

**User Management and Authentication Policies**

A blue and white octagon with black text

AI-generated content may be incorrect.

|  |  |
| --- | --- |
| **Role** | Network Administrator / Security Engineer |
| **Scope** | * Create limited-privilege users and assign permissions * Integrate pfSense with external authentication (LDAP) * Assign users to services like Captive Portal and VPN * Enforce secure access policies |
| **Prerequisits** | * pfSense VM installed and accessible via Client-VM * Admin credentials for pfSense GUI * TurnKey Domain Controller VM downloaded and imported * Internal networks configured (hr-net for client, server-net for server) * VirtualBox or compatible virtualization software installed |

**Objective**

To implement user account management, role-based access control (RBAC), and authentication policies in pfSense by creating local users and groups, assigning limited permissions, enforcing password policies, and integrating with external authentication sources.

**Tasks**

1. **Local User and Role Creation**

* Log in to pfSense GUI as admin.
* Navigate to System > User Manager > Groups.
* Add a new group:
  + Name: Firewall Viewers
  + Scope: Local
  + Description: Read-only access to firewall rules and status
* Assign privileges:
  + WebCfg - Firewall: Rules (view only)
  + WebCfg - Diagnostics: all (exclude authentication/edit)
* Save the group.
* Navigate to Users tab, add a new user:
  + Username: jradmin
  + Password: jradmin@123
  + Full Name: Junior Admin
* Add the user to Firewall Viewers group.
* Test access restrictions:
  + Log in as jradmin and verify read-only access to Firewall Rules and Diagnostics (ARP Table).
  + Confirm JR Admin cannot access other admin functions.

**2. Integration with External Authentication (LDAP)**

* + Import TurnKey Domain Controller VM and assign network adapter to server-net.
  + Configure TurnKey domain: innovatech.local.
  + Set static IP via pfSense DHCP: e.g., 192.168.10.10.
  + Reboot TurnKey VM.
  + Access TurnKey Webmin: <https://192.168.10.10:12321>
  + Log in as root.
  + Create a new user for testing:
    - Username: testuser
    - Password: Password123!
    - Real Name: Test User
  + Configure password policies:
    - Minimum days: 1
    - Maximum days: 90
    - Warning days: 14
    - Force password change at next login: Yes
  + Configure pfSense LDAP server:
    - Name: TurnKey AD
    - Type: LDAP
    - Hostname/IP: 192.168.10.10
    - Port: 389, TCP
    - Bind DN: CN=Administrator,CN=Users,DC=innovatech,DC=local
    - Bind Password: TurnKey admin password
    - Base DN: DC=innovatech,DC=local
    - Authentication container: CN=Users,DC=innovatech,DC=local
    - User naming attribute: sAMAccountName
  + Test authentication with testuser to verify connectivity.

**3. Captive Portal Configuration**

* + Navigate to Services > Captive Portal, add a zone:
    - Description: Captive Portal Demo
    - Interface: HR
  + Enable Captive Portal.
  + Select Authentication method: TurnKey AD.
  + Test portal access:
    - On Client-VM, navigate to HTTP site (e.g., <http://neverssl.com>)
    - Confirm redirect to Captive Portal login
    - Log in with LDAP credentials (testuser)
    - Verify internet access

**4. VPN Configuration and User Assignment**

* + Launch VPN Wizard: VPN > OpenVPN > Wizards, select Local User Access
  + Create Certificate Authority (CA):
    - Name: MyCompanyCA
    - Default settings for key, algorithm, lifetime, country, state, city
  + Create Server Certificate:
    - Name: pfSenseVPNServerCert
  + Configure OpenVPN Server:
    - Interface: WAN
    - Protocol: UDP IPv4
    - Local Port: 1194
    - Tunnel Network: 10.0.8.0/24
    - Local Network: 10.1.1.0/24
    - DNS Server: 10.1.1.1
    - Max concurrent connections: as required
  + Configure Firewall Rules via wizard:
    - Allow traffic from VPN clients to LAN
    - Allow traffic from internet to OpenVPN server
  + Create VPN User:
    - Username: remoteuser
    - Password: strong password
    - Enable user certificate creation
    - Certificate Authority: MyCompanyCA
  + Export Client Configuration File (.ovpn) using openvpn-client-export package
  + Test VPN connection with exported file and credentials
  + Implement Captive Portal on server-net interface using TurnKey AD authentication
  + Verify login from Client-VM and internet access

**Outcome**

* JR Admin has **read-only access** to firewall rules and diagnostics.
* LDAP integration allows pfSense to authenticate external users (testuser).
* Captive Portal restricts network access to authenticated users.
* VPN access is secure, with only authenticated users able to connect.
* Overall, RBAC and authentication policies are implemented successfully across pfSense services.

