IP Office Technical Tip

Tip No: **205**

Release Date: **10 June 2008**

Region: **GLOBAL**

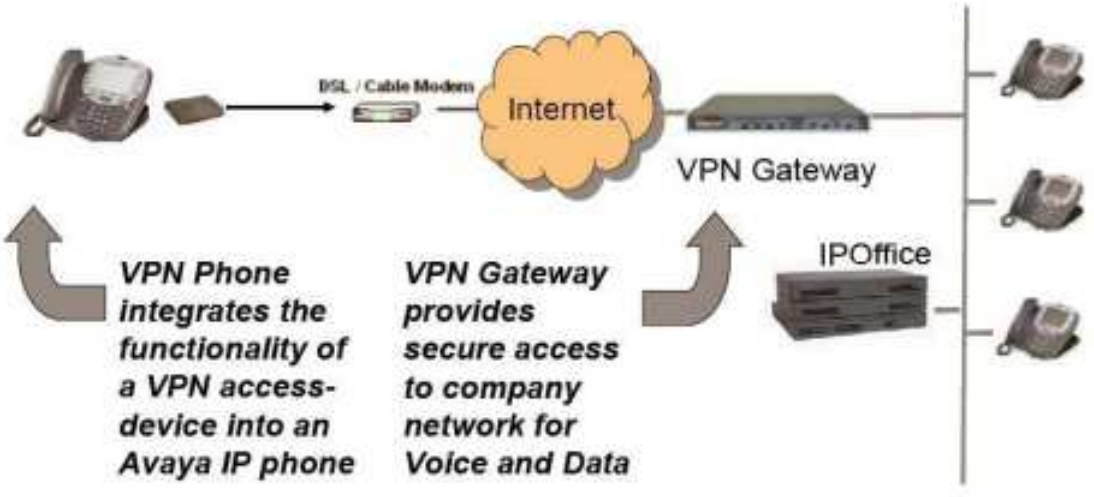
VPN Telephone Deployment Guide for IP Office

This document describes how to install and deploy the Avaya VPN Telephones for IP Office.

Introduction

The Avaya VPN Telephone provides remote users with an extension on the IP Office over a secure VPN connection in a single-box solution. The VPN Telephone is an H.323 IP Telephone with an integrated virtual private network (VPN) client. The built in client eliminates the need for a separate VPN gateway at the remote location. Upon boot up the VPN Telephone establishes a secure IPSec tunnel to the office VPN gateway and then registers to the IP Office. Once registered to the IP Office, all features available to an on site IP Telephone are now available to the remote VPN Telephone user.

The following diagram illustrates a typical IP Office VPN Telephone deployment.



Converting 4600 and 5600 IP Telephones into VPN Telephones

VPN Telephones share the same hardware as the 4600 series and the 5600 series IP telephones. Installing the VPN firmware converts a 4600 or 5600 IP Telephone into a VPN Telephone. Below is a list of the 6 convertible Telephones that are supported on IP Office.

- 4610SW - 5610SW
- 4620SW - 5620SW
- 4621SW - 5621SW

VPN firmware must first be installed on the telephone before it is deployed to the end user home location, but after deployment subsequent upgrades of the VPN firmware can be done while the telephone is at the remote location. Firmware installation is done via a download from a TFTP or HTTP file server to the telephone. It is recommended that a dedicated file server be created for VPN telephones, but it is also possible to have one file server for both VPN Telephones and non-VPN IP Telephones.

VPN Telephone files and its significance

The VPN firmware is now available in the Admin CD in the bin directory. The zip file contains the following script, settings and binary files.

1) 46xxvpn.scr – *upgrade script file that specifies the boot code for all VPN Telephone types*
2) 46vpnupgrade.scr – *upgrade script file that specifies the VPN firmware*
3) 46vpnsetting_readme.txt – *readme file for setting up VPN parameters*
4) 46vpnsetting_Template.txt – *template for setting up VPN parameters*
5) a10bVPNxxxxx.bin* - *VPN firmware for the 4610SW*
6) a20bVPNxxxxx.bin* - *VPN firmware for the 4620SW and the 4621SW*
7) i10aVPNxxxxx.bin* - *VPN firmware for the 5610SW*
8) i20aVPNxxxxx.bin* - *VPN firmware for the 5620SW and the 5621SW*

* xxxxx denotes the VPN firmware version number.

