Avaya Solution & Interoperability Test Lab

Configuring Cisco 2821 Integrated Services Router (ISR) using the Command Line Interface (CLI) for Policy-Based IPSec VPN and XAuth Enhanced Authentication to support Avaya VPNremote™ Phone –Issue 1.0

Abstract

These Application Notes provide a sample configuration for Cisco 2821 Integrated Services Router (ISR) with IPSec VPN tunnel termination and Enhanced Authentication (XAuth) to support the use of the Avaya VPNremote™ Phone. The configuration is completed using the Command Line Interface (CLI). Testing was conducted via the Interoperability Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe the steps to configure a Cisco 2821 Integrated Services Router (ISR) using Command Line Interface (CLI) to establish an IPSec Virtual Private Network (IPSec VPN) tunnel with Avaya VPNremote™ Phone. Authentication is accomplished by using Extended Authentication (Xauth) between the Avaya VPNremote Phone and Cisco 2811 ISR. References in parenthesis will be used throughout the remainder of these application notes.

The Avaya VPNremote Phone is a software based IPSec VPN client integrated into the firmware of Avaya 4600 Series IP Telephones. This capability allows the Avaya IP Telephone to be plugged in and used over a secure IPSec VPN from any broadband Internet connection. An end user experiences the same IP telephone features as if the phone were being used in the office. Avaya IP Telephone models supporting the Avaya VPNremote Phone firmware include the 4610SW, 4620SW, 4621SW, 4622SW and 4625SW. Release 2 of the Avaya VPNremote Phone used in these Application Notes extends the support of head-end VPN gateways to include Cisco security platforms.

XAuth is a draft RFC developed by the Internet Engineering Task Force (IETF) based on the Internet Key Exchange (IKE) protocol. The Avaya VPNremote Phone communicates with the Cisco 2821 ISR using IKE with pre-shared key. XAuth allows security gateways to perform user authentication in a separate phase after the IKE authentication phase 1 exchange is complete. The Avaya VPNremote Phone uses a pre-shared key to authenticate with the ISR and create a temporary secure path (IPSec Tunnel) to allow the Avaya VPNremote Phone user to present “username” and “password” credentials to the ISR. The ISR uses the “local user authentication” mechanism in this sample configuration.

After the Avaya VPNremote Phone user authentication is successful, the ISR assigns an IP address to the Avaya VPNremote Phone from a pre-configured IP Address Pool.

1.1 Avaya VPNremote Phone Start-up Event

The steps shown in **Figure 1** below describe the high level events that take place during the start-up of an Avaya VPNremote Phone.

- Avaya VPNremote Phone establishes an IPSec VPN tunnel upon boot up with the designated IPSec VPN head-end.
- Avaya VPNremote Phone initiates a TFTP, HTTP, or HTTPS session with the file server PC for configuration file download (46vpnuprgade.scr, 46vpnsetting.txt, 46xxsettings.txt).
- Avaya VPNremote Phone registers with Avaya Communication Manager and is ready for Service.

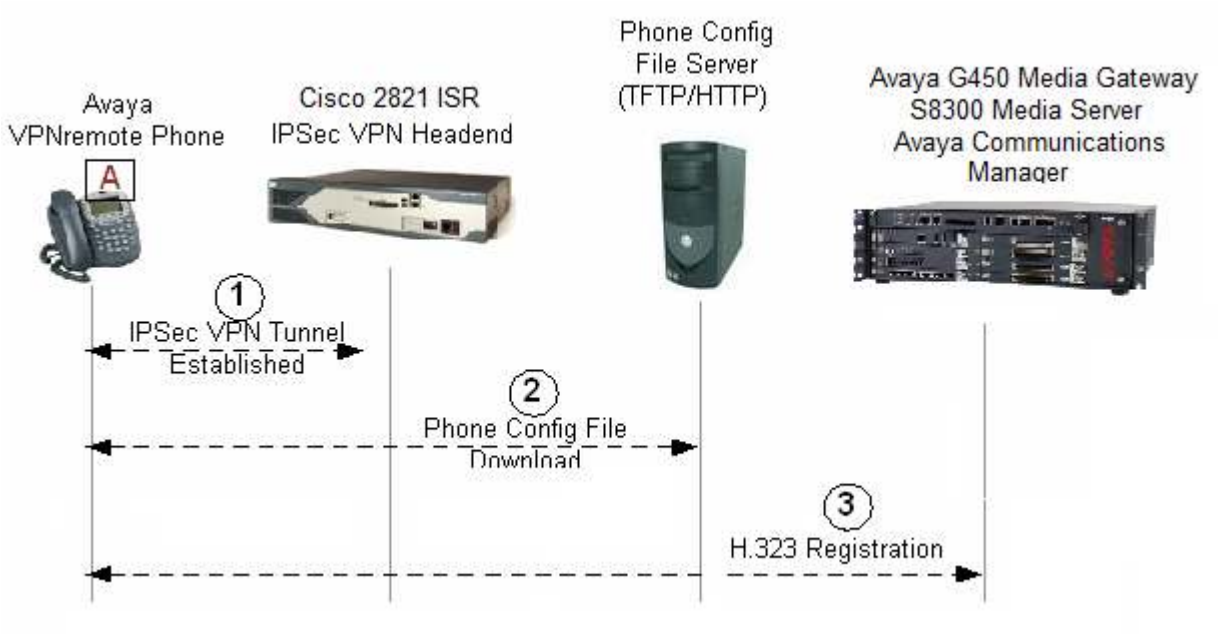

Figure 1: Avaya VPNremote Phone Start-up Events

1.2 Network Topology

The sample network implemented for these Application Notes is shown in **Figure 2** outlines a private network containing an ISR functioning as a perimeter security device and VPN head-end.

