Com.X IP PBX

The complete communications solution in a box

TECHNICAL NOTE

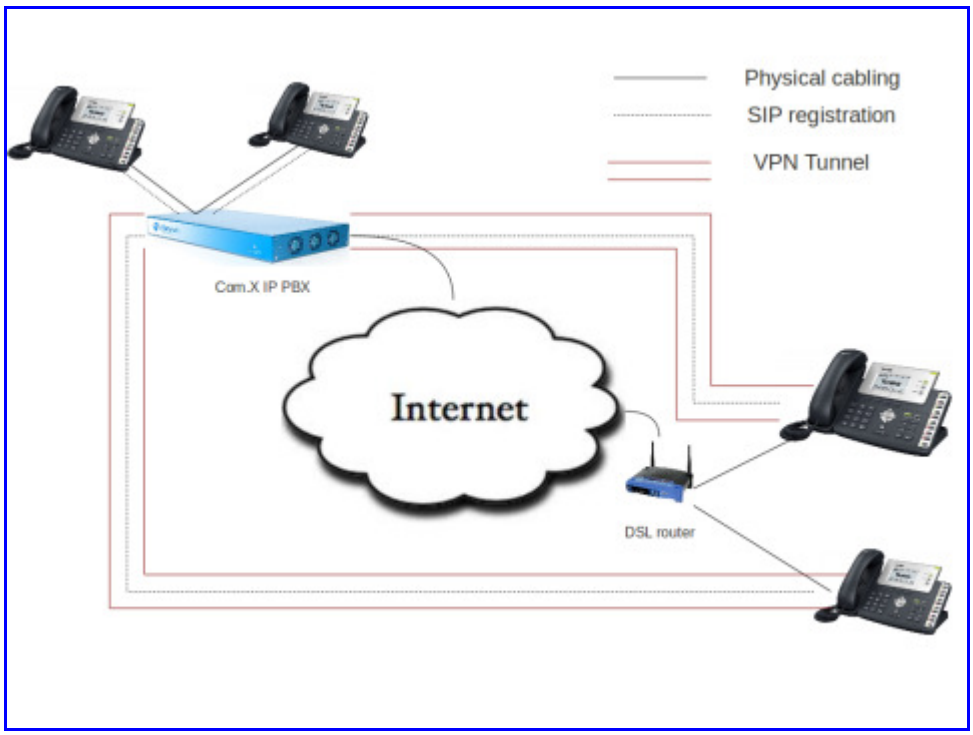
Utilising VPN security when extending PBX services to remote users

Virtual Private Network

It is not uncommon for a single company to occupy more than one set of premises. Individual users on geographically separated sites require seamless access to the same voice and data services. Moreover, there is a growing trend towards part-time or full-time work from home. A Virtual Private Network (VPN) makes use of the internet to securely connect remote sites and devices to the main corporate network. To ensure security, a VPN allows registration only to authenticated devices and makes use of encryption on all data transfers.

Why would I need a VPN?

Using a VPN allows for SIP endpoints (VoIP phones or softphones) on remote sites to register as extensions on a Com.X that physically resides elsewhere. A VPN will ensure that all traffic traversing the public internet is safely routed through an encrypted tunnel. This provides the remote user all the privileges of local access, including the ability to make use of outbound routes, transfer to local extensions, enable and disable call recording, voicemail etc. The remote user maintains registration across the VPN, so that inbound, internal or transferred calls to the user ring at the remote device. It also allows users on separate sites to avoid carrier charges (on net rates) by making internal phone calls to each other.



