



**Avaya Solution & Interoperability Test Lab**

---

## **Configuring Juniper Networks SSL VPN Security Appliance to Support Avaya IP Softphone – Issue 1.0**

### **Abstract**

These Application Notes describe the steps to configure the Juniper Networks Secure Access SSL VPN appliance to support the Avaya IP Softphone application.

The Juniper Instant Virtual Extranet (IVE) serves as the underlying operating system for all Juniper SSL VPN appliances. The configuration steps described in these Application Notes utilize a Juniper Secure Access model 4000 (Juniper SA-4000). However, these configuration steps can be applied to other Juniper Secure Access models using the IVE software version specified.

# TABLE OF CONTENTS

<b>1. INTRODUCTION.....</b>	<b>3</b>
1.1. OVERVIEW .....	3
<b>2. NETWORK TOPOLOGY .....</b>	<b>6</b>
<b>3. EQUIPMENT AND SOFTWARE VALIDATED.....</b>	<b>8</b>
<b>4. JUNIPER SA-4000 CONFIGURATION .....</b>	<b>8</b>
4.1. NETWORK CONNECT LICENSE VERIFICATION .....	9
4.2. USER ROLE.....	10
4.3. NETWORK CONNECT .....	14
4.4. USER ACCOUNTS.....	17
4.5. AUTHENTICATION REALM .....	20
<b>5. AVAYA COMMUNICATION MANAGER CONFIGURATION .....</b>	<b>24</b>
5.1. OVERVIEW .....	24
5.2. ADD IP SOFTPHONE STATIONS .....	24
5.3. ASSIGNMENT OF ENDPOINTS TO NETWORK REGIONS.....	25
5.4. CODEC SET CONFIGURATION .....	25
5.5. IP NETWORK REGION CONFIGURATION .....	27
<b>6. REMOTE PC .....</b>	<b>29</b>
6.1. STARTING THE SSL VPN AND NETWORK CONNECT SESSION .....	29
6.2. STARTING THE AVAYA IP SOFTPHONE .....	33
<b>7. VERIFICATION.....</b>	<b>34</b>
7.1. NETWORK CONNECT VIRTUAL ADAPTER .....	34
7.2. CONNECTIVITY .....	35
7.3. ACTIVE SSL VPN USERS .....	37
7.4. NETWORK CONNECT TRANSPORT MODE.....	37
7.5. AVAYA COMMUNICATION MANAGER “LIST REGISTERED-IP-STATIONS” .....	38
7.6. AVAYA COMMUNICATION MANAGER “STATUS STATION” .....	38
<b>8. TROUBLESHOOTING .....</b>	<b>40</b>
8.1. JUNIPER SA-4000 LOGS .....	40
<b>9. CONCLUSION.....</b>	<b>44</b>
<b>10. REFERENCES .....</b>	<b>44</b>

# 1. Introduction

These Application Notes describe the steps to configure a Juniper Networks Secure Access SSL VPN appliance to support the Avaya IP Softphone application.

While all configuration modes offered by the Avaya IP Softphone are expected to interoperate with a Juniper SSL VPN, the Road Warrior configuration option is utilized in the sample configuration presented in these Application Notes. The Road Warrior configuration, also referred to as the Voice over IP configuration, makes full use of the PC's IP network connection for all signaling (H.323) and voice (Real-time Transport Protocol - RTP) communications.

Juniper Instant Virtual Extranet (IVE) serves as the underlying operating system for all Juniper SSL VPN appliances. IVE is a hardened network operating system serving as a secure intermediary for data flows between external users on the public Internet and private internal corporate networks and resources.

The configuration steps described in these Application Notes utilize a Juniper Secure Access model 4000, referred to as "Juniper SA-4000" throughout the remainder of these Application Notes. These configuration steps can be applied to other Juniper Secure Access models using the IVE software version specified in **Table 2**.

## 1.1. Overview

The Juniper SA-4000 is a Secure Sockets Layer (SSL) Virtual Private Network (VPN) appliance capable of terminating SSL encrypted sessions from remote connections. One of the fundamental benefits of SSL VPNs is the ability to use a Web browser to securely access internal corporate resources of a private enterprise network taking advantage of the inherent SSL functionality built into standard Web browsers. Secure access to the enterprise network from a Web browser accommodates most users' application needs operating at the application-layer, i.e., e-mail, web browsing and file sharing. However, not all applications operate at the application layer, with some requiring direct network layer access.

Applications requiring direct network layer access, such as Avaya IP Softphone, interface directly with the IP network resources of the computer's operating system on which the application is running. To function in an SSL VPN environment, these applications require a network layer client application, referred to by Juniper as a "lightweight client". The name of Juniper's network-layer client application is Network Connect.

Juniper's Network Connect client is pushed (downloaded) from the Juniper SA-4000 to the remote PC and installed automatically as either an Active-X control or a Java applet when a user with Network Connect privileges first starts an SSL VPN session. Upon subsequent SSL VPN sessions, the Juniper SA-4000 will first check for the existence of the Network Connect client on the remote PC, then check the Network Connect client version (upgrade if necessary) and lastly start the Network Connect session automatically based on the user's profile settings.

Juniper Network Connect can be configured to operate in two transport modes: ESP mode or oNCP mode. The names of these two Juniper Network Connect transport modes are associated with the transport protocol used for each. ESP mode uses the Encapsulating Security Payload (ESP) protocol (RFC 2406) [6] while oNCP uses Juniper's Optimized Network Communications Protocol (oNCP). ESP, being a key component of IPSec, utilizes traditional IPSec encryption and authentication methods (AES/SHA1/MD5) using UDP port 4500 while oNCP utilizes SSL encryption methods (RC4-128) using TCP port 443.

NC Mode	Encryption	Transport Protocol	Port
oNCP: Optimized Network Communications Protocol	SSL: Rivest Cipher 4-128 (RC4-128)	TCP	443
ESP: Encapsulating Security Payload	IPSec: AES / SHA1 AES / MD5	UDP	4500

**Table 1 – Juniper Network Connect Transport Mode Summary**

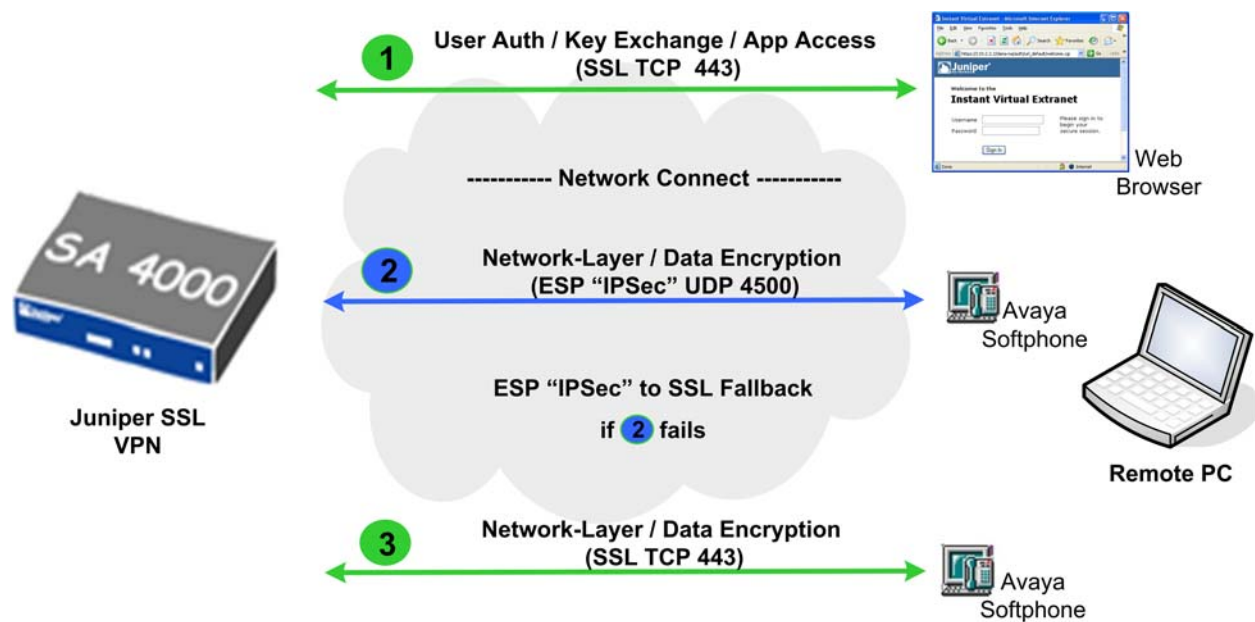
**Note:** oNCP supersedes Juniper's older NCP protocol. References to NCP remain in IVE for backwards compatibility.

Because ESP mode has many IPSec components, it provides an IPSec like transport connection. The primary difference between Juniper Network Connect operating in ESP mode and a traditional IPSec client has to do with remote user authentication. In Juniper Network Connect ESP mode, remote user authentication is performed through a web browser of the remote PC over the SSL (HTTPS) connection to the Juniper SA-4000. Once user authentication has successfully completed and encryption keys have been exchanged, the Juniper Network Connect client starts an ESP connection to the Juniper SA-4000 encrypting all network layer traffic destined to the enterprise network i.e., Avaya IP Softphone signaling and voice traffic.