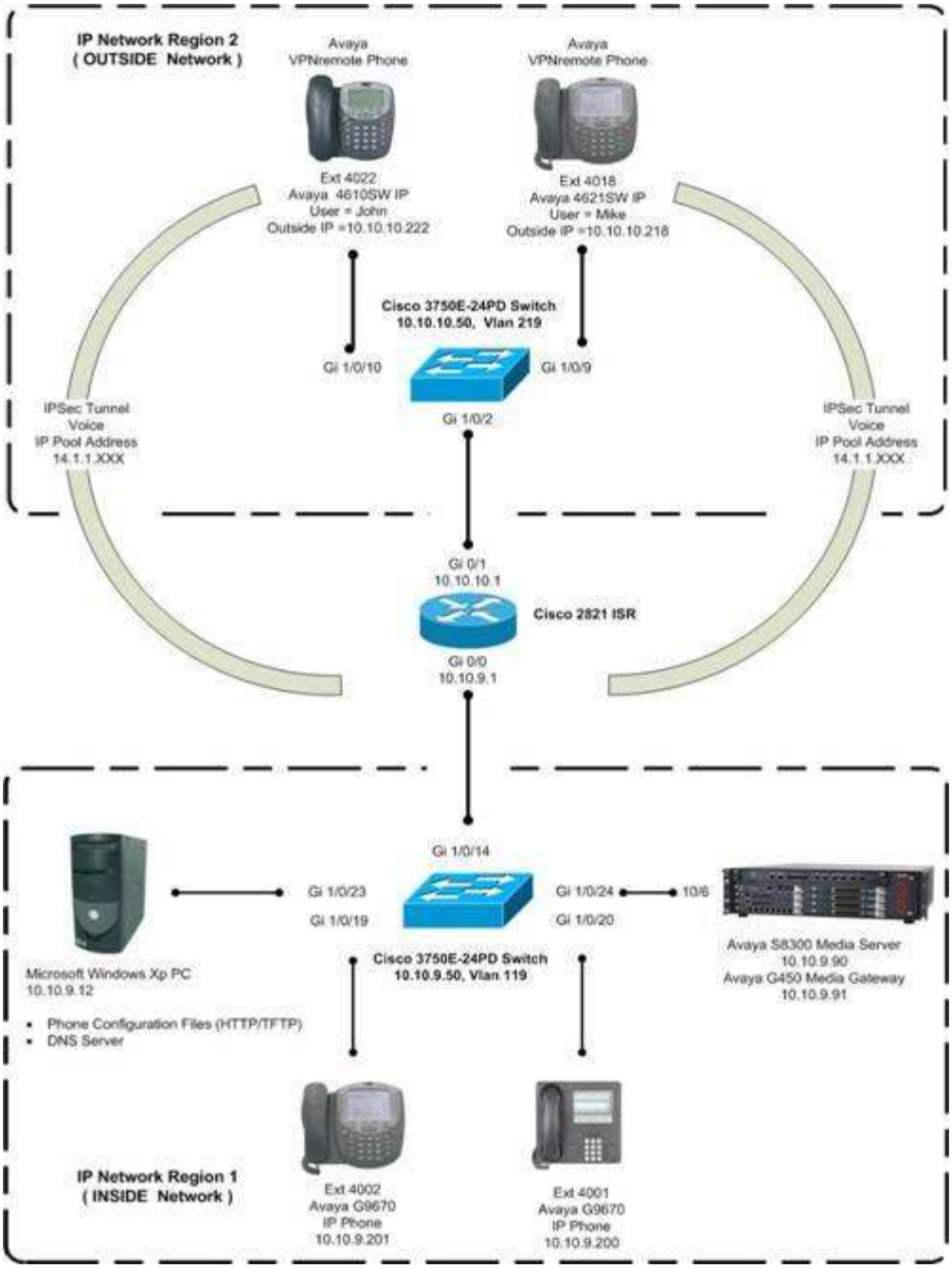

Figure 2: Network Diagram

The Avaya VPNremote Phones are located in the OUTSIDE (public) network and configured to establish an IPSec tunnel to the OUTSIDE IP address of the ISR. The ISR assigns IP addresses to the Avaya VPNremote Phones after successful authentication. The assigned IP addresses, also known as the **inner addresses**, will be used by the ISR when communicating inside the IPSec tunnel and in the INSIDE (private) network to Avaya Communication Manager. Once the IPSec tunnel is established, the Avaya VPNremote Phones access the Phone Configuration File Server and DNS server. The Avaya VPNremote Phones then initiate H.323 registration with the Avaya Communication Manager.

2. Equipment and Software Validated

The information in these Application Notes is based on the software and hardware versions listed in **Table 1** below.

Equipment	Software
Avaya S8300 Media Server	Avaya Communication Manager R5.1 (R015x.01.0.415.1)
Avaya G450 Media Gateway	27.31.0
Avaya VPNremote Phone (4610SW IP)	a10bVPN232_4.bin
Avaya VPNremote Phone (4621SW IP)	a20bVPN232_4.bin
Cisco 2821 Integrated Services Router	Cisco IOS Ver. 12.4(22)YB1
Cisco Catalyst 3750E-24PD Series POE Switch	Cisco IOS Ver. 12.2(35)SE5

Table 1 – Software/Hardware Version Information

3. Cisco 2821 ISR Configuration

Only the options used in this test scenario are illustrated for brevity.

Step	Description
1	This part describes how to configure Cisco's authentication, authorization, and accounting (AAA) paradigm. AAA is an architectural framework for configuring a set of three independent security functions in a consistent and modular manner. • **Authentication** is the way a user is identified prior to being allowed access to the network and network services. Authentication defines a named list of authentication methods and then applying that list to various interfaces. • **Authorization** provides the method for remote access control, including one-time authorization or authorization for each service, per-user account list and profile, user group support and support of IP, IPX, ARA and Telnet. Authorization works by assembling a set of attributes that describe what the user is authorized to perform. These attributes are compared with the information contained in a database for a given user, and the result is returned to AAA to determine the user's actual capabilities and restrictions. • **Accounting** is a method for collecting and sending security server information used for billing, auditing, and reporting, such as user identities, start and stop times, executed commands (such as PPP), number of packets, and number of bytes. Accounting enables you to track the services users are accessing, as well as the amount of network resources they are consuming. The following illustrates the **AAA** defined for this configuration. 2821(config)# **aaa new-model** 2821(config)# **aaa authentication login userauthen local** 2821(config)# **aaa authorization network groupauthor local**
2	Configure users for logging into the Avaya VPNremote Phone. Add **Username, privilege level** and **password** for user(s). 2821(config)#**username mike privilege 15 password mike1234**

3.1 ISAKMP Configuration

The sample configuration uses the Internet Key Exchange (IKE) protocol to establish a secure Internet Security Association and Key Management Protocol (ISAKMP) control channel between peers. In this case the Avaya VPNremote phone and the Cisco 2821 ISR.

ISAKMP defines procedures and packet formats to establish, negotiate, modify and delete Security Associations (SA) containing all the information required for execution of various network security services. ISAKMP defines payloads for exchanging key generation and authentication data. ISAKMP serves as a common framework for agreeing to the format of SA attributes and for negotiating, modifying and deleting SA's of different key exchange protocols, independent of the key generation technique, encryption algorithm and authentication mechanism.

IKE establishes an ISAKMP SA by negotiating proposals in an exchange known as Phase 1. In order to successfully establish an ISAKMP SA, both peers must agree to a common set of security attributes contained within the Phase 1 proposal.

1. ISAKMP Phase One

a. Negotiate and establish an ISAKMP SA, a secure communication channel for further IKE communication. The two systems generate a *Diffie-Hellman* shared value (a method to generate a symmetric key where two parties can exchange values and generate the same symmetric key) that is used as the base for a symmetric shared key and further IKE communication is encrypted using this symmetric key.
b. Verify the remote system's identity (primary authentication)

The following ISAKMP security attributes are administered on both peers, the Avaya VPNremote Phone and Cisco 2821 ISR, in the sample configuration.

- *ISAKMP (Phase 1) proposal:*
  - Encryption Algorithm: 3DES
  - Hash Algorithm: SHA
  - Lifetime (seconds): 86400
  - Diffie-Hellman Group: 2

Once an ISAKMP SA is established, both peers can negotiate IPSec security attributes necessary to establish IPSec SA's. The IKE protocol does this in a second proposal exchange known as Phase 2.

2. ISAKMP Phase Two

- Using the secure communication channel provided by the ISAKMP SA to negotiate the SA's for IPSec transforms. A Phase Two negotiation typically negotiates two SA's for an IPSec transform: one for inbound and one for outbound traffic.

The following are the steps used to configure ISAKMP for this test scenario

Step	Description
1	Enable encrypted **ISAKMP** on the Router 2821(config)#**Crypto isakmp enable** **Note:** Crypto isakmp enable setting does not appear in configuration.
2	Configure an encrypted **ISAKMP** pre-shared key for security access and an associated Peer IP address 2821(config)#**Crypto isakmp key456 address 10.10.10.218**
3	Configure an encrypted **ISAKMP Client** 2821(config)# **crypto isakmp client configuration group myclient** 2821(config-isakmp-group)#**key key123** 2821(config-isakmp-group)#**dns 14.1.1.10** 2821(config-isakmp-group)#**wins 14.1.1.20** 2821(config-isakmp-group)#**domain mydomain.com** 2821(config-isakmp-group)#**pool blackpool** 2821(config-isakmp-group)#**acl 101** 2821(config-isakmp-group)#**netmask 255.255.255.0** 2821(config-isakmp-group)#**exit**
4	Configure encrypted **ISAKMP Policy** for suite protection 2821(config)#**Crypto isakmp policy 3** 2821(config-isakmp)#**encryption 3des** 2821(config-isakmp)#**authentication pre-share** 2821(config-isakmp)#**group 2**

3.2 IPSEC Configuration

IPSec provides a process for the definition of secure *tunnels* between peers, allowing for the secure routing of sensitive data. The following are the steps used in configuring the various IPSec parameters for this test scenario.

Step	Description
1	Configure encrypted IPSec Profile and Security association (SA) parameters 2821(config)# **Crypto ipsec profile vpnclient** 2821(cfg-ipsec-profile)# **set security-association idle-time 86400 default** 2821(cfg-ipsec-profile)# **set transform-set myset**
2	Configure an encrypted IPSec transform and settings A transform set is an acceptable combination of security protocols, algorithms and other settings to apply to IPSec protected traffic. During the IPSec security association negotiation, the peers agree to use a particular transform set when protecting a particular data flow. A transform set must be defined regardless of the tunneling protocol used. 2821(config)#**Crypto ipsec transform-set myset esp-3des esp-sha-hmac** 2821(cfg-Crypto-trans)#**mode** **Note:** Mode setting does not appear in configuration.

