Avaya Solution & Interoperability Test Lab

Application Notes for Configuring the VPN IPSec Tunnel between Avaya 96xx Series IP Phone and Prosafe Quad WAN Gigabit SSL VPN Firewall SRX5308 and Avaya IP Office Release 8.1 - Issue 1.0

Abstract

These Application Notes present a sample configuration for an Avaya IP Office release 8.1 remote user with an Avaya 96xx IP Phone with VPN (IPSec) whereby the IPSec Tunnel is terminated in the main office location with the Prosafe Quad WAN Gigabit SSL VPN Firewall SRX5308.

These Application Notes provide information for the setup, configuration, and verification of the call flows tested on this solution.

1. Introduction

These Application Notes describe the steps to configure the Netgear Prosafe Quad WAN Gigabit SSL VPN Firewall SRX5308 (hereafter referred to as VPN Firewall) to support IPSec VPN (Virtual Private Network) tunnel termination using XAuth (eXtended Authentication) and local credential authentication for Avaya 96xx Series IP Phone. The Avaya 96xx Series IP Phone, release 3.1, is a software based IPSec Virtual Private Network (VPN) client integrated into the firmware of an Avaya 96xx Series IP Phone. This capability allows Avaya IP Telephone to be plugged in and used over a secure IPSec VPN connection from any broadband Internet connection. End users experience the same IP telephone features of the Avaya IP Office release 8.1, as if they were using the telephone in the office. Avaya IP telephone models supporting the Avaya 96xx Series IP Phone firmware include the 9620, 9620C, 9620L, 9630, 9640, 9650, 9650C and 9670.

2. Interoperability Testing

The focus of this testing was to verify that the 9600 series IP phones can establish a VPN IPSec tunnel with Netgear VPN Firewall. After successful establishment of the VPN IPSec tunnel, the VPN enabled 9600 series IP phone should be able to register to the IP Office server.

2.1. Test Description and Coverage

Testing was performed using the VPN enabled Avaya 9600 series IP phones, as a remote user, establishing a VPN IPSec tunnel with Netgear VPN Firewall where these IP phones are registering to the IP Office via VPN IPSec tunnel. Calls were then placed from other IP Office telephone clients/users to and from the VPN enabled 9600 series IP phones. Other telephony features were also verified: busy, hold, DTMF, MWI, voicemail, transfer and conference.

2.2. Test Results and Observations

The testing was completed successfully. The objectives outlined in **Section 2.1** were verified. The 9600 series IP phone was registered to IP Office successfully via VPN IPSec tunnel establishment between Netgear VPN Firewall and the 9600 series IP phone. Calls were made between IP Office telephones and VPN enabled 9600 series IP phone with clear voice path. The following notes are being observed during the testing:

1. The IP Phones may require a Virtual IP Address to be configured in the VPN settings. Please take care in choosing a Virtual IP Range. The user should ensure that there is no conflict between the IP address in the Home Router's dynamic pool, with the IP address selected for the VPN network. If manually configuring a Virtual IP Address on the IP Hard-phone, ensure that accurate records are kept of IP Address allocations to avoid IP Address conflicts.

2. Many VPN Routers will not allow a direct media path to be established between two VPN Endpoints. It will be necessary to uncheck the Direct Media Path checkbox in the Extension Configuration in IP Office if the router does not support direct media paths between two VPN endpoints. Failure to do so will result in No Speech path when two VPN extensions try and establish a call. By default this is enabled.

3. Reference Configurations

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 a 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 onsite IP Telephone are now available to the remote VPN Telephone user.

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

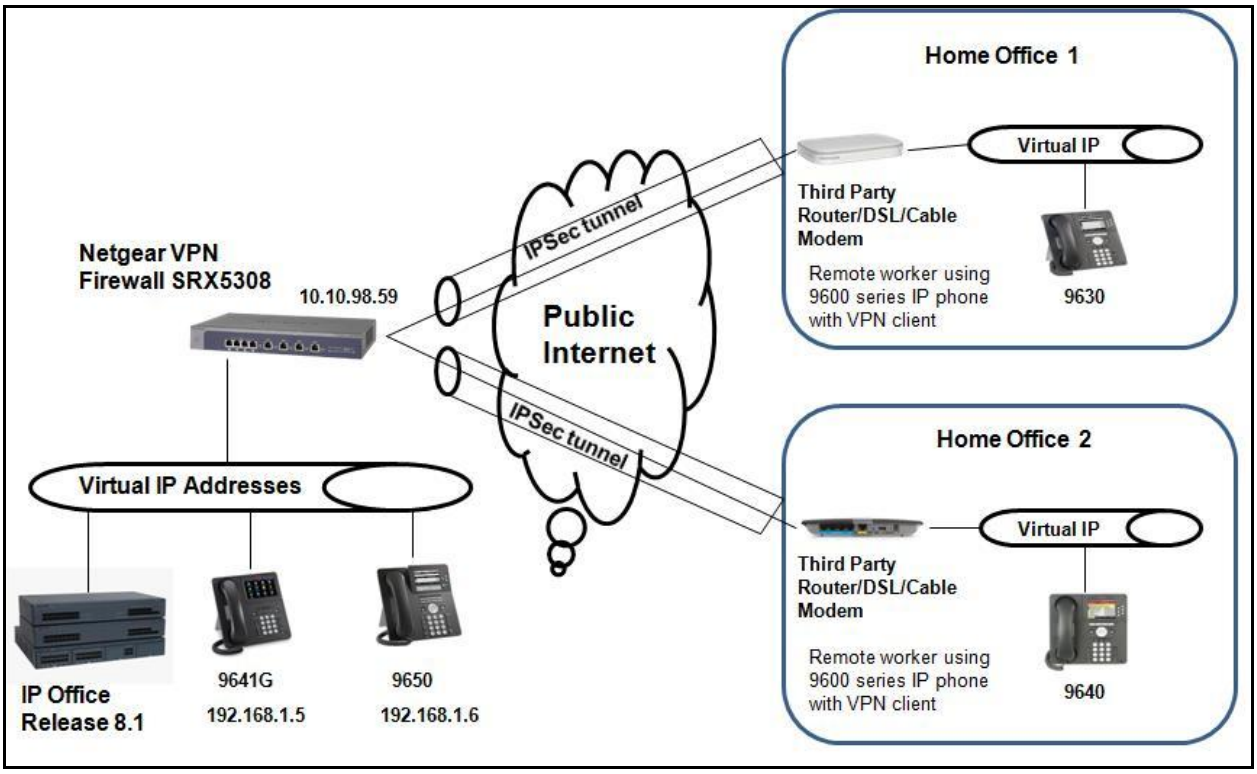


Figure 1: Remote User Home Office Connecting via IPSec tunnel (established by Netgear VPN) to IP Office Configuration

4. Equipment and Software Validated

The following equipment and software/firmware were used for the reference configuration:

Equipment	Software Version
Avaya IP Office (IP500 v2)	8.1.43
Avaya IP Office Manager	10.1.43
Avaya 9630 IP Telephone (VPN mode) Avaya 9640 IP Telephone (VPN mode) Avaya 9641G IP Telephone Avaya 9650 IP Telephone	S3.104S S3.171E S6.2119U S3.104S
Avaya Voicemail	Embedded
Prosafe Quad WAN Gigabit SSL VPN Firewall SRX5308	3.0.7-24

