Avaya Solution & Interoperability Test Lab

Configuring an IPSec VPN Tunnel between Avaya 96xx Series IP Telephones and a Cisco 2811 ISR Router – Issue 1.0

Abstract

These Application Notes present a sample configuration for a remote user with an Avaya 96xx Series Telephone connected to a Cisco 2811 Intergraded Service Router at a main office via an IPSec VPN tunnel. For the sample configuration, the Avaya 96xx Series IP Telephones registered with Avaya Aura™ Communication Manager 5.2 after establishing the IPSec VPN tunnel.

Table of Contents

1. Introduction

These Application Notes describe the steps to configure the Cisco Integrated Service Router (ISR) to support IPSec VPN (Virtual Private Network) tunnel termination using XAuth (eXtended Authentication) and local credential authentication for Avaya 96xx Series IP Telephones. The Avaya 96xx Series IP Telephones have a software based IPSec Virtual Private Network (VPN) client integrated into the firmware. This capability allows Avaya IP Telephones 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 as if they were using the telephone in the office. Avaya IP telephone models supporting the Avaya 96xx Series IP Telephone VPN firmware include the 9620, 9620C, 9620L, 9630, 9640, 9650, 9650C and 9670.

Note: Avaya 9610 does not support VPN.

Release 3.1 of the Avaya 96xx Series IP Telephone firmware, used in these Application Notes, extends the support of VPN gateways to include Cisco ISR family with the proper IPSec features enabled. The configuration steps described in these Application Notes utilize a Cisco ISR 2811. The sample network implemented in these Application Notes is shown in **Figure 1.**

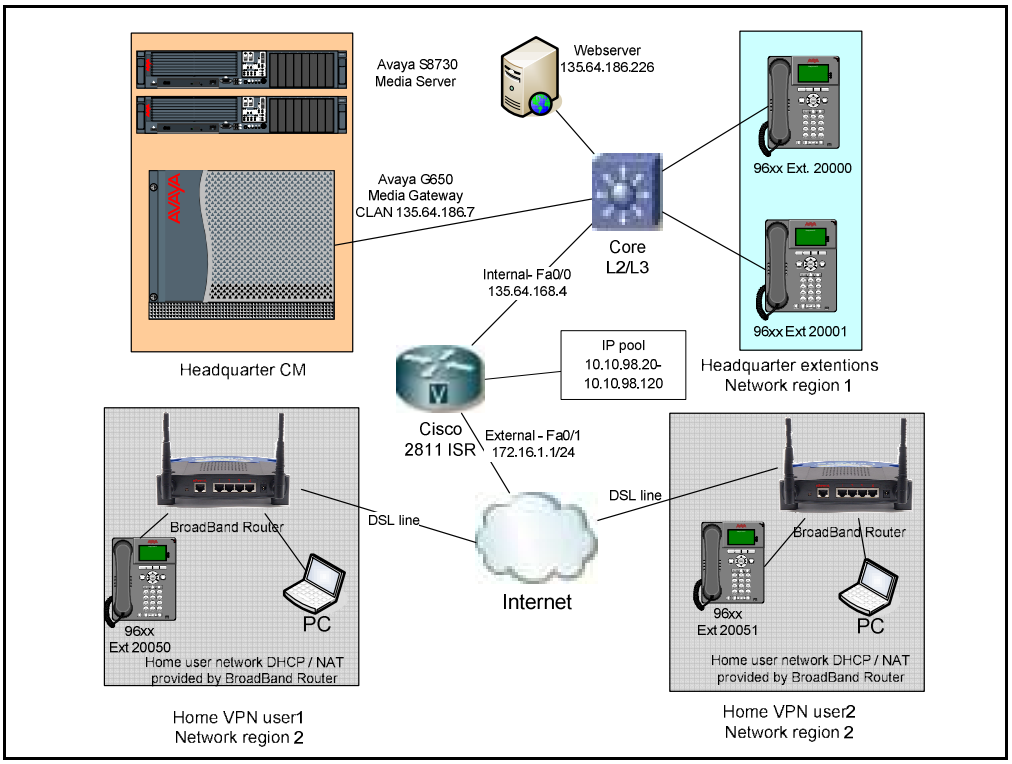


Figure 1 – Test Configuration used in these Application Notes

The Headquarter location contains the Cisco ISR functioning as VPN head-end. Avaya Aura™ Communication Manager and a Web server (Phone Configuration File Server) are located in the same datacenter.