3.3 Crypto Map Configuration

Step	Description
1	Configure an encrypted **Dynamic Map** 2821(config)#**Crypto dynamic-map mydynmap 10** 2821(config-crypto-map)#**set transform-set myset** **Note:** The software only refers to the first dynamic access list defined.
2	Configure an encrypted **Client Map** 2821(config)#**crypto map clientmap client authentication list userauthen** 2821 (config)#**crypto map clientmap isakmp authorization list groupauthor** 2821(config)#**crypto map clientmap client configuration address initiate** 2821(config)#**crypto map clientmap client configuration address respond**
3	Configure an encrypted **Static Map** as a subset of the defined encrypted Crypto Map 2821(config)#**crypto map clientmap 20** 2821(config-crypto-map)#**set peer 10.10.9.1** 2821(config-crypto-map)#**set transform-set myset** 2821(config-crypto-map)#**match address 101** 2821(config-crypto-map)#**reverse-route**
4	Configure an Dynamic map as a subset of the defined encrypted Client Map A dynamic crypto map set is included by reference as part of a crypto map set. Any crypto map entries that reference dynamic crypto map sets should be the lowest priority crypto map entries in the cryptomap set (that is, have the highest sequence numbers) so that the other crypto map entries are evaluated first; that way, the dynamic crypto map set is examined only when the other (static) map entries are not successfully matched. 2821(config)#**crypto map clientmap 100 ipsec-isakmp dynamic mydynmap**

3.4 Configuring IP Settings

Step	Description
1	Define the **IP address pool.** The XAuth protocol enables the router to dynamically assign IP addresses from a specific address pool. 2821(config)#**ip address-pool local**
2	Configure **IP address pool** description and address range definition. Create an IP Address Pool for assigning IP addresses by the Cisco 2821 ISR to Avaya VPNremote Phones as **inner address** for when an IPSec tunnel is established. Successfully. Ensure the address range does not conflict with other addresses used in network 2821(config)# **ip local pool blackpool 14.1.1.100 14.1.1.200**
3	Configure **IP Default Gateway** to use. The default gateway is set to the outside (public) interface for the sample configuration. 2821(config)#**ip default-gateway 10.10.10.1**
4	Configure **ip http timeout-policy** 2821(config)#**ip http timeout-policy idle 600 life 86400 requests 10000**

3.5 Access Lists Configuration

Access lists are used to define what specific IP traffic will and will not be protected by a Crypto policy. There are 2 types of access lists that can be defined, Standard and Extended. Standard and static extended access lists provide basic traffic filtering capabilities.

Access lists describe which packets should be forwarded and which packets should be dropped at an interface. Criteria based on each packet's network layer information determines if specific packets are to be **permitted** or **denied** access allowing for a fine tuning of the security policy facilitating traffic flow across the network. Extended access lists can also examine transport layer information to determine whether to block or forward packets. It is the Crypto map entry referencing the specific access list that defines whether IPSec processing is applied to the traffic matching a permit in the access list.

Step	Description
1	Configure a **Standard** access list. 2821(config)#**access-list 23 permit any log**
2	Configuring an **Extended** access list. 2821(config)#**access-list 101 permit ip 10.10.10.0 0.0.0.255 10.10.9.0 0.0.0.255 log** 2821(config)#**access-list 102 deny ip 10.10.10.0 0.0.0.255 10.10.9.0 0.0.0.255 log** 2821(config)#**access-list 102 permit ip 10.10.10.0 0.0.0.255 any log** 2821(config)#**access-list 199 deny ip any any log** 2821(config)#**access-list 199 permit ip any 10.10.9.0 0.0.0.255 log**
3	Verifying Crypto Access Lists 2821(config)#**show access-lists 101**

3.6 Ethernet Interfaces Configuration

This section shows the specific interface configurations made for use in this test configuration.

Step	Description
1	Configuring Ethernet Interface GigabitEthernet 0/0 2821(config)#**conf t** 2821(config)#**interface GigabitEthernet 0/0** 2821(config)#**description INSIDE** 2821(config)#**ip address 10.10.9.1 255.255.255.0** 2821(config)#**duplex auto** 2821(config)#**speed auto**
2	Configuring Ethernet Interface GigabitEthernet 0/1 2821(config)#**conf t** 2821(config)#**interface GigabitEthernet 0/1** 2821(config)#**description OUTSIDE** 2821(config)#**ip address 10.10.10.1 255.255.255.0** 2821(config)#**duplex auto** 2821(config)#**speed auto** 2821(config)#**crypto map clientmap** **Note:** It is important to define Crypto Map on Outer interface

3.7 Access Management Configuration

Virtual Terminal (VTY) ports for user access administration on the router using configuration. Configuring the **transport input all** defines Telnet as a protocol to use for command line mode. Users must open a Telnet session into the router to be authenticated before they can gain access through the router. If multiple VTY ports are specified, they must all be configured identically because the software hunts for available VTY ports on a round-robin basis.

Step	Description
1	Configure the Access Management on the Router 2821(config)#**conf t** 2821(config)#**line con 0** 2821(config)#**line aux 0** 2821(config-line)#**exec-timeout 0 0** 2821(config)#**line vty 0 4** 2821(config-line)#**access-class 23 in** 2821(config-line)#**privilege level 15** 2821(config-line)#**transport input all**

4. Cisco Catalyst 3750E-24PD Switch Configuration

The complete configuration related to Cisco Catalyst 3750E-24PD is beyond the scope of these Application Notes and thus is not shown. This section only shows the specific configurations for use in this test scenario.

Step	Description
1	Configure Vlan(s) on the switch 3750(config)#**vlan 119** 3750(config-vlan)#**name INSIDE** 3750(config)#**vlan 219** 3750(config-vlan)#**name OUTSIDE**
2	Assign an IP address to the vlans 119 and 219 3750(config)#**interface vlan 119** 3750(config-if)#**ip address 10.10.9.50 255.255.255.0** 3750(config)#**interface vlan 219** 3750(config-if)#**ip address 10.10.10.50 255.255.255.0**

3	Create a range of trunked ports tagged to the vlans 119 and 219 3750(config)#**interface range gigabitEthernet1/0/9-10** 3750(config-if)#**switchport trunk encapsulation dot1q** 3750(config-if)#**switchport trunk allowed vlan 119** 3750(config-if)#**switchport mode trunk** 3750(config)#**interface range gigabitEthernet1/0/19-20** 3750(config-if)#**switchport trunk encapsulation dot1q** 3750(config-if)#**switchport trunk allowed vlan 219** 3750(config-if)#**switchport mode trunk**
4	Create a range of access ports tagged to the vlans 119 and 219 3750(config)#**interface range gigabitEthernet1/0/1-8,11,12** 3750(config-if)#**switchport access vlan 119** 3750(config-if)#**spanning-tree portfast** 3750(config)#**interface range gigabitEthernet1/0/13-1.8,21,22,23** 3750(config-if)#**switchport access vlan 219** 3750(config-if)#**spanning-tree portfast**
5	Configure a trunk port as uplink port to accept both vlan 119 and vlan 219 3750(config)# **interface gigabitEthernet1/0/24** 3750(config-if)#**switchport trunk encapsulation dot1q** 3750(config-if)#**switchport trunk allowed vlan 119,219** 3750(config-if)#**switchport mode trunk** 3750(config-if)#**spanning-tree portfast**

5. Avaya Communication Manager Configuration

This section describes the configuration of Avaya Communication Manager. This section describes the configuration of the components necessary to support the Avaya VPNremote Phone. This includes the following components or services:

- IP network map
- IP network region
- IP codec set
- Stations

The configuration of Avaya Communication Manager was performed using the System Access Terminal (**SAT**). After the completion of the configuration, perform a **save translation** command to make the changes permanent. The Avaya VPNremote Phone is administered within Avaya Communication Manager the same as the other IP telephones used in the sample configuration. Even though the Avaya VPNremote Phone is physically located on the OUTSIDE network, it behaves the same as the other IP telephones located on the corporate INSIDE network once the VPN tunnel has been established.