5. Avaya IP Office & Extension Configuration

5.1. Avaya IP Office Configuration

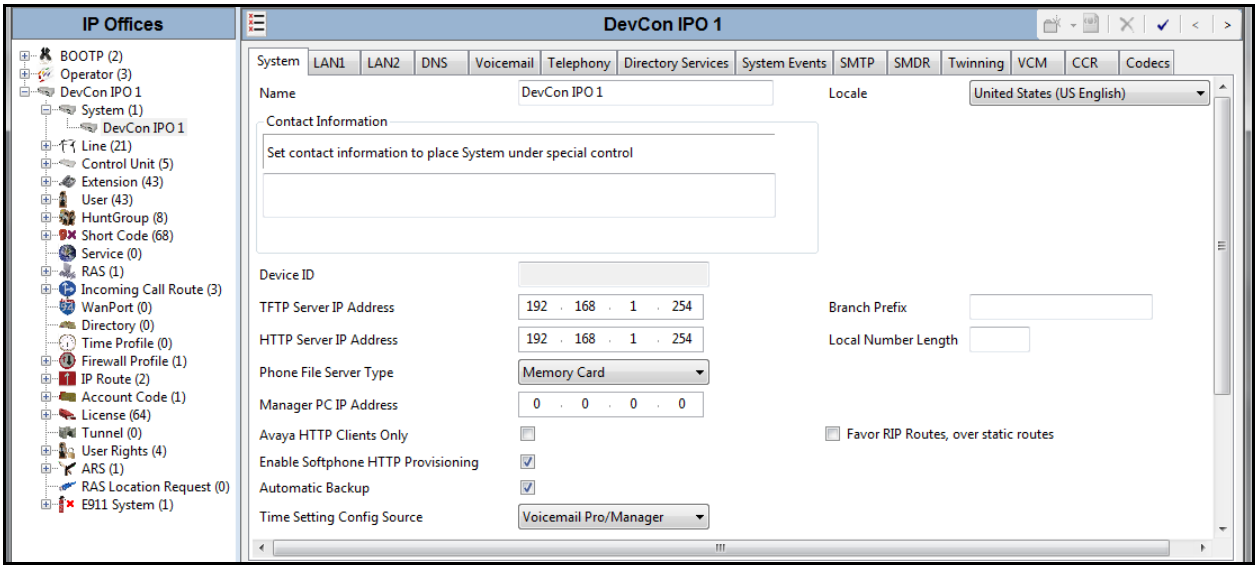
This section was included to verify that Avaya IP Office was configured correctly. Except where stated, the parameters in all steps are the default settings and are supplied for reference. For all other provisioning information such as provisioning of the trunks, call coverage and voice mail, please refer to the Avaya IP Office product documentation in **Section 10.**

Step 1

Avaya IP Office is configured via the Avaya IP Office Manager program. Log into the Avaya IP Office Manager PC and select **Start → Programs → IP Office → Manager** to launch the Avaya IP Office Manager application. Select **File → Open** to search for IP Offices in the network. Click on appropriate Avaya IP Office. Click **OK** to continue (not shown). Log in to the Avaya IP Office Manager application using the appropriate credentials.

Step 2

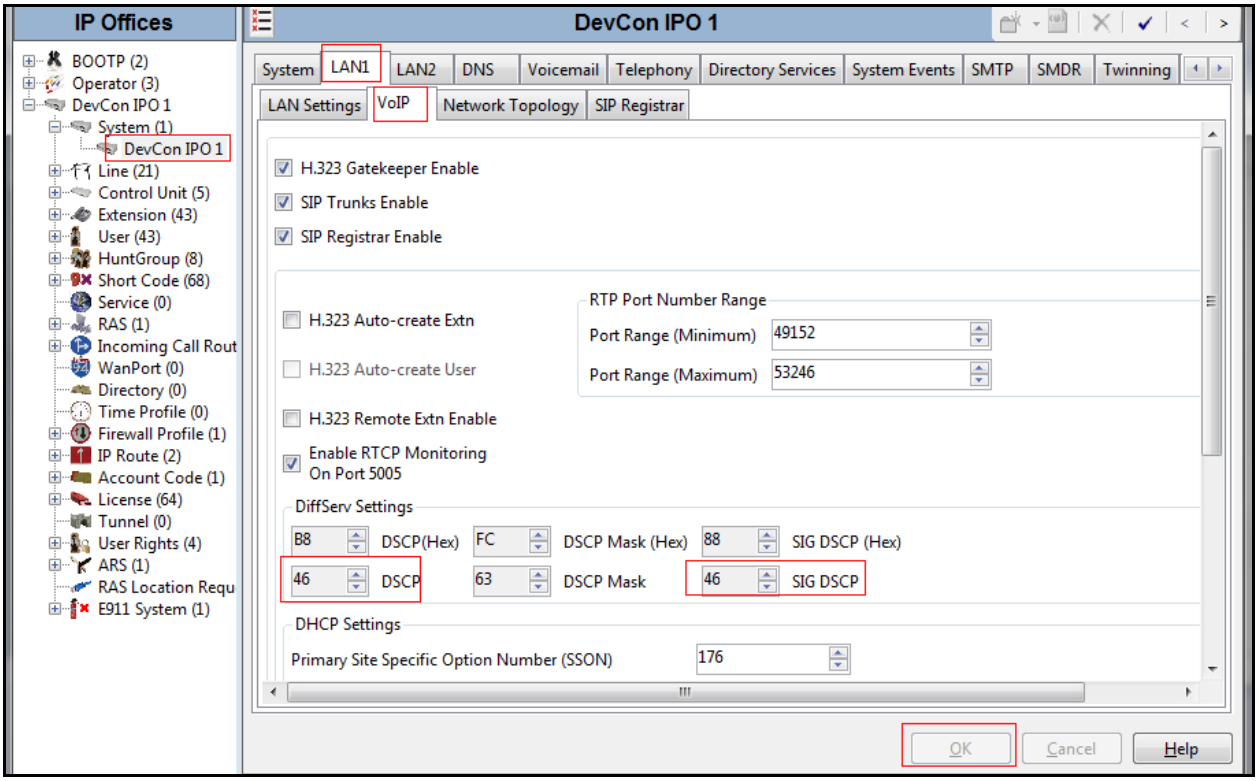
The main IP Office Manager window appears. The following steps refer to the Configuration Tree which is in the left pane of the window and under the heading **IP Offices**.



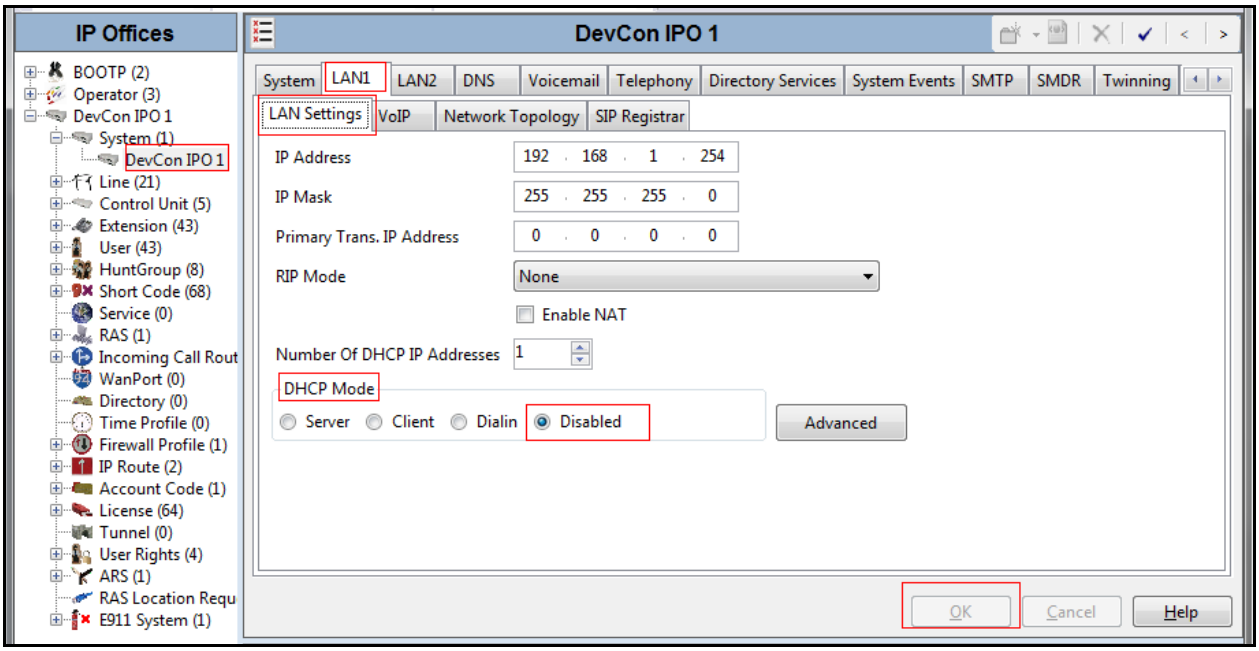
Step 3

Verify VoIP information.

