Avaya Solution & Interoperability Test Lab

Application Notes for Configuring a Site-to-Site IPsec VPN Tunnel between a Cisco ASA5520 and a NETGEAR FVS338 in Support of the Avaya A175 Desktop Video Device and Multi-modal Communication – Issue 1.1

Abstract

These Application Notes describe the necessary steps to configure a Site-to-Site IPsec VPN tunnel between a Cisco ASA5520 and a NETGEAR FVS338. The Cisco device is representative of a VPN gateway located at a Corporate Data Center while the NETGEAR was used to represent the Home Office user. The VPN tunnel is expected to be able to support multi-modal communication between an Avaya A175 Desktop Video Device on one end of the tunnel and various Avaya endpoints and services at the other end of the tunnel. The endpoints include additional A175DVD's, Avaya one-X® Communicator (SIP & H.323 versions) and the 9600 one-X® Deskphone SIP Edition. Services that are supplied at the corporate location included Call Processing, SIP routing, Conferencing, Voice Messaging, and Presence.

TABLE OF CONTENTS

1. Introduction

These Application Notes describe the necessary steps to setup a Site-to-Site IPsec VPN tunnel between a Cisco ASA5520 and a NETGEAR FVS338. The Cisco device is representative of a VPN gateway located at a Corporate Data Center while the NETGEAR was represents the 'Home Office' user. The VPN tunnel is expected to be able to support multi-modal communication between an Avaya A175 Desktop Video Device on one end of the tunnel and various Avaya endpoints and services at the other end of the tunnel. These endpoints include additional A175DVD's, Avaya one-X® Communicator (SIP & H.323 versions) and the Avaya one-X® Deskphone SIP for 9600 Series IP Telephones. Services being supplied at the corporate location included Call Processing, SIP routing, Conferencing, Voice Messaging, and Presence.

These Application Notes are written from the perspective that many of the basic installation steps for an Avaya Aura® Solution have already been completed. It is intended to specifically illustrate the addition of an IPsec VPN tunnel to an existing solution. If attempting to install all the components in the solution it is strongly recommended to download and review each of the documents listed in **Section 12.**

1.1. Sample Configuration Overview

In the sample configuration shown below in **Figure 1** a Site-to-Site IPsec VPN tunnel was configured between a Cisco Adaptive Security Appliance (ASA) 5520 and a NETGEAR ProSafe VPN Firewall device. The ASA5520 represents a VPN appliance likely to be located at the Corporate LAN/WAN data center providing VPN and Firewall services to multiple remote sites, whereas the FVS338 appliance is more likely to be found at the Home-Office intended to support a single user.

In the sample configuration each appliance has an 'inside' interface used to connect to the local LAN/WAN, and an 'outside' interface which will typically be connection to the Internet. All communication between 'outside' interfaces is encrypted using the IPsec encryption method. In the sample configuration both appliances were configured to support the following encryption and authentication protocols:

- IKE
- IPsec

The VPN tunnel was established using Passphrase authentication.

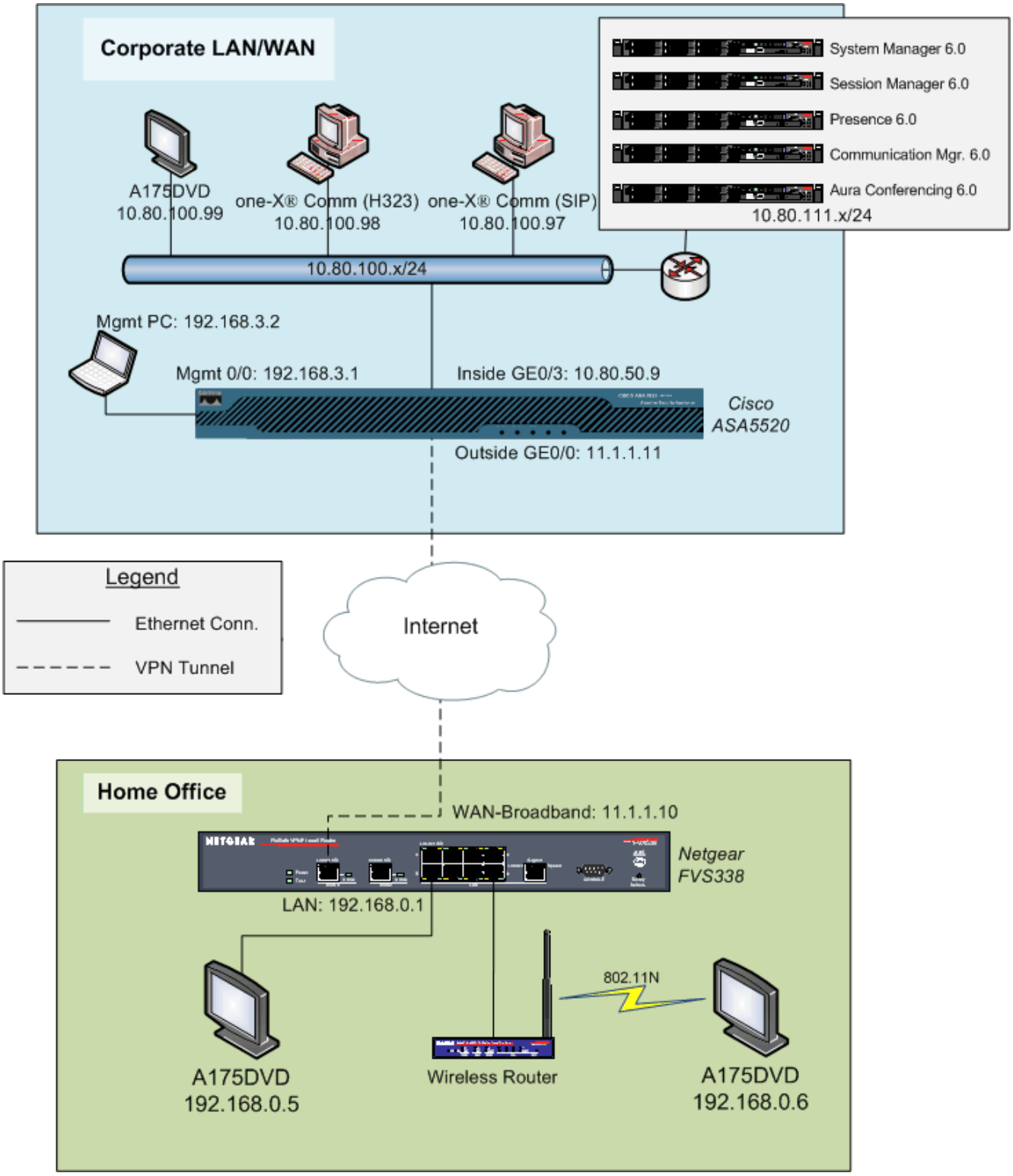


Figure 1

2. Equipment and Software Validated

The following equipment and software were used for the sample configuration shown in **Figure 1** above:

Provider	Hardware Component	Software Version
Avaya	A175 Desktop Video Device	1.0.0.002775
Avaya	S8880 Server	Avaya Aura® Session Manager 6.0 SP1
		Avaya Aura® System Manager 6.0 SP2
		Avaya Aura® Presence Services 6.0 SP2
		Avaya Aura® Conferencing 6.0
Avaya	S8300D Server	Avaya Aura® Communication Mgr 6.0 SP2 (2372) –Evolution Server
Avaya	Avaya one-X® 9630 IP Telephone (SIP)	2.6 SP4
Avaya	Avaya one-X® Communicator on Windows XP	6.0.1 SP1 (SIP)
Avaya	Avaya one-X® Communicator on Windows XP	6.0.1 SP1 (H.323)
Logitech	USB Camera	Communicate STX
Cisco	Adaptive Security Appliance (ASA) 5520	8.2(3)
Cisco	Adaptive Security Device Mgr (ASDM)	6.3(1)
NETGEAR	FVS338 ProSafe™ VPN Firewall Router	3.0.6-25

3. Observed Limitations

1. Because of the limited DHCP option settings on the NETGEAR FVS338, it is not possible to set the HTTP server value on the A175DVD via DHCP SSON 242. Therefore it is necessary to set this parameter manually. See **Section 12** Reference **[5]** for more information on this topic.
2. Using Communication Manager's Call Access Control feature to limit video bandwidth utilization proved to be somewhat unpredictable. Avaya Aura Session Manager 6.1 provides better tools for managing video and audio bandwidth utilization across multiple locations than what is offered in release 6.0.

4. Administer Avaya Aura® Session Manager

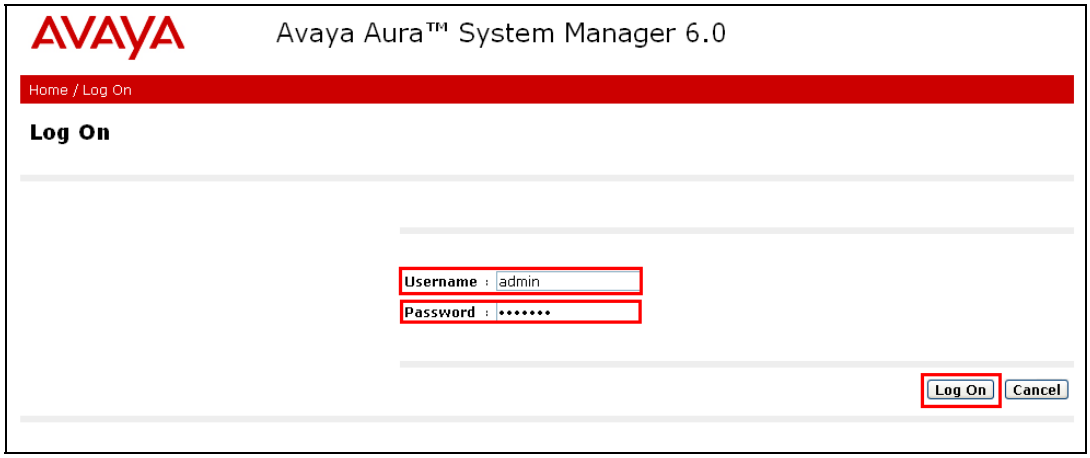
This section describes the additional configuration of Session Manager (via System Manager) when adding new network elements and configuring the Avaya A175 Desktop Video Device. Configuring SIP trunks between the various SIP entities shown in **Figure 1** is beyond the scope of this document though additional information on the topic can be found in **Section 12**.

Perform the following steps in order to support the remote users at a VPN location:

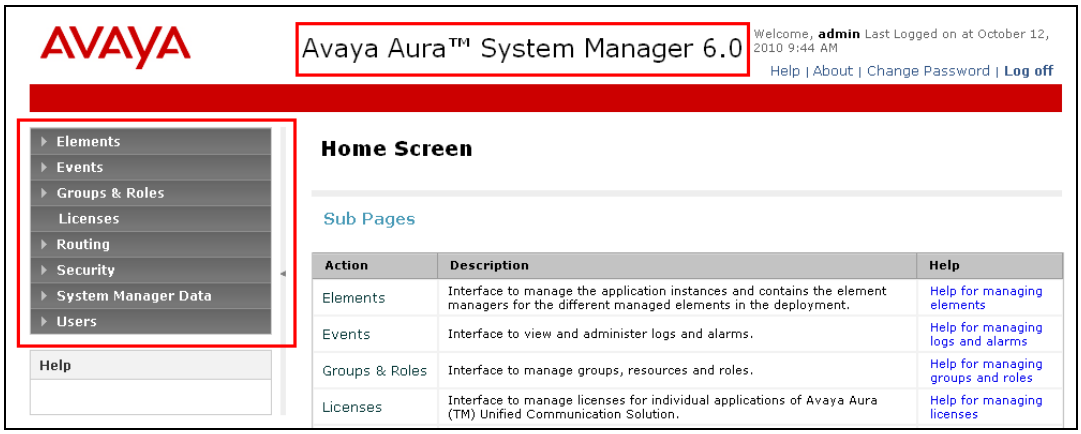
1) Create a Location
2) Administer a SIP user and associated station

4.1. Access Avaya Aura® System Manager

Access the System Manager web interface, by entering **http://<ip-addr>/SMGR** as the URL in an Internet browser, where *<ip-addr>* is the IP address of the server running System Manager graphical user interface. Log in with the appropriate **Username** and **Password** and press the **Log On** button to access Session Manager.



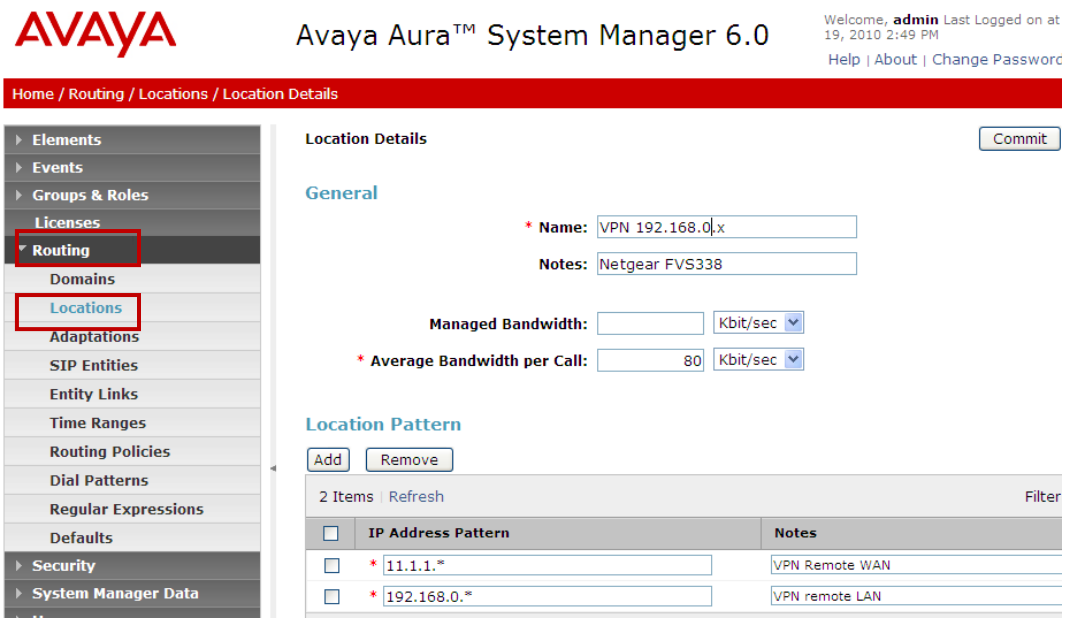
The **main menu** of the **System Manager Graphical User Interface** is displayed in the following screenshot.



4.2. Add Location

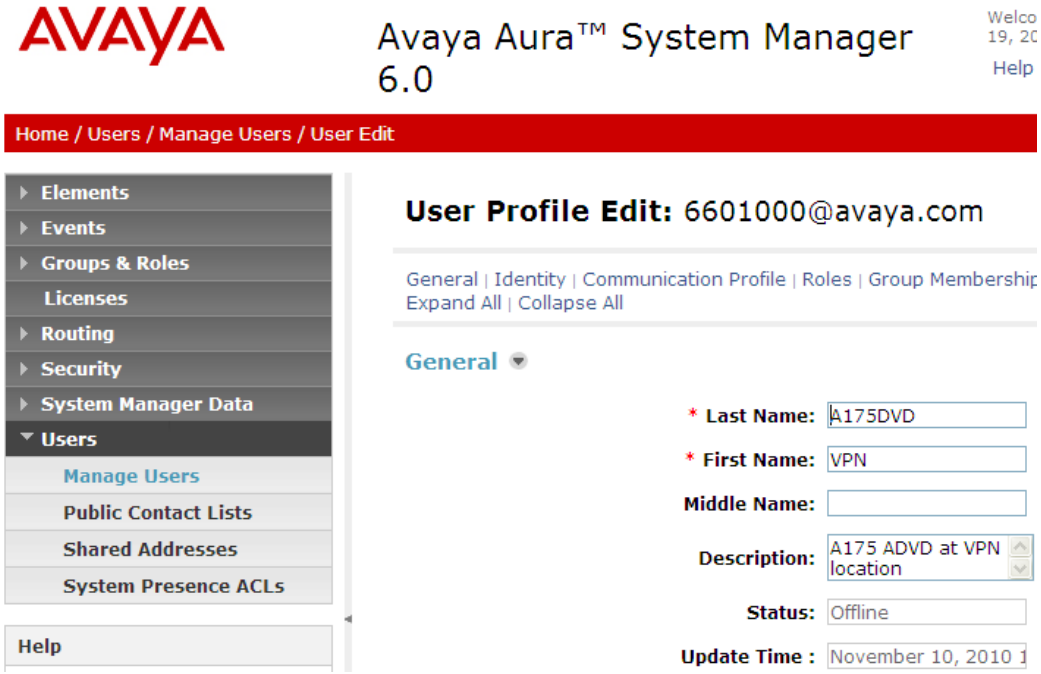
A new Location to represent the Home-Office network located at the far-end of the VPN tunnel should be added to Session Manager. Locations are used to identify logical and physical locations where SIP entities reside for the purposes of bandwidth management or location based routing.