VPN Telephone startup sequence

At Startup VPN Telephones download the following script files from the file server in the order given below:

1) 46vpnupgrade.scr
2) 46vpnsettings.txt
3) 46xxsettings.txt

This arrangement has been provided so that you can administer

1) All options specific to IP telephone functionality in the 46xxsettings.txt file
2) All options specific to VPN Telephones in the 46vpnsettings.txt file
3) Upgrade/Downgrade VPN Telephones through 46vpnupgrade.scr

Setting up a Dedicated VPN Telephone file server

A dedicated VPN Telephone file server has its advantages. One advantage is that you can do bulk install of VPN firmware easily by setting the appropriate file server IP address in the telephones. Once you power up the telephones, the VPN firmware will be downloaded to the telephones.

To setup a dedicated file server, rename the 46xxvpn.scr file to 46xxupgrade.scr file. Then copy this renamed 46xxupgrade.scr file, 46vpnupgrade.scr file and all the binary (.bin) files into the appropriate TFTP or HTTP server home directory.

Setting up a Single File server for both VPN and Non-VPN telephones
The obvious advantage to a single file server is the cost associated in setting up and maintaining multiple file servers for VPN and non-VPN telephones.

To enable an existing non-VPN telephone file server to additionally serve VPN Telephones, the current 46xxupgrade.scr file needs to be modified along with adding the appropriate files to the file server home directory.

Add the following text (if it is not already there) to the beginning of the existing 46xxupgrade.scr.

```
IF $GROUP SEQ 876 GOTO DEFVPN
GOTO NOVPN
# DEFVPN
GET 46xxvpn.scr
# NOVPN
```

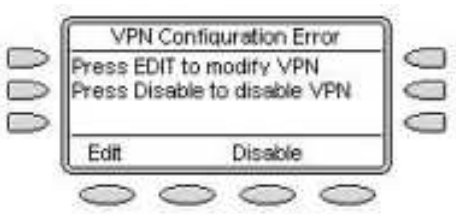
Copy the 46xxvpn.scr file, 46vpnupgrade.scr and all the .bin files into the appropriate TFTP or HTTP server home directory.

To install the VPN firmware, the telephone must first register with the IP Office as a non-VPN telephone. Once it is registered with an extension then you must modify the Group to 876 by pressing the following key sequence on the telephone keypad

```
MUTE 4 7 6 8 7 #
8 7 6 # #
MUTE 7 3 7 3 8 # * #
```

When the telephone reboots, the 46xxupgrade.scr script file will direct the telephone to upgrade to the VPN firmware.

Post Firmware installation
Depending on the speed of your network and the existing firmware version on the telephone, it may take up to 5 minutes to load the necessary VPN firmware. When the telephone has loaded the VPN firmware, it should show the following screen when it restarts. This error message is shown as the configuration details for the VPN tunnel have not yet been entered.



The administrator can manually pre-configure the VPN settings in the telephone or provide the configuration details to the end user for input. At this point the telephone is ready for deployment to the end user home location. The VPN configuration settings depend on the type of VPN Gateway being used. Please refer to the appropriate technical tip listed in the VPN Gateway section for the telephone VPN configuration settings.

Instead of manually configuring the VPN settings, the administrator can create a 46vpnsettings.txt file with all the necessary parameters and place it in the file server home directory. This is useful for deploying a large number of VPN Telephones. When a VPN Telephone boots up it will read the 46vpnsettings.txt file and configure itself based on that file. Please see the 46vpnsetting_readme.txt and 46vpnsetting_template.txt files for details on creating the file and setting the various parameters.

Setting the IP address parameters of the telephone in the home network
Most home routers will provide minimum DHCP configuration items to the VPN Telephone when plugged in the home network. This will not include the Call Server and File Server information that the VPN Telephone needs. This information can be statically assigned when the telephone boots up. Following is a table of IP address assignments needed when the VPN telephone is powered up in the remote user home network.