The Avaya IP Telephones will get Differentiated Services information from the Avaya IP Office. In the Manager window, from the Configuration Tree under the **DevCon IPO1**, click **System → DevCon IPO1 → LAN1 → VoIP.** Verify that the **DiffServ Settings** for **DSCP** and **SIG DSCP** are both set to **46**. If they are not **46**, change them and then click **OK** to continue.



Step 4
Disable DHCP server on Avaya IP Office.
From the Configuration Tree, click **System → LAN1 → LAN Settings**. Set the **DHCP Mode** to **Disabled**. Click **OK** to continue.



Step 5
Click on the icon (not shown) in order to save configuration.

5.2. H.323 Extension Configuration

This section displays the basic H.323 Extension configuration. Except where stated, the parameters in all steps are the default settings and are supplied for reference. For all other provisioning information such as provisioning of the trunks, call coverage and voice mail, please refer to the Avaya IP Office product documentation in **Section 10.**

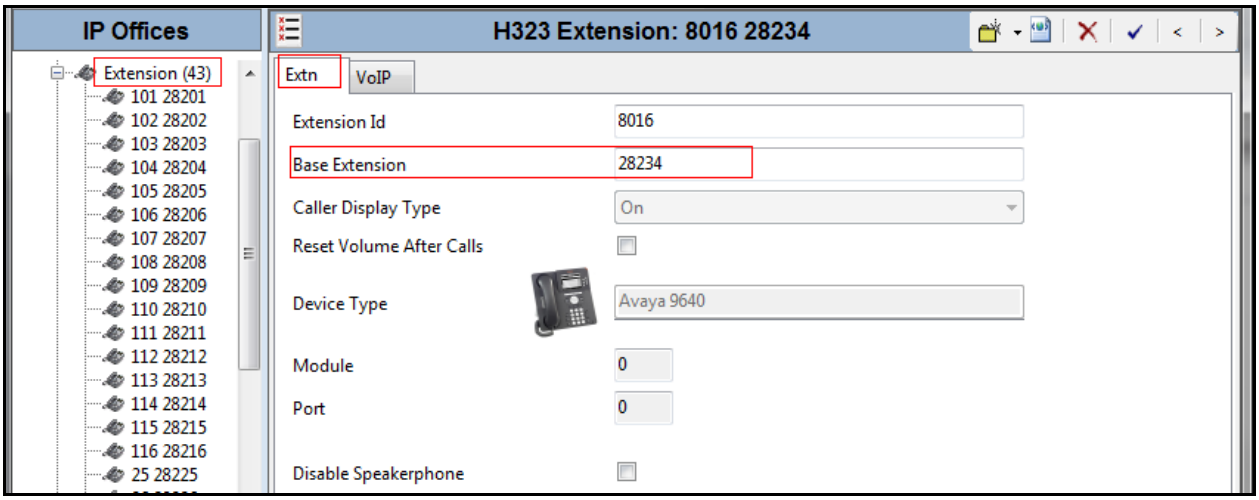
Step 1
Avaya IP Office is configured via the Avaya IP Office Manager program. Log into the Avaya IP Office Manager PC and select **Start → Programs → IP Office → Manager** to launch the Avaya IP Office Manager application. Select **File → Open** to search for IP Offices in the network. Click on appropriate Avaya IP Office. Click **OK** to continue (not shown). Log in to the Avaya IP Office Manager application using the appropriate credentials.

Step 2
The main IP Office Manager window appears. The following steps refer to the Configuration Tree which is in the left pane of the window and under the heading **IP Offices** as shown in **Section 5.1, Step 2**.

Step 3

Create H.323 Extension.

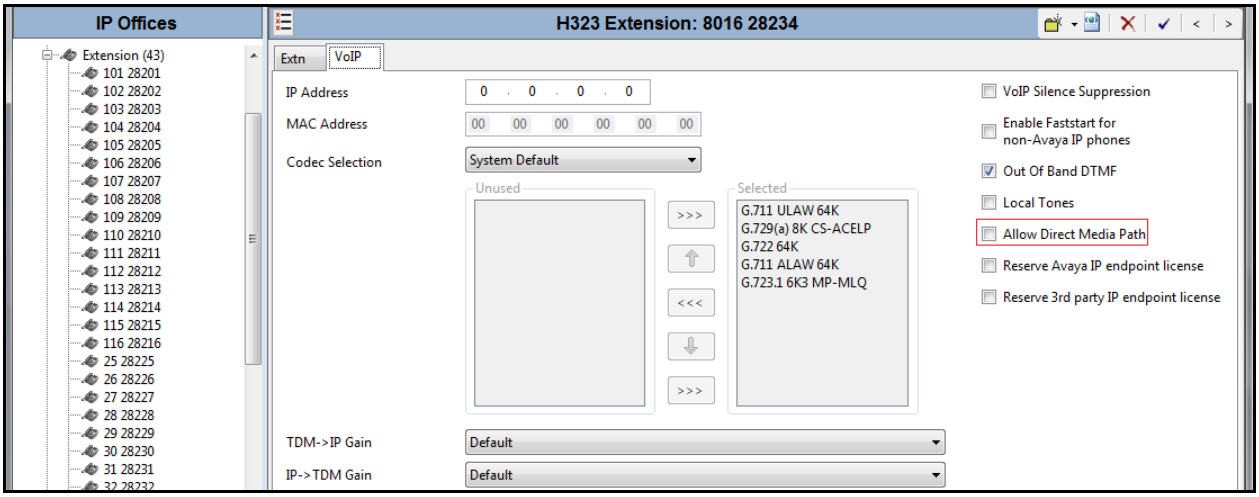
From the Configuration Tree, right mouse click on **Extension** and select **New → H.323 Extension** (not shown). Enter a unique **Base Extension.**



Step 4

Disable Direct Media Path.

Click the **VoIP** tab. Verify that **Allow Direct Media Path** is NOT checked. Click **OK** (not shown) to continue.



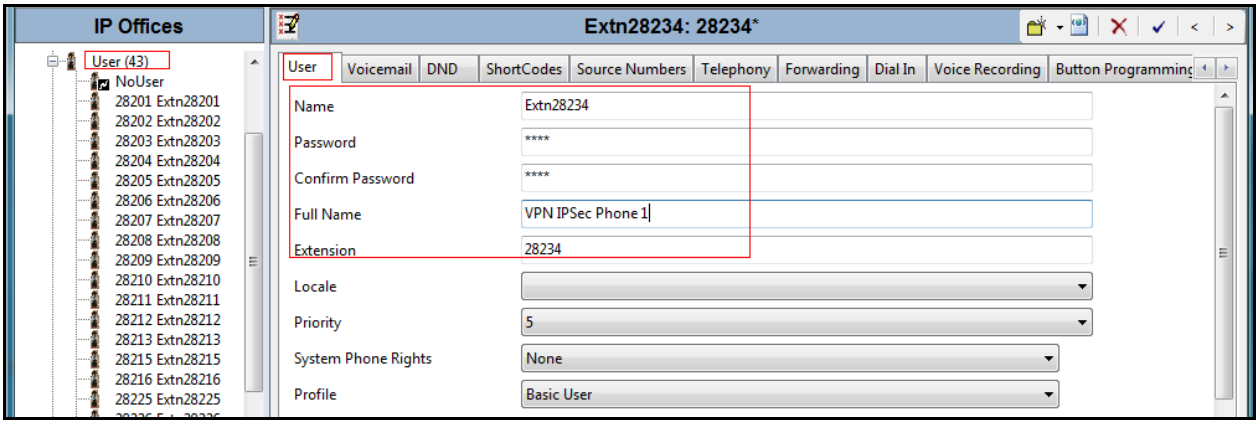
Important Note:

For VPN Extensions, "Allow Direct Media Path" is enabled by default. Remember to disable direct media path by unchecking the check box of "Allow Direct Media Path".