A common deployment for the Avaya VPNremote Phones is in a home network environment with limited bandwidth. The **G.729 codec** is recommended for such bandwidth constrained environments. Avaya Communication Manager IP Network Regions allow IP endpoints to be logically grouped together to apply unique configuration settings, including the assignment of specific codec's. As shown in **Figure 2**, the OUTSIDE network is assigned to IP Network Region 2 configured with the **G.729 codec**. The INSIDE network is assigned to IP Network Region 1 using the **G.711 codec.**

5.1 IP Network Map

Use the **change ip-network-map** command to define the IP address to Network Region mapping for Avaya VPNremote Phones.

```
change ip-network-map                                          Page   1 of  32
                           IP ADDRESS MAPPING

                                                                Emergency
                                      Subnet                    Location
 From IP Address  (To IP Address   or Mask)  Region    VLAN    Extension
 10 .10 .9  .0    10 .10 .9  .255             1        n
 10 .10 .10 .0    10 .10 .10 .255             2        n
```

5.2 IP Network Region

Determine the IP network region in which the Avaya VPNremote Phones will reside. Avaya VPNremote Phones reside in the IP network region 2 which is the OUTSIDE network. The Avaya S8300 Server is located in IP network region 1 which is the INSIDE network. **Intra-region** and **Inter-region IP-IP Direct Audio** (also known as shuffling) determines the flow of RTP audio packets. Setting these fields to **yes** enables the most efficient audio path to be taken. **Codec Set 1**, defined in **Section 6.1**, is assigned to IP Network Region 1, and **Intra-region** and **Inter-region IP-IP Direct Audio** was enabled. The example below shows the IP network region 1 settings used in the test scenario. Use the **change ip-network-region n** command to configure IP Network Region parameters where **n** is the IP Network Region number. Configure the highlighted fields shown below. All remaining fields can be left at the default values.

```
change ip-network-region 1                                      Page   1 of  19
                              IP NETWORK REGION
  Region: 1
Location: 1       Authoritative Domain: mydomain.com
    Name: INSIDE Network
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: 3327
DIFFSERV/TOS PARAMETERS                 RTCP Reporting Enabled? y
 Call Control PHB Value: 46      RTCP MONITOR SERVER PARAMETERS
        Audio PHB Value: 46       Use Default Server Parameters? y
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                     RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```

Page 3 of the IP-Network-Region form, shown below, defines the codec set to use for inter-region calls. Avaya VPNremote Phones are mapped to Region 2. Calls within IP Network Region 1 use Codec Set 1 (G.711MU) while calls between IP Network Region 1 and IP Network Region 2 use Codec Set 2 (G.729).

```
change ip-network-region 1                                      Page   3 of  19

                    Inter Network Region Connection Management

 src dst codec direct   WAN-BW-limits   Video      Intervening      Dyn
 rgn rgn  set   WAN  Units    Total Norm  Prio Shr Regions          CAC IGAR AGL
 1   1    1                                                                  all
 1   2    2     y    NoLimit                                            n   all
```

Use the **change ip-network-region 2** command to configure IP Network Region 2 parameters. Configure the highlighted fields shown below. Calls within IP Network Region 2 (i.e., Avaya VPNremote Phone calling another Avaya VPNremote Phone) use Codec Set 2 (G.729). All remaining fields can be left at the default values.

```
change ip-network-region 2                                      Page   1 of  19
                              IP NETWORK REGION
  Region: 2
Location: 1        Authoritative Domain: mydomain.com
    Name: OUTSIDE Network
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 2              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                     IP Audio Hairpinning? y
   UDP Port Max: 3327
DIFFSERV/TOS PARAMETERS                 RTCP Reporting Enabled? y
 Call Control PHB Value: 46      RTCP MONITOR SERVER PARAMETERS
        Audio PHB Value: 46       Use Default Server Parameters? y
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                     RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```

Page 3 defines the codec set to use for inter-region calls. Avaya VPNremote Phones are mapped to Region 2. Calls between IP Network Region 2 and IP Network Region 1 will also use Codec Set 2 (G.729).

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

                    Inter Network Region Connection Management

 src dst codec direct   WAN-BW-limits   Video      Intervening      Dyn
 rgn rgn  set   WAN  Units    Total Norm  Prio Shr Regions          CAC IGAR AGL
 2   1    2     y    NoLimit                                            n
 2   2    1                                                                  all
```

5.3 IP Codec Set

The **change ip-codec-set** defines the codecs to be used. The configuration below shows the setting of both G.711MU and G.729A codecs. The **change ip-codec-set 1** command configures the highlighted fields shown to define an IP Codec Set for the **G.711** codec. Similarly using the **change ip-codec-set 2** command define the IP Codec Set for the **G.729** codec. The remaining fields can be left at the default values.

```
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:
```

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

                          IP Codec Set

    Codec Set: 2

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

Use the **list ip-codec-set** command to verify the codec assignments.

```
List ip-codec-set

                                IP CODEC SETS

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

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

5.4 Add Stations

Add a station for each Avaya VPNremote Phone to be supported. The configuration of the station is the same as with any other Avaya IP H.323 Telephone. The example below shows the use of the **add station** command to add station **4018** which is one of the Avaya VPNremote Phones located at the remote OUTSIDE network. The **Type** field is set to **4621**. The **Port** field is set to **IP**. The **Name** field should be set to a descriptive name for this **user**. The **Security Code** field contains the password used by the user to access the telephone. Extension numbers need to be defined for all the phones listed in Table 1. The '**add station**' command is used to configure a phone extension. The **Type** parameter is selected for the model type or nearest representative model listed in the software database. A generic **Security Code** is allocated to all the phones under test. The **Name** for the particular phone to be used at this extension can be given as a specific name or the extension number of the phone tested. The screens below show, for example, the first two **add station** pages for the 4610SW Avaya VPNremote Phone used for these Application Notes. The **Direct IP-IP Audio Connections** option on **Page 2** must be set to **y** to take advantage of the configuration in **Section 5.2**

```
add station 4018                                              Page   1 of   6
                                     STATION

Extension: 4018                          Lock Messages? n
     Type: 4621                          Security Code: 1234             TN: 1
     Port: S00037                      Coverage Path 1:                 COR: 1
     Name: Mike                        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: 4018
            Speakerphone: 2-way               Mute Button Enabled? y
        Display Language: english                Expansion Module? y
 Survivable GK Node Name:
          Survivable COR: internal              Media Complex Ext:
   Survivable Trunk Dest? y                          IP SoftPhone? n

                                              Customizable Labels? Y
```

```
add station 4018                                              Page   2 of   6
                                     STATION
FEATURE OPTIONS

                                              Display Client Redirection? n
              AUDIX Name:                    Select Last Used Appearance? N
                                               Coverage After Forwarding? s
                                          Direct IP-IP Audio Connections? y
  Emergency Location Ext: 4018          Always Use? n IP Audio Hairpinning? n
```

6. Avaya VPNremote Phone Configuration

6.1 Avaya VPNremote Phone Firmware

The Avaya VPNremote Phone firmware must be installed on the phone prior to the phone being deployed in the remote location. The firmware includes the letters **VPN** in the name allowing for easy identification of versions incorporating VPN capabilities. Refer to documentation for details on installing Avaya VPNremote 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 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.

6.2 Configuring Avaya VPNremote Phone

The Avaya VPNremote Phone configuration can be administered centrally from a TFTP/HTTP/HTTPS server or locally on the phone. These Application Notes utilize the local phone configuration method. The phone options must match exactly the Configuration of the 2821 ISR, otherwise it will not operate successfully. Refer to **[1]** and **[2]** for details

1. There are two methods available to access the **VPN Configuration Options** menu from the Avaya VPNremote Phone.

   a. During Telephone Boot:

   During the Avaya VPNremote Phone boot up, the option to press the * key to enter the local configuration mode is displayed on the telephone screen as shown below.

```
DHCP
* to program
```

   When the * key is pressed, several configuration parameters are presented such as the phone's IP Address, the Call Server's IP Address, etc. Press # to accept the current settings or set to an appropriate value. The final configuration option displayed is the VPN Start Mode option shown below. Press the * key to enter the VPN Options menu.

```
VPN Start Mode: Boot
*=Modify #=OK
```

b. During Telephone Operation:

While the Avaya VPNremote Phone is in an operational state, e.g., registered with Avaya Communication Manager, press the following key sequence on the telephone to enter VPN configuration mode:

```
Mute-V-P-N-M-O-D-# or (Mute-8-7-6-6-6-3-#)
```

The following is displayed:

```
VPN Start Mode: Boot
*=Modify #=OK
```

Press the * key to enter the VPN Options menu

2. The configuration option values of Avaya VPNremote Phone Extension 4018 used in the sample configuration is shown in **Table 2**.