Juniper Network Connect can be configured to first attempt a connection using the ESP mode. If the connection is not able to be established (i.e. a firewall is blocking UDP port 4500 between the remote PC and the Juniper SA-4000) a connection using oNCP (SSL) will be attempted. This feature is referred to by Juniper as ESP-to-NCP fallback.

**Figure 1** below shows the typical flow of a Juniper Network Connect session:

1. The session starts with an HTTPS (SSL) connection from a Web browser to the SA-4000 for user authentication.
2. If the authenticated user profile is configured to auto start the Network Connect session; the Network Connect client initiates a connection to the Juniper SA-4000 using the ESP transport mode.
3. If the first Network Connect connection attempt using ESP fails, (i.e., a firewall between the Remote PC and the SA-4000 is blocking UDP port 4500) the Network Connect client “falls back” to the oNCP transport mode making another connection attempt using SSL.



**Figure 1 – Juniper Network Connect**

## 2. Network Topology

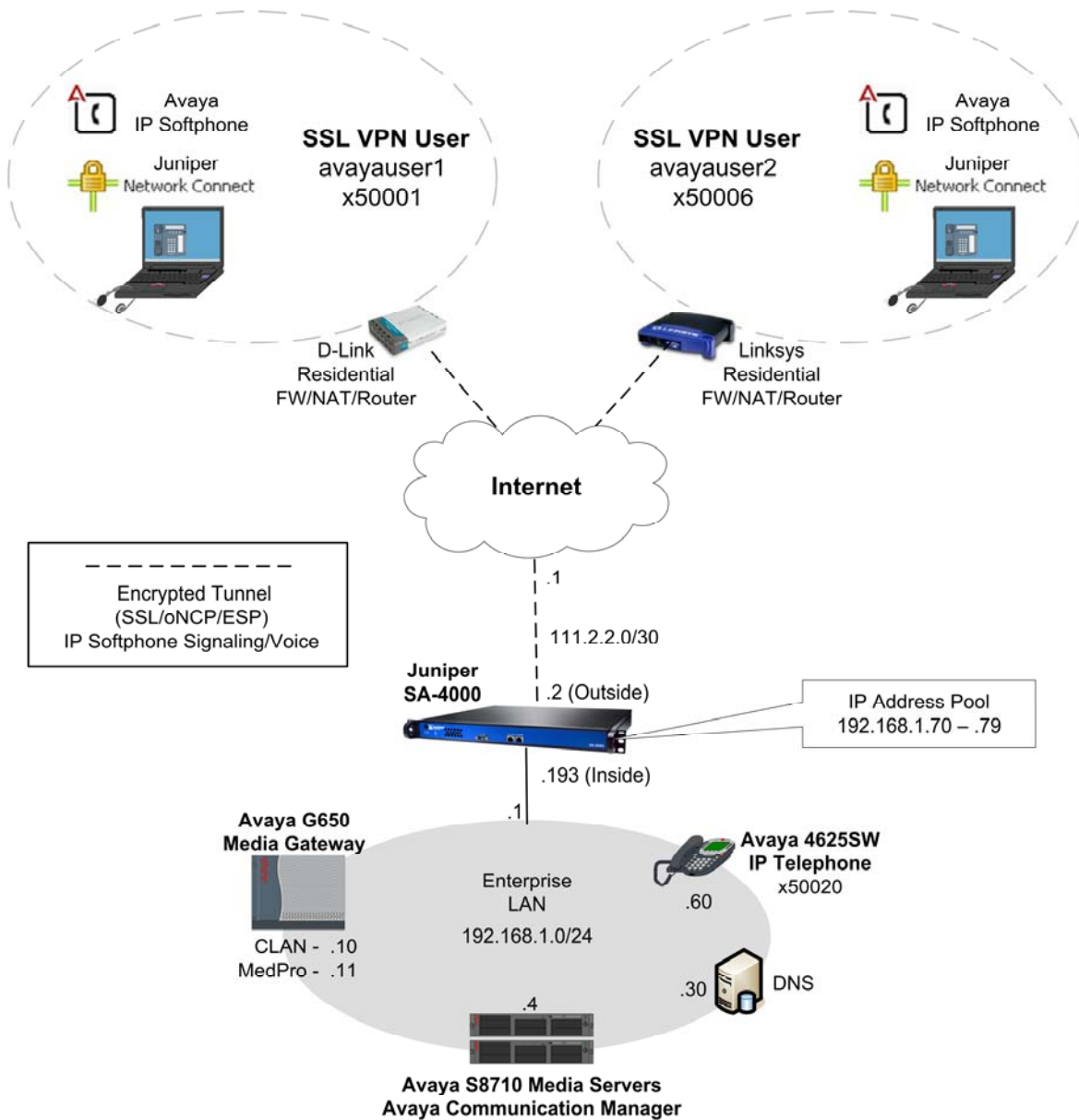
The sample network implemented for these Application Notes is shown in **Figure 2**.

Two remote SSL VPN user locations are included in the sample network. Each location consists of a computer running Microsoft Windows XP with the Avaya IP Softphone application installed. The Juniper Network Connect client application (Active-X) is installed on each computer over an SSL VPN connection. Each remote location includes a residential broadband router/firewall/NAT device, D-Link and Linksys, for Internet accesses.

The Juniper SA-4000 has one LAN port labeled “Outside” and one LAN port labeled “Inside”. The Outside port interconnects with the public Internet to be accessed by remote users for termination of SSL VPN connections. The Inside port interconnects with the private enterprise LAN. An IP address pool is also configured on the Juniper SA-4000 for IP address assignment to Network Connect client connections.

The enterprise LAN consists of a redundant set of Avaya S8710 Media Servers running Avaya Communication Manager, a G650 Media Gateway and IP/digital/analog Telephones.

**Note:** In the sample configuration, the Juniper SA-4000 is positioned as an exterior security device with a direct Internet connection. If the Juniper SA-4000 is installed in a traditional De-Militarized Zone (DMZ) configuration, ensure any exterior firewalls are configured to allow SSL connections (TCP port 443) as well as Network Connect ESP connections (UDP 4500 by default) through to the Juniper SA-4000.



**Figure 2 - Network Diagram**

### 3. Equipment and Software Validated

The information in these Application Notes is based on the software and hardware versions list in **Table 2** below.

Equipment	Software Version
Avaya S8710 Media Servers	Avaya Communication Manager 3.1.2 (R013x.01.2.632.1)
Avaya G650 Media Gateway IPSI (TN2312BP) C-LAN (TN799DP) MedPro (TN2302AP)	FW 022 (HW6) FW 016 (HW1) FW 108 (HW12)
Avaya IP Softphone	R6.0 (Product Version: 6.00.54)
Avaya 4625SW IP Telephone	R2.5 (H.323)
Juniper SA-4000	IVE 5.4 R2.1 (build 11529)
Dell Laptop	Windows XP Professional
Dell Laptop	Windows XP Professional
D-Link – DI-604	Firmware 3.51
Linksys - BEFSR41	Firmware 1.04.05

**Table 2 – Software/Hardware Version Information**

### 4. Juniper SA-4000 Configuration

This section describes the steps necessary to configure the Juniper SA-4000 to support users of the Avaya IP Softphone application over an SSL VPN connection. It is assumed that the installation and basic administration of the SA-4000 has been performed. Refer to [2] and [3] for additional information.

The following areas will be covered in this section.

- 1. Network Connect license verification**
- 2. User Role creation**
- 3. Network Connect configuration**
- 4. User Accounts creation**
- 5. User Realm configuration**

## 4.1. Network Connect License Verification

As stated in the Section 1, the Juniper SA-4000 Network Connect feature is required to use the Avaya IP Softphone application with the SSL VPN.

To verify the licensed features of the SA-4000, click **System > Configuration > Licensing** from the SA-4000 left navigation menu. The installed license details are displayed. A specific reference to Network Connect or All Features must be present to use the Network Connect feature. The license displayed below shows all features enabled.

The screenshot displays the Juniper Central Manager web interface. The top navigation bar includes the Juniper logo, a 'Root' dropdown menu, a 'Go' button, and links for 'Help', 'Guidance', and 'Sign Out'. The left sidebar contains a navigation tree with categories: System, Authentication, Administrators, Users, and Maintenance. The 'Configuration' section is expanded, and the 'Licensing' sub-menu is selected. The main content area shows the 'Configuration' page for 'Licensing'. It includes a warning message: 'Entering your license key signifies that you have read and agree to the license agreement.' Below this is a text area for 'License key(s):' with an 'Add' button. The 'Installed license details' section shows 'Maximum Concurrent Users: 1000' and a list of licenses. The first license is 'localhost2 - (1000 users)' with 'Licensing Hardware ID: 0153M2IK50NZL0IO'. Below this, a list item shows '1. SA 4000 with 1000 concurrent users, all features, 8 week license' with a 'Key: diploma hearth operation copper particle triangle poplar'.

