Can save bandwidth, but is potentially insecure and may expose data. This setting has no effect if compression is not allowed. Adaptive compression will dynamically disable compression for a period of time if OpenVPN

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**.



Wizard / OpenVPN Remote Access Server Setup / Firewall Rule Configuration

Step 10 of 11

Firewall Rule Configuration

OpenVPN Remote Access Server Setup Wizard

Firewall Rule Configuration

Firewall rules control what network traffic is permitted. Rules must be added to allow traffic to the OpenVPN port, as well as allowing traffic from connected clients through the tunnel. These rules can be automatically configured manually after completing the wizard.

Traffic from clients to server

Firewall Rule ☒

Add a rule to permit connections to this OpenVPN server process from clients anywhere on the Internet.

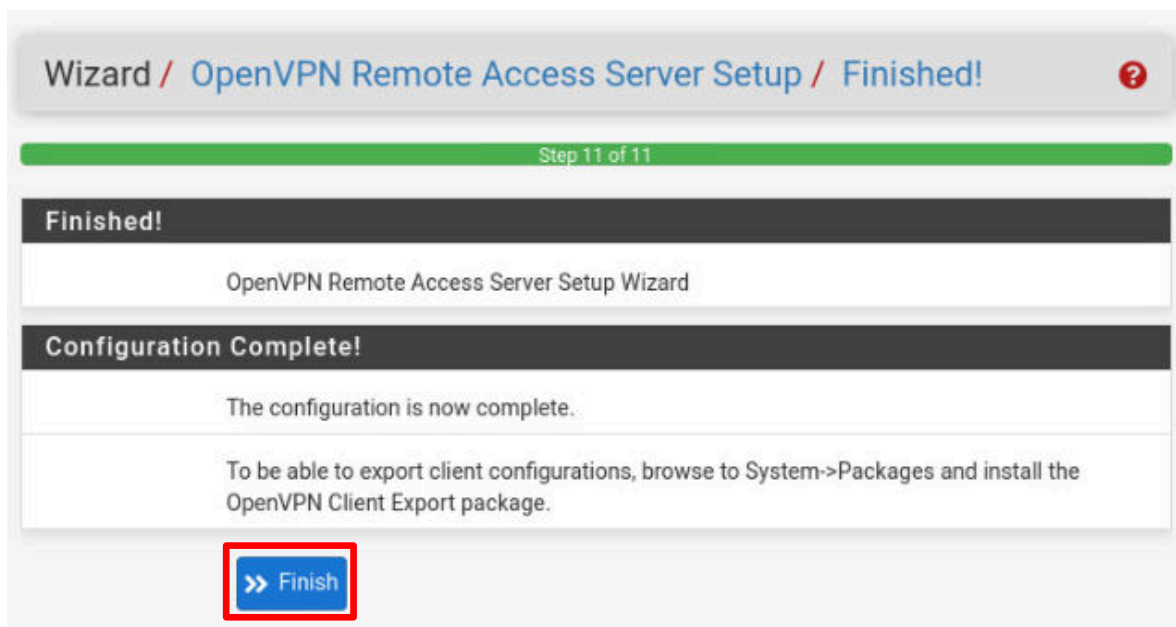
Traffic from clients through VPN

OpenVPN rule ☒

Add a rule to allow all traffic from connected clients to pass inside the VPN tunnel.

[» Next](#)

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



Wizard / OpenVPN Remote Access Server Setup / Finished!

Step 11 of 11

Finished!

OpenVPN Remote Access Server Setup Wizard

Configuration Complete!

The configuration is now complete.

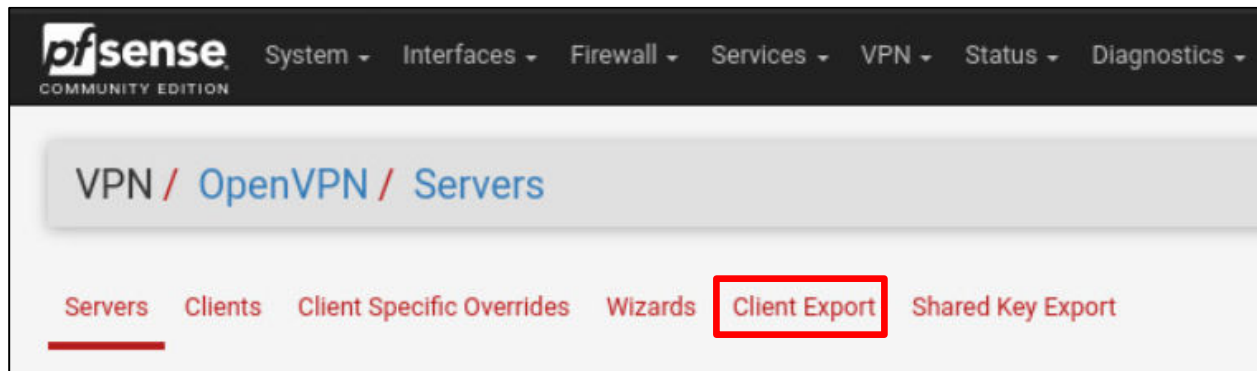
To be able to export client configurations, browse to System->Packages and install the OpenVPN Client Export package.

[» Finish](#)

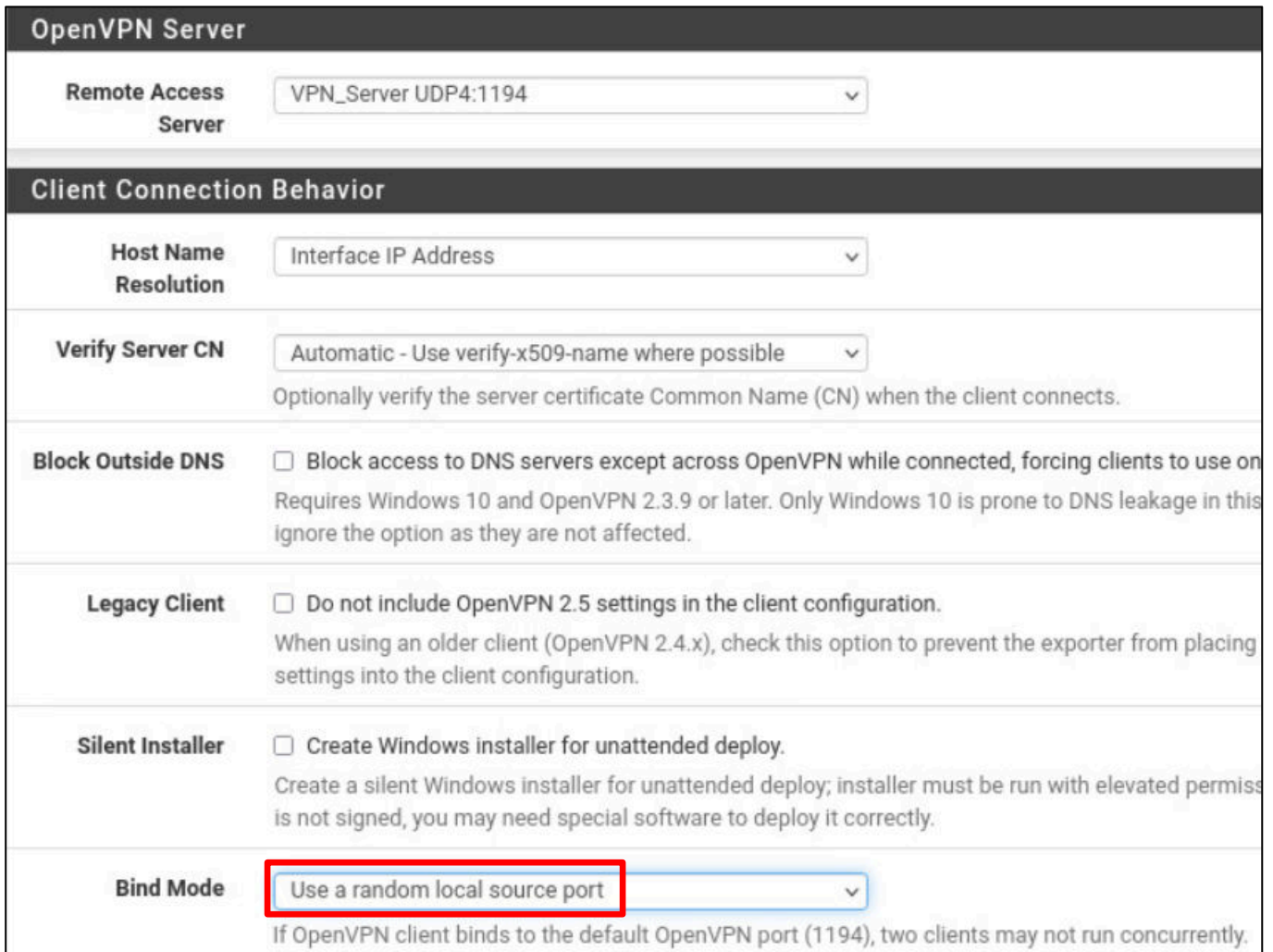
11. Remain in the *MintOS* tab and leave the *pfSense* web page open and proceed to the next task.

