**Overall Lab Objective**

To understand and implement user account management, role-based access control (RBAC), and authentication policies within pfSense. Students will create local users and groups, assign limited permissions, enforce password policies, and learn how to integrate with external authentication sources.

**Lab 1: Local User Creation and Role-Based Controls**

**Objective:** To create a junior administrator account that has read-only access to the firewall rules, demonstrating the principle of least privilege.

**Step 1: Create a Limited-Privilege Group**

1. From your Client-VM, log into the pfSense web interface as the admin user.
2. Navigate to **System > User Manager**.
3. Click on the **Groups** tab.
4. Click the **+ Add** button to create a new group.
5. **Group name:** Firewall Viewers
6. **Scope:** Local
7. **Description:** Read-only access to firewall status and rules.
8. Click **Save**. You will now be on the "Edit Group" page.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

Click on edit and follow the images

A screenshot of a computer

AI-generated content may be incorrect.

1. Under "Assigned Privileges," click the **+ Add** button.
2. A popup will appear with a long list of system privileges. We will only assign permissions to *view* pages, not save or change anything. Select the following two privileges:
   * WebCfg - Firewall: Rules (Allows viewing the rules page)

A screenshot of a computer

AI-generated content may be incorrect.

* + WebCfg - Diagnostics: all (expect authentication and edit)

1. Click **Save** on the privileges popup, and then click **Save** again on the group page.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

**Step 2: Create a Local User and Assign to the Group**

1. While still in **System > User Manager**, click on the **Users** tab.
2. Click **+ Add**.

A screenshot of a computer

AI-generated content may be incorrect.

1. **Username:** jradmin (for Junior Admin)
2. **Password:** jradmin@123 (or any other password)
3. **Full name:** Junior Admin
4. Under "Group Memberships," find Firewall Viewers in the "Not Member Of" box, click on it, and then click the **"Move to Member of" arrow** to add the user to the group.

A screenshot of a computer

AI-generated content may be incorrect.

1. Click **Save**.

A screenshot of a computer

AI-generated content may be incorrect.

**Step 3: Testing Access Restrictions**

1. Open a new private browsing window in Firefox on your Client-VM (or log out of the admin account).
2. Navigate to https://192.168.1.1.
3. Log in with the new credentials: **Username:** jradmin, **Password:** Password123!.

A screen shot of a login screen

AI-generated content may be incorrect.

1. **Verification:**
   * **SUCCESS:** Try to navigate to Firewall -> Rules. You should be able to see the page and the rules you created earlier.
   * **SUCCESS:** Try to navigate to Diagnostics -> ARP Table. You should be able to see the logs.
   * The Dashboard for the JRAdmin has only the Assigned navigation pane attributes. Therefore, the JR ADMIN cannot access the rest of the attributes of the Pfsense navigation pane.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

The navigation bar of Admin and Jr Admin is different which shows that RBAC is implemented.

**Conclusion:** You have successfully created a role with limited permissions and assigned a user to it, enforcing role-based access control.

**Lab 2: Integration with External Authentication (LDAP - Theory & Diagnostics)**

**Phase 1: Environment & TurnKey VM Setup**

**Goal:** Import the TurnKey VM into VirtualBox, place it on the correct virtual network, and perform its initial setup.

**Step 1: Download and Import the TurnKey Appliance**

1. **Download:** Go to the official TurnKey GNU/Linux website.   
   <https://www.turnkeylinux.org/domain-controller> download the file
2. **Step 2: Configure VM Network Adapters**

**IMPORTANT:** Do this *before* you power on the TurnKey VM for the first time.

1. We will use a dedicated "server network" for this lab. Let's call it server-net.
2. Lubuntu is already configured to get connected to hr-net.
3. **pfsense vm Settings:**
   * Go to the settings for your pfsense vm.
   * Go to **Network**.
   * We will use **Adapter 3**. Ensure it is set to Internal Network with the name hr-net.

A screenshot of a computer

AI-generated content may be incorrect.

1. **TurnKey Domain Controller VM Settings:**
   * Go to the settings for the TurnKey VM you just imported.
   * Go to **Network**.
   * Follow the images to install

A screenshot of a computer

AI-generated content may be incorrect.

