**Avaya Solution & Interoperability Test Lab**

# Configuring an Avaya G250 Media Gateway as a VPN IKE Responder for a Cisco 877 Access Router and an Avaya G350 Media Gateway – Issue 1.0

## Abstract

These Application Notes present the steps necessary to configure an Avaya G250 Media Gateway as a VPN IKE responder, and a Cisco 877 Access Router and an Avaya G350 Media Gateways as VPN IKE initiators. The Avaya G250 Media Gateway is configured to accept a dynamic VPN connection based on the Fully Qualified Domain Name (FQDN) identities of remote peers. Configuration for PPP over Ethernet (PPPoE) and ADSL over POTS are also covered for the Cisco 877 Access Router and Avaya G350 Media Gateway.

# 1 Introduction

The network diagram in **Figure 1** shows three offices. The Main Office contains an Avaya G250-DS1 Media Gateway configured as an Access Router and an Avaya S8500 Media Server with an Avaya G650 Media Gateway. Remote Office 1 contains a Cisco 877 Access Router with an Avaya IP telephone. Remote Office 2 contains an Avaya G350 Media Gateway configured as an Access Router. The Avaya G250-DS1 Media Gateway, the Cisco 877 Access Router and the Avaya G350 Media Gateway are configured as VPN appliances.

Refer to [1] for detailed configuration of the Avaya Voice over IP devices including Avaya S8500 Media Server, Avaya Media Gateways and Avaya IP telephones.

In **Figure 1**, the Avaya G250-DS1 Media Gateway in the Main Office is configured as a VPN IKE responder. The Cisco 877 Access Router in Remote Office 1 and the Avaya G350 Media Gateway in Remote Office 2 are configured as IKE initiators. In the sample configuration, Remote Office 1 and Remote Office 2 access the Internet using Asymmetric Digital Subscriber Line (ADSL) over Plain Old Telephone Service (POTS). The Main Office is connected to the Internet over an Ethernet connection. These Application Notes provide detailed configuration for the VPN connection and ADSL access.

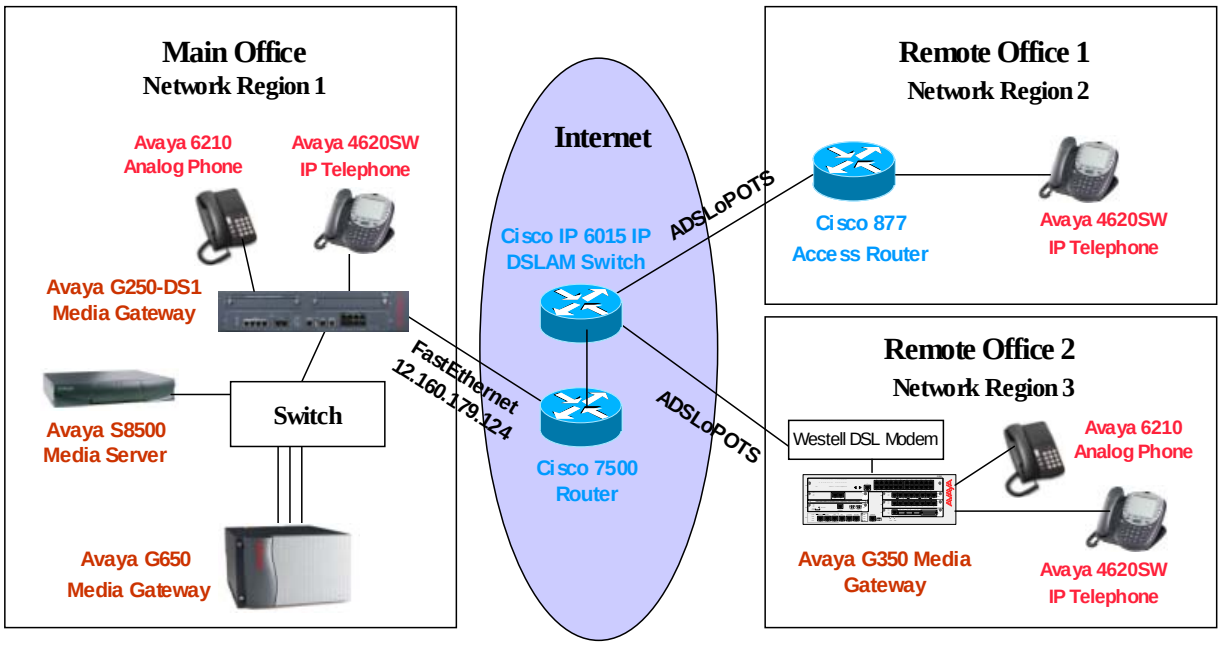



**Figure 1: Network Configuration**

# 2 Equipment and Software Validated

**Table 1** below shows the versions verified in these Application Notes.

| Equipment | Software |
|---|---|
| Avaya Communication Manager<br>Avaya S8500 Media Server | <br>3.1 (load 626) |
| Avaya G650 Media Gateway<br>IPSI (TN2312BP)<br>C-LAN (TN799DP)<br>MEDPRO (TN2302AP) | <br>HW12 FW021<br>HW01 FW016<br>HW11 FW108 |
| Avaya G250-DS1 Media Gateway | 25.22.0 |
| Avaya G350 Media Gateway | 25.22.0 |
| Avaya 4620SW IP Telephone | 2.30 |
| Cisco 877 Access Router | 12.3(8)YI2 |
| Cisco 6015 IP DSLAM Switch | 12.2(12)DA |
| Cisco 7500 Router | 12.2(32) |
| Westell 2200 DSL Modem | 01.06.53 |
| Avaya 6210 Analog Phone | N/A |

**Table 1: Equipment and Software Validated**

# 3 Configurations

Based on the IPSec standard, IKE protocol is used to negotiate the IPSec Security Associations (SAs). The negotiation process requires that the IPSec systems authenticate themselves to each other and establish Internet Security Association and Key Management Protocol (ISAKMP), or IKE, shared keys. In IKE phase 1, IKE creates an authenticated secure channel between the two IKE peers referred to as the IKE Security Association. In IKE phase 2, IKE negotiates the IPSec security associations and generates the required key material for IPSec.

IKE phase 1 occurs in two modes, the IKE main mode and the IKE aggressive mode. The IKE main mode has three two-way exchanges between the initiator and receiver, and the IKE aggressive mode has fewer exchanges with fewer packets than the main mode. The aggressive mode is faster than the main mode, but is not as secure as the main mode. In the sample configuration, the Avaya G250-DS1 Media Gateway is configured as an IKE responder in the aggressive mode.

For a successful VPN tunnel connection, IKE phase 1 and phase 2 must be negotiated successfully between the two IKE peers.

For the sample configuration, the following IKE phase 1 security attributes were used all VPN peers:

- Encryption Algorithm: 3DES
- Hash Algorithm: SHA
- Diffie-Hellman Group: 2
- Pre-shared key

The following IKE phase 2 security attributes were used on all VPN peers in the sample configuration:

- Encryption Algorithm: 3DES-ESP
- Hash Algorithm: ESP-SHA-HMAC

## 3.1 Configure Avaya G250-DS1 Media Gateway In the Main Office

The following commands show the configuration of VLAN 1 and Interface FastEthernet 10/2. VLAN 1 is associated with network 192.168.88.0/24. This is a local network used by the Avaya G250-DS1 Media Gateway. The ETH WAN port on the G250-DS1 Media Gateway corresponds to interface FastEthernet 10/2 in the configuration. In the sample configuration, the ETH WAN port is connected to the Internet with a fixed public IP address 12.160.179.124.

```
interface Vlan 1
 icc-vlan
 ip address 192.168.88.4    255.255.255.0
 pmi
 exit
!
interface FastEthernet 10/2
 ip crypto-group 901
 ip address 12.160.179.124  255.255.255.0
 exit
```

Configure the default route to the Internet Gateway.

```
ip default-gateway 12.160.179.1
```

The following shows the IKE phase 1 policy configuration on the Avaya G250-DS1 Media Gateway. In the sample configuration, the Cisco 877 Access Router and the Avaya G350 Media Gateway share this policy. The IKE phase 1 proposal on the Avaya G350 Media Gateway and the Avaya G250-DS1 Media Gateway must match this policy for a successfully IKE negotiation.

```
crypto isakmp policy 1
 description "High Phase 1 Proposal"
 encryption 3des
 hash sha
 group 2
 authentication pre-share
```

The following shows the Internet Security Association and Key Management Protocol (ISAKMP) peer configuration on the Avaya G250-DS1 Media Gateway. The Avaya G250-DS1 Media Gateway is configured to identify a remote peer by its fully qualified domain name (FQDN). In the sample configuration, FQDN "**C870.vpn.avaya.com**" is used to identify the Cisco C877 Access Router and "**G350.vpn.avaya.com**" is used to identify the Avaya G350 Media Gateway. The Cisco C877 Access Router and the Avaya G350 Media Gateway must send their identities to match the configuration on the Avaya G250-DS1 Media Gateway.

