



---

## **A Sample VPN Tunnel Configuration Using Cisco 3640 and 7100 Routers for Avaya™ Media Servers and Media Gateways running Avaya MultiVantage™ Software - Issue 1.1**

### **Abstract**

These Application Notes outline the VPN configurations on Cisco 3640 and 7100 routers to protect the VoIP traffic for Avaya™ Media Servers, Gateways, and IP endpoints. The test scenarios will cover a Site-to-Site VPN tunnel between Cisco 3640 and 7100 VPN routers and a dynamic tunnel between an Avaya™ IP Softphone with a Cisco 3640 router.

# 1. Introduction

A Virtual Private Network (VPN) provides a mechanism to protect a company's communication channels when using the public network infrastructure. A VPN can employ the same security, management, and quality of service policies applied in a private network. Benefits of using VPNs include cost savings and extending connectivity to telecommuters, mobile users and remote offices.

These Application Notes illustrate implementations of Avaya VoIP in VPN environments and show configurations for creating a Site-to-Site VPN tunnel as well as a dynamic VPN tunnel for remote users using Cisco routers. The equipment used in this configuration includes Cisco 3640 and 7100 routers with VPN Acceleration module, Avaya™ S8700 Media Server, Avaya™ S8300 Media Server, Avaya™ G600 and Avaya™ G700 Media Gateways, and Avaya™ IP Telephones and Avaya™ IP Softphones.

The network in **Figure 1** was used to verify that a Site-to-Site VPN Tunnel can be established to carry VoIP traffic using a simulated public network via a T1 link. The network in **Figure 2** was used to verify that a dynamic VPN tunnel can be set up by an Avaya IP Softphone to communicate with both Avaya S8700 and Avaya 8300 Media Servers.