Juniper®  
Central Manager  
Root  
Help | Guidance | Sign Out

System  
Status  
Configuration  
Network  
Clustering  
Virtual Systems  
Log/Monitoring  
Authentication  
Signing In  
Endpoint Security  
Auth. Servers  
Administrators  
Users  
User Realms  
User Roles  
Resource Profiles  
Resource Policies  
Maintenance  
System  
Import/Export  
Push Config  
Archiving  
Troubleshooting

Configuration  
Licensing  
Security  
Certificates  
NCP  
Sensors  
Client Types

Security Certificates NCP Sensors Client Types

Entering your license key signifies that you have read and agree to the license agreement.

License key(s):

Add

Installed license details

Maximum Concurrent Users: 1000

localhost2 - (1000 users)  
Licensing Hardware ID: 0153M2IK50NZL0IO

1. SA 4000 with 1000 concurrent users, all features, 8 week license  
Key: diploma hearth operation copper particle triangle poplar

## 4.2. User Role

A **User Role** defines user session parameters and access features. The sample configuration creates a new User Role called Avaya Softphone Users. By grouping all softphone users into a specific User Role, configuration options, such as extending the maximum session time, can be set to only affect softphone users.

The following steps create a new **User Role** for Avaya Softphone users with the Network Connect and Web access features enabled.

1. From the SA-4000 left navigation menu, click **Users > Users Roles**.
2. Click **New Role**.
3. In the **Name** and **Description** fields, enter descriptive text for this user role.

4. Under **Access features**, select the features to enable for this user role. The minimum feature required to support the Avaya Softphone application is **Network Connect**. The **Web** feature is a common user feature and also enabled in the sample configuration. All remaining fields may be left default. Click **Save Changes** when finished.

Roles >  
**New Role**

Name:

Description:

---

**Options**

Session and appearance options are specified in [Default Options](#). Check the following if this role should override these defaults.

☐ VLAN/Source IP

☒ Session Options

☒ UI Options

---

**Access features**

Check the features to enable for this user role, and specify any role-based options. Note that features disabled here may be granted by other roles assigned to the user.

☒ Web

☐ Files, Windows

☐ Files, UNIX/NFS

☐ Secure Application Manager

☐ Windows version

☐ Java version

☐ Telnet/SSH

☐ Terminal Services

☐ Meetings

☐ Email Client

☒ Network Connect

---

**Save changes?**

### 4.2.1. Session Options

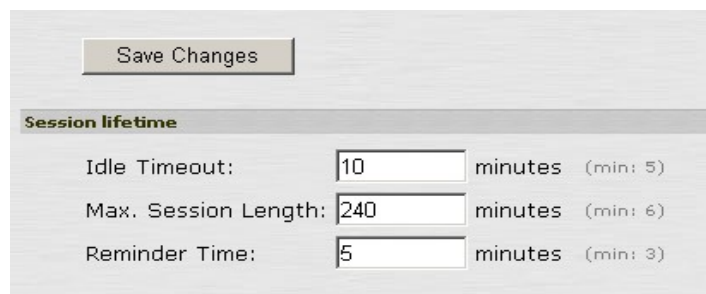
The Avaya IP Softphone application, being a communication tool and requiring access to the enterprise network for extended periods, may require the Juniper SA-4000 default session options to be modified for Avaya IP Softphone users.

The following steps set the Session Options for the new Avaya Softphone Users user role.

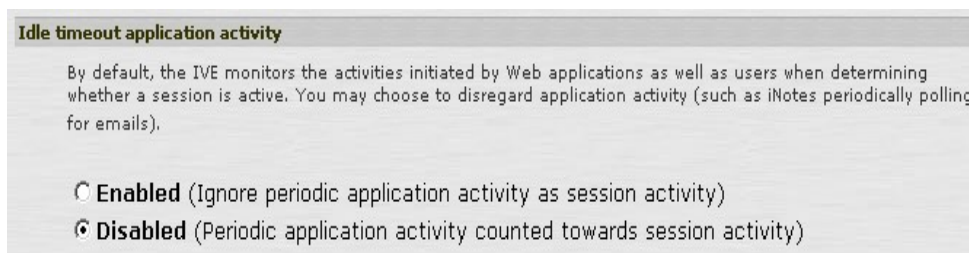
1. From the left navigation menu, click **Users > Users Roles > Avaya Softphone Users > General > Session Options**

The **Session Options** default values are displayed for the new Avaya Softphone Users user role. The **Maximum Session Length** has been extended from the default of 60 minutes to 240 minutes (4 hours) in the sample configuration as shown below.

**NOTE:** The value used for the Maximum Session Length is specific to the enterprise security policies and network environment in which the SA-4000 is installed. While the Avaya Softphone application will function properly with shorter Maximum Session Length intervals, the Avaya IP Softphone user experience may be negatively impacted due to Network Connect session terminations requiring the user to manually start a new session.



2. For Avaya Softphone users who leave the PC idle for extended periods of time, the **Idle Timeout** value may be of concern. However, it will not have an impact on the Avaya Softphone application as long as the **Idle timeout application activity** option remains at the default value of **Disabled**. This allows periodic application activity from Avaya Softphone (e.g., H.323 messages, ICMP keepalives) to be counted as session activity and maintain the session until the **Maximum Session Length** is reached.



All remaining fields may be left default. Click **Save Changes** when finished.

### 4.2.2. Network Connect Settings

The following Network Connect settings are specific to a User Role allowing independent groups of users to have different settings.

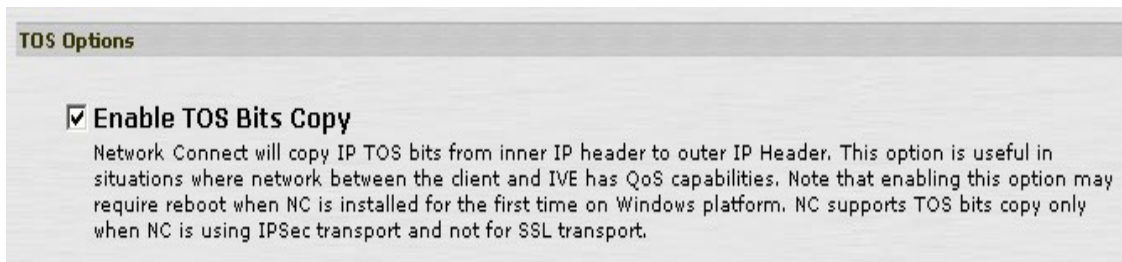
1. From the left navigation menu, click **Users > Users Roles > Avaya Softphone Users > Network Connect**

The **Network Connect** default values are displayed for the new “Avaya Softphone Users” user role. Enable the **Auto-launch Network Connect** feature to start the Network Connect client application on the remote PC automatically when the user authentication successfully completes using an HTTPS Web connection.



2. **Enable TOS Bits Copy** feature: Network Connect can copy IP TOS bits from the inner IP packet header to the outer IP packet header. Enable this feature to take advantage of QoS prioritization options offered by network service providers. Routers in the network are able to identify, prioritize, and appropriately forward Network Connect ESP packets across the network.

**NOTE:** This Network Connect QoS feature applies to UDP packets while in Network Connect ESP mode only. Network Connect in oNCP mode, using SSL packet encapsulation, is unchanged by this QoS feature. Also, the Network Connect client does not inter-work with the Microsoft QoS Packet Scheduler.



All remaining fields may be left default. Click **Save Changes** when finished.

## 4.3. Network Connect

### 4.3.1. Access Policies

The Network Connect Access Control allows policies to be written that control the network resources that users can connect to when using Network Connect. The sample configuration shown below uses the default “Initial Network Connect Policy” which allows full access to all network resources for all User Roles.

From the left navigation menu, click **Users > Resource Policies > Network Connect > Network Connect Access Control** to view the default policy.

The screenshot shows the 'Network Connect Access Policies' configuration page. At the top, there's a breadcrumb 'Resource Policies >' and the title 'Network Connect Access Policies'. Below the title are four tabs: 'Access' (selected), 'Logging', 'NC Connection Profiles', and 'Split-tunneling Networks'. A filter bar shows 'Show policies that apply to: All roles' with a dropdown arrow and an 'Update' button. Below this are buttons for 'New Policy...', 'Duplicate', 'Delete...', and up/down arrows, followed by a 'Save Changes' button. The main area is a table with columns: 'Policies', 'Action', 'Resources', and 'Applies to role'. The first row shows a checkbox, the number '1.', the policy name 'Initial Network Connect Policy' with a description 'Allows all network connect! Remove to restrict access.', the action 'Allow', resources '\*,\*', and 'All roles'.

Policies		Action	Resources	Applies to role
<input type="checkbox"/>	1. <u>Initial Network Connect Policy</u> Allows all network connect! Remove to restrict access.	Allow	*,*	All roles

### 4.3.2. Connection Profile

A Network Connect Connection Profile defines the mechanism to use for IP address assignment to Network Connect clients as well as the details of the Network Connect Transport mode and settings. The sample configuration creates a new Connection Profile called Avaya Softphone NC and maps to the Avaya Softphone Users user role created in Section 4.2.