By configuring "**initiate mode none"** for an ISAKMP peer configuration, the Avaya G250-DS1 Media Gateway acts as an IKE responder in an aggressive mode. That means that the Avaya G250-DS1 Media Gateway will not initiate IKE and only accept IKE initiation in an aggressive mode from that peer. For the sample configuration, the Avaya G250-DS1 Media Gateway acts as an IKE responder for the Cisco 877 Access Router and Avaya G350 Media Gateway.

```
crypto isakmp peer fqdn "C870.vpn.avaya.com"
 pre-shared-key ****
 isakmp-policy 1
 initiate mode none
 exit
!
crypto isakmp peer fqdn "G350.vpn.avaya.com"
 pre-shared-key ****
 isakmp-policy 1
 initiate mode none
 exit
```

The following creates an IKE phase 2 transform-set proposal.

```
crypto ipsec transform-set H2 esp-3des esp-sha-hmac
```

Use the **crypto map** command to associate an IKE phase 2 proposal to each remote peer.

```
crypto map 1
 set peer "C870.vpn.avaya.com"
 set transform-set H2
 exit
!
crypto map 2
 set peer "G350.vpn.avaya.com"
 set transform-set H2
 exit
```

The following commands configure a **crypto-list 901** to define the VPN traffic between the Avaya G250-DS1 Media Gateway and the remote peers. The source IP address and destination IP addresses must match the configuration on the Cisco C877 Access Router and the Avaya G350 Media Gateway.

```
ip crypto-list 901
 local-address FastEthernet 10/2.0
!
 ip-rule 1
  protect crypto map 1
  source-ip 192.168.0.0 0.0.127.255
  destination-ip 192.168.133.0 0.0.0.255
 exit

 ip-rule 2

  protect crypto map 2
  source-ip 192.168.0.0 0.0.127.255
  destination-ip 192.168.132.0 0.0.0.255
 exit
```

Apply the IP crypto-list to the public facing interface FastEthernet 10/2:

```
interface FastEthernet 10/2
 ip crypto-group 901
 ip address 12.160.179.124  255.255.255.0
 exit
```

## 3.2 Configure Avaya G350 Media Gateway In Remote Office 2

The Avaya G350 Media Gateway can be configured as a DHCP and TFTP server. Refer to [2] for detailed configuration. The DHCP configuration is shown below. VLAN 1 is associated with network 192.168.132.0/24. This is a local network used by the Avaya G350 Media Gateway and Avaya IP telephones in Remote Office 2.

```
ip dhcp-server
ip dhcp pool 1
 start-ip-addr 192.168.132.110
 end-ip-addr 192.168.132.120
 default-router 192.168.132.1
 option 176
  value ascii "MCIPADD=192.168.88.22"
 exit
exit
ip dhcp activate pool 1

interface Vlan 1
 icc-vlan
 ip address 192.168.132.1   255.255.255.0
 pmi
 exit
```

The Avaya G350 Media Gateway is connected to the Internet via a Westell DSL modem. The ETH WAN port on the Avaya G350 Media Gateway is connected to the Ethernet port on the DSL modem. In the sample configuration, the ETH WAN port is configured with PPPoE encapsulation and a dynamic IP address. The DSL modem is configured in a bridge mode to pass the PPPoE frames to the Cisco DSL Access Multiplexer (DSLAM) Switch.

The following shows the ETH WAN port configuration. The ETH WAN port on the Avaya G350 Media Gateway corresponds to interface FastEthernet 10/2 in the configuration. Encapsulation is configured to **pppoe** and CHAP is configured for PPP negotiation. Appropriate credentials (hostname and password) must be configured for successful PPP negotiation.

```
interface FastEthernet 10/2
 encapsulation  pppoe
 ip crypto-group 901
 mtu 1492
 ppp chap hostname "avaya"
 ppp chap password xxxx
 ip address negotiated
```

Configure the default route to the Internet.

```
ip default-gateway FastEthernet 10/2
```

The following shows the IKE phase 1 policy configuration. The IKE phase 1 proposal on the Avaya G350 Media Gateway and the Avaya G250-DS1 Media Gateway must match.

```
crypto isakmp policy 1
 description "High Phase 1 Proposal"
 encryption 3des
 hash sha
 group 2
 authentication pre-share
```

The following commands show the ISAKMP peer configuration with the Avaya G250-DS1 Media Gateway. The Avaya G350 Media Gateway is configured to initiate the IKE connection in an aggressive mode. Compared to a main mode, an aggressive mode eliminates several steps for the IKE negotiation. The Avaya G250-DS1 Media Gateway will respond in an aggressive mode to an IKE peer that initiates an aggressive mode. The Avaya G350 Media Gateway is configured with the self-identity "**G350.vpn.avaya.com**".

```
crypto isakmp peer address "12.160.179.124"
 pre-shared-key ****
 isakmp-policy 1
 self-identity fqdn "G350.vpn.avaya.com"
initiate mode aggressive
```

The following creates an IPSec Phase 2 transform-set proposal.

```
crypto ipsec transform-set H2 esp-3des esp-sha-hmac
```

Use the **crypto map** command to associate IPSec phase 2 proposal to a remote peer.

```
crypto map 1
 description "Phase 2 Proposal"
 set peer "12.160.179.124"
 set transform-set H2
```

The following commands configure a **crypto-list 901** to define the VPN traffic between the Avaya G350 Media Gateway and the Avaya G250-DS1 Media Gateway. The source IP address 192.168.132.0 with a wild card 0.0.0.255 defines a local network 192.168.132.0/24. The destination IP 192.168.0.0 with a wild card 0.0.127.255 defines networks 192.168.0.0/24 to 192.168.127.0/24 (in the Main Office).

```
ip crypto-list 901
 name "To-Cisco-Access-Router"
--type q to quit or space key to continue--
 local-address FastEthernet 10/2.0
!
 ip-rule 1
  protect crypto map 1
  source-ip 192.168.132.0 0.0.0.255
  destination-ip 192.168.0.0 0.0.127.255
```

Apply the IP crypto-list to the public facing interface FastEthernet 10/2:

```
interface FastEthernet 10/2
 encapsulation  pppoe
 ip crypto-group 901
 mtu 1492
 ppp chap hostname "avaya"
 ip address negotiated
```

## 3.3 Configure Cisco 877 Access Router in Remote Office 1

The following shows the configuration of VLAN 1. VLAN 1 is associated with network 192.168.133.0/24. This is a local network used by the Cisco 877 Access Router and the Avaya IP telephone in Remote Office 1.

```
interface Vlan1
 ip address 192.168.133.1 255.255.255.0
```

The Cisco 877 Access Router comes with an ADSLoPOTS interface. In the sample configuration, this interface is connected to the Cisco 6015 DSLAM Switch. The following shows the annotated ADSLoPOTS and dialer configuration. Interface Dialer 1 is associated with the ADSLoPOTS interface (Interface ATM 0.1) and is configured for PPP CHAP with the username and password.

```
! --- Configure the ADSLoPOTS interface to a dial-pool-number 1
! --- Configure pppoe client
! --- Configure atm0.1 in dialer pool 1

interface ATM0.1 point-to-point
 pvc 0/101
  pppoe-client dial-pool-number 1

 ! --- Configure Dialer 1 with PPP encapsulation with CHAP authentication

interface Dialer1
 ip address negotiated
 encapsulation ppp
 dialer pool 1
 no cdp enable
 ppp authentication chap callin
 ppp chap hostname avaya
 ppp chap password 0 1234
 crypto map G250-HUB
```

Configure the default router to the Internet (interface dialer 1). By configuring the default route to interface Dialer 1, interface Dialer 1 will be activated and become an interface facing the Internet (equivalent to interface FastEthernet 10/2 on the Avaya G250 Media Gateway in **Section 3.1**).

```
ip route 0.0.0.0 0.0.0.0 Dialer1
```