Press the ► hard button on the telephone to access the next configuration option.

Press the button opposite the specific VPN Option displayed on the screen to scroll through and change the configuration options. Phone models with larger displays (e.g., 4621SW) will present more configuration options per page.
Note: The values entered on the Avaya VPNremote Phone below are case sensitive and must match User settings created in the ISR Configuration.

Configuration Options	Value	Description
Server ►	**10.10.10.1**	IP address of the ISR OUTSIDE (Public)interface
User Name ►	**mike**	Match User settings in ISR Config
Password ►	********	Match Password set in ISR Config
Group Name ►	**myclient**	Match Group set in ISR Config
Group PSK ►	********	Match Key created in ISR Config
VPN Start Mode ►	**BOOT**	IPSec tunnel dynamically starts on Phone power up.
Password Type►	**Save in Flash**	User is not prompted at phone boot up.
Encapsulation ►	**2070-500**	Value set on the phone
Syslog Server ►	**-**	Locally log phone events

IKE Parameters►	**Define DH2-3DES-SHA1**	
	IKE ID Type►	**KEY-ID**
	Diffie-Hellman Grp►	**2**
	Encryption Alg ►	**3DES**
	Authentication Alg ►	**SHA1**
	IKE Xchg Mode ►	**Aggressive**
	IKE Config Mode ►	**Enable**
	XAUTH ►	**Enable**
	Cert Expiry Check ►	**Disable**
	Cert DN Check ►	**Disable**

IPSec Parameters►	**Define DH2-3DES-SHA1**	
	Encryption Alg ►	**3DES**
	Authentication Alg ►	**SHA1**
	Diffie-Hellman Grp ►	**2**

Protected Net►		
	Virtual IP: ►	
	Remote Net #1: ►	**0.0.0.0/0** for
	Remote Net #2: ►	Access to all private nets
	Remote Net #3: ►	
	Remote Net #4: ►	
	Remote Net #5: ►	
Copy TOS: ►	**Yes**	Option
File Srvr: ►	**10.10.9.12**	TFTP/HTTP Phone File Server
Connectivity Check: ►	**First Time**	Test initial IPSec connectivity
Qtest:►	**Enable**	

Table 2 – Avaya VPNremote Phone Configuration

The Avaya VPNremote Phone can interoperate with several VPN head-end vendors. The Avaya VPNremote Phone must be configured with the VPN head-end vendor to be used so the appropriate protocol dialogs can take place. This is done by setting the **VPN Configuration Profile** values for the Avaya VPNremote Phone from the options menu as displayed.

Press the **Profile** soft button at the bottom of the Avaya VPNremote Phones display while in the VPN Options mode. The **VPN Configuration Profile** options, shown below, are displayed. The **Cisco Xauth with PSK** profile was selected for use on the Avaya VPN remote phones used in this scenario.

If a profile other then **Cisco Xauth with PSK** is already chosen, press the **Modify** soft button to see this list.

- Avaya Security Gateway
- Cisco Xauth with PSK
- Juniper Xauth with PSK
- Checkpoint
- Cisco Xauth with Certs
- Juniper Xauth with Certs
- Generic PSK
- Nortel Connectivity

Press the button aligned with the **Cisco Xauth with PSK** profile option to select it and then press the **Done** soft button. When all VPN configuration options have been set, press the **Done** soft button. The following is displayed.

```
Save New Values ?
*= no  #= yes
```

Press # to save the configuration and reboot the phone.

7. Verification

7.1 Avaya VPNremote Phone IPSec Statistics

Once the Avaya VPNremote Phone establishes an IPSec tunnel, registers with Avaya Communication Manager and becomes functional, from the telephone keypad, press the **OPTIONS** hard button (with √ icon). From the telephone keypad, press the ► hard button until the **VPN Status…** option appears. Select **VPN Status.** The VPN statistics of the active IPSec tunnel will be displayed. Press the ► hard button to access the next screen. Press the **Refresh** soft button to update the displayed statistics. The list below shows the statistics from the Avaya VPNremote Phone, Extension 4018 was used in the sample configuration.

VPN Status	
PKT S/R	**1/1**
FRAG RCVD	0
Comp/Decomp	0/0
Auth Failures	0
Recv Errors	0
Send Errors	0
Gateway	**10.10.10.1**
Outer IP	**10.10.10.218**
Inner IP	**14.1.1.174**
Gateway Version	**Cisco IOS So**.
Inactivity Timeout	**0**
	unknown

Table 4 – Avaya VPNremote Phone IPSEC Statistics.

7.2 Avaya Communication Manager Phone registration status

7.2.1 List registered-ip-stations

The Avaya Communication Manager **list registered-ip-stations** command run from the SAT interface can be used to verify the registration status of the Avaya VPNremote Phones and associated parameters as highlighted below.

```
list registered-ip-stations

                            REGISTERED IP STATIONS

Station Ext/  Set     Product    Prod   Station         Net Gatekeeper     TCP
 Orig Port    Type    ID         Rel    IP Address      Rgn IP Address     Skt
4001          9640    IP_Phone   2.0000 10.10.9.200     1   10.10.9.90      y
4002          4621    IP_Phone   2.9000 10.10.9.201     1   10.10.9.90      y
4018          4621    IP_Phone   2.3000 10.10.10.218    2   10.10.9.90      y
4022          4610    IP_Phone   2.3000 10.10.10.222    2   10.10.9.90      y
```

7.2.2 Status Station

The Avaya Communication Manager **status station** command run from SAT verifies the current status of an administered station. The **Service State: in-service/off-hook** shown on **Page 1** below indicates the Avaya VPNremote Phone with extension **4018 (10. 10. 10.218)** is participating in an active call.

```
status station 4018                                            Page   1 of   8
                              GENERAL STATUS
     Administered Type: 4620               Service State: in-service/off-hook
        Connected Type: 4621           TCP Signal Status: connected
             Extension: 4018
                  Port: S00037        Parameter Download: pending

           Call Parked? no                 SAC Activated? no
      Ring Cut Off Act? no
Active Coverage Option: 1

          EC500 Status: N/A        Off-PBX Service State: N/A
   Message Waiting:
   Connected Ports: S00000

 Limit Incoming Calls? no

 User Cntrl Restr: none                        HOSPITALITY STATUS
Group Cntrl Restr: none                     Awaken at:
                                             User DND: not activated
                                            Group DND: not activated
                                          Room Status: non-guest room

                                              Room Status: non-guest room
```

Page 5 shown below, displays the audio status of the **active call** as being between **two Avaya VPNremote Phones,** extension **4018 (10. 10. 10.218)** and extension **4022 (10. 10. 10.222)** located in the **OUTSIDE** network, **IP Network Region 2.**

The highlighted fields indicate the following:

- **Other-end IP Address** value indicates the call is between the Avaya VPNremote Phones
- Audio connection type **ip-direct** indicated that the Audio RTP packets are going direct between Avaya VPNremote Phones.
- Both Avaya VPNremote Phones are located in IP Network Region 2.
- Defined codec **G.729A** is being used.

```
status station 4018                                          Page   5 of   8

                          AUDIO CHANNEL Port: S00037
G.729A        Switch-End Audio Location:
            IP Address                                Port  Node Name       Rgn
Other-End:  10. 10. 10.222                            2428                   2
  Set-End:  10. 10. 10.218                            2782                   2
Audio Connection Type: ip-direct
```

When the **Avaya VPNremote Phone,** extension **4018** located in **IP Network Region 2** is participating in an **active call** with an **IP telephone,** extension **4001 (10. 10. 9.200)** located in the **INSIDE** network, **IP Network Region 1**, then **Page 5 of 8** will display the audio status for the call.