To add a new Location, click on **Routing** and access the **Locations** sub heading. For the sample configuration a location named **VPN 192.168.0.x** was created. The **Average Bandwidth per Call** was left at the default value of **80 Kbit/sec**. The IP Address patterns of **11.1.1.*** and **192.168.0**.* were used to identify the location.

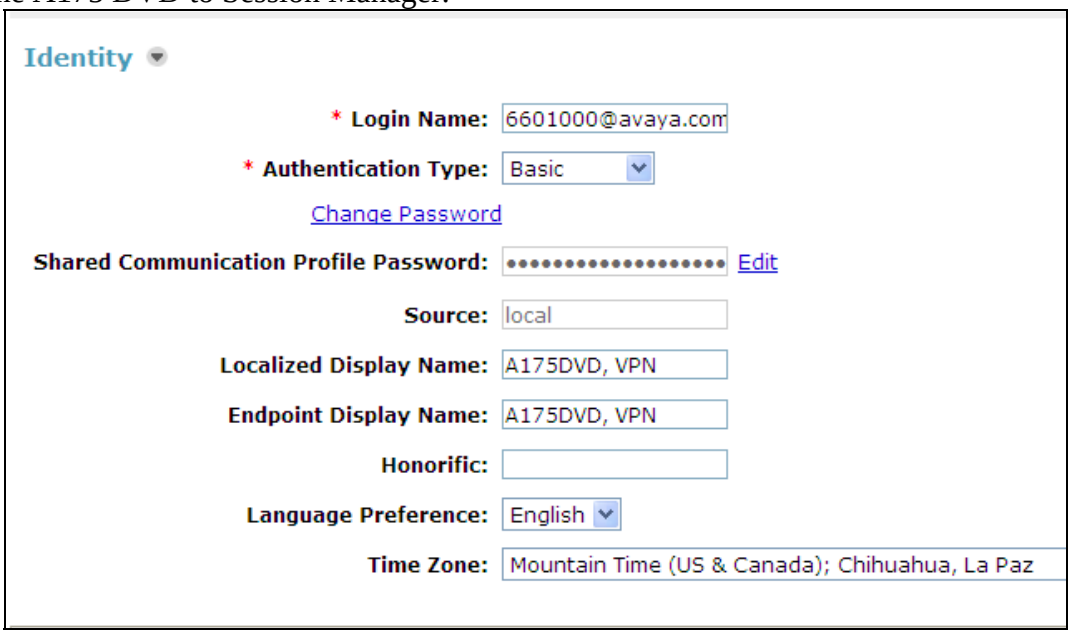


4.3. Add SIP User

To add a SIP User to Session Manager, select the **Users →Manage Users**. Then select the **New** button (not shown). The screen below shows the addition of the SIP User that will login to the A175DVD at the Home-Office location.

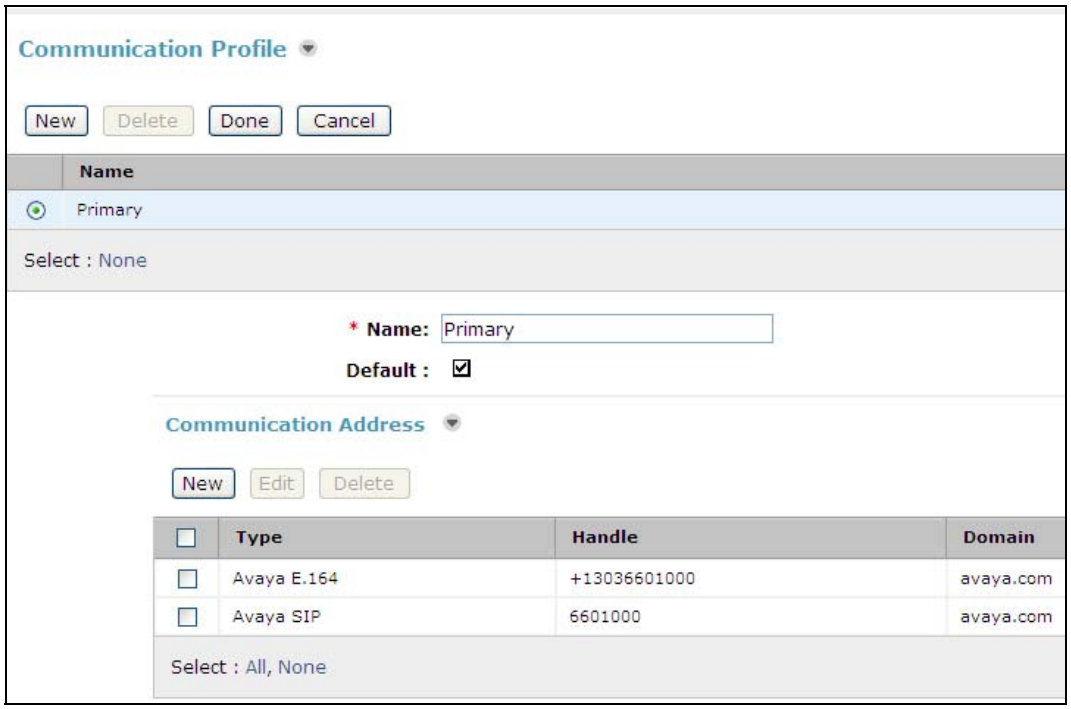


Under the **Identity** section for the SIP User in the following screenshot the **Login Name** was set to 6601000@avaya.com**.** The **Authentication Type** was set to **Basic.** The **SMGR Login Password** was set to the login and password of the Session Manager. The **Shared Communication Profile Password** was set to 123456 (not shown) which is what will be used to login the A175 DVD to Session Manager.

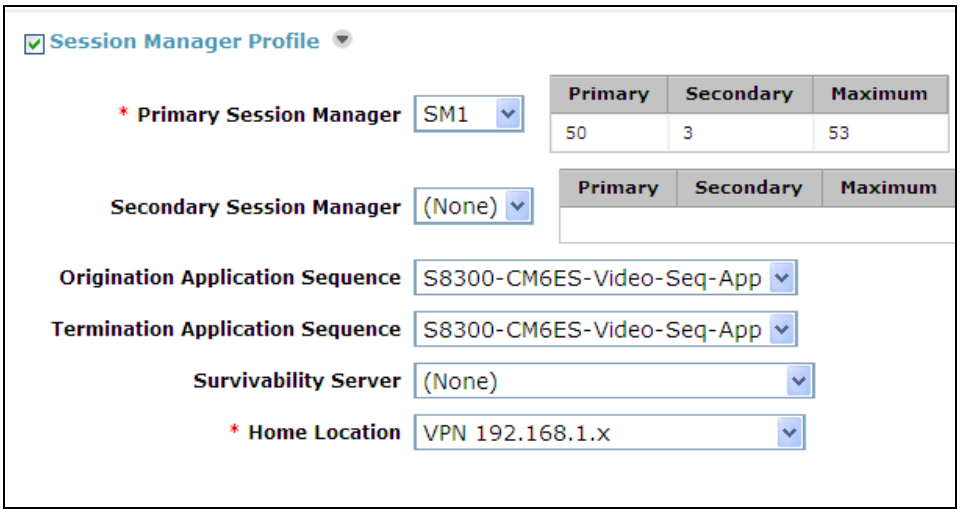


Expand the **Communication Profile** heading and set the **Name** to **Primary**. Enable the **Default** setting. Under **Communication Address** select the **New** button and add two addresses:

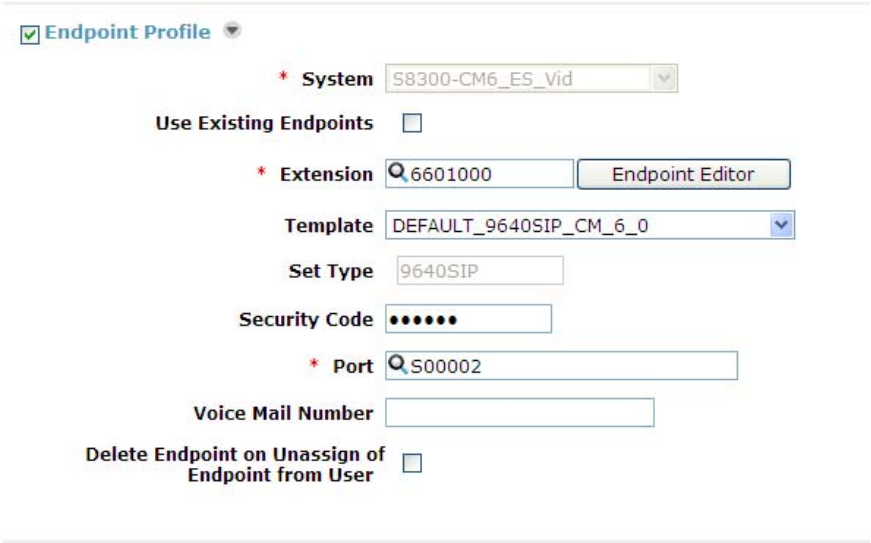
1) For the first address **Type** was set to **Avaya Sip** and a **Fully Qualified Address** that is the same as the extension. Select the
2) A second address of type **Avaya E.164** was added in support of Presence Services' Buddy Lists. The handle **+13036601000** is in E.164 format and the domain is **avaya.com**. See **Section 12** Reference **[7]** for more info.



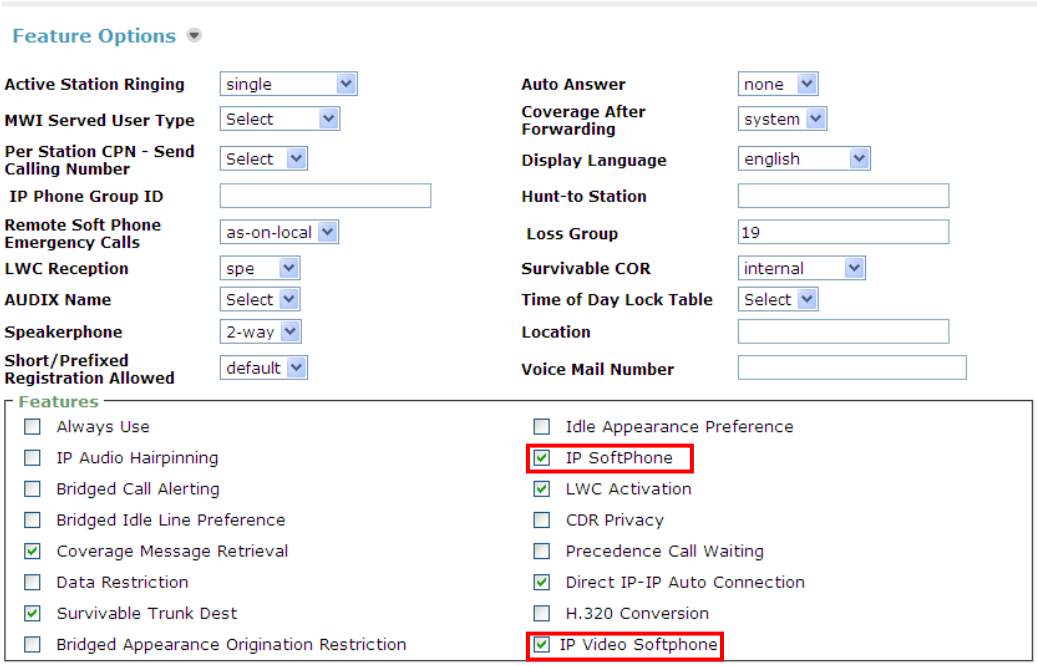
Next, expand the **Session Manager Profile** heading and select the checkbox. The **Primary Session Manager** was set to **SM1** as shown below. This equates to the Session Manager SIP entity. A **secondary Session Manager** could also be set to support failover. The **Origination** and **Termination Application Sequence** was set to an existing Sequenced Application called **S8300-CM6ES-Video-Seq-App.** This is the Communication Manager Application Sequence name. From the drop-down set the **Home Location** to the one created in **Section 4.2**.



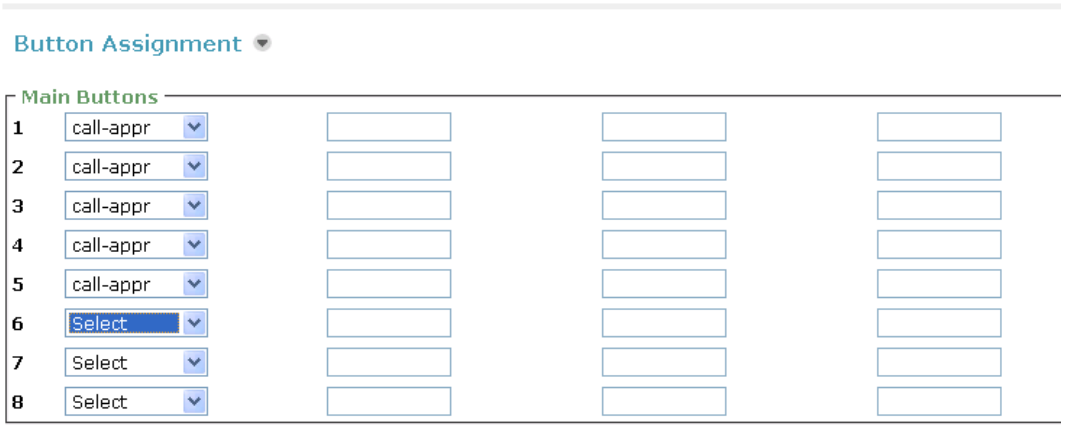
In order for the Station Profile template information to be pushed from the Session Manager down to the Communication Manager, **enable** the **Endpoint Profile** box. The System was set to the already administered Communication Manager instance called **S8300-CM6_ES_Vid.** This is the Managed Entity Name. The **Extension** was set to **6601000** and the **Template** was set to **DEFAULT_9640SIP_CM_6_0.** The **Port** is initially set to **IP** (though as shown below this screen will later show the actual IP port being used by Communication Manager).



Select the **Endpoint Editor** button (shown above) and a new screen will appear. Scroll down to the section titled **Feature Options** and ensure that **IP Softphone** and **IP Video Softphone** are checked.



Scroll down to the section titled **Button Assignment** and expand it by selecting the icon (it may take a few seconds for the button fields to appear). By default there will already be three buttons labeled as **call-appr**. From the drop-down, assign this same value to buttons 4 & 5 as shown below.



Select the **Done** button (not shown) to return to the SIP User page. Then select the **Commit** button (not shown) to complete administration of the SIP User.

5. Administer Avaya Aura® Communication Manager

This section describes the additional configuration of Communication Manager when adding users at a new location such as that represented by the Home-Office.
Oftentimes, there is limited bandwidth available over a VPN connection in which case it is desirable to configure Communication Manager to limit the amount of bandwidth that each end point can utilize for video and/or voice.

5.1. Verify Network Region for SIP Signaling Group

In order to control voice codec and bandwidth utilization, its important to understand in which network region the endpoints are located. For SIP endpoints such as the A175DVD which register to Session Manager but get calling features from Communication Manager via SIP, the codec used and bandwidth limit set will be determined in part by the network region used on the SIP signaling-group form. Use the command **display signaling-group x** where '**x**' is signaling group used to connect Communication Manager to Session Manager. For the sample configuration SIP signaling-group 10 was created.

