**Practical 8a : pfSense Firewall with OpenVPN**

**Objectives: To set up a OpenVPN Server on pfSense**

**Description of pfSense:**

pfSense ([www.pfsense.org](http://www.pfsense.org)) is an open source software firewall based on the FreeBSD operating system. For this practical, we have installed pfSense onto a VM.

Internal Network

External Network

InternalClient1

Network Adapter : Host-only

Static IP : 172.25.8.101/24

Win10

pfSense Firewall

Network Adapter : NAT

WAN interface

DHCP IP

Network Adapter : Host-only

Static IP : 172.25.8.110/24

Network Adapter : NAT

DHCP IP

Network Adapter : Host-only

LAN interface

Static IP : 172.25.8.5/24

InternalServer1

The pfSense Firewall has two network adapters, one for the External Network, and one for the Internal Network. We will use the VMware Host-only Network Connection to represent the Internal Network.

The InternalClient1 and InternalServer1 are in the Internal Network protected by the pfSense Firewall. All the IPs in the Internal Network are set using Static IPs.

|  |  |  |
| --- | --- | --- |
| **Internal Network Images** | **IP** | **Login details** |
| pfSense LAN | 172.25.8.5/24 | Web login username : admin  Password : pfsense |
| InternalClient1 | 172.25.8.101/24 | Username : root  Password : password |
| InternalServer1 | 172.25.8.110/24 | Username : root  Password : password |

We will use our Win10 image to act as a staff currently in the External Network, wanting to do a remote connection back to the office network. We will use the VMware NAT Network Connection to represent the External Network. All the IPs in the External Network will be assigned through DHCP.

**Network Traffic Direction**

Traffic from External Network to the Internal Network will enter through the WAN interface of the Firewall and will be considered as **incoming**.

Traffic from Internal Network to the External Network will enter through the LAN interface of the Firewall and will be considered as **outgoing**.

**Requirements**

A staff who is now in the External Network wants to access some files in a shared folder in InternalClient1. We will configure a VPN Server on the pfSense Firewall to allow the staff to access the InternalClient1 through a secure tunnel.

WinXP

(Remote User)

InternalClient1

(Shared Folder)

pfSense Firewall

(with VPN Server)

External Network

Internal Network

VPN tunnel

**Exercise Starting up the pfSense and InternalClient1 images**

If you have not set up the pfSense network from a previous practical, download and unzip the two images : pfSense 2.4.4 and InternalClient1. This pfSense 2.4.4 image already has the OpenVPN Client Export package installed.

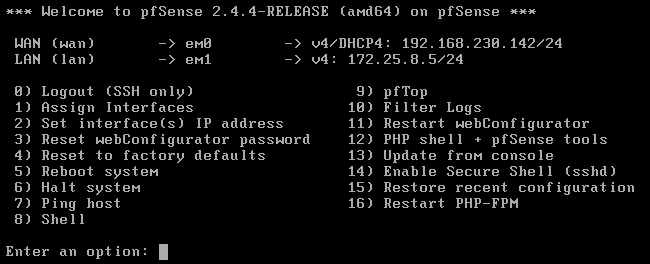
1. If you are in the Cyber Wargame Centre network, you can download the pfSense 2.4.4 image from \\studentserver.dmit.local\student\ehd. Or download from the following Dropbox link:

<https://www.dropbox.com/sh/119mcwvbl8qq782/AABH4TCZtwGFgMBC1lvLrDROa>

1. Power on the two images – pfSense 2.4.4 and InternalClient1.

In pfSense

1. Take note of the IPs of the 2 network interfaces. The WAN interface is the one assigned to the External Network. The LAN interface is the one assigned to the Internal Network.