The highlighted fields indicate the following:

- **Other-end IP Address** value indicates the call is between the Avaya VPNremote Phone and the IP telephone.
- Audio connection type **ip-direct** indicated that the Audio RTP packets are going direct between Avaya VPNremote Phone and the IP telephone.
- The call is between Avaya VPNremote Phone located in IP Network Region 2 and IP telephone located in IP Network Region 1
- Defined codec **G.729A** is being used.

```
Status station 4018                                          Page   5 of   8

                          AUDIO CHANNEL Port: S00037
G.729A        Switch-End Audio Location:
            IP Address                                Port  Node Name       Rgn
Other-End:  10. 10.  9.200                            2300                   1
  Set-End:  10. 10. 10.218                            3320                   2
Audio Connection Type: ip-direct
```

7.3 Avaya VPNremote Phone Quality Test

The Avaya VPNremote Phone **Quality Test** feature is used to predict the quality of voice across the network between the Avaya VPNremote Phone and VPN Head-end through the IPSec tunnel.

The Avaya VPNremote Phone runs a QTest sanity test against the VPN Head-end in quiet mode just after the IPSec tunnel has been established. The ISR characterizes the QTest packets sent by the Avaya VPNremote Phone as a "Land Attack" type of Denial of Service attack due to the makeup of the QTest packets. If this QTest sanity test is executed successfully (i.e., if the VPN Head-end responded to the QTest packets), the QTest soft button is made available to the Avaya VPNremote Phone user. If the ISR drops these QTest packets without responding, resulting in the QTest feature sanity test not complete successfully, the QTest soft button is disabled and not presented to the Avaya VPNremote Phone user.

Select the **QTest** soft button at the bottom of the Avaya VPNremote Phone display to enter the QTest menu similar to the display shown below. Select the **Start** soft button to start Qtest. Record the reported statistics to determine the network connection quality. Once the Avaya VPNremote Phone establishes an IPSec tunnel, registers with Avaya Communication Manager and becomes functional, enter the Avaya VPNremote Phone configuration mode as previously described. The ISR log entries shown below are the QTest packets being denied.

Time Elapsed x Secs	
Packets Lost:	**0%**
Round Trip Delay:	**0ms**
Packets Late:	**0%**
Packets Sent:	**0**
Packets Received:	**0**
Average Delay:	**0ms**
Maximum Delay:	**0ms**
Packets Lost	**0**
Maximum Burst Lost:	**0**
Packets out of seq:	**0**
Interruptions:	**0**

Table 3 – Avaya VPNremote Phone QTest display

7.4 Cisco 2821 ISR Logging

The Logging Console displays the current event log contents of the VPN Router and contains the IKE Phase1 and IKE Phase2 events logged as a single Avaya VPNremote Phone successfully authenticates and establishes an IPSec tunnel. The command followed by "**?**" displays further **options** in each category.

```
2821_vpn#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
2821_vpn(config)#logging console ?
  <0-7>          Logging severity level
  alerts         Immediate action needed           (severity=1)
  critical       Critical conditions               (severity=2)
  debugging      Debugging messages                (severity=7)
  discriminator  Establish MD-Console association
  emergencies    System is unusable                (severity=0)
  errors         Error conditions                  (severity=3)
  guaranteed     Guarantee console messages
  informational  Informational messages            (severity=6)
  notifications  Normal but significant conditions (severity=5)
  warnings       Warning conditions                (severity=4)
  xml            Enable logging in XML
  <cr>

2821_vpn(config)#logging console 7
2821_vpn#
```

The following **debug** commands are supported on the Cisco 2821 ISR:

- **Debug crypto ipsec** Displays IPsec events.
- **Debug crypto isakmp** Displays messages about IKE events.
- **Debug crypto engine** Displays information that pertains to the crypto engine, such as when Cisco IOS software performs encryption or decryption operations.

These commands allow the analysis output to be reviewed. The ***no*** form of these commands disables debugging output.

Cisco ISR Active VPN Sessions
Additional information regarding the Avaya VPNremote phone can be obtained by using the following **crypto commands** to observe tunnel activity. A command followed by "**?**" indicates that further **options are available** in that specific category.

7.4.1 Crypto Session

The **sho crypto session** illustrates the active crypto sessions

```
2821_vpn#sho crypto session
Crypto session current status

Interface: GigabitEthernet0/1
Session status: DOWN
Peer: 10.10.9.1 port 500
  IPSEC FLOW: permit ip 10.10.10.0/255.255.255.0 10.10.9.0/255.255.255.0
        Active SAs: 0, origin: crypto map

Interface: GigabitEthernet0/1
Username: mike
Group: myclient1
Assigned address: 14.1.1.174
Session status: UP-IDLE
Peer: 10.10.10.218 port 2070
  IKE SA: local 10.10.10.1/500 remote 10.10.10.218/2070 Active

Interface: GigabitEthernet0/1
Username: john
Group: myclient2
Assigned address: 14.1.1.173
Session status: UP-ACTIVE
Peer: 10.10.10.222 port 2070
  IKE SA: local 10.10.10.1/500 remote 10.10.10.222/2070 Active
  IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 host 14.1.1.173

        Active SAs: 2, origin: dynamic crypto map

2821_vpn
```

7.4.2 Crypto Map

The **crypto map** joins together the IPSec access list and transforms set and specifies where the protected traffic is sent. Crypto map entries created for IPSec pull together the various parts used to set up IPSec security associations (SA's)

```
2821_vpn#sho crypto map
Crypto Map "clientmap" 20 ipsec-isakmp
        Peer = 10.10.9.1
        Extended IP access list 101
            access-list 101 permit ip 10.10.10.0 0.0.0.255 10.10.9.0 0.0.0.255
        Current peer: 10.10.9.1
        Security association lifetime: 4608000 kilobytes/86400 seconds
        PFS (Y/N): N
        Transform sets={
                myset:  { esp-3des esp-sha-hmac  } ,
        }

Crypto Map "clientmap" 100 ipsec-isakmp
        Dynamic map template tag: mydynmap
        Interfaces using crypto map clientmap:
                GigabitEthernet0/1


2821_vpn#sho crypto dynamic-map
Crypto Map Template"mydynmap" 10
        No matching address list set.
        Security association lifetime: 4608000 kilobytes/86400 seconds
        PFS (Y/N): N
        Transform sets={
                myset:  { esp-3des esp-sha-hmac  } ,
```

7.5 Clearing IKE Connections

To assist in troubleshooting IKE, use the following commands in the router EXEC mode:

7.5.1 Crypto ISAKMP SA

The **show crypto isakmp sa** command displays existing IKE connection identifiers for connections to be cleared.

```
2821_vpn#sho crypto isakmp sa

IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
10.10.10.1      10.10.10.218    QM_IDLE           1066 ACTIVE
10.10.10.1      10.10.10.222    QM_IDLE           1067 ACTIVE

IPv6 Crypto ISAKMP SA

2821_vpn#
```

7.5.2 Crypto ISAKMP Key(s)

The **sho crypto isakmp key** command shows the configured Pre-shared Keys

```
2821_vpn#sho crypto isakmp key
Keyring      Hostname/Address                              Preshared Key

default      10.10.10.218                                  key456
             10.10.10.222                                  key789
```

7.5.3 Crypto IPSEC Transform-set

The **show crypto ipsec transform-set** shows the configured transform-set.

```
2821_vpn#show crypto ipsec transform-set myset

Transform set myset: { esp-3des esp-sha-hmac  }
   will negotiate = { Tunnel,  },
```