3.3 Export VPN Client Configuration Data

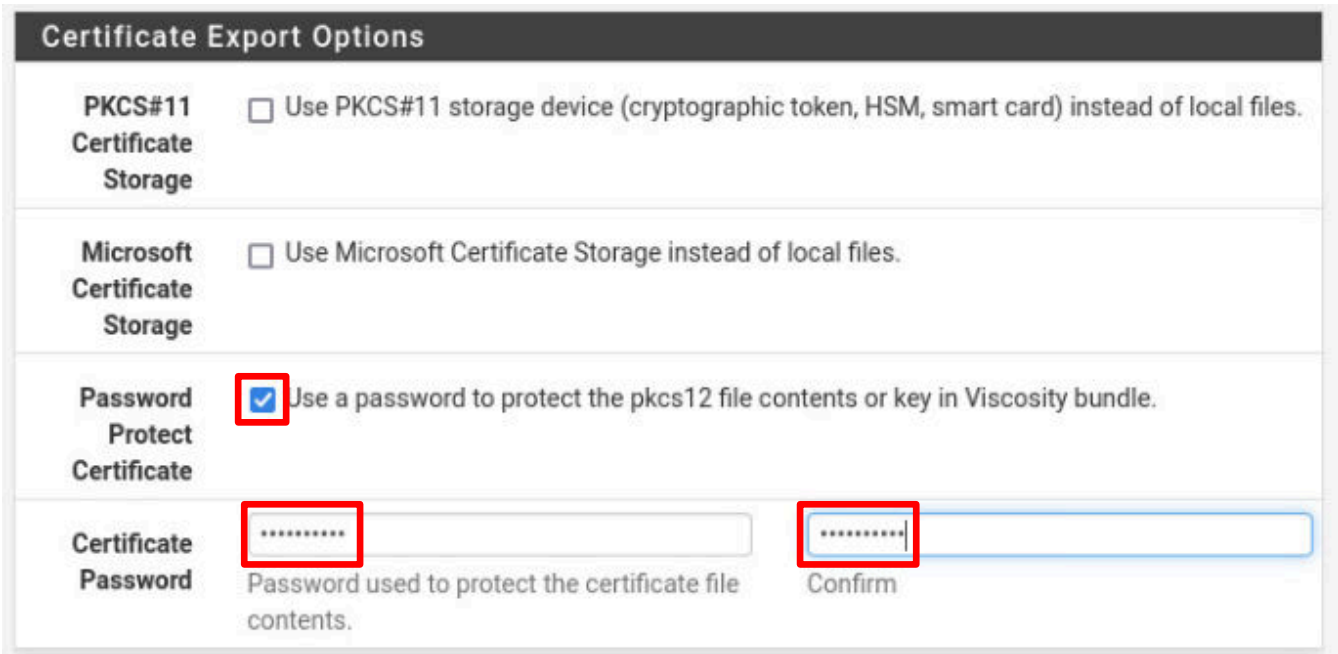
1. On the *VPN/OpenVPN/Servers* page, click on **Client Export**.



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

The screenshot displays the 'OpenVPN Server' configuration page. The 'Client Connection Behavior' section is expanded. It contains several settings: 'Remote Access Server' (set to 'VPN_Server UDP4:1194'), 'Host Name Resolution' (set to 'Interface IP Address'), 'Verify Server CN' (set to 'Automatic - Use verify-x509-name where possible'), 'Block Outside DNS' (unchecked), 'Legacy Client' (unchecked), 'Silent Installer' (unchecked), and 'Bind Mode' (set to 'Use a random local source port', which is highlighted with a red box). Below the 'Bind Mode' dropdown, a note states: 'If OpenVPN client binds to the default OpenVPN port (1194), two clients may not run concurrently.'

- 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.



Certificate Export Options

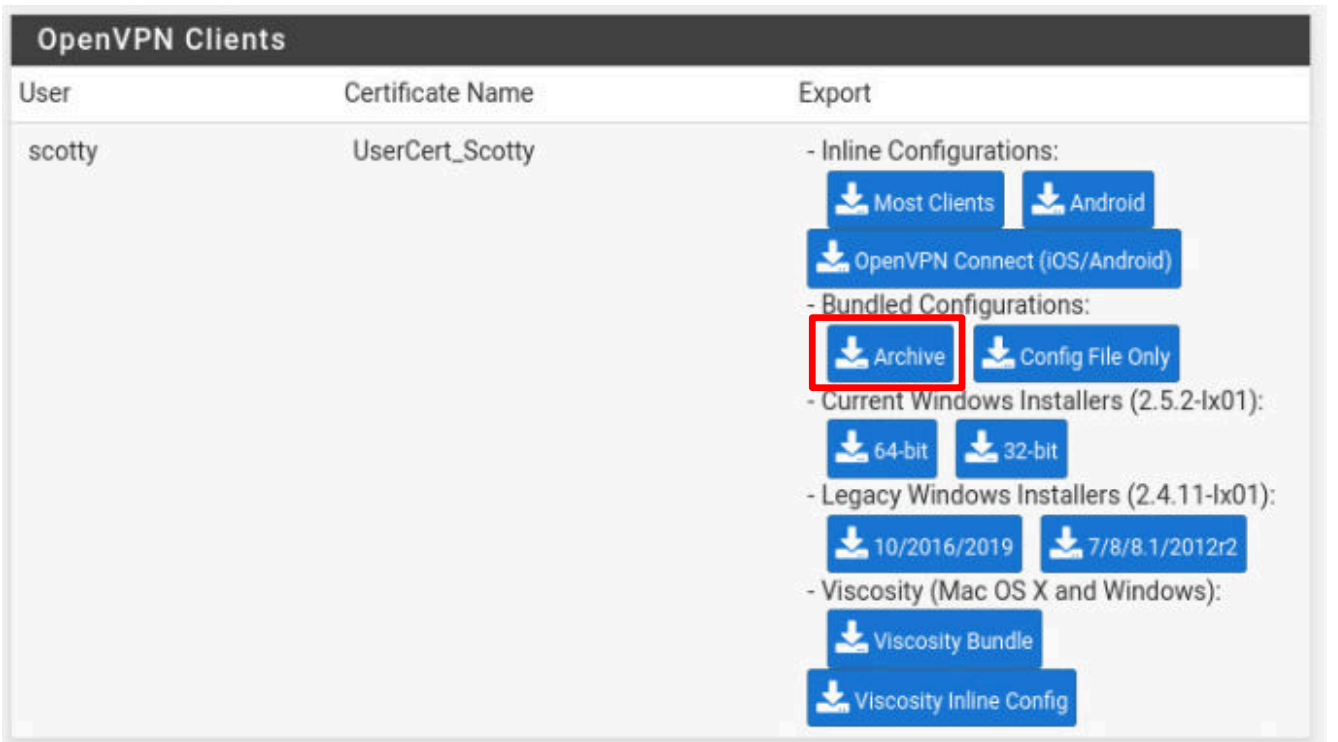
PKCS#11 Certificate Storage ☐ Use PKCS#11 storage device (cryptographic token, HSM, smart card) instead of local files.

Microsoft Certificate Storage ☐ Use Microsoft Certificate Storage instead of local files.

Password Protect Certificate ☒ Use a password to protect the pkcs12 file contents or key in Viscosity bundle.

Certificate Password Password used to protect the certificate file contents. Confirm

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



OpenVPN Clients

User	Certificate Name	Export
scotty	UserCert_Scotty	<p>- Inline Configurations:</p> <p>Most Clients Android</p> <p>OpenVPN Connect (iOS/Android)</p> <p>- Bundled Configurations:</p> <p>Archive Config File Only</p> <p>- Current Windows Installers (2.5.2-lx01):</p> <p>64-bit 32-bit</p> <p>- Legacy Windows Installers (2.4.11-lx01):</p> <p>10/2016/2019 7/8/8.1/2012r2</p> <p>- Viscosity (Mac OS X and Windows):</p> <p>Viscosity Bundle</p> <p>Viscosity Inline Config</p>

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

- 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
```

```
(sysadmin@kali)-[~]
$ ping 172.16.1.10 -c2
PING 172.16.1.10 (172.16.1.10) 56(84) bytes of data.