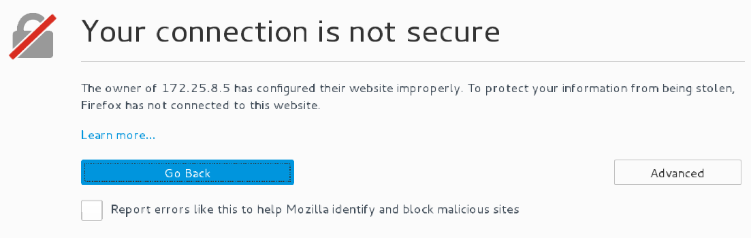


In InternalClient1

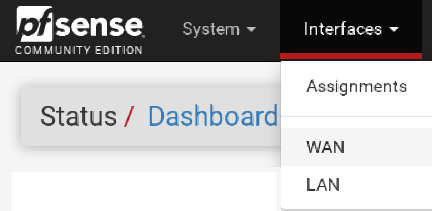
1. Login as user “lim” and password “password” (or you can also login as user “root” and password “password”).
2. Start the Firefox web browser and browse to the Internal IP of the pfSense firewall.

https://172.25.8.5

1. You may see a warning because by default, pfSense is using a self-signed certificate. Click on the Advanced button to view details of the warning.

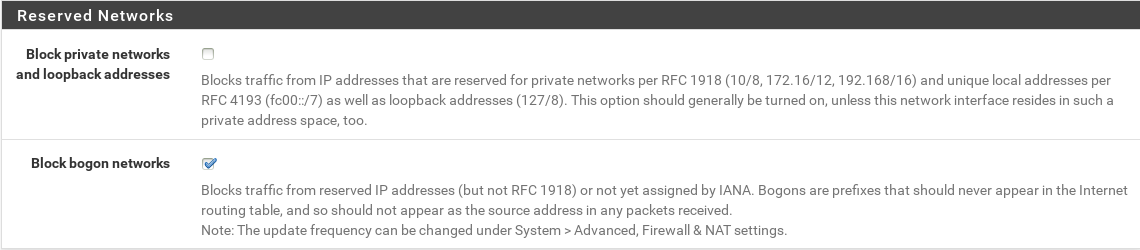


1. To accept the self-signed certificate, click on “Add Exception”. Click “Confirm Security Exception”.
2. Login to the pfSense Web Configurator with username “admin” and password “pfsense”.
3. Go to the Interfaces menu and select WAN. (see following diagram).

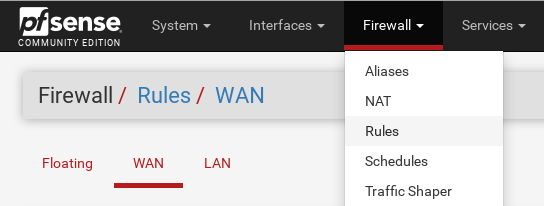


1. Scroll down to the Reserved Networks section. Uncheck the box “Block private networks and loopback addresses”.

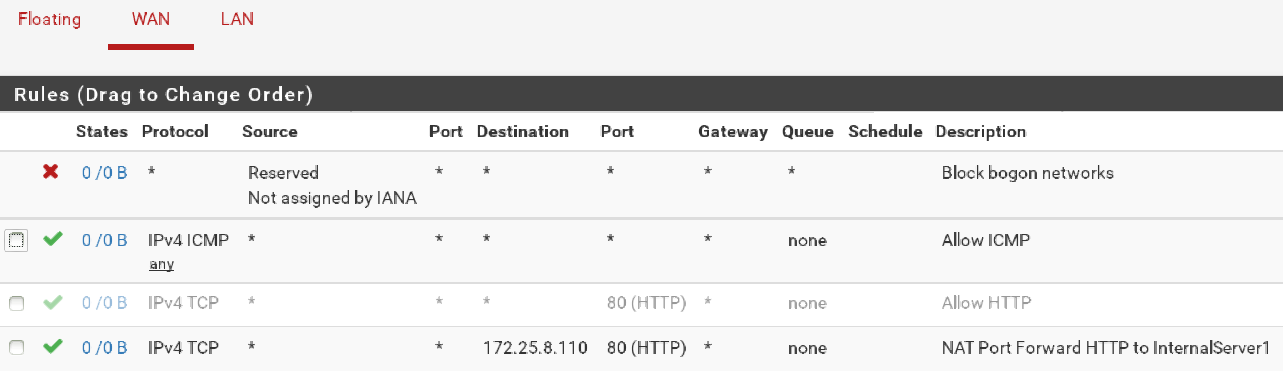
This is required because in our practical, we are using our WinXP image to represent a system in the External Network, and our WinXP image has a private IP address.