As shown below signaling-group 10 uses **ip-network-region 1** at the **far-end**.

```
display signaling-group 10
                                SIGNALING GROUP

 Group Number: 10             Group Type: sip
  IMS Enabled? n        Transport Method: tls
        Q-SIP? n                                          SIP Enabled LSP? n
     IP Video? y          Priority Video? n        Enforce SIPS URI for SRTP? y
  Peer Detection Enabled? y  Peer Server: SM



   Near-end Node Name: procr                 Far-end Node Name: ASM1
 Near-end Listen Port: 5061                Far-end Listen Port: 5061
                                        Far-end Network Region: 1

Far-end Domain: avaya.com
                                            Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate                 RFC 3389 Comfort Noise? n
         DTMF over IP: rtp-payload            Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3                     IP Audio Hairpinning? n
         Enable Layer 3 Test? n                   Initial IP-IP Direct Media? n
H.323 Station Outgoing Direct Media? n            Alternate Route Timer(sec): 6
```

5.2. Administer IP-Network-Map

In order for Communication Manager to measure and limit the amount of bandwidth utilized by the A175DVD devices, particularly for video, each of the subnets where one the device resides should be placed into its own **ip-network-region**. For IP hosts this is accomplished by administering the appropriate host or subnet address in the **ip-network-map** form. Use the command **change ip-network-map** to place the 192.168.0.x subnet into ip-network-region 2 and the 10.80.100.x subnet into ip-network-region 3.

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

                                                 Subnet Network     Emergency
 IP Address                                      Bits   Region VLAN Location Ext
 ------------------------------------------- ------ ------ ---- -------------
 FROM: 192.168.0.0                               /24    2      n
   TO: 192.168.0.255
 FROM: 10.80.100.0                               /24    3      n
   TO: 10.80.100.255
```

5.3. Administer IP Network Regions

This section describes the **IP Network Region** screens**. Section 5.2** placed endpoints into network-regions. This section will define how the regions are connected to each other.

5.3.1. Administer IP Network Region 1

Use the command **change ip-network-region 1** to configure this region. On **Page 1** the **Authoritative Domain** must mirror the domain name of Session Manager. This was **avaya.com**. Endpoint to endpoints calls with network region 1 will use **Codec Set 1**. IP Shuffling was turned on so both **Intra-region IP-IP Direct Audio** and **Inter-region IP-IP Direct Audio** were set to **yes.**

```
change ip-network-region 1                                      Page   1 of  20
                              IP NETWORK REGION
  Region: 2
Location: 1       Authoritative Domain: avaya.com
    Name:VPN1 Remote Users
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 1              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                      IP Audio Hairpinning? n
   UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS                  RTCP Reporting Enabled? y
 Call Control PHB Value: 46      RTCP MONITOR SERVER PARAMETERS
        Audio PHB Value: 46       Use Default Server Parameters? y
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                   RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```

On **Page 4** ensure that ip-network-region 1 is connected to ip-network-region **2** and region **3** and that ip-codec-set 2 is used for calls between the regions. In addition notice below that WAN bandwidth limits are set for calls to each of these regions. In a production environment there is often a limited amount of bandwidth available on an Internet VPN connection. Without setting a limit here an A175DVD-to-A175DVD video call can use as much **4Mbits** of bandwidth. As

shown below calls from region 1 to region 2 or region 3 cannot use more than 1024 Kbits of bandwidth with normal video limited to 256 Kbits and priority video limited to 512 Kbits.

```
change ip-network-region 1                                      Page   4 of  20

 Source Region: 1     Inter Network Region Connection Management     I       M
                                                                     G  A    t
 dst codec direct   WAN-BW-limits   Video      Intervening      Dyn  A  G    c
 rgn  set   WAN  Units    Total Norm  Prio Shr Regions          CAC  R  L    e
 1    1                                                               all
 2    2     y    Kbits    1024   256   512  y                        n       t
 3    2     y    Kbits    1024   256   512  y                        n       t
```

5.3.2. Administer IP Network Regions 2 and 3

Since the IP endpoints were placed into ip-network-region 2 and 3, it's necessary to administer these regions as well. Use the command **change-ip-network-region 2** to make the changes. The screenshot below shows the values used in the sample configuration. Use the same settings on **Page 1** for ip-network-region **3** (not shown).

```
change ip-network-region 2                                      Page   1 of  20
                              IP NETWORK REGION
  Region: 2
Location: 1       Authoritative Domain: avaya.com
    Name:VPN1 Remote Users
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 1              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                     IP Audio Hairpinning? n
   UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS                 RTCP Reporting Enabled? y
 Call Control PHB Value: 46      RTCP MONITOR SERVER PARAMETERS
        Audio PHB Value: 46       Use Default Server Parameters? y
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                     RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```

On **Page 4** connect ip-network-region **2** to region **3** as shown below. Use the same bandwidth settings as shown in **Section 5.3.1**.

```
change ip-network-region 2                                      Page   4 of  20

 Source Region: 2     Inter Network Region Connection Management     I       M
                                                                     G  A    t
 dst codec direct   WAN-BW-limits   Video      Intervening      Dyn  A  G    c
 rgn  set   WAN  Units    Total Norm  Prio Shr Regions          CAC  R  L    e
 1    2     y    Kbits    1024   256   512  y                        n       t
 2    1                                                               all
 3    2     y    Kbits    1024   256   512  y                        n       t
```

5.4. Administer IP Codec Sets

This section describes the **IP Codec Set** screen. In the sample configuration ip-codec-sets 1 and 2 were utilized. Calls that stay within the Corporate LAN/WAN or Home-Office will use **ip-codec-set 1** and calls between the 3 regions will use **ip-codec-set 2**. The only difference between the two regions will be the bandwidth limit set on page-2 of the ip-codec-set form.

Page 1 sets the audio codecs in priority order. For ip-codec-set 2, which is used for calls over the VPN, G.729A is the preferred codec as it uses the least amount of bandwidth. For ip-codec-set 1**, G.726A-32K** appears first on the list (not shown) as it offers better audio quality at the expense of bandwidth so it is better suited for calls that stay within a region.

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

                          IP Codec Set

    Codec Set: 2

    Audio        Silence      Frames   Packet
    Codec        Suppression  Per Pkt  Size(ms)
 1: G.729A            n         2        20
 2: G.726A-32K        n         2        20
 3: G.711MU           n         2        20
 4:
```

On **Page 2** set **Allow Direct-IP Multimedia** to **'y'**. For the sample configuration a **Maximum Call Rate** of **15360** Kbits (the maximum value) was set. While these fields can be used to limit the amount of bandwidth consumed for a call that stays within a given ip-network-region, sections **6.3.1 and 6.3.2** inter-region bandwidth settings were configured therfore it is not necessary to do that here. For **ip-codec-set 1** this value was also set to **15360** Kbits (not shown).

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

                          IP Codec Set

                             Allow Direct-IP Multimedia? y
              Maximum Call Rate for Direct-IP Multimedia:   15360:Kbits
     Maximum Call Rate for Priority Direct-IP Multimedia:   15360:Kbits