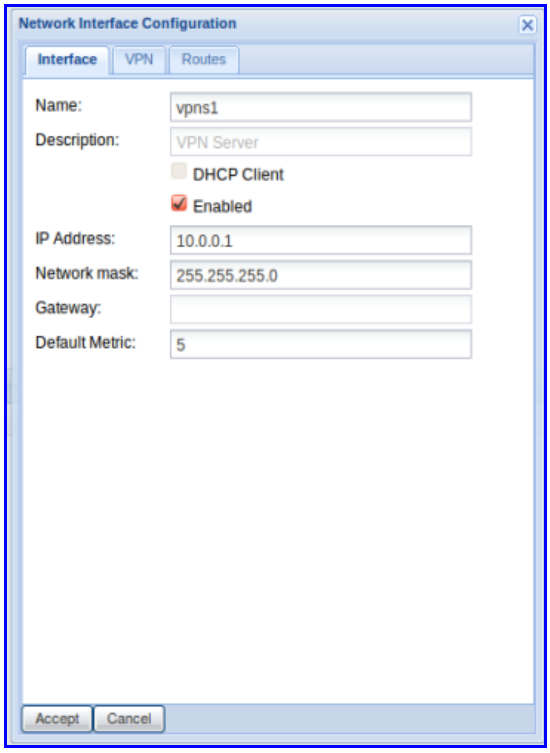
TECHNICAL NOTE

The Scenario presented below describes the configuration required on the Com.X and on a Yealink SIP handset to allow the Yealink to register as an extension on the Com.X through a VPN tunnel. First the VPN server on the Com.X is configured. Then a free SIP extension is configured on the Com.X. After the Com.X is completely configured, the VPN certificates are uploaded to the handset, and finally the handset is configured with account details to register with the free SIP extension created on the Com.X.

Configuring a VPN Server on the Com.X

To configure a VPN server on your Com.X system, navigate to the Network page of the Com.X GUI and select the VPN server port Vpns1 from the interfaces list.

Note: The VPN application presented below is available on all Com.X s./w revision 1.3.13 releases and above.



Enable the VPN server by ticking the "enabled" box, and choose an appropriate IP address for the server (typically 10.0.0.1). Select the VPN tab and set the required transport protocol and set the correct public IP address and port for the VPN server.

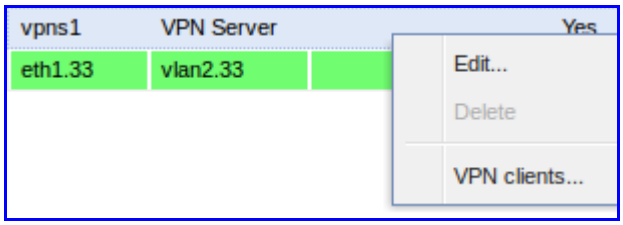
Note: In the above example the Com.X has a local IP address of 192.168.0.7. A VPN server has been configured on the Com.X with an IP address of 10.0.0.1. External traffic to the VPN server needs to reach the Com.X at 192.168.0.7:1194.
The VPN Public IP and VPN Public port fields are used in the generation of certificates for client devices. When the certificates are uploaded and activated on the end point clients, they automatically attempt to find and authenticate with a host at the public port of the public IP (DNS is used if the VPN Public IP is in the form of a domain).
Thus for this example, a firewall route would need be created to forward port 1194 of 192.168.0.7 to be externally visible as port 1194 of fsn.dnsalias.com.

Accept and Apply the configuration.

Generating Certificates for Client devices

In order for a device to authenticate as a client with the Com.X VPN server, the client needs to present its certificate issued by that server. The appropriate certificates are generated and packaged by the Com.X.

Right-click the Vpns1 interface in the interfaces list, and select VPN clients.

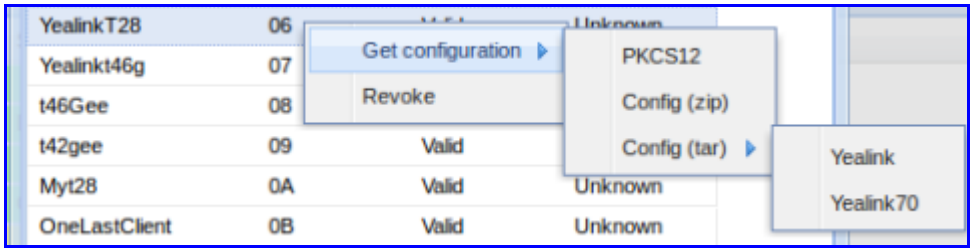


Follow the steps below to generate the VPN client's certificates:

1. Select New, and name the new client sensibly.
2. Apply the configuration to generate certificates.
3. Select the client from the clients list and select Get Configuration.