The Avaya 96xx Series IP Telephones are located in public network and configured to establish an IPSec tunnel to the External (Fa0/1) IP address of the Cisco ISR. Upon successful authentication of the user, the Cisco ISR assigns IP addresses from a specified IP pool. The assigned IP addresses also known as the inner addresses will be used by the Avaya 96xx Series IP Telephones when communicating inside the IPSec tunnel and the corporate network to Avaya Aura™ Communication Manager. Once the IPSec tunnel is established, the Avaya 96xx Series Telephones, access the Web server to retrieve its configuration and then initiate H323 registration with Avaya Aura™ Communication Manager.
Communication Manager runs on an Avaya S8730 Server with Avaya G650 Media Gateway. The results in these Application Notes are applicable to other Communication Manager Server and Media Gateway combinations. In regards to the Cisco ISR configuration presented, these should work on different models as long as they provide the same feature set. Please consult with the vendor.

2. Equipment and Software Validated

The following equipment and software were used for the sample configuration provided:

Product / Hardware Platform	Version
Avaya IP Telephones (9620, 9630, 9640, 9650 &9670)	R3.1
Avaya S8730 Media Server	Avaya Aura™ Communication Manager 5.2.1
Avaya G650 Media Gateway	• TN2312BP HW15 FW049 • TN2602AP HW08 FW049 • TN799DP HW01 FW034
Cisco ISR 2811	c2800nm-adventerprisek9_ivs-mz.124-24.T.bin
Cisco VPN Client	Version 5.0.06.0110

Table 1 - Software/Hardware Version Information

3. Configure Avaya Aura™ Communication Manager

This section provides the procedures for configuring Communication Manager on the following areas:

- IP Codec Sets Configuration
- IP Network Map Configuration
- IP Network Region Configuration
- Adding station for the remote user

These instructions assume that the Communication Manager has been installed, configured, licensed and provided with a functional dial plan. Refer to **[3]** for more details**.** Throughout this section the administration of Communication Manager is performed using a System Access Terminal (SAT). The commands are entered on the system with the appropriate administrative permissions. Some administration screens have been abbreviated for clarity. The Avaya 96xx Series IP Telephones with VPN are assigned to IP Network region 2 using the IP address range of the VPN Client IP address pool defined on Cisco ISR. In order to save bandwidth and improve the user experience in the remote location, the G.729 codec is assigned to IP Network Region 2 for calls within this region and with IP Network Region 1.

3.1. IP Codec Sets Configuration

Use the **change ip-codec-set n** command to configure IP Codec Set paramentes where **n** is the IP Codec Set number. In these Application Notes **codec-set 1** was used for the **Headquarter** network and **codec-set 4** for the remote user's telephones. In order to configure the codec set for the headquarter network region, use the command **change ip-codec-set n** command, where **n** is codec set used in the configuration. Enter the following values:

- **Audio Codec** set for **G.711MU**.
- **Silence Suppression**: Retain the default value **n.**
- **Frames Per Pkt:** Enter **2**.
- **Packet Size (ms):** Enter **20**.

Retain the default values for the remaining fields, and submit these changes.

```
change ip-codec-set 1                                        Page   1 of   2
                          IP Codec Set

    Codec Set: 1

    Audio         Silence      Frames   Packet
    Codec         Suppression  Per Pkt  Size(ms)
 1: G.711MU            n          2        20
 2:
```

For the Avaya 96xx Series IP Telephones a different codec set is used. Use the command **change ip-codec-set n** command, where **n** is codec set used in the configuration. Enter the following values:

- **Audio Codec:** set for **G.729** needed to support 96xx Series IP Telephones with VPN
- **Silence Suppression:** Retain the default value **n.**
- **Frames Per Pkt:** Enter **3**.
- **Packet Size (ms):** Enter **30**

The following screenshot shows the configuration of **ip-codec-set 4** for the VPN users and telephones.

```
change ip-codec-set 4                                          Page   1 of   2

                           IP Codec Set

    Codec Set: 4

    Audio          Silence      Frames   Packet
    Codec          Suppression  Per Pkt  Size(ms)
 1: G.729               n          3        30
 2:
```

Use **list ip-codec-set** command to verify the codec assignments, as shown in the following screen capture.

```
list ip-codec-set

                                IP CODEC SETS

Codec  Codec 1     Codec 2     Codec 3     Codec 4     Codec 5
Set

  1    G.711MU
  2
  3
  4    G.729
```