— 172.16.1.10 ping statistics —
2 packets transmitted, 0 received, 100% packet loss, time 1006ms


(sysadmin@kali)-[~]
$ ping 172.16.1.2 -c2
PING 172.16.1.2 (172.16.1.2) 56(84) bytes of data.

— 172.16.1.2 ping statistics —
2 packets transmitted, 0 received, 100% packet loss, time 1005ms
```

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

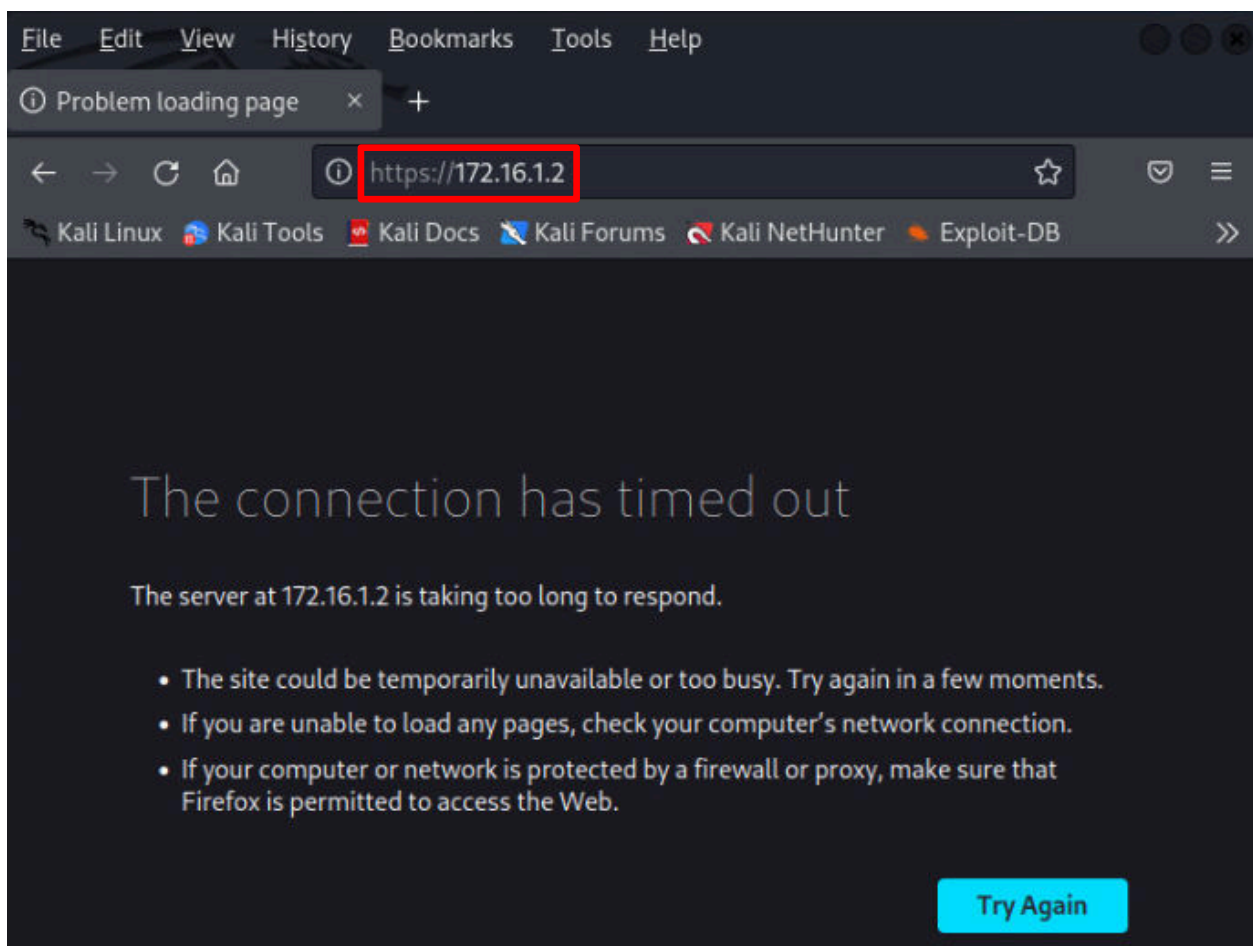
```
ssh 172.16.1.10
```

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



```
(sysadmin@kali)-[~]  
$ ssh 172.16.1.10  
ssh: connect to host 172.16.1.10 port 22: Connection timed out
```

- 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`.

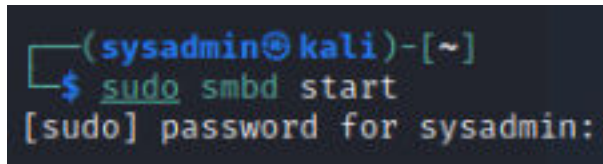


After a couple of minutes, the connection will time out.

- Close the browser window.

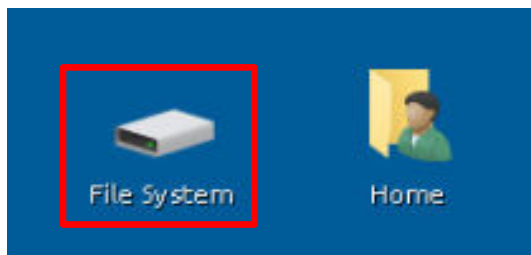
6. In the terminal window, type the following command to start the *Samba* service on the *Kali* computer. If asked for the **[sudo] password for sysadmin**, type: **NDGlabpass123!**

