**Avaya Solution & Interoperability Test Lab**

# Configuring VPN Tunnels Using the WAN Module on Avaya G350 Media Gateways Controlled by Avaya S8700 Media Servers and Avaya G600 Media Gateways – Issue 1.0

## Abstract

These Application Notes present a sample configuration of a VPN tunnel using the WAN module on the Avaya G350 Media Gateway with the Avaya SG203 Security Gateway. A Cisco PIX and an access router are used in the main office. The Avaya S8700 Media Servers and Avaya G600 Media Gateways in the main office control the Avaya G350 Media Gateway in the small office. These Application Notes focus on how to configure the Avaya G350 Media Gateway working with the Avaya SG203 Security Gateway for providing the Virtual Private Network (VPN) and Firewall services, and do not cover WAN, Avaya S8700 Media Servers, etc.

# 1. Introduction

The network diagram in **Figure 1** shows two offices. The office labeled "Main Office" uses Avaya Communication Manager, Avaya S8700 Media Servers, and Avaya G600 Media Gateway. The office labeled "Small Office" contains an Avaya G350 Media Gateway with an Avaya S8300 Media Server, configured as a Local Survivable Processor (LSP).

In the main office, a Cisco 3640 access router is used for the WAN access while a Cisco Catalyst 6509 is used for the LAN access. Cisco PIX is located between the Cisco access router and the Cisco Catalyst 6509 to provide the Virtual Private Network (VPN) and Firewall services. In the small office, the Avaya G350 Media Gateway is used for WAN and LAN access while the Avaya SG203 Security Gateway provides VPN service. Since the Avaya G350 Media Gateway is connected to the Internet, it must be configured to provide FW service for its local networks and the Avaya SG203 Security Gateway.