1. From the left navigation menu, click **Users > Resource Policies > Network Connect > NC Connection Profiles**. Click **New Profile**.
2. In the **Name** and **Description** fields, enter descriptive text for this Network Connect profile.

The screenshot shows the 'New Profile' form. It has two fields: '\* Name:' with the value 'Avaya Softphone NC' and 'Description:' with the value 'Network Connect profile to be used by Avaya Softphone Users'.

\* Name: Avaya Softphone NC

Description: Network Connect profile to be used by Avaya Softphone Users

3. Under **IP address assignment**, select how IP addresses are to be assigned to remote Network Connect clients. The DHCP server option allows a DHCP server located in the private enterprise network to assign the IP addresses while the IP address pool option allows the SA-4000 to assign the IP addresses from a defined address range. The IP address pool option is used in the sample configuration.

The IP address range used for the IP address pool must not conflict with any IP address assignments used throughout the enterprise private LAN and must also be routable within the enterprise private LAN.

The screenshot shows a configuration window titled "IP address assignment". Below the title bar, it says "Specify how IP addresses are assigned to clients." There are two radio button options. The first is "DHCP server" with an empty text box labeled "Name or IP address" next to it. The second option, "IP address pool", is selected. Below it, it says "Specify the assignable IP address ranges for this profile, one per line." There is a text area containing "192.168.1.70-79" and a list box to its right showing "Examples:" with "10.10.10.10-100" and "10.10.10.50", and "IP Pool limits:".

4. Under **Connection Settings** ensure the **Transport** option of **ESP** is selected using the associated default values. Encapsulating Security Payload (ESP) is the preferred Network Connect transport protocol to use for performance sensitive “real-time” applications, such as Avaya IP Softphone.

**Note:** Avaya test results confirm the ESP Network Connect transport mode provides superior performance for voice packets over a variety of network conditions compared to the oNCP transport mode when using Avaya IP Softphone.

The choice of Encryption and Compression options are specific to the corporate security policies of the enterprise customer. Test results using all available Encryption and Compression options had no measurable impact to voice performance.

**Connection Settings**

Transport: ☒ **ESP** (maximize performance)

UDP port:

ESP to NCP fallback timeout:  seconds

Key lifetime (time based):  minutes

Key lifetime (bytes transferred):  bytes (0 implies no limits)

Replay Protection: ☒

☐ **NCP / NCP** (maximize compatibility)

Encryption: ☒ **AES/SHA1** (maximize security)

☐ **AES/MD5** (maximize performance)

Compression: ☒ **Compress**

☐ **No Compression**

5. Under **Roles**, select **Policy applies to SELECTED roles**. Select **Avaya Softphone Users** from the **Available roles** list. Click **Add** to move to the **Selected roles** list.

**Roles**

☐ Policy applies to ALL roles

☒ Policy applies to SELECTED roles

☐ Policy applies to all roles OTHER THAN those selected below

Available roles:

Selected roles:

6. All remaining fields may be left at default values. Click **Save Changes** when finished.

## 4.4. User Accounts

The IVE operating system running on the SA-4000 supports many common authentication mechanisms, including Windows NT Domain, Active Directory, RADIUS, LDAP, NIS, and RSA. IVE also supports a local authentication server with a local user database. IVE is pre-configured with one local user authentication server called “System Local.” The default “System Local” authentication server is used in this sample configuration. The steps below create a new user account in the local authentication server with a username of “avayauser1”. A second user account with a username of “avayauser2” is also created, but not shown, for illustration purposes later in these Application Notes.

1. From the left navigation menu, click **Authentication > Auth. Servers**. Under the Authentication/Authorization Servers column, click **System Local**.



**Authentication Servers**

New: (Select server type) [v] [New Server...] [Delete...]

<input checked="" type="checkbox"/>	Authentication/Authorization Servers	Type
<input checked="" type="checkbox"/>	<u>Administrators</u>	Local Authentication
<input type="checkbox"/>	<u>System Local</u>	Local Authentication
<input type="checkbox"/>		

2. Make note of the default **Password options** and **Password management** parameters that appear. An understanding of these parameters is needed when creating user accounts. The password options used for the sample configuration are shown below. Click the **Users** tab then **New**.

Auth Servers >

## System Local

Settings Users Admin Users

Name:  Label to reference this server.

### Password options

Minimum length:  characters

Maximum length:  characters

☐ Password must have at least  digits

☐ Password must have at least  letters

☐ Password must have mix of UPPERCASE and lowercase letters

☐ Password must be different from username

☒ New passwords must be different from previous password

### Password management

☒ Allow users to change their passwords

☐ Force password change after  days

☐ Prompt users to change their password  days before current password expires

Note: Use options on the Administrators/Users > Authentication > [Realm] > Authentication Policy > Password page to specify which realms should inherit the server's password management capabilities

3. Enter a new user name and password. All remaining fields may be left at default values. Click **Save Changes** when finished.

[Servers](#) > [System Local](#) >

## New Local User

Username:

Full Name:

Authenticate using: System Local

Password:

Confirm Password:

☐ One-time use (disable account after the next successful sign-in)

☒ Enabled

☐ Require user to change password at next sign in

Note: You must also configure password management on the [Authentication server Settings](#) with 'Allow users to change their passwords' option enabled. Use options on the Administrators/Users > Authentication > [Realm] > Authentication Policy > Password page to specify which realms should inherit the server's password management capabilities.

## 4.5. Authentication Realm

An Authentication Realm specifies the server to use for authentication, user access policies and user to User Role mapping.

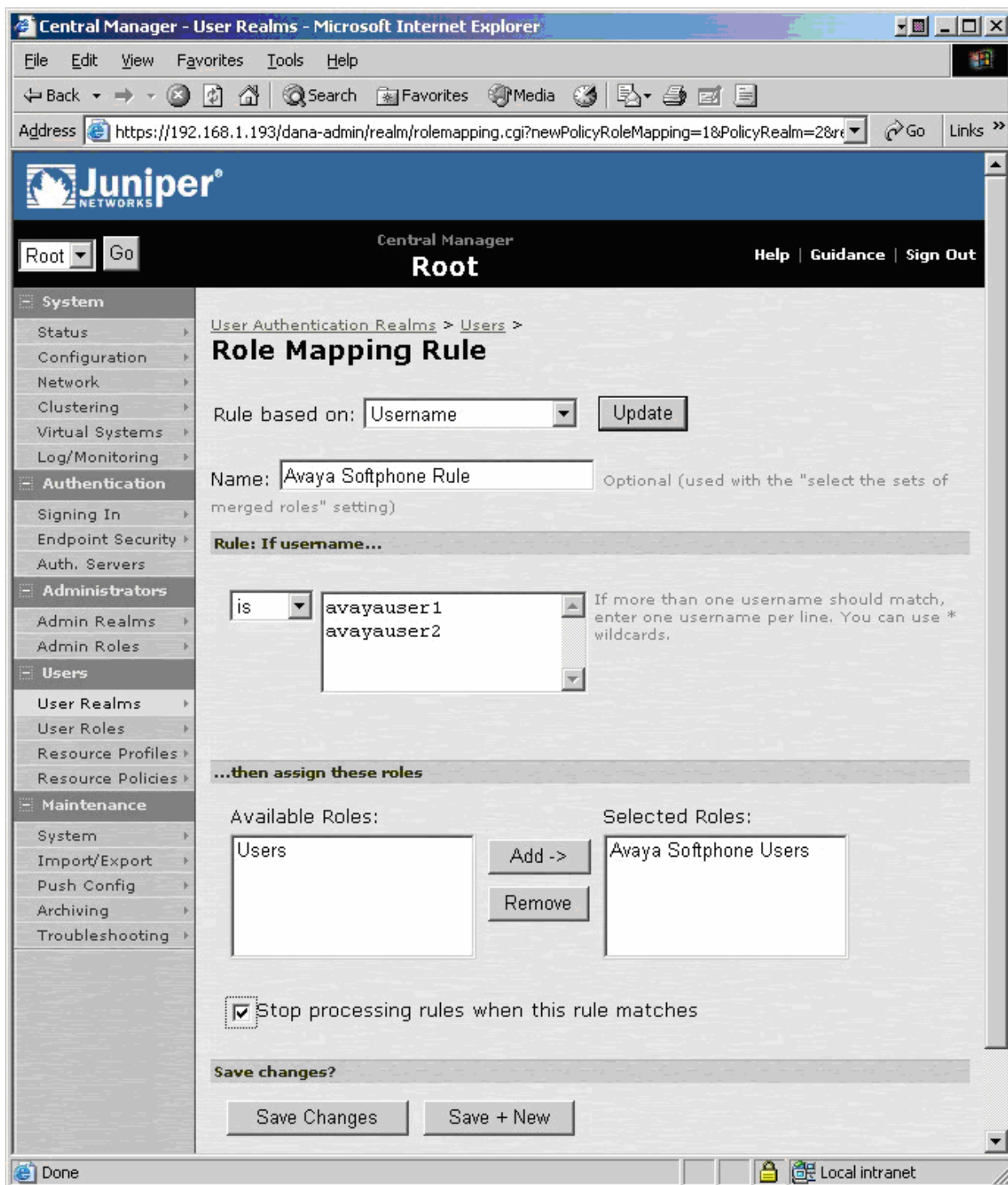
The default IVE **Authentication Realm**, named **Users**, is used in the sample configuration. The “Users Authentication Realm” default values for the Authentication Server (“System Local” the same Auth Server used in Section 4.4 ) and Authentication Policy (allow users to sign in from any IP address) are maintained in this sample configuration.