                     Mode                Redundancy
    FAX              relay                0
    Modem            off                  0
    TDD/TTY          US                   3
    Clear-channel    n                    0
```

6. Configure the Cisco ASA5520

For the sample configuration, Cisco's Adaptive Security Device Manager (ASDM) was used to configure the ASA5520. This application runs on a Windows PC and can be downloaded either from the ASA5520 via HTTP or from the Cisco's Internet home page. See **Section 12** Reference **[12]** for more information on installing and configuring Cisco's ASDM.

The ASA5520 is highly complex routing device whose capabilities extend well beyond simply being able to create a VPN tunnel and route IP traffic to and from it. However, for the sample configuration only the necessary steps to create the VPN tunnel and routing policies are shown in these Application Notes. For additional information see **Section 12** Reference **[11]** for advanced topics on administering the ASA5520.

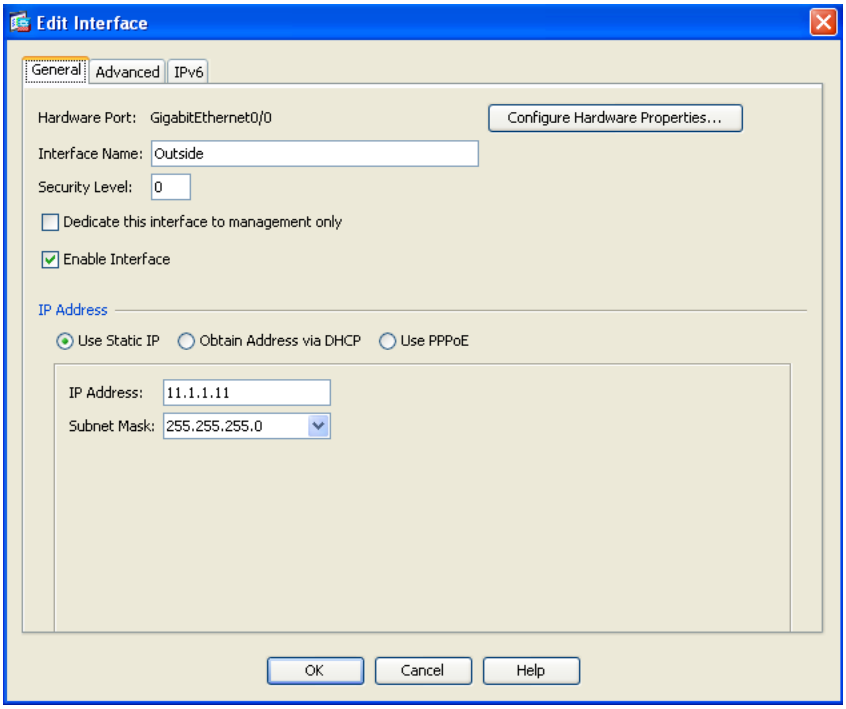
6.1. Configure Ethernet Interfaces

In the sample configuration two interfaces were configured:

- **GigabitEthernet 0/0:** Labeled as "Outside" and used to connect to the "internet" and to host the VPN tunnel
- **GigabitEthernet 0/3:** Labeled as "Inside" and used to connect the ASA5520 to rest of the corporate network

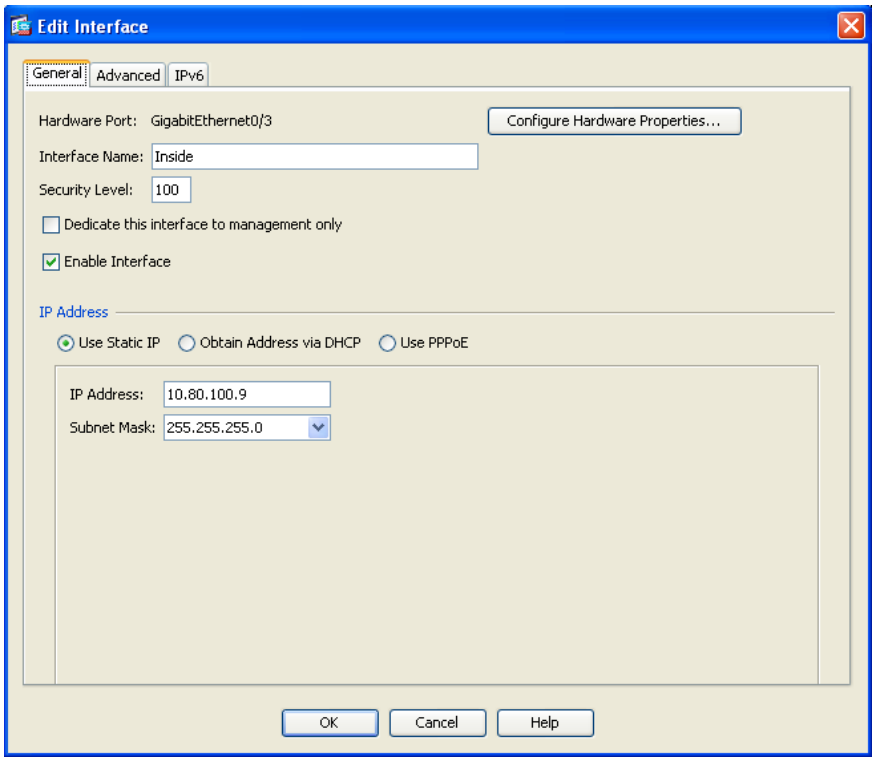
In addition there is a dedicated interface for device management called **Management0/0.** The default address for this interface is **192.168.0.1**. Initial administration of the ASA5520 is performed by directly connecting an ethernet cable between a PC's Ethernet interface and this one. See **Section 12** Reference **[12]** for more information on this topic.

1) To configure the "outside" interface from ASDM select Configuration → Interfaces. In the table on the right, double-click on the row labeled **GigabitEthernet 0/0.** The following entries were used in the sample configuration.
   - **Interface Name:** Outside
   - **Security Level:** 0
   - **Enable interface** Select the checkbox
   - **Use Static** Select this radio button
   - **IP Address:** 11.1.1.11
   - **Subnet Mask:** 255.255.255.0



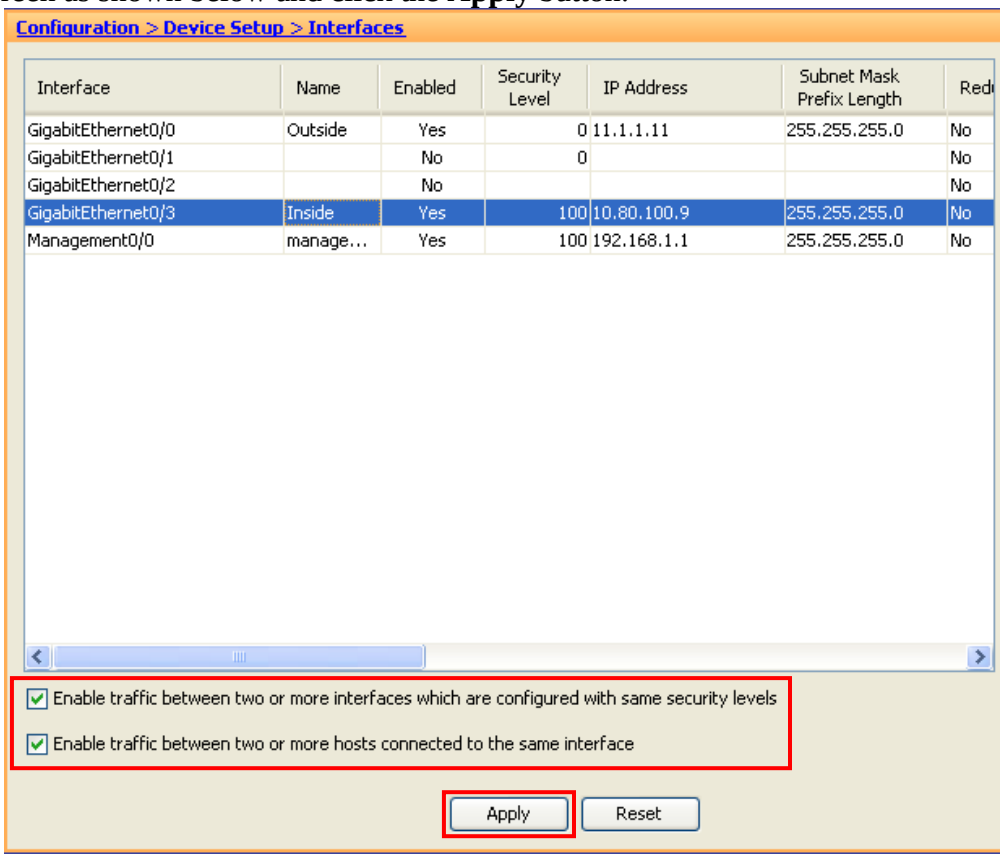
Click the **OK** button when complete

2) Repeat step 1 for the "inside" interface, **GigabitEthernet 0/3.**
   - **Interface Name:** Inside
   - **Security Level:** 100
   - **Enable interface** Select the checkbox
   - **Use Static** Select this radio button
   - **IP Address:** 10.80.100.9
   - **Subnet Mask:** 255.255.255.0



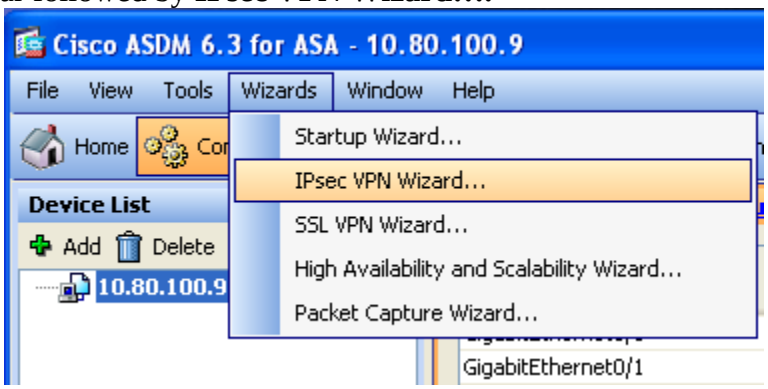
Click the **OK** button when complete.

3) Once the interfaces have been configured select the two check boxes at the bottom of the screen as shown below and click the **Apply** button.



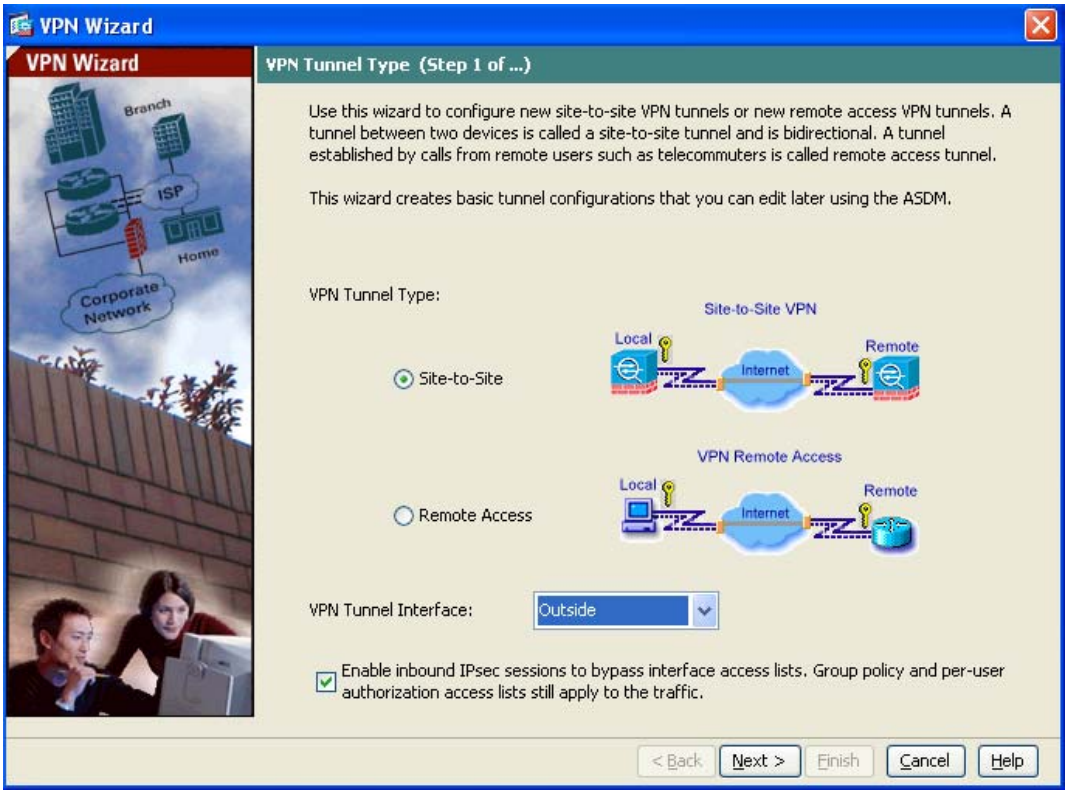
6.2. Configure the VPN Tunnel

1) Begin configuring the VPN tunnel in ASDM by selecting the **Wizards** menu item at the top menu bar followed by **IPsec VPN Wizard….**



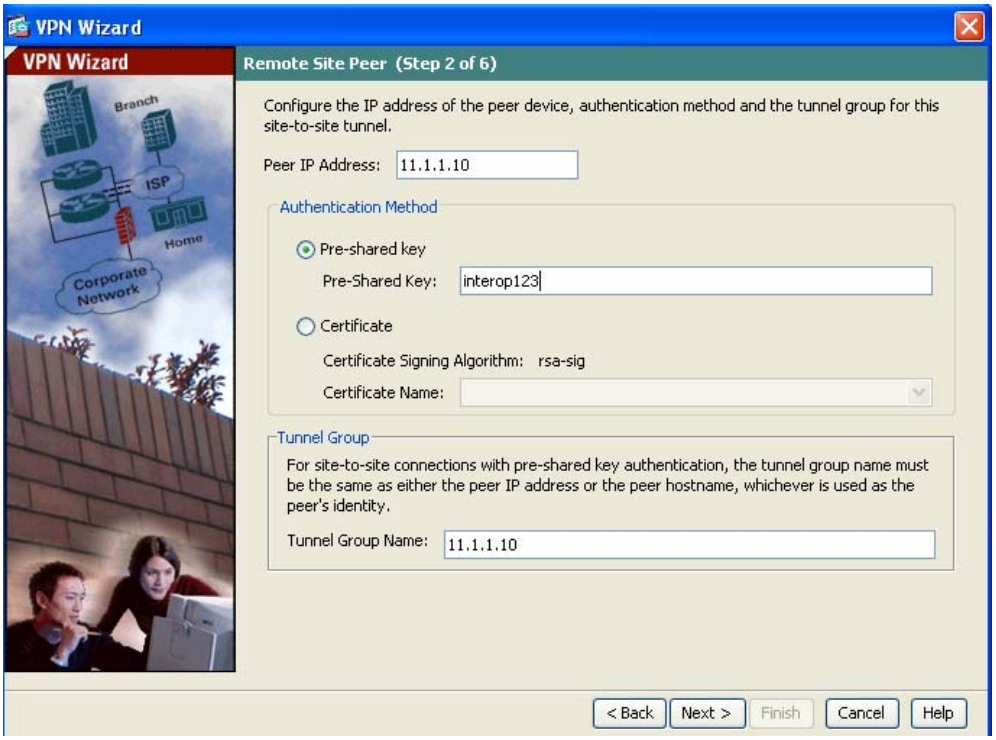
2) In the next screen that appears select the **Site-to-Site** radio button and appropriate interface from the drop-down list next to **VPN Tunnel Interface**. For the sample configuration this is the **Outside** interface defined in **Section 6.1**.

Note: For the sake of simplicity, the checkbox next to "Enable Inbound IPsec sessions to bypass…." was checked though for security reasons, a more advanced administrator may prefer to uncheck this box and set their Access Control Lists (ACL's) explicitly.



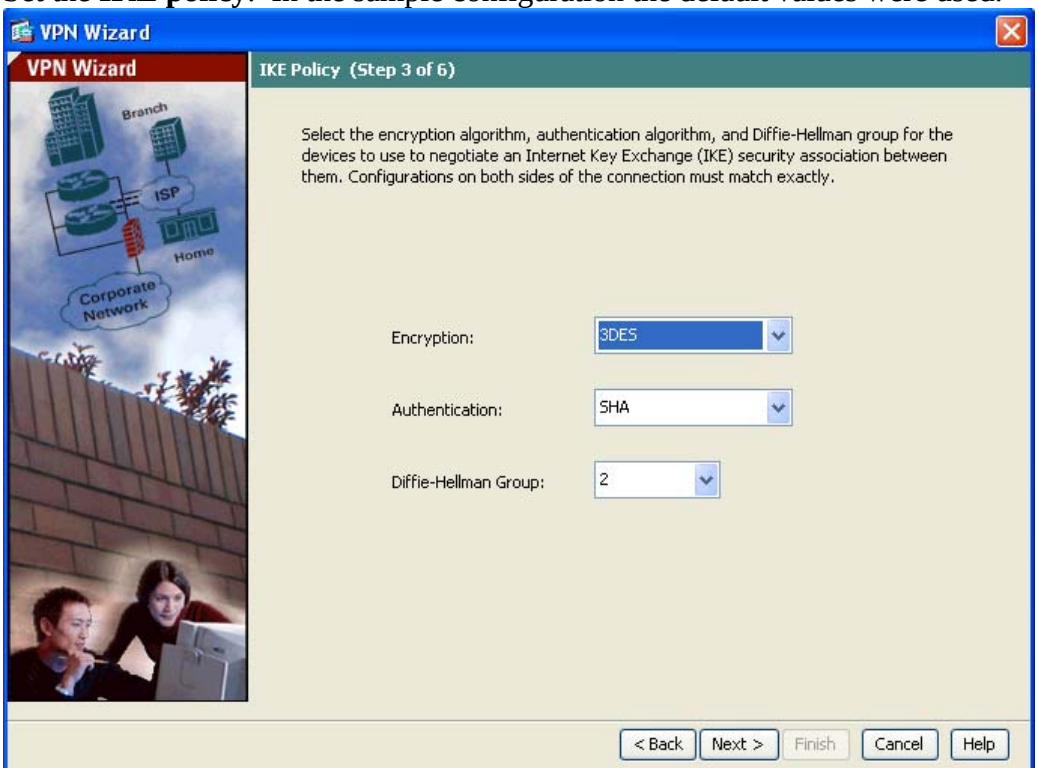
Select the **Next** > button.

3) In the **Peer IP Address** field, enter the WAN interface for the NETFEAR FVS338 which will be defined in **Section 7**. In the Pre-Shared key filed enter in a password which will be used to establish the tunnel. Make a note of this password as it will also be required in **Section 7**.



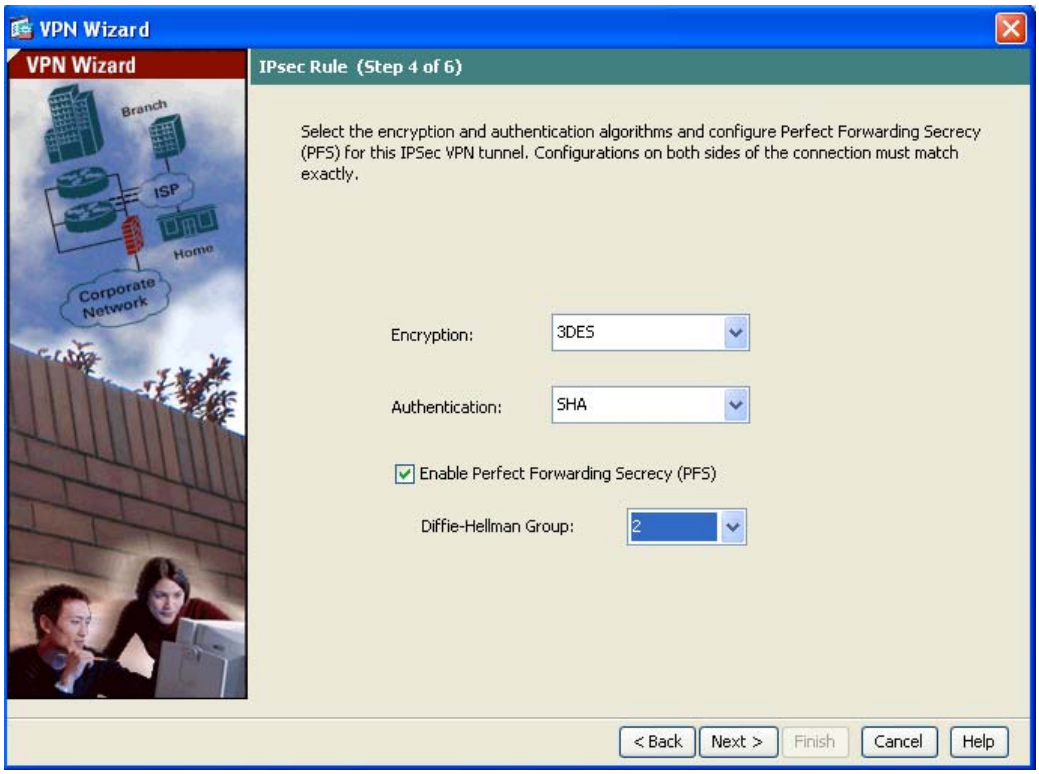
Select the **Next** > button

4) Set the **IKE policy**. In the sample configuration the default values were used.



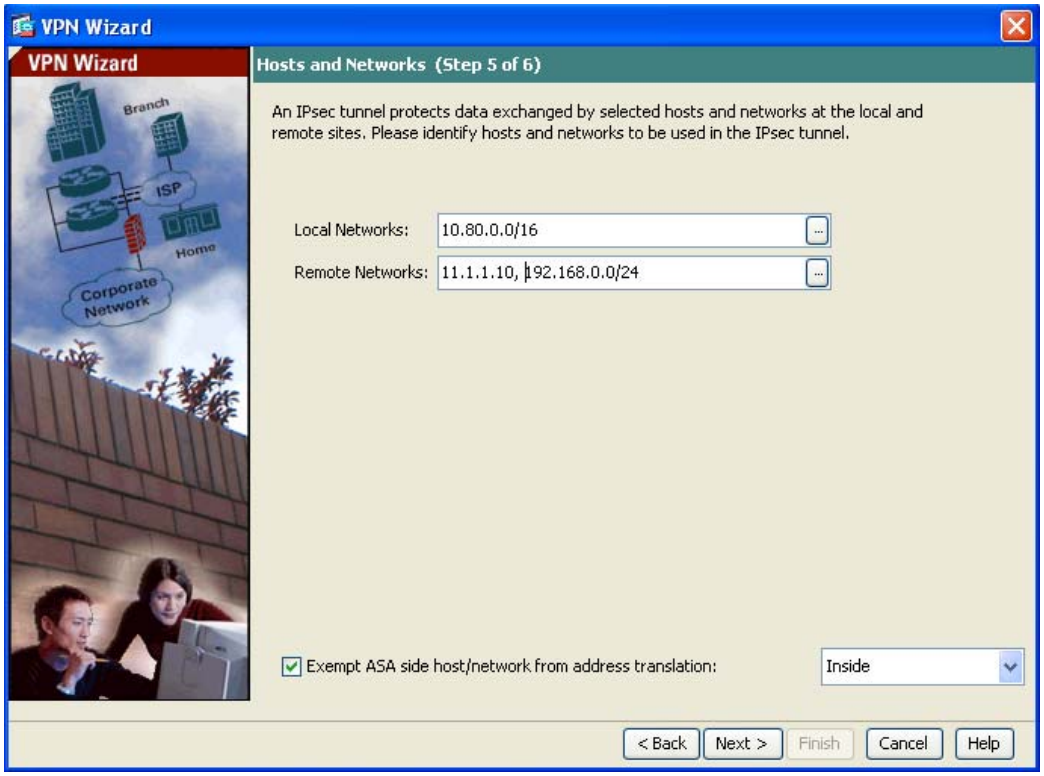
Select the **Next** > button

5) Set the **IPsec Rule**. In the sample configuration only the **Diffie-Hellman Group** value was changed from its default of **1** to **2** which matches the default value used on the NETGEAR FVS338.



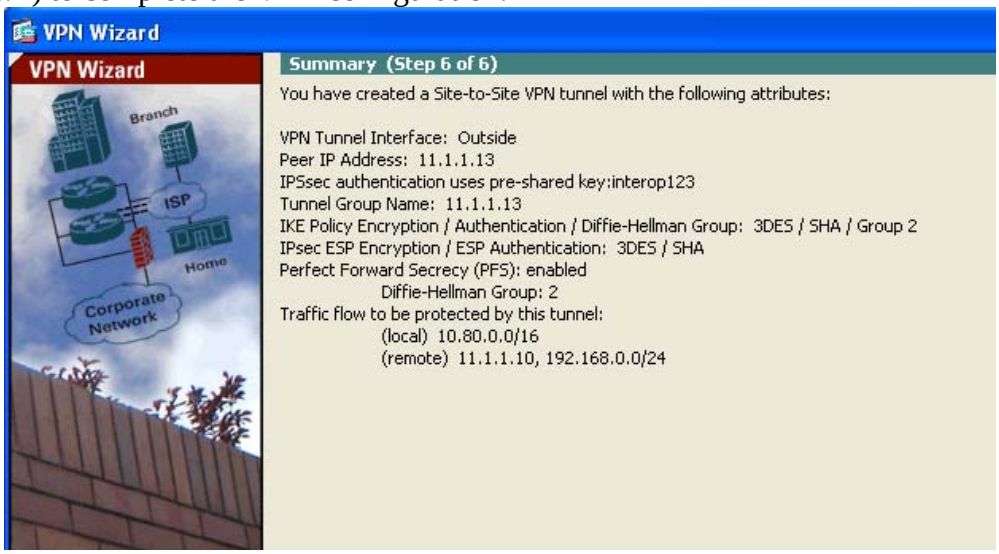
Select the **Next** > button

6) Configure **Hosts and Networks.** For **Local Networks** use network address associated with the inside interface of the ASA5520. For the sample configuration **10.80.0.0/16** was used. For the **Remote Networks** use the WAN interface **11.1.1.10** and inside network **192.168.0.0/24** of the NETGEAR FVS338 defined in **Section 7**.



Select the **Next** > button

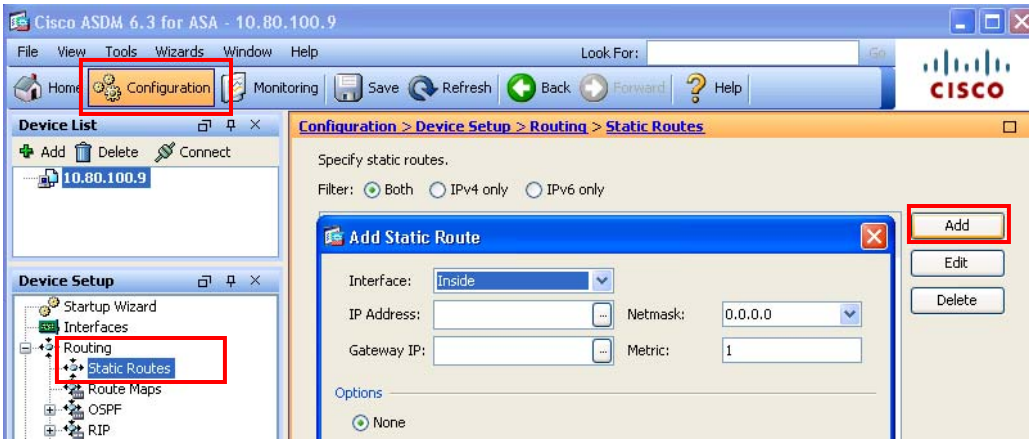
7) Cisco ASDM displays a summary of the configuration. Select the **Finish** button (not shown) to complete the VPN configuration.



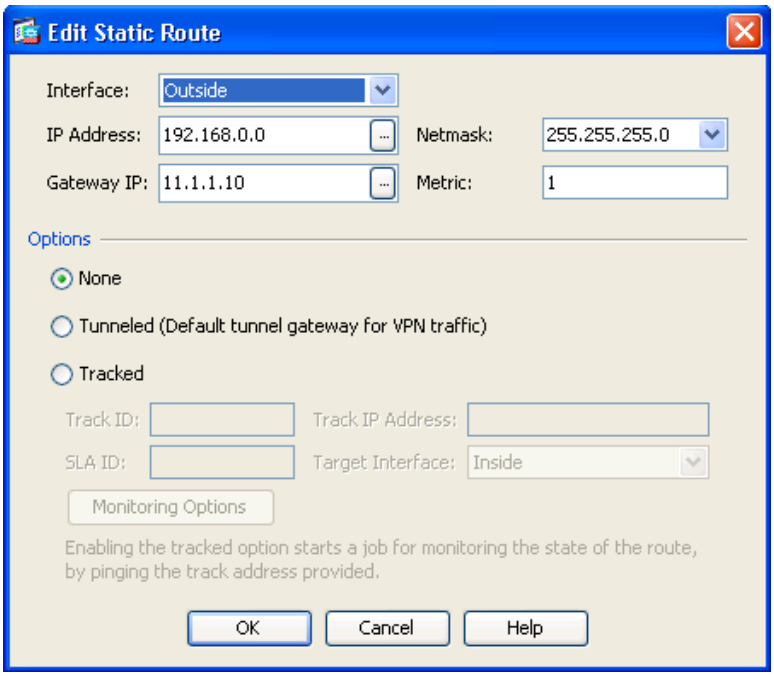
6.3. Configure Routing

Two routing rules must be set on the ASA5520. One for traffic that will be sent over the VPN tunnel and the other for traffic from devices behind the NETGEAR FV338 destined for any and all subnets inside the Corporate LAN/WAN.

1) In ASDM navigate to **Configuration → Routing→ Static Routes**. Click the **ADD** button.



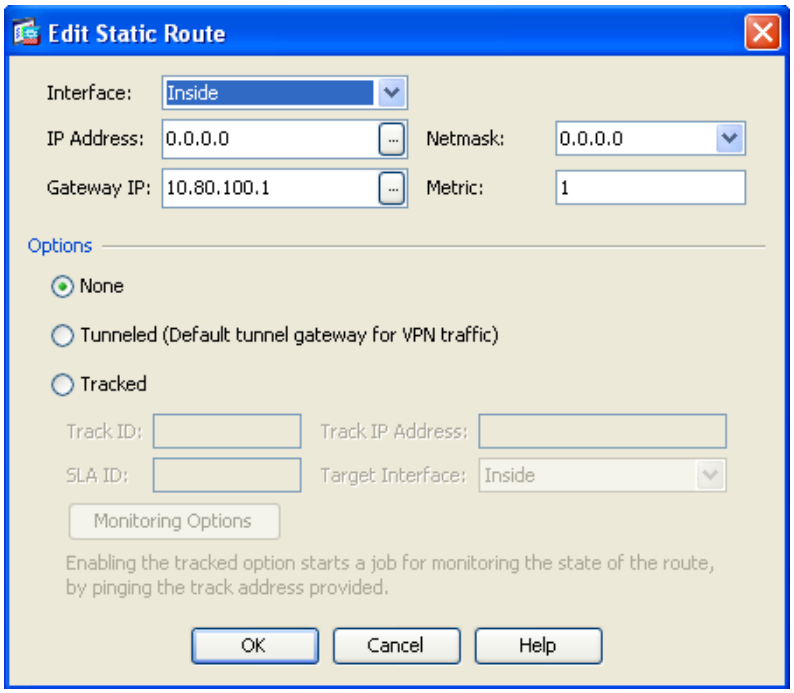
2) Enter the following values for traffic destined for the VPN tunnel:
   - **Interface:** Outside
   - **IP Address:** 192.168.0.0
   - **Mask:** 255.255.255.0
   - **Gateway IP:** 11.1.1.10
   - **Metric:** 1 (which is the default value)



Click **OK** when complete

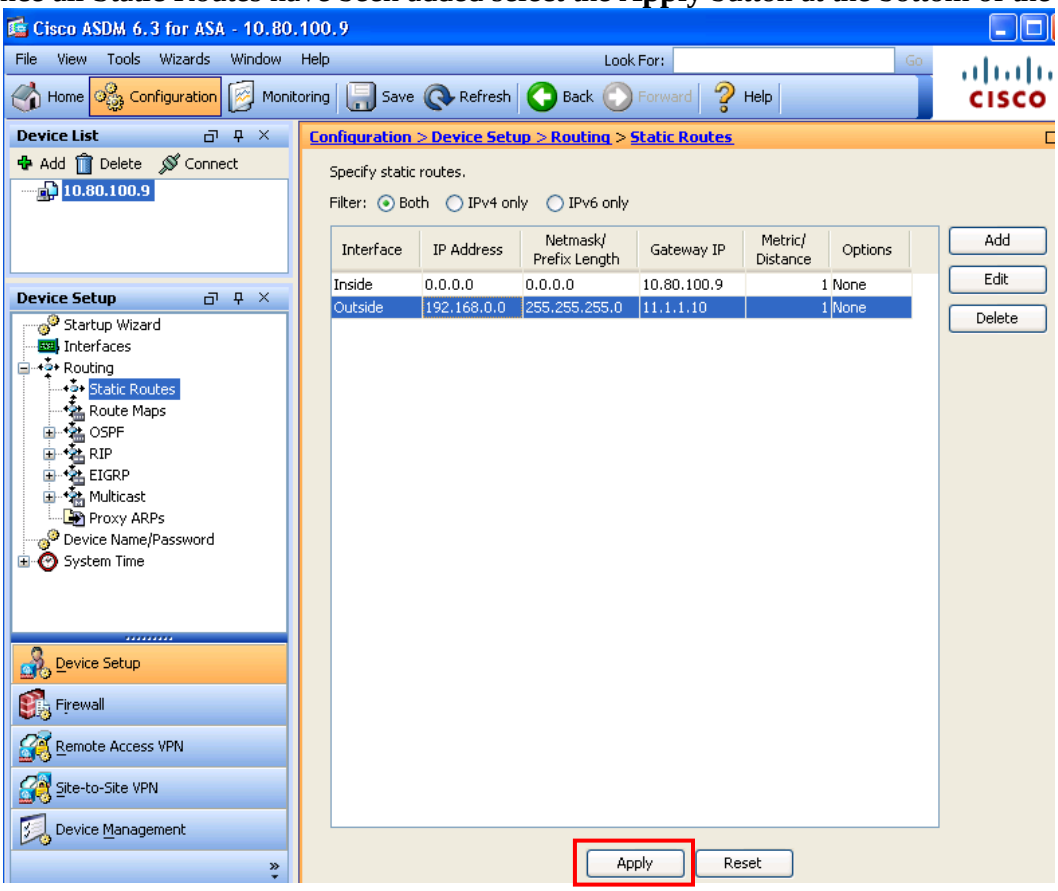
3) Select the **Add** button and enter the following values for all other traffic destined for the Corporate LAN/WAN. This is the 'Default Route'.

- **Interface:** Inside
- **IP Address:** 0.0.0.0
- **Mask:** 0.0.0.0
- **Gateway IP:** 10.80.100.1
- **Metric:** 1 (which is the default value)



Click **OK** when complete

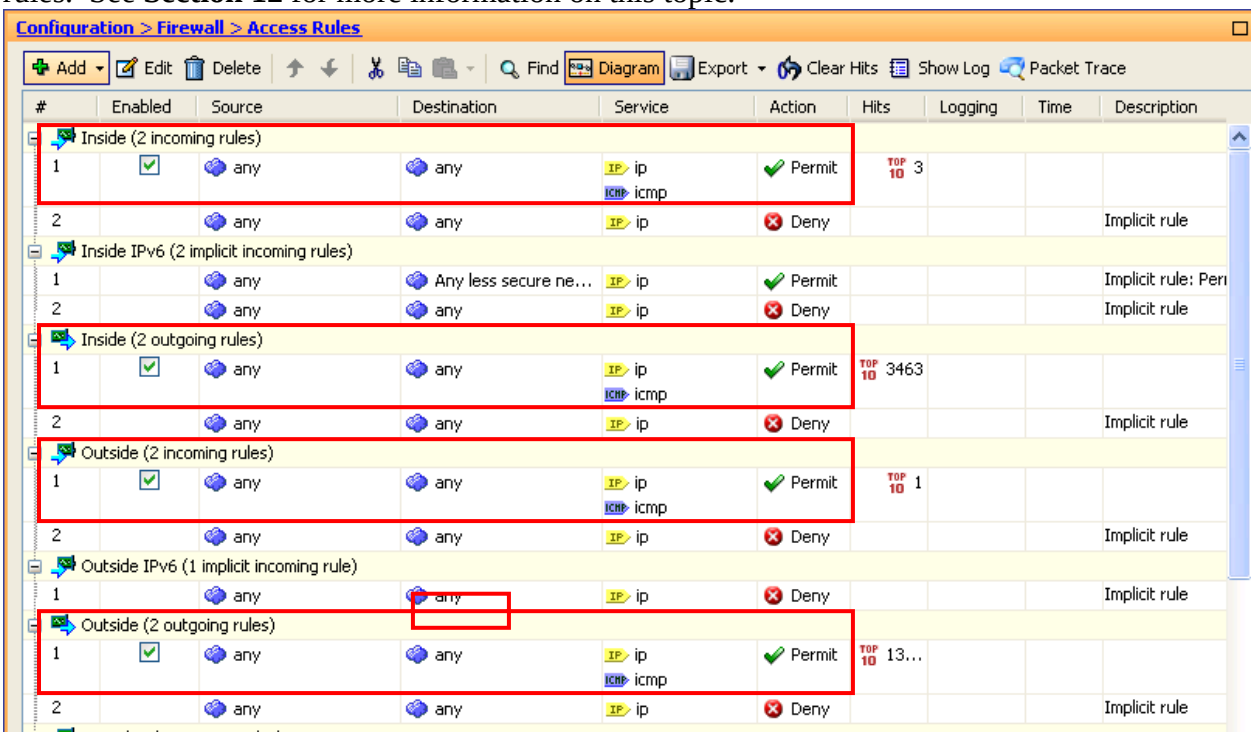
4) Once all Static Routes have been added select the **Apply** button at the bottom of the screen.



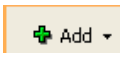
6.4. Configure Firewall Rules

By default the Cisco ASA5520 running FW 8.2(3) will have firewall rules in place to deny all traffic. Naturally for the sample configuration to function these rules needed to be overridden with less restrictive ones.

As shown below the rules highlighted in the red boxes are the ones that were added in support of the sample configuration. Its important to note that these added rules are intentionally simplistic. For an actual production environment, the network administrator may prefer to set more explicit rules. See **Section 12** for more information on this topic.

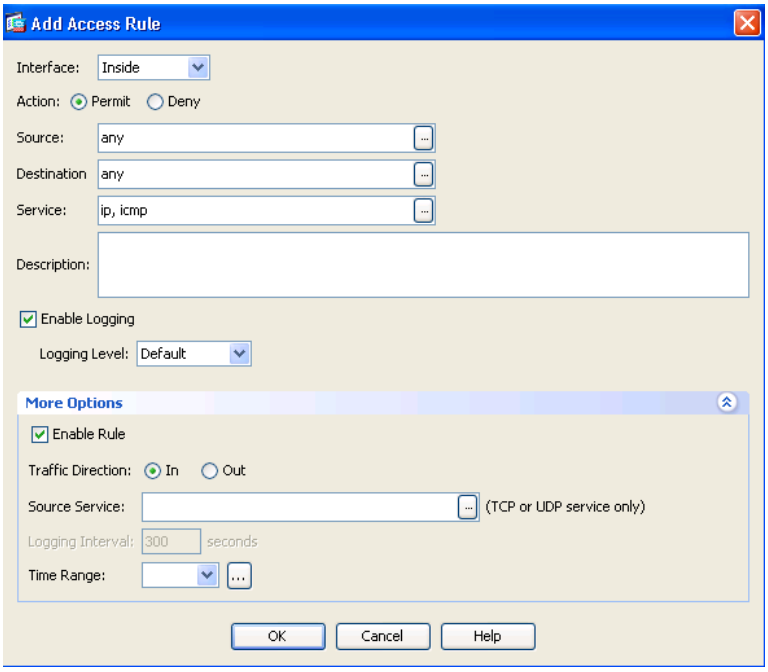


For the sample configuration two rules, an **incoming** rule and an **outgoing** rule were added for the **Inside** and **Outside** interfaces defined in **Section 6.1**. To add these rules, in ASDM navigate to **Configuration →Firewall→Access Rules**. A screen similar to that shown above will appear.

1) Begin by selecting one of the existing 'Implicit Rules' for either the **Inside** or **Outside** interfaces (do not select the IPv6 rules) so that it is highlighted in blue. Then from the top of the screen select the 

button followed by **Add Access Rule** from the drop-down. In the window that appears expand the **More Options** drop-down field and fill in the following information:
Interface will already be selected but indicates which interface the rule will be applied to.