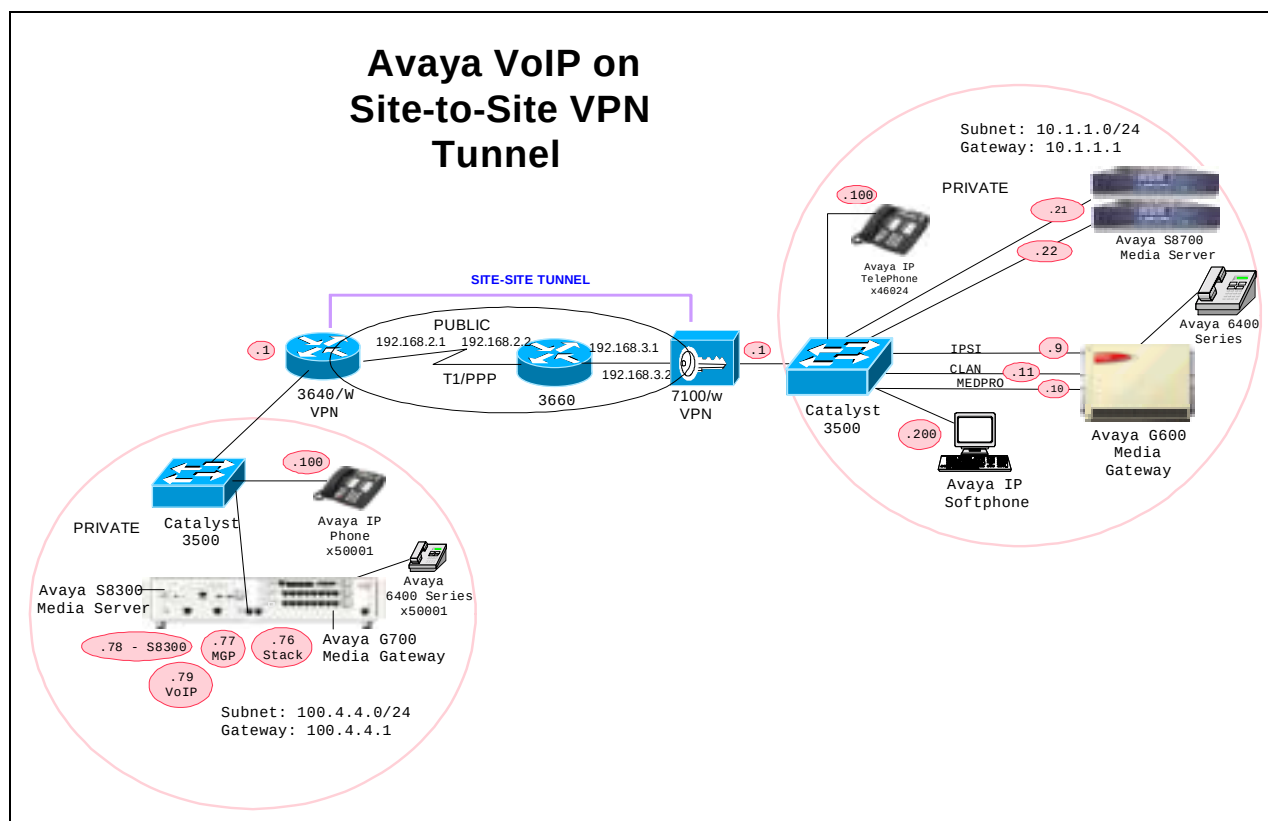


**Figure 1: Avaya VoIP Configuration using Site-to-Site VPN Tunnel**

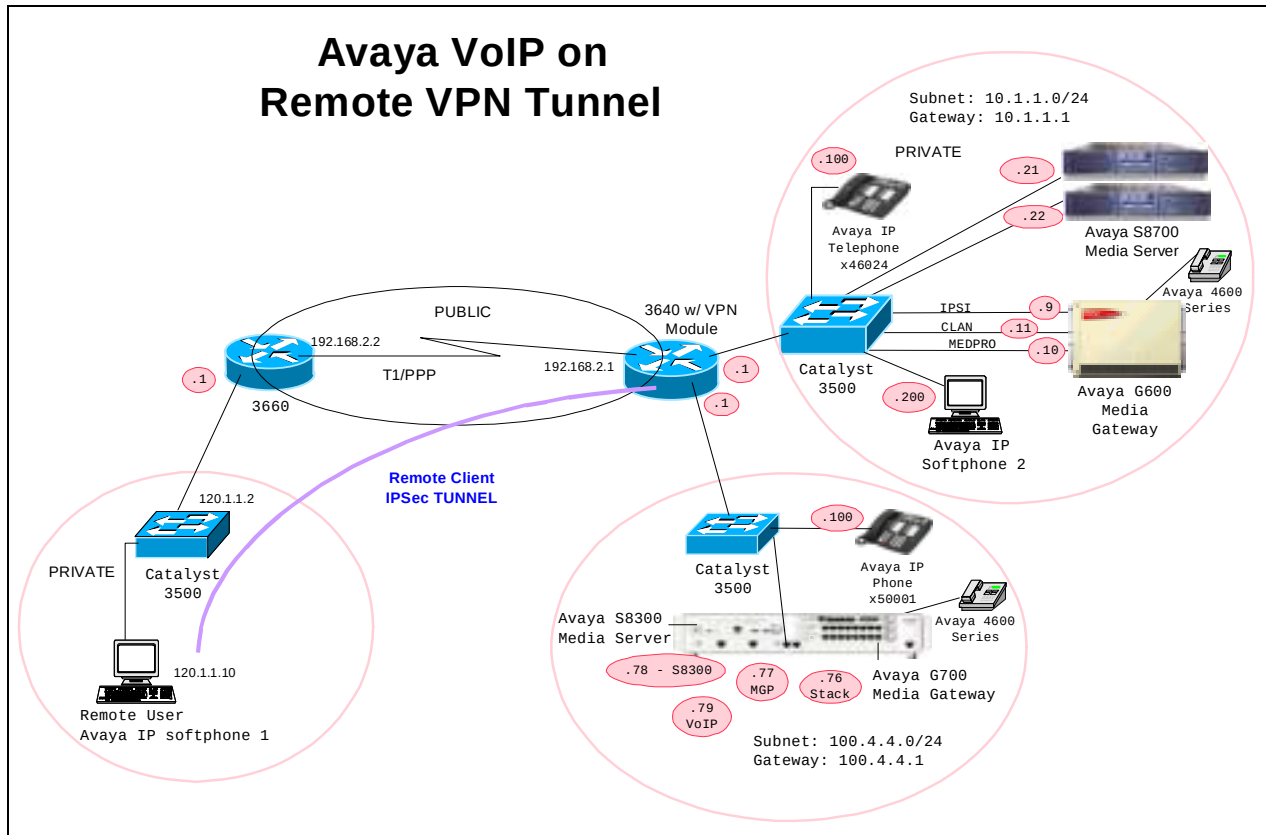


**Figure 2: Network Topology for Remote Client VPN Tunnel**

## 2. Equipment and Software Validated

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

| Equipment                                                | Software         |
|----------------------------------------------------------|------------------|
| Avaya™ S8300 Media Server with Avaya™ G700 Media Gateway | R011x.02.0.110.4 |
| Avaya™ S8700 Media Server with Avaya™ G600 Media Gateway | R011x.02.0.110.4 |
| Avaya MultiVantage™ Software                             | R011x.02.0.110.4 |
| Avaya™ 4612 IP Telephone                                 | Version 1.669    |

|                                       |                    |
|---------------------------------------|--------------------|
| Avaya™ IP Softphone                   | Version 4.1.3.6    |
| Cisco 7100 VPN Router with VPN Module | Version 12.1(5c)E9 |
| Cisco 3640 Router with VPN Module     | IOS 12.2(13)T      |
| Cisco 3660 Router                     | IOS 12.1(5)T9      |
| Cisco Catalyst 3500XL switch          | IOS 12.1(9)EA1C    |
| Cisco Secure VPN Client               | Version 1.1 (3DES) |

## 3. Configuration

Before configuring the VPN features on the routers, make sure that the network connectivity has been set up and IP endpoints from both sides can call each other via the T1 link. For detailed configurations, please refer to the Avaya MultiVantage Configuration Guide. The Site-to-Site VPN tunnel will be configured between the Cisco 3640 and Cisco 7100 routers' T1 interfaces. All VoIP traffic between these two sites is protected by this tunnel.

### 3.1. Site-to-Site VPN Tunnel Configuration

#### 3.1.1. Cisco 3640 Router Configuration

```

version 12.2
hostname C3640
!
enable password cisco
!
ip subnet-zero
!

crypto isakmp policy 1           (Creating an Internet Security Association and Key Management
hash md5                     Protocol policy for phase 1 negotiations for the LAN-to-LAN tunnel)
authentication pre-share

! (Specify the PreShared key for the LAN-to-LAN tunnel and define the peer interface IP address)

crypto isakmp key 12345678901234567890 address 192.168.3.2

!
! (Create the phase 2 policy for actual data encryption and create transform-set vpn-1)

crypto ipsec transform-set vpn-1 esp-des esp-md5-hmac
!
! (Create the actual crypto map and specify a local address – physical interface – to be used for the IPsec traffic. )

crypto map mymap local-address Serial0/0

! (Configure the crypto map to use IKE to establish SAs. Use sequence number 1 and IKE for crypto map mymap)
crypto map mymap 1 ipsec-isakmp
set peer 192.168.3.2           (Specify a remote IPsec peer by its IP address)
set transform-set vpn-1       (Specify using transform-set vpn-1)