A computer screen shot of a computer

AI-generated content may be incorrect.

A computer screen shot of a computer

AI-generated content may be incorrect.

A screenshot of a computer screen

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer error

AI-generated content may be incorrect.

A screenshot of a computer error

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screen shot of a computer

AI-generated content may be incorrect.

A computer screen shot of a computer error

AI-generated content may be incorrect.

A computer screen shot of a computer screen

AI-generated content may be incorrect.

A screenshot of a computer error

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

Delete the default text DOMAIN.LAN.

Type in the domain name we planned to use in the lab guide: **innovatech.local**

Use the **Tab** key on your keyboard to move the cursor from the text box to the <Apply> button.

Press **Enter**.

A screenshot of a computer

AI-generated content may be incorrect.

In the text box, type the first part of your domain name, in all capital letters: **INNOVATECH**

Use the **Tab** key to move the cursor down to the <Apply> button.

Press **Enter**.

A computer screen shot of a password

AI-generated content may be incorrect.

A computer screen shot of a computer error

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A computer screen shot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer error

AI-generated content may be incorrect.

A screenshot of a computer program

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A computer screen shot of a computer

AI-generated content may be incorrect.

Now let’s change the network setting once the server is installed. Turn of the TurnKeyVM

* Go to the settings for the TurnKey VM you just imported.
* Go to **Network**.
* Change the adapter from the default (Bridged) to Internal Network with the name server-net.

A computer screen shot of a computer

AI-generated content may be incorrect.

We see that the IP address has changed as the network adapter is changed.

We have configured the TurnKey server and received the above IP address.

**Step 3: Set a Static IP for the TurnKey Server**

Servers should always have a static IP. We will do this from the pfSense DHCP server.

1. Go to your kali machine and log into the pfSense GUI.
2. Navigate to **Status > DHCP Leases**.
3. You will see an entry for your TurnKey VM. Click the **"Add Static Mapping"** icon on the right.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

1. On the next page, assign it a static IP outside of your DHCP range. Example: 192.168.10.10.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

1. Click **Save**.

A screenshot of a computer

AI-generated content may be incorrect.

1. Go back to your TurnKey VM console and reboot it by typing reboot and pressing Enter.
2. After it reboots, it will now have the static IP 192.168.10.10.

A computer screen with a blue and white screen

AI-generated content may be incorrect.

**Phase 2: Create Users in TurnKey and Password Policies**

**To connect to Turnkey webmin we need create a Firewall rule so that the machine where pfsense GUI is used can talk to Turnkey webmin**

**In the LAN of firewall make a rule to pass from any protocol of LAN Subnets to any protocol of HR Subnets**

A screenshot of a computer

AI-generated content may be incorrect.

**Goal:** Use the Webmin interface to create the test user for our captive portal.

1. From your kali machine's web browser, navigate to the Webmin address for your TurnKey server: https://192.168.10.10:12321.

A screenshot of a computer

AI-generated content may be incorrect.

1. You will get a browser security warning. Accept the risk and proceed.

A screen shot of a computer

AI-generated content may be incorrect.

1. Log in with the username root and the password you set in Step 3.

A screenshot of a login page

AI-generated content may be incorrect.

1. In the left-hand menu, navigate to **System > Users and Groups**.

A screenshot of a computer

AI-generated content may be incorrect.

1. Click on **Create a new user**.

A screenshot of a computer

AI-generated content may be incorrect.

1. Fill in the details:
   * **Username:** testuser
   * **Real name:** Test User
   * **Password:** Set to Normal password and enter a password (e.g., Password123!).
   * Leave other settings as default.
2. Click **Create**. You have now created the user pfSense will authenticate.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

**Password changed**

* **What it does:** This is an informational field that shows the date the user last changed their password. For a new user, this will say "Never."
* **Lab Action:** No action needed. This field is not editable.

