

Lab 5.5.4: Configuring a VPN Server on a pfSense Security Appliance using OpenVPN Tunneling

From TestOut CompTIA Security+ Course

In this lab I will be setting up a VPN Server within the pfSense environment as well as creating a Certificate Authority to use with clients.

The scenario for this lab is as follows:

You work as the IT security administrator for a small corporate network. Occasionally, you and your co-administrators need to access internal resources when you are away from the office. You would like to set up a Remote Access VPN using pfSense to allow secure access.

In this lab, your task is to use the pfSense wizard to create and configure an OpenVPN Remote Access server using the following guidelines:

- **Sign in to pfSense using:**
 - Username: admin
 - Password: P@ssw0rd (zero)
- **Create a new certificate authority certificate using the following settings:**
 - Name: CorpNet-CA
 - Country Code: GB
 - State: Cambridgeshire
 - City: Woodwalton
 - Organization: CorpNet
- **Create a new server certificate using the following settings:**
 - Name: CorpNet
 - Country Code: GB
 - State: Cambridgeshire
 - City: Woodwalton
- **Configure the VPN server using the following settings:**
 - Interface: WAN
 - Protocol: UDP on IPv4 only
 - Description: CorpNet-VPN

Robert Carpenter

github.com/robertmcarpenter

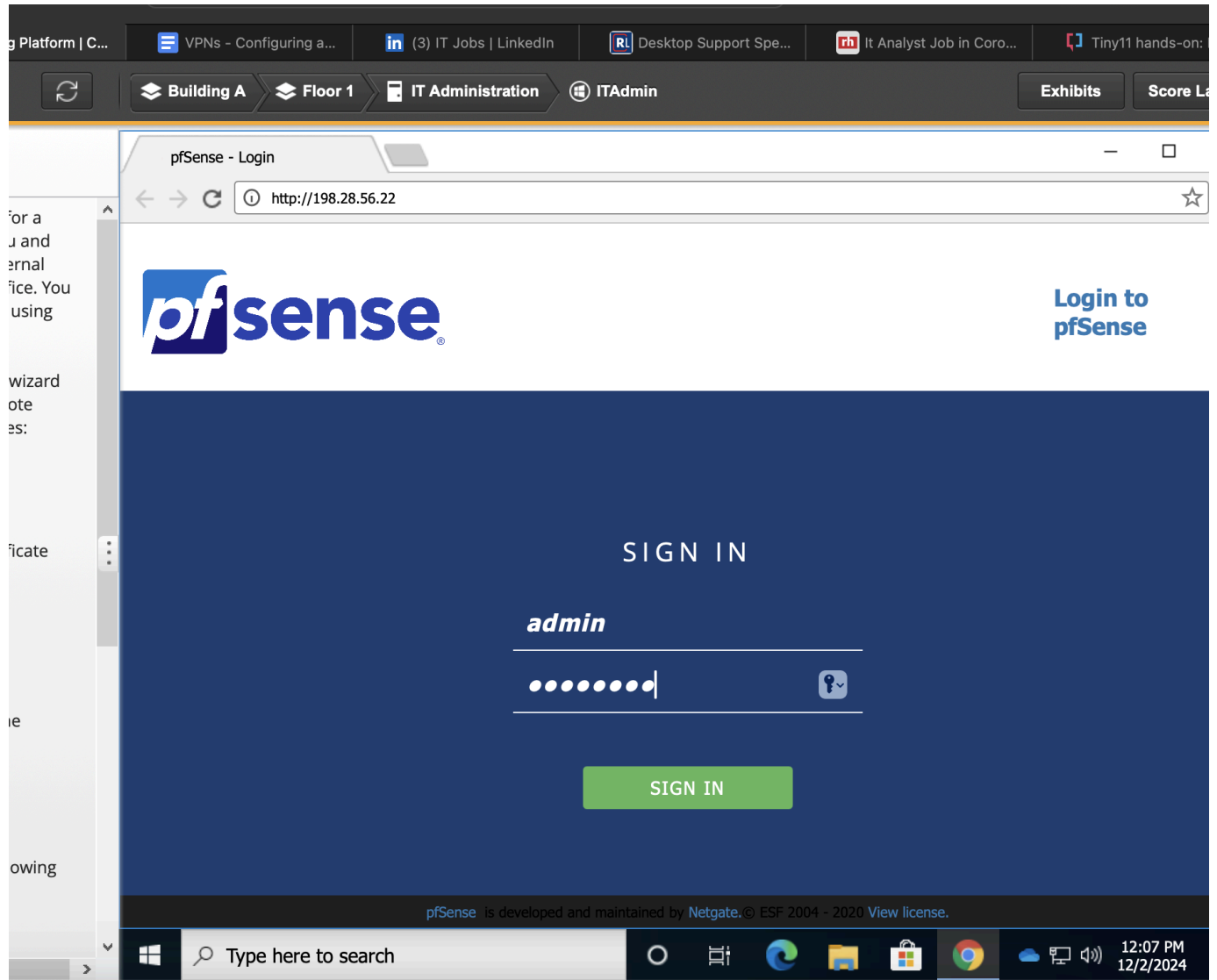
Mon December 2nd 2024

- Tunnel network IP: 198.28.20.0/24
 - Local network IP: 198.28.56.18/24
 - Concurrent Connections: 4
 - DNS Server 1: 198.28.56.1
- Configure the following:
 - A firewall rule
 - An OpenVPN rule
- Set the OpenVPN server just created to Remote Access (User Auth).
- Create and configure the following standard remote VPN users:

Username	Password	Full Name
blindley	L3tM31nNow	Brian Lindley
jphillips	L3tM31nToo	Jacob Phillips

Looks like we have a lot to do in this lab! Since we are going to be configuring everything within pfSense's GUI environment I'll need to login first.