```

```

match address 101                                (Traffic matched by access-list 101 will be protected by IPSec.)
!
call rsvp-sync
!
interface FastEthernet0/0
ip address 100.4.4.1 255.255.255.0
ip helper-address 10.3.3.6
no ip mroute-cache
speed 100
full-duplex
!
interface Serial0/0
ip address 192.168.2.1 255.255.255.0
encapsulation ppp
no ip mroute-cache
service-module t1 clock source internal
crypto map mymap                                (Apply the crypto map set to the physical interface)
!
router RIP
version 2
network 100.4.4.0
network 192.168.2.0
!
ip classless

! (Creating an access-list 101 to protect traffic from network 100.4.4.0 to 10.1.1.0 and deny RIP routing protocol using IPSec.)

access-list 101 deny udp any eq RIP any
access-list 101 deny udp any any eq RIP
access-list 101 permit ip 100.4.4.0 0.0.0.255 10.1.1.0 0.0.0.255
!
end

```

### 3.1.2. Cisco 7100 Router Configuration

```

version 12.1
hostname 7100-VPN
!

crypto isakmp policy 1                            (Creating an Internet Security Association and Key Management Protocol policy for phase 1 negotiations for the LAN-to-LAN tunnel)
hash md5
authentication pre-share

! (Specify the PreShared key for the LAN-to-LAN tunnel and define the peer interface IP address)

crypto isakmp key 12345678901234567890 address 192.168.2.1
!
! (Create the phase 2 policy for actual data encryption and create transform-set vpn-1)

crypto ipsec transform-set vpn-1 esp-des esp-md5-hmac

```

```

! (Create the actual crypto map and specify a local address – physical interface – to be used for
the IPsec traffic. )

crypto map mymap local-address FastEthernet0/1
!

! (Configure the crypto map to use IKE to establish SAs. Use sequence number 1 and IKE for crypto
map mymap)
crypto map mymap 1 ipsec-isakmp

set peer 192.168.2.1          (Specify a remote IPsec peer by its IP address)
set transform-set vpn-1      (Specify using transform-set vpn-1)
match address 101            (Traffic matched by access-list 101 will be protected by
                              IPsec.)
!

controller ISA 5/1
!

interface FastEthernet0/0
ip address 10.1.1.1 255.255.255.0
duplex full
speed 100
!
interface FastEthernet0/1
ip address 192.168.3.2 255.255.255.0
duplex full
speed 100
crypto map mymap          (Apply the crypto map set to the physical interface)
!
router RIP
version 2
network 10.0.0.0
network 192.168.3.0
!
ip classless
no ip http server
!

! (Creating an access-list 101 to protect traffic from network 10.1.1.0 to 100.4.4.0 and deny RIP
routing protocol using IPsec.)

access-list 101 deny  udp any eq RIP any
access-list 101 deny  udp any any eq RIP
access-list 101 permit ip 10.1.1.0 0.0.0.255 100.4.4.0 0.0.0.255
!
line con 0
transport input noneaux 0
line vty 0 4
password cisco
login
line vty 5 15
login
!

```

```
end
```

## 3.2. Dynamic VPN Tunnel Configuration for Remote User

The dynamic VPN tunnel will be set up from Avaya IP Softphone1 to the Cisco 3640 VPN Router as shown in **Figure 2**. All traffic between Avaya IP Softphones and the Avaya Media Gateway will be protected by this VPN tunnel.

### 3.2.1. Cisco 3640 Router Configuration

```
version 12.2
!
hostname C3640
!
enable secret 5 $1$pXro$dcYU3fgvKc93XrvdYQKLS.
enable password cisco
!
ip subnet-zero
!

! -- (Creating an Internet Security Association and Key Management Protocol policy for phase 1
      negotiations and specify using pre-shared key for user authentication for remote client)

crypto isakmp policy 5
 hash md5
 authentication pre-share
!

! (Specify the PreShared key for the remote client and define the wild card for all remote clients)

crypto isakmp key avaya123 address 0.0.0.0 0.0.0.0

!
! (Create the phase 2 policy for actual data encryption and create transform-set trans1.
  The tunnel mode is configured for trans1 for an IPSec encrypted tunnel.)

crypto ipsec transform-set trans1 esp-des esp-md5-hmac
 mode tunnel
!

! (Define a dynamic crypto map entry with dynamic map name dynmap and sequence number 5.
  Specify that IPSec Transform trans1 is applied to this dynamic map. Match address 101
  Command determines which traffic should or should not be protected by IPSec.)

crypto dynamic-map dynmap 5
 set transform-set trans1
 match address 101
!

! (Creating a crypto map mapclient with sequence number 5 and using IKE to establish SAs)

crypto map mapclient 5 ipsec-isakmp dynamic dynmap
```

*(Configure access-list 101 to protect traffic from Avaya IP Softphone1 to 100.4.4.0 and 10.1.1.0 network)*

```
access-list 101 permit ip 100.4.4.0 255.255.255.0 host 120.1.1.10
access-list 101 permit ip 10.1.1.0 255.255.255.0 host 120.1.1.10
!
call rsvp-sync
!
interface FastEthernet0/0
ip address 100.4.4.1 255.255.255.0
ip helper-address 10.3.3.6
no ip mroute-cache
speed 100
full-duplex
!

interface Serial 0/0
ip address 192.168.2.1 255.255.255.0
no ip mroute-cache
half-duplex
no mop enabled
crypto map mapclient (Apply the crypto map set mapclient to the physical interface and make this interface as a tunnel endpoint)
!
router RIP
version 2
network 100.4.4.0
network 110.0.0.0
network 192.168.2.0
!
ip classless
!
end
```

### 3.2.2. Cisco Secure VPN Client Configuration

Follow instructions to install the Secure VPN client on a PC or laptop running Windows NT or Windows 2000. Before configuring VPN policies, verify the network connectivity by pinging from Avaya IP Softphone1 to the remote site. The configuration below will demonstrate the detailed steps to create a dynamic IPSec VPN tunnel between the IP endpoint (Avaya IP Softphone1) and the Cisco 3640 router.