   - Action: Select **Permit**
   - Source: **any**
   - Destination **any**
   - Service Enter **ip, icmp**

- Description: Optional field to record additional information
- Enable Logging: Check this box to log traffic that is allowed by this rule.
- Logging Level: Leave this at **Default** unless troubleshooting.
- Enable Rule: Check the box to ensure the rule is active.
- Traffic Direction: Default is '**In**'.

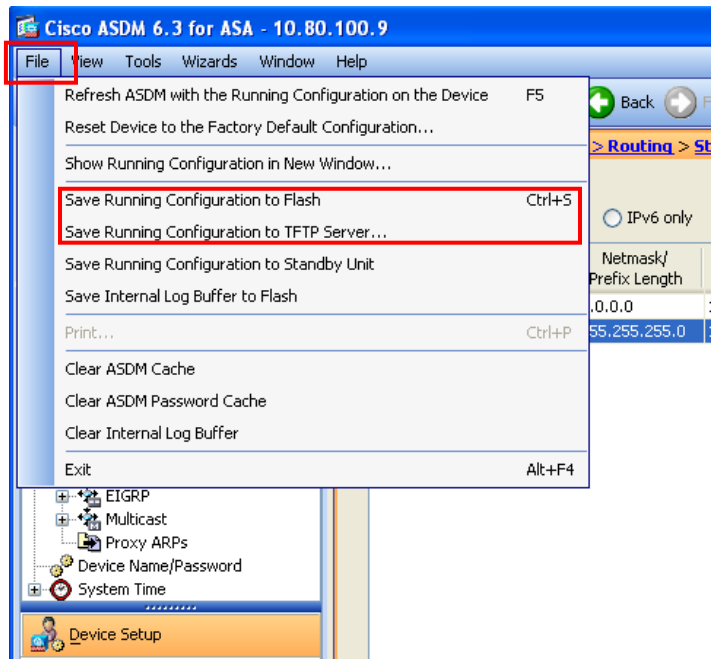


Click the **OK** button when complete

2) As shown above, an Incoming rule to allow IP and ICMP on the **Inside** interface was created. Next create an identical rule only select **Out** for **Traffic Direction**.
3) Repeat steps 1 & 2 for the **Outside** interface.
4) Once all four rules have been created select the **Apply** button to submit the new rules to the ASA5520.

6.5. Save Cisco ASA5520 Configuration

Once all changes on the ASA5520 are it's recommended to save the device configuration to flash memory. From ASDM first select the **File** menu at the upper-left corner, then select **Save Running Configuration to Flash** from the drop-down menu that appears. Optionally, to backup the configuration to a remote TFTP server, also select **Save Running Configuration to TFTP Server**.



7. Configure the NETGEAR ProSafe VPN Firewall FVS338

All administration of the FVS338 is accomplished via web browser. Initial administration of the FVS338 generally requires an Ethernet cable connected directly between a PC and a LAN interface on the FVS338. Please see **Section 12** Reference **[13]** for more information on this topic.

To begin administering the FVS338, launch a web browser and enter the following URL:
http://<IP address of the NETGEAR FVS338>
The default IP address of the FVS338 is 192.168.1.1 though for the sample configuration this was changed to 192.168.0.1 so as not to conflict with the dedicated management interface on the Cisco ASA5520. Log in using the appropriate credentials.

7.1. Configure NETGEAR FVS338 Ethernet Interfaces

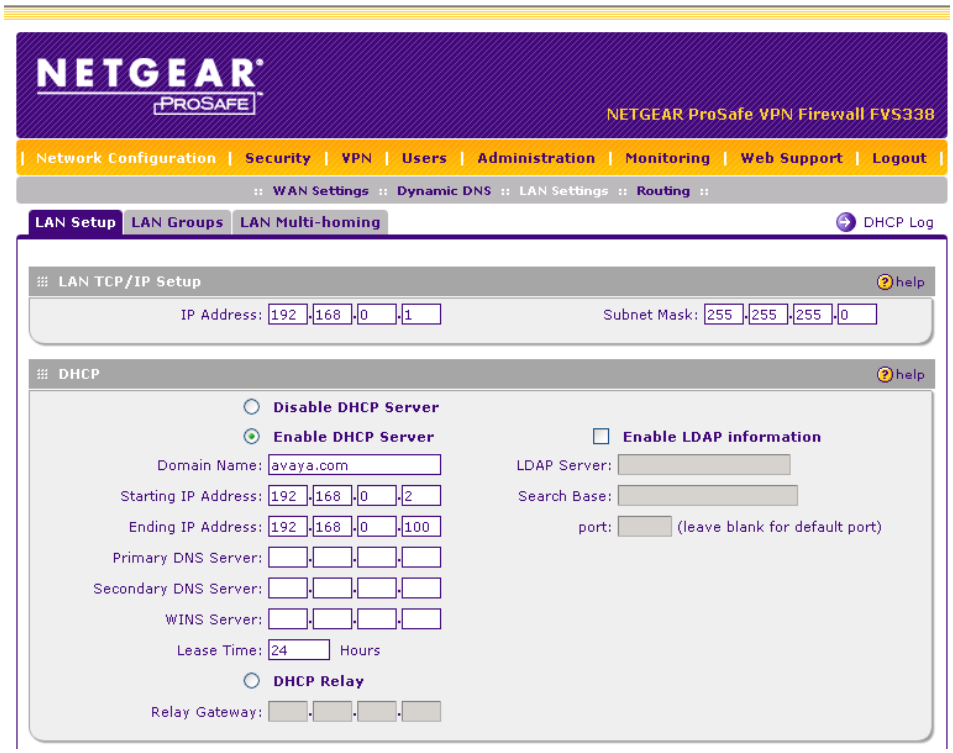
The steps below configure the IP addresses of the local LAN and WAN Ethernet interfaces for the configuration shown in **Figure 1**. The Cisco ASA5520 will use the IP address of the WAN Ethernet interface to establish an IPSec Tunnel.

NOTE: When deploying multiple VPN Gateways its important to consider the following:

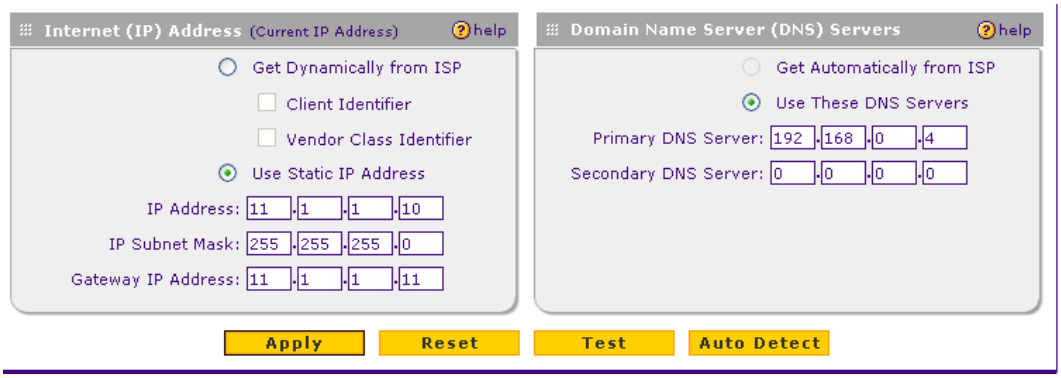
- Each VPN Gateway deployed on the Corporate LAN/WAN will need its LAN subnet to be unique across the entire enterprise.
- Whatever subnet is assigned to the LAN side of the VPN gateway will need to be routable throughout the corporate LAN/WAN.

1. *Configure IP address of the LAN interface**. Select **Network Configuration → LAN Settings → LAN Setup** from the top menu bar. Assign IP address **192.168.0.1** with a subnet mask of **255.255.255.0** for the LAN interface of the NETGEAR FVS338. Enable the DHCP Server so that it can automatically assign IP addresses to any Host that needs to connect to the Internet and VPN tunnel. Leave all other fields at their defaults.

* *Note*: Changing the LAN settings on the FVS338 is optional. Doing so will likely require reconfiguring the Ethernet interface on the PC being used to administer the FVS338.



2. *Configure the IP address of the WAN interface*. Select **Network Configuration → WAN Settings →Broadband ISP Settings** from the top menu bar. Scroll down to the section titled **Internet (IP) Address** and assign IP address **11.1.1.10** with an IP Subnet Mask of **255.255.255.0** and **Gateway IP address of 11.1.1.11** for the WAN interface of the NETGEAR FVS338.



7.2. Configure the VPN Tunnel

The NETGEAR FVS338 simplifies IPsec VPN tunnel configuration by utilizing a wizard for the initial configuration of both the IKE and VPN policies. The wizard sets the following default security parameters:

VPN Wizard default values

VPN Wizard default values for IKE:

	Gateway Policies	Client Policies
Exchange Mode:	Main	Aggressive
ID Type:	Local Wan IP	FQDN
Local WAN ID:	Local Wan IP	fvx_local.com
Remote WAN ID:	N/A	fvx_remote.com
Encryption Algorithm:	3DES	3DES
Authentication Algorithm:	SHA-1	SHA-1
Authentication Method:	Pre-shared Key	Pre-shared Key
Key-Group:	DH-Group 2 (1024 bit)	DH-Group 2 (1024 bit)
Life Time:	8 hours	8 hours

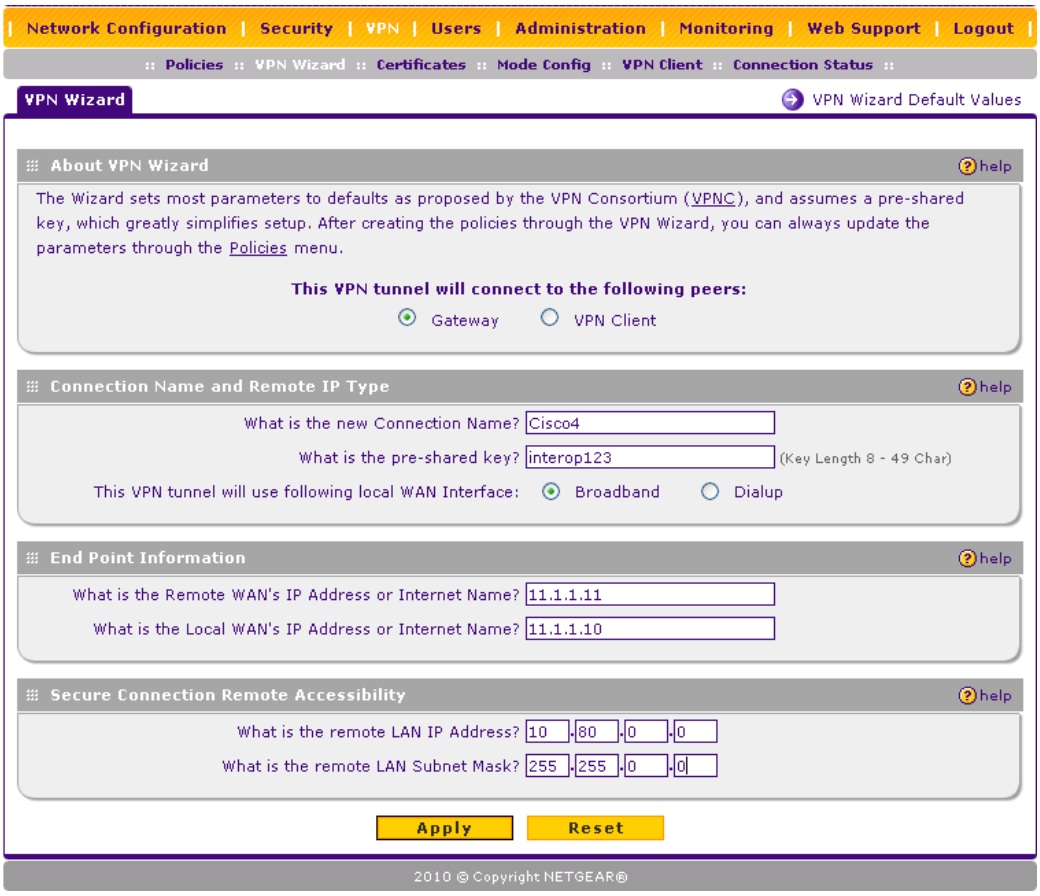
VPN Wizard default values for VPN:

Encryption Algorithm:	3DES
Authentication Algorithm:	SHA-1
Life Time:	1 hour
PFS Key Group:	DH-Group 2(1024 bit)
NETBIOS:	Enabled (Gateway Policies)
	Disabled (Client Policies)

2010 © Copyright NETGEAR®

Begin the VPN tunnel configuration by selecting **VPN → VPN Wizard.** In the screen that appears next the following values were used to create the sample configuration VPN tunnel:

- **This VPN Tunnel will connect to the following peers:** Gateway
- **What is the new connection name?** Cisco4
- **What is the pre-shared key?** interop123
- **This VPN tunnel will use the following local WAN interface:** Broadband
- **What is the Remote WAN's IP Address or Internet Name?** 11.1.1.11 (the 'Outside' interface on the ASA5520)
- **What is the Local WAN's IP Address or Internet Name?** 11.1.1.10 (the 'Internet' address of the FVS338)
- **What is the remote LAN IP Address?** 10.80.0.0 (the 'Inside' network on the ASA5520)
- **What is the remote LAN Subnet Mask?** 255.255.0.0

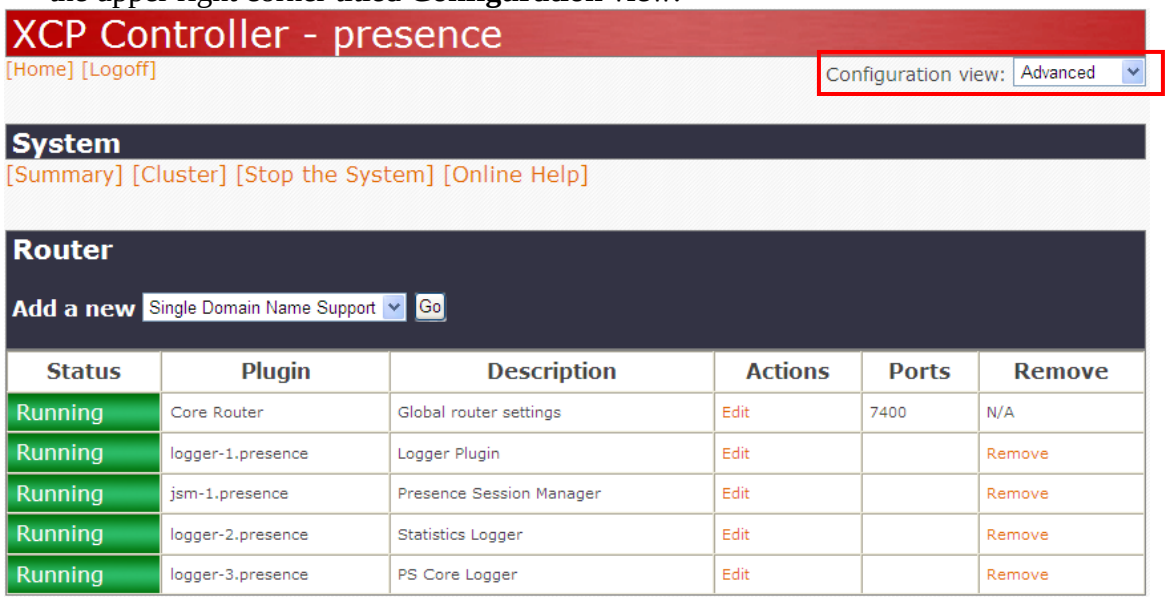


Click the **Apply** button when complete.

8. Configure Avaya Aura® Presence Services

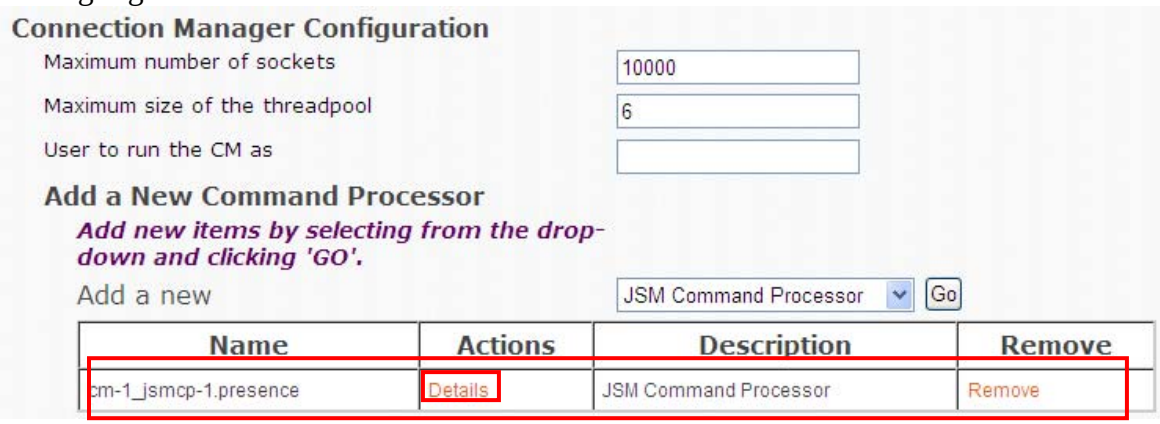
The A175DVD uses the XMPP protocol and port 5222 to communicate with the Avaya Aura® Presence Services server. Upon logging in to Session Manager, the A175DVD will open a socket to the Presence Server on this port. Eventually if no data is sent over the VPN connection to this port (such as an instant message), the VPN gateway will tear down the connection due to a lack of activity. This can cause an active call on the A175DVD to drop. To prevent this from happening one must simply enable the keep-alive mechanism on the Presence Server.

1) Begin by pointing a browser at the IP Address or FQDN of the Presence Server. In the screen that appears select the link titled "**Enter the Avaya Aura™ Presence Services Web Controller**"(not shown).
2) After logging in with the appropriate credentials select **Advanced** from the drop down in the upper right corner titled **Configuration view**.

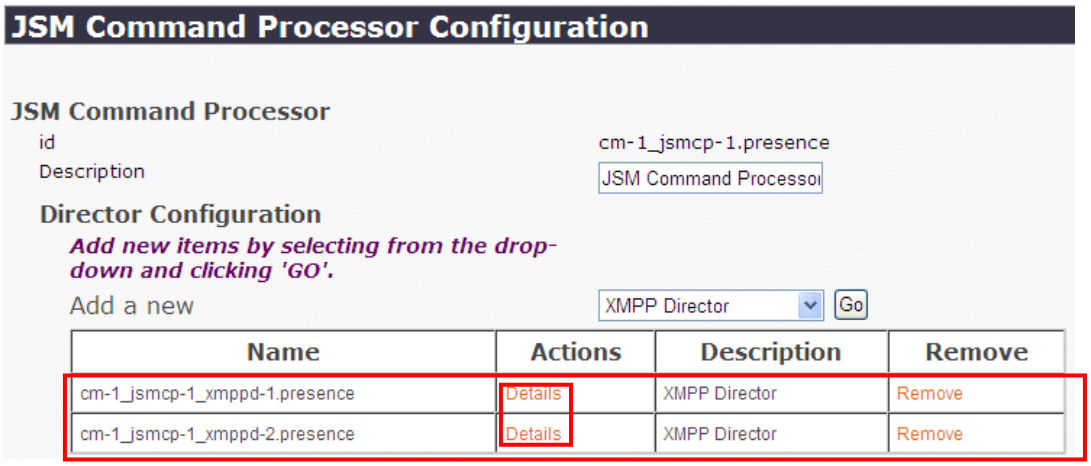


3) Scroll down and select the **Edit** link in row titled **Connection Manager**.

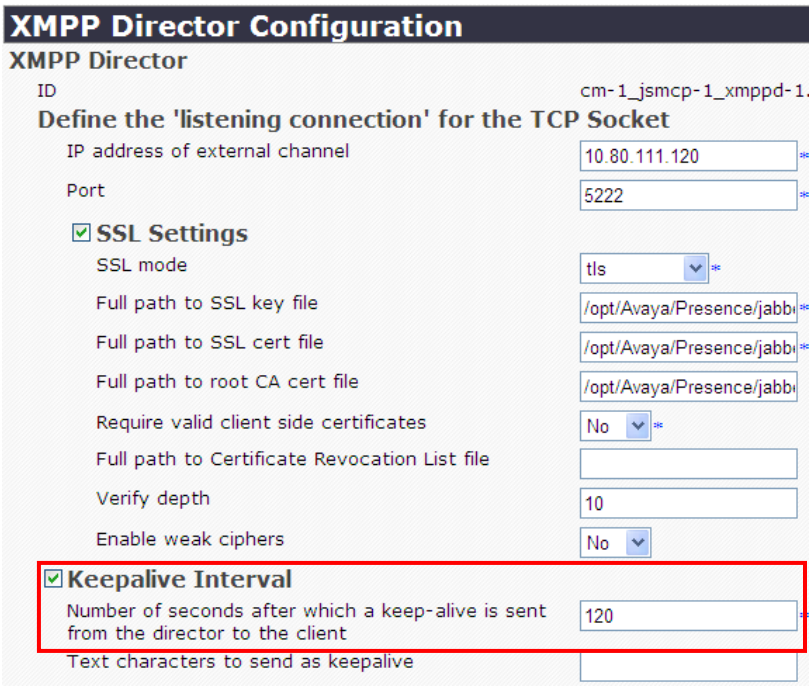
4) In the screen that appears next verify that in the upper right corner the **Configuration view** is set to **advanced** (not shown). Then scroll down to the section titled **Connection Manager Configuration**. Select the **Details** link in the existing **Command Processor** as highlighted below.



5) In the screen that appears next select the **Details** link for each of the **XMPP Directors** as shown below.



6) For each **XMPP Director** shown above select the checkbox next to **Keepalive Interval** and enter in a value for **Number of seconds after which a keep-alive is sent from the director to the client.** A value of **120** is sufficient to keep the connection to port 5222 active even when there are no Instant Messages being sent or received by the A175DVD.



7) Be sure to set the keep-alive for each **XMPP Director** listed in **Step 5** above. After setting this value, scroll down to the bottom of the screen and hit the **Select** button (not shown). Then select the **Submit** button on each screen until returning to main **XCP Controller** page.