Robert Carpenter
github.com/robertmcarpenter
Mon December 2nd 2024



Once, I'm logged in I'll go to the **VPN > OpenVPN** menu. Notice how other VPN protocols are listed in this menu. For our implementation we would like to use the OpenVPN protocol but keep in mind there are others like Wireguard Ipsec and so on!

Mon December 2nd 2024

TestOut Building A Floor 1 IT Administration ITAdmin Exhibits Score L

Scenario

You work as the IT security administrator for a small corporate network. Occasionally, you and your co-administrators need to access internal resources when you are away from the office. You would like to set up a Remote Access VPN using pfSense to allow secure access.

In this lab, your task is to use the pfSense wizard to create and configure an OpenVPN Remote Access server using the following guidelines:

- Sign in to pfSense using:
 - Username: admin
 - Password: P@ssw0rd (zero)
- Create a new certificate authority certificate using the following settings:
 - Name: CorpNet-CA
 - Country Code: GB
 - State: Cambridgeshire
 - City: Woodwalton
 - Organization: CorpNet
- Create a new server certificate using the following settings:
 - Name: CorpNet
 - Country Code: GB
 - State: Cambridgeshire
 - City: Woodwalton
- Configure the VPN server using the following settings:
 - Interface: WAN
 - Protocol: UDP on IPv4 only

pfSense - VPN: OpenVPN: S...
http://198.28.56.22/vpn_openvpn_server.php

pfSense COMMUNITY EDITION System Interfaces Firewall Services VPN Status Diagnostics Help

VPN / OpenVPN / Servers

Servers Clients Client Specific Overrides Wizards

OpenVPN Servers

Interface	Protocol/Port	Tunnel Network	Crypto	Description	Actions
-----------	---------------	----------------	--------	-------------	---------

+ Add

pfSense is developed and maintained by Netgate. © ESF 2004 - 2020 View license

Type here to search

2:36 PM 12/2/2024

Once I'm here I'll click the Add button and click the Wizard option from the Breadcrumb menu.