#### Step 1 Configuring a New Gateway for Security Policy

Click **Start → Program → Cisco Secure VPN Client → Security Policy Editor**.

Select **Non-secure** option to allow for IP communications to occur without encryption, as shown in Figure3. This option is necessary to allow the user to change any settings under the user's Internet Interface or Local Network Interface.

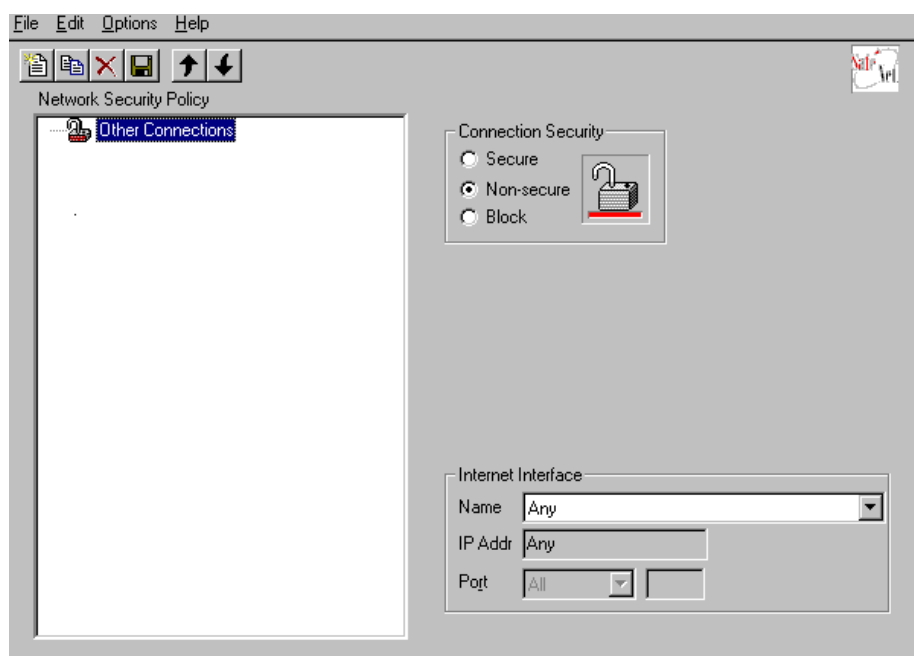


**Figure 3: Define the Policy for Non-Secured Connection**

#### Step 2 Configuring a Global Policy Settings for New Gateway

Select the **Options** Menu item and open **Global Policy Settings** menu. Check the box **Allow to Specify Internal Network Address**, as shown in **Figure 4**. This feature will allow the client's IP address to be used in policy setting configuration.

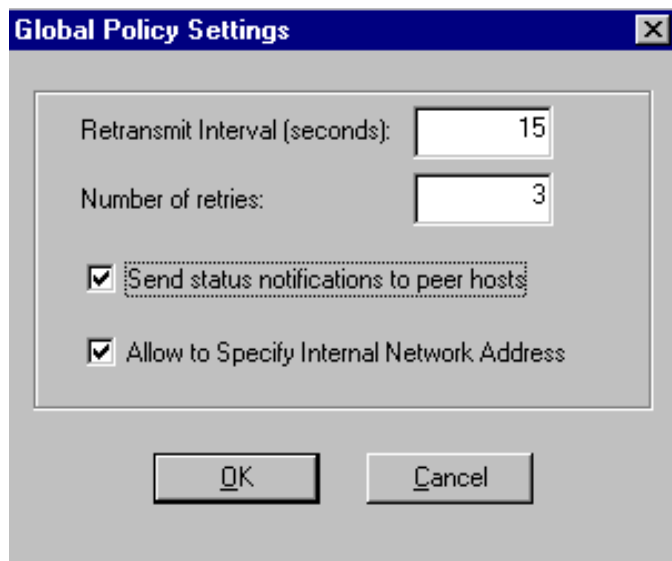


**Figure 4: Specify the Property of Global Policy Setting**

### **Step 3 Creating and Renaming a New Connection**

Open the **File** menu item and select **New Connections** shown in **Figure 5**. Type the connection name **Myconnection** as shown in **Figure 6**.