**Expiry date**

* **What it does:** Sets a specific calendar date on which the user's account will be permanently disabled.
* **Lab Example:** You would use this for temporary accounts, like a contractor who is only working until December 31st.
* **Lab Action:** Leave this blank. We want our policy to be recurring, not tied to a specific date.

**Minimum days**

* **What it does:** Sets the minimum number of days a user must wait before they are allowed to change their password again.
* **Real-world Context:** This prevents a user from changing their password and then immediately changing it back to their old, comfortable one, bypassing the spirit of the expiration policy.
* **Lab Action:** Enter 1. This means the user must keep a new password for at least one day.

**Maximum days**

* **What it does:** This is the core of the expiration policy. It sets the maximum number of days a password is valid. After this period, the password expires, and the user will be forced to create a new one.
* **Real-world Context:** A common corporate policy is 90 days to ensure passwords are regularly updated.
* **Lab Action:** Enter 90.

**Warning days**

* **What it does:** Sets the number of days before the password expires that the system will start warning the user to change it.
* **Real-world Context:** This gives users ample notice to think of a new password instead of being surprised on the last day. A 14-day warning period is common.
* **Lab Action:** Enter 14.

**Inactive days**

* **What it does:** Sets the number of days an account can be inactive (not logged into) before it is automatically disabled.
* **Real-world Context:** This is a great security feature to automatically disable accounts that have been abandoned or belong to employees who have left the company.
* **Lab Action:** Leave this blank for this lab.

**Force change at next login**

* **What it does:** This is a crucial setting for new users or after a password reset. When set to "Yes," the user will be unable to do anything else until they change the temporary password you assigned them.
* **Real-world Context:** When an IT admin creates a new account or resets a password, they give the user a temporary password. This setting ensures the user immediately changes that temporary password to something private that only they know.
* **Lab Action:** Select **Yes**.

A screenshot of a computer

AI-generated content may be incorrect.

**Phase 3: pfSense Configuration (Connecting to LDAP)**

**Goal:** Configure pfSense to use your new TurnKey server as an authentication provider.

**Step 1: Create the Authentication Server in pfSense**

1. In the pfSense GUI, navigate to **System > User Manager > Authentication Servers**

A screenshot of a computer

AI-generated content may be incorrect.

1. Click **+ Add**.
2. Fill out the form:
   * **Descriptive name:** TurnKey AD
   * **Type:** LDAP
   * **Hostname or IP address:** 192.168.10.10 (the static IP of your TurnKey server)
   * **Port:** 389
   * **Transport:** TCP - Standard
   * **Bind credentials:** Check this box.
     + **User DN:** CN=Administrator,CN=Users,DC=innovatech,DC=local
     + **Password:** The Administrator password you set during the TurnKey setup.
   * **Search scope - Base DN:** DC=innovatech,DC=local
   * **Authentication containers:** CN=Users,DC=innovatech,DC=local (This is the default location for users in Samba/TurnKey).
   * **User naming attribute:** sAMAccountName

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

1. Click **Save**.

**Step 2: Test the Connection**

1. Navigate to **Diagnostics > Authentication**.
2. **Authentication Server:** Select your new TurnKey AD.
3. **Username:** testuser
4. **Password:** The password you set for testuser.
5. Click **Test**.
6. You should see a message: **"User: testuser authenticated successfully."** This confirms pfSense can communicate with your TurnKey server.

A screenshot of a computer

AI-generated content may be incorrect.

**Lab 3: Assigning Users to Services (Captive Portal)**

**Objective:** To demonstrate how users can be authenticated for a specific service, in this case, gaining internet access via a captive portal

**Step 1: Enable and Configure the Captive Portal**

1. Navigate to **Services > Captive Portal**.
2. Click **+ Add**.
3. **Description:** Captive Portal Demo
4. Select the **HR** interface to enable the portal on.
5. Click **Save & Continue**.
6. On the next page, check the box to **Enable Captive Portal**.
7. Scroll down to the "Authentication" section.
8. For **Authentication method**, ensure Turnkey-AD is selected
9. Click **Save** at the bottom of the page.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

**Step 3: Testing the Captive Portal**

1. On your Client-VM, open the Firefox web browser.
2. Try to navigate to any HTTP website, for example, http://neverssl.com (using HTTP is important for the initial redirect).