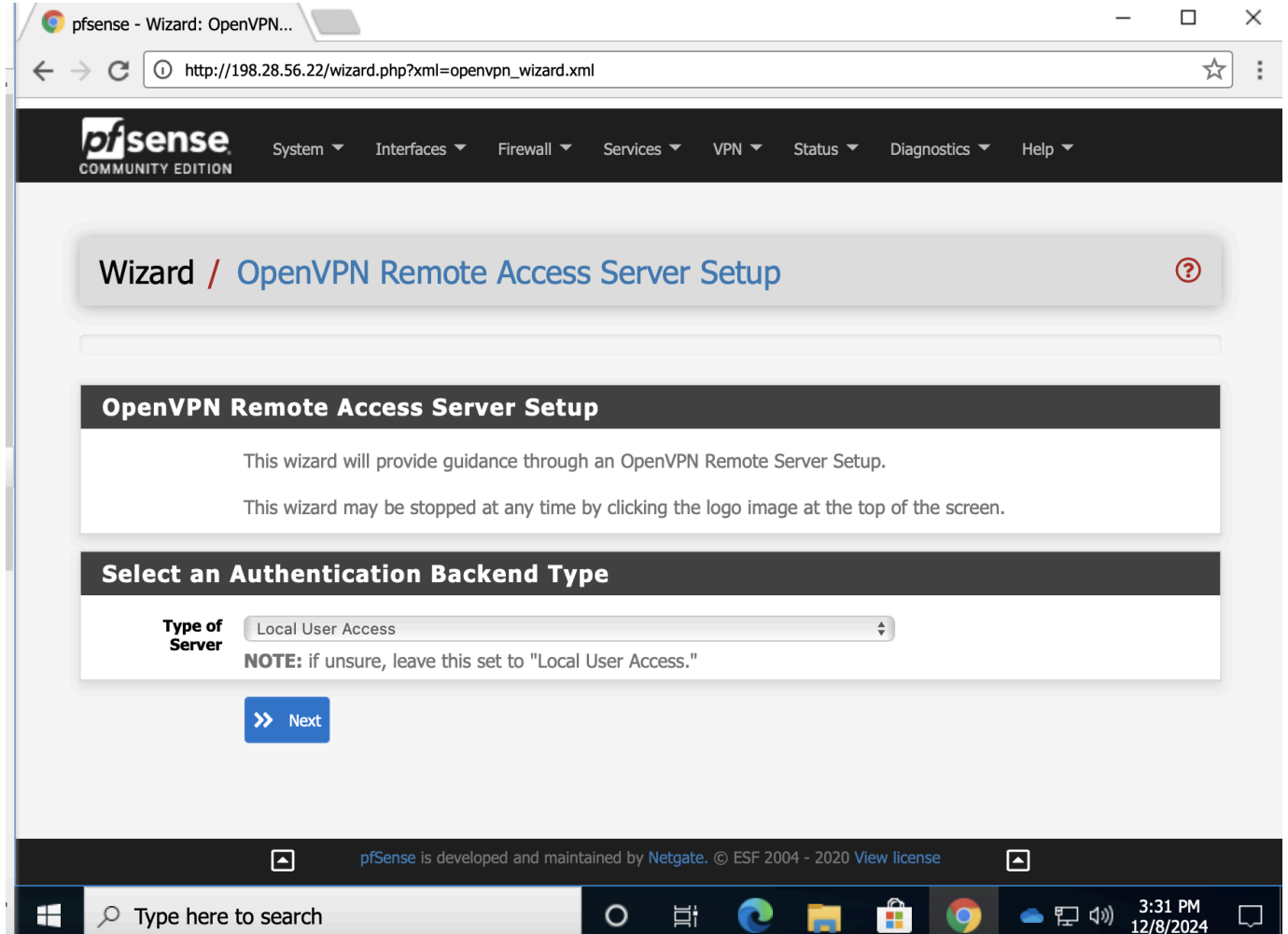
pfSense COMMUNITY EDITION System Interfaces Firewall Services VPN

VPN / OpenVPN / Servers

Servers Clients Client Specific Overrides Wizards

OpenVPN Servers

After clicking it, I'll begin to enter the information provided to me by the Lab. On the first screen it asks what kind of **Authentication**, if any, we would like to use. We have the option to use LDAP as a backend authentication. For our purpose, we'll follow the instructions on screen which states to simply use **Local User Access** if we're unsure.



After, I'll click next. The wizard now prompts us to create a Certificate Authority to use for VPN encryption.