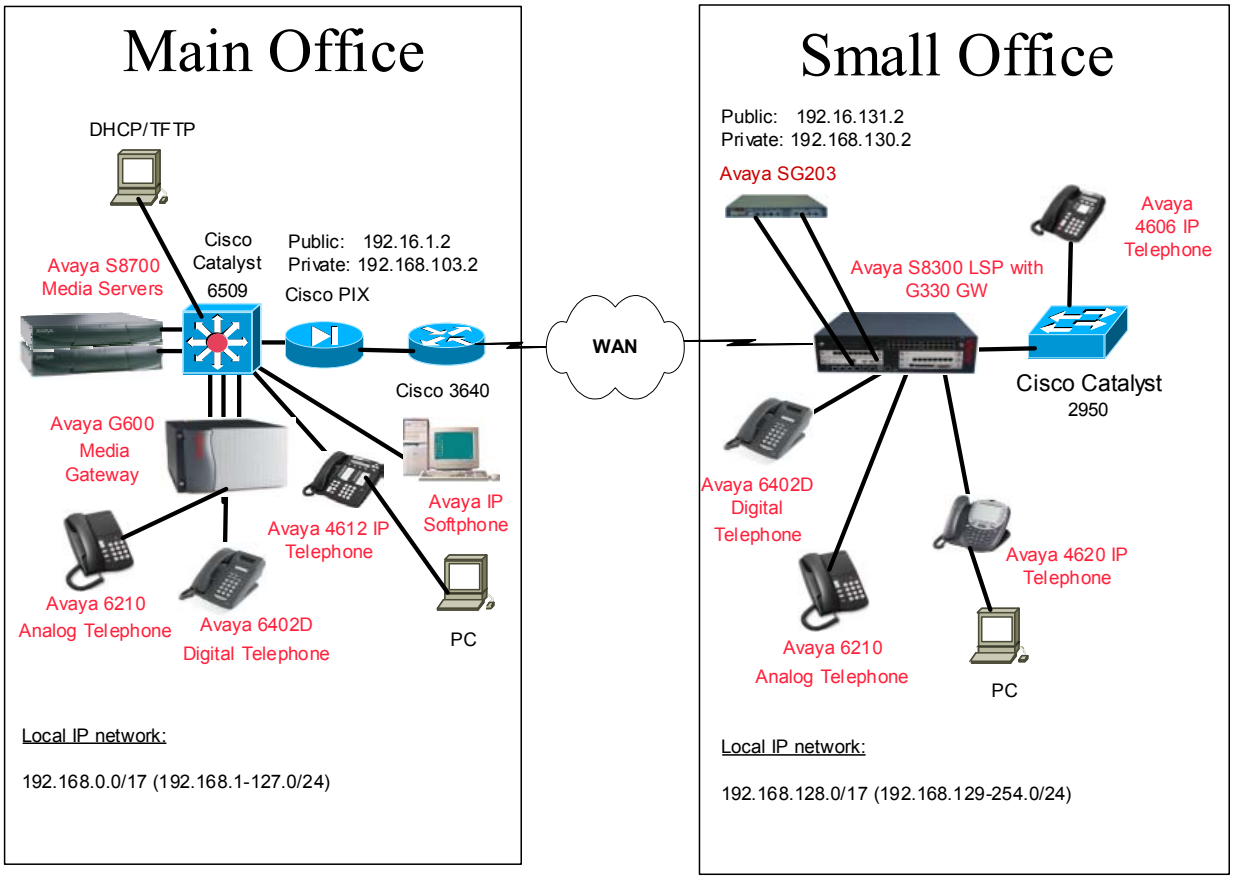


**Figure 1: Network Configuration**

# 2. Equipment and Software Validated

**Table 1** below shows the versions used for these Application Notes.

| Equipment | Software |
|---|---|
| Avaya Communication Manager<br>Avaya S8700 Media Server<br>Avaya S8300 Media Server LSP | <br>R012x.00.0.215.0<br>R012x.00.0.215.0 |
| Avaya G600 Media Gateway<br>IPSI (TN2312AP)<br>C-LAN (TN799DP)<br>MEDPRO (TN2302AP) | <br>HW32 FW005<br>HW00 FW010<br>HW03 FW055 |
| Avaya G350 Media Gateway | 21.16.1 |
| Avaya IP telephones | 1.81 |
| Avaya IP Softphones | 4.1.3.28 |
| Avaya SG203 Security Gateway | 4.31.26 |
| Cisco 3640 Access Router | IOS 12.2(19) |
| Cisco Catalyst 6509 Switch<br>Layer 2<br>Layer 3 | <br>7.6(1)<br>12.1(16)E6 |
| Cisco Catalyst 2950 Switch | IOS 12.0 (5.3) WC (1) |
| Cisco PIX 525 | 6.1(2) |

**Table 1: Software Versions**

# 3. Configurations

Refer to reference [1] for configuring Avaya S8700 Media Servers and Avaya G600 Media Gateways Controlling Avaya G350 Media Gateways. Refer to reference [2] for VPN configuration on Avaya Security Gateway and Cisco PIX. These Application Notes focus on how to configure the Avaya G350 Media Gateway to work with the Avaya Security Gateway for providing the VPN/FW services. Note that the public IP addresses of the SG203 and the Cisco PIX must be replaced in real scenarios.

## 3.1. Configuring Avaya SG203 Security Gateway

Configure the Avaya SG203 Security Gateway with the following IP parameters:

Public IP: 192.16.131.2
Default Gateway: 192.16.131.1
Private IP: 192.168.130.2
Static Route: 192.168.128.0/17 with next hop 192.168.130.1

Note that 192.168.128.0 with the netmask 255.255.128.0 is a super net covering all the local networks configured on the Avaya G350 Media Gateway. 192.16.131.1 is a public IP address (Internet accessible) while 192.168.130.1 is the local IP address (a private network) configured on the G350 Media Gateway.

Configure the Avaya SG203 Security Gateway with the following parameters for the VPN configuration.

Local IP Groups: 192.168.128.0/17
Member Remote TEPs: 192.16.1.2
IP Groups for 192.16.1.2: 192.168.0.0/17

Note that 192.168.0.0 with the netmask 255.255.128.0 is a super net covering all the local networks configured on the Cisco Catalyst 6509. 192.16.1.2 is a public IP address (Internet accessible) on the Cisco PIX.