Step 5

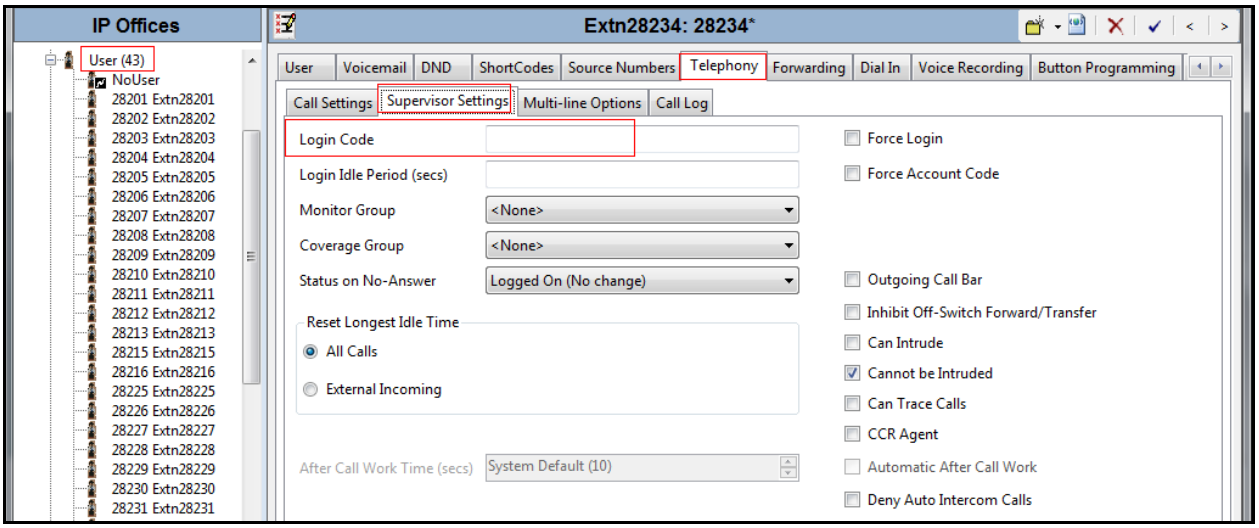
Create User.

From the Configuration Tree, right mouse click on **User** and select **New** (not shown). Enter a user **Name** for the extension that was created in **Step 3**. Enter a **Password** and **Confirm Password** value. Enter the **Extension** that was created in **Step 3**.



Step 6

Click **Telephony** tab and **Supervisor Settings** sub-tab. Enter a **Login Code**. 1234 was used for the compliance testing. The **Login Code** is used by the IP phones to log into the Avaya IP Office**.** Click **OK** (not shown) to continue.



Step 7

Click on the icon (not shown) in order to save the configuration.

Step 8

Repeat **Step 3** through to **Step 7** for additional Extensions.

6. Configure Netgear VPN Firewall SRX5308

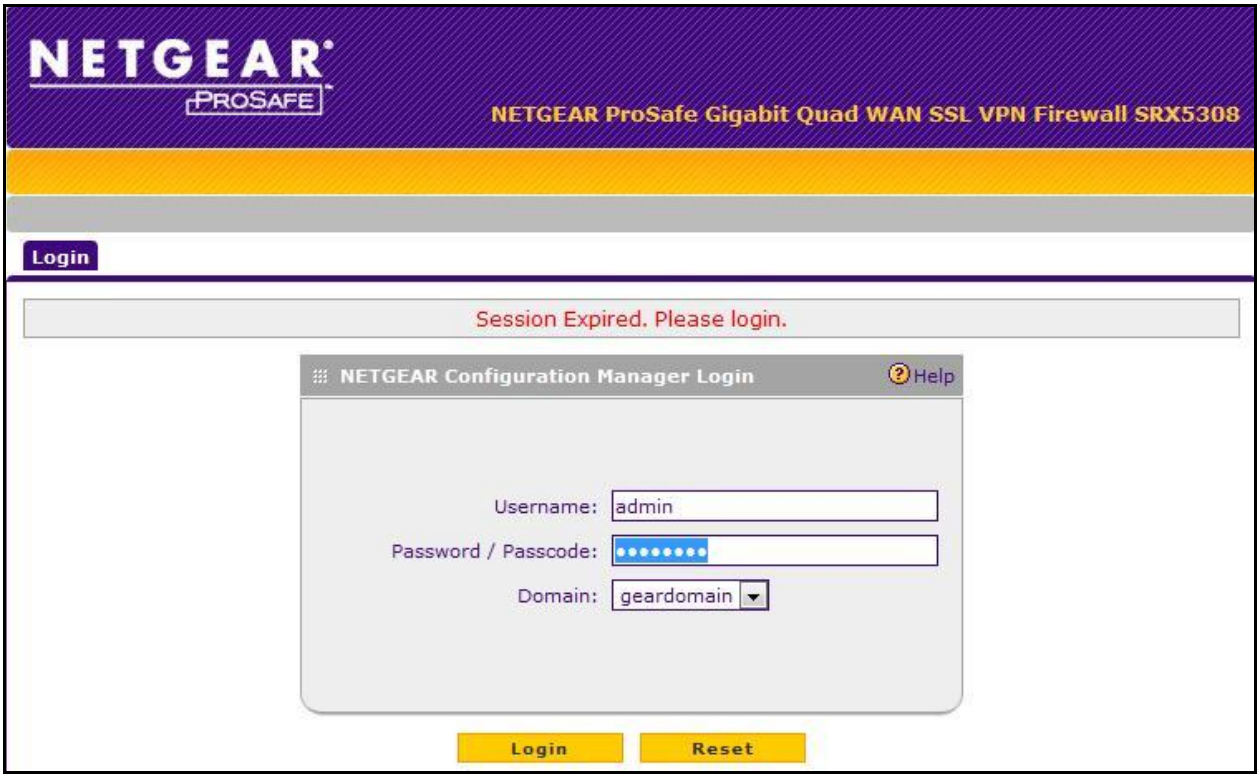
This section describes how to access the Netgear VPN Firewall web interface and configure the VPN for testing.

6.1. Configure WAN Interface

This section shows how to configure the WAN interface to connect to an Internet Service Provider (ISP). This interface will have the public IP address. For the purpose of safety and security, the public IP address is changed to private with 10.xxx.xxx.xxx.

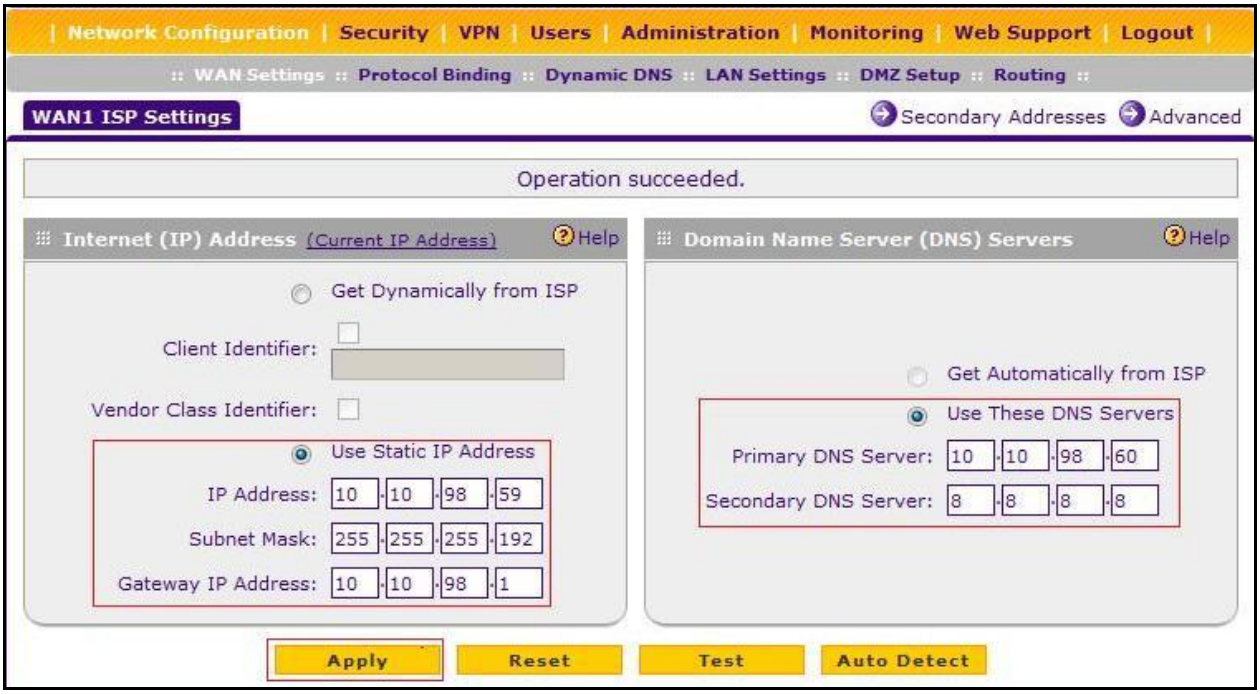
Step 1

Access VPN via web interface by typing *http://192.168.1.1*. Log into the VPN Firewall web interface using their default user name, *admin*, and password, *password*.