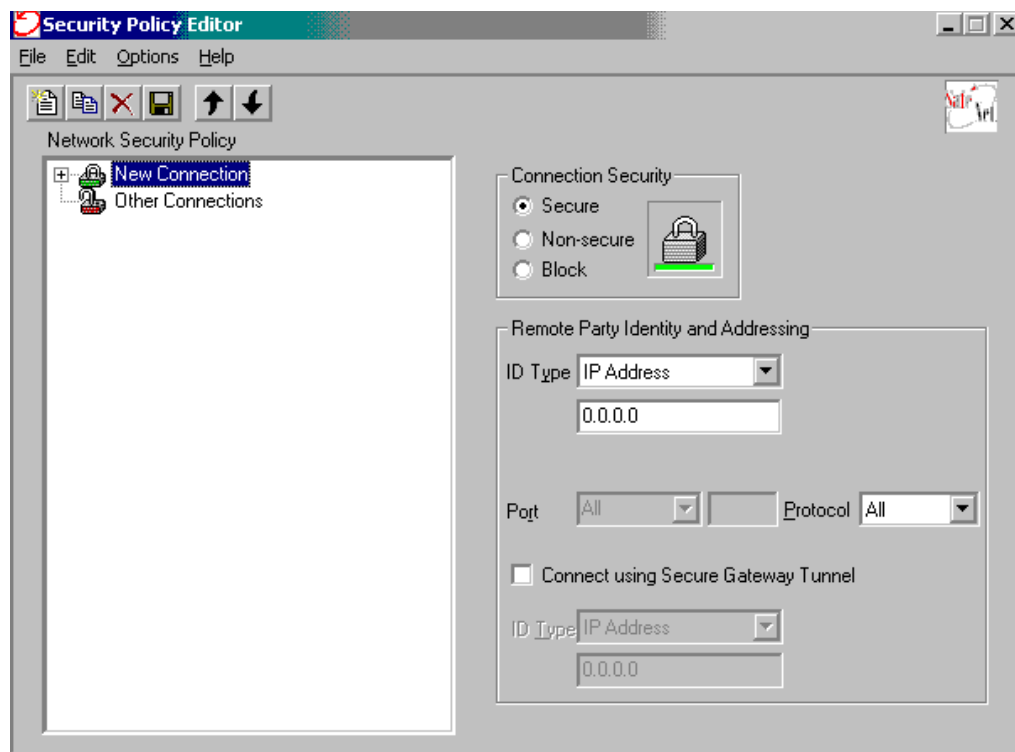


**Figure 5: Create a New Connection**

#### Step 4 Defining a New Connection for Pre-Shared Key

In this new connection panel, select **Secure** under **Connection Security**. Select **IP Subnet** as **ID Type** and enter the IP network address 10.1.1.0 and mask 255.255.255.0 into the **Remote Party Identity and Addressing** fields. Check the box **Connect using Secure Gateway Tunnel** as shown in **Figure 6**. This will create a secure connection from IP Softphone1 to the Avaya S8700 Media Server side (10.1.1.0 subnet).

**Note:** To create a secure connection to the 100.4.4.0 network where the S8300 Media Server is located, enter 100.4.4.0 and 255.255.255.0 in the **Subnet** and **Mask** fields.

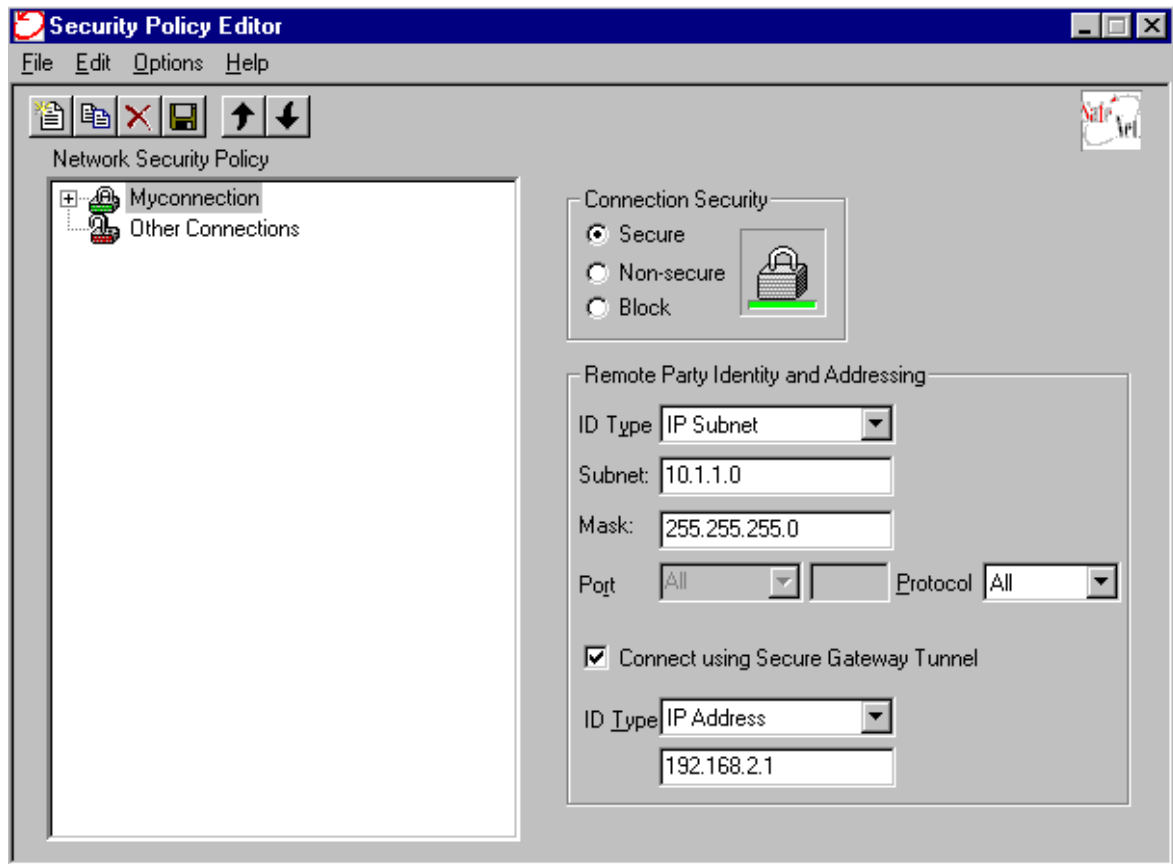


Figure 6: Specify the New Connection Properties

#### Step 5 Specifying a VPN Client's Identity

Expand **Myconnection** and highlight the **My Identity** icon and fill out these fields as indicated in **Figure 7**. Use "IP Address" as **ID Type** and the PC's NIC IP address as **Internal Network IP Address**.