A screenshot of a computer

AI-generated content may be incorrect.

1. You should be automatically redirected to the pfSense Captive Portal login page.

A screenshot of a computer

AI-generated content may be incorrect.

1. Enter the credentials for the guest user:
   * **Username:** the one which is created in LDAP
   * **Password:** assigned password for the user in LDAP
2. Click **Log in**.
3. You should now be authenticated and can browse the internet freely. You can verify this by going to <https://google.com>.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

**Conclusion:** You have successfully assigned a user to a network service. Only authenticated users can pass through the firewall, demonstrating a powerful use case for the User Manager.

**Lab 4: VPN creation and assigning users to VPN**

**Objective:** To demonstrate how users can be authenticated for a specific service, in this case, gaining internet access via a VPN or connecting to VPN **Step 1: Launch the OpenVPN Wizard**

1. Log into your pfSense web interface.
2. Navigate to **VPN > OpenVPN**.
3. Click on the **Wizards** tab to start the configuration process.

A screenshot of a computer

AI-generated content may be incorrect.

**Step 2: Authentication Setup**

The wizard will first ask how to authenticate users. For this guide, we will use the built-in pfSense User Manager.

* **Type of Server:** Leave this as Local User Access.
* Click **Next**.

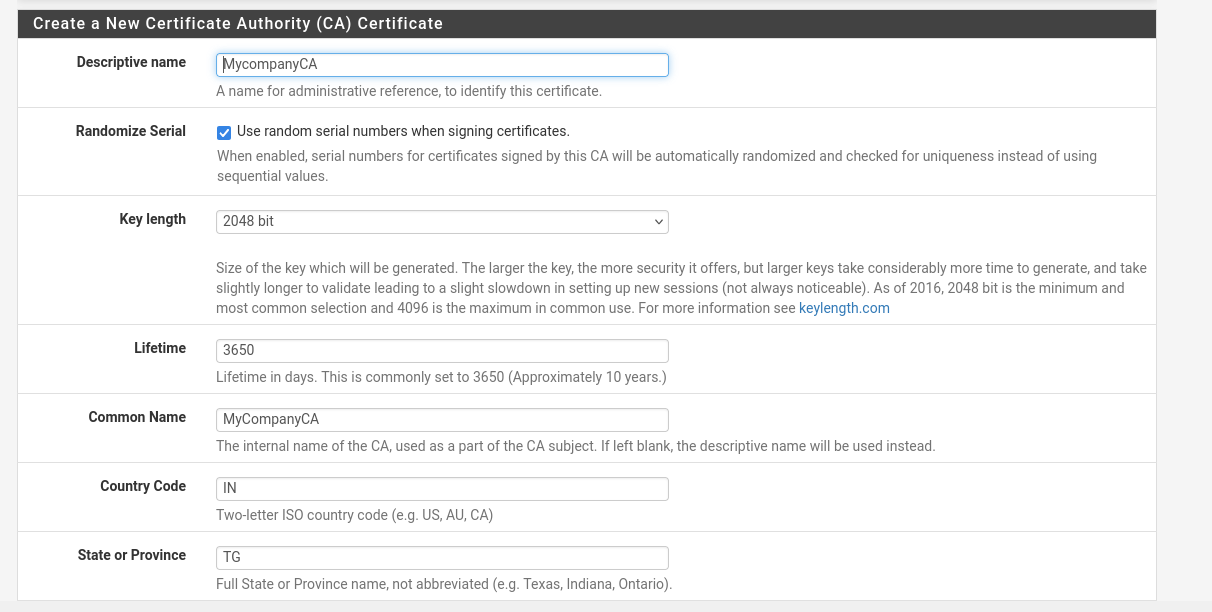
A screenshot of a computer

AI-generated content may be incorrect.

**Step 3: Create the Certificate Authority (CA)**

The VPN needs a "root of trust" to issue certificates. This is your own internal Certificate Authority.