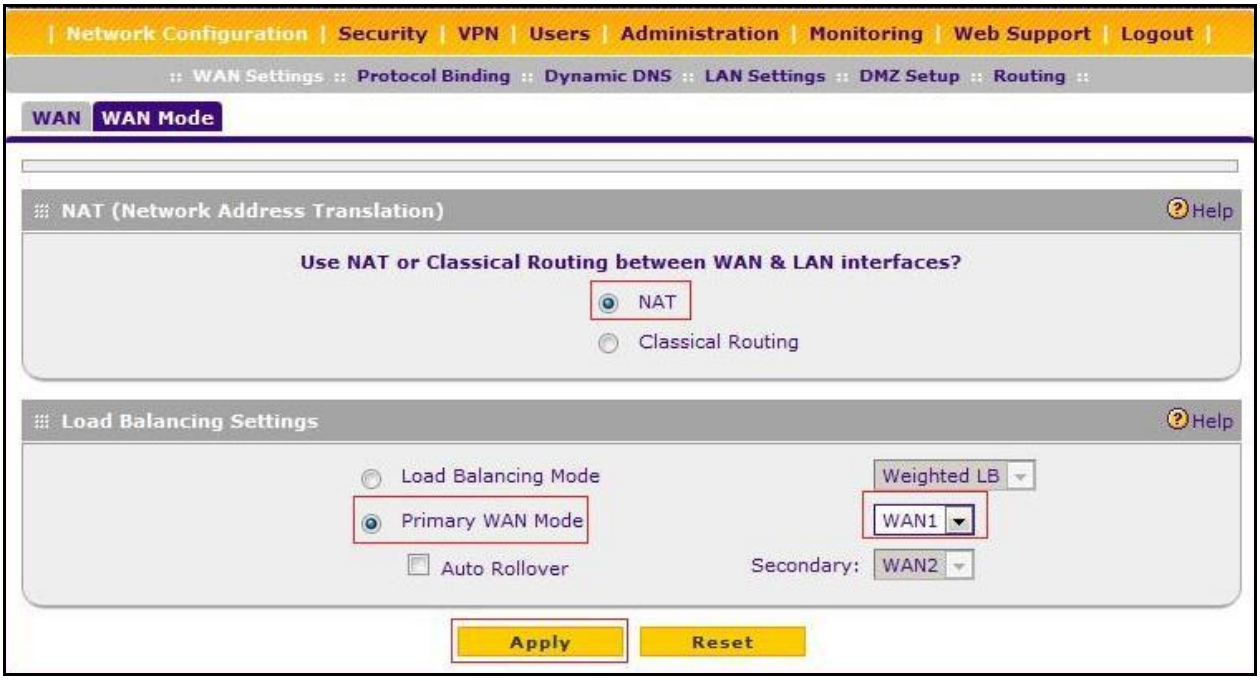
Step 2

Navigate to **Network Configuration → WAN Settings → WAN**. Click **Edit** on the WAN1 interface (not shown). Modify the settings as shown below. Click **Apply**.



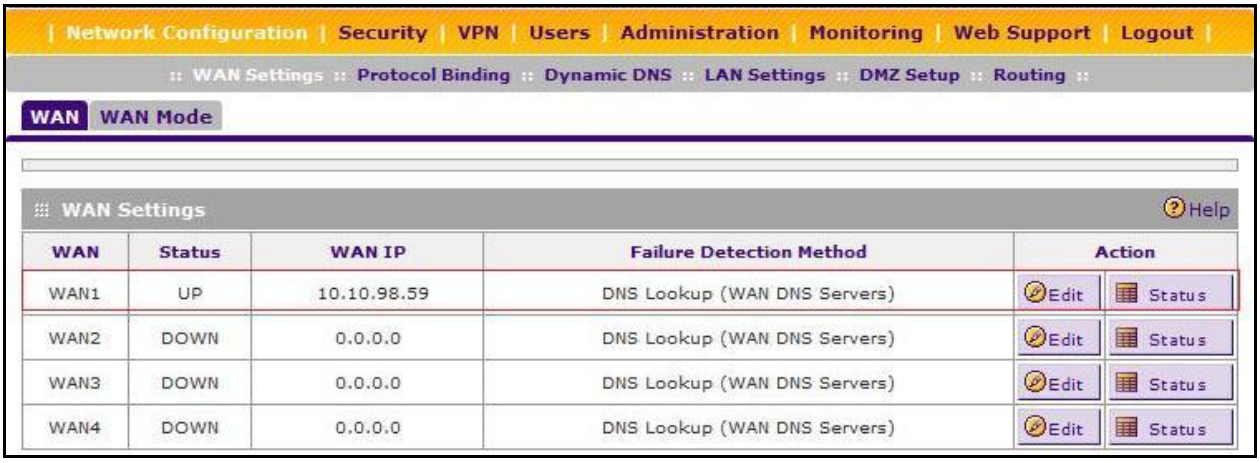
Step 3

From **Network Configuration → WAN Settings → WAN Mode**. Make sure the settings are as shown in the screenshot below. If not, make changes and click **Apply**.



Upon completion of the network configuration, the **WAN1** interface will be like the screenshot below.

Note: Give a few minutes for the connection to be established with the ISP. The status should be *UP* as shown in screenshot below.



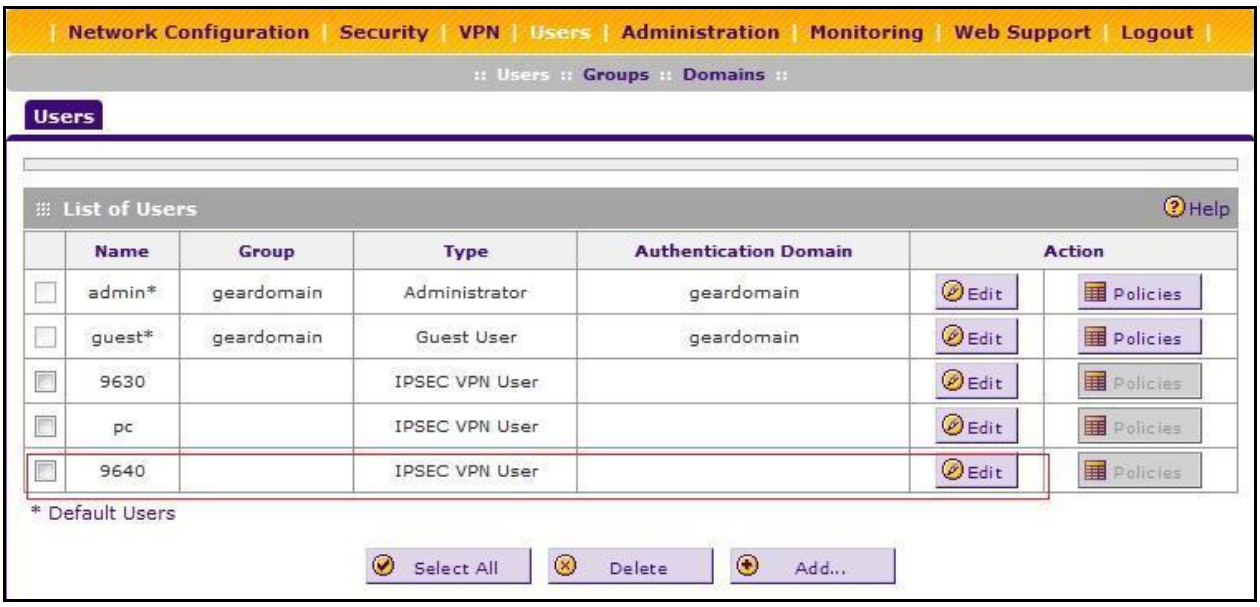
6.2. Configure Users

This section describes how to create users using VPN IPSec tunnel. The users here are the 9600 series IP phones.