The steps below create a new Role Mapping Rule under the Users Authentication Realm. This Role Mapping Rule uses the user names of Avaya Softphone users created in Section 4.4 as the matching criteria of the rule. When a match occurs, the user is assigned to the User Role of Avaya Softphone Users created in Section 4.2.

1. From the left navigation menu, click **Users > User Realms > Users > Role Mapping**
2. Click **New Rule**. The Role Mapping Rule page is displayed as shown below.
3. For the **Rule based on** field select **Username** from the drop down menu.
4. In the **Name** field, enter descriptive text for this Role Mapping Rule.
5. Under the **Rule: If username...** section, select **is** from the drop down list. In the next field, enter the user names of the Avaya Softphone users created in Section 4.4 (avayauser1 and avayauser2).
6. Under the **...then assign these roles** section, select **Avaya Softphone Users** from the **Available Roles** list. Click **Add** to move to the **Selected Roles** list.
7. **Stop processing rules when this rule matches:**
  - a. Not checked, allows additional rules to be checked for a match if this rule matches
  - b. Checked, stops checking for additional rules if this rule matches.

The sample configuration prevents additional rules from being checked if a match is found. This limits the roles assigned to softphone users to only the Avaya Softphone Users role.

8. All remaining fields may be left at default values. Click **Save Changes** when finished.



- The Users Authentication Realm Role Mapping summary page is displayed. The new Avaya Softphone Rule is shown at the bottom of the list. The rules are executed in order with one being the first rule to execute.

Central Manager - User Realms - Rules - Microsoft Internet Explorer

Address: <https://192.168.1.193/dana-admin/realms/rules.cgi?SavedRule=1&PolicyRealm=2&realmType=user>

**Juniper** NETWORKS

Central Manager  
**Root**

Root Go Help Guidance Sign Out

**System**

- Status
- Configuration
- Network
- Clustering
- Virtual Systems
- Log/Monitoring

**Authentication**

- Signing In
- Endpoint Security
- Auth. Servers

**Administrators**

- Admin Realms
- Admin Roles

**Users**

- User Realms
- User Roles
- Resource Profiles
- Resource Policies

**Maintenance**

- System
- Import/Export
- Push Config
- Archiving
- Troubleshooting

User Authentication Realms >  
**Users**

General Authentication Policy **Role Mapping**

Specify how to assign roles to users when they sign in. Users that are not assigned a role will not be able to sign in.

New Rule... Duplicate Delete Up Down Save Changes

	When users meet these conditions	assign these roles	Rule Name	Stop
<input type="checkbox"/> 1.	username is ""	→ Users		
<input type="checkbox"/> 2.	username is "avayauser1" or "avayauser2"	→ Avaya Softphone Users	Avaya Softphone Rule	✓

When more than one role is assigned to a user:

- ☒ Merge settings for all assigned roles
- ☐ User must select from among assigned roles
- ☐ User must select the sets of merged roles assigned by each rule

Note: Users that do not meet any of the above rules will not be able to sign into this realm.

Local intranet

The sample configuration prioritizes the Avaya Softphone Rule by moving it to the top of the list. Based on the setting chosen in Step 7 above, when a match occurs, no other rules are checked. To move the Avaya Softphone Rule to the top of the list, select the check box for the Avaya Softphone Rule then select the up arrow icon until it has been repositioned to the top of the list.

The screenshot shows a configuration window with buttons at the top: 'New Rule...', 'Duplicate', 'Delete', up/down arrows, and 'Save Changes'. Below is a table with columns: a checkbox, a sequence number, a condition description, an arrow, a role name, a rule name, and a 'Stop' checkbox.

<input type="checkbox"/>		When users meet these conditions	→	assign these roles	Rule Name	Stop
<input checked="" type="checkbox"/>	2.	username is "avayauser1" or "avayauser2"	→	Avaya Softphone Users	Avaya Softphone Rule	<input checked="" type="checkbox"/>
<input type="checkbox"/>	1.	username is ""	→	Users		<input type="checkbox"/>

Clicking **Save Changes** makes the change permanent and rennumbers the rules as shown below.

The screenshot shows the same configuration window after saving. The rules have been renumbered: Rule 1 is now at the top and Rule 2 is at the bottom.

<input type="checkbox"/>		When users meet these conditions	→	assign these roles	Rule Name	Stop
<input type="checkbox"/>	1.	username is "avayauser1" or "avayauser2"	→	Avaya Softphone Users	Avaya Softphone Rule	<input checked="" type="checkbox"/>
<input type="checkbox"/>	2.	username is ""	→	Users		<input type="checkbox"/>

## 5. Avaya Communication Manager Configuration

This section illustrates the configuration steps for Avaya Communication Manager specific to the sample configuration presented in these Application Notes. It is assumed that the basic configuration on Avaya Communication Manager has already been completed; see [1] for additional information. All administrative commands discussed in this section are executed on Avaya Communication Manager using the System Access Terminal (SAT). After the completion of the configuration in this section, perform a **save translation** command to make the changes permanent.

### 5.1. Overview

The following provides an overview of the tasks to be performed in this section. IP Softphone stations are created and assigned extension numbers. The IP Softphone stations are mapped to network region 6 using the IP address assigned by the Juniper SA-4000 at the start of an SSL VPN session. Endpoints on the enterprise LAN are in network region 1. Calls between remote IP Softphones, network region 6, and endpoints at the enterprise site, network region 1, and will use either the G.711 or G.729a codec (codec set 1 defined in Section 5.3). The IP Softphone user has the ability to choose either the G.711 or G.729a codec for these calls by either selecting “Local Area Network” (G.711) or “Cable, xDSL or ISDN” (G.729a) from the “Bandwidth Settings” option in the IP Softphone application. Which codec to use will be based on the quality of the network and available bandwidth available from the location the SSL VPN and IP Softphone application is running. For calls between two remote IP Softphone users with SSL VPN connections, the G.729a codec will be the only codec available (codec set 2 defined in Section 5.4). The IP Softphone user does not have control of the codec selection in this case.

### 5.2. Add IP Softphone Stations

Add an IP Softphone station using the “add station” command. For the sample configuration, extensions 50001 and 50006 are created as IP Softphone stations. The parameters relevant to the sample configuration are shown in bold below for station 50001. With the **IP Softphone** field set to “y”, Avaya Communication Manager knows to apply the appropriate treatment to this station.

add station 50001		Page	1 of	4
STATION				
Extension: 50001	Lock Messages? n	BCC: 0		
Type: 4620	Security Code: 1234	TN: 1		
Port: IP	Coverage Path 1:	COR: 1		
Name: avayauser1	Coverage Path 2:	COS: 1		
	Hunt-to Station:			
STATION OPTIONS				
Loss Group: 19	Personalized Ringing Pattern: 1			
	Message Lamp Ext: 50001			
Speakerphone: 2-way	Mute Button Enabled? y			
Display Language: english				
Survivable GK Node Name:				
Survivable COR: internal	Media Complex Ext:			
Survivable Trunk Dest? y	IP SoftPhone? y			
IP Video Softphone? n				

### 5.3. Assignment of Endpoints to Network Regions

Mapping IP Softphone users to a dedicated network region enables configuration parameters to be set specifically for IP Softphone users. IP endpoints, both Telephones and Softphones, can be explicitly assigned to a network region based on an IP address mapping. IP Softphone users connecting to the enterprise network over an SSL VPN are dynamically assigned an IP address from the IP address pool configured on the Juniper SA-4000, Section 4.3.2. The IP address to network region map is defined in Avaya Communication Manager using the “change ip-network-map” command.

As shown in Figure 1, the sample configuration maps all IP Softphone users connecting through the Juniper SA-4000 SSL VPN to network region 6. The parameters relevant to the sample configuration are shown in bold below.

change ip-network-map						Page	1 of	32
IP ADDRESS MAPPING								
From IP Address		(To IP Address		Subnet or Mask)	Region	VLAN	Emergency Location Extension	
192.168.1	.70	192.168.1	.79		6	n		
.	.	.	.	.		n		
.	.	.	.	.		n		
.	.	.	.	.		n		

### 5.4. Codec Set Configuration

IP Softphone users will likely be connecting to the enterprise network through the SSL VPN over the public Internet with no network Quality of Service capabilities. Therefore, codec selection is essential for a good user experience. To provide a flexible configuration for IP Softphone users, the sample configuration defines two codec sets. Codec set 1 is configured with both the G.711 mu-law and G.729a codecs, with G.711 listed first to designate it as the preferred codec. Codec set 2 is configured with only the G.729a codec. All codec definitions in both codec sets are defined with 2 voice frames per packet.