The following shows the annotated VPN configuration on the Cisco 877 Access Router.

```
! --- Configure IKE phase 1 policy

crypto isakmp policy 1
 encr 3des
 authentication pre-share
 group 2
!
! --- Configure IKE phase 1 in an aggressive mode
! --- Configure FQDN as its self identity for the IKE phase 1 initiation

crypto isakmp peer address 12.160.179.124
 set aggressive-mode password xxxx
 set aggressive-mode client-endpoint fqdn C870.vpn.avaya.com
!
! --- IKE phase 2 configuration

crypto ipsec transform-set H2 esp-3des esp-sha-hmac
!
! --- Crypto map configuration

crypto map G250-HUB 10 ipsec-isakmp
 set peer 12.160.179.124
 set transform-set H2
 match address 100
!
! --- Configure VPN traffic

access-list 100 permit ip 192.168.133.0 0.0.0.255 192.168.0.0 0.0.127.255
```

Apply crypto map **G250-HUB** to interface Dialer 1.

```
interface Dialer1
 ip address negotiated
 encapsulation ppp
 dialer pool 1
 no cdp enable
 ppp authentication chap callin
 ppp chap hostname avaya
 ppp chap password 0 1234
 crypto map G250-HUB
```

## 3.4 Configure Cisco 6015 IP DSLAM Switch

For the sample configuration, the Cisco 877 Access Router and the Westell DSL modem are ADSLoPOTS clients. Therefore, an ADSL over POTS line card must be used on the Cisco 6015 DSLAM Switch. Use the command "**show hardware**" to display hardware information. The following shows that the **ATUC-1-DMT8** line card is in slot 2. The **ATUC-1-DMT8** line card supports POTS access.

```
DSLAM#show hardware
Chassis Type: C6015
I/O Card: 6015-DS3/T1-IO

Slot 1 : ATUC-1-DMT8-I                          Slot 5 : EMPTY
Slot 2 : ATUC-1-DMT8                            Slot 6 : EMPTY
Slot 3 : EMPTY                                  Slot 7 : NI-2-DS3-T1E1
Slot 4 : STUC-8-TCPAM

Fan Module:  Present

Power Supply Module: 6015-PEM-DC
```

The ATM access is terminated on the Cisco 7500 Router in **Figure 1** through ATM trunk 0/1 interface (an OC-3 link). Refer to Cisco configuration guide for detailed information. As shown below, two PVCs are configured for the Cisco 877 Access Router and the Westell DSL modem.

```
interface ATM2/1
 no ip address
 no atm ilmi-keepalive
 atm pvc 0 100  interface  ATM0/1 0 100
!
interface ATM2/2
 no ip address
 no atm ilmi-keepalive
 atm pvc 0 101  interface  ATM0/1 0 101
!
```

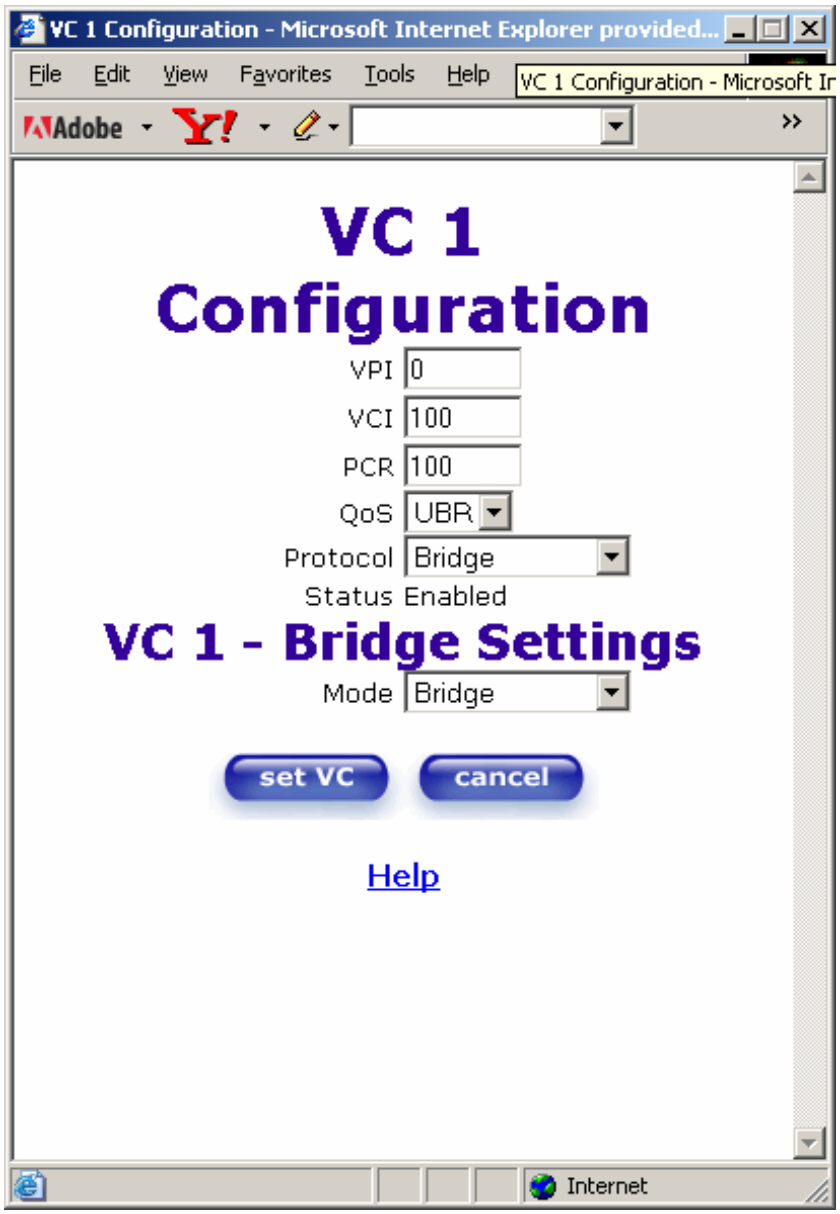
## 3.5 Configure Cisco 7500 Router

The Cisco 7500 Router is configured to terminate ATM access from the Cisco 6015 IP DSLAM Switch and provide dynamic IP addresses for the DSL clients. The following shows the annotated configuration. Refer to Cisco configuration guide for detailed information.

```
! --- Enable VPDN

vpdn enable
!
! --- Configure VPDN group to accept an incoming pppoe client

vpdn-group g250
 accept-dialin
  protocol pppoe
  virtual-template 1

! --- Terminate ATM PVCs on the ATM trunk 3/1

interface ATM3/1/0.1 point-to-point
 no ip route-cache
 no ip mroute-cache
 pvc 0/100
  encapsulation aal5snap
  protocol pppoe
 !
!
interface ATM3/1/0.2 point-to-point
 no ip route-cache
 no ip mroute-cache
 pvc 0/101
  encapsulation aal5snap
  protocol pppoe
 !

! --- Configure a virtual template for each pppoe session with PPP CHAP

interface Virtual-Template1
 mtu 1492
 ip address 10.8.8.1 255.255.255.0
 peer default ip address pool fast1
 ppp authentication pap chap

! --- Pool "fast1" is used to provide dynamic IP address for a DSL client

ip local pool fast1 10.8.8.100 10.8.8.105
```

## 3.6 Configure the Westell 2200 ADSL Modem

Refer to [3] for detailed configuration on the Westell 2200 ADSL Modem. In the sample configuration, the Westell 2200 ADSL Modem is configured in bridge mode so that the PPPoE frames from the Avaya G350 Media Gateway can be passed to the DSLAM Switch. In the sample configuration, VC 1 (a Virtual Circuit template) is used and configured with ATM VPI/VCI value 0/100 in Bridge Mode. The ATM VPI/VCI value must match the Cisco 6015 IP DSLAM Switch configuration in **Section 3.4**.