```
sudo smb start
```

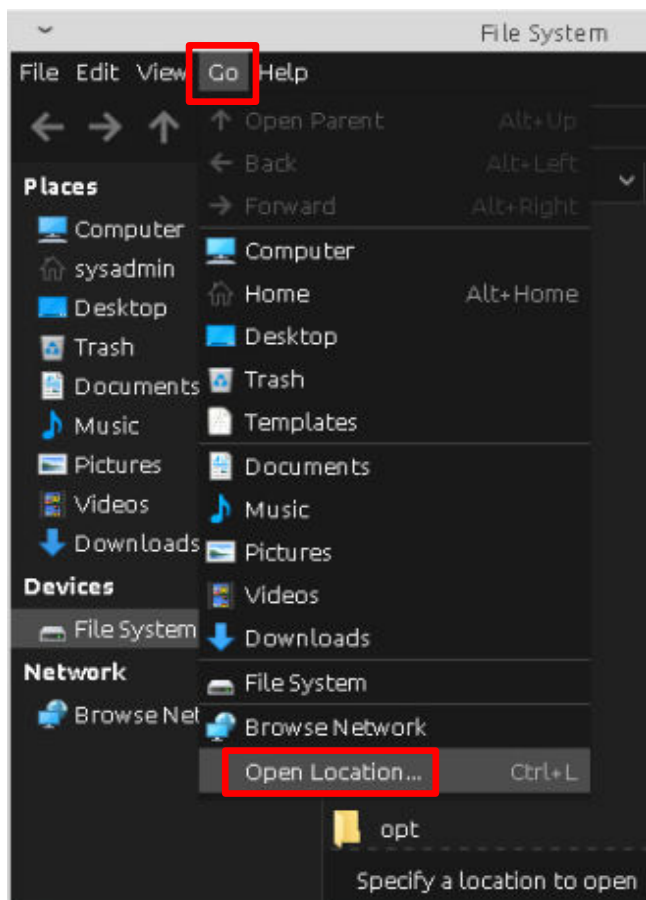


```
(sysadmin@kali)-[~]  
$ sudo smb start  
[sudo] password for sysadmin:
```

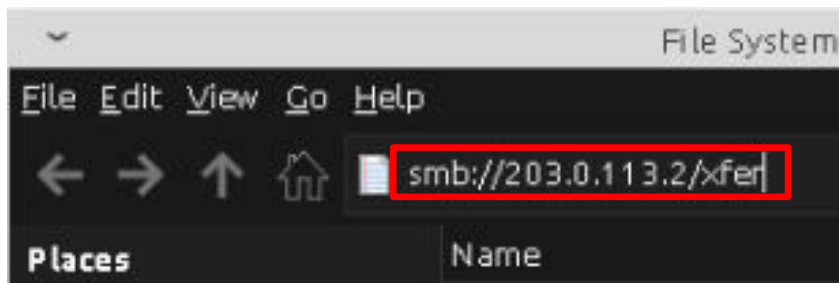
7. Set the focus on the **MintOS** computer and then double-click on the **File System** icon on the desktop:



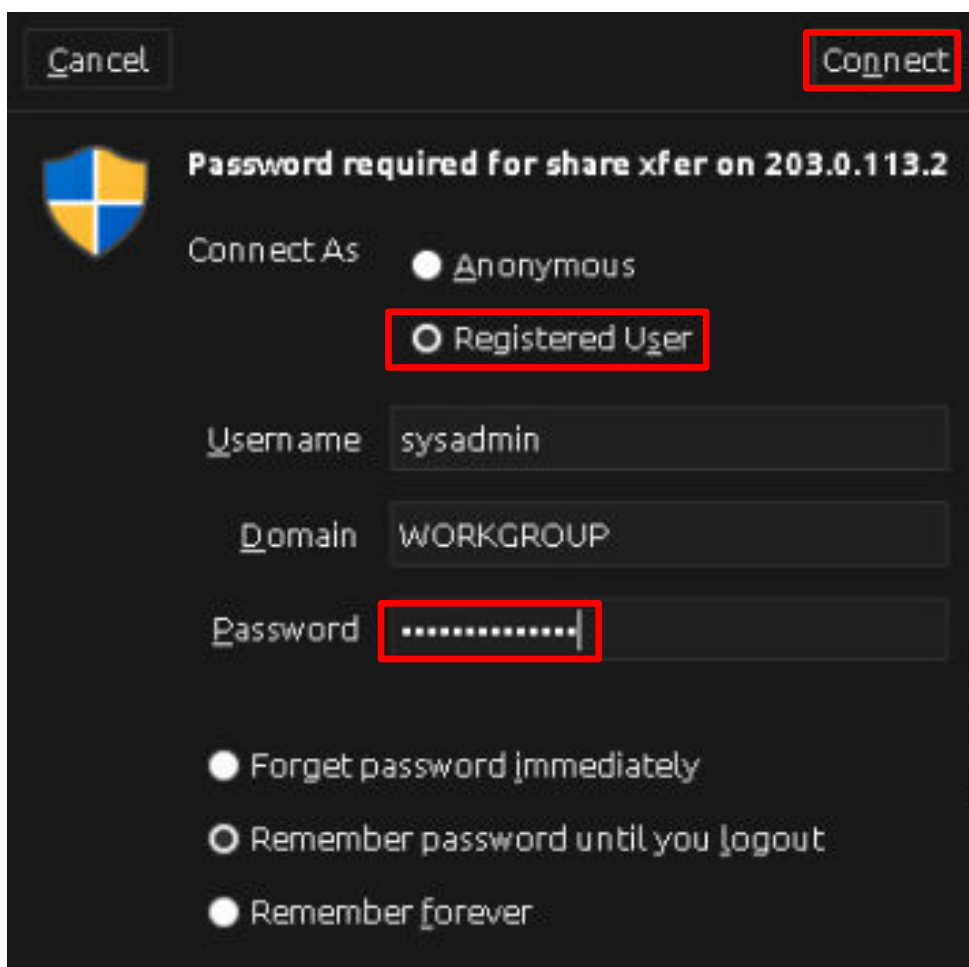
8. On the *File System* window, click on the **Go** menu item, and click on **Open Location** on the dropdown menu.



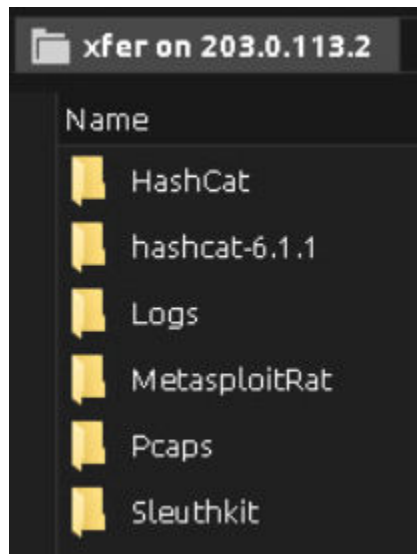
9. In the address bar, type in the location `smb://203.0.113.2/xfer` and press **Enter**.



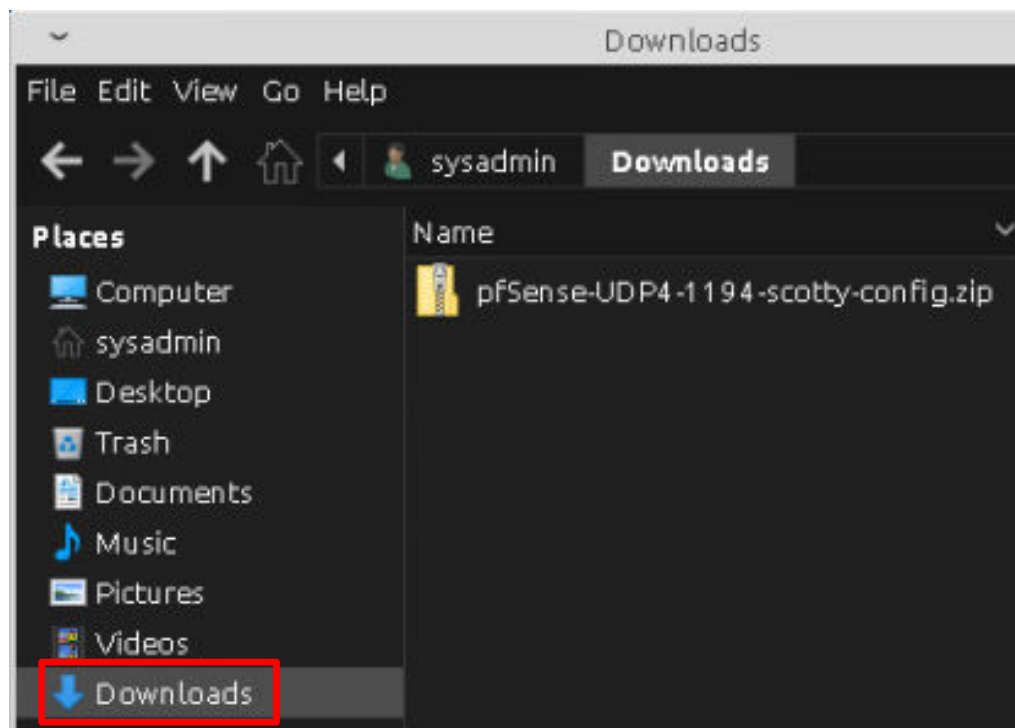
10. On the *Authentication* window, asking for the share password, click on the **Registered User** radio button, confirm the *Username* is `sysadmin` and the *Domain* is `WORKGROUP`. In the *Password* field, type `NDGlabpass123!` and then click **Connect** in the upper-right of the window.



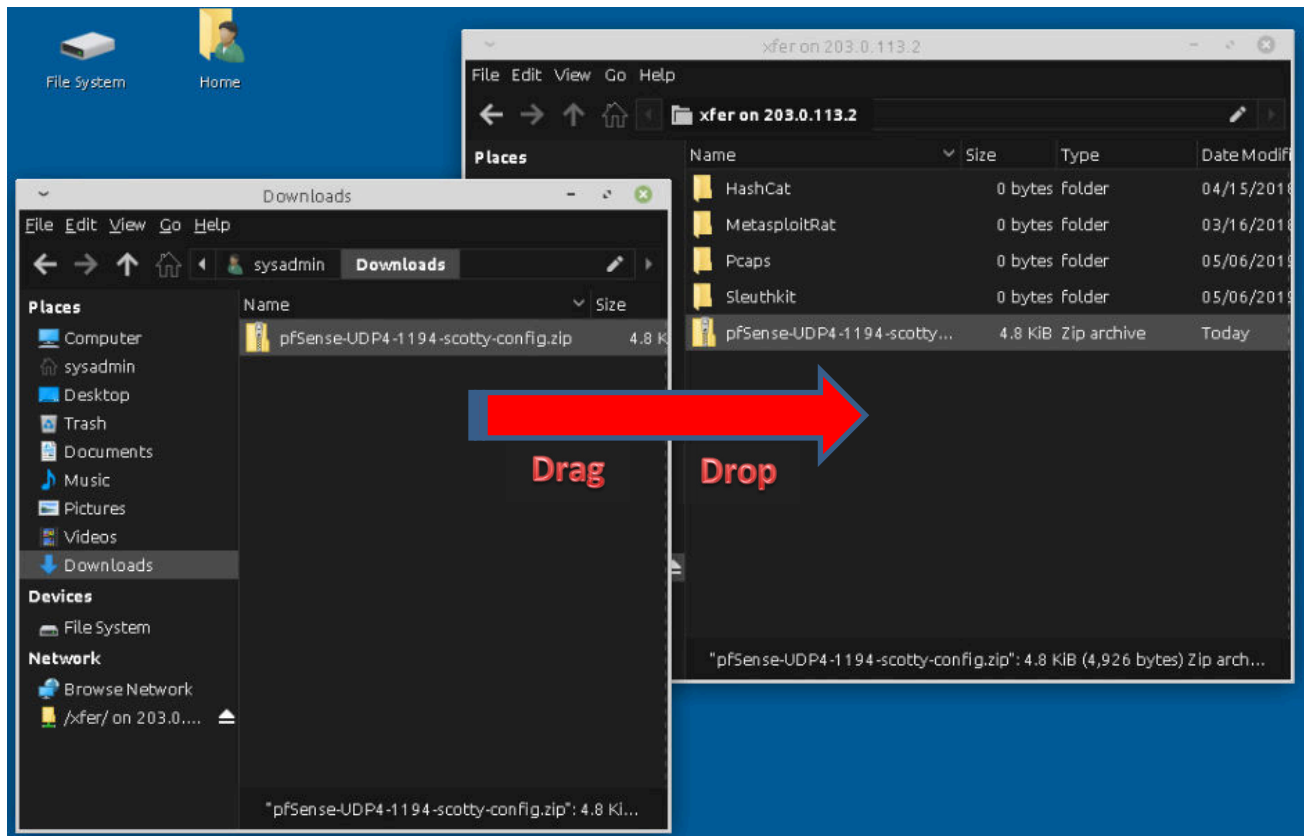
You should see the window with the six folders that are in the *LabFiles* directory.



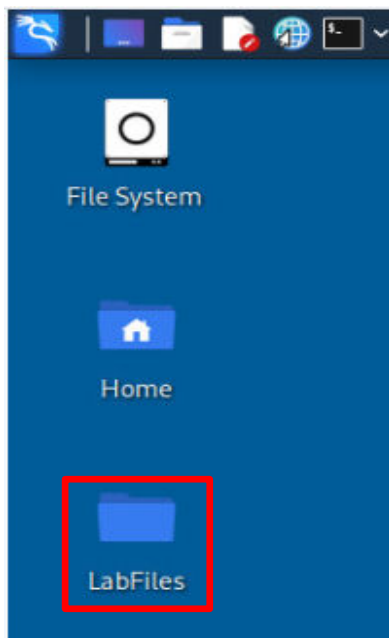
11. Double-click on the **File System** icon on the desktop again to open another *File System* instance.
12. Under **Places** on the left side of the window, click on **Downloads**.



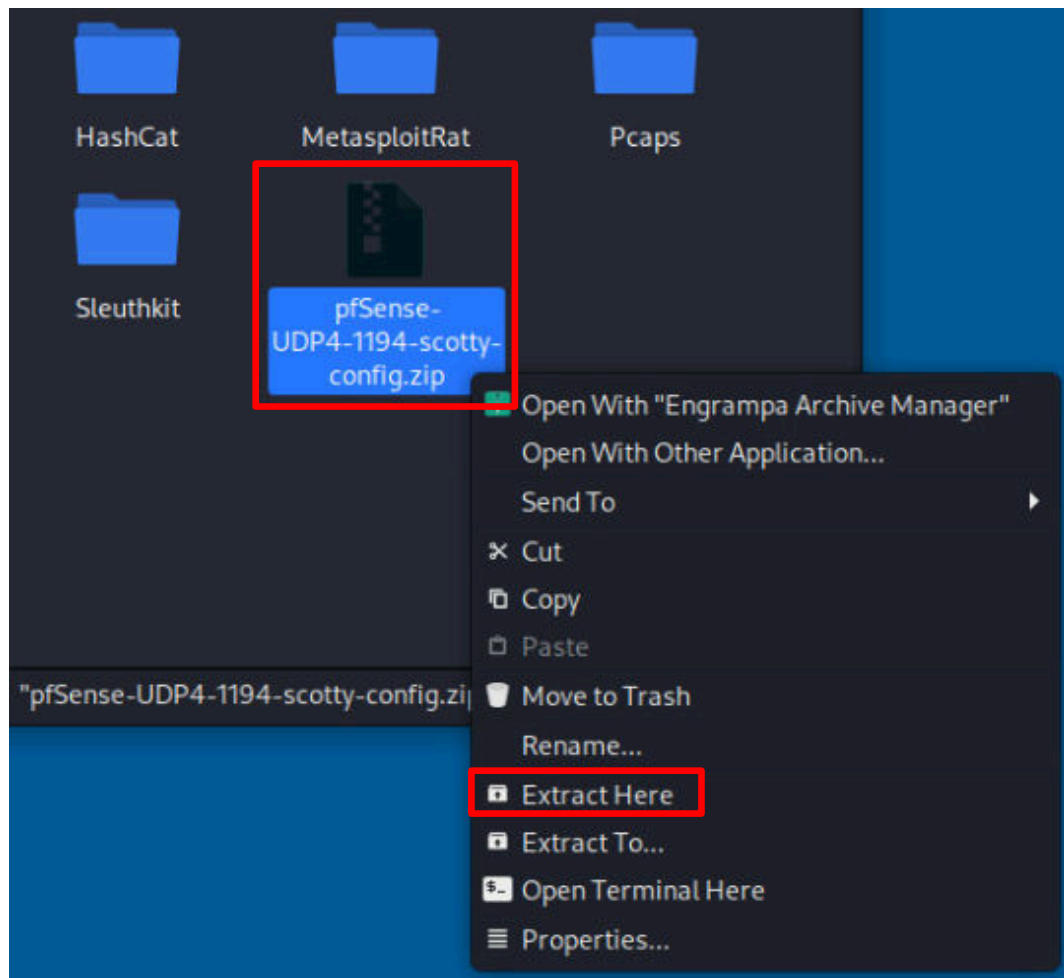
13. Drag and drop the **pfSense-UDP4-1194-scotty-config.zip** file in the *Downloads* folder to the *xfer on 203.0.113.2* folder (which is on the *Kali* computer).



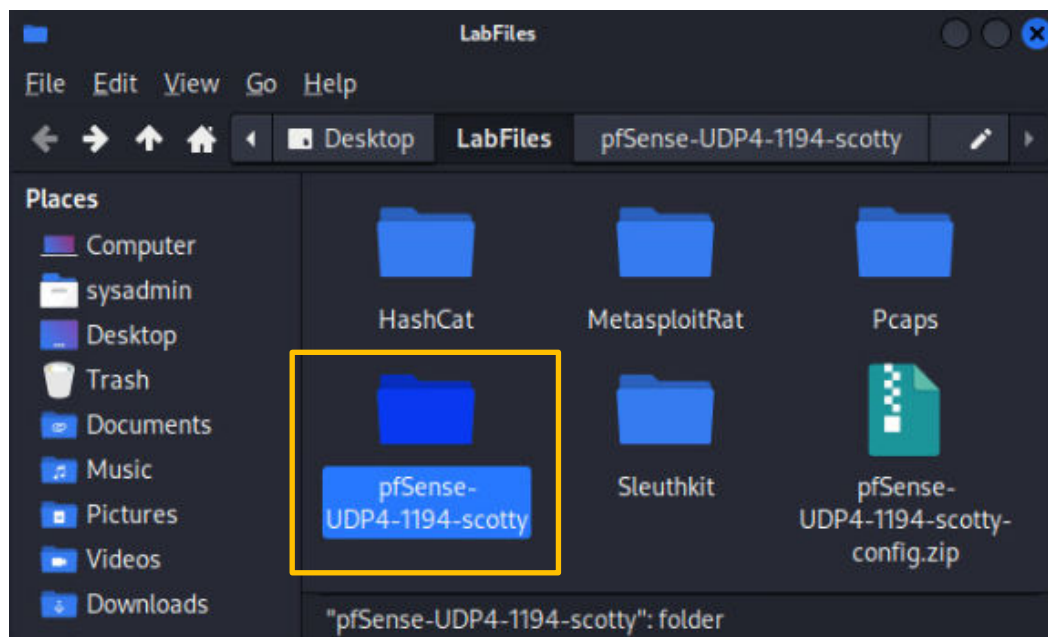
14. Close the two **File System** windows.
15. Return to the **Kali** computer. On the desktop, double-click to open the **LabFiles** folder.



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
```