**Solution**

**1. Local User and Role Creation**

* Create Limited-Privilege Group
* From your Client-VM, log into the pfSense web interface as the admin user.
* Navigate to System > User Manager.
* Click on the Groups tab.
* Click the + Add button to create a new group.
* Group name: Firewall Viewers
* Scope: Local
* Description: Read-only access to firewall status and rules.
* 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.

* Under "Assigned Privileges," click the + Add button.
* 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.

* + We7bCfg - Diagnostics: all (expect authentication and edit)
* 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.

* Create a Local User and Assign to the Group
* While still in System > User Manager, click on the Users tab.
* Click + Add.

A screenshot of a computer

AI-generated content may be incorrect.

* Username: jradmin (for Junior Admin)
* Password: jradmin@123 (or any other password)
* Full name: Junior Admin
* 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.

* **Click Save.**

A screenshot of a computer

AI-generated content may be incorrect.

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

A screen shot of a login screen

AI-generated content may be incorrect.

* **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.

**2. Integration with External Authentication (LDAP)**

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.

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

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

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

A screenshot of a computer

AI-generated content may be incorrect.

* 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.

* Set a Static IP for the TurnKey Server

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

* Go to your kali machine and log into the pfSense GUI.
* Navigate to Status > DHCP Leases.
* 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.

* 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.

* Click Save.

A screenshot of a computer

AI-generated content may be incorrect.

* Go back to your TurnKey VM console and reboot it by typing reboot and pressing Enter.
* 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.

**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.

* 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.

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

A screen shot of a computer

AI-generated content may be incorrect.

* 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.

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

A screenshot of a computer

AI-generated content may be incorrect.

* Click on Create a new user.

A screenshot of a computer

AI-generated content may be incorrect.

* **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.
* 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.

**pfSense Configuration (Connecting to LDAP)**

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

* **Create the Authentication Server in pfSense**
* In the pfSense GUI, navigate to System > User Manager > Authentication Servers

A screenshot of a computer

AI-generated content may be incorrect.

* **Click + Add.**
* **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.

* Click Save.

Test the Connection

* Navigate to Diagnostics > Authentication.
* Authentication Server: Select your new TurnKey AD.
* Username: testuser
* Password: The password you set for testuser.
* Click Test.
* 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.

**3. Captive Portal Configuration**

* **Enable and Configure the Captive Portal**
* **Navigate to Services > Captive Portal.**
* **Click + Add.**
* **Description: Captive Portal Demo**
* **Select the HR interface to enable the portal on.**
* **Click Save & Continue.**
* **On the next page, check the box to Enable Captive Portal.**
* **Scroll down to the "Authentication" section.**
* **For Authentication method, ensure Turnkey-AD is selected**
* **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.

* **Testing the Captive Portal**
* **On your Client-VM, open the Firefox web browser.**
* **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.

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

A screenshot of a computer

AI-generated content may be incorrect.

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

**4. VPN Configuration and User Assignment**

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

A screenshot of a computer

AI-generated content may be incorrect.

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.