1. **Descriptive name:** Give your CA a name, like MyCompanyCA.
2. **Key length / Algorithm:** The defaults are secure and fine to use.
3. **Lifetime:** The default of 3650 days (10 years) is fine.
4. **Common Name:** This can be anything, for example, MyCompanyVPN.
5. Fill in your Country, State, and City.
6. Click the **Add new CA** button.



A screenshot of a computer

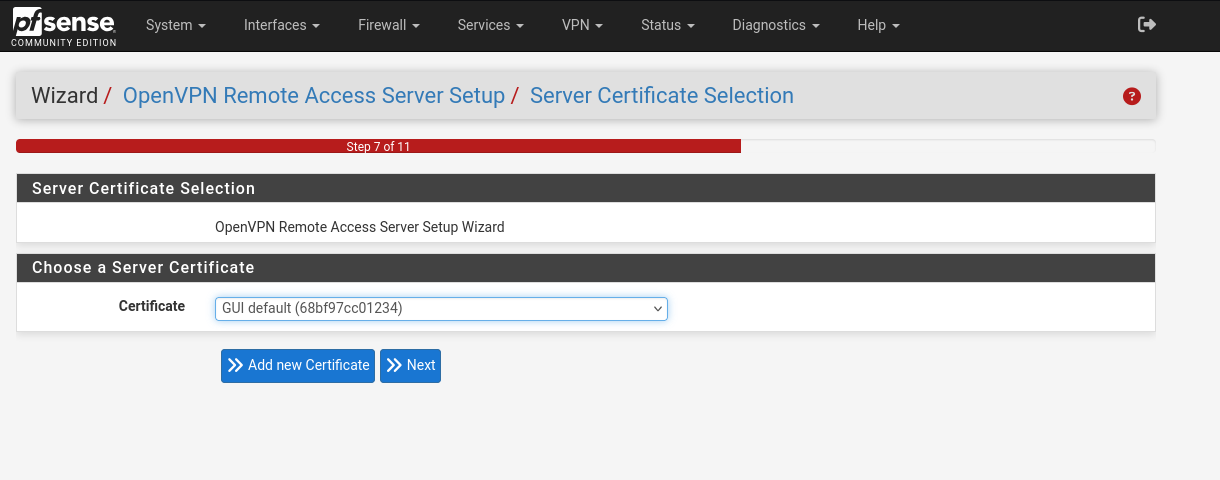
AI-generated content may be incorrect.

MyCompanyCA should be looking something similar

**Step 4: Create the Server Certificate**

Now that you have a CA, you need to issue a certificate for the OpenVPN server itself.

1. **Descriptive name:** Give the server certificate a name, like pfSenseVPNServerCert.
2. All other fields can be left at their defaults, as they are inherited from the CA.
3. Click the **Create new Certificate** button.