## 3.2. Configuring Avaya G350 Media Gateways

### 3.2.1. Configuring static routes on the Avaya G350 Media Gateway to support the Avaya SG203 Security Gateway

The public port of the Avaya SG203 Security Gateway in **Figure 1** is connected to the Ethernet WAN port of the Avaya G350 Media Gateway, which is identified as FastEthernet 10/2. This interface is configured with an IP address 192.16.131.1. A serial interface 5/1 on the Avaya G350 Media Gateway is used for the WAN access and this interface is also configured as the default gateway. In order to force all the VPN traffic to go through the Avaya SG203 Security Gateway, static routes must be configured to the private interface of the Avaya SG203 Security Gateway for the VPN traffic. These configurations are shown below.

```
interface Vlan 1
 icc-vlan
 ip address 192.168.129.1   255.255.255.0
 pmi
 ip bootp-dhcp server 192.168.89.5
 exit
!
interface Vlan 2
 ip address 192.168.130.1   255.255.255.0
 ip bootp-dhcp server 192.168.89.5
 exit
!
interface FastEthernet 10/2
 ip address 192.16.131.1    255.255.255.0
 exit
!
interface Serial 5/1
 encapsulation ppp
 ip access-group 301 in
 ip access-group 302 out
 ip address 192.16.101.2    255.255.255.0
 exit

ip default-gateway Serial 5/1      1 low
ip route   192.168.0.0     255.255.128.0   192.168.130.2   1 low
```

### 3.2.2. Configuring Firewall service on the Avaya G350 Media Gateway

Because the Avaya G350 Media Gateway is an integrated WAN and LAN device, an IP access control list must be configured on its WAN interface to protect its local networks and the Avaya SG203 Security Gateway. Note that the Avaya SG203 Security Gateway cannot protect these local networks although it can provide FW services on its public and private interfaces.

The following shows the configuration for an IP access control list 301, which is applied to the WAN interface serial 5/1 for the incoming traffic. Note that only the following VPN protocols destined for the public interface of the Avaya SG203 Security Gateway are opened for Internet access. The default rule is to deny all traffic.

IKE-IN: UDP port 500
IKE-AVAYA-IN: UDP 4500
IPSEC-NAT-IN: UDP 2700
AH: IP Protocol 51
ESP: IP Protocol 50

Refer to the Avaya Security Gateway Configuration Guide for detailed information.

```
ip access-control-list 301
 name "list #301"
!
 ip-rule 1
  ip-protocol udp
  destination-ip host 192.16.131.2
  udp destination-port eq Ike
 exit
 ip-rule 2
  ip-protocol udp
  destination-ip host 192.16.131.2
  udp destination-port eq 2070
 exit
 ip-rule 3
  ip-protocol udp
  destination-ip host 192.16.131.2
  udp destination-port eq 4500
 exit
 ip-rule 4
  ip-protocol esp
  destination-ip host 192.16.131.2
 exit
 ip-rule 5
  ip-protocol ah
  destination-ip host 192.16.131.2
 exit
 ip-rule default
  composite-operation "Deny"
 exit
```

A similar reversed IP access control list 302 is configured for the outgoing traffic. Use the command **show ip access-control-list** to verify these configurations.

```
G350-001(super)# show ip access-control-list 301

Index Name                            Owner
----- ------------------------------- --------------------------
301   list #301                       other

ip options: Permit
ip fragments : Permit

Index Protocol     IP               Wildcard        Port          Operation
----- -------- --- ---------------- --------------- ------------ ------------
--
1      udp     Src  Any                              Any          Permit
               Dst  192.16.131.2    Host             eq Ike
2      udp     Src  Any                              Any          Permit
               Dst  192.16.131.2    Host             eq 2070
3      udp     Src  Any                              Any          Permit
               Dst  192.16.131.2    Host             eq 4500
4      esp     Src  Any                              Any          Permit
               Dst  192.16.131.2    Host             Any
5      ah      Src  Any                              Any          Permit
               Dst  192.16.131.2    Host             Any
Deflt  Any     Src  Any                              Any          Deny
               Dst  Any                              Any
…
G350-001(super)# show ip access-control-list 302

Index Name                            Owner
----- ------------------------------- --------------------------
302   list #302                       other

ip options: Permit
ip fragments : Permit

Index Protocol     IP               Wildcard        Port          Operation
----- -------- --- ---------------- --------------- ------------ ------------
--
1      udp     Src  192.16.131.2    Host             eq Ike       Permit
               Dst  Any                              Any
2      udp     Src  192.16.131.2    Host             eq 2070      Permit
               Dst  Any                              Any
3      udp     Src  192.16.131.2    Host             eq 4500      Permit
               Dst  Any                              Any
4      esp     Src  192.16.131.2    Host             Any          Permit
               Dst  Any                              Any
5      ah      Src  192.16.131.2    Host             Any          Permit
               Dst  Any                              Any
Deflt  Any     Src  Any                              Any          Deny
               Dst  Any                              Any
…
```