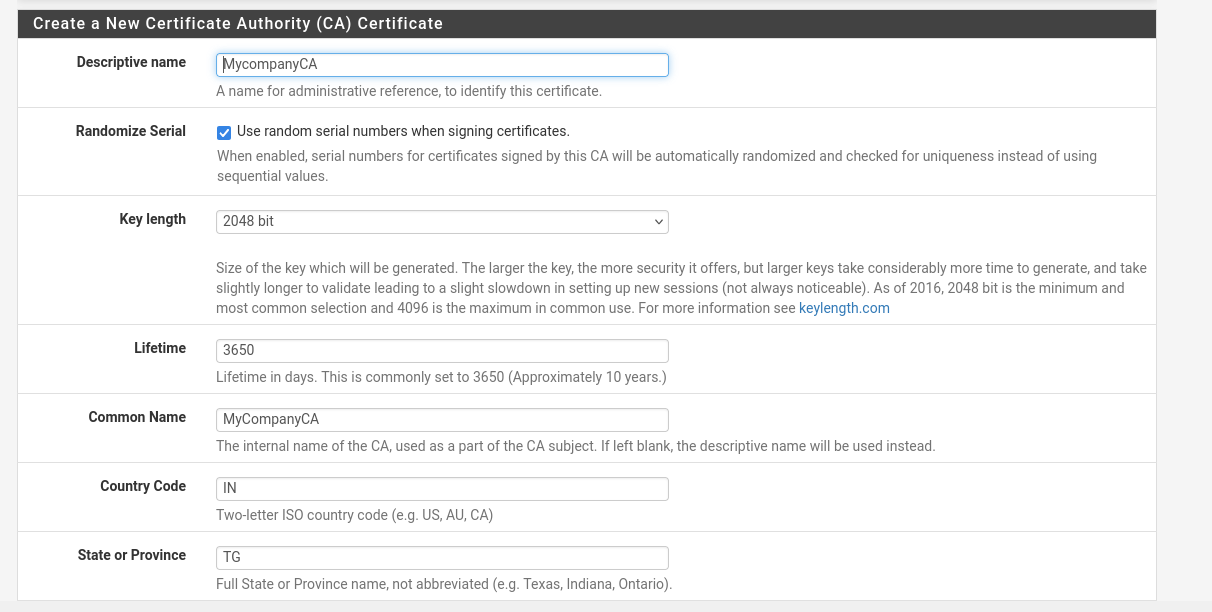
A screenshot of a computer

AI-generated content may be incorrect.

Create the Certificate Authority (CA)

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

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



A screenshot of a computer

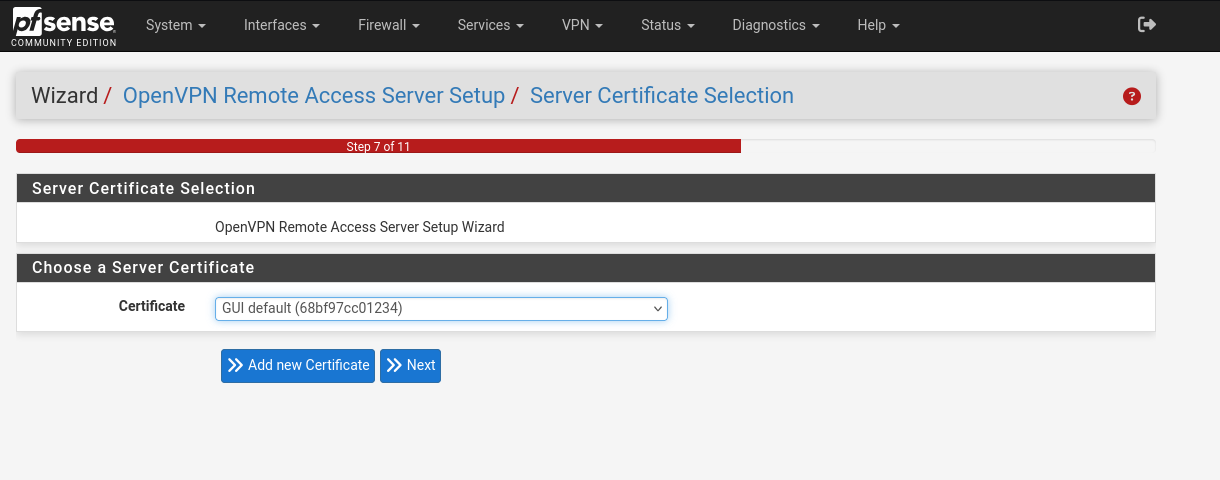
AI-generated content may be incorrect.