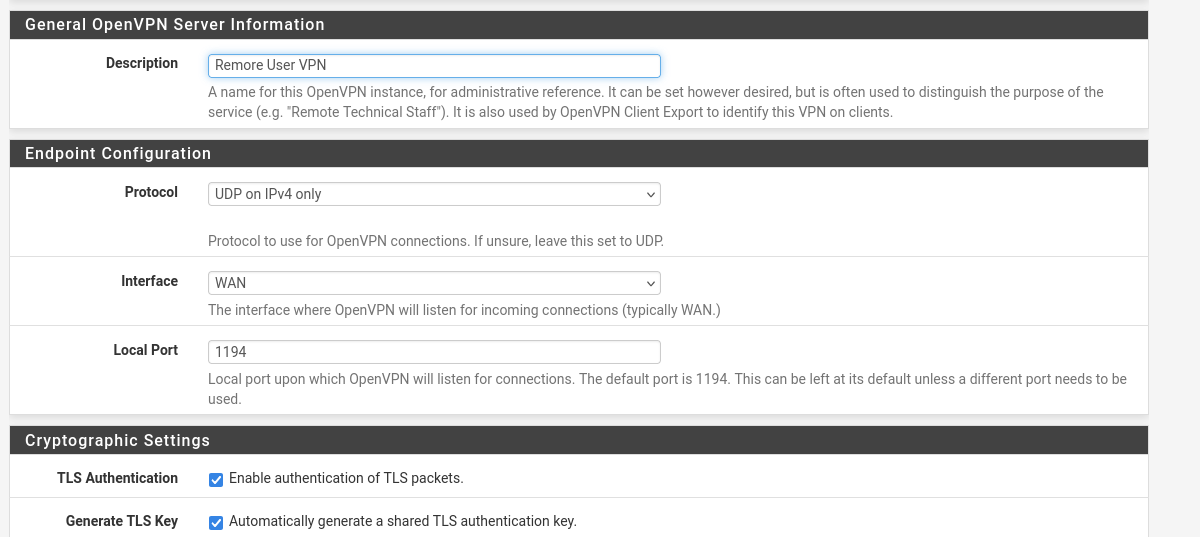




**Step 5: Configure the OpenVPN Server**

This is the most important step where you define the network settings for the VPN.

* **Interface:** Select **WAN**. This is the interface remote users will connect to from the internet.
* **Protocol:** UDP on IPv4 only is the best choice for performance.
* **Local Port:** Leave the default of 1194.
* **Description:** Remote User VPN.
* **Tunnel Network:** **This is critical.** You must enter a private IP network that is **NOT** used anywhere else on your network. A common choice is 10.0.8.0/24. This will be the virtual IP address pool for your connected VPN clients.
* **Local Network:** Enter your LAN network address so that VPN users can access it. Based on your information, this is **10.1.1.0/24**.
* **Concurrent connections:** Set the maximum number of users you want connected at once.
* **DNS Default Domain:** You can enter your pfSense domain if you have one.
* **DNS Server(s):** It's highly recommended to provide your pfSense LAN IP here. Check **"Provide a DNS server list to clients"** and enter **10.1.1.1(your LAN IP)** in the DNS Server 1 box. This allows VPN users to resolve names on your local network.
* Leave all other settings at their default values.
* Click **Next**.



A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

**Step 6: Configure Firewall Rules**

The wizard will automatically create the necessary firewall rules to allow the VPN to function.

1. Check the box for **"Firewall Rule: Allow traffic from clients to the Local Network"**.
2. Check the box for **"OpenVPN rule: Allow traffic from the internet to the OpenVPN server port"**.
3. Click **Next**.
4. Click **Finish** to save the configuration.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.**Your OpenVPN server is now configured and running!** The next step is to create a user who is allowed to connect.

**Step 7: Create a VPN User**

1. Navigate to **System > User Manager**.
2. Click the **+ Add** button.
3. **Username:** Enter a username, for example, remoteuser.
4. **Password:** Set a strong, unique password for this user.
5. **Full name:** Remote VPN User.
6. **Crucial Step:** Scroll down and check the box **"Click to create a user certificate."** This will create the client certificate required for this user.
   * **Descriptive name:** It will auto-populate with the username, which is fine.
   * **Certificate authority:** Ensure your MyCompanyCA is selected.
7. Click **Save**.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

**Step 8: Export the Client Configuration File**

To make it easy for your user to connect, you need to give them a configuration file.

1. First, you must install a helper package. Go to **System > Package Manager > Available Packages**.
2. Search for openvpn-client-export and click the green **+ Install** button. Confirm the installation.
3. Once installed, navigate to **VPN > OpenVPN > Client Export**.

**A screenshot of a computer

AI-generated content may be incorrect.**

A screenshot of a computer

AI-generated content may be incorrect.

**A screenshot of a computer

AI-generated content may be incorrect.**

**A screenshot of a computer

AI-generated content may be incorrect.**

**A screenshot of a computer

AI-generated content may be incorrect.**

A screenshot of a computer

AI-generated content may be incorrect.

**A screenshot of a computer

AI-generated content may be incorrect.**

1. You will see your remoteuser listed. Find the best export option for your user's operating system. **"Most Clients"** is a generic .ovpn file that works with almost all modern OpenVPN clients.
2. Click the appropriate button to download the configuration file.