We want to configure the following as given to us by the lab:

- Name: **CorpNet-CA**
- Country Code: **GB**
- State: **Cambridgeshire**
- City: **Woodwalton**
- Organization: **CorpNet**

Mon December 2nd 2024

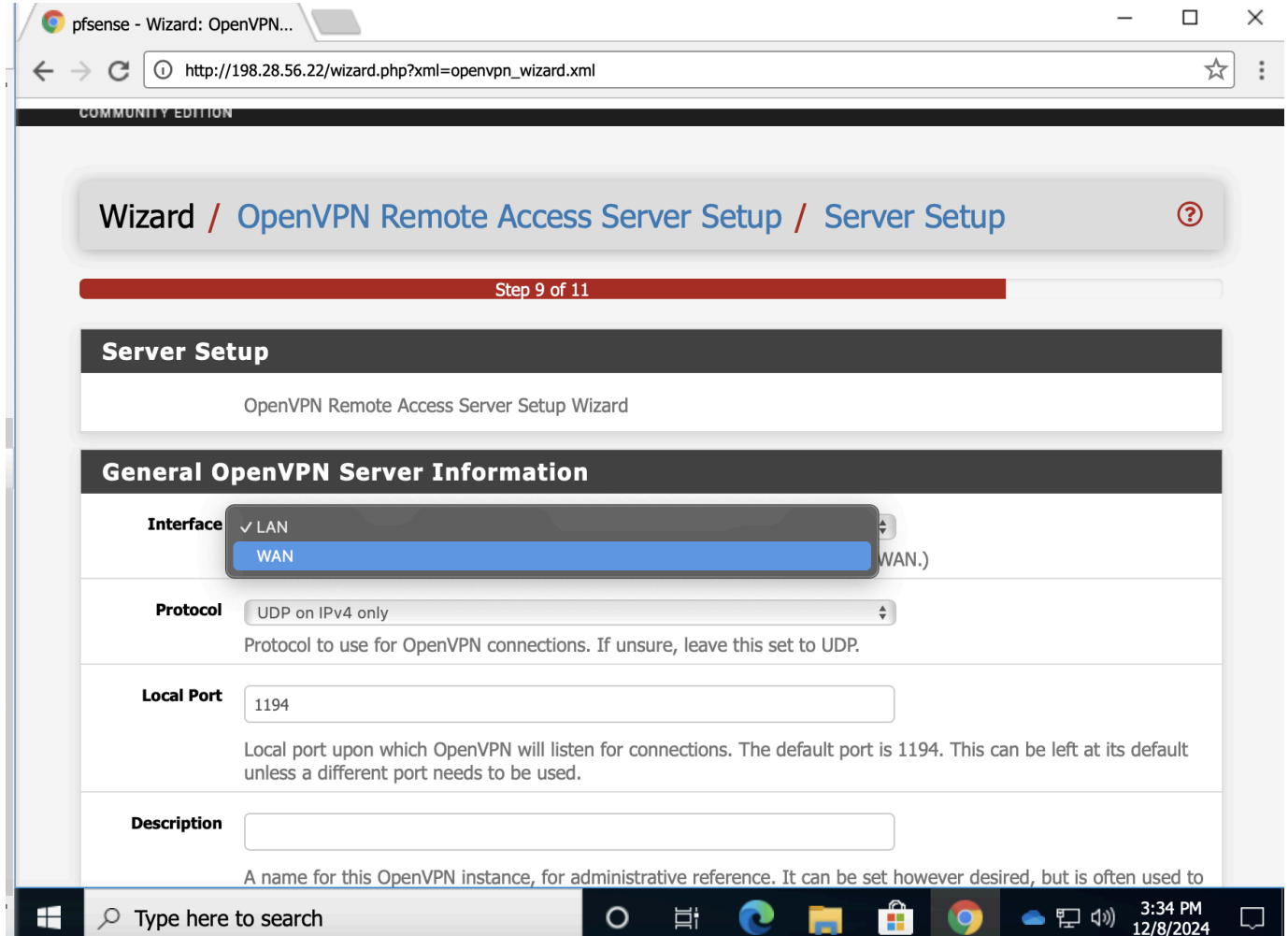
The screenshot shows the 'OpenVPN Wizard' configuration page in a web browser. The browser's address bar shows the URL `http://198.28.56.22/wizard.php?xml=openvpn_wizard.xml`. The page contains several form fields for configuring a certificate:

- Name:** A text field for administrative reference.
- Key length:** A dropdown menu set to 2048. A description below states: "Size of the key which will be generated. The larger the key, the more security it offers, but larger keys take considerably more time to generate, and take slightly longer to validate leading to a slight slowdown in setting up new sessions (not always noticeable). As of 2016, 2048 bit is the minimum and most common selection and 4096 is the maximum in common use. For more information see keylength.com".
- Lifetime:** A text field set to 3650. A description below states: "Lifetime in days. This is commonly set to 3650 (Approximately 10 years.)".
- Country Code:** A text field set to GB. A description below states: "Two-letter ISO country code (e.g. US, AU, CA)".
- State or Province:** A text field set to Cambridgeshire. A description below states: "Full State or Province name, not abbreviated (e.g. Kentucky, Indiana, Ontario)".
- City:** A text field set to Woodwalton. A description below states: "City or other Locality name (e.g. Louisville, Indianapolis, Toronto)".
- Organization:** A text field set to CorpNet. A description below states: "Organization name, often the Company or Group name."

