VPN Settings

CooVox-U20/U50/U60/U100

ZYCOO

We Focus · We Deliver

The purpose of this document is to detail how to configure the VPN Server and Client settings on a CooVox IP PBX. Note: If your IP PBX is behind a Router and you want to use L2TP, PPTP or the OpenVPN server, then you must setup port forwarding on your router to your IP PBX.

Depending on your VPN choice will depend which port needs forwarding?

L2TP: forward UDP port 1701

PPTP: forward TCP port 1723

OpenVPN: forward both UDP & TCP port 1194

The following examples shows the steps necessary in order to setup a VPN on a Local (internal) network. If you need to setup VPNs for an External network, then please just change the client VPN server's address as required.

1. L2TP Settings

1.1 To enable the L2TP Server see the diagrams below:

Reference:

Item	Explanation
Remote Start/End IP	This is used to assign an VPN IP range to the VPN Clients
Local IP	This is the local VPN Server IP
Enable the L2TP Server, click "Save" and the Status will change to "L2TP(Enable)".	

1.2 Create a L2TP client account that will connect to the L2TP Server

1.3 L2TP Client Settings

Once the L2TP settings have been saved, you can check the L2TP VPN client's status, by looking at the Status section underneath the VPN Client's settings, if it shows both the local and remote IP addresses, then the L2TP VPN client has connected to the L2TP VPN Server.

1.4 To verify whether the Client has connected to the server successfully

Open "Network Settings/Troubleshooting", input the remote IP address of the L2TP VPN Client and click on the "Run" button to perform a ping test.

Troubleshooting

Ping	Traceroute

Ping 10.10.10.1_____ Packets: 4__ Run Stop

```
PING 10.10.10.1 (10.10.10.1): 56 data bytes
64 bytes from 10.10.10.1: seq=0 ttl=64 time=5.701 ms
64 bytes from 10.10.10.1: seq=1 ttl=64 time=5.702 ms
64 bytes from 10.10.10.1: seq=2 ttl=64 time=5.024 ms
64 bytes from 10.10.10.1: seq=3 ttl=64 time=4.818 ms

--- 10.10.10.1 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 4.818/5.311/5.702 ms
```

From the above ping statistics, we can see that the L2TP VPN has been correctly configured, and is fully working.

2. PPTP Settings

2.1 To Enable the PPTP Server follow the diagrams below:

VPN Server

VPN Server	VPN Users Management

VPN Server

○ L2TP ◉ PPTP ○ OpenVPN

Enable:	☑
Remote IP:	10.20.10.3_____ - 10__
Local IP:	10.20.10.1_____
Primary DNS:	8.8.8.8_____
Alternate DNS:	8.8.8.8_____
Timeout(sec):	20___
Authentication Method:	☐ chap ☐ pap ☑ mschap ☑ mschap-v2
Enable mppe128:	☑
Debug:	☑

Save Cancel

Status: PPTP (Enable)

Reference:

Item	Explanation
Remote Start/End IP	This is used to assign an VPN IP range to the VPN Clients
Local IP	This is the local VPN Server IP
Enable the PPTP Server, click "Save" and the Status will change to "PPTP(Enable)".	

2.2 Create a PPTP client account that will connect to the PPTP Server

2.3 PPTP Client Settings

Enable the PPTP Client:


```
Status:  local  IP address 10.20.10.2
         remote IP address 10.20.10.1
```

Once the PPTP settings have been saved, you can check the PPTP VPN client's status, by looking at the Status section underneath the VPN Client's settings, if it shows both the local and remote

IP addresses, then the PPTP VPN client has connected to the PPTP VPN Server.