# 4 Verification Steps

## 4.1 Verify VPN Status On the Avaya G250-DS1 Media Gateway

Use the command **show crypto isakmp sa** on the Avaya G250-DS1 Media Gateway to display the current IKE SA. As shown in the following screen, the Avaya G350-DS1 Media Gateway and Cisco 877 Access router are identified by their FQDNs.

```
G250-DS1-002# show crypto isakmp sa

C-id Local           Remote          State   Encr    Hash Aut DH TTL   DPD Nat-T
---- --------------- --------------- ------- ------- ---- --- -- ----- --- -----
   3 12.160.179.124  10.8.8.101      Ready   3des    sha  psk  2  1210 Yes No
                     G350.vpn.avaya.com
  11 12.160.179.124  10.8.8.100      Ready   3des    sha  psk  2 84476 Yes No
                     C870.vpn.avaya.com
```

Use the command **show crypto ipsec sa** on the Avaya G250-DS1 Media Gateway to display the current IPSec status.

```
G250-DS1-002# show crypto ipsec sa

Interface: FastEthernet 10/2
 Crypto list id: 901, Local address: FastEthernet 10/2.0

  Rule: 1, Crypto map: 1
  Local address:   12.160.179.124
  Remote address: C870.vpn.avaya.com (10.8.8.100)
  Local identity:  192.168.0.0/255.255.128.0
  Remote identity: 192.168.133.0/255.255.255.0
  path mtu 1500, media mtu 1500, configured min PMTU 300
  Current outbound spi: 0x36662fd0

  Inbound packets                       Outbound packets
  ----------------------------------    ----------------------------------
  Total                          1020   Total                           972
    Total OK                     1020     Total OK                      972
      Decrypt                    1020       Encrypt                     972
      Verify                     1020       Digest                      972
      Decaps                     1020       Encaps                      972
    Total discards                  0     Total discards                  0

   SA Type         SPI        Transform     PFS Secs left  KB left    Mode

   --------------- ---------- ------------- --- ---------- ---------- ---------

   Outbound ESP    0x36662fd0 esp-3des      No        1498    4607982 Tunnel
                              esp-sha-hmac

   Inbound ESP     0x2a30     esp-3des      No        1498    4607984 Tunnel
                              esp-sha-hmac

================================================================================
```

```
  Rule: 2, Crypto map: 2
  Local address:   12.160.179.124
  Remote address: G350.vpn.avaya.com (10.8.8.101)
  Local identity:  192.168.0.0/255.255.128.0
  Remote identity: 192.168.132.0/255.255.255.0
  path mtu 1500, media mtu 1500, configured min PMTU 300
  Current outbound spi: 0x7a37

  Inbound packets                          Outbound packets
  ---------------------------------------  ---------------------------------------
  Total                            2933    Total                            2885
    Total OK                       2933      Total OK                       2884
      Decrypt                      2933        Encrypt                      2884
      Verify                       2933        Digest                       2884
      Decaps                       2933        Encaps                       2884
    Total discards                    0      Total discards                    1

   SA Type         SPI        Transform     PFS Secs left  KB left    Mode
   --------------- ---------- ------------- --- ---------- ---------- ---------
   Inbound ESP     0x5ff6     esp-3des      No        1257    4607907 Tunnel
                              esp-sha-hmac

   Outbound ESP    0x7a37     esp-3des      No        1257    4607909 Tunnel
                              esp-sha-hmac
```

Debugging can be enabled on the G250-DS1 to troubleshoot VPN issues. Enter the following commands from the console port to enable VPN debugging.

```
G250-DS1-002# set logging session condition isakmp debug
Done!
G250-DS1-002# set logging session condition ipsec debug
Done!
G250-DS1-002# set logging session enable
Done!
```

The following shows annotated syslog debug messages from the Avaya G250-DS1 Media Gateway:

```
! --- Avaya G250-DS1 receives IKE phase 1 initiation in a aggressive mode
! --- from the G350

02/02/2006,15:23:46:ISAKMP-Informational:
    Begin IKE phase 1 negotiation, initiated by 10.8.8.101:
       Peers 12.160.179.124<->10.8.8.101, mode aggressive


02/02/2006,15:23:46:ISAKMP-Debug:
    Received vendor ID from 10.8.8.101 (VID length = 16):
       Peers 12.160.179.124<->10.8.8.101
       Avaya Gateway VPN v1.0 (0x133bc1e3f926a020cad5bed4ffe04c8f)

! --- Avaya G250-DS1 receives IKE phase 1 proposal from the G350
```

```
02/02/2006,15:23:46:ISAKMP-Debug:
    Received vendor ID from 10.8.8.101 (VID length = 16):
       Peers 12.160.179.124<->10.8.8.101
       draft-ietf-ipsec-dpd-00.txt (0xafcad71368a1f1c96b8696fc77570100)

02/02/2006,15:23:46:ISAKMP-Debug:
    Received vendor ID from 10.8.8.101 (VID length = 16):
       Peers 12.160.179.124<->10.8.8.101
       Avaya VPNos v3.2 (0x4485152d18b6bbcc0be8a8469579ddcc)

02/02/2006,15:23:46:ISAKMP-Debug:
    Received vendor ID from 10.8.8.101 (VID length = 16):
       Peers 12.160.179.124<->10.8.8.101
       draft-ietf-ipsec-nat-t-ike-00 (0x4485152d18b6bbcd0be8a8469579ddcc)

02/02/2006,15:23:46:ISAKMP-Debug:
    Received vendor ID from 10.8.8.101 (VID length = 16):
       Peers 12.160.179.124<->10.8.8.101
       draft-ietf-ipsec-nat-t-ike-02 (0xcd60464335df21f87cfdb2fc68b6a448)

02/02/2006,15:23:46:ISAKMP-Debug:
    Received vendor ID from 10.8.8.101 (VID length = 16):
       Peers 12.160.179.124<->10.8.8.101
       draft-ietf-ipsec-nat-t-ike-02-ci (0x90cb80913ebb696e086381b5ec427b1f)

02/02/2006,15:23:46:ISAKMP-Debug:
    Received vendor ID from 10.8.8.101 (VID length = 16):
       Peers 12.160.179.124<->10.8.8.101
       draft-ietf-ipsec-nat-t-ike-03 (0x7d9419a65310ca6f2c179d9215529d56)

02/02/2006,15:23:46:ISAKMP-Debug:
    Received vendor ID from 10.8.8.101 (VID length = 16):
       Peers 12.160.179.124<->10.8.8.101
       RFC 3947 (0x4a131c81070358455c5728f20e95452f)

! --- Avaya G250-DS1 selects IKE phase 1 proposal (NAT-T)

02/02/2006,15:23:46:ISAKMP-Informational:
    Selected NAT-T draft:
       RFC 3947
       Peers 12.160.179.124<->10.8.8.101

02/02/2006,15:23:46:ISAKMP-Debug:
    Sending vendor ID to 10.8.8.101 (VID length = 16):
       Peers 12.160.179.124<->10.8.8.101
       draft-ietf-ipsec-dpd-00.txt (0xafcad71368a1f1c96b8696fc77570100)

02/02/2006,15:23:46:ISAKMP-Debug:
    Sending vendor ID to 10.8.8.101 (VID length = 16):
       Peers 12.160.179.124<->10.8.8.101
       RFC 3947 (0x4a131c81070358455c5728f20e95452f)


02/02/2006,15:23:46:ISAKMP-Informational:
    No NAT device was detected:
       Peers 12.160.179.124<->10.8.8.101

! ---Finished IKE phase 1 negotiation and create ISAKMP SA

02/02/2006,15:23:46:ISAKMP-Informational:
    Finished IKE phase 1 negotiation, creating ISAKMP SA:
       Peers  12.160.179.124<->10.8.8.101
```

```
       Icookie - 5146570ee05732ec, Rcookie - 5d5e59f9c952ffad
       esp-3des, esp-sha-hmac, DH group 2, Lifetime 86400 seconds
       DPD enabled

! --- Avaya G250-DS1 receives IKE phase 2 proposal from the G350

02/02/2006,15:23:46:ISAKMP-Informational:
    Begin IKE phase 2 negotiation, initiated by 10.8.8.101:
       Peers 12.160.179.124<->10.8.8.101

02/02/2006,15:23:46:IPSEC-Warning:
    Received invalid SPI from 10.8.8.101:
       SPI 0x3816, Peers 10.8.8.101<->12.160.179.124

! ---Finish IKE phase 2 and create inbound and outbound IPSEC SAs.

02/02/2006,15:23:46:ISAKMP-Informational:
    Finished IKE phase 2, creating outbound IPSEC SA:
       SPI 0x7191, Peers 12.160.179.124<->10.8.8.101
       Identities: 192.168.0.0/255.255.128.0->192.168.132.0/255.255.255.0
       esp-3des, esp-sha-hmac, 3600 seconds, 4608000 KB, No PFS
       Tunnel mode

02/02/2006,15:23:46:ISAKMP-Informational:
    Finished IKE phase 2, creating inbound IPSEC SA:
       SPI 0x3816, Peers 10.8.8.101<->12.160.179.124
       Identities: 192.168.132.0/255.255.255.0->192.168.0.0/255.255.128.0
       esp-3des, esp-sha-hmac, 3600 seconds, 4608000 KB, No PFS
       Tunnel mode

! --- Avaya G250-DS1 receives IKE phase 1 initiation in a aggressive mode
! --- from the Cisco 877 Access Router


02/02/2006,15:23:48:ISAKMP-Informational:
    Begin IKE phase 1 negotiation, initiated by 10.8.8.100:
       Peers 12.160.179.124<->10.8.8.100, mode aggressive

02/02/2006,15:23:48:ISAKMP-Debug:
    Received vendor ID from 10.8.8.100 (VID length = 16):
       Peers 12.160.179.124<->10.8.8.100
       Unknown (0x439b59f8ba676c4c7737ae22eab8f582)

! --- Avaya G250-DS1 receives IKE phase 1 proposal from the Cisco 877 Router

02/02/2006,15:23:48:ISAKMP-Debug:
    Received vendor ID from 10.8.8.100 (VID length = 16):
       Peers 12.160.179.124<->10.8.8.100
       draft-ietf-ipsec-nat-t-ike-03 (0x7d9419a65310ca6f2c179d9215529d56)

! --- Avaya G250-DS1 selects IKE phase 1 proposal (NAT-T)

02/02/2006,15:23:48:ISAKMP-Informational:
    Selected NAT-T draft:
       draft-ietf-ipsec-nat-t-ike-03
       Peers 12.160.179.124<->10.8.8.100

02/02/2006,15:23:48:ISAKMP-Debug:
    Sending vendor ID to 10.8.8.100 (VID length = 16):
       Peers 12.160.179.124<->10.8.8.100
       draft-ietf-ipsec-dpd-00.txt (0xafcad71368a1f1c96b8696fc77570100)
```

```
02/02/2006,15:23:49:ISAKMP-Debug:
    Sending vendor ID to 10.8.8.100 (VID length = 16):
       Peers 12.160.179.124<->10.8.8.100
       draft-ietf-ipsec-nat-t-ike-03 (0x7d9419a65310ca6f2c179d9215529d56)

02/02/2006,15:23:49:ISAKMP-Informational:
    Received IKE notify message:
       Type INITIAL_CONTACT (24578)
       Peers 12.160.179.124<->10.8.8.100
       Icookie - 48880c3efb519bcc, Rcookie - cb153a9ef3f4f8a9

02/02/2006,15:23:49:ISAKMP-Informational:
    No NAT device was detected:
       Peers 12.160.179.124<->10.8.8.100

! ---Finished IKE phase 1 negotiation and create ISAKMP SA

02/02/2006,15:23:49:ISAKMP-Informational:
    Finished IKE phase 1 negotiation, creating ISAKMP SA:
       Peers  12.160.179.124<->10.8.8.100
       Icookie - 48880c3efb519bcc, Rcookie - cb153a9ef3f4f8a9
       esp-3des, esp-sha-hmac, DH group 2, Lifetime 86400 seconds
       DPD enabled

! --- Avaya G250-DS1 receives IKE phase 2 from the Cisco 877 Access Router

02/02/2006,15:23:49:ISAKMP-Informational:
    Begin IKE phase 2 negotiation, initiated by 10.8.8.100:
       Peers 12.160.179.124<->10.8.8.100

02/02/2006,15:23:49:ISAKMP-Informational:
    Begin IKE phase 2 negotiation, initiated by 10.8.8.100:
       Peers 12.160.179.124<->10.8.8.100

! ---Finished IKE phase 2 and created inbound and outbound IPSEC SAs.

02/02/2006,15:23:49:ISAKMP-Informational:
    Finished IKE phase 2, creating outbound IPSEC SA:
       SPI 0xbf3dd82b, Peers 12.160.179.124<->10.8.8.100
       Identities: 192.168.0.0/255.255.128.0->192.168.133.0/255.255.255.0
       esp-3des, esp-sha-hmac, 3600 seconds, 4608000 KB, No PFS
       Tunnel mode

02/02/2006,15:23:49:ISAKMP-Informational:
    Finished IKE phase 2, creating inbound IPSEC SA:
       SPI 0x34f3, Peers 10.8.8.100<->12.160.179.124
       Identities: 192.168.133.0/255.255.255.0->192.168.0.0/255.255.128.0
       esp-3des, esp-sha-hmac, 3600 seconds, 4608000 KB, No PFS
       Tunnel mode
```