1. Click Save. Click Apply Changes.
2. From the Firewall menu, select Rules. Click the WAN interface. (see following diagram)



1. Check if you have a WAN rule that allows incoming ICMP packets. (see following diagram)



WAN rule that allows incoming ICMP packets

1. If you do not have a WAN rule allowing ICMP packets, follow the steps in Exercise 2 to add the rule.

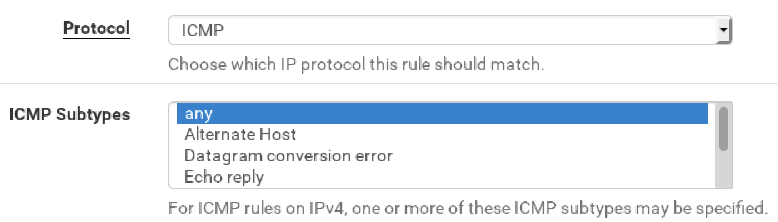
If you already have a WAN rule to allow ICMP, proceed to Exercise 3.

**Exercise Add a WAN rule to allow incoming ICMP packets**

Do this exercise only if the pfSense firewall does not already have a WAN rule to allow ICMP.

In InternalClient1

1. Browse to the pfSense Web Configurator. From the Firewall menu, click Rules.
2. Click on the WAN tab.
3. At the bottom of the page, click on the green button that will Add a Rule to the end of the list.
4. Under Edit Firewall Rules, for Protocol, select ICMP. For ICMP Subtypes, select “any”.



1. Under Extra Options, for Description, enter “Allow ICMP”.
2. Scroll to the bottom and click Save. Click Apply Changes.

**Exercise Starting up the Win10 image (external client)**

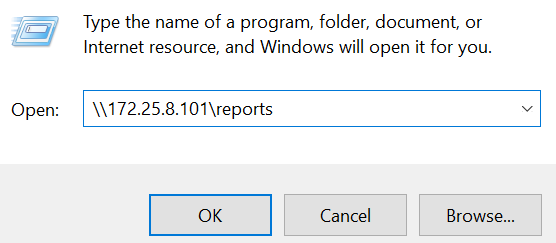
In WinXP (External Network)

1. Check that your Win10 virtual machine is using NAT. Power it on.
2. Check that your Win10 can ping the WAN IP of your pfSense Firewall.

There is a shared folder on InternalClient1. Let’s test to see if you can access this shared folder from Win10.

In Win10 VM (External Network)

1. In the left-hand corner, right-click on the Windows icon and go to Run.
2. Type “\\172.25.8.101\reports” and click OK.



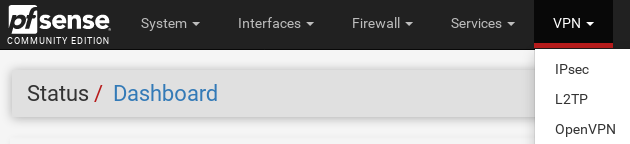
1. You should not be successful as the External Network should not be able to access the Internal Network.

**Exercise Setting up OpenVPN Server on the pfSense Firewall**

You will set up a Certificate Authority (CA) and generate a certificate for the OpenVPN Server on the pfSense Firewall. You will also specify the private subnet that will be used for the VPN tunnel.