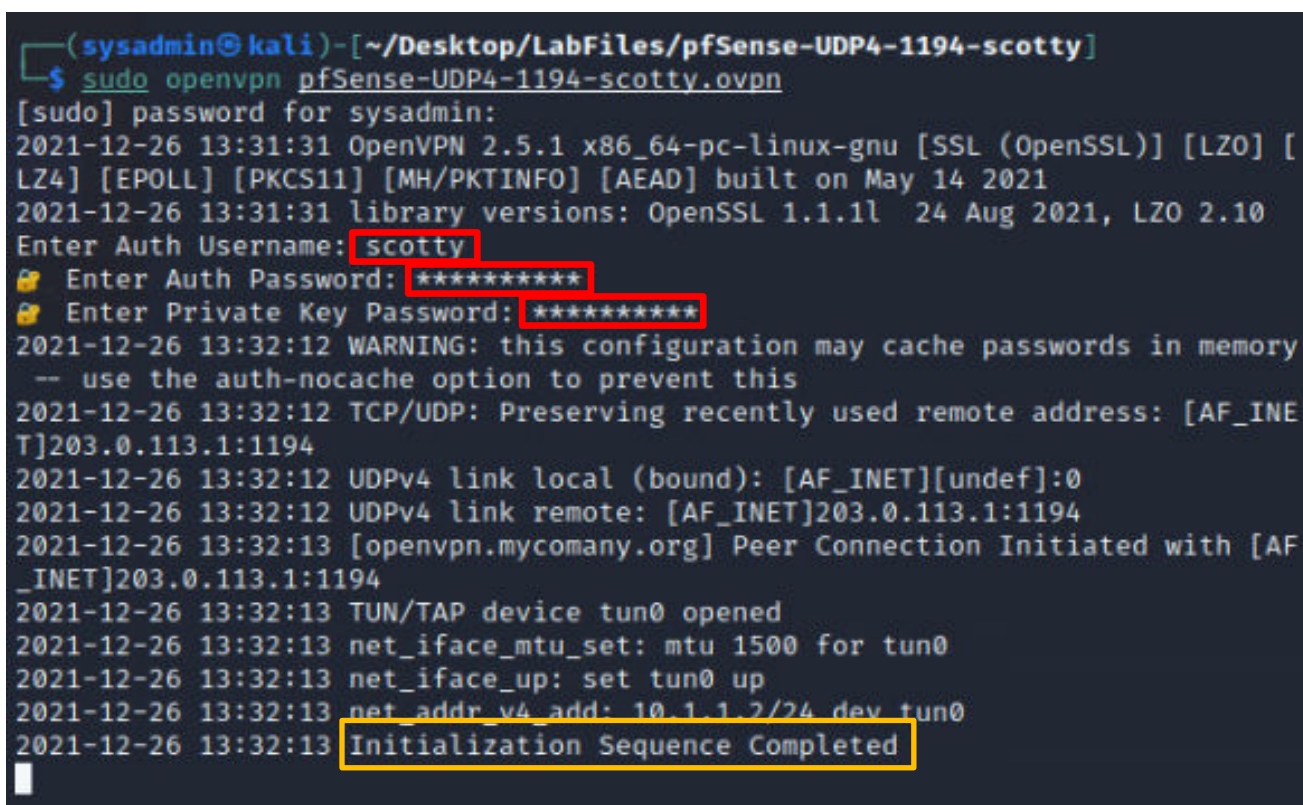
```
(sysadmin@kali)-[~]
$ cd Desktop/LabFiles/pfSense-UDP4-1194-scotty
```