## 4.2 Verify VPN Status On the Avaya G350 Media Gateway

Use the command **show crypto isakmp sa** on the Avaya G350 Media Gateway to display the current IKE SA.

```
G350-003# show crypto isakmp sa

C-id Local           Remote          State   Encr    Hash Aut DH TTL   DPD Nat-T
---- --------------- --------------- ------- ------- ---- --- -- ----- --- -----
   1 10.8.8.101      12.160.179.124  Ready   3des    sha  psk  2   749 Yes No
```

Use the command **show crypto ipsec sa** on the Avaya G350 Media Gateway to display the current IPSec status.

```
G350-003# show crypto ipsec sa

Interface: FastEthernet 10/2
 Crypto list id: 901, Local address: FastEthernet 10/2.0
  Rule: 1, Crypto map: 1, "Phase 2 Proposal"
  Local address:   10.8.8.101
  Remote address: 12.160.179.124
  Local identity:  192.168.132.0/255.255.255.0
  Remote identity: 192.168.0.0/255.255.128.0
  path mtu 1492, media mtu 1492, configured min PMTU 300
  Current outbound spi: 0x5ff6
  Inbound packets                          Outbound packets
  ---------------------------------        ---------------------------------
  Total                          23977     Total                          24299
    Total OK                     23977       Total OK                     24218
      Decrypt                    23977         Encrypt                    24218
      Verify                     23977         Digest                     24218
      Decaps                     23977         Encaps                     24218
    Total discards                   0       Total discards                  81

   SA Type         SPI        Transform     PFS Secs left  KB left    Mode
   --------------- ---------- ------------- --- ---------- ---------- ---------
   Outbound ESP    0x5ff6     esp-3des      No         923    4607879 Tunnel
                              esp-sha-hmac

   Inbound ESP     0x7a37     esp-3des      No         923    4607878 Tunnel
                              esp-sha-hmac
```

Syslog debugging can be enabled on the G250-DS1 to troubleshoot VPN issues. Enter the following commands from the console port to enable VPN debugging.

```
G350-???# set logging session condition isakmp debug
Done!
G350-???# set logging session condition ipsec debug
Done!
G350-???# set logging session enable
Done!
```