7.5.4 Crypto IPSEC SA

The **sho crypto ipsec sa** shows the configured security associations (SA) on the interface the **Crypto map** tagged as **clientmap** is applied to.

```
2821_vpn#sho crypto ipsec sa
     PFS (Y/N): N, DH group: none
     PFS (Y/N): Y, DH group: group2

interface: GigabitEthernet0/1
    Crypto map tag: clientmap, local addr 10.10.10.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (10.10.10.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (10.10.9.0/255.255.255.0/0/0)
   current_peer 10.10.9.1 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
    #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 10.10.10.1, remote crypto endpt.: 10.10.9.1
     path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/1
     current outbound spi: 0x0(0)

     inbound esp sas:

     inbound ah sas:
```

```
     inbound pcp sas:

     outbound esp sas:

     outbound ah sas:

     outbound pcp sas:

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   remote ident (addr/mask/prot/port): (14.1.1.173/255.255.255.255/0/0)
   current_peer 10.10.10.222 port 2070
     PERMIT, flags={}
    #pkts encaps: 28, #pkts encrypt: 28, #pkts digest: 28
    #pkts decaps: 28, #pkts decrypt: 28, #pkts verify: 28
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 10.10.10.1, remote crypto endpt.: 10.10.10.222
     path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/1
     current outbound spi: 0x7B840731(2072250161)

     inbound esp sas:
      spi: 0xD3274F3F(3542568767)
        transform: esp-3des esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2383, flow_id: NETGX:383, sibling_flags 80000046, crypto map: c
lientmap
        sa timing: remaining key lifetime (k/sec): (4494742/85937)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x7B840731(2072250161)
        transform: esp-3des esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2384, flow_id: NETGX:384, sibling_flags 80000046, crypto map:
clientmap
        sa timing: remaining key lifetime (k/sec): (4494741/85937)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE

     outbound ah sas:

     outbound pcp sas:

local crypto endpt.: 10.10.10.1, remote crypto endpt.: 10.10.10.222
     path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/1
     current outbound spi: 0x7B840731(2072250161)

     inbound esp sas:
      spi: 0xD3FD9F8A(3556614026)
        transform: esp-3des esp-sha-hmac ,
```

```
        in use settings ={Tunnel, }
        conn id: 2317, flow_id: NETGX:317, sibling_flags 80000046, crypto map:
clientmap
        sa timing: remaining key lifetime (k/sec): (4499366/86284)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0xBD444A1C(3175369244)
        transform: esp-3des esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2318, flow_id: NETGX:318, sibling_flags 80000046, crypto map:
clientmap
        sa timing: remaining key lifetime (k/sec): (4499372/86284)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE

     outbound ah sas:

     outbound pcp sas:

   protected vrf: (none)

local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   remote ident (addr/mask/prot/port): (14.1.1.174/255.255.255.255/0/0)
   current_peer 10.10.10.218 port 2070
     PERMIT, flags={}
    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
    #pkts decaps: 19, #pkts decrypt: 19, #pkts verify: 19
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 10.10.10.1, remote crypto endpt.: 10.10.10.218
     path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/1
     current outbound spi: 0x5EB4E6AE(1588913838)

     inbound esp sas:
      spi: 0xD52141F(223482911)
        transform: esp-3des esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2319, flow_id: NETGX:319, sibling_flags 80000046, crypto map:
clientmap
        sa timing: remaining key lifetime (k/sec): (4423598/86338)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x5EB4E6AE(1588913838)
```

```
        transform: esp-3des esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2320, flow_id: NETGX:320, sibling_flags 80000046, crypto map:
clientmap
        sa timing: remaining key lifetime (k/sec): (4423603/86338)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE

     outbound ah sas:

     outbound pcp sas:
2821_vpn#
```

7.5.5 Debug Crypto VPN Sessions

To debug Cisco ISR Active VPN Sessions, select the following **debug crypto** command highlighted options in the router EXEC mode. The command followed by "**?**" displays further **options** in each category.

```
2821_vpn#debug crypto ?
  ber           decode ASN.1 BER data
  condition     Define debug condition filters
  ctcp          cTCP debugging
  engine        Crypto Engine Debug
  gdoi          Crypto GDOI Group Key Management debug
  ha            Crypto High Availability (generic) debug
  ipsec         IPSEC processing
  ipv6          Crypto IPv6 debug
  isakmp        ISAKMP Key Management
  kmi           Crypto Key Management Interface debug
  mib           IPSEC Management Transactions
  pki           PKI Client
  provisioning  Crypto provisioning configuration
  rmal          Crypto RMAL debug
  routing       IPSEC Route Events
  socket        Crypto Secure Socket Debug
  verbose       verbose decode

2821_vpn#debug crypto ipsec
Crypto IPSEC debugging is on
2821_vpn#
2821_vpn#debug crypto isakmp
Crypto ISAKMP debugging is on
2821_vpn#
2821_vpn#debug crypto pki transactions
Crypto PKI Trans debugging is on
2821_vpn#
2821_vpn#debug crypto routing
Crypto Routing debugging is on
2821_vpn#
Etc:
```

7.5.6 Clear Crypto VPN Sessions

To flush active **Crypto VPN Sessions,** select the following **clear crypto** command highlighted options in the router EXEC mode.

```
2821_vpn#clear crypto ?
  call      Clear crypto call admission info
  ctcp      cTCP connections
  datapath  Clear crypto data path counters
  dh        Clear stored DH values
  engine    Clear crypto engine
  gdoi      Clear crypto gdoi
  ipsec     IPSec
  isakmp    Flush the ISAKMP database
  mtree     Clear Mtree Manager Command Stats
  pki       pki subsystem
  sa        Clear all crypto SAs
  session   clear crypto sessions (tunnels)

2821_vpn#clear crypto isakmp
2821_vpn#clear crypto sa
2821_vpn#clear crypto session ?
```

7.6 Call Tracing

On Communication Manager use the command **list trace station n**, where **n** is the extention of an administered station, to trace the call's activity.

The following example illustrates an **IP telephone Extension 4001**, which **IP Address** is **10.10.9.200** on the **INSIDE network** calling to the **Avaya VPNremote phone Extension 4018,** which **IP Address** is **10.10.10.218** in the **OUTSIDE network.**

```
list trace station 4001                                          Page   1

                                LIST TRACE

time            data

17:51:50     idle station    4001 cid 0xd9
17:51:56     active station    4001 cid 0xdb
17:51:56     G711MU ss:off ps:20 rn:1/1 10.10.9.200:2372 10.10.9.91:2060
17:52:00     idle station    4001 cid 0xdb
17:52:01     active station    4001 cid 0xdc
17:52:01     G711MU ss:off ps:20 rn:1/1 10.10.9.200:2372 10.10.9.91:2056
17:52:02     dial 4018
17:52:02     ring station    4018 cid 0xdc
17:52:02     G729A ss:off ps:30 rn:2/1 10.10.10.218:2470 10.10.9.91:2054
17:52:03     active station    4018 cid 0xdc
17:52:03     G729A ss:off ps:30 rn:1/2 10.10.9.200:2372 10.10.10.218:2470
17:52:03     G729A ss:off ps:30 rn:2/1 10.10.10.218:2470 10.10.9.200:2372
17:52:55     idle station    4001 cid 0xdc
17:53:10 TRACE COMPLETE station 4001  cid 0x0
```

The following example illustrates an **Avaya VPNremote phone Extension 4018**, **IP Address 10.10.9.218** on the **OUTSIDE network** calling **Extension 4001, IP telephone IP Address 10.10.10.200** in the **INSIDE network.**

```
list trace station 4018                                          Page   1

                                LIST TRACE

time            data
17:26:35   rcv GRQ endpt 14.1.1.161:49302 switch 10.10.9.90:1719 ext 4018
17:26:35   snd GCF endpt 14.1.1.161:49302 switch 10.10.9.90:1719 ext 4018
17:27:53   rcv GRQ endpt 10.10.10.218:49300 switch 10.10.9.90:1719 ext 4018
17:27:53   snd GCF endpt 10.10.10.218:49300 switch 10.10.9.90:1719 ext 4018
17:27:53   rcv RRQ endpt 10.10.10.218:49300 switch 10.10.9.90:1719 ext 4018
17:27:53   snd RCF endpt 10.10.10.218:49300 switch 10.10.9.90:1719 ext 4018
17:27:54   TCP connected (fe)   endpt:10.10.10.218:4544 switch:10.10.9.90:1720
17:27:54   Q.931 Setup received endpt:10.10.10.218:4544 switch:10.10.9.90:1720
17:27:54   Q.931 CallProc sent  endpt:10.10.10.218:4544 switch:10.10.9.90:1720
17:27:54   Q.931 Connect sent   endpt:10.10.10.218:4544 switch:10.10.9.90:1720
17:34:23     active station    4018 cid 0xd2
17:34:23     G729A ss:off ps:30 rn:2/1 10.10.10.218:2470 10.10.9.91:2050
17:34:25     dial 4001
17:34:25     ring station    4001 cid 0xd2
17:34:39     idle station    4018 cid 0xd2
17:34:44     active station    4018 cid 0xd4
17:34:44     G729A ss:off ps:30 rn:2/1 10.10.10.218:2470 10.10.9.91:2056

17:34:46     dial 4001
17:34:46     ring station    4001 cid 0xd4
17:34:56     idle station    4018 cid 0xd4
17:35:04     active station    4018 cid 0xd5
17:35:04     G729A ss:off ps:30 rn:2/1 10.10.10.218:2470 10.10.9.91:2060
17:35:06     dial 4001
17:35:06     ring station    4001 cid 0xd5
17:35:06     G711MU ss:off ps:20 rn:1/1 10.10.9.200:2372 10.10.9.91:2054
17:35:07     active station    4001 cid 0xd5
17:35:07     G729A ss:off ps:30 rn:2/1 10.10.10.218:2470 10.10.9.200:2372
17:35:07     G729A ss:off ps:30 rn:1/2 10.10.9.200:2372 10.10.10.218:2470
17:39:34     idle station    4018 cid 0xd5
```