3.2. IP Network Map Configuration

Use **change ip-network-map** command to define the IP address to Network Region mapping for Avaya 96xx Series IP Telephones. The IP address range will be the same as configured on the IP pool in the Cisco ISR for the VPN clients. Enter the following values:

- **FROM:** the beginning of the address range (here **10.10.98.20**)
- **To:** the end of the address range (here **10.10.98.120**)
- **Network Region:** the IP Network region used by 96xx Series IP Telephones with VPN Telephones (**2** in these notes)
- **Subnet Bits:** Equivalent to netmask (in this example **24**)

The following screenshot represents the association of the Cisco ISR IP Pool to the VPN users.

```
change ip-network-map                                          Page   1 of  63
                              IP ADDRESS MAPPING

                                                 Subnet Network     Emergency
IP Address                                       Bits   Region VLAN Location Ext
----------------------------------------- ------ ------ ---- -------------
 FROM: 10.10.98.20                                /24    2      n
   TO: 10.10.98.120
 FROM:                                            /             n
   TO:
```

3.3. Configure IP Network Region

Use the **change ip-network-region n**, where **n** is the number of the network region used and set the **Intra-region IP-IP Direct Audio**, and **Inter-region IP-IP Direct Audio** fields to **yes**. For the **Codec Set** enter the corresponding audio codec set configured in **Section 3.1**. Retain the default values for the remaining fields, and submit these changes.

Note: In the test configuration, **IP Network Region 1** was used. If you are creating a new network region or modifying another one, ensure to configure it with the correct parameters.

```
change ip-network-region 1                              Page   1 of  19
                             IP NETWORK REGION
  Region: 1
Location: 1       Authoritative Domain: avaya.com
    Name: Headquarter
MEDIA PARAMETERS                 Intra-region IP-IP Direct Audio: yes
      Codec Set: 1               Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                        IP Audio Hairpinning? n
   UDP Port Max: 3329
```

Repeat the configuration for the IP Network Region assigned to the remote 96xx Series IP Telephones. In these Application Notes, **IP network region 2** was assigned for the purpose.

```
change ip-network-region 2                              Page   1 of  19
                              IP NETWORK REGION
  Region: 2
Location: 1       Authoritative Domain: avaya.com
    Name: HomeUsers
MEDIA PARAMETERS                 Intra-region IP-IP Direct Audio: yes
      Codec Set: 4               Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                        IP Audio Hairpinning? n
   UDP Port Max: 3329
```

Navigate to **Page 3** and ensure that the **codec set 4** defined previously, is used when connecting calls to **dst region 1** and **2**.

```
change ip-network-region 2                              Page   3 of  19

Source Region: 2     Inter Network Region Connection Management     I       M
                                                                   G  A    e
dst codec direct   WAN-BW-limits   Video      Intervening      Dyn  A  G    a
rgn  set   WAN  Units    Total Norm  Prio Shr Regions          CAC  R  L    s
 1    4     y    NoLimit                                          n all
 2    4                                                          all
```

3.4. Adding station for remote user

An Avaya 96xx Series IP Telephone with the VPN feature enabled is administered similar to other IP telephones within Communication Manager. The following screens shows extension 20050 for an Avaya 9640 Telephone being added to the system using the command **add station 20050.** Enter the following values:

- **Type:** <select between **9620, 9630, 9640** or **9650** >
- **IP SoftPhone?** **y** (if required for the home user)
- **Name:** Name for the extension (in this example **Test 20050**)
- **Security Code:** A security code (in this example **1234**)

```
add station 20050                                    Page   1 of   5
                                    STATION

Extension: 20050                      Lock Messages? n              BCC: 0
     Type: 9640                       Security Code: 1234            TN: 1
     Port: S00054                     Coverage Path 1: 1              COR: 1
     Name: Test 20050                 Coverage Path 2:                COS: 1
                                      Hunt-to Station:
STATION OPTIONS
                                          Time of Day Lock Table:
             Loss Group: 19         Personalized Ringing Pattern: 1
                                           Message Lamp Ext: 20050
           Speakerphone: 2-way           Mute Button Enabled? y
        Display Language: english             Button Modules: 0
 Survivable GK Node Name:
          Survivable COR: internal          Media Complex Ext:
   Survivable Trunk Dest? y                      IP SoftPhone? y

                                         IP Video Softphone? n
                                        Customizable Labels? Y
```