Item	Value	Description
Phone=	If DHCP is being used, set to 0.0.0.0. Otherwise, enter the IP address used by the telephone in the home network.	This is the IP address for the telephone in the Home network.
CallSv=	Enter the IP address if the IP Office.	IP address of the Call Server which is the IP Office.
CallSvPort=	Accept default of 1719 unless using a different port	This is the Call Server port used for signaling.
Router=	If DHCP is being used, set to 0.0.0.0. Otherwise, enter the IP address of the Home router.	Home router IP Address
Mask=	If DHCP is being used, set to 0.0.0.0. Otherwise, enter the Home network mask	Home network Mask
FileSv=	Enter the IP address of the HTTP or TFTP file server in the office network	HTTP or TFTP file server in the office network that serves the VPN telephones.

If the telephone VPN settings have been pre-configured, then once the telephone boots up, it will attempt to start the VPN connection. If it is unable to connect the telephone will show an error message. If the Telephone has not been pre-configured, then the user will have to input the VPN configuration parameters.

VPN Gateways

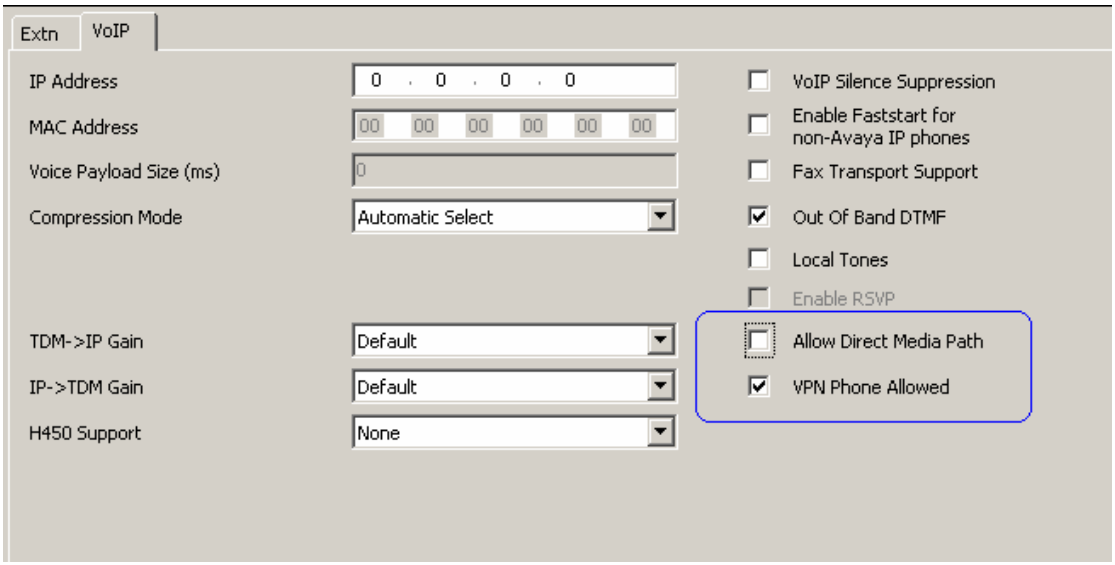
The VPN Telephone will communicate with a third party VPN gateway that strictly implements the Xauth with Pre-Shared Key. Below is a list of Avaya tested VPN gateways that are recommended for use with the IP Office. Please refer to the corresponding Technical Tip to setup the VPN gateway and the VPN telephone parameters.

1) Kentrox Q2300 Router - Global Technical Tip No. 185 issued Sept 2007
2) NetGear FVS338 Router – Global Technical Tip No. 184 issued Aug 2007
3) Adtran NetVanta 3305 – Global Technical Tip No. 186 issued Sept 2007
4) NetGear FVX538 Router - Global Technical Tip No. 196 issued Jan 2008
5) Sonicwall Tz170 Standard/Enhanced VPN Router - Global Technical Tip No. 190 issued Sept 2007

Security Association Lifetime
The VPN Telephone always proposes Security Association life time of 1 Day. This value cannot be modified in the telephone; however, if the VPN gateway is configured to offer a different life time, the telephone will accept the lifetime offered by the VPN gateway. It is recommended that the VPN gateway be configured with a Security Association lifetime of 5 days in order to minimize the complex calculations required by a re-key transaction.