2.4 To verify whether the PPTP Client has connected to the server successfully

Open "Network Settings/Troubleshooting", input the remote IP address of the PPTP VPN Client and click on the "Run" button to perform a ping test.
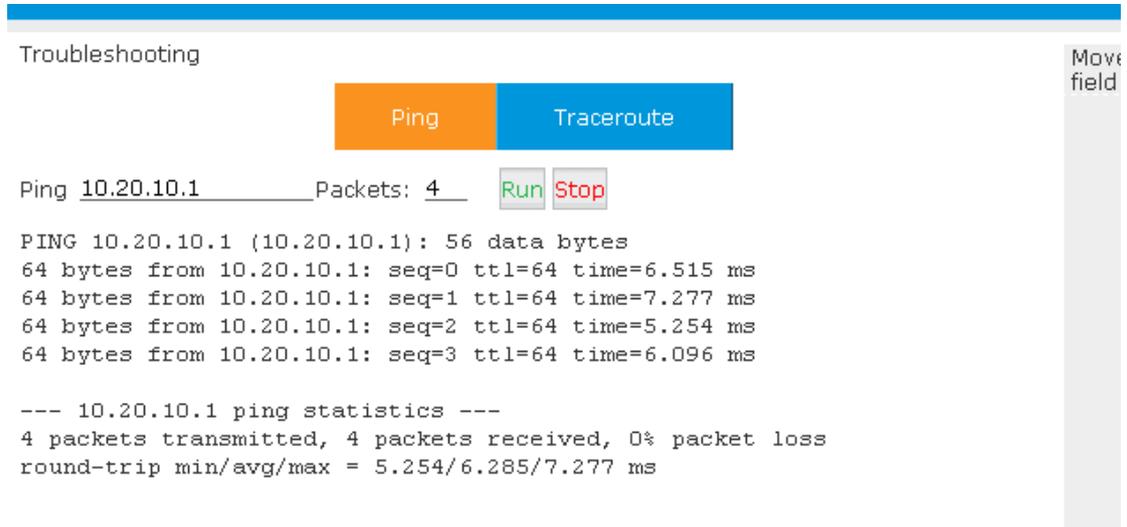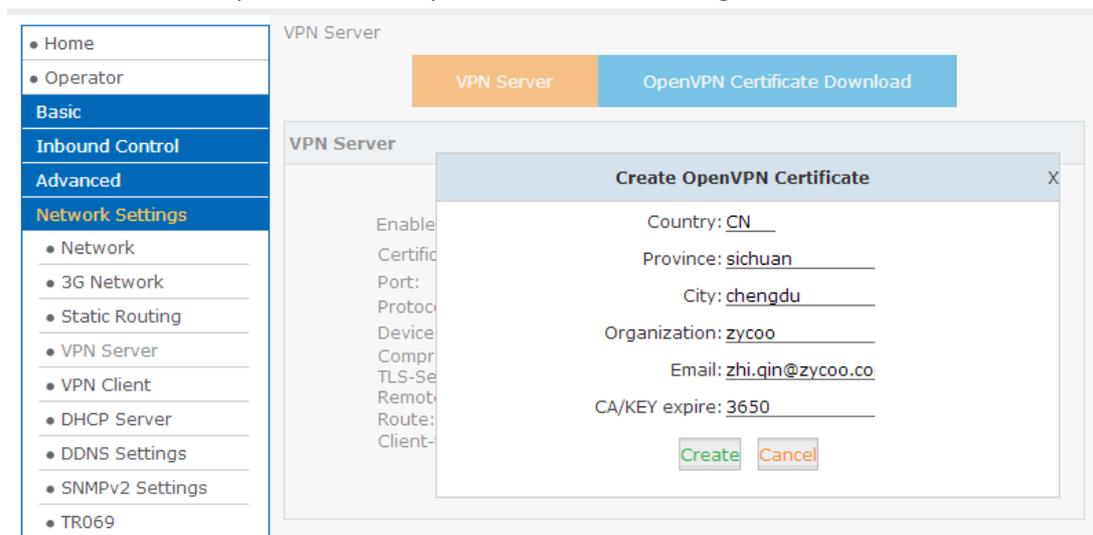

From the above ping statistics, we can see that the PPTP VPN has been correctly configured, and is fully working.

3. OpenVPN Settings

3.1 Before you can configure the OpenVPN server, you will need to create an OpenVPN Certificate.

Click【Create】to open the Create OpenVPN Certificate settings box

Input your certificate parameters including country, province, city, organization, email and the CA/KEY expiry time (days) and click on the "Create" button to create the new certificate.

3.2 To Enable the OpenVPN Server follow the diagrams below:

Remote Network: This setting is used to define the network segment from which an IP will be assigned to the OpenVPN Client.

3.3 Download the OpenVPN Certificate

Click "OpenVPN Certificate Download" and then Click【New Certificate】to Create a new certificate, the certificate name can be customized.

Input a Certificate Name and then click the "Create" button, once this has been created, you will need to download and save the new certificate locally.

To download the newly created certificate, click on the "Download" button, the downloaded TAR file once extracted contains two certificates and a key that are required by the OpenVPN client.

3.4 OpenVPN Client Settings

On the VPN Client you will need to enable the OpenVPN client, before you can upload the OpenVPN certificates that you downloaded and saved locally from the OpenVPN Server shown in the previous step.

Note: CA Certificate<----->ca.crt

Client Certificate<--->test.crt

Client Key<------->test.key

You must upload the two Certificates and Key, one at a time and in the above order and click on the "Save" button to complete the OpenVPN setup..

Now please try to connect to the OpenVPN Server:

When the Client has successfully connected to the OpenVPN server, the status will change and

show the OpenVPN client's IP address which can be seen in the diagram below.

3.5   To verify whether the OpenVPN Client has connected to the OpenVPN server successfully

Find the VPN Server IP address using the ifconfig command (this requires ssh access) and check the tun0 configuration to find the server IP Address. In the example below you can see the IP Address is 192.168.100. 1.

```
tun0      Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
          inet addr:192.168.100.1  P-t-P:192.168.100.2  Mask:255.255.255.255
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

Next from the VPN Client try to ping the OpenVPN servers IP address

From the above ping statistics, we can see that the PPTP VPN has been correctly configured, and is fully working.