The Windows taskbar at the bottom shows the search bar with the text "Type here to search", several application icons, and the system clock displaying "3:32 PM 12/8/2024".

On the next screen, we are prompted to create a certificate for the Server to use. We'll enter the information given to us by the lab:

- Name: **CorpNet**
- Country Code: **GB**
- State: **Cambridgeshire**
- City: **Woodwalton**



Now, we will set up the config for the OpenVPN server. We want the Server to listen in on the WAN interface because this server is for our remote users who are not in the scope of the LAN.

The Lab requires us to set the following:

- Interface: **WAN**
- Protocol: **UDP on IPv4 only**
- Description: **CorpNet-VPN**
- Tunnel network IP: **198.28.20.0/24**
- Local network IP: **198.28.56.18/24**
- Concurrent Connections: **4**
- DNS Server 1: **198.28.56.1**

Notice the Tunnel Network is different from the Local IP. The Tunnel Network is expressed as an IP address followed by /24 which states that the first 3 octets are

Robert Carpenter

github.com/robertmcarpenter

Mon December 2nd 2024

the Network portion. All users who connect to the VPN server will be put on a VLAN within the server within the **198.28.20.1 - 192.28.20.255**

The screenshot shows the 'OpenVPN Wizard' configuration page in a web browser. The browser's address bar shows the URL 'http://198.28.56.22/wizard.php?xml=openvpn_wizard.xml'. The page is divided into several sections:

- Algorithm:** A text box with the description: 'The algorithm used to encrypt traffic between endpoints. This setting must match on the client and server side, but is otherwise set however desired. Certain algorithms will perform better on different hardware, depending on the availability of supported VPN accelerator chips.'
- Auth Digest Algorithm:** A dropdown menu set to 'SHA256 (256-bit)' with the description: 'The method used to authenticate traffic between endpoints. This setting must match on the client and server side, but is otherwise set however desired.'
- Hardware Crypto:** A dropdown menu set to 'No Hardware Crypto Acceleration' with the description: 'The hardware cryptographic accelerator to use for this VPN connection, if any.'
- Tunnel Settings:** A section header followed by three sub-sections:
 - Tunnel Network:** A text box containing '198.28.20.0/24'. The description states: '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:** An unchecked checkbox with the description: 'Force all client generated traffic through the tunnel.'
 - Local Network:** An empty text box. The description states: '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:** A partially visible section at the bottom.

The Windows taskbar at the bottom shows the search bar, task view button, and several application icons. The system clock indicates 3:37 PM on 12/8/2024.

After setting the VLAN for our VPN Users, we will need to direct them to our actual internal LAN. The Lab says for us to point our users to the **198.28.56.18/24** network. I'll enter that now.

After doing so we need to add a Firewall rule to allow users to connect. Luckily the Wizard on pfSense can do this for us.

TestOut Building A Floor 1 IT Administration ITAdmin Exhibits Score Lab

Scenario

- Create a new server certificate using the following settings:
 - Name: CorpNet
 - Country Code: GB
 - State: Cambridgeshire
 - City: Woodwalton
- Configure the VPN server using the following settings:
 - Interface: WAN
 - Protocol: UDP on IPv4 only
 - Description: CorpNet-VPN
 - Tunnel network IP: 198.28.20.0/24
 - Local network IP: 198.28.56.18/24
 - Concurrent Connections: 4
 - DNS Server 1: 198.28.56.1
- Configure the following:
 - A firewall rule
 - An OpenVPN rule
- Set the OpenVPN server just created to Remote Access (User Auth).
- Create and configure the following standard remote VPN users:

Username	Password	Full Name
blindley	L3tM31nNow	Brian Lindley
jphillips	L3tM31nToo	Jacob Phillips

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 server's IP and port, as well as allowing traffic from connected clients through the tunnel. These rules can be automatically added here, or 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

Now we need to click the edit button after finishing the wizard to change the Local Access type to User Auth.