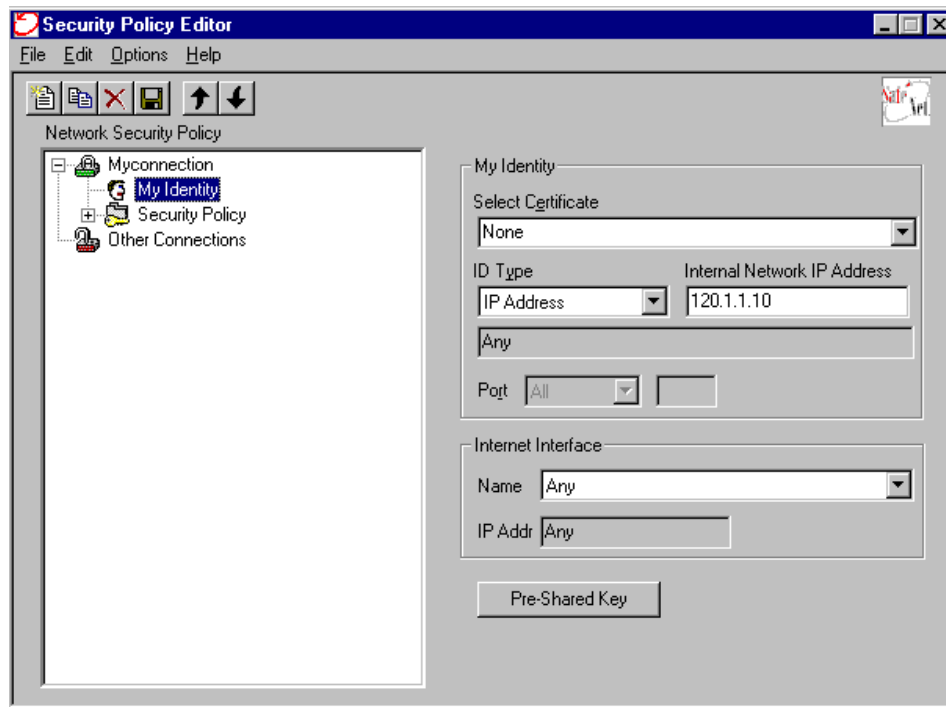


**Figure 7: Specify a VPN Client's Identity**

#### **Step 6 Specifying a Pre-Shared Key**

Click **Pre-Shared Key** and type in **avaya123** as a key string as shown in **Figure 8**. Click **OK**.

**Note:** This key must match the key defined in router's configuration.

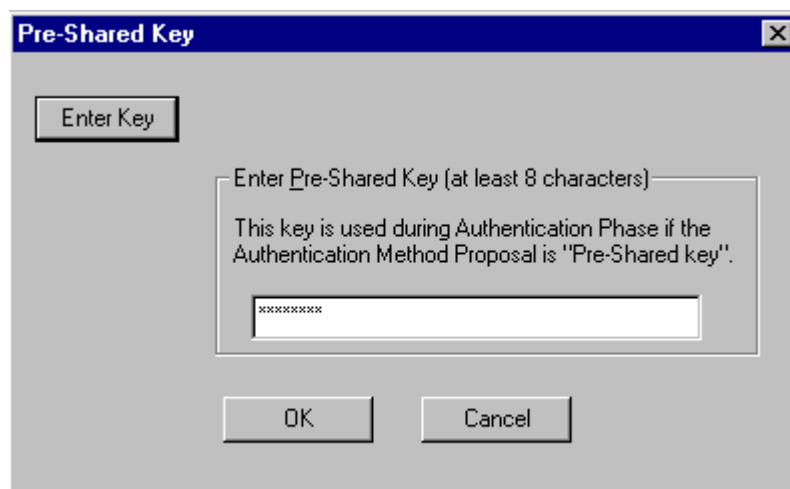


**Figure 8: Enter Pre-Shared Key**

## Step 7 Defining Security Policy

In the left pane, below **My Identity**, double-click **Security Policy**, select **Aggressive Mode** and check box **Enable Replay Detection**, as shown in **Figure 9**. Note the differences among these Negotiation Modes.

- **Main Mode** – This option allows identities not to be revealed until all secure communications have been established, which requires a longer processing time.
- **Aggressive Mode** – This option allows identities to be viewed while secure communications are taking place, which makes for a faster processing time.
- **Use Manual Keys** – This option is available for troubleshooting purposes only.

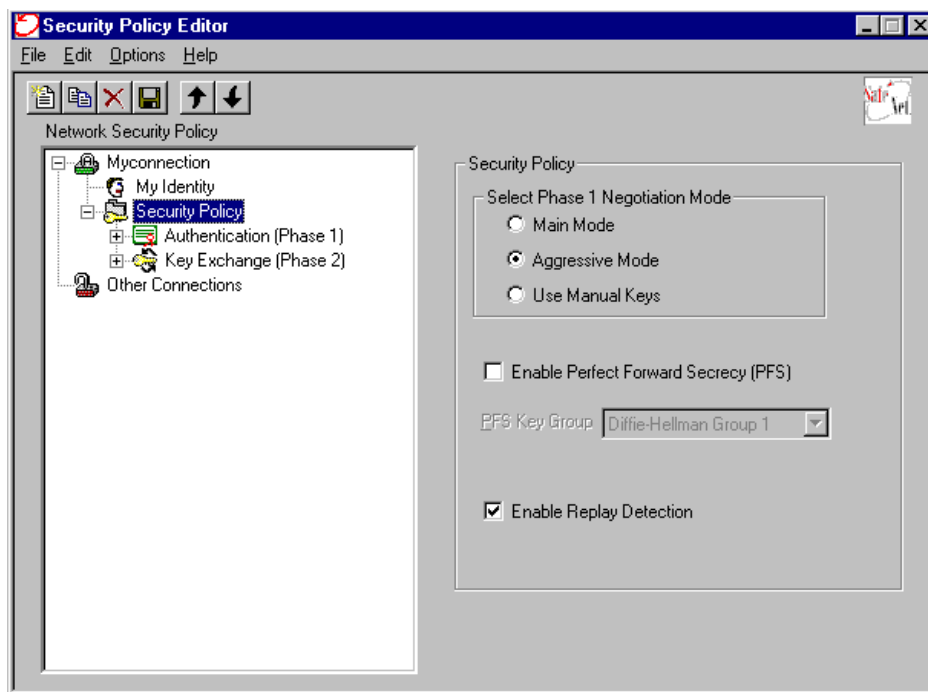


**Figure 9: Defining Security Policy for Myconnection**

## Step 8 Configuring Authentication Proposal (Phase 1)

In **Security Policy**, double-click **Authentication (Phase 1)** and select the settings as shown in **Figure 10**.