8) Once at the main **XCP Controller** page select the **Apply** link for the **Connection Manager** followed by the **Stop** link as shown below.

9) Wait for the **Connection Manager** status to change to **Stopped** and select the **Start** link. The service should once again show a status of **Running** (not shown). Hit **F5** to refresh the browser if the service does appear as Running after a few seconds.

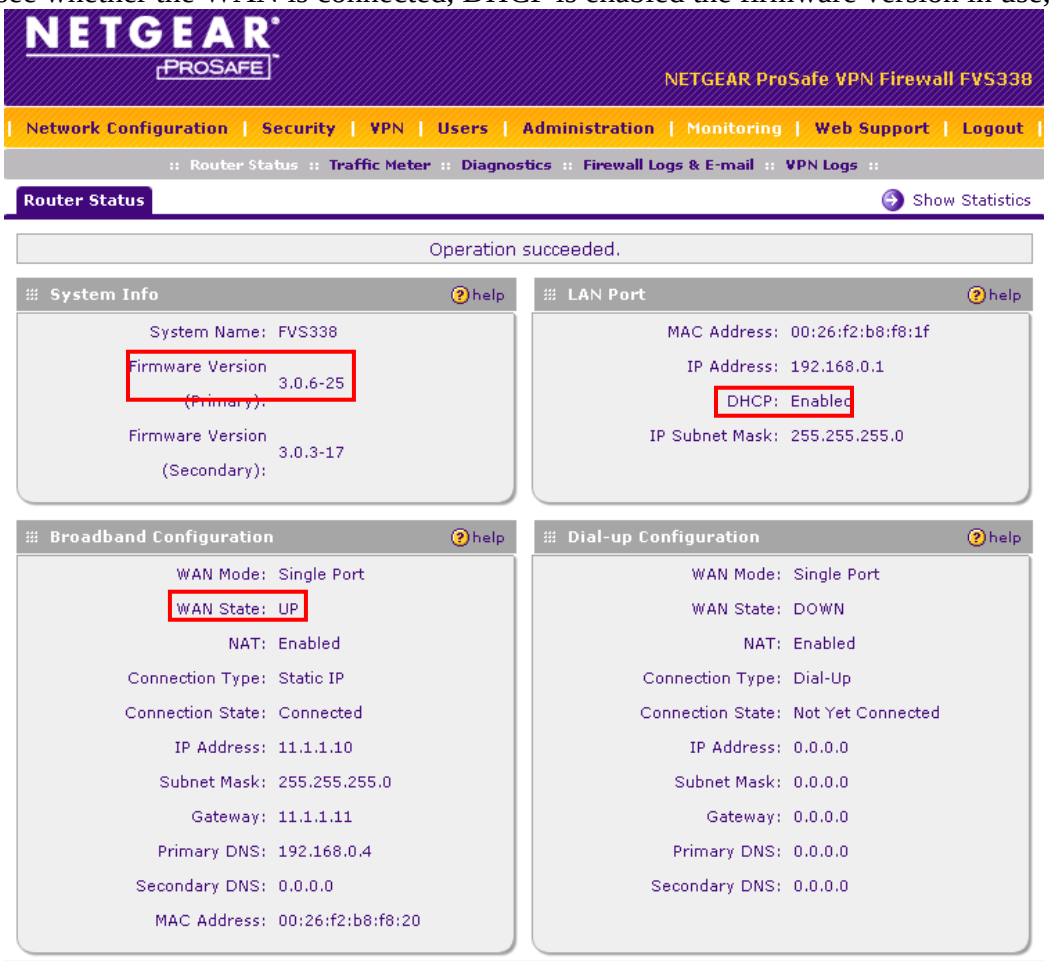
9. Verify VPN and WAN Connectivity

Both the ASA5520 and FVS338 provide tools to help verify WAN connectivity and the status of the VPN tunnel. Avaya Aura® System Manager also provides several useful tools.

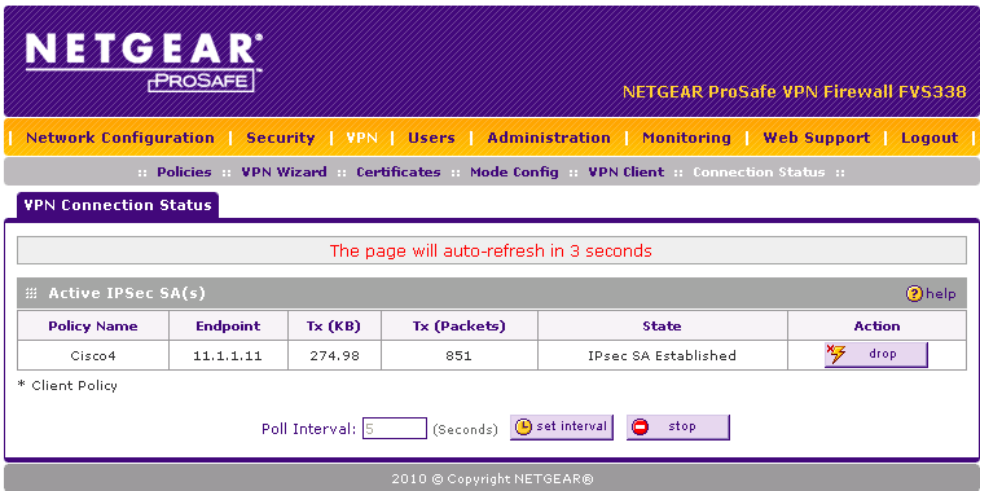
9.1. Verify Status of the NETGEAR FVS338

There are several tools available on the FVS338 admin web page one can utilize to verify connectivity status.

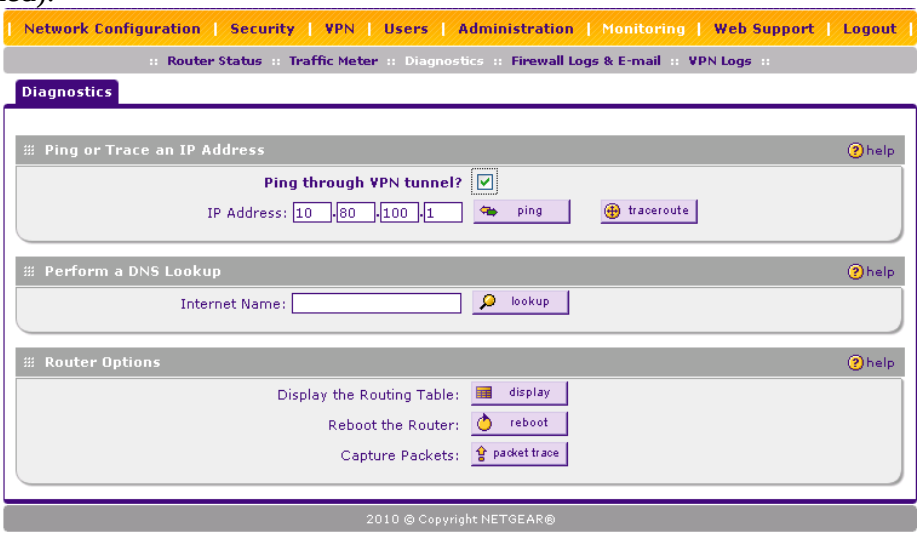
1) Upon login to web admin page the **Router Status** page is displayed. From here one can see whether the WAN is connected, DHCP is enabled the firmware version in use, etc.



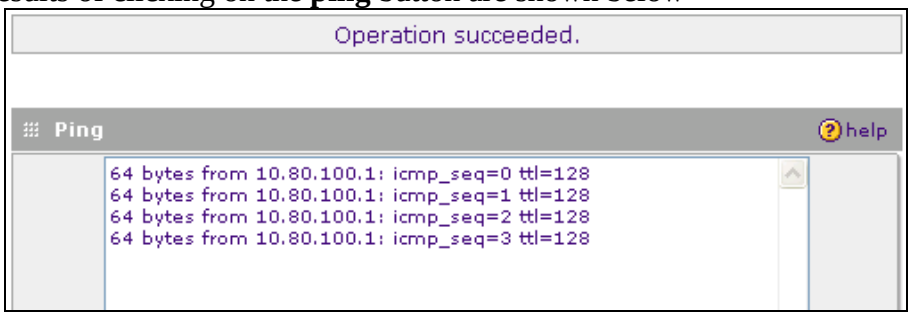
2) From the FVS338 web admin page navigate to **VPN→Connection Status**. As shown below the VPN Connection Status show the IPsec tunnel is established.



3) From the FVS338 web admin page navigate to **Monitoring→Diagnostics** and enter in an IP address to PING. If the tunnel is functional this should succeed for an IP address on Corporate LAN/WAN side of the tunnel (note that **Ping through VPN tunnel** is checked).



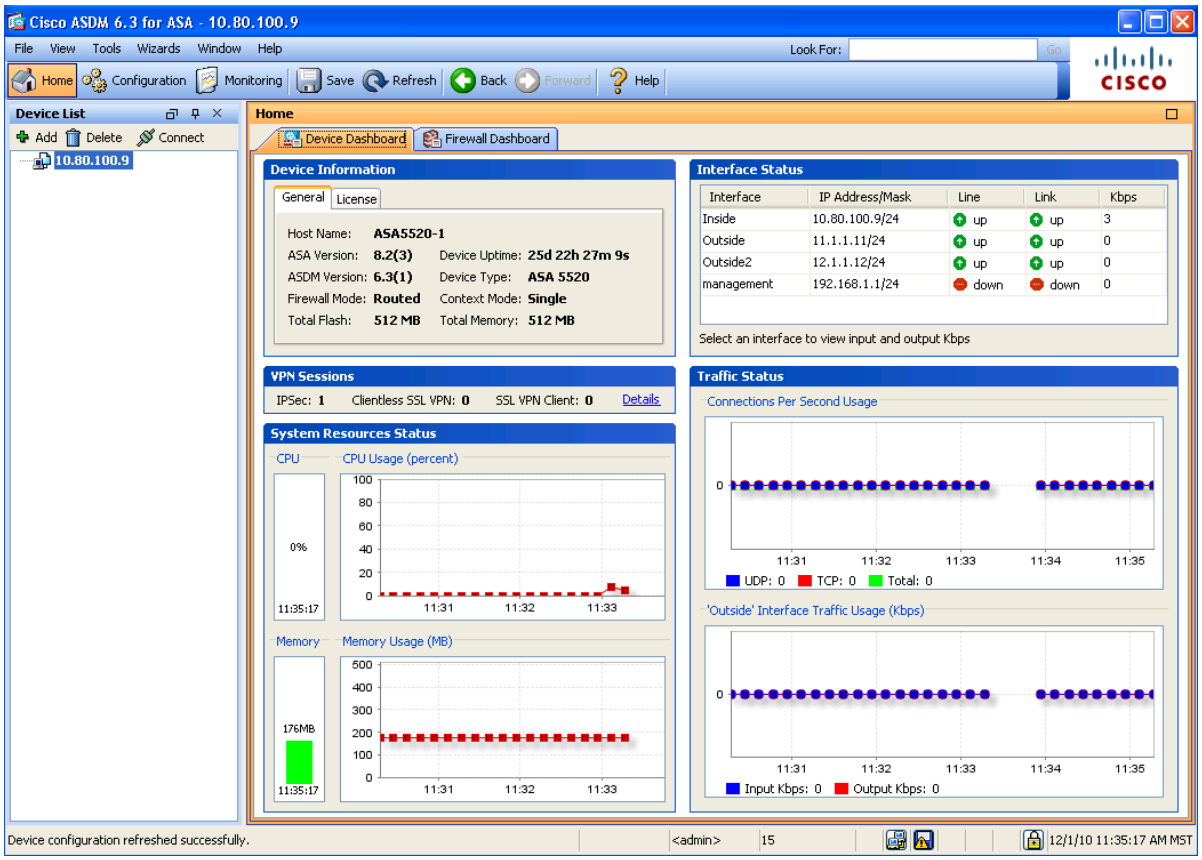
The results of clicking on the **ping** button are shown below



9.2. Verify Status of the Cisco ASA5520

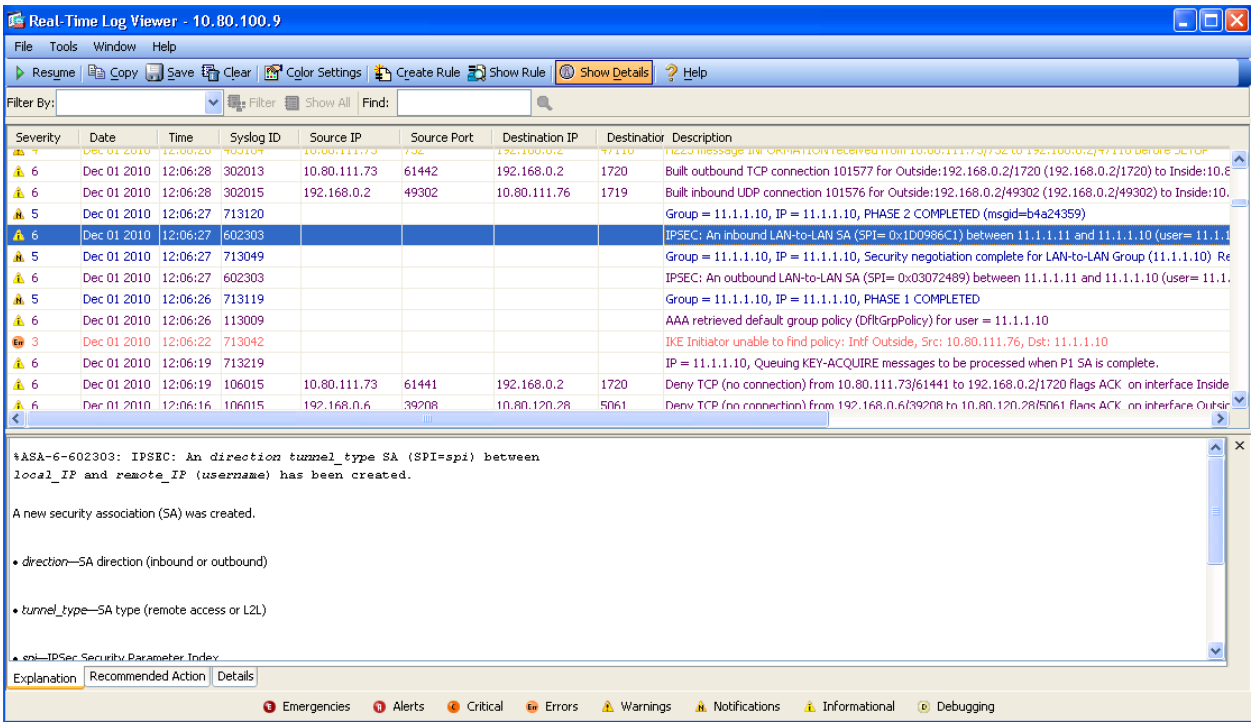
Cisco ASDM also provides a number of monitoring and troubleshooting tools

1) Upon logging to ASDM the Home screen will display the **Device Dashboard**. From this dashboard its possible a number of items can be verified. As shown from the sample configuration the ASA version is **8.2(3)**, the **Inside & Outside** interfaces are 'up', while the **management** interface is 'down'. The VPN Sessions box shows that there is one active IPsec tunnel and the Traffic Status window shows 0 Kbps of traffic on the Outside interface.



2) Another useful tool available in ASDM is the Real-time Log Viewer. To access this tool, in ASDM navigate to **Monitoring→Logging→Real-Time Log Viewer.** In the screen that appears select Debugging from the drop-down next to Logging Level: then select the **View** button (not shown).

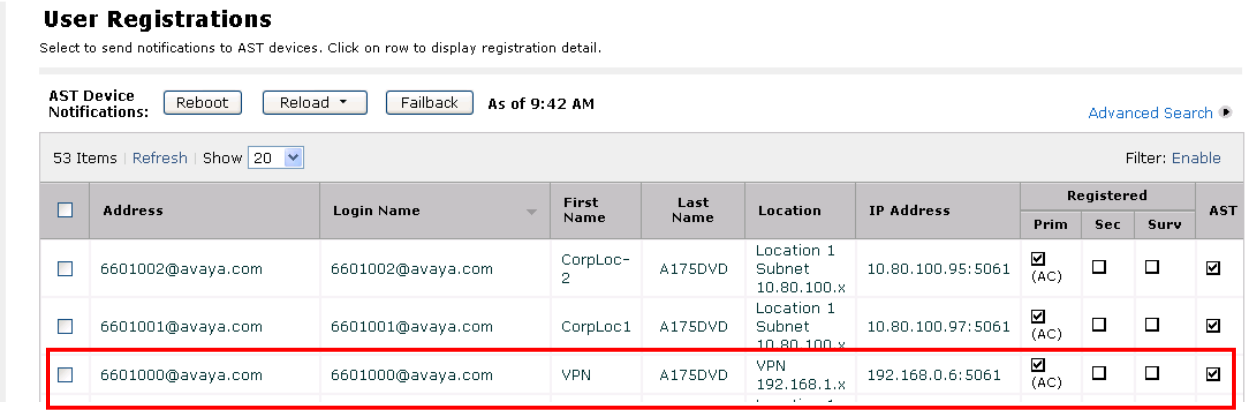
   As shown below the Real-Time Log viewer in debug mode displays information about all IP conversations happening in the ASA5520. The screenshot below shows the some of the packets being exchanged in order to establish the IPsec VPN tunnel. By selecting a row in the log viewer additional information about the log entry is displayed in the lower-half of the split window.



9.3. Verify Registration of A175DVD

Once the ASA5520 and FVS338 have successfully established a VPN tunnel it should be possible to register an A175DVD at the home-office location. Avaya Aura® System Manager provides a way to verify the registration of SIP devices.

In the left pane of System Manager select Elements→**Session Manager→System Status→User Registrations** to see the SIP endpoint registration status including the A175DVD extension **6601000** at the home-office.



10. Validation

The following validation steps were tested using the sample configuration. The following steps can be used to verify installation in the field.

1. Verify on both the FVS338 and ASA5520 that the VPN tunnel has been successfully established.
2. Verify that the Avaya A175 Desktop Video Device extension 6601000 located at the Home-Office will bootup, receive an IP address from the FVS338 and is able to register to Session Manager across the VPN tunnel (with manual configuration of the HTTP server).
3. Verify an audio call can be made with clear audio between the A175DVD located at each end of the VPN tunnel. Verify the call is active on the SIP Trunk within Communication Manager.
4. Verify a video call can be made with clear audio & video between s A175DVD stations located at each end of the VPN tunnel. Verified the call was seen to be active on the SIP Trunk within Communication Manager.
5. Verify bandwidth limits as set on the ip-network-region form are honored for voice and video calls.
6. Verify audio and video between the A175DVD at the home-office location and one-X Communicator at the Corporate LAN/WAN location.
7. Verify supplementary features such as Call Hold, Call Forward, Conference and Transfer could be completed between the Avaya Desktop Video Devices. Verify Presence status updates for Contacts in the Buddy List when those contacts Presence status changes (off-hook, manually made unavailable, etc.)
8. Verify instant messages can be sent back-and-forth between two A175DVD's and between an A175DVD and one-X Communicator across the VPN tunnel.
9. Verify conferencing reservations created on the Avaya Aura® Conferencing server the first time a new A175DVD logged in from the Home-Office
10. Verify ad-hoc audio and video conferences can be created between the A175DVD at the home-office and endpoints located at Corporate LAN/WAN.

11. Conclusion

These Application Notes have described the basic administration steps required to create a Site-to-Site IPsec VPN tunnel between a Cisco ASA5520 and a NETGEAR FVS338 in support of an Avaya A175 Desktop Video Device located at a remote location at the far-end of the VPN tunnel. While the sample configuration uses a very basic setup, it should provide the basis for configuring a similar setup in a production environment.

12. Additional References

This section references additional documentation relevant to these Application Notes.

Avaya Documentation

Additional Avaya product documentation is available at http://support.avaya.com.

[1] *Administering Avaya Aura® Session Manager.* August 2010. DocID 03-603324.

[2] *Installing Avaya Aura® Session Manager*, January 2010. DocID 03-603473
[3] *Administering Avaya Aura® Communication Manager Server Options*, June 2010. DocID 03-603479
[4] *Administering Avaya Aura® System Manager*. June 2010.
[5] *Application Notes for Configuring Avaya Desktop Video Device to connect to Avaya Aura® Session Manager with Avaya Aura® Communication Manager as an Evolution Server Issue* – Issue 1.0
[6] *Application Notes for configuring Avaya Desktop Video Device to connect to Avaya Aura® Session Manager with Avaya Aura® Communication Manager as a Feature Server Issue* – Issue 1.0
[7] *Administering Avaya Aura® Presence Services 6.0.* Issue 1, August 2010.
[8] *Troubleshooting Avaya Aura® Presence Services 6.0.* August 2010.
[9] *Implementing Avaya Aura® Conferencing*. Issue 1, DocID 04-603508.

Cisco Documentation

Additional **Cisco** product documentation is available at http://www.cisco.com.

[10] *Cisco ASA 5500 Series Getting Started Guide*. Software Version 8.0. DOC-78-18002-01.
[11] *Cisco ASA 5500 Series Configuration Guide using ASDM.* Software Version 6.3. (on-line only)
[12] *Release Notes for Cisco ASDM 6.2(x).*
http://www.cisco.com/en/US/docs/security/asa/asa83/asdm63/release/notes/asdmrn63.html

NETGEAR Documentation

Additional **NETGEAR** product documentation is available at http://www. netgear.com.

[13] *ProSafe VPN Firewall 50 FVS338 Reference Manual*.v1.0. Doc 202-10046-09

13. Appendix A – Cisco ASA5520 Configuration

Shown below is the complete configuration of the Cisco ASA5520. Many of the parameters not discussed in these Application Notes are present by default.