The following shows annotated syslog debug messages from the Avaya G350 Media Gateway:

```
! --- Initiate IKE phase 1 with the G250-DS1 in an aggressive mode

02/03/2006,08:03:00:IPSEC-Informational:
    Call IKE negotiation for outgoing SPD entry 901_1:
       Peers 10.8.8.101<->12.160.179.124

02/03/2006,08:03:00:ISAKMP-Informational:
    Initiating IKE phase 1 negotiation:
       Peers 10.8.8.101<->12.160.179.124, mode aggressive

! --- Send IKE phase 1 proposals and self identity FQDN

02/03/2006,08:03:00:ISAKMP-Debug:
    Sending vendor ID to 12.160.179.124 (VID length = 16):
       Peers 10.8.8.101<->12.160.179.124
       Avaya Gateway VPN v1.0 (0x133bc1e3f926a020cad5bed4ffe04c8f)

02/03/2006,08:03:00:ISAKMP-Debug:
    Sending vendor ID to 12.160.179.124 (VID length = 16):
       Peers 10.8.8.101<->12.160.179.124
       draft-ietf-ipsec-dpd-00.txt (0xafcad71368a1f1c96b8696fc77570100)


02/03/2006,08:03:00:ISAKMP-Informational:
    Sending self identity FQDN "G350.vpn.avaya.com" in ID payload:
       Peers 10.8.8.101<->12.160.179.124

02/03/2006,08:03:00:ISAKMP-Debug:
    Sending vendor ID to 12.160.179.124 (VID length = 16):
       Peers 10.8.8.101<->12.160.179.124
       Avaya VPNos v3.2 (0x4485152d18b6bbcc0be8a8469579ddcc)

02/03/2006,08:03:00:ISAKMP-Debug:
    Sending vendor ID to 12.160.179.124 (VID length = 16):
       Peers 10.8.8.101<->12.160.179.124
       draft-ietf-ipsec-nat-t-ike-00 (0x4485152d18b6bbcd0be8a8469579ddcc)

02/03/2006,08:03:00:ISAKMP-Debug:
    Sending vendor ID to 12.160.179.124 (VID length = 16):
       Peers 10.8.8.101<->12.160.179.124
       draft-ietf-ipsec-nat-t-ike-02 (0xcd60464335df21f87cfdb2fc68b6a448)

02/03/2006,08:03:00:ISAKMP-Debug:
    Sending vendor ID to 12.160.179.124 (VID length = 16):
       Peers 10.8.8.101<->12.160.179.124
       draft-ietf-ipsec-nat-t-ike-02-cisco (0x90cb80913ebb696e086381b5ec427b1f)

02/03/2006,08:03:00:ISAKMP-Debug:
    Sending vendor ID to 12.160.179.124 (VID length = 16):
       Peers 10.8.8.101<->12.160.179.124
       draft-ietf-ipsec-nat-t-ike-03 (0x7d9419a65310ca6f2c179d9215529d56)

02/03/2006,08:03:00:ISAKMP-Debug:
    Sending vendor ID to 12.160.179.124 (VID length = 16):
       Peers 10.8.8.101<->12.160.179.124
       RFC 3947 (0x4a131c81070358455c5728f20e95452f)
```

```
02/03/2006,08:03:01:ISAKMP-Debug:
    Received vendor ID from 12.160.179.124 (VID length = 16):
       Peers 10.8.8.101<->12.160.179.124
       draft-ietf-ipsec-dpd-00.txt (0xafcad71368a1f1c96b8696fc77570100)

02/03/2006,08:03:01:ISAKMP-Debug:
    Received vendor ID from 12.160.179.124 (VID length = 16):
       Peers 10.8.8.101<->12.160.179.124
       RFC 3947 (0x4a131c81070358455c5728f20e95452f)

! --- IKE phase 1 proposal was selected (NAT-T)

02/03/2006,08:03:01:ISAKMP-Informational:
    Selected NAT-T draft:
       RFC 3947
       Peers 10.8.8.101<->12.160.179.124

02/03/2006,08:03:01:ISAKMP-Informational:
    No NAT device was detected:
       Peers 10.8.8.101<->12.160.179.124

! ---Finished IKE phase 1 negotiation and create ISAKMP SA

02/03/2006,08:03:01:ISAKMP-Informational:
    Finished IKE phase 1 negotiation, creating ISAKMP SA:
       Peers  10.8.8.101<->12.160.179.124
       Icookie - 9a4d36818cac51e1, Rcookie - 3d3a8669b2196af2
       esp-3des, esp-sha-hmac, DH group 2, Lifetime 86400 seconds
       DPD enabled

! --- Initiate IKE phase 2 negotiation

02/03/2006,08:03:01:ISAKMP-Informational:
    Initiating IKE phase 2 negotiation:
       SPD entry - 901_1
       Peers 10.8.8.101<->12.160.179.124

! --- Finish IKE phase 2 negotiation
! --- Create inbound and outbound IPSEC SAs.


02/03/2006,08:03:01:ISAKMP-Informational:
    Finished IKE phase 2, creating outbound IPSEC SA:
       SPI 0x485e, Peers 10.8.8.101<->12.160.179.124
       Identities: 192.168.132.0/255.255.255.0->192.168.0.0/255.255.128.0
       esp-3des, esp-sha-hmac, 3600 seconds, 4608000 KB, No PFS
       Tunnel mode

02/03/2006,08:03:01:ISAKMP-Informational:
    Finished IKE phase 2, creating inbound IPSEC SA:
       SPI 0x3aca, Peers 12.160.179.124<->10.8.8.101
       Identities: 192.168.0.0/255.255.128.0->192.168.132.0/255.255.255.0
       esp-3des, esp-sha-hmac, 3600 seconds, 4608000 KB, No PFS
       Tunnel mode
```

## 4.3 Verify VPN Status on the Cisco 877 Access Router

Use the command **show crypto isakmp sa detail** on the Cisco 877 Access Router to display the current IKE SA.

```
C870#show crypto isakmp sa detail
Codes: C - IKE configuration mode, D - Dead Peer Detection
       K - Keepalives, N - NAT-traversal
       X - IKE Extended Authentication
       psk - Preshared key, rsig - RSA signature
       renc - RSA encryption

C-id  Local           Remote          I-VRF    Status Encr Hash Auth DH Lifetime
 Cap.
4     10.8.8.100      12.160.179.124           ACTIVE 3des sha  psk  2  23:16:29

       Connection-id:Engine-id =  4:2(hardware)
```

Use the command **show crypto ipsec sa** on the Cisco 877 Access Router to display the current IPSec status.

```
C870#show crypto ipsec sa

interface: Dialer1
    Crypto map tag: G250-HUB, local addr 10.8.8.100

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.133.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (192.168.0.0/255.255.128.0/0/0)
   current_peer 12.160.179.124 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 219, #pkts encrypt: 219, #pkts digest: 219
    #pkts decaps: 216, #pkts decrypt: 216, #pkts verify: 216
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 1, #recv errors 0

     local crypto endpt.: 10.8.8.100, remote crypto endpt.: 12.160.179.124
     path mtu 1500, ip mtu 1500
     current outbound spi: 0x2A30(10800)

     inbound esp sas:
      spi: 0x36662FD0(912666576)
        transform: esp-3des esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2001, flow_id: C87X_MBRD:1, crypto map: G250-HUB
        sa timing: remaining key lifetime (k/sec): (4463201/934)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE

     inbound ah sas:

     inbound pcp sas:
```

```
     outbound esp sas:
      spi: 0x2A30(10800)
        transform: esp-3des esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2002, flow_id: C87X_MBRD:2, crypto map: G250-HUB
        sa timing: remaining key lifetime (k/sec): (4463205/933)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE

     outbound ah sas:

     outbound pcp sas:

interface: Virtual-Access1
    Crypto map tag: G250-HUB, local addr 0.0.0.0

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.133.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (192.168.0.0/255.255.128.0/0/0)
   current_peer 12.160.179.124 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.: 0.0.0.0, remote crypto endpt.: 12.160.179.124
     path mtu 1500, ip mtu 1500
     current outbound spi: 0x0(0)

     inbound esp sas:

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:

     outbound ah sas:

     outbound pcp sas:
```

Enter the following commands on the Cisco Access Router to enable VPN debugging.

```
870#debug crypto isakmp sa
Crypto ISAKMP debugging is on

C870#debug crypto ipsec
Crypto IPSEC debugging is on
```