In the next page, enable media shuffling by selecting

- **Direct IP-IP Audio Connection? y**

.

```
display station 20050                                          Page   2 of   5
                                    STATION
FEATURE OPTIONS
           LWC Reception: spe              Auto Select Any Idle Appearance? n
          LWC Activation? y                          Coverage Msg Retrieval? y
  LWC Log External Calls? n                                   Auto Answer:
none
              CDR Privacy? n                                Data Restriction? n
   Redirect Notification? y                     Idle Appearance Preference? n
 Per Button Ring Control? n                   Bridged Idle Line Preference? n
   Bridged Call Alerting? n                       Restrict Last Appearance? y
  Active Station Ringing: single
                                                          EMU Login Allowed? n
        H.320 Conversion? n          Per Station CPN - Send Calling Number? y
       Service Link Mode: as-needed                      EC500 State: disabled
         Multimedia Mode: enhanced
    MWI Served User Type: sip-adjunct           Display Client Redirection? n
                                               Select Last Used Appearance? n
                                                 Coverage After Forwarding? s
                                                   Multimedia Early Answer? n
Remote Softphone Emergency Calls:as-on-local Direct IP-IP Audio Connections?y
Emergency Location Ext: 20050         Always Use? n IP Audio Hairpinning? n
```

3.5. Save Translations

Configuration of Communication Manager is complete. Use the **save translations** command to save these changes.

4. Avaya 96xx Series IP Telephone Configuration

4.1. 96xx Series IP Telephone Firmware

The Avaya 96xx Series (3.1) VPN-Enabled IP Telephone firmware must be installed on the telephone prior to the telephone being deployed in the remote location. Refer to **[2]** for details on installing 96xx Series IP Telephone firmware. The firmware version of Avaya IP telephones can be identified by viewing the version displayed on the telephone upon boot up or when the phone is operational by selecting the **Options** hard button ⇨ **View IP** ⇨ **Settings** ⇨ soft button **Miscellaneous** ⇨ soft button ⇨ **Right arrow** hard button. The **Application file name** displayed denotes the installed firmware version. As displayed in **Table 1**, 96xx Series IP Telephone firmware includes **3_1** in the name. Ensure that in the **About Avaya one-X menu** on the telephone's display **Application file name** contains **3_1**. This allows for easy identification of firmware versions incorporating VPN capabilities.

4.2. Configuring Avaya 96xx Series IP Telephones

The Avaya 96xx Series IP Telephone configuration can be administered centrally from an HTTP server through the 46xxsettings.txt file (mentioned in **Section 5.3**) or locally on the phone. These Application Notes utilize the local phone configuration method. Refer to **[1]** and **[2]** for details on a centralized configuration. There are two methods available to access the **VPN Configuration Options** menu from the 96xx Series IP Telephones.

4.2.1. During Telephone Boot

During the 96xx Series IP Telephone boot up, the "*****" key can be used to enter the Configuration mode as shown below.

(Please note that the "*****" key can also be used to enter the configuration mode before the tunnel building procedures are complete). 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. 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	135.64.186.7 (Avaya Communication Manager 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	135.64.186.226 (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

Table 2 - Settings on Avaya 96xx Series telephones

Press **Exit** to come out of the **ADDR** procedures. Scroll down to the last option: VPN. Note that the VPN configuration parameters will not be edited until the value of **VPNPROC** parameter is set to 2. (To do this open the upload directory of the file server, open the file 46xxsettings.txt file and add **SET VPNPROC 2** and upload this new 46xxsettings.txt file into the Avaya 96xx Series IP Telephone). It is recommended to set the value of VPNPROC to 2 while uploading the VPN enabled binary into the telephone. Use Right Navigation key to go to the next screen options. (Note that the values will not be saved until the Right-Navigation key is pressed even if **Save button is pressed**). The External addresses will be reflected only after rebooting the telephone.

The configuration values of one of the 96xx Series IP Telephones used in the sample configurations are shown in **Table 3** below.