**Note:** There is a default proposal (**Proposal 1**) available under **Authentication**. Also, a new proposal can be created according to the user's needs. In these Application Notes, the default proposal has been used.

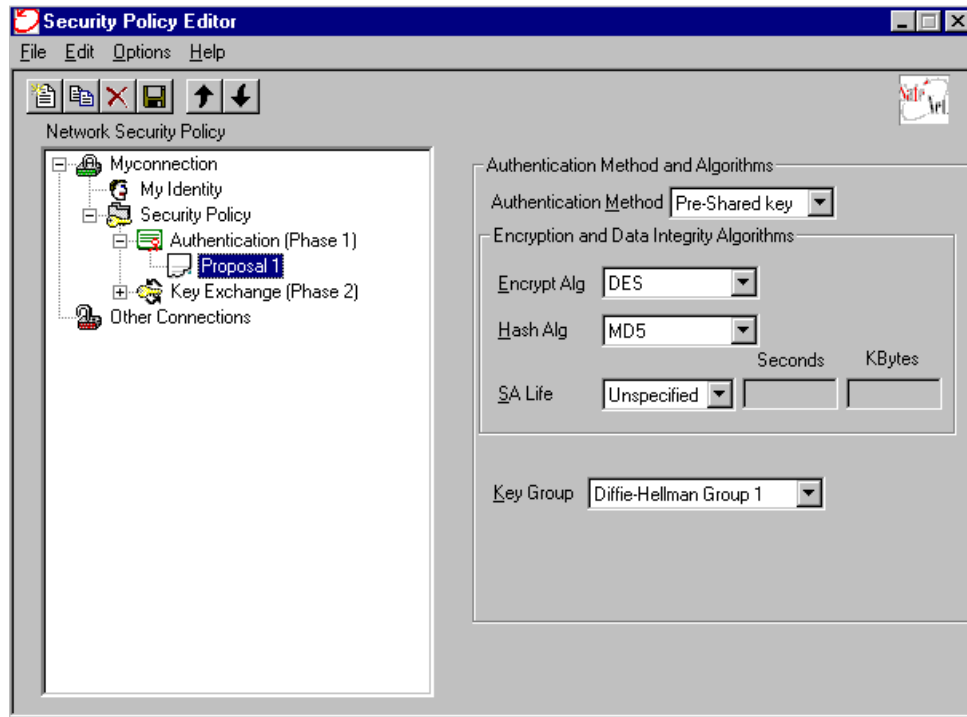


**Figure 10: Configuring Authentication Proposal (Phase 1)**

### **Step 9 Configuring Authentication Proposal (Phase 2)**

In **Security Policy**, double-click **Key Exchange (Phase 2)** and select the settings as shown in **Figure 11**.

**Note:** There is a default proposal (**Proposal 2**) available under **Key Exchange**. Also, a new proposal can be created according to the user's needs. In these Application Notes, the default proposal has been used.

### **Step 10 Save Configuration**

When finished, make sure to click the disk icon  on the tool bar and save the configuration.

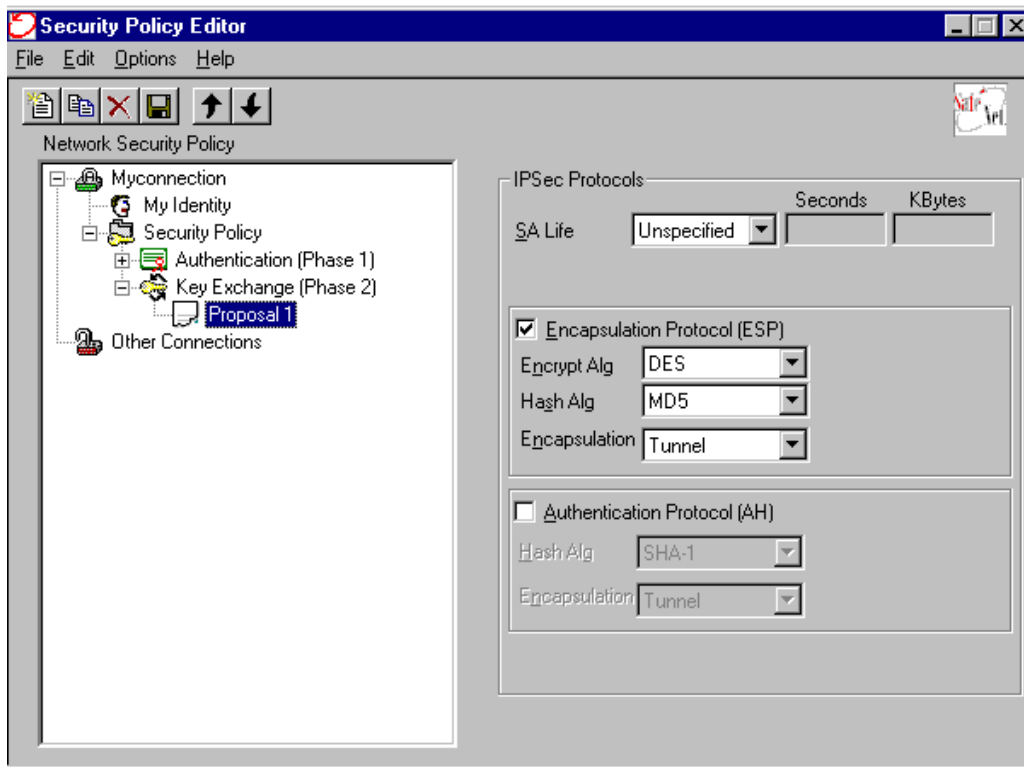


Figure 11: Configuring Key Exchange (Phase 2)

## 4. Verification Steps

### 4.1. Verify Site-to-Site VPN Tunnel

After the tunnel is up, use the **ping** command to verify that packets can travel through the tunnel between the two sites. Also, make calls between the two IP telephones to verify the call quality. In addition, the results of the following commands also display the status of the tunnel between the Cisco 3640 and 7100 routers.