MyCompanyCA should be looking something similar

Create the Server Certificate

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

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

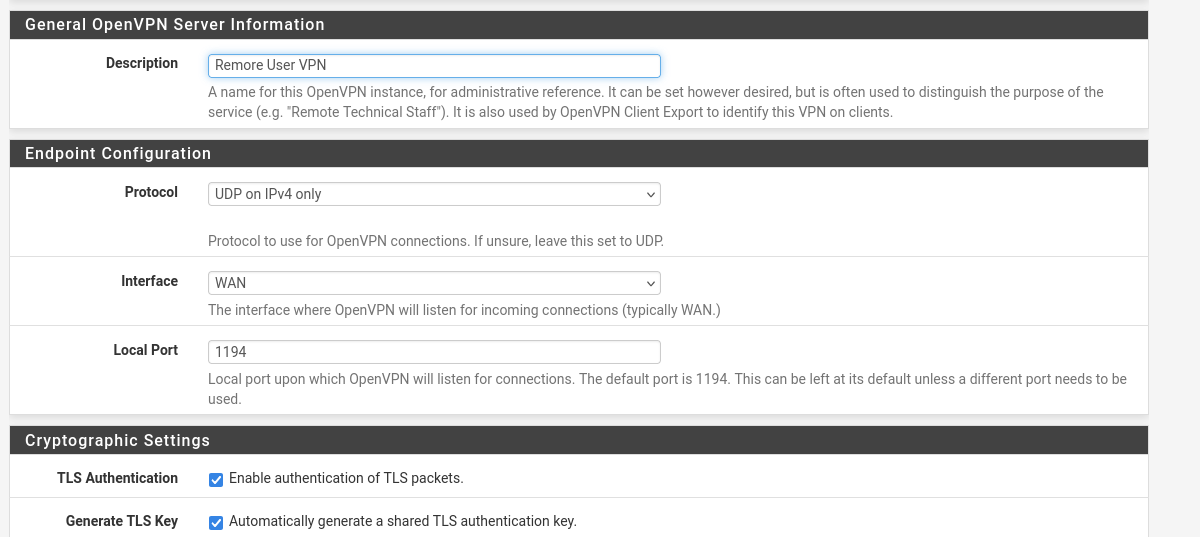




Configure the OpenVPN Server

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.

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.

* Create a VPN User
* Navigate to System > User Manager.
* Click the + Add button.
* Username: Enter a username, for example, remoteuser.
* Password: Set a strong, unique password for this user.
* Full name: Remote VPN User.
* 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.
* 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.

Export the Client Configuration File

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

* First, you must install a helper package. Go to System > Package Manager > Available Packages.
* Search for openvpn-client-export and click the green + Install button. Confirm the installation.
* 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.

* 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.
* 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

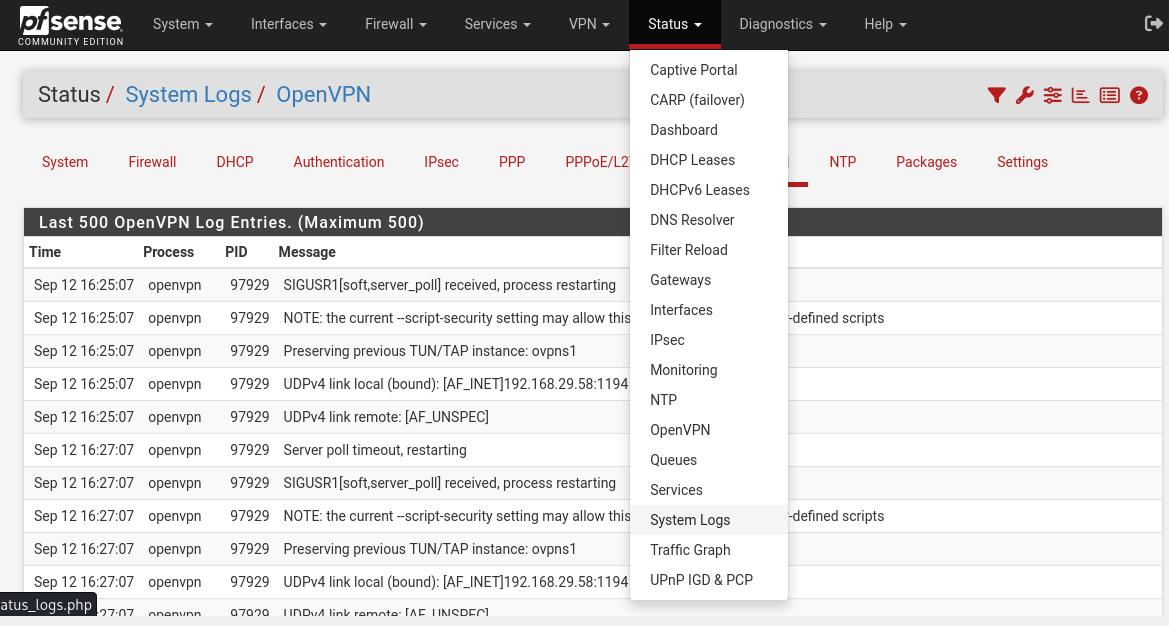
AI-generated content may be incorrect.**

Connecting as a Remote User

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

**Captive Portal Implementation**

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

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

**Testing the Full System**

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