No.	Option	Value
1	VPN :	Enabled
2	VPN Vendor:	Cisco
3	Gateway Address:	172.16.1.1 ("External" interface IP address of VPN gateway)
4	External Router:	0.0.0.0 (Or provided by dhcp from home Network).
5	External Telephone IP Address:	0.0.0.0 (Or Same as above).
6	External Subnet Mask:	0.0.0.0 (Or Same as above).
7	External DNS Server:	(Provided by Service provider).
8	Encapsulation :	4500-4500
9	Copy TOS:	No
10	Auth. Type:	PSK with XAUTH
11	VPN User Type:	Any
12	VPN User:	(VPN username i.e. testphone2 as per our notes)
13	Password Type:	Save in Flash
14	User Password:	****** (i.e. Remote password i.e. vpnpass as per our notes).
15	IKE ID (Group Name):	(Group name i.e. groupauthor as per our notes).
16	Pre-Shared Key (PSK)	********* (The preshared key defined in the gateway, vpnvpn as per our notes).
17	IKE ID Type:	KEY_ID
18	IKE Xchg Mode:	Aggressive.
19	IKE DH Group:	2
20	IKE Encryption Alg:	Any
21	IKE Auth. Alg. :	Any
22	IKE Config. Mode:	Enabled
23	IPsec PFS DH Group:	2
24	IPsec Encryption Alg:	Any
25	IPsec Auth. Alg.:	Any
26	Protected Network:	0.0.0.0/0
27	IKE Over TCP:	Never

Table 3 - VPN settings

4.2.2. Telephone is operational in VPN enabled Mode.

Press "**Mute** button + **PROCPSWD** + #" to enter the craft procedures and follow the above steps to program the VPN enabled telephone.

4.3. Sample 46xxsettings.txt file

The **46xxsetting.txt** file stored in the Web Server contains the configuration used by the Avaya 96xx Series IP Telephone during the setup of the IPSec VPN tunnel. The following listing details the settings used in these Application Notes. Refer to **[1]** for a detailed explanation of all the fields.

```
## ************************************************
## The Clan or the Proc interface used for phone
## registration
## ************************************************
SET MCIPADD 135.64.186.7

## ************************************************
## 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  3

## ************************************************
## VPN server
## The "external" interface of Cisco ISR 2811
## ************************************************
SET NVSGIP "172.16.1.1"

## ************************************************
## Encapsulation
##
## 4500-4500            0
## Disable              1
## 2070-500             2
## RFC                  4
## ************************************************
SET NVVPNENCAPS 0

## ************************************************
```

```
## Copy TOS
##
## YES                  1
## NO                   2
## ***********************************************
SET NVVPNCOPYTOS 2

##***********************************************
## User Type
## Any                  1
## 1 User               2
##***********************************************
SET NVVPNUSERTYPE 1

## ***********************************************
## 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 "testphone2"

## ***********************************************
## 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 "groupauthor"

## ***********************************************
## Group PSK
## ***********************************************
SET NVIKEPSK "vpnvpn"

## ***********************************************
## IKE ID Type
##
## IP-Address                 1
## FQDN                       2
## USER-FQDN                  3
## DER-ASN                    9
## KEY-ID                     11
## ***********************************************
SET NVIKEIDTYPE 11

## ***********************************************
## Ike exchange mode
```

```
##
## Aggressive                  1
## Main mode                   2
## ************************************************
SET NVIKEXCHGMODE 1

## ************************************************
## 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 0

## ************************************************
## IKE Authentication Algorithm
##
## ANY                        0
## MD5                        1
## SHA1                       2
## ************************************************
SET NVIKEP1ENCALG 0

## ************************************************
## IKE config mode
##
## Enabled                1
## Disabled               2
## ************************************************
SET NVIKECONFIGMODE 1

## ************************************************
## 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

## ************************************************
## IPsec Encryption Algorithm
##
## ANY                              0
## AES-128                          1
## 3DES                             2
## DES                              3
## AES-192                          4
## AES-256                          5
## ************************************************
SET NVIKEP2ENCALG 0

## ************************************************
## IPsec Authentication Algorithm
##
## ANY                        0
## MD5                        1
## SHA1                       2
## ************************************************
SET NVIKEP2AUTHALG 0

## ************************************************
## IKE over TCP
##
## IKE_OVER_TCP_NEVER   0
## IKE_OVER_TCP_AUTO    1
## IKE_OVER_TCP_ALWAYS  2
## ************************************************
SET NVIKEOVERTCP 0

## ************************************************
## VPNCODE
## ************************************************
SET VPNCODE "876"
## Craft code
## ************************************************
SET PROCPSWD 27238

## ************************************************
## 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
```