In InternalClient1

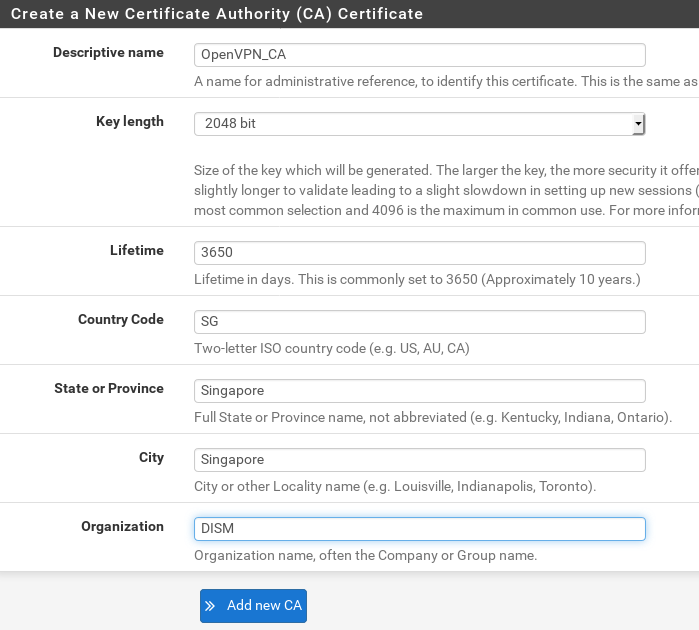
1. Browse to the pfSense Web Configurator. From the VPN menu, click OpenVPN.



1. Click the Wizards tab.
2. For Authentication Backend Type, Type of Server, use the default “Local User Access”.
3. Click Next.

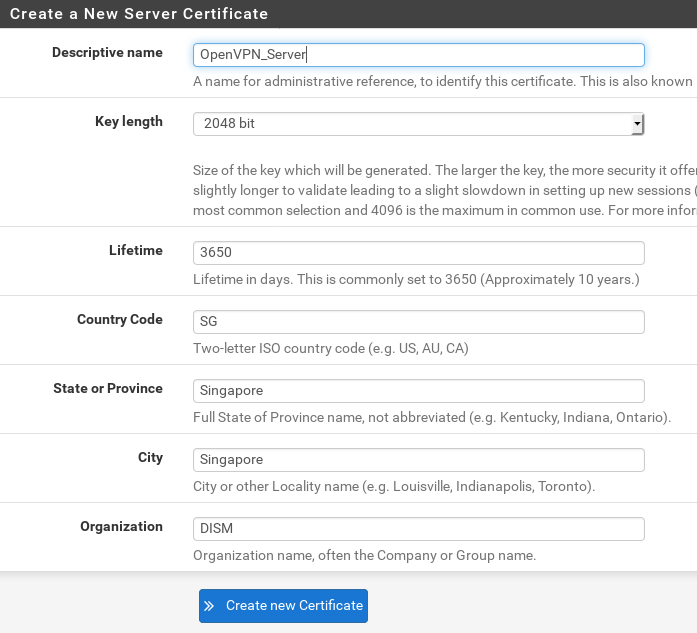
Set up a Certificate Authority that will be used to generate certificates for the VPN Server and Users.

1. For Descriptive Name, you can type “OpenVPN\_CA” (or you can type any name).
2. For Country Code, type “SG”.
3. For State or Province, type “Singapore”.
4. For City, type “Singapore”.
5. For Organisation, you can type “DISM” (or you can type any organisation name).
6. Click Add new CA. (see following diagram)



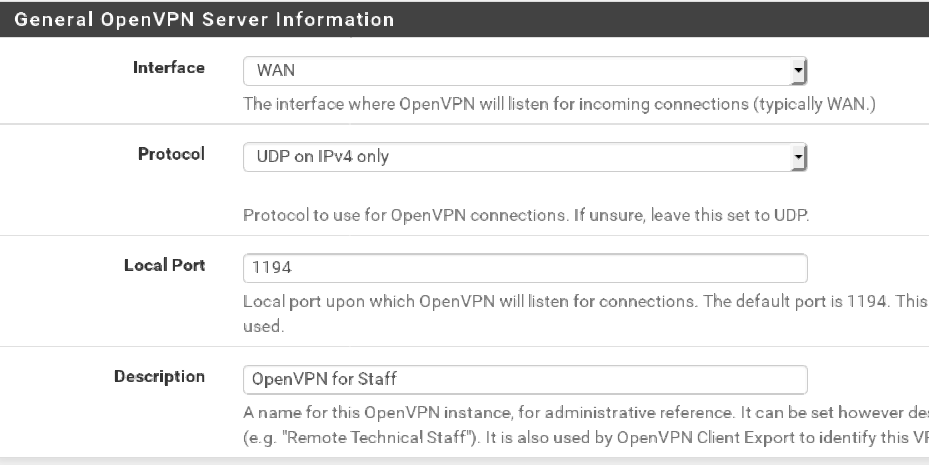
Next create a new certificate for your VPN Server.