Although not required, the sample configuration enables media encryption in both codec sets using the Advanced Encryption Standard (AES). While enabling AES media encryption has no benefit while RTP voice packets are traversing the SSL VPN connection, when the packets exit the SSL VPN and enter the enterprise network the AES encryption will be effective.

Define an IP Codec Set using the “change ip-codec-set” command. The parameters relevant to the sample configuration are shown in bold below for both codec set 1 and 2.

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

#### IP Codec Set

Codec Set: 1

	Audio Codec	Silence Suppression	Frames Per Pkt	Packet Size(ms)
1:	<b>G.711MU</b>	<b>n</b>	<b>2</b>	<b>20</b>
2:	<b>G.729A</b>	<b>n</b>	<b>2</b>	<b>20</b>
3:				
4:				
5:				
6:				
7:				

#### Media Encryption

1: **aes**  
2:  
3:

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

#### IP Codec Set

Codec Set: 2

	Audio Codec	Silence Suppression	Frames Per Pkt	Packet Size(ms)
1:	<b>G.729A</b>	<b>n</b>	<b>2</b>	<b>20</b>
2:				
3:				
4:				
5:				
6:				
7:				

#### Media Encryption

1: **aes**  
2:  
3:

## 5.5. IP Network Region Configuration

Two network regions are configured in the sample configuration. Network region 1 is local to the enterprise main site, while network region 6 is mapped to IP Softphone users connecting to the enterprise network through the Juniper SA-4000 SSL VPN.

### 5.5.1. Network Region 1

The following screens illustrate the configuration for Page 1 of network region 1. The parameters relevant to the sample configuration are shown in bold. While the focus of this section is inter-region connectivity, observe that the **Codec Set** to be used for intra-region connections is set to “1”. **Intra-region** and **Inter-region IP-IP Direct Audio** determines the flow of RTP audio packets. Setting these fields to “yes” enables the most efficient audio path be taken.