5. Configure Cisco 2811 ISR

These Application Notes assume that Cisco ISR is installed on the network in an operational state. The information in this document is based on the Cisco 2811 hardware running 12.4.24T firmware. All the configuration steps are performed on the command line interface with the proper authorization credentials. Output of **show version** command on the router is shown below.

```
Cisco IOS Software, 2800 Software (C2800NM-ADVENTERPRISEK9_IVS-M), Version
12.4(24)T, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2009 by Cisco Systems, Inc.
Compiled Wed 25-Feb-09 17:54 by prod_rel_team

ROM: System Bootstrap, Version 12.4(13r)T, RELEASE SOFTWARE (fc1)

2811-router uptime is 2 weeks, 6 days, 17 hours, 18 minutes
System returned to ROM by power-on
System image file is "flash:c2800nm-adventerprisek9_ivs-mz.124-24.T.bin"


This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found
at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

Cisco 2811 (revision 53.51) with 247808K/14336K bytes of memory.
Processor board ID FHK1306F476
2 FastEthernet interfaces
2 Channelized (E1 or T1)/PRI ports
1 Virtual Private Network (VPN) Module
4 Voice FXO interfaces
DRAM configuration is 64 bits wide with parity enabled.
239K bytes of non-volatile configuration memory.
125440K bytes of ATA CompactFlash (Read/Write)

Configuration register is 0x2102
```

As a prerequisite, an IP pool for the VPN clients routable inside the organization implementing the VPN gateway is needed. In these application notes the **10.10.98.0/24 network** was assigned for the purpose. In order implement IPSec VPN head end on the Cisco ISR, the following configuration as to be performed.

- Enable Authentication Authorization and Accounting
- Create users in the local database
- Create an Internet Security Association and Key Management Protocol (ISAKMP) for Phase 1 negotiation
- Create a group along with pre-shared key for authentication
- Create Phase 2 policy for data encryption
- Create a dynamic map
- Create a crypto map
- Apply Crypto map on the outside interface
- Create a pool of addresses to be assigned to VPN Clients

5.1. Enable authentication, authorization and accounting (AAA)

Use the command **aaa new-model** to enable AAA process. In order to enable extended authentication (Xauth) for user authentication, enable the AAA authentication commands.

```
aaa new-model
!
aaa authentication login groupauthor local
aaa authentication login userauthen local
aaa authorization network groupauthor local
```

local specifies user authentication to be used to use against the local database.

5.2. Create users in the local database

To create the username in the configuration database, use the command **username** followed by name to be assigned by the user, the keyword **password 0** and the plain text password. The following example display command used for creating user **testphone2** with password **vpnpass**.

```
username testphone2 password 0 vpnpass
```

5.3. Create an ISAKMP policy

To create an Internet Security Association and Key Management Protocol (ISAKMP) and policy for Phase 1 negotiation, by using the **crypto isakmp policy n**, where **n** is the policy number. Note that multiple policies may coexist, and the Cisco ISR gateway will evaluate them in the encryption negotiation, starting from the lowest policy number to the highest. The following example shows the creation of two policies in order to support different encryptions for the phase one.

```
 crypto isakmp policy 3
 encr 3des
 hash md5
 authentication pre-share
 group 2
!
crypto isakmp policy 4
 encr aes
 authentication pre-share
 group 2
```

5.4. Create a group along with pre-shared key for authentication

Using the command **crypto isakmp client** to create a **configuration group** to match the authentication **group** defined previously (**groupauthor**). With the **key** subcommand specify the pre-shared, and with the **pool** sub-command define the address pool to use for inner IP Address of the VPN clients (if required WINS and DNS for VPN clients can be specified here).

```
crypto isakmp client configuration group groupauthor
 key vpnvpn
 pool ippool
 pfs
```

5.5. Create Phase 2 policy for data encryption

Define a **crypto ipsec transform-set** to specify which encryption will we used for the actual tunnel. In the example shown below two different sets are defined, **myset** and **myset2** .The first is using **3des** for encryption and **md5** for hashing while the second set is using **aes** (128 bit is default) and **sha** for hashing.

```
crypto ipsec transform-set myset esp-3des esp-md5-hmac
!
crypto ipsec transform-set myset2 esp-aes esp-sha-hmac
!
```

Allow the system to recover from invalid **spi** event with the command:

```
 crypto isakmp invalid-spi-recovery
```

Define life time for a security association with the command:

```
crypto ipsec security-association lifetime seconds 86400
```