The following shows sample annotated debug messages from the Cisco 877 Access Router.

```
! ---Send IKE phase 1 proposal using its FQDN identity

*Mar 25 16:18:00.323: IPSEC(sa_request): ,
  (key eng. msg.) OUTBOUND local= 10.8.8.100, remote= 12.160.179.124,
    local_proxy= 192.168.133.0/255.255.255.0/0/0 (type=4),
    remote_proxy= 192.168.0.0/255.255.128.0/0/0 (type=4),
    protocol= ESP, transform= esp-3des esp-sha-hmac  (Tunnel),
    lifedur= 3600s and 4608000kb,
    spi= 0xA03923E6(2688099302), conn_id= 0, keysize= 0, flags= 0x400A
*Mar 25 16:18:00.323: ISAKMP: received ke message (1/1)
*Mar 25 16:18:00.323: ISAKMP:(0:0:N/A:0): SA request profile is (NULL)
*Mar 25 16:18:00.323: ISAKMP: Created a peer struct for 12.160.179.124, peer port 500
*Mar 25 16:18:00.323: ISAKMP: Locking peer struct 0x827F2334, IKE refcount 1 for
isakmp_initiator
*Mar 25 16:18:00.327: ISAKMP: local port 500, remote port 500
*Mar 25 16:18:00.327: ISAKMP: set new node 0 to QM_IDLE
*Mar 25 16:18:00.327: insert sa successfully sa = 824D7334
*Mar 25 16:18:00.327: ISAKMP:(0:0:N/A:0):SA has tunnel attributes set.
*Mar 25 16:18:00.327: ISAKMP:(0:0:N/A:0): constructed NAT-T vendor-07 ID
*Mar 25 16:18:00.327: ISAKMP:(0:0:N/A:0): constructed NAT-T vendor-03 ID
*Mar 25 16:18:00.327: ISAKMP:(0:0:N/A:0): constructed NAT-T vendor-02 ID
*Mar 25 16:18:00.359: ISAKMP:(0:10:HW:2):SA is doing pre-shared key authentication
using id type ID_FQDN
*Mar 25 16:18:00.359: ISAKMP (0:268435466): ID payload
                              next-payload : 13
                              type         : 2
                        FQDN name    : C870.vpn.avaya.com
                              protocol     : 17
                              port         : 0
                              length       : 26
*Mar 25 16:18:00.359: ISAKMP:(0:10:HW:2):Total payload length: 26
*Mar 25 16:18:00.359: ISAKMP:(0:10:HW:2):Input = IKE_MESG_FROM_IPSEC, IKE_SA_REQ_AM
*Mar 25 16:18:00.359: ISAKMP:(0:10:HW:2):Old State = IKE_READY  New State = IKE_I_AM1

! --- Begin IKE phase 1 initiation in an aggressive mode

*Mar 25 16:18:00.359: ISAKMP:(0:10:HW:2): beginning Aggressive Mode exchange
*Mar 25 16:18:00.359: ISAKMP:(0:10:HW:2): sending packet to 12.160.179.124 my_port
500 peer_port 500 (I) AG_INIT_EXCH
*Mar 25 16:18:00.763: ISAKMP (0:268435466): received packet from 12.160.179.124 dport
500 sport 500 Global (I) AG_INIT_EXCH
*Mar 25 16:18:00.763: ISAKMP:(0:10:HW:2): processing SA payload. message ID = 0
*Mar 25 16:18:00.763: ISAKMP:(0:10:HW:2): processing ID payload. message ID = 0
*Mar 25 16:18:00.763: ISAKMP (0:268435466): ID payload
                              next-payload : 8
                              type         : 1
                           address      : 12.160.179.124
                              protocol     : 0
                              port         : 0
                              length       : 12
*Mar 25 16:18:00.763: ISAKMP:(0:10:HW:2):: peer matches *none* of the profiles
*Mar 25 16:18:00.763: ISAKMP:(0:10:HW:2): processing vendor id payload
*Mar 25 16:18:00.763: ISAKMP:(0:10:HW:2): vendor ID is DPD
*Mar 25 16:18:00.763: ISAKMP:(0:10:HW:2):SA using tunnel password as pre-shared key.

! ---Match pre-shared key for the G250-DS1

*Mar 25 16:18:00.767: ISAKMP:(0:10:HW:2): local preshared key found
```

```
*Mar 25 16:18:00.767: ISAKMP : Scanning profiles for xauth ...
*Mar 25 16:18:00.767: ISAKMP:(0:10:HW:2):Checking ISAKMP transform 1 against priority
1 policy
*Mar 25 16:18:00.767: ISAKMP:      encryption 3DES-CBC
*Mar 25 16:18:00.767: ISAKMP:      hash SHA
*Mar 25 16:18:00.767: ISAKMP:      default group 2
*Mar 25 16:18:00.767: ISAKMP:      auth pre-share
*Mar 25 16:18:00.767: ISAKMP:      life type in seconds
*Mar 25 16:18:00.767: ISAKMP:      life duration (VPI) of  0x0 0x1 0x51 0x80

! --- Attributes for IKE phase 1 negotiation completed

*Mar 25 16:18:00.767: ISAKMP:(0:10:HW:2):atts are acceptable. Next payload is 0
*Mar 25 16:18:00.767: ISAKMP:(0:10:HW:2): processing vendor id payload
*Mar 25 16:18:00.767: ISAKMP:(0:10:HW:2): vendor ID is DPD
*Mar 25 16:18:00.767: ISAKMP:(0:10:HW:2): processing KE payload. message ID = 0
*Mar 25 16:18:00.799: ISAKMP:(0:10:HW:2): processing NONCE payload. message ID = 0
*Mar 25 16:18:00.799: ISAKMP:(0:10:HW:2):SA using tunnel password as pre-shared key.
*Mar 25 16:18:00.799: ISAKMP:(0:10:HW:2):SKEYID state generated
*Mar 25 16:18:00.799: ISAKMP:(0:10:HW:2): processing HASH payload. message ID = 0
*Mar 25 16:18:00.799: ISAKMP:(0:10:HW:2): processing vendor id payload
*Mar 25 16:18:00.799: ISAKMP:(0:10:HW:2): vendor ID seems Unity/DPD but major 157
mismatch
*Mar 25 16:18:00.799: ISAKMP:(0:10:HW:2): vendor ID is NAT-T v3
*Mar 25 16:18:00.803: ISAKMP:received payload type 20
*Mar 25 16:18:00.803: ISAKMP:received payload type 20

! --- Finished phase 1 negotiation

*Mar 25 16:18:00.803: ISAKMP:(0:10:HW:2):SA authentication status: authenticated
*Mar 25 16:18:00.803: ISAKMP:(0:10:HW:2):SA has been authenticated with
12.160.179.124
*Mar 25 16:18:00.803: ISAKMP: Trying to insert a peer 10.8.8.100/12.160.179.124/500/,
and inserted successfully 827F2334.
*Mar 25 16:18:00.803: ISAKMP:(0:10:HW:2):Send initial contact
*Mar 25 16:18:00.803: ISAKMP:(0:10:HW:2): sending packet to 12.160.179.124 my_port
500 peer_port 500 (I) AG_INIT_EXCH
*Mar 25 16:18:00.803: ISAKMP:(0:10:HW:2):Input = IKE_MESG_FROM_PEER, IKE_AM_EXCH
*Mar 25 16:18:00.803: ISAKMP:(0:10:HW:2):Old State = IKE_I_AM1  New State =
IKE_P1_COMPLETE

*Mar 25 16:18:00.807: ISAKMP:(0:10:HW:2):beginning Quick Mode exchange, M-ID of
318640706
*Mar 25 16:18:00.807: ISAKMP:(0:10:HW:2): sending packet to 12.160.179.124 my_port
500 peer_port 500 (I) QM_IDLE
*Mar 25 16:18:00.811: ISAKMP:(0:10:HW:2):Node 318640706, Input = IKE_MESG_INTERNAL,
IKE_INIT_QM
*Mar 25 16:18:00.811: ISAKMP:(0:10:HW:2):Old State = IKE_QM_READY  New State =
IKE_QM_I_QM1
*Mar 25 16:18:00.811: ISAKMP:(0:10:HW:2):Input = IKE_MESG_INTERNAL,
IKE_PHASE1_COMPLETE
*Mar 25 16:18:00.811: ISAKMP:(0:10:HW:2):Old State = IKE_P1_COMPLETE  New State =
IKE_P1_COMPLETE

*Mar 25 16:18:00.915: ISAKMP (0:268435466): received packet from 12.160.179.124 dport
500 sport 500 Global (I) QM_IDLE
*Mar 25 16:18:00.915: ISAKMP:(0:10:HW:2): processing HASH payload. message ID =
318640706
*Mar 25 16:18:00.915: ISAKMP:(0:10:HW:2): processing SA payload. message ID =
318640706

*Mar 25 16:18:00.915: ISAKMP:(0:10:HW:2):Checking IPSec proposal 1
```

```
*Mar 25 16:18:00.915: ISAKMP: transform 1, ESP_3DES
*Mar 25 16:18:00.915: ISAKMP:   attributes in transform:
*Mar 25 16:18:00.915: ISAKMP:      encaps is 1 (Tunnel)
*Mar 25 16:18:00.915: ISAKMP:      SA life type in seconds
*Mar 25 16:18:00.915: ISAKMP:      SA life duration (basic) of 3600
*Mar 25 16:18:00.915: ISAKMP:      SA life type in kilobytes
*Mar 25 16:18:00.915: ISAKMP:      SA life duration (VPI) of  0x0 0x46 0x50 0x0
*Mar 25 16:18:00.915: ISAKMP:      authenticator is HMAC-SHA
*Mar 25 16:18:00.915: ISAKMP:(0:10:HW:2):atts are acceptable.

! --- Send IKE phase 2 proposal to the G250-DS1 Media Gateway

*Mar 25 16:18:00.919: IPSEC(validate_proposal_request): proposal part #1,
  (key eng. msg.) INBOUND local= 10.8.8.100, remote= 12.160.179.124,
    local_proxy= 192.168.133.0/255.255.255.0/0/0 (type=4),
    remote_proxy= 192.168.0.0/255.255.128.0/0/0 (type=4),
    protocol= ESP, transform= esp-3des esp-sha-hmac  (Tunnel),
    lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2
*Mar 25 16:18:00.919: Crypto mapdb : proxy_match
                        src addr     : 192.168.133.0
                         dst addr     : 192.168.0.0
                              protocol     : 0
                              src port     : 0
                              dst port     : 0
*Mar 25 16:18:00.919: ISAKMP:(0:10:HW:2): processing NONCE payload. message ID =
318640706
*Mar 25 16:18:00.919: ISAKMP:(0:10:HW:2): processing ID payload. message ID =
318640706
*Mar 25 16:18:00.919: ISAKMP:(0:10:HW:2): processing ID payload. message ID =
318640706
*Mar 25 16:18:00.923: ISAKMP: Locking peer struct 0x827F2334, IPSEC refcount 1 for
for stuff_ke

! --- Finished phase 2. Create inbound and outbound IPSec SAs

*Mar 25 16:18:00.923: ISAKMP:(0:10:HW:2): Creating IPSec SAs
*Mar 25 16:18:00.923:         inbound SA from 12.160.179.124 to 10.8.8.100 (f/i)  0/
0
        (proxy 192.168.0.0 to 192.168.133.0)
*Mar 25 16:18:00.923:         has spi 0xA03923E6 and conn_id 0 and flags 2
*Mar 25 16:18:00.923:         lifetime of 3600 seconds
*Mar 25 16:18:00.923:         lifetime of 4608000 kilobytes
*Mar 25 16:18:00.923:         has client flags 0x0
*Mar 25 16:18:00.923:         outbound SA from 10.8.8.100 to 12.160.179.124 (f/i) 0/0
        (proxy 192.168.133.0 to 192.168.0.0)
*Mar 25 16:18:00.923:         has spi 25216 and conn_id 0 and flags A
*Mar 25 16:18:00.923:         lifetime of 3600 seconds
*Mar 25 16:18:00.923:         lifetime of 4608000 kilobytes
*Mar 25 16:18:00.923:         has client flags 0x0
*Mar 25 16:18:00.923: IPSEC(key_engine): got a queue event with 2 kei messages
*Mar 25 16:18:00.923: IPSEC(initialize_sas): ,
  (key eng. msg.) INBOUND local= 10.8.8.100, remote= 12.160.179.124,
    local_proxy= 192.168.133.0/255.255.255.0/0/0 (type=4),
    remote_proxy= 192.168.0.0/255.255.128.0/0/0 (type=4),
    protocol= ESP, transform= esp-3des esp-sha-hmac  (Tunnel),
    lifedur= 3600s and 4608000kb,
    spi= 0xA03923E6(2688099302), conn_id= 0, keysize= 0, flags= 0x2
*Mar 25 16:18:00.927: IPSEC(initialize_sas): ,
  (key eng. msg.) OUTBOUND local= 10.8.8.100, remote= 12.160.179.124,
    local_proxy= 192.168.133.0/255.255.255.0/0/0 (type=4),
    remote_proxy= 192.168.0.0/255.255.128.0/0/0 (type=4),
```

```
    protocol= ESP, transform= esp-3des esp-sha-hmac  (Tunnel),
    lifedur= 3600s and 4608000kb,
    spi= 0x6280(25216), conn_id= 0, keysize= 0, flags= 0xA
*Mar 25 16:18:00.927: Crypto mapdb : proxy_match
                        src addr     : 192.168.133.0
                         dst addr     : 192.168.0.0
                              protocol     : 0
                              src port     : 0
                              dst port     : 0
*Mar 25 16:18:00.927: IPSEC(crypto_ipsec_sa_find_ident_head): reconnecting with the
same proxies and 130.107.221.76
*Mar 25 16:18:00.927: IPSec: Flow_switching Allocated flow for sibling 80000019
*Mar 25 16:18:00.927: IPSEC(policy_db_add_ident): src 192.168.133.0, dest
192.168.0.0, dest_port 0

*Mar 25 16:18:00.927: IPSEC(create_sa): sa created,
  (sa) sa_dest= 10.8.8.100, sa_proto= 50,
    sa_spi= 0xA03923E6(2688099302),
    sa_trans= esp-3des esp-sha-hmac , sa_conn_id= 2004
*Mar 25 16:18:00.927: IPSEC(create_sa): sa created,
  (sa) sa_dest= 12.160.179.124, sa_proto= 50,
    sa_spi= 0x6280(25216),
    sa_trans= esp-3des esp-sha-hmac , sa_conn_id= 2003
```