C7100-VPN# **show crypto engine connection active**

| ID  | Interface       | IP-Address  | State | Algorithm          | Encrypt | Decrypt |
|-----|-----------------|-------------|-------|--------------------|---------|---------|
| 261 | FastEthernet0/1 | 192.168.2.1 | set   | HMAC_MD5+DES_56_CB | 0       | 866     |
| 262 | FastEthernet0/1 | 192.168.2.1 | set   | HMAC_MD5+DES_56_CB | 866     | 0       |

C7100-VPN# **show crypto map**

Crypto Map "mymap" 1 ipsec-isakmp

```

Peer = 192.168.2.1
Extended IP access list
  access-list permit ip 10.1.1.0 0.0.0.255 100.4.4.0 0.0.0.255
Current peer: 192.168.2.1
Security association lifetime: 4608000 kilobytes/3600 seconds
PFS (Y/N): N
  
```

```

Transform sets={
    vpn-1,
}
Interfaces using crypto map mymap:
    FastEthernet1/0

```

## 4.2. Verify Dynamic VPN Tunnel

Ping the Avaya Media Server and Media Gateway from the IP Softphone PC and verify that the ping is successful. Register the IP Softphone to the Avaya™ S8300 Media Server, make a call from the IP Softphone to the Avaya IP Telephone (x50001) and verify the quality.

Use the following commands to verify the dynamic VPN tunnel status between the Avaya IP Softphone and Cisco 3640 router.

```
C3640# show crypto ipsec sa
```

```

interface: Serial0/0
  Crypto map tag: intmap, local addr. 192.168.2.1

  local ident (addr/mask/prot/port): (100.4.4.0/255.255.255.0/0/0)
  remote ident (addr/mask/prot/port): (120.1.1.10/255.255.255.255/0/0)
  current_peer: 120.1.1.10:500
    PERMIT, flags={}
    #pkts encaps: 29, #pkts encrypt: 29, #pkts digest 29
    #pkts decaps: 29, #pkts decrypt: 29, #pkts verify 29
    #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.: 192.168.2.1, remote crypto endpt.: 120.1.1.10
    path mtu 1500, media mtu 1500
    current outbound spi: 4A47F8ED

  inbound esp sas:
    spi: 0xFE040A4D(4261677645)
      transform: esp-des esp-md5-hmac ,
      in use settings = {Tunnel, }
    slot: 0, conn id: 940, flow_id: 1, crypto map: intmap
      sa timing: remaining key lifetime (k/sec): (4607996/3400)
      IV size: 8 bytes
      replay detection support: Y

  inbound ah sas:

  inbound pcp sas:

  outbound esp sas:
    spi: 0x4A47F8ED(1246230765)
      transform: esp-des esp-md5-hmac ,
      in use settings = {Tunnel, }
    slot: 0, conn id: 941, flow_id: 2, crypto map: intmap

```

```
sa timing: remaining key lifetime (k/sec): (4607996/3400)
IV size: 8 bytes
replay detection support: Y
```

outbound ah sas:

outbound pcp sas:

C3640# **show crypto engine connection active**

| ID  | Interface | IP-Address  | State | Algorithm          | Encrypt | Decrypt |
|-----|-----------|-------------|-------|--------------------|---------|---------|
| 1   | Serial0/0 | 192.168.2.1 | set   | HMAC_MD5+DES_56_CB | 0       | 0       |
| 940 | Serial0/0 | 192.168.2.1 | set   | HMAC_MD5+DES_56_CB | 0       | 29      |
| 941 | Serial0/0 | 192.168.2.1 | set   | HMAC_MD5+DES_56_CB | 29      | 0       |

C3640# **show crypto map**

Crypto Map "intmap" 5 ipsec-isakmp  
Dynamic map template tag: dynmap

Crypto Map "intmap" 6 ipsec-isakmp  
Peer = 120.1.1.10  
Extended IP access list  
    access-list permit ip 100.4.4.0 0.0.0.255 host 120.1.1.10  
    dynamic (created from dynamic map dynmap/5)  
Current peer: 120.1.1.10  
Security association lifetime: 4608000 kilobytes/3600 seconds  
PFS (Y/N): N  
Transform sets={  
    trans1,  
}  
Interfaces using crypto map intmap:  
    Serial0/0

C3640# **show crypto map dynamic-map**

Crypto Map Template "dynmap" 5  
Extended IP access list 112  
    access-list 112 permit ip 100.4.4.0 0.0.0.255 120.1.1.10 0.0.0.255  
    access-list 112 permit ip 10.1.1.0 0.0.0.255 host 120.1.1.10  
Security association lifetime: 4608000 kilobytes/3600 seconds  
PFS (Y/N): N  
Transform sets={  
    trans1,  
}

## 5. Conclusion

A Virtual Private Network (VPN) provides a solution to protect VoIP traffic going through the public network. As illustrated by these Application Notes, Avaya MultiVantage™ Software with the Avaya™ S8700 and S8300 Media Servers, G600, G700 Media Gateways and IP endpoints (Avaya IP Telephones and Avaya IP Softphones) can work in a Cisco-based VPN tunnel environment.

---

**©2003 Avaya Inc. All Rights Reserved.**

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

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](mailto:interoplabnotes@list.avaya.com)