5.6. Create a dynamic map

Define a dynamic map associating one of the transformation set, setting the Diffie-Hellman **group 2** and **reverse route** (this is required to de-encapsulating packets coming from the VPN tunnel).

```
crypto dynamic-map dynmap2 20
set transform-set myset2
set pfs group2
reverse-route
```

5.7. Create a crypto map

Create a crypto map and apply the AAA lists created earlier as presented in example below:

```
crypto map clientmap client authentication list userauthen
crypto map clientmap isakmp authorization list groupauthor
crypto map clientmap client configuration address respond
crypto map clientmap 20 ipsec-isakmp dynamic dynmap2
!
```

5.8. Apply Crypto map on the outside interface

Associate the crypto map defined to the network interface that is facing the outside internet, by using the **crypto map** command in the proper FastEthernet configuration context. The following screenshot displays the addition of the **clientmap** to the interface **FastEthernet0/1**

```
interface FastEthernet0/1
ip address 172.16.1.1 255.255.255.0
duplex auto
speed auto
crypto map clientmap
```

5.9. Create IP Address Pool to Assign to VPN Clients

Define a local pool of IP address to be used for the VPN Telephone / Clients, using the **ip local pool** command. The following example shows addition of an IP Address pool called **ippool** ranging from **10.10.98.20** to **10.10.98.120** for the VPN clients.

Note: Ensure that the routing processes in the Headquarters know how to route packets for these IP Addresses

```
ip local pool ippool 10.10.98.20 10.10.98.120
```

5.10. Save Configuration Changes

In order to make permanent the configuration changes made, issue the command **write memory** on the command line interface.

```
write memory
```

6. Verification Steps

6.1. Communication Manager Verification

From the Communication Manager SAT terminal, use the command **list registered-ip-stations** to show that the VPN Telephones are registered with Communication Manager. The IP Telephones use the inner IP address assigned from the address pool on Cisco 2811 ISR to register with Communication Manager.

```
list registered-ip-stations

                          REGISTERED IP STATIONS

Station Ext   Set Type/ Prod ID/   TCP Station IP Address/
or Orig Port  Net Rgn   Release    Skt Gatekeeper IP Address
------------ --------- ---------- --- ---------------------------------------
-
20036         9620      IP_Phone    y  135.64.186.144
              1         3.1000         135.64.186.7
20040         9630      IP_Phone    y  135.64.186.147
              1         3.1000         135.64.186.6
20041         9630      IP_Phone    y  135.64.186.155
              1         3.1000         135.64.186.7
20050         9640      IP_Phone    y  10.10.98.65
              2         3.1000         135.64.186.7
20051         9650      IP_Phone    y  10.10.98.70
              2         3.1000         135.64.186.7
```

Make a call from the VPN phone1 (**20050**) to VPN phone2 (20051). Use the command **status station x**, where **x** represent the extension number, to verify the status of the VPN Telephone as shown below. Notice on **Page 1**, the VPN phone1 status is **in-service/off-hook**

```
status station 20050                                      Page   1 of   8
                            GENERAL STATUS
     Administered Type: 9640              Service State: in-service/off-hook
        Connected Type: 9640           TCP Signal Status: connected
             Extension: 20050
                  Port: S00054        Parameter Download: complete
```

Page 4, the VPN Telephone uses IP address **10.10.98.65**, which is assigned from the IP Address pool defined on the Cisco 2811 ISR. Note that IP Address **135.64.186.7** is IP Address assigned to the C-LAN circuit pack in Region 1 as shown below.

```
 status station 20050                                    Page   4 of   8
                              CALL CONTROL SIGNALING
Port: S00054         Switch-End IP Signaling Loc: 01B0317  H.245 Port:
            IP Address                                 Port  Node Name     Rgn
Switch-End: 135.64.186.7                               1720  clan1b3         1
   Set End: 10.10.98.65                                3437                  2
H.245 Near:
 H.245 Set:
```

Page 5 shows that the audio is between the two VPN Telephones and the Audio Connection Type is **ip-direct** (shuffling).

```
 status station 20050                                      Page   5 of   8

                           AUDIO CHANNEL Port: S00054
G.729A       Switch-End Audio Location:
            IP Address                                 Port  Node Name     Rgn
Other-End: 10.10.98.70                                 2878                  2
  Set-End: 10.10.98.65                                 3124                  2
Audio Connection Type: ip-direct
```