## 4.4 Verify Avaya Voice over IP Operation

Use the command **show mgc** on the Avaya G350 Media Gateway in Office 2 to verify that the Avaya G350 Media Gateway has been registered to Avaya Communication Manager successfully. 192.168.88.22 is the C-LAN IP address of the Avaya G650 Media Gateway in the Main Office.

```
G350-003# show mgc

CALL CONTROLLER STATUS
------------------------------------------
Registered          : YES
Active Controller   : 192.168.88.22
H248 Link Status    : UP
H248 Link Error Code: 0x0

CONFIGURED MGC HOST
--------------------
192.168.88.22
-- Not Available --
-- Not Available --
-- Not Available --
```

If a call is made between Remote Offices 1 and 2, the called phone will ring, but there is no media path. This is because there is no IP connection between Remote Offices 1 and 2. The following are suggested to address this issue:

- Configure another VPN tunnel between Remote Offices 1 and 2 so that Remote Offices 1 and 2 can communicate with each other through the VPN tunnel between them. Note that this cannot be used in the sample configuration since both endpoints have dynamic IP addresses.

- Configure Generic Routing Encapsulation (GRE) over VPN tunnels with IP routing between the Main Office and the two remote offices. Remote Offices 1 and 2 can then communicate with each other via the Main Office. Refer to [4] for detailed configuration for GRE over IPSec VPN.

- Disable direct Media Path between Remote Offices 1 and 2 so that the Media Path between Remote Offices 1 and 2 goes through the Main Office. As shown in **Figure 1**, Network Regions 1, 2 and 3 are assigned for each office. Use the command **change ip-network-region 2** from Avaya Communication Manager to leave the Codec Set blank between Network Regions 2 and 3 since there is IP connection between them. Use the command **change ip-network-region 1** to configure the Codec Set used between Network Regions 1 and 2, and between Network Regions 1 and 3. In the sample configuration, Codec G.729 is configured for Codec Set 2 to save bandwidth.

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

                   Inter Network Region Connection Management

 src dst  codec  direct                                          Dynamic CAC
 rgn  rgn    set      WAN      WAN-BW-limits   Intervening-regions      Gateway
IGAR
 2   1     2       y           :NoLimit                                    n
 2   2     1
 2   3
```

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

                   Inter Network Region Connection Management

 src dst  codec  direct                                          Dynamic CAC
 rgn  rgn    set      WAN      WAN-BW-limits   Intervening-regions      Gateway
IGAR
 1   1     1
 1   2     2       y           :NoLimit                                    n
 1   3     2       y           :NoLimit                                    n
```

Make a call between the Main Office and Remote Office 1, and between the Main Office and Remote Office 2 and use the command **status station <station #>** to verify that the call is IP direct. The following screen shows that the Media Path is IP-direct between two phones.

```
status station 30000                                          Page   5 of   6
                      SRC PORT TO DEST PORT TALKPATH
src port: S00011
S00011:TX:192.168.132.110:2660/g729a/20ms
S00005:RX:192.168.88.54:25830/g729a/20ms
```

Make a call between Remote Offices 1 and 2, use the command **status station <station #>** to verify that the Media Path goes through the Main Office. The following screen shows that the Media Path goes through the Main Office (192.168.88.21 is the IP address of the MEDPRO in the Main Office).

```
status station 30000
                      SRC PORT TO DEST PORT TALKPATH
src port: S00011
S00011:TX:192.168.132.110:2660/g729ab/20ms
003V037:RX:192.168.132.1:2052/g729b/20ms   TX:ctxID:11
003V038:RX:ctxID:11   TX:192.168.132.1:2050/g729/20ms
01A0308:RX:192.168.88.21:17172/g729/20ms   TX:tdm:a72
01A0301:RX:tdm:a72   TX:192.168.88.21:17168/g729a/20ms
S00003:RX:192.168.133.2:8164/g729a/20ms
```

# 5 Conclusion

As illustrated in these Application Notes, an Avaya G250-DS1 can be configured as a VPN IKE responder in an aggressive mode, and Cisco 877 Access Router and Avaya G350 Media Gateways as VPN IKE initiators. The Avaya G250-DS1 Media Gateway can be configured to accept a dynamic VPN connection based on the FQDN identities of remote peers. The Avaya G350 Media Gateway can be configured with PPPoE encapsulation and PPP CHAP authentication to access the Internet over a DSL modem.

# 6 Additional References

The following Applications Notes can be found at http://www.avaya.com.


[1] *Configuring Avaya Communication Manager with Inter-Gateway Alternate Routing (IGAR) and Call Administration Control-Bandwidth Limit (CAC-BL) Features*

[2] *Configuring DHCP and TFTP Servers on Avaya G350 and G250 Media Gateways for Avaya IP 4600 Series Telephones*

*[3] A Configuration of Avaya IP Office with the Westell 2200 ADSL Modem for Internet Access and Voice over IP Virtual Private Networking*

*[4] Configuring a Generic Routing Encapsulation (GRE) Tunnel Over IPSec VPN Using Transport Mode with Open Shortest Path First (OSPF) Routing Protocol between an Avaya G250 Media Gateway and a Cisco Access Router*


# 7. Glossary

| Technical Term | Definition as it pertains to this document |
|---|---|
| **ADSL** | Asymmetric Digital Subscriber Line |
| **POTS** | Plain Old Telephone Service |
| **DSLAM** | DSL Access Multiplexer |
| **VPDN** | Virtual Private Dialup Network |
| **IKE** | Internet Key Exchange |
| **ISAKMP** | Internet Security Association and Key Management Protocol |
| **FQDN** | Fully Qualified Domain Name |

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