This guide will walk you through configuring an OpenVPN server instance in pfSense to allow Yealink IP Phones (T26P, T28P, T32G, and T38G) to connect to your PBX remotely over a VPN tunnel. Not only is this more secure as your conversations are now encrypted, this also alleviates any of the NAT/firewalling issues that all too often come along with running remote SIP extensions. Although we are using the OpenVPN server that comes with pfSense in this example, the settings can be applied to any OpenVPN server. You could just as easily apply this to OpenVPN running on some other appliance or even run the OpenVPN server directly on your PBX.

Overview

1. Create a new certificate authority (CA) for the remote phones
2. Create a new server certificate for our remote phone OpenVPN server instance
3. Create a new OpenVPN server instance for the remote phones
4. Create necessary firewall rules
5. Create a new certificate for each remote phone
6. Create the Yealink OpenVPN configuration file
7. Register the phone to the PBX and upload the OpenVPN configuration file

Tested with:

pfSense 2.1
OpenVPN Client Export Utility 1.1.4

*If a field is not specifically mentioned in this guide leave it at its default setting
Create a new certificate authority (CA) for remote phones

1. Navigate to **System → Cert Manager**
2. On the **CA** tab click the + to add a new CA

**System: Certificate Authority Manager**

<table>
<thead>
<tr>
<th>Name</th>
<th>Internal</th>
<th>Issuer</th>
<th>Certificates</th>
<th>Distinguished Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Road Warrior CA</td>
<td>YES</td>
<td>self-signed</td>
<td>2</td>
<td>emailAddress=<a href="mailto:cscardefield@sunstatetech.com">cscardefield@sunstatetech.com</a>, ST=Arizona, C=sunstate Technology Group, L=Scottsdale, CN=Road Warrior CA, C=US</td>
</tr>
</tbody>
</table>

Additional trusted Certificate Authorities can be added here.

3. Use the following settings for the new CA:

- **Descriptive Name**: Remote Phone CA
- **Method**: Create an internal Certificate Authority
- **Digest Algorithm**: SHA1
- **Distinguished Name**: Your contact info
- **Common Name**: RemotePhoneCA

**System: Certificate Authority Manager**

- **Descriptive Name**: Remote Phone CA
- **Method**: Create an internal Certificate Authority

**Internal Certificate Authority**

- **Key length**: 2048 bits
- **Digest Algorithm**: SHA1
  - NOTE: It is recommended to use an algorithm stronger than SHA1 when possible.
- **Lifetime**: 3650 days

- **Distinguished Name**:
  - Country Code: US
  - State or Province: Arizona
  - City: Scottsdale
  - Organization: Sunstate Technology Group
  - Email Address: cscardefield@sunstatetech.com
  - Common Name: RemotePhoneCA

**Save**
Create a new server certificate for our remote phone OpenVPN server instance

1. Navigate to System → Cert Manager
2. Click on the Certificates tab
3. Click the + to add a new certificate

4. Use the following settings for your new server certificate:
   
   **Method**: Create an internal Certificate  
   **Descriptive name**: Remote Phone Server Cert  
   **Certificate authority**: Remote Phone CA  
   **Digest Algorithm**: SHA1  
   **Certificate Type**: Server Certificate  
   **Distinguished name**: Your contact info  
   **Common Name**: RemotePhoneServerCert
Create new OpenVPN server instance for remote phones

1. Navigate to VPN → OpenVPN
2. On the Server tab click the + to add a new OpenVPN instance

OpenVPN: Server

3. Use the following settings for the new OpenVPN server instance:

   **Server Mode:** Remote Access (SSL/TLS)\(^1\)

   **Protocol:** UDP

   **Device Mode:** tun

   **Interface:** The interface you want OpenVPN to listen on, usually WAN

   **Local port:** Default OpenVPN port is 1194, but you can use any port not already in use

   **Description:** Remote Phone VPN

   **TLS Authentication:** Uncheck the box for “Enable authentication of TLS packets.”

   **Peer Certificate Authority:** Remote Phone CA

   **Server Certificate:** Remote Phone Server Cert

   **Encryption algorithm:** BF-CBC (128-bit)

   **Tunnel Network:** 10.15.20.0/24 (can be any unused network expressed in CIDR)

   **Local Network:** The network your PBX is on, usually your LAN (expressed as CIDR)

   **Concurrent connections:** However many concurrent VPN sessions you want to allow

---

\(^1\) At the time of this writing, the Yealink VPN client only supports authentication by certificate, User Auth will not work.
Create firewall rules for OpenVPN and SIP/RTP traffic across the VPN tunnel