The following example illustrates **Avaya VPNremote phone Extension 4018**, **IP address 10.10.10.218** in **OUTSIDE network** calling another **Avaya VPNremote phone Extension 4022 IP Address 10.10.10.222** in the **OUTSIDE network.**

```
list trace station 4018

                                LIST TRACE

time            data

18:13:29     idle station    4018 cid 0xe4
18:13:32     active station    4018 cid 0xe6
18:13:32     G729A ss:off ps:30 rn:2/1 10.10.10.218:2470 10.10.9.91:2050
18:13:36     dial 4022
18:13:36     ring station    4022 cid 0xe6
18:13:36     G729A ss:off ps:30 rn:2/1 10.10.10.222:2388 10.10.9.91:2052
18:13:41     active station    4022 cid 0xe6
18:13:41     G729A ss:off ps:30 rn:2/2 10.10.10.218:2470 10.10.10.222:2388
18:13:41     G729A ss:off ps:30 rn:2/2 10.10.10.222:2388 10.10.10.218:2470
18:15:53     idle station    4018 cid 0xe6
18:15:58 TRACE COMPLETE station 4018  cid 0x0
```

8. Conclusion

These Application Notes have described the administrative steps required to configure the Cisco 2821 Integrated Services Router to support an Avaya VPNremote phone solution.

9. References

This section references the product documentation relevant to these Application Notes. Avaya Application Notes and additional resources can be found at the Avaya Product Support web site, at: http://support.avaya.com.

1. ***Avaya VPNremote for the 4600 Series IP Telephones Release 2.1 Administrator Guide,*** Doc ID: 19-600753, Issue 3, June 2007
2. ***Avaya VPNremote for 46xx Series IP Telephone Installation and Deployment Guide****,* Doc ID: 1022006
3. ***Avaya VPNremote for 4600 Series IP Telephone Installation and Configuration Quick Start,*** Doc ID: 19-601608, Issue 2, June 2007
4. ***Administration for the Avaya G450 Media Gateway,*** *Doc ID:* 03-602055, Issue 1, January 2008
5. ***Administrators Guide for Avaya Communication Manager****, Doc ID: 03-300509*, Issue 4.0, Release 5.0 January 2008
6. ***Avaya Application Notes A Sample Configuration using Cisco Catalyst 3750E-24PD to Provide Power over Ethernet to Avaya IP Telephones ,*** Issue 1.0

Cisco Product Support can be found at:http://www.cisco.com

7. ***Cisco 2800 Series Integrated Services Routers Quick Start Guide.*** Ref. 78-16015-07
8. ***Cisco 2821 ISR Basic Software Configuration Using the Cisco IOS Command-Line Interface*****"** Ref.OL-5593-01
9. ***Cisco IOS Security Configuration Guide Rel 12.4 Book, Updated Dec***
10. ***Cisco IOS Security Command Reference, July 2009 avai*****lable**
11. ***Cisco Router and Security Device Manager User's Guide,*** Ver.2.5***,*** Ref OL-4015-12
12. ***Cisco Security Appliance Command Line Configuration Guide,*** Ver.8.*0*, Ref. OL-12172-03
13. ***Cisco Configuration Professional User Guide, Ver.1.4,*** Ref. OL-19185-01

Appendix A

ISR Command Line Configuration

The complete command line configuration of the ISR is provided below. This section provides the CLI generated running configuration of the Cisco 2821 ISR used in the sample network. The following VPN elements of the ISR are configured to support Avaya VPNremote Phone:

- VPN Tunnel Group
- Pre-shared Key
- User Authentication
- IP Address Pool
- Security Associations
- IPSec Encryption and Authentication Algorithms

```
User Access Verification

Username: cisco
Password:

2821_vpn#sho run
Building configuration...

Current configuration : 3501 bytes
!
version 12.4
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname 2821_vpn
!
boot-start-marker
boot-end-marker
!
logging message-counter syslog
logging buffered 51200 warnings
!
aaa new-model
!
!
aaa authentication login userauthen local
aaa authorization network groupauthor local
!
!
aaa session-id common
!
dot11 syslog
ip source-route
!
```

```
!
ip cef
!
!
ip address-pool local
!
multilink bundle-name authenticated
!
!
!
!
!
!
username mike privilege 15 password 0 mike1234
username john privilege 15 password 0 john1234
username cisco privilege 15 password 0 cisco
username noel privilege 15 password 0 noel1234
username ravi privilege 15 password 0 ravi1234
archive
 log config
  hidekeys
!
!
crypto isakmp policy 3
 encr 3des
 authentication pre-share
 group 2
crypto isakmp key key456 address 10.10.10.218
crypto isakmp key key789 address 10.10.10.222
crypto isakmp key key123 address 10.10.10.223
!
crypto isakmp client configuration group myclient
 key key123
 dns 14.1.1.10
 wins 14.1.1.20
 domain mydomain.com
 pool blackpool
 acl 101
 netmask 255.255.255.0
!
crypto isakmp client configuration group myclient1
 key key456
 dns 14.1.1.10
 wins 14.1.1.20
 domain mydomain.com
 pool blackpool
 acl 101
 netmask 255.255.255.0
!
crypto isakmp client configuration group myclient2
 key key789
 dns 14.1.1.10
 wins 14.1.1.20
 domain mydomain.com
 pool blackpool
```

```
 acl 101
 netmask 255.255.255.0
!
crypto ipsec security-association lifetime seconds 86400
!
crypto ipsec transform-set myset esp-3des esp-sha-hmac
!
crypto ipsec profile vpnclient
 set security-association idle-time 86400 default
 set transform-set myset
!
!
crypto dynamic-map mydynmap 10
 set transform-set myset
 reverse-route
!
!
crypto map clientmap client authentication list userauthen
crypto map clientmap isakmp authorization list groupauthor
crypto map clientmap client configuration address initiate
crypto map clientmap client configuration address respond
crypto map clientmap 20 ipsec-isakmp
 set peer 10.10.9.1
 set transform-set myset
 match address 101
crypto map clientmap 100 ipsec-isakmp dynamic mydynmap
!
!
!
!
!
!
interface GigabitEthernet0/0
 description INSIDE
 ip address 10.10.9.1 255.255.255.0
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 duplex auto
 speed auto
 no mop enabled
!
interface GigabitEthernet0/1
 description OUTSIDE
 ip address 10.10.10.1 255.255.255.0
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 duplex auto
 speed auto
 no mop enabled
 crypto map clientmap
!
ip local pool blackpool 14.1.1.100 14.1.1.200
ip default-gateway 10.10.10.1
```

```
no ip forward-protocol nd
no ip forward-protocol udp
ip http server
ip http authentication local
no ip http secure-server
ip http timeout-policy idle 600 life 86400 requests 10000
!
!
!
logging source-interface GigabitEthernet0/1
logging 10.10.10.1
access-list 23 permit any log
access-list 101 permit ip 10.10.10.0 0.0.0.255 10.10.9.0 0.0.0.255 log
access-list 102 deny   ip 10.10.10.0 0.0.0.255 10.10.9.0 0.0.0.255 log
access-list 102 permit ip 10.10.10.0 0.0.0.255 any log
access-list 199 deny   ip any any log
access-list 199 permit ip any 10.10.9.0 0.0.0.255 log
!
!
!
!
!
control-plane
!
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 access-class 23 in
 privilege level 15
 transport input all
line vty 5 15
 access-class 23 in
 privilege level 15
 transport input all
!
scheduler allocate 20000 1000
end

2821_vpn#
```

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