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

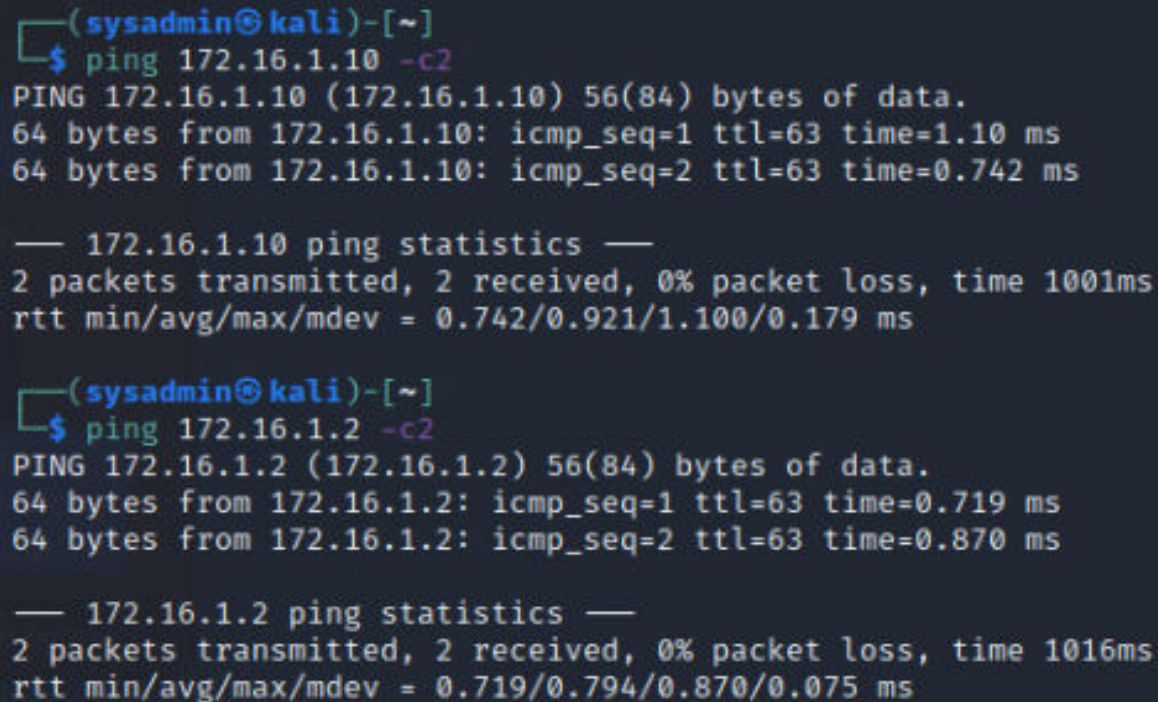


```
(sysadmin@kali)-[~/Desktop/LabFiles/pfSense-UDP4-1194-scotty]
$ sudo openvpn pfSense-UDP4-1194-scotty.ovpn
[sudo] password for sysadmin:
2021-12-26 13:31:31 OpenVPN 2.5.1 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [
LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] built on May 14 2021
2021-12-26 13:31:31 library versions: OpenSSL 1.1.1l 24 Aug 2021, LZO 2.10
Enter Auth Username: scotty
Enter Auth Password: *****
Enter Private Key Password: *****
2021-12-26 13:32:12 WARNING: this configuration may cache passwords in memory
-- use the auth-nocache option to prevent this
2021-12-26 13:32:12 TCP/UDP: Preserving recently used remote address: [AF_INE
T]203.0.113.1:1194
2021-12-26 13:32:12 UDPv4 link local (bound): [AF_INET][undef]:0
2021-12-26 13:32:12 UDPv4 link remote: [AF_INET]203.0.113.1:1194
2021-12-26 13:32:13 [openvpn.mycamany.org] Peer Connection Initiated with [AF
_INET]203.0.113.1:1194
2021-12-26 13:32:13 TUN/TAP device tun0 opened
2021-12-26 13:32:13 net_iface_mtu_set: mtu 1500 for tun0
2021-12-26 13:32:13 net_iface_up: set tun0 up
2021-12-26 13:32:13 net_addr_v4_add: 10.1.1.2/24 dev tun0
2021-12-26 13:32:13 Initialization Sequence Completed
```

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
```



```
(sysadmin@kali)-[~]  
$ ping 172.16.1.10 -c2  
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=1.10 ms  
64 bytes from 172.16.1.10: icmp_seq=2 ttl=63 time=0.742 ms  
  
— 172.16.1.10 ping statistics —  
2 packets transmitted, 2 received, 0% packet loss, time 1001ms  
rtt min/avg/max/mdev = 0.742/0.921/1.100/0.179 ms  
  
(sysadmin@kali)-[~]  
$ ping 172.16.1.2 -c2  
PING 172.16.1.2 (172.16.1.2) 56(84) bytes of data.  
64 bytes from 172.16.1.2: icmp_seq=1 ttl=63 time=0.719 ms  
64 bytes from 172.16.1.2: icmp_seq=2 ttl=63 time=0.870 ms  
  
— 172.16.1.2 ping statistics —  
2 packets transmitted, 2 received, 0% packet loss, time 1016ms  
rtt min/avg/max/mdev = 0.719/0.794/0.870/0.075 ms
```

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!