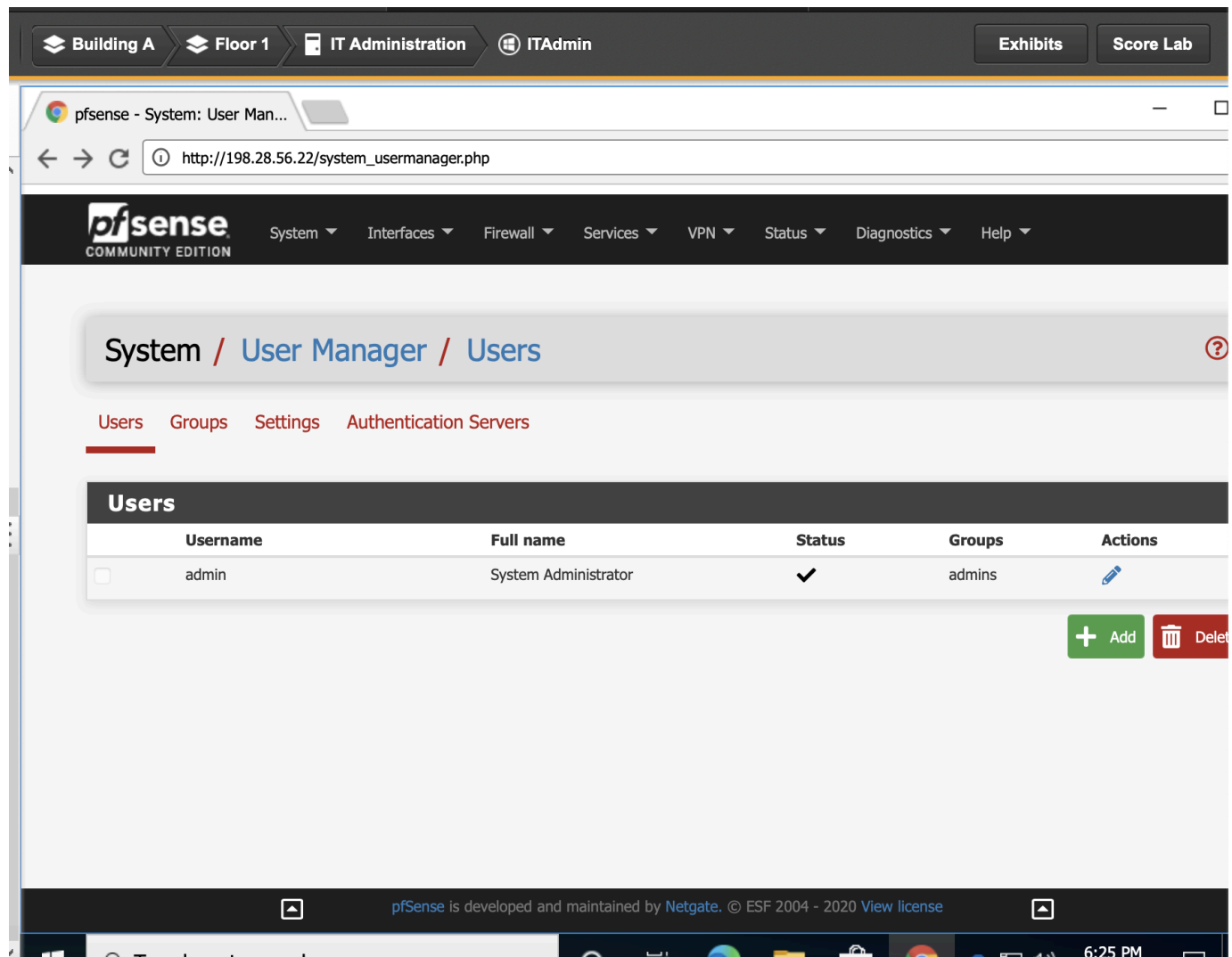
After that, the lab wants us to add 2 VPN users.