**A screenshot of a computer

AI-generated content may be incorrect.**

**A screenshot of a computer

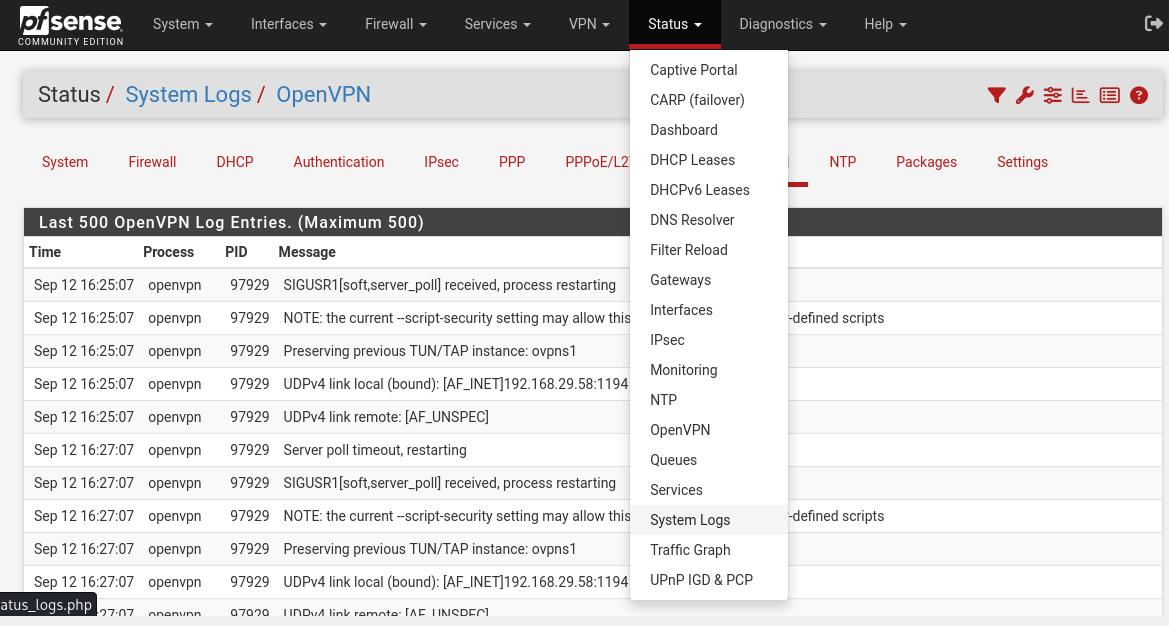
AI-generated content may be incorrect.**

**Final Step: Connecting as a Remote User**

1. Send the downloaded configuration file (e.g., pfsense-udp-1194-remoteuser.ovpn) to your remote user.
2. The user needs to install an OpenVPN client on their computer (the official "OpenVPN Connect" client is recommended).
3. In their OpenVPN client, they will import the .ovpn file.
4. They will then connect by providing the **username** (remoteuser) and **password** you set in Step 7.
5. Connect from the same client system

A computer screen shot of a program

AI-generated content may be incorrect.



A screenshot of a computer

AI-generated content may be incorrect.

The logs also confirm that remote\_users have logged into and using password.

**Phase 4: Captive Portal Implementation**

**Goal:** Force users on the server-net to log in with their domain credentials.

1. Navigate to **Services > Captive Portal**.
2. Click **+ Add**.
3. **Zone name:** serverzone
4. **Interfaces:** Select **IT** (the pfSense interface connected to server-net).
5. Click **Save & Continue**.
6. On the main configuration page:
   * Check **Enable Captive Portal**.
   * Under **Authentication**, in the **Authentication method** dropdown, select your TurnKey AD server.
7. Scroll to the bottom and click **Save**.

**Phase 5: Testing the Full System**

1. **Start your lubuntu 2 VM.** It should get an IP address from pfSense (e.g., 192.168.20.101).
2. Open a web browser and try to navigate to an HTTP site like http://neverssl.com.
3. You will be redirected to the pfSense captive portal login page.
4. Enter the credentials:
   * Username: testuser
   * Password: Password123!
5. Click **Log in**.
6. You should now be authenticated and have full internet access. You can test this by browsing to any website.