1. For Descriptive Name, you can type “OpenVPN\_Server” (or you can type any name).
2. You can leave the default values for the rest of the fields. Click Create new Certificate.

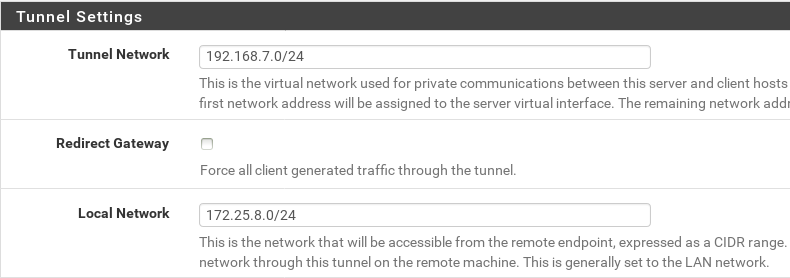


Next you configure your VPN Server.

1. For Interface, check that it is set to WAN.
2. For Description, you can type “OpenVPN for Staff”.



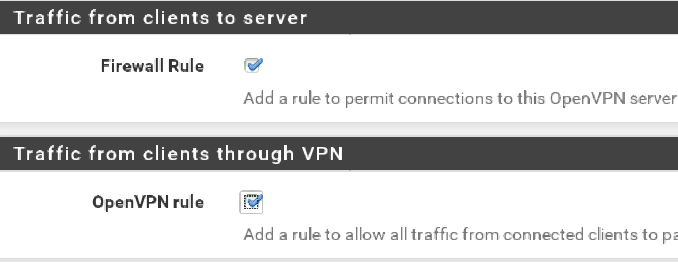
1. For Tunnel Network you can use “192.168.7.0/24”. (this is the private network that will be set up when the remote user connects to the VPN Server, you can use any other private subnets)
2. For Local Network, type in the subnet of the Internal Network “172.25.8.0/24”.



1. For the rest of the fields, you can configure the type of encryption used, etc. For this practical, leave the rest of the fields as default.
2. Click Next.

Next you configure the Firewall rules for your VPN Server.

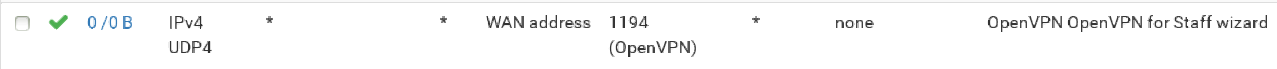
1. Check the two boxes for Firewall Rule and OpenVPN Rule to allow remote clients to connect to your VPN Server and access the Internal Network.



1. Click Next. Click Finish.

Check the Firewall rules that have been created.

1. From the Firewall menu, click Rules. Click on the WAN tab.
2. Check that a new WAN rule has been added for the OpenVPN Server.