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

                                IP NETWORK REGION

Region: 1
Location: 1             Authoritative Domain: avaya.com
    Name: Main Campus
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? y
        UDP Port Max: 3029
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
H.323 IP ENDPOINTS                                AUDIO RESOURCE RESERVATION PARAMETERS
    H.323 Link Bounce Recovery? y                            RSVP Enabled? n
    Idle Traffic Interval (sec): 20
    Keep-Alive Interval (sec): 5
    Keep-Alive Count: 5
```

The following screen illustrates Page 3 for network region 1, which defines the inter-network region connectivity. The focus is the connectivity between network region 1 endpoints and the IP Softphone endpoints in network region 6. These connections will use codec set 1.

change ip-network-region 1									
Page 3 of 19									
Inter Network Region Connection Management									
src rgn	dst rgn	codec set	direct WAN	Total WAN-BW-limits	Video WAN-BW-limits	Intervening-regions	Dyn CAC	IGAR	
1	1	1							
1	2	2	y	:NoLimit	:NoLimit				n
1	3	2	y	:NoLimit	:NoLimit				n
1	4	2	y	:NoLimit	:NoLimit				n
1	5	2	y	:NoLimit	:NoLimit				n
1	6	1	y	:NoLimit	:NoLimit				n
1	7								

### 5.5.2. Network Region 6

The following screens illustrate the configuration for Page 1 of network region 6. The parameters relevant to the sample configuration are shown in bold. Observe that the **Codec Set** to be used for connections within region 6 is set to “2”. More specifically, IP Softphone to IP Softphone calls will use Codec Set 2. **Intra-region** and **Inter-region IP-IP Direct Audio** determines the flow of RTP audio packets. Setting these fields to “yes” enables the most efficient audio path be taken. With the Juniper SA-4000 Policies set appropriately and Inter-region IP-IP Direct Audio enabled, RTP audio packets for IP Softphone to IP Softphone calls will route between the IP Softphone SSL VPN connections local to the Juniper SA-4000.

change ip-network-region 6		Page 1 of 19
IP NETWORK REGION		
Region: 6		
Location: 6		Authoritative Domain: avaya.com
Name: IP Softphone Users		
MEDIA PARAMETERS		Intra-region IP-IP Direct Audio: yes
Codec Set: 2		Inter-region IP-IP Direct Audio: yes
UDP Port Min: 2048		IP Audio Hairpinning? y
UDP Port Max: 3029		
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		
H.323 IP ENDPOINTS		AUDIO RESOURCE RESERVATION PARAMETERS
H.323 Link Bounce Recovery? y		RSVP Enabled? n
Idle Traffic Interval (sec): 20		
Keep-Alive Interval (sec): 5		
Keep-Alive Count: 5		

The following screen illustrates Page 3 for network region 6, which defines the inter-network region connectivity. The assignment of the inter-network region connectivity between network region 1 and 6 in Section 5.5.1, automatically created a symmetrical configuration for region 6. This is illustrated in the first line of the configuration shown below.

change ip-network-region 6									
Page 3 of 19									
Inter Network Region Connection Management									
src	dst	codec	direct	Total	Video			Dyn	
rgn	rgn	set	WAN	WAN-BW-limits	WAN-BW-limits	Intervening-regions	CAC	IGAR	
6	1	1	y	:NoLimit	:NoLimit			n	
6	2								
6	3								

## 6. Remote PC

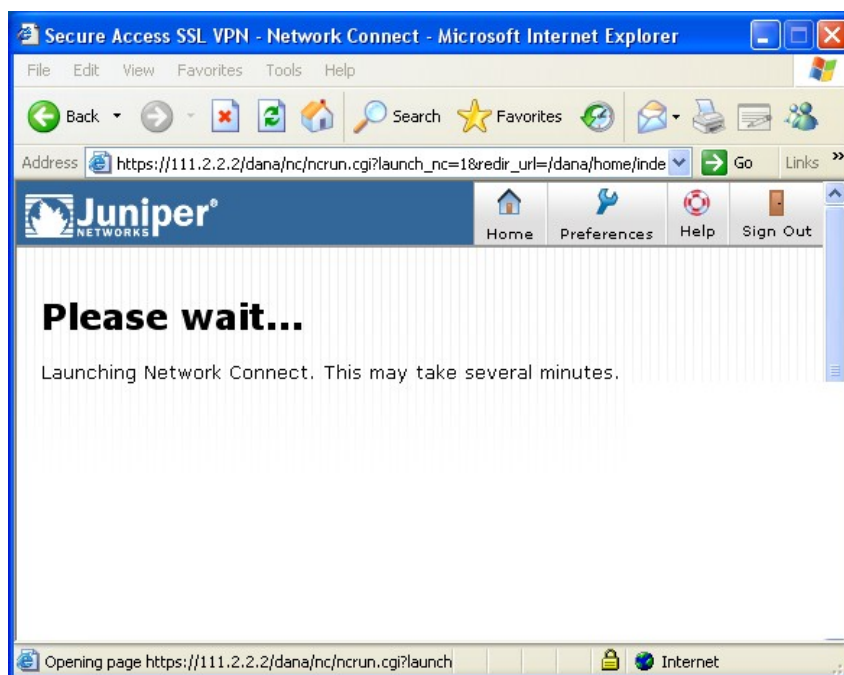
This section describes the steps necessary to start an SSL VPN session from a remote PC to the Juniper SA-4000 and using the Avaya IP Softphone application over the VPN. This section assumes the Avaya IP Softphone application is installed on the remote PC.

### 6.1. Starting the SSL VPN and Network Connect Session

From a Web browser, enter the URL of the Juniper SA-4000, “http://<IP address or FQDN of SA-4000>”. The SA-4000 will automatically redirect the browser request to a Welcome login screen over an HTTPS connection. Log in using a user name mapped to the “Avaya Softphone Users” role on the SA-4000.



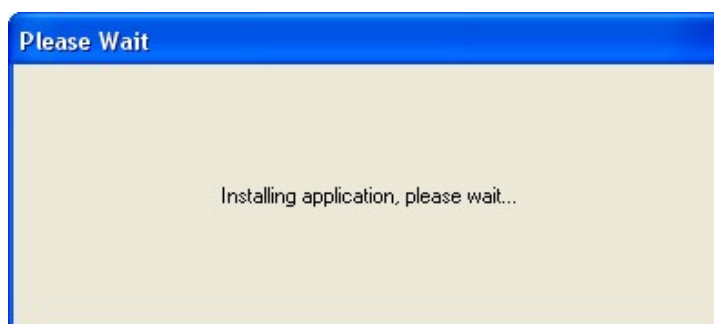
Because the “Auto-Launch Network Connect” feature was enabled in Section 4.2.2, Network Connect automatically starts once users mapped to the “Avaya Users Role” are authenticated. A web page similar to the one shown below is displayed indicating Network Connect is starting.



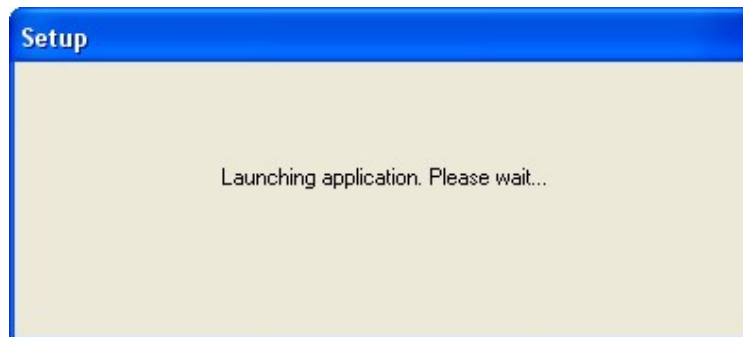
The first time users log in to the SSL VPN, the Network Connect client application must be installed on the remote PC. This is done automatically by the Juniper SA-4000 by pushing the Network Connect client to the PC over the SSL VPN connection and initiating the install remotely. A status window, similar to the one shown below, is displayed informing the user that the Network Connect client is being installed.

**Note:** To install Network Connect, users must have appropriate privileges on the Microsoft Windows PC; see [2], [4] and [5] for additional information. If the user does not have these privileges, use the Juniper Installer Service available on the SA-4000 from the **Maintenance > System > Installers** page to manually install the Network Connect client on the remote PC.

**Note:** Network Connect requires signed ActiveX or signed Java applets to be enabled within the web browser to download, install, and launch the Network Connect client application.



Once installed, the Network Connect client application is automatically launched on the remote PC. A status window similar to the one shown below is displayed informing the user that the Network Connect client is being started.



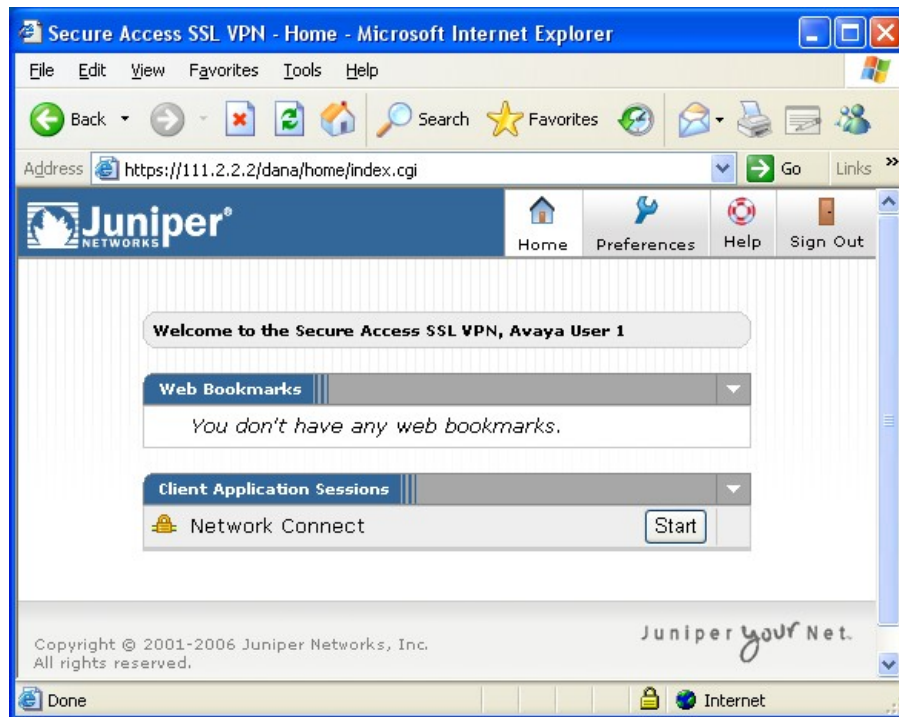
The Network Connect client status window is displayed. At this stage, the Network Connect client has been started and is attempting to contact the Juniper SA-4000 and negotiate the protocols to use for the connection.



Once the Network Connect session has started, the above Network Connect status window disappears and the Network Connect icon appears in the Microsoft Windows system tray as highlighted below.

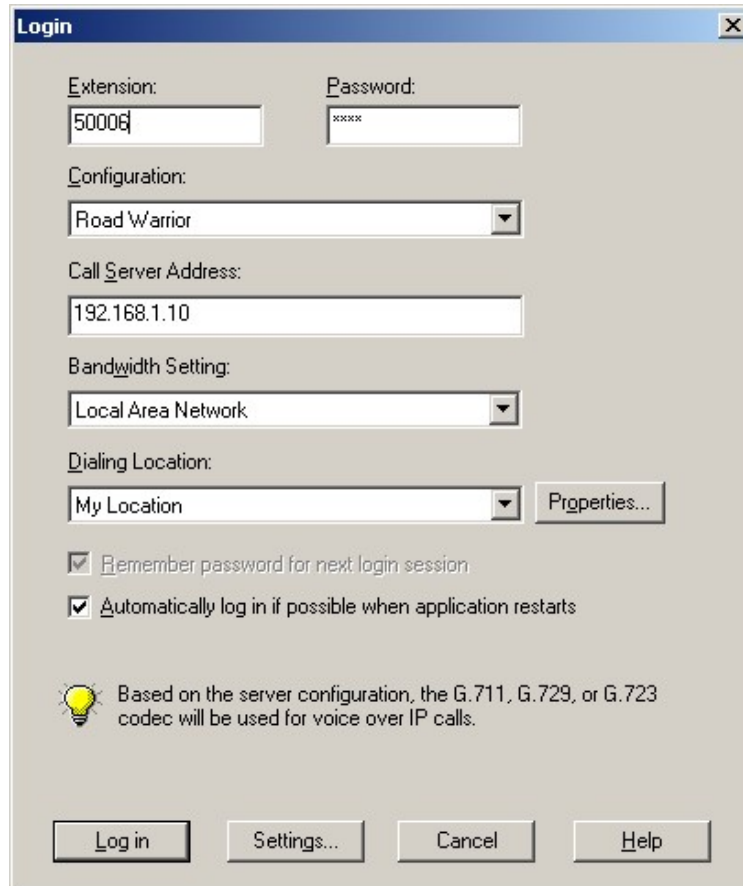


At this point the SSL VPN and Network Connect session has started successfully and the web browser displays the users SSL VPN home page. The sample configuration uses the Juniper SA-4000 default home page, as shown below.

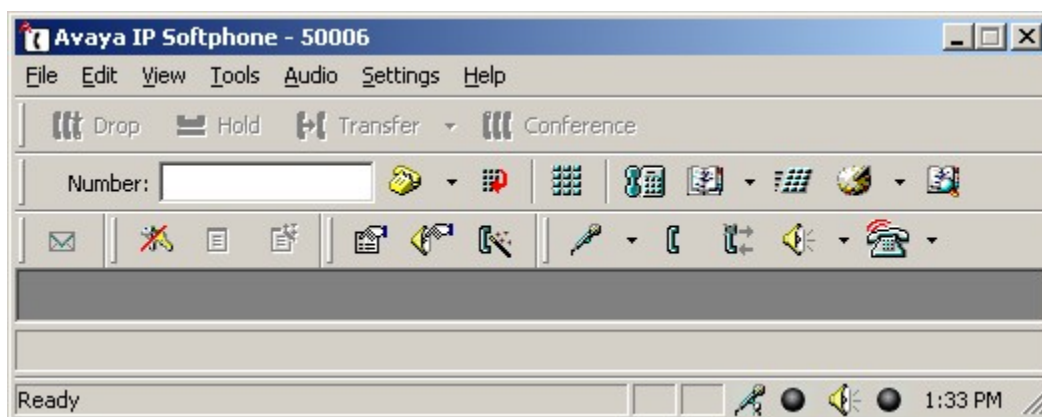


## 6.2. Starting the Avaya IP Softphone

With the Juniper Network Connect session started on the remote PC, start the Avaya IP Softphone application. The following screen illustrates the parameters used by IP Softphone in the sample configuration.



Once successfully register with Avaya Communication Manager over the Network Connect SSL VPN connection, the IP Softphone window appears similar to the one shown below.



## 7. Verification

This section provides some options to verify the SSL VPN and Network Connect session has been established and IP Softphone is able to register with Avaya Communication Manager and make calls.

### 7.1. Network Connect Virtual Adapter

When the Juniper Network Connect client is installed on the remote PC, a virtual network adapter is created on the PC. Running the “ipconfig /all” command in a Command Prompt window on the PC will show the details the virtual adapter. The abridged output of the “ipconfig /all” command run on the PC used in the sample configuration is shown below. Although the DHCP parameters are shown in the output, the configuration of the SA-4000 in Section 4.3.2 used an IP address pool for client IP address assignments. The IP address assigned to this PC, 192.168.1.70, is in the range of the designated address pool.