```
(sysadmin@kali)-[~]
$ ssh 172.16.1.10
The authenticity of host '172.16.1.10 (172.16.1.10)' can't be established.
ED25519 key fingerprint is SHA256:vOBYJ7UYiijFLONsFeOS3z0N1f80nVALSZPrzeaf1Y
.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '172.16.1.10' (ED25519) to the list of known hosts
.
sysadmin@172.16.1.10's password:
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.4.0-91-generic x86_64)

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

 * 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.

Last login: Sat Dec 25 21:06:56 2021
sysadmin@ubuntusrv:~$
```

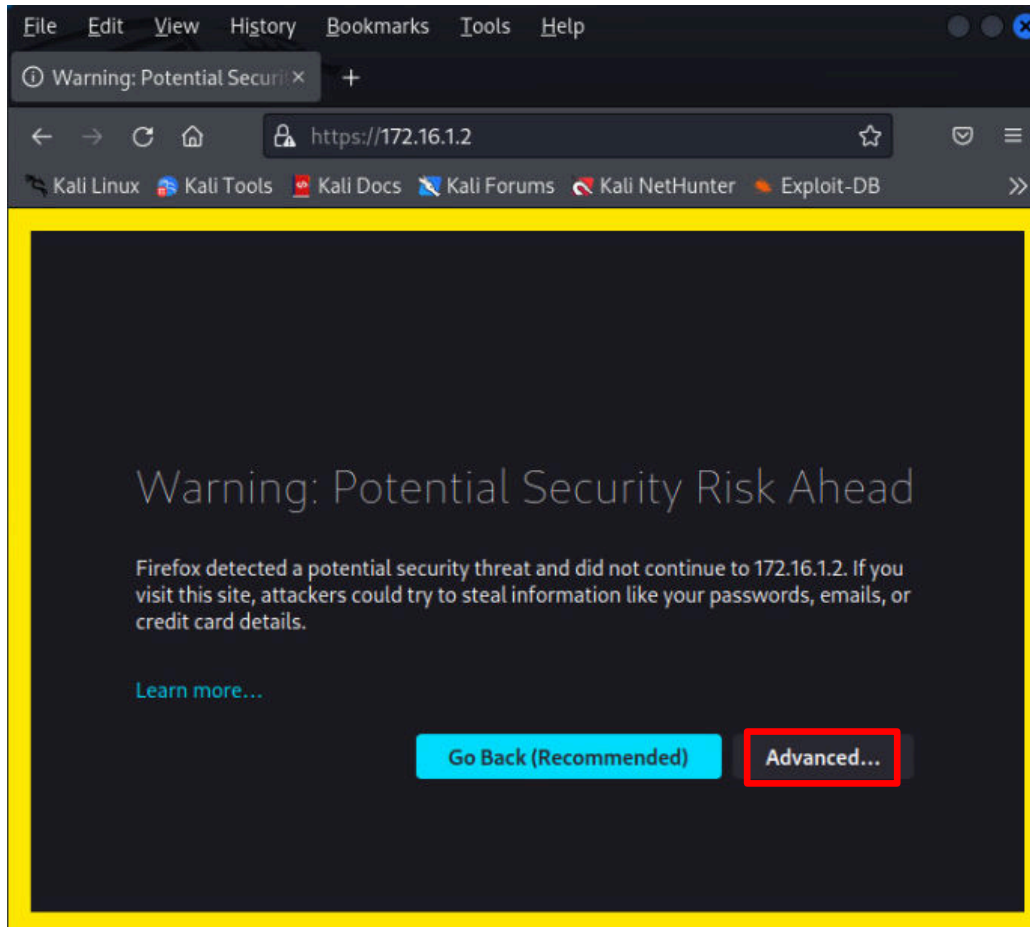
You should see the **sysadmin@ubuntusrv:~\$** prompt.

23. Leave the SSH session by typing the following:

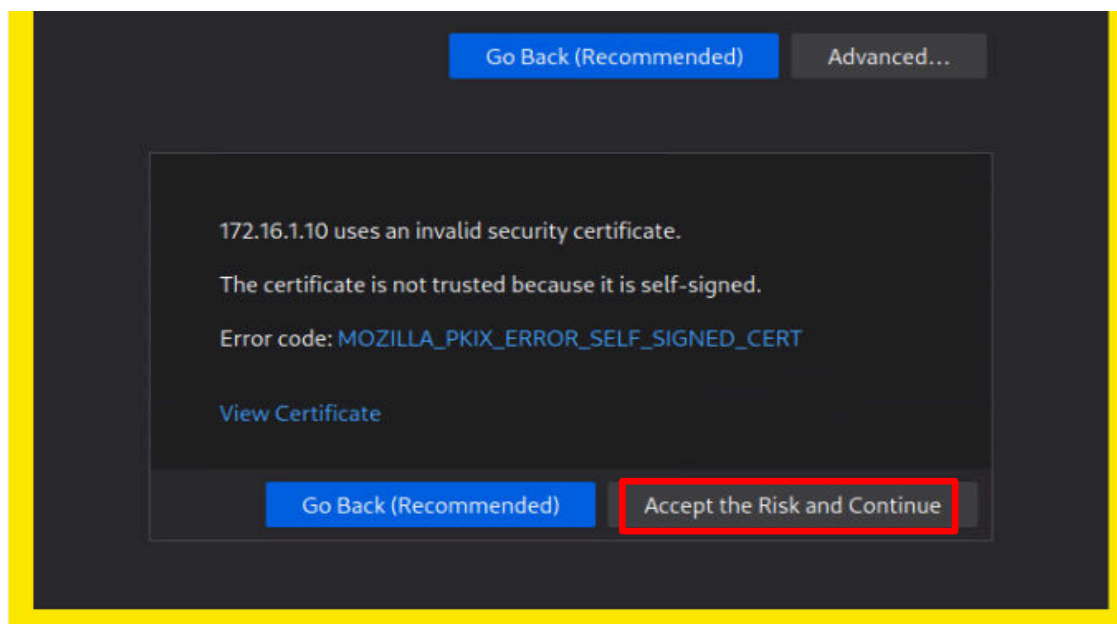
```
exit
```