1. Navigate to Firewall → Rules
2. Click on the WAN tab
3. Click on the + to add a new firewall rule

<table>
<thead>
<tr>
<th>Interface</th>
<th>Protocol</th>
<th>Source</th>
<th>Port</th>
<th>Destination</th>
<th>Port</th>
<th>Gateway</th>
<th>Queue</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>WAN</td>
<td>UDP</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>9000</td>
<td>9049</td>
<td>none</td>
<td>SIP RTP</td>
</tr>
<tr>
<td>WAN</td>
<td>UDP</td>
<td>172.24.32.5</td>
<td>1194</td>
<td>OpenVPN</td>
<td>*</td>
<td>none</td>
<td>OpenVPN Remote Access</td>
<td></td>
</tr>
</tbody>
</table>

4. Use the following settings for the new firewall rule:
   - **Interface**: WAN
   - **Protocol**: UDP
   - **Destination**: WAN address (or whatever address OpenVPN is listening on)
   - **Destination port range**: whatever port your OpenVPN instance is running on
   - **Description**: OpenVPN Remote Phones

5. Navigate to Firewall → Rules
6. Click on the OpenVPN tab
7. Click on the + to add a new firewall rule

<table>
<thead>
<tr>
<th>ID</th>
<th>Proto</th>
<th>Source</th>
<th>Port</th>
<th>Destination</th>
<th>Port</th>
<th>Gateway</th>
<th>Queue</th>
<th>Schedule</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>UDP</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>OpenVPN</td>
<td>none</td>
<td></td>
<td>Remote Access – SIP</td>
</tr>
</tbody>
</table>

8. Use the following settings for the new firewall rule:
   - **Interface**: OpenVPN
   - **Protocol**: UDP
   - **Source**: Network 10.15.20.0/24 (whatever tunnel network you used in OpenVPN)
   - **Destination**: Any
   - **Destination port range**: 5060
   - **Description**: Remote Phones – SIP
9. Add another firewall rule on the **OpenVPN** tab with the following settings:

   - **Interface**: OpenVPN
   - **Protocol**: UDP
   - **Source**: Network 10.15.20.0/24 (whatever tunnel network you used in OpenVPN)
   - **Destination**: Any
   - **Destination port range**: 7000-7499 (whatever RTP ports your PBX uses for internal calls)
   - **Description**: Remote Phones – RTP

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Source</th>
<th>Destination</th>
<th>Port Range</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>UDP</td>
<td>10.15.20.0/24</td>
<td>*</td>
<td>5060 (SIP)</td>
<td>Remote Phones – SIP</td>
</tr>
<tr>
<td>UDP</td>
<td>10.15.20.0/24</td>
<td>*</td>
<td>7000 – 7499</td>
<td>Remote Phones – RTP</td>
</tr>
</tbody>
</table>

**Create a new certificate for each remote phone**

1. Navigate to **System → Cert Manager**
2. On the **Certificates** tab click on the + to add a new user certificate
3. Use the following settings for each certificate:

   - **Method**: Create an internal Certificate
   - **Descriptive name**: Descriptive name for the phone
   - **Certificate authority**: Remote Phone CA
   - **Digest Algorithm**: SHA1
   - **Certificate Type**: User Certificate
   - **Distinguished name**: Fill in all the information
Create the Yealink OpenVPN configuration file

1. Install the OpenVPN Client Export Utility package:
   a. Navigate to System → Packages
   b. On the Available Packages tab click the + next to OpenVPN Client Export Utility to install it.

2. Export the Yealink OpenVPN config file via the Client Export Utility:
   a. Navigate to VPN → OpenVPN → Client Export
   b. Select your OpenVPN instance for Remote Access Server
   c. Select the correct option for Host Name Resolution
   d. Under Client Install Packages click on T28 next to the certificate that you created for the phone

Register the phone to the PBX and upload the OpenVPN configuration file

1. Configure the phone to register to the PBX internally and verify it is working properly
2. Log into the phones web configuration interface and navigate to Network → Advanced
3. Scroll down to the VPN section
4. Click Browse and find the OpenVPN configuration tar archive we made earlier
5. Click Import
6. Make sure VPN Active is set to Enabled, then scroll down to the bottom and click Confirm
7. Reboot the phone

If everything goes right the phone will come up registered and you will see the VPN icon in the upper right hand corner of the display.

Wasn’t that fun? 😄