```
: Saved
:
ASA Version 8.2(3)
!
hostname ASA5520-1
domain-name avaya.com
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
!
interface GigabitEthernet0/0
 nameif Outside
 security-level 0
 ip address 11.1.1.11 255.255.255.0
!
interface GigabitEthernet0/1
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/2
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/3
 nameif Inside
 security-level 100
 ip address 10.80.100.9 255.255.255.0
!
interface Management0/0
 nameif management
 security-level 100
 ip address 192.168.1.1 255.255.255.0
 management-only
!
boot system disk0:/asa823-k8.bin
ftp mode passive
clock timezone MST -7
clock summer-time MDT recurring
dns server-group DefaultDNS
 domain-name avaya.com
same-security-traffic permit inter-interface
same-security-traffic permit intra-interface
object-group network DM_INLINE_NETWORK_1
 network-object host 11.1.1.10
```

```
 network-object 192.168.0.0 255.255.255.0
object-group protocol DM_INLINE_PROTOCOL_1
 protocol-object ip
 protocol-object icmp
object-group protocol DM_INLINE_PROTOCOL_2
 protocol-object ip
 protocol-object icmp
object-group network DM_INLINE_NETWORK_2
 network-object host 12.1.1.10
 network-object 192.168.10.0 255.255.255.0
object-group protocol DM_INLINE_PROTOCOL_3
 protocol-object ip
 protocol-object icmp
object-group protocol DM_INLINE_PROTOCOL_4
 protocol-object ip
 protocol-object icmp
object-group protocol DM_INLINE_PROTOCOL_5
 protocol-object ip
 protocol-object icmp
object-group protocol DM_INLINE_PROTOCOL_6
 protocol-object ip
 protocol-object icmp
access-list Outside_access_in extended permit object-group
DM_INLINE_PROTOCOL_6 any any
access-list Outside_access_out extended permit object-group
DM_INLINE_PROTOCOL_1 any any
access-list Inside_access_in extended permit object-group
DM_INLINE_PROTOCOL_5 any any
access-list Inside_access_out extended permit object-group
DM_INLINE_PROTOCOL_2 any any
access-list Outside_1_cryptomap extended permit ip 10.80.0.0 255.255.0.0
object-group DM_INLINE_NETWORK_1
access-list Inside_nat0_outbound extended permit ip 10.80.0.0 255.255.0.0
host 11.1.1.10
access-list Inside_nat0_outbound extended permit ip 10.80.0.0 255.255.0.0
object-group DM_INLINE_NETWORK_2
access-list Outside2_access_out extended permit object-group
DM_INLINE_PROTOCOL_4 any any
access-list Outside2_access_in extended permit object-group
DM_INLINE_PROTOCOL_3 any any inactive
pager lines 24
logging enable
logging asdm informational
mtu Outside 1500
mtu Inside 1500
mtu management 1500
mtu Outside2 1500
no failover
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm-631.bin
no asdm history enable
arp timeout 14400
nat (Inside) 0 access-list Inside_nat0_outbound
nat (management) 0 0.0.0.0 0.0.0.0
access-group Outside_access_in in interface Outside
access-group Outside_access_out out interface Outside
```