Page 7 shows the **G.729a** codec is used for the call

```
status station 20050                                    Page   7 of   8
                      SRC PORT TO DEST PORT TALKPATH
src port: S00054
S00054:TX:10.10.98.65:3124/g729a/30ms
S00057:RX:10.10.98.70:2878/g729a/30ms
```

6.2. Verification on the Cisco ISR

In order to verify debugging information, turn on debugging with the commands:

```
term mon
debug crypto isakmp
debug crypto ipsec
```

Remember to disable debugging with the command:

```
no debug all
```

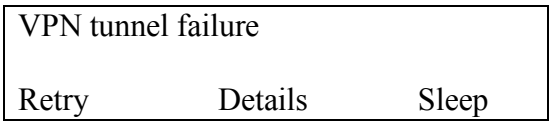
Refer to **[5]** for additional details on debugging on Cisco ISR

7. Troubleshooting

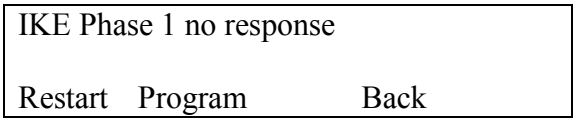
This section describes how to troubleshoot common configuration mismatches between the 96xx Series IP Telephones and the Cisco ISR. The key events in the logs are highlighted in bold. Cisco ISR log messages can be accessed through the command line interface.

7.1. IKE Phase 1 no response.

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



By pressing the **Retry** Soft key again, it will attempt to reestablish the tunnel. If the **Details** Soft key it is pressed, the Telephone display shows the IKE Phase 1 no response

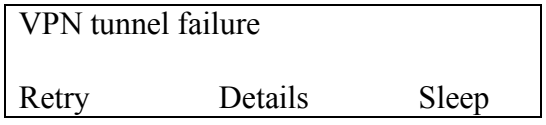


If the **Program** soft key it is pressed, it will redirect to the Craft Code Screen

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

7.2. Incorrect IKE Phase 2

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



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

Invalid configuration Restart Program Back

If we press the **Program** soft key it will redirect to Craft Code Screen

Enter Code: # = OK

Given the correct **PROCPSWD,** it will redirect you to the **local configuration Procedures** Screen. Here, select **VPN** and press **Start** soft key' Press **Forward** soft key on the Telephone and it will go to IKE Phase 2 Screen, here check that the IKE Phase 2 Screen Settings are correct.

7.3. Invalid Username, password:

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

7.4. Invalid IKEID and PSK:

Go to the local procedure configuration page (using details **Softkey ⇨ program ⇨ procpswd**) on the Telephone and re-enter the correct (configured on the Cisco ISR gateway) group name and group password.

7.5. Telephone displaying "connecting…"

This issue can be resolved by the administrators who have access to the core network infrastructure and Cisco ISR Gateway. Ensure that the core network infrastructure knows how to route the address in the IP Pool to the Cisco ISR and that the gateway can reach the C-LAN circuit pack.

7.6. "Need IKE ID/PSK" Message:

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

7.7. No gateway address:

Go to the local procedures configuration page. Using details **Softkey ⇨ program ⇨ procpswd⇨ ADDR ⇨Enter the valid Gateway** address.

8. Conclusion

As illustrated in these Application Notes, the Avaya 96xx Series IP Telephones combined with the Cisco 2811 ISR, provide a secure solution for remote worker telephony over any broadband Internet connection. The Avaya 96xx Series IP Telephones demonstrated successful interoperability with the Cisco ISR 2811 Router.

9. References

Avaya references, available at http://support.avaya.com

Avaya Aura™ Communication Manager:

1. *Administering Avaya Aura™ Communication Manager*, Doc ID 03-300509

Avaya 9600 Series IP Telephone:

2. *Avaya one-X™ Deskphone Edition for 9600 Series IP Telephones Administrator Guide Release 3.1,* Doc ID 16-300698
3. Avaya VPN Setup Guide for 9600 Series IP Telephones Release 3.1, Doc ID 16-602968

Cisco references, available at http://www.cisco.com

4. *Configuring Cisco VPN Client 3.x for Windows to IOS Using Local Extended Authentication* Document ID 20621
5. Cisco IOS Debug Command Reference
   http://www.cisco.com/en/US/docs/ios/debug/command/reference/db_book.html
6. Cisco IOS Security Command Reference
   http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html

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