Navigate to **Users → Users**, click **Add** button. Enter the user information as shown below and click **Apply**.

- TIP: Using the Serial Number of the IP Phone as the **Username**. Configure the 46vpnsetting.txt file and consider using the [SET NVVPNUSER "SERIALNUM"] option. Assign a common **password** to all users and use the [SET NVVPNPSWD] option.
- Note: Some phone Serial Numbers may contain letters, while others will be all numbers. Letters must be entered in capitals, not lower case or the Router will not accept the username and authentication will fail.

Upon completion of creating new user, a user list is as shown below on the **Users** page.

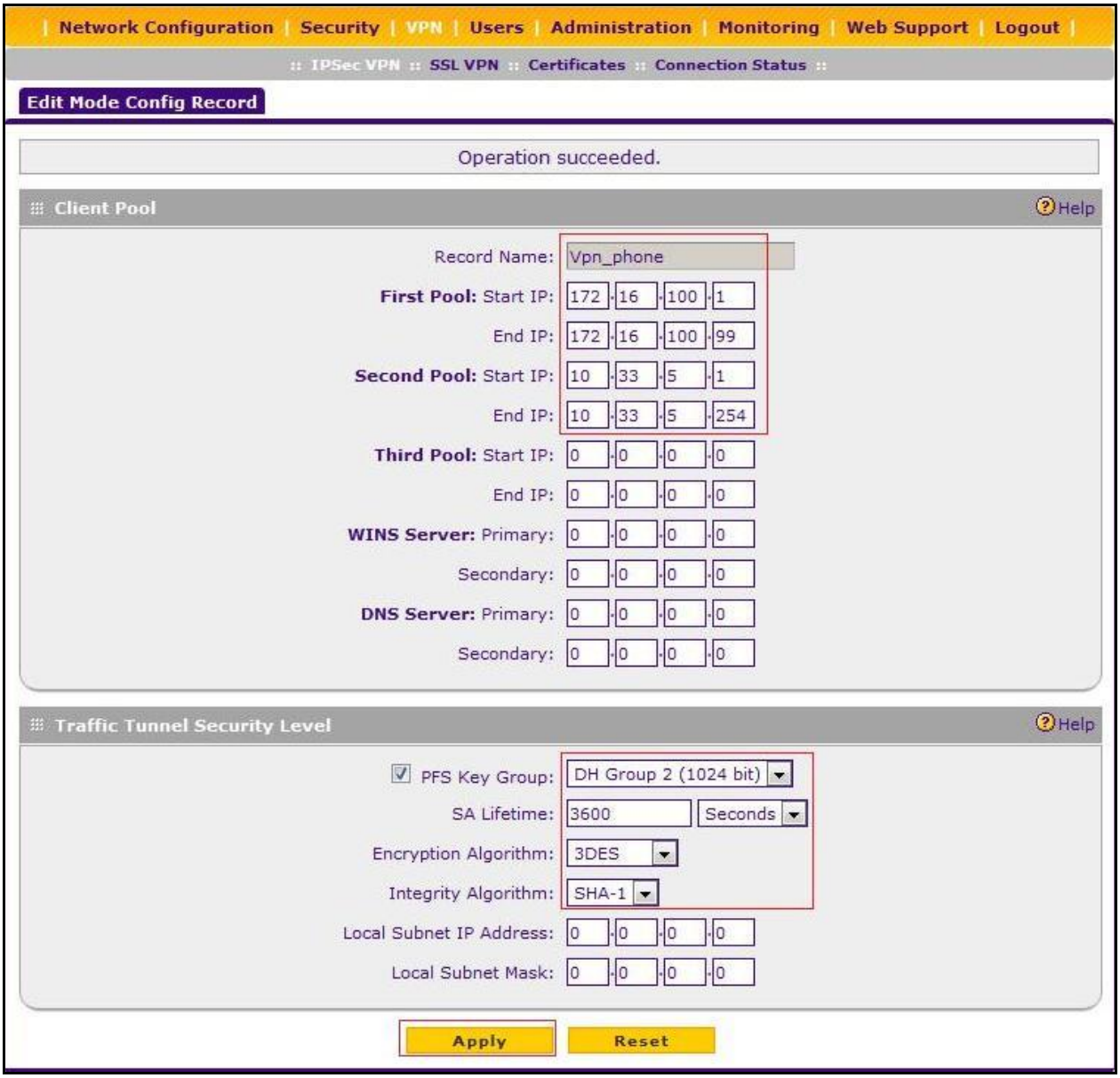


6.3. Configure VPN

This section describes how to configure VPN IPSec tunnel in the Mode Config and X-Auth methods to establish the connection between VPN Firewall server and VPN client, namely Avaya 9600 series IP phones.

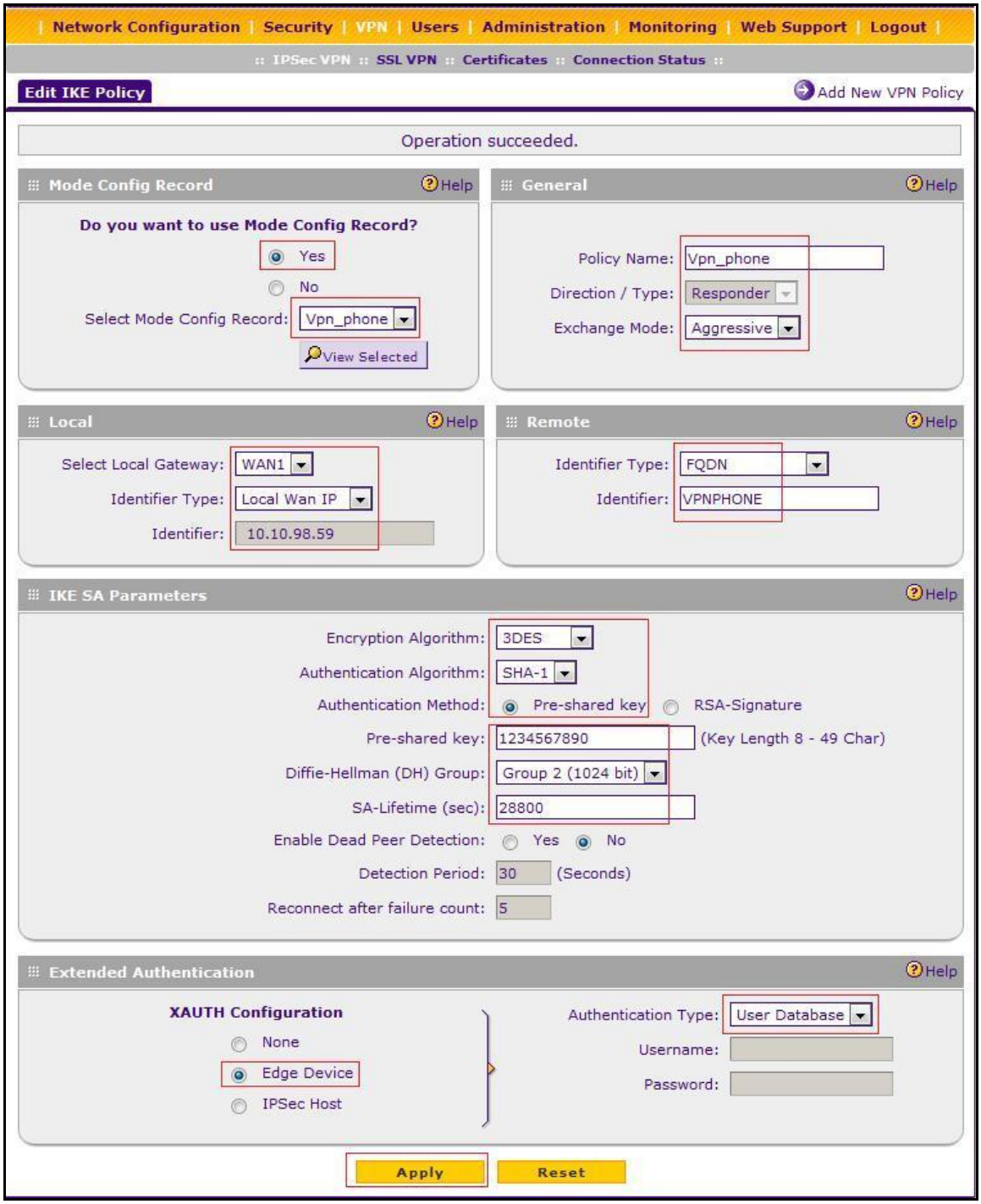
Step 1

Navigate to **VPN → IPSec VPN → Mode Config**. Click **Add** button (not shown). Enter the values as shown in screenshot below:

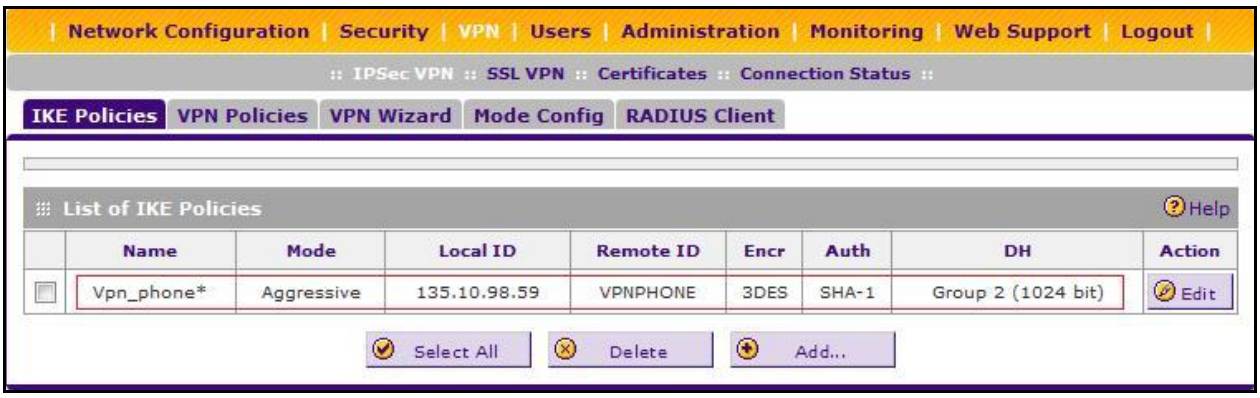


Step 2

Navigate to **VPN → IPSec VPN → IKE Policies**. Click **Add** button (not shown). Enter the values as shown in screenshot below.



Upon completion of IKE policies configuration, the policy list is as shown below in the list of IKE Policies.



7. Configure VPN Client on Avaya 9600 Series IP Phone

This section describes how to configure the 9600 series IP phone in VPN mode as a remote VPN client. For more information, refer to **Section 10**.

7.1. 96xx Series IP Phone Firmware

The Avaya 96xx Series (3.1) VPN-Enabled IP Phone firmware must be installed on the phone prior to the phone being deployed in the remote location. Refer to **Section 10** for details on installing 96xx Series IP Phone firmware. The firmware version of Avaya IP telephones can be identified by viewing the version displayed on the phone upon boot up or when the phone is operational.

Step 1

Press **Mute** Button + PROCPSWD (default 27238) (**Mute + 2-7-2-3-8 + #**) and then press # to enter into the phone configuration mode.
Scroll down to select **View** option.
Scroll down to check the **Application file name** displayed denotes the installed firmware version.

Step 2

As displayed in table of **Section 4,** 96xx Series IP Phone firmware includes **3_1** in the name. Ensure that in the **About Avaya one-X menu** on the phone's display **Application file name** contains **3_1**. This allows for easy identification of firmware versions incorporating VPN capabilities.

7.2. Configure Avaya 96xx Series IP Phone

The Avaya 96xx Series IP Phone configuration can be administered centrally from a HTTP server (IP Office) through the 46xxsettings.txt file or locally on the phone. These Application Notes utilize the local HTTP server (10.10.98.59 is the IP address used in this example) for easy editing/modification of the 46xxsettings.txt file. Refer to **Section 10** for details on a centralized configuration. There are two methods available to access the **VPN Configuration Options** menu from the 96xx Series IP Phone, refer to **Section 10**.

7.2.1. During Telephone Boot

During the 96xx Series IP Phone boot up, "*****" key can be used to enter the configuration mode and is displayed on the telephone screen as shown below.

100 Mbps Ethernet
*** to program**

Step 1
When the ***** key is pressed, it will display **Enter Code**: Press **Mute** Button + PROCPSWD (default 27238) (**Mute + 2-7-2-3-8 + #**) and then press **#** to enter into the phone configuration mode.

Step 2
Go to **ADDR** (Address Procedures) and update it with the below details.

Phones IP Address	0.0.0.0 (Will be assigned from the IP pool configured on the VPN gateway or by the Internal DHCP server if the VPN gateway is configured as DHCP Relay).
Call Servers IP Address	192.168.1.254 (Avaya IP Office IP address).
Router IP Address	0.0.0.0 (Will be assigned by the DHCP server on the Home Gateway).
Subnet Mask	0.0.0.0 (Will be assigned by the DHCP server on the Home Gateway).
HTTP Server	10.10.98.60 (Internal HTTP server IP address in dotted decimal format, which is serving the 46xxsetting.txt file).
Https Server IP Address	A.B.C.D (Internal HTTPS server IP address in dotted decimal format if it's preferred delivering the configuration over HTTPS).
802.1Q	Auto
VLAN ID	0
VLAN Test	60

Step 3
Press **Back** to come out of the **ADDR** procedures. Press **Exit** to come out of craft procedure. The phone is now rebooting. During booting up process, the phone will load and execute the 46xxsettings.txt file from http server (10.10.98.60 in this example). After the boot process is finished, the phone will display "Discover 192.168.1. 254".

Step 4
Enter the craft mode by pressing "**Mute** button + procpswd + #". Scroll down to the last option **VPN**, verify that the VPN mode is Enabled.
Press **Cancel** button to exit VPN procedures. Scroll down to **RESTART PHONE** option and press **Start**. Then press **Restart**.

Step 5
The phone will start the rebooting sequence. It will go through the booting sequence, load firmware and execute the 46xxsettings.txt file again. When complete, it will prompt at "**VPN username**". Enter *9640* as user in this example. Then enter "**VPN password**", enter *1234567890* as password used in this example.
The phone will go through the process of authentication for phase 1 and then building the VPN tunnel. Upon completion, it will register to IP Office server.

7.2.2. Table of sample values for IPSec parameters

The configuration values of one of the 96xx Series IP Phones used in the sample configurations is shown in table below.

VPN Remote Phone Configuration	
VPN Start Mode	Boot
VPN Profile	Juniper with XAuth
VPN Server	10.10.98.59
Username	9640
Password	1234567890
Group Name	VPNPHONE
Group PSK	1234567890
IKE Parameters	
IKE ID Type	FQDN
Diffie Hellman Group	2
Encryption ALG	3DES
Authentication ALG	Sha1
IKE Xchange Mode	Aggressive
IKE Config Mode	Enable
XAUTH	Enable
Cert Expiry Check	Disable
Cert DN Check	Disable
IPSEC Parameters	
Encryption ALG	3DES
Authentication ALG	Sha1
Diffie Hellman Group	2
VPN Password type	1 (Save in Flash)
Protected Nets	
Remote Net #1	192.168.1.0/24
Copy TOS	No