```
access-group Inside_access_in in interface Inside
access-group Inside_access_out out interface Inside
access-group Outside2_access_in in interface Outside2
access-group Outside2_access_out out interface Outside2
route Inside 0.0.0.0 0.0.0.0 10.80.100.1 1
route Outside 192.168.0.0 255.255.255.0 11.1.1.10 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat
0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect
0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
dynamic-access-policy-record DfltAccessPolicy
http server enable
http 10.80.0.0 255.255.0.0 Inside
http 192.45.130.0 255.255.255.0 Inside
http 192.168.1.0 255.255.255.0 management
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
crypto ipsec transform-set ESP-3DES-SHA esp-3des esp-sha-hmac
crypto ipsec security-association lifetime seconds 28800
crypto ipsec security-association lifetime kilobytes 4608000
crypto map Outside_map 1 match address Outside_1_cryptomap
crypto map Outside_map 1 set pfs
crypto map Outside_map 1 set peer 11.1.1.10
crypto map Outside_map 1 set transform-set ESP-3DES-SHA
crypto map Outside_map interface Outside
crypto isakmp enable Outside
crypto isakmp enable Outside2
crypto isakmp policy 10
 authentication pre-share
 encryption 3des
 hash sha
 group 2
 lifetime 86400
telnet 10.80.0.0 255.255.0.0 Inside
telnet 192.45.130.0 255.255.255.0 Inside
telnet timeout 5
ssh timeout 5
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
ntp server 10.80.111.30 source Inside prefer
ntp server 10.80.60.2 source Inside
webvpn
tunnel-group 11.1.1.10 type ipsec-l2l
tunnel-group 11.1.1.10 ipsec-attributes
 pre-shared-key *****
!
class-map inspection_default
 match default-inspection-traffic
!
```

```
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
  inspect ip-options
!
service-policy global_policy global
prompt hostname context
call-home
 profile CiscoTAC-1
  no active
  destination address http
https://tools.cisco.com/its/service/oddce/services/DDCEService
  destination address email callhome@cisco.com
  destination transport-method http
  subscribe-to-alert-group diagnostic
  subscribe-to-alert-group environment
  subscribe-to-alert-group inventory periodic monthly
  subscribe-to-alert-group configuration periodic monthly
  subscribe-to-alert-group telemetry periodic daily
Cryptochecksum:daccfab0bf83f1069f7546b13ae47662
: end
asdm image disk0:/asdm-631.bin
no asdm history enable
```

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