The certificates are available in a variety of packages, to suit the client device.

Note: Applying the configuration generates the certificate configuration folders for the client devices. Only after a client has been applied will the certificate package become available for exporting.

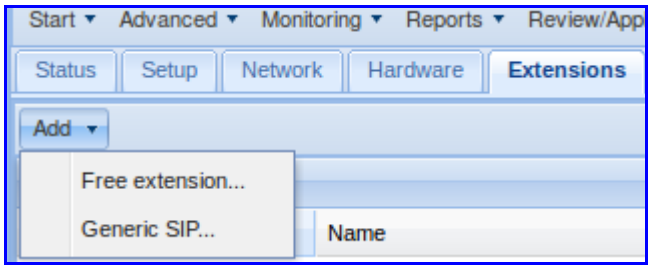


For Yealink handsets, select Config(tar) and then either Yealink (for devices with older firmware) or Yealink 70 (for devices running firmware version 9.70 or more recent). Save this folder to your PC or terminal, to later be uploaded onto the relevant IP endpoint.

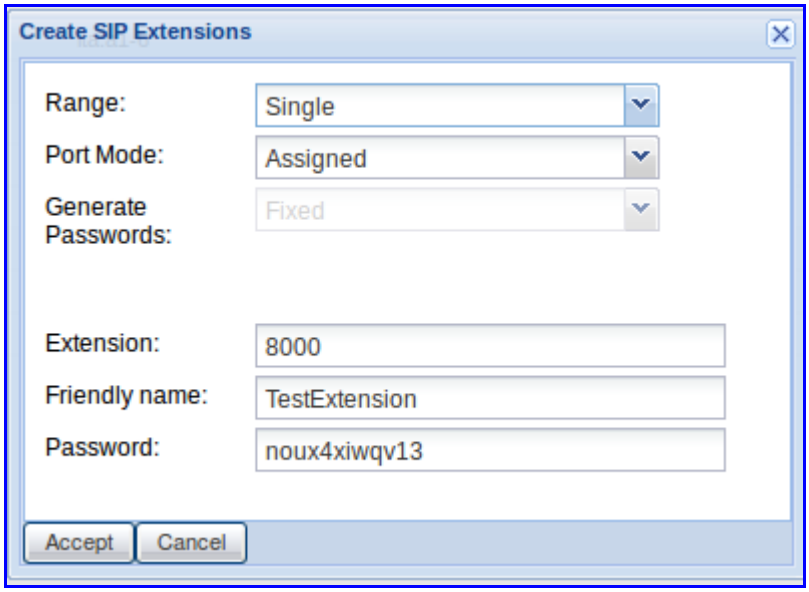
Configuring a Sip Extension on the Com.X

A generic SIP extension needs to be configured on the Com.X. The remote phone will register as this extension, through the VPN tunnel.

Navigate to the extensions tab of the Com.X GUI and select Add, Generic SIP.



Select a suitable name and extension number and make note of the generated password. (It would be best to record this password and extension number as you will later need to configure the handset with these details).