1. Still under Firewall Rules, click on the OpenVPN tab.
2. Check that a new OpenVPN rule has been added.

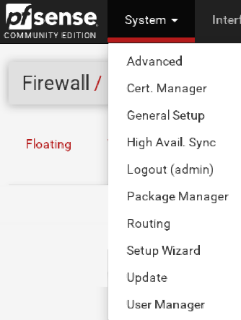


**Exercise Set up the User and the User certificate**

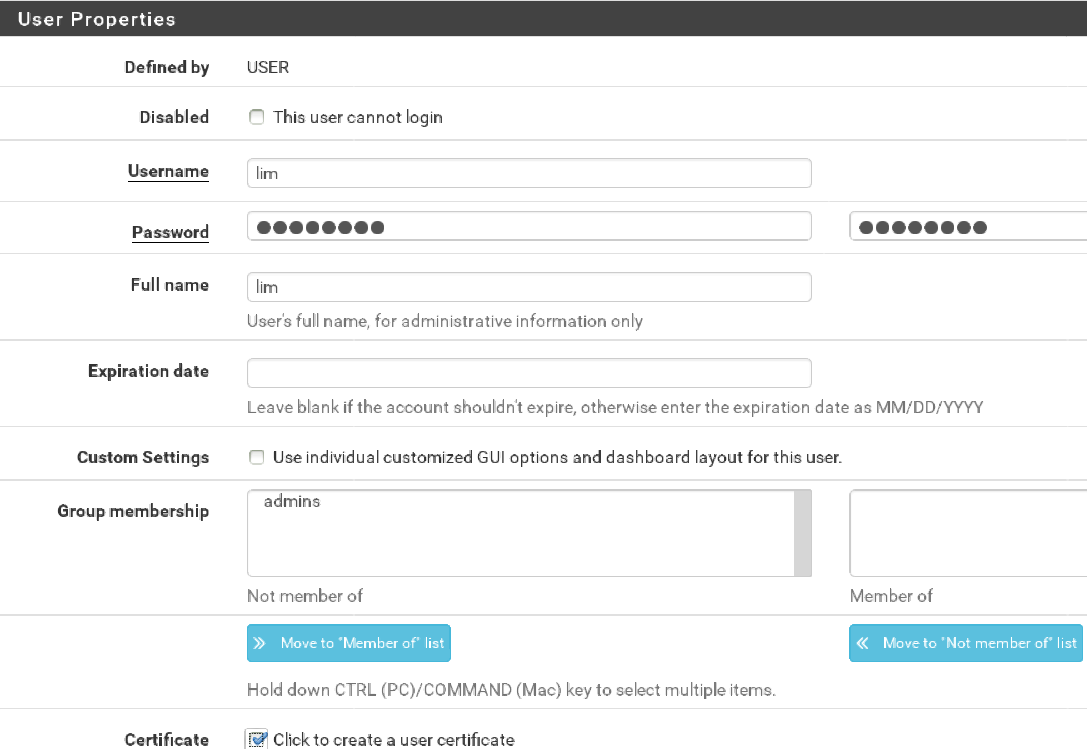
You will set up a user account and a user certificate.

In InternalClient1

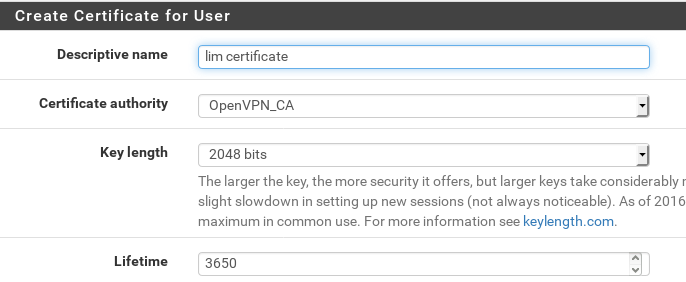
1. In the pfSense Web Configurator, go to the System menu, click User Manager.



1. Click on the green Add button to add a new user.
2. For Username, you can type “lim” (this is the user on InternalClient1).
3. Enter the Password and Confirm Password as “password” (this is the password for user lim on InternalClient1)
4. For Full Name, you can type “lim”.
5. Check the box “Click to create a user certificate”. (see following diagram)



1. Under “Create Certificate for User”, for Descriptive Name, you can type “lim certificate”. (or any name you like)
2. Check that the Certificate Authority is your OpenVPN\_CA.



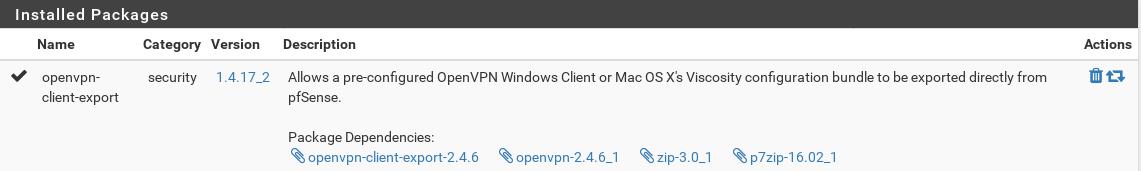
1. Click Save.