Configuring IP Office for VPN Telephones

IP Office Manager Settings
Each VPN Telephones requires a license to register to the IP Office. Starting with IP Office release 4.1, a checkbox called “VPN Telephone Allowed” has been added to the Extension\VoIP configuration form for IP Telephones in the Manager application. To allow a VPN telephone to register, this setting must be enabled. This checkbox is greyed out until a valid VPN Telephone license has been loaded. Once the number of VPN telephones configured matches the VPN IP Extension license value this checkbox will be greyed out again.



***IMPORTANT**: Many VPN routers will not allow a direct media path to be established between two VPN endpoints. It is necessary to uncheck the Allow Direct Media Path checkbox for VPN Telephone extensions as shown above. Failure to do so may result in no speech path when two VPN extensions establish a call.*

Special consideration when using 4600 series telephones

By default, a 4600 series VPN telephone will register to an IP Office system without using a VPN telephone license. In this mode the telephone is un-licensed and will stop working after 180 days from the time the VPN firmware was installed. To ensure that the 4600 VPN telephone continues to work past the 180 day limit, the SMBLIC parameter must be enabled by adding the string “SET SMBLIC 1” in the 46vpnsettings.txt file. This will force the telephone to consume a license and ignore the 180 day timeout.

An easy way to test that the telephone has picked this setting up is to make sure that the VPN Telephone Allowed checkbox is not selected for this user. If the telephone has correctly picked up this setting it will display ‘Wrong Set Type’ on the telephone screen when it attempts to register. Once you see this message open the IP Office configuration and select the VPN Telephone Allowed checkbox and restart the VPN telephone to allow it to successfully register with the IP Office.

Other Considerations

Voice Quality over the Public Internet

Voice quality over an unmanaged IP network i.e the Public Internet is unpredictable. While great care has been taken to make the VPN Telephone highly reliable, Avaya has no influence and therefore cannot guarantee the quality of the IP network used. Avaya therefore cannot assume responsibility for voice quality problems incurred.

Verifying VPN Tunnel Configuration

When setting up a Security Gateway you can verify the configuration by using the manufacturer provided IPsec Client to setup a VPN tunnel using the protocol selected. If the VPN tunnel is successfully established, you have verified that the VPN gateway is correctly configured and the steps for creating a VPN tunnel between the VPN telephone and the security gateway should be successful.

Command to Display/Modify VPN Settings
Once the VPN telephone is running you can make any changes to the VPN settings by doing the following:

- MUTE 8 7 6 6 6 3 #
- Press ***** to modify the settings (* = Modify # = OK)

You can then view the settings and make any changes required. Pressing the button labeled 'Profile' allows you to change the type of VPN device that you are connecting to.

Testing IPSec Tunnel Quality
The VPN Telephone has a utility (Qtest) that allows the user to test the quality of the path from the telephone through the home network, the ISP, and the Internet to the VPN gateway.

To invoke the Qtest, press following key sequence:

- MUTE 8 7 6 6 6 3 #
- Press ***** to modify the settings (* = Modify # = OK)
- Press the "QTEST" softkey, to bring up the QTEST application screen. In the QTEST application screen press START soft key to start the QTEST and STOP softkey to stop the QTEST. The following QTEST statistics are displayed on the telephone screen while QTEST is running (Use Page Left / Right Keys to scroll between pages).

  - 1. Percent packet lost.
  - 2. Round trip delay of the last packet received.
  - 3. Percent packet late. (RTT was more than 400 ms)
  - 4. Number of packets sent.
  - 5. Number of packets received.
  - 6. Average round trip delay.
  - 7. Maximum round trip delay.
  - 8. Number of packets lost.
  - 9. Size of biggest burst lost.
  - 10. Number of packets received out of sequence.
  - 11. Number of interruptions encountered.

Issued by:
Avaya SSD Tier 4 Support
Contact details:-
EMEA/APAC
Tel: +44 1707 392200
Fax: +44 (0) 1707 376933
Email: gsstier4@avaya.com

NA/CALA
Tel: +1 732 852 1955
Fax: +1 732 852 1943
Email: IPOUST4ENG@Avaya.com

Internet: http://www.avaya.com