The following shows how to apply the IP access control lists 301 and 302 to the serial interface 5/1:

```
G350-001(super)# interface Serial 5/1
G350-001(super-if:Serial 5/1)# ip access-group 301 in
Done!
G350-001(super-if:Serial 5/1)#
G350-001(super-if:Serial 5/1)# ip access-group 302 out
Done!
```

Use the command **show ip active-lists** to verify the configuration.

```
G350-001(super)# show ip active-lists 301

Interface Name                   Dir. Type Idx List Name
-------------------------------- ---- ---- --- ------------------------------
Serial 5/1                       In   ACL  301 list #301


G350-001(super)# show ip active-lists 302

Interface Name                   Dir. Type Idx List Name
-------------------------------- ---- ---- --- ------------------------------
Serial 5/1                       Out  ACL  302 list #302
```

## 3.3. Configuring Cisco PIX

The following shows the related Cisco PIX configuration using CLI.

```
!--- Fixup must be disabled for VoIP signals.
no fixup protocol h323 1720

!--- Access list for the VPN traffic to the SG203.
access-list SG203-tunnel permit ip 192.168.0.0 255.255.128.0 192.168.128.0
255.255.128.0

!--- Access list for the VoIP traffic to the SG203 without NAT.
access-list noNATtoSG permit ip 192.168.0.0 255.255.128.0 192.168.128.0
255.255.128.0

!--- IP address configuration for the PIX.
ip address outside 192.16.1.2 255.255.255.0
ip address inside 192.168.103.2 255.255.255.0

!--- Do not do NAT for the VoIP traffic to the SG203.
nat (inside) 0 access-list noNATtoSG

!--- Configure the default and static routes.
route outside 0.0.0.0 0.0.0.0 192.16.1.1 1
route inside 192.168.0.0 255.255.128.0 192.168.103.1 1

!--- Permit all inbound IPSec sessions.
sysopt connection permit-ipsec

!--- Define Ipsec encryption and authentication algorithms.
crypto ipsec transform-set SG203-Set esp-3des esp-sha-hmac

!--- Define crypto map.
crypto map mapforsgs 12 ipsec-isakmp
crypto map mapforsgs 12 match address SG203-tunnel
crypto map mapforsgs 12 set peer 192.16.131.2
crypto map mapforsgs 12 set transform-set SG203-Set

!--- Apply crypto map on the outside interface.
crypto map mapforsgs interface outside
isakmp enable outside

!--- Define pre-shared secret for IKE authentication.
isakmp key ******** address 192.16.131.2 netmask 255.255.255.255

!--- Define ISAKMP policy.
isakmp identity address
isakmp policy 11 authentication pre-share
isakmp policy 11 encryption 3des
isakmp policy 11 hash sha
isakmp policy 11 group 2
isakmp policy 11 lifetime 86400
…
```

# 4. Verification Steps

Verify the VPN configuration using the following procedures:

- Verify successful ping between the Avaya SG203 Security Gateway and Cisco PIX. If not, verify the IP routing. Note that the public interfaces of the Avaya SG203 Security Gateway and the Cisco PIX must be on the public networks, which are routable through the Internet.

- Apply the VPN configuration to the Avaya SG203 Security Gateway and the Cisco PIX. Verify that the VPN traffic between the main and small offices can get through. If not, refer to reference [2] for troubleshooting the VPN tunnel.

- Apply the IP access control lists on the Avaya G350 Media Gateway. Verify that the VPN traffic can get through. If not, verify that the IP access control lists are configured correctly for incoming and outgoing traffic.

- If the IP access list must be configured on the Cisco access router, apply it and verify that the VPN traffic can get through. If not, verify that the IP access control list is configured correctly on the Cisco access router.

- Follow the verification steps in Section 14 of reference [1] to ensure that the VoIP traffic can get through the VPN tunnel.

# 5. Conclusion

As illustrated by these Application Notes, the Avaya G350 Media Gateway can be configured to work with an external Avaya SG203 Security Gateway to provide the WAN access as well as VPN/FW services for a small office. All the VoIP capacities can be supported through this VPN tunnel.

# 6. Additional References

Application Notes:


[1] Configuring Avaya Communication Manager for Avaya S8700 Media Servers and Avaya G600 Media Gateways Controlling Avaya G350 Media Gateways with Avaya S8300 Media Servers as Local Survivable Processors

[2] Configuring VPN backup for Avaya S8700 Media Servers and Avaya G600 Media Gateways Controlling Avaya G350 Media Gateways using Avaya Security Gateway and Cisco PIX

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