**Exercise Install the OpenVPN Client Export Package**

The OpenVPN Client Export Package will provide the OpenVPN client installation programs that needs to be installed on the external clients wishing to access the Internal Network.

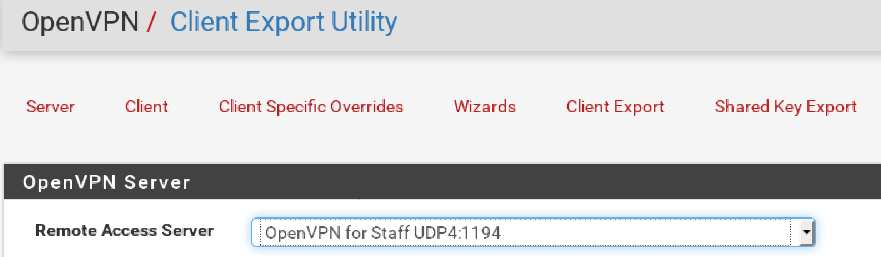
In InternalClient1

1. In the pfSense Web Configurator, go to the System menu, click Package Manager.
2. Select Installed Packages tab. The openvpn-client-export package has already been installed on this pfSense image so you do not need to download and install it.

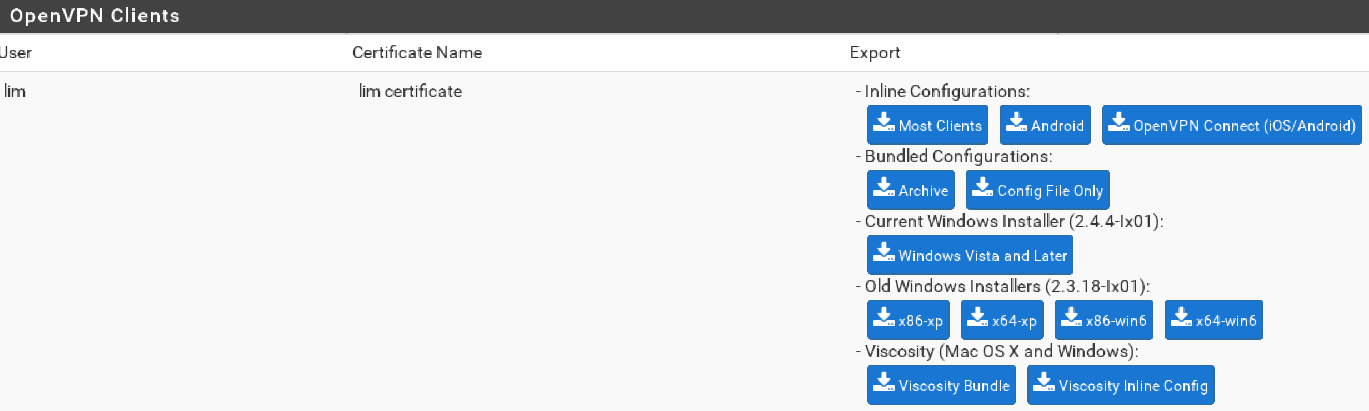


The openvpn-client-export package is already installed

1. Go to the VPN menu and select OpenVPN.
2. Click on the Client Export tab.
3. Check that the Remote Access Server is your OpenVPN Server.



1. Scroll down to the OpenVPN Clients section. The user lim is listed, together with the different OpenVPN client platforms that can be exported for him. Click on “Current Windows Installer” and save the OpenVPN client certificate installation to any folder on InternalClient1.



Export the “Current Windows installer”

This OpenVPN Client installation file contains the OpenVPN for client software, the connection configuration for your OpenVPN\_Server, plus the certificate for user lim.