```
sysadmin@ubuntusrv:~$ exit
logout
Connection to 172.16.1.10 closed.
```

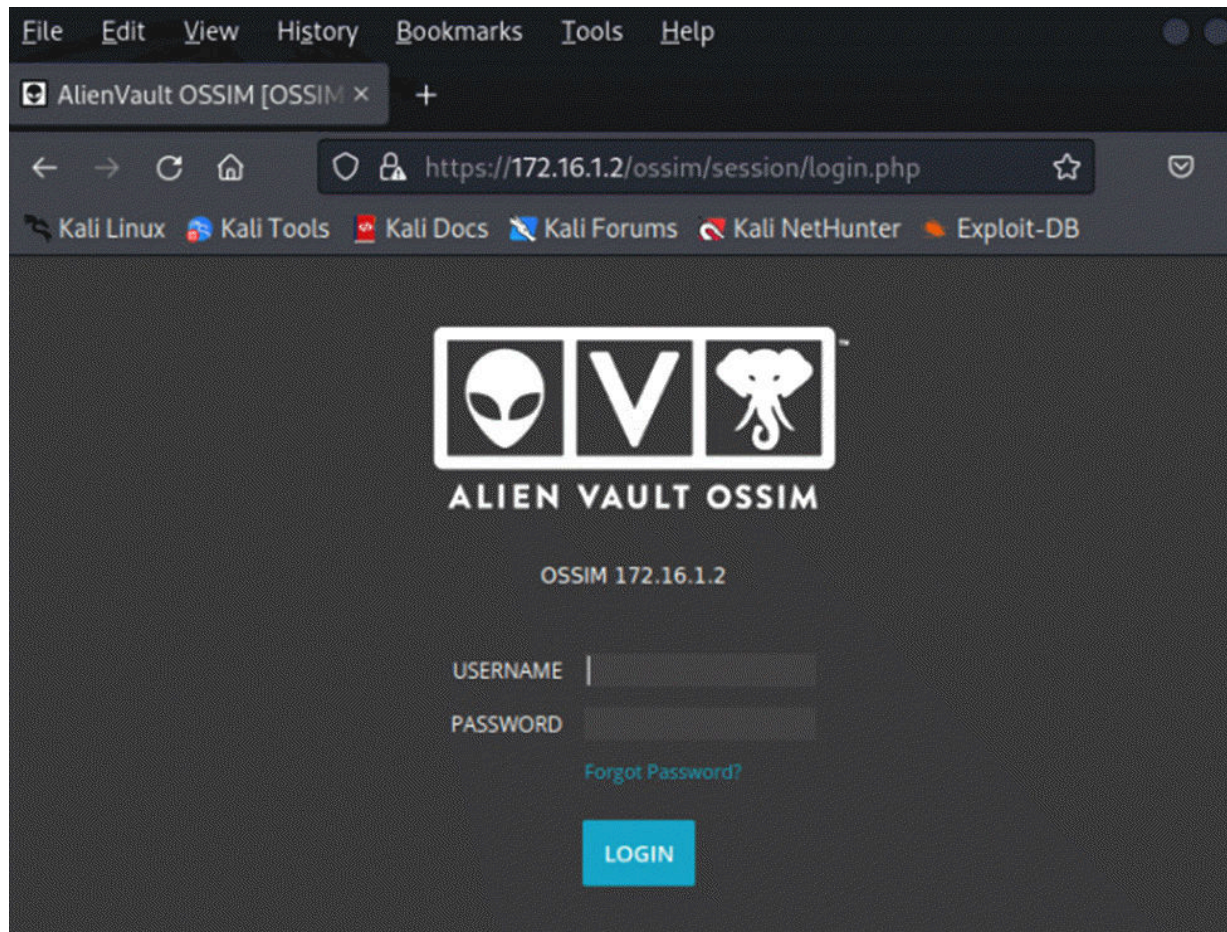
24. Open the *Firefox* web browser and try connecting to the *OSSIM Web Manager* by typing the address `https://172.16.1.2`. You should receive a security risk warning. Click the **Advanced** button.



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.



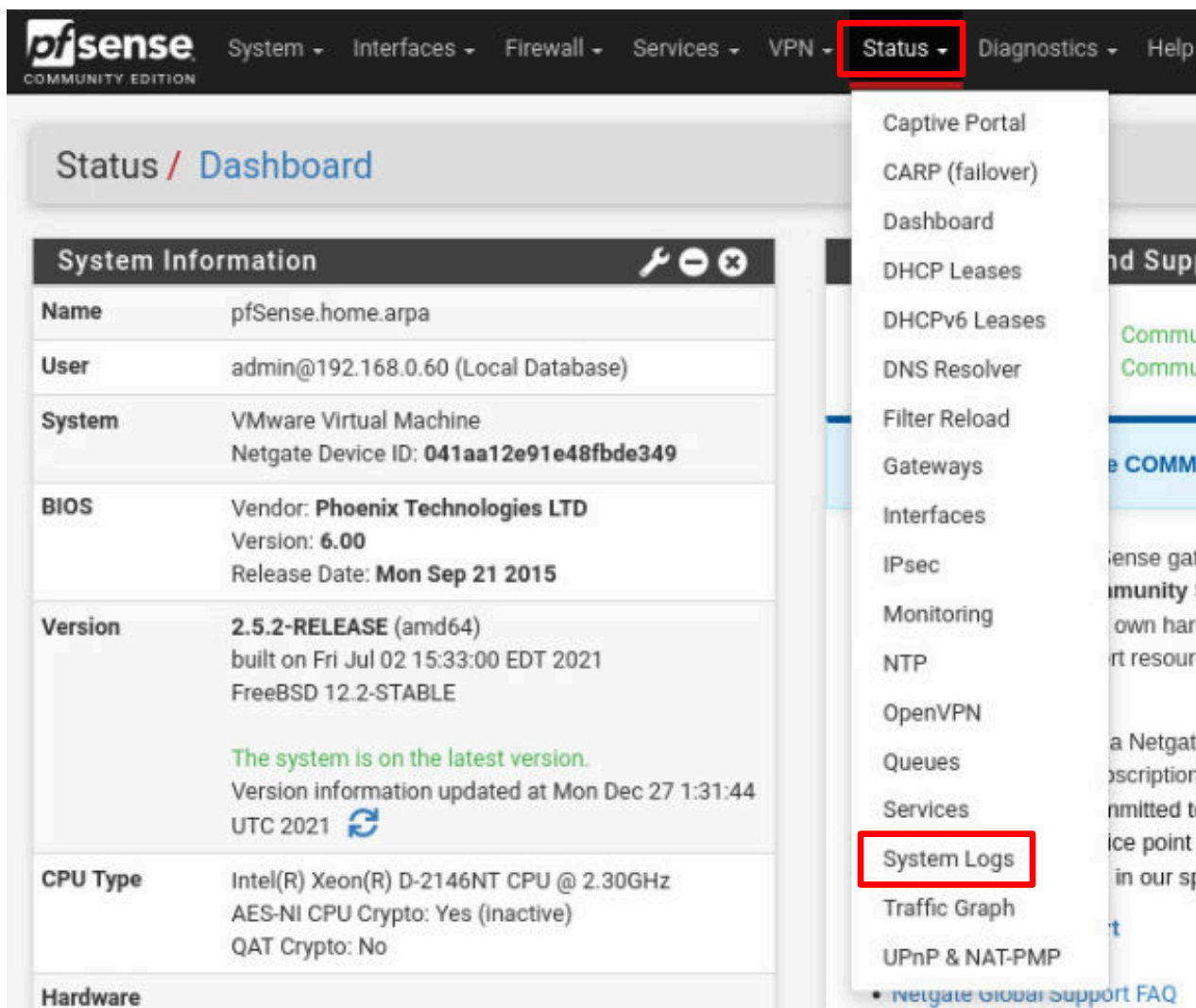
27. Restore the terminal session window where the *OpenVPN* client is running and press **Ctrl+C** to end the *OpenVPN* session.

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.

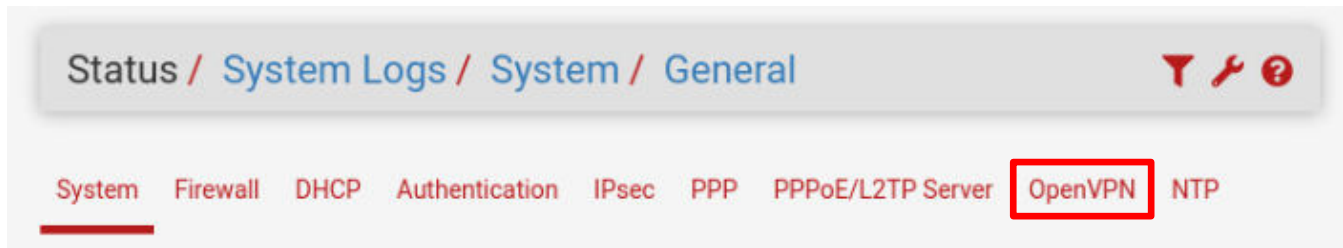
1. Set the focus to the **MintOS** computer.
2. Restore the **pfSense** page.
3. Click on the **Status** menu item, then click on **System Logs** in the dropdown menu.



The screenshot shows the pfSense web interface. The top navigation bar includes links for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. The 'Status' menu is open, showing a list of options: Captive Portal, CARP (failover), Dashboard, DHCP Leases, DHCPv6 Leases, DNS Resolver, Filter Reload, Gateways, Interfaces, IPsec, Monitoring, NTP, OpenVPN, Queues, Services, System Logs, Traffic Graph, and UPnP & NAT-PMP. The 'System Logs' option is highlighted with a red box. The main content area displays the 'Status / Dashboard' page, which includes a 'System Information' section with details about the system, BIOS, version, and CPU type.

System Information	
Name	pfSense.home.arpa
User	admin@192.168.0.60 (Local Database)
System	VMware Virtual Machine Netgate Device ID: 041aa12e91e48fbde349
BIOS	Vendor: Phoenix Technologies LTD Version: 6.00 Release Date: Mon Sep 21 2015
Version	2.5.2-RELEASE (amd64) built on Fri Jul 02 15:33:00 EDT 2021 FreeBSD 12.2-STABLE The system is on the latest version. Version information updated at Mon Dec 27 1:31:44 UTC 2021
CPU Type	Intel(R) Xeon(R) D-2146NT CPU @ 2.30GHz AES-NI CPU Crypto: Yes (inactive) QAT Crypto: No
Hardware	

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.