- Create and configure the following standard remote VPN users:

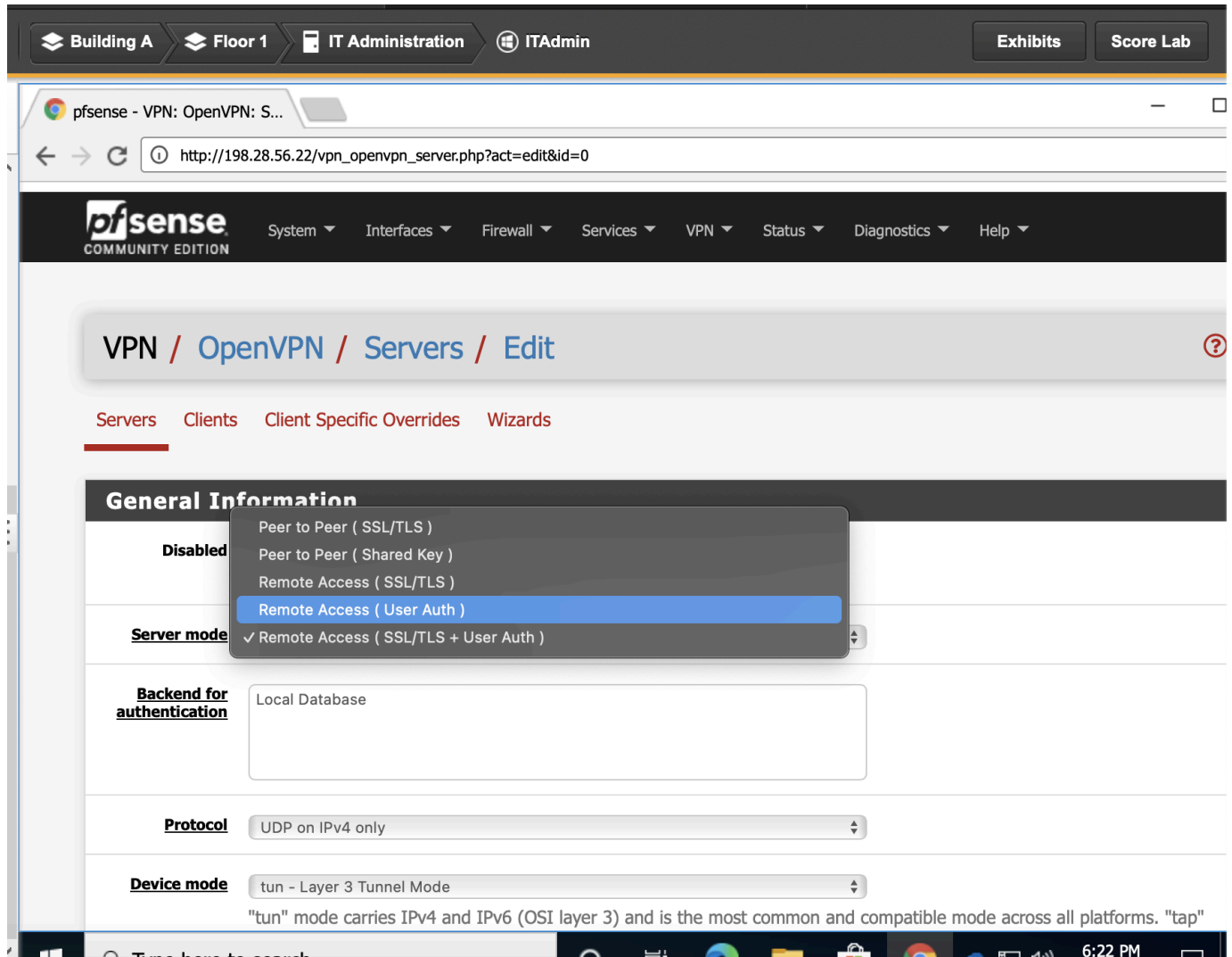
Username	Password	Full Name
blindley	L3tM31nNow	Brian Lindley
jphillips	L3tM31nToo	Jacob Phillips

These users above can be added through **System > User Manager** tab within the top menu bar in pfSense. I'll do that now.

Robert Carpenter
github.com/robertmcarpenter
Mon December 2nd 2024



I'll need to click that Green add button to configure our 2 users.



Once that is completed I'll hit the Blue "Save" button towards to bottom.

We are all done! We've completed all the steps! This now concludes this lab.