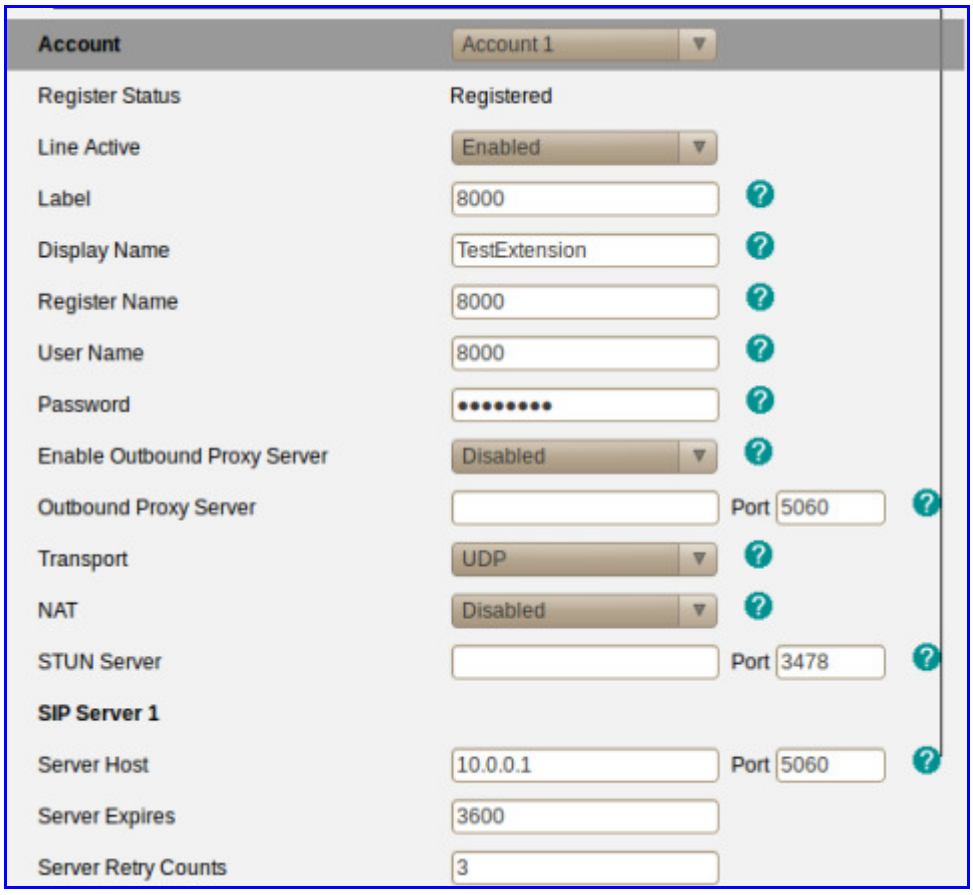
Accept and Apply the configuration.

Configuring the handset

Your handset will need to have the VPN settings and the extension account settings configured manually. For this example, a Yealink T46G is configured as a remote extension on the VPN.

Navigate to the advanced Network settings page, enable VPN and upload the .tar certificates file that you downloaded from the Com.X GUI. Confirm the VPN settings.

Then navigate to the account settings and configure the handset with the corresponding extension number and password configured on the Com.X. Set the Server IP address to that of the VPN server on the Com.X (the server IP port is the correct IP, not the public IP, which is used only for the VPN to be authenticated. Once the VPN is active, the device can contact the VPN server through the VPN tunnel)



Diagnostics

Confirming whether a client has successfully registered with the VPN host can be a little bit tricky.

There are a few methods that can be used to obtain such a confirmation and useful diagnostics for diagnosing unsuccessful connections.

From the Com.X terminal:

- Firstly, using “ifconfig” it can be confirmed whether the VPN tunnel is active by confirming that both transmitted and received packets are not zero. This is useful for confirming an active VPN but shares no information about the number of clients connected and the status of each client

- From the Asterisk CLI “sip show peers” returns a list of configured sip peers. When an extension is registered through the VPN, the SIP peer should show an IP address on the VPN subnet.

- If all else fails, a packet capture performed on the interface will show all traffic received and sent and can be analysed using tools such as Wireshark.

From the phone:

- If the phone shows a “registered” status, and can place and receive calls then the VPN tunnel is active.
- To obtain a packet capture from the phone, navigate to the GUI of the phone, then to Settings, then Upgrade and start the Pcap feature. After attempting to register the extension, stop the Pcap feature and select export to save a copy of the packet capture for analysis