7.3. Sample 46xxsettings.txt File

The **46xxsetting.txt** file stored in the Web Server, contains values used by the Avaya 96xx Series IP Phone during the setup of the IPSec VPN tunnel. The following details the settings used in these Application Notes. Refer to **Section 10** for a detailed explanation of all the fields.

```
## ************************************************
## VPN Start mode
##
## Disable 0
## Enabled 1
## ************************************************
SET NVVPNMODE 1
##
##************************************************
##VPN Vendor
##
## PROFILE_ID_AVAYA_SG 1
## PROFILE_ID_CHECKPOINT 2
## PROFILE_ID_CISCO_PSK_XAUTH 3
## PROFILE_ID_CISCO_HYBRID_XAUTH 4
## PROFILE_ID_JNPR_PSK_XAUTH 5
## PROFILE_ID_GENERIC_PSK 6
## PROFILE_ID_GENERIC_PSK_XAUTH 7
## PROFILE_ID_CISCO_CERT_XAUTH 8
## PROFILE_ID_JNPR_CERT_XAUTH 9
## PROFILE_ID_GENERIC_CERT_XAUTH 10
## PROFILE_ID_NORTEL_CONTIVITY 11
##************************************************
SET NVVPNCFGPROF 5
##
##************************************************
## VPN Server IP
##************************************************
SET NVSGIP 135.10.98.59
##
## ************************************************
## user Id & password
## If left blank, the first time starts the vpn negotiation, the phone will prompt the username and
## password and time and save in memory
## ************************************************
SET NVVPNUSER ""
##
## ************************************************
## Password type
```

##
Save in flash 1
Erase on power-off 2
Numeric OTP 3
Alpha-Numeric OTP 4
PASSWORD_TYPE_ERASE_ON_VPN_TERMINATION 5
**
SET NVVPNPSWDTYPE 1
##
**
Group name / ike id
**
SET NVIKEID "VPNPHONE"
##
**
Group PSK
**
SET NVIKEPSK "1234567890"
##
**
IKE ID Type
##
IP-Address 1
FQDN 2
USER-FQDN 3
DER-ASN 9
KEY-ID 11
**
SET NVIKEIDTYPE 2
##
**
IKE DH group set
DH Group 1 1
DH Group 2 2
DH Group 5 5
DH Group 14 14
DH Group 15 15
DH Group Detect 254
**
SET NVIKEDHGRP 2
##
**
IKE Encryption Algorithm
##
ANY 0
AES-128 1

3DES 2
DES 3
AES-192 4
AES-256 5
****
SET NVIKEP1ENCALG 2
##
##********
Specifies the authentication algorithm to use during IKE Phase 1 negotiation.
1 ASCII numeric digit. Validvalues are:
0 = Any
1 = MD5 (per RFC 2403)
2 = SHA (per RFC 2404)
##********
SET NVIKEP1AUTHALG 2
##
****
Ike exchange mode
##
Aggressive 1
Main mode 2
****
SET NVIKEXCHGMODE 1
##
##********
Specifies whether to disable XAUTH user authentication for profiles that enable XAUTH by
default. 1 ASCII numeric digit. Valid values are:
1= XAUTH user authentication enabled
2 = XAUTH user authentication disabled
##********
SET NVXAUTH 1
##
****
IKE config mode
##
Enabled 1
Disabled 2
****
SET NVIKECONFIGMODE 1
##
****
IPsec Encryption Algorithm
##
ANY 0
AES-128 1
3DES 2

DES 3
AES-192 4
AES-256 5
****
SET NVIKEP2ENCALG 2
##
****
IPsec Authentication Algorithm
##
ANY 0
MD5 1
SHA1 2
****
SET NVIKEP2AUTHALG 2
##
****
IPsec DH group set
##
DH Group 1 1
DH Group 2 2
DH Group 5 5
DH Group 14 14
DH Group 15 15
DH Group Detect 254
****
SET NVPFSDHGRP 2
##
****
Encapsulation
##
4500-4500 0
Disable 1
2070-500 2
RFC 4
****
SET NVVPNENCAPS 0
##
****
Copy TOS
##
YES 1
NO 2
****
SET NVVPNCOPYTOS 2
##
##

****
VPNPROC
Valid Values: 1 ASCII numeric digit,“0”,“1” or “2”
Description: Specifies whether VPNCODE can be used
to access the VPN procedure at all, in
view-only mode, or in view/modify mode
****
SET VPNPROC 2
##
##********
Specifies IP address ranges that will use the VPN tunnel. 0 to 255 ASCII characters: zero or
more dotted decimal IP address/integer strings, separated by commas without any intervening
spaces.
##**********
SET NVIPSECSUBNET 192.168.1.0/24
##
****
IKE over TCP
##
IKE_OVER_TCP_NEVER 0
IKE_OVER_TCP_AUTO 1
IKE_OVER_TCP_ALWAYS 2
****
SET NVIKEOVERTCP 0

8. Verification and Troubleshooting Tips

This section offers some common configuration mismatches between the 96xx series IP phone and Netgear VPN Firewall to assist in troubleshooting. The key events of the logs are highlighted in bold. Netgear VPN Firewall log messages can be accessed through the Monitoring and VPN Connection Status on the VPN Firewall itself.

8.1. IKE Phase 1 no response

If the given IKE parameters are incorrect, we will get a VPN Tunnel Failure message.

VPN tunnel failure		
Retry	Details	Sleep

By pressing the **Retry** key, it will attempt to re-establish the tunnel again. If the **Details** key is pressed, the phone display shows the IKE Phase 1 response.

IKE Phase 1 no response		
Restart	Program	Back

If the **Program** key is pressed, it will redirect to the Craft Code screen.

Enter Code:
#=OK

Given the correct Craft Code, it will redirect to **Craft Procedures** screen. From here select **VPN** and press the **Start** key. Press forward soft key on the phone and check the IKE Exchange mode, check **IKE Phase1** parameters on VPN gateway and phone is correct.

8.2. Incorrect IKE Phase 2

If we have given incorrect IKE Phase 2 settings, then we will get a VPN Tunnel Failure message.

VPN tunnel failure		
Retry	Details	Sleep

If we press the **Retry** key, it will attempt to re-establish the tunnel again. If we press the **Details** key, we can see **Invalid configuration** screen.

Invalid configuration		
Restart	Program	Back

If we press the **Program** key, it will redirect to Craft Code screen.

Enter Code: #=OK

Given the correct Craft Code, it will redirect to **Local configuration Procedures** screen. From here select **VPN** and press **Start** key. Press forward soft key on the phone and it will go to IKE Phase 2 screen, check that the **IKE Phase2** parameters are correct or not.

8.3. Invalid Username, password

Re-enter the correct VPN Username (as configured in the user database) and correct VPN user password.

8.4. Invalid IKEID and PSK

Go to the local procedure configuration page (using details **Softkey → program → procpswd**) on the phone and re-enter the correct (configured on the Netgear Firewall) group name and group password.

8.5. Phone displaying "connecting…"

This issue can be resolved by the administrators who have access to the core network infrastructure and Netgear Firewall. Ensure that the core network infrastructure knows how to route the address in the IP Pool to the Netgear Firewall.

8.6. "Need IKE ID/PSK" Message

Go to the local VPN configuration page and configure **IKE ID** and **PSK** as configured on the Netgear Firewall.

8.7. No gateway address

Go to the local procedures configuration page (using details **Softkey → program → Procpswd → ADDR) Enter the valid Gateway** address.

9. Conclusion

These Application Notes illustrate the procedures necessary for configuring the Netgear VPN Firewall to establish VPN IPSec tunnel with VPN enabled Avaya 9600 series IP phones. Additionally these Application Notes also cover the configuration of Avaya IP Office to establish calls with VPN enabled 9600 series IP phones (see **Section 5**).

10. Additional References

This section references documentation relevant to these Application Notes.

[1] Product documentation for the Avaya may be found at:
https://support.avaya.com/css/Products/

For IP Office 8.1, refer to https://support.avaya.com/search-landing/?query=ip office 8.1
VPN Setup Guide for 9600 Series IP Telephones Release 3.1, Nov. 09, Issue 1, Document Number 16-602968.
Avaya one-X™ Deskphone Edition for 9600 Series IP Telephones Administrator Guide Release 3.1, Nov. 09, Issue 07, Document Number 16-300698.

[2] Netgear's technical documentation for Netgear Prosafe Quad WAN Gigabit SSL VPN Firewall SRX5308 is available at:
http://www.netgear.com/business/products/security/wired-vpn-firewalls/srx5308.aspx#

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya Solution & Interoperability Test Lab at interoplabnotes@list.avaya.com