1. Copy the OpenVPN Client installation for user lim file from the InternalClient1 to the Win10 VM. (you may need to copy the installation file to your Host PC and then to your Win10 VM)

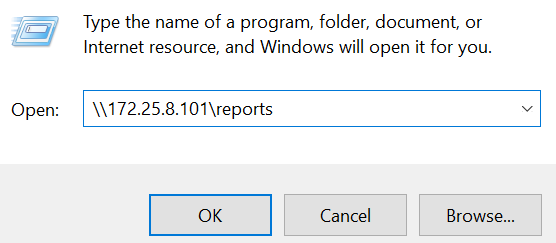
In Win10 VM

1. Double-click on the OpenVPN Client file to install it with default options
2. If you see a message about installing “TAP-Windows”, click Install.

**Exercise Connect to the InternalNetwork through OpenVPN**

In Win10 VM

1. In the left hand corner, click on the Windows icon and choose All apps. Look for OpenVPN and run OpenVPN GUI. An OpenVPN GUI icon will appear in the System tray of the Taskbar.
2. Right-click on the OpenVPN GUI icon and choose Connect.
3. Login as user lim and the password you have set previously.
4. If a Windows Firewall popup appears asking if you want to allow OpenVPN to communicate on private networks, click “Allow access” so that Windows Firewall will allow connections to the OpenVPN. (you can always make changes to the Windows Firewall later)
5. When the connection is successful, the OpenVPN GUI icon in the System Tray will turn green. Use ipconfig to see your VPN IP address (in the Tunnel Network 192.168.7.0 subnet).
6. Ping the InternalClient1 172.25.8.101. You should be successful.
7. Access the shared folder \\172.25.8.101\reports on InternalClient1.



1. The connection may take a while to be set up (1 or 2 minutes). Login as user “lim” and password “password”.
2. You should be successful, as you are connected to the Internal Network through the VPN connection. You can see the “report1” file that is on the shared folder from the InternalClient1.

Possible configuration errors:

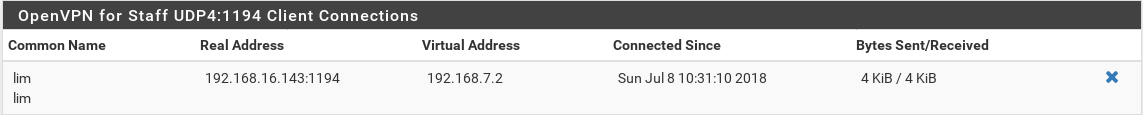
If the VPN connection is not successful, it could be due to the following factors :

1. When configuring the VPN Server, the Tunnel Network or Local Network is not set properly. In the pfSense Web Configurator, go to VPN menu and click OpenVPN. Edit the OpenVPN for Staff VPN Server, and check the Tunnel Network and Local Network settings.
2. The date and time of the Win10 VPN client is wrong (eg one day behind the VPN Server). Check that the date and time of the Win10 is correct.

In InternalClient1

1. In the pfSense Web Configurator, go to the Status menu, click OpenVPN.

You can see details of the current VPN connections.



**Exercise Shutting down**

In Win10 VM

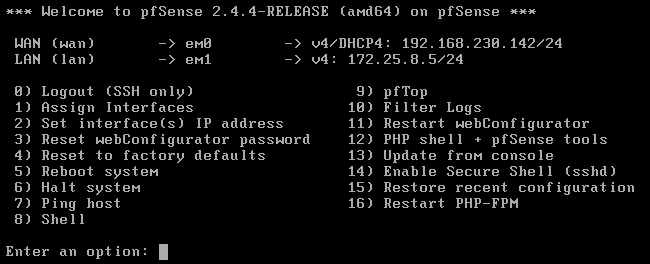
1. Right-click on the OpenVPN GUI icon and choose Disconnect.
2. Shutdown Win10.

In InternalClient1

1. If you are logged into the pfSense Web Configurator, log out and close the Firefox web browser.
2. Using user root and password “password”, run “init 0” to shutdown.

In pfSense

1. Type “6” to halt the firewall system. (see following diagram)



*End of Practical*