```
C:\>ipconfig /all

Ethernet adapter Network Connect Adapter:

    Connection-specific DNS Suffix  . : 
    Description . . . . . : Juniper Network Connect Virtual Adapter
    Physical Address. . . . . : 00-FF-08-21-C0-84
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes
    IP Address. . . . . : 192.168.1.70
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.70
    DHCP Server . . . . . : 10.200.200.200
    DNS Servers . . . . . : 192.168.1.30
    Lease Obtained. . . . . : Wednesday, March 21, 2007 3:09:34 PM

    Lease Expires . . . . . : Wednesday, March 28, 2007 3:09:34 PM
```

## 7.2. Connectivity

### 7.2.1. Remote PC to Avaya Communication Manager

Verify the connectivity from the remote PC to Avaya Communication Manager through the Juniper Network Connect VPN connection. This can be accomplished with a simple ping test from the remote PC to the IP address of the Avaya gatekeeper device the IP Softphone will register with. Open a Command Prompt window on the remote PC and enter the ping command followed by the IP address.

In the sample configuration, the IP Softphone registers to the C-LAN interface of the Avaya G650 Media Gateway. The C-LAN interface is assigned with IP address 192.168.1.10. The following screen illustrates the ping test in the sample configuration.

```
C:\>ping 192.168.1.10

Pinging 192.168.1.10 with 32 bytes of data:

Reply from 192.168.1.10: bytes=32 time<10ms TTL=63
Reply from 192.168.1.10: bytes=32 time<10ms TTL=63
Reply from 192.168.1.10: bytes=32 time<10ms TTL=63
Reply from 192.168.1.10: bytes=32 time<10ms TTL=63

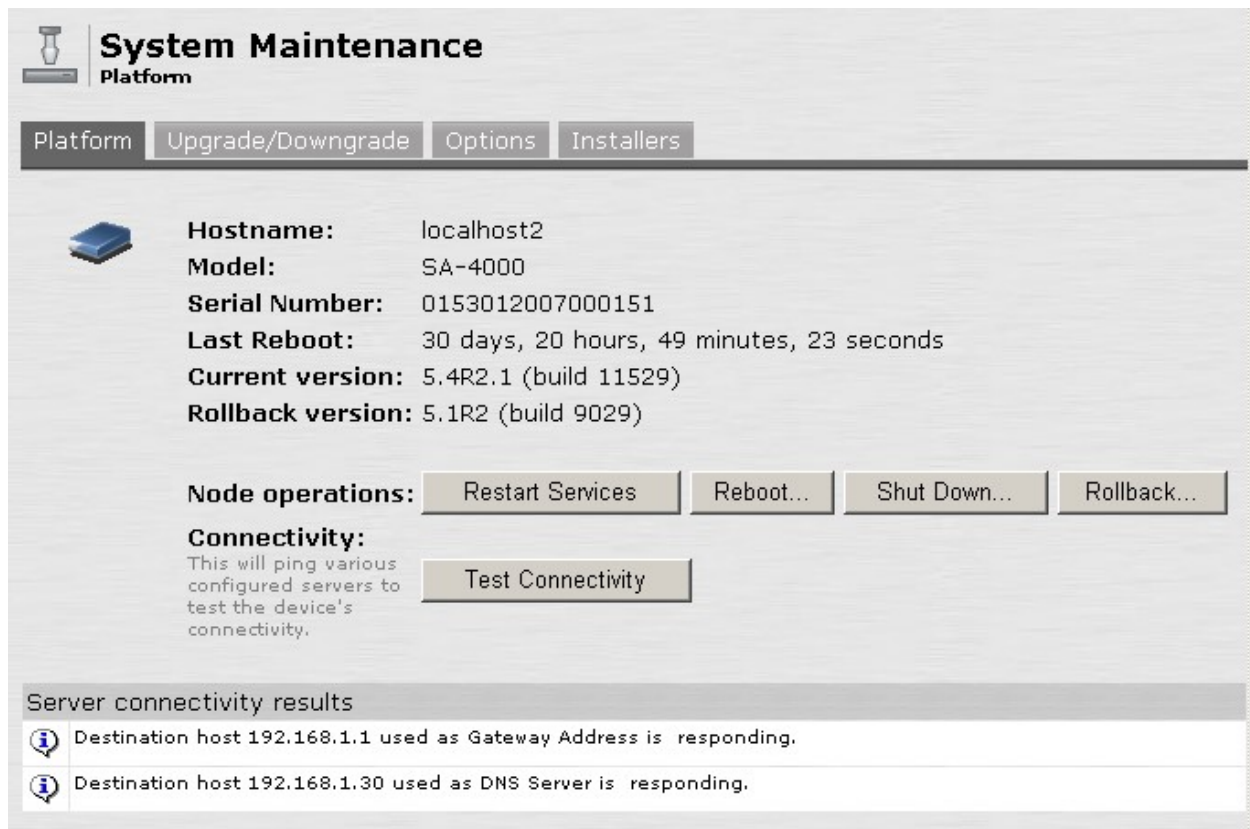
Ping statistics for 192.168.1.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```



## 7.2.2. Juniper SA-4000 to Internal Servers

Verify the connectivity from the Juniper SA-4000 to the configured servers on the private network (e.g., default route, DNS). This can be done from the Systems Maintenance page of the SA-4000.

From the left navigation menu of the SA-4000, click **Maintenance > System**. Click **Test Connectivity** to run the test. The following screens illustrates the Connectivity Test results from the sample configuration. The DNS and default gateway of the private network successfully responded.



The screenshot displays the 'System Maintenance' interface for a Juniper SA-4000 device. The top navigation bar includes 'Platform', 'Upgrade/Downgrade', 'Options', and 'Installers'. The main content area shows system details: Hostname (localhost2), Model (SA-4000), Serial Number (0153012007000151), Last Reboot (30 days, 20 hours, 49 minutes, 23 seconds), Current version (5.4R2.1), and Rollback version (5.1R2). Below this, 'Node operations' include buttons for 'Restart Services', 'Reboot...', 'Shut Down...', and 'Rollback...'. The 'Connectivity' section explains that the test pings configured servers and includes a 'Test Connectivity' button. At the bottom, a 'Server connectivity results' table shows two successful pings: one to the Gateway Address (192.168.1.1) and one to the DNS Server (192.168.1.30).

Server connectivity results	
	Destination host 192.168.1.1 used as Gateway Address is responding.
	Destination host 192.168.1.30 used as DNS Server is responding.

### 7.3. Active SSL VPN Users

Displaying all active SSL VPN users is a useful administrative tool offered by the Juniper SA-4000 to see details of the active SSL VPN sessions. From the left navigation menu of the SA-4000, click **System > Status > Active Users**. The page displayed below from the sample configuration shows three active users; one from the Administrator Realm and two from the Users Realm mapped to the “Avaya Softphone Users” Role.



	User	Realm	Roles	Signed in	Network Connect IP
<input type="checkbox"/>	avayauser1	Users	Avaya Softphone Users	2007/3/22 11:10:24	192.168.1.70
<input type="checkbox"/>	avayauser2	Users	Avaya Softphone Users	2007/3/22 11:13:01	192.168.1.71
<input type="checkbox"/>	interop	Admin Users	Administrators	2007/3/22 09:18:01	

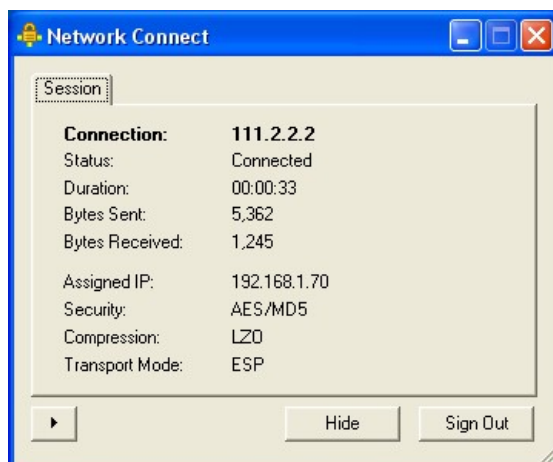
### 7.4. Network Connect Transport Mode

If the Network Connect transport mode is configured on the SA-4000 for ESP, the Network Connect client will attempt to start the Network Connection session using ESP. If the ESP session can not be started for some reason, i.e., a firewall between the remote PC and the SA-4000 is blocking UDP port 4500, the Network Connect client will “fallback” to oNCP transport mode and attempt the connection using oNCP (TCP port 443).

To determine which transport mode the Network Connect session is using from the remote PC, ESP or oNCP, double-click the Network Connect icon in the Microsoft Windows system tray, as highlighted below. This will open the Network Connect status window.



The sample Network Connect status window shown below indicates the Transport Mode being used as well as other useful information about the active Network Connect session.



## 7.5. Avaya Communication Manager “list registered-ip-stations”

The Avaya Communication Manager “list registered-ip-stations” command, run from the SAT, can be used to verify the registration status of the IP Softphones and associated parameters as highlighted below.

```
list registered-ip-stations
```

REGISTERED IP STATIONS							
Station	Set	Product	Prod	Station	Net Orig	Gatekeeper	TCP
Ext	Type	ID	Rel	IP Address	Rgn Port	IP Address	Skt
50001	4620	IP_Soft	5.242	192.168.1.71	6	192.168.1.10	y
50006	4620	IP_Soft	5.242	192.168.1.70	6	192.168.1.10	y
50020	4625	IP_Phone	2.500	192.168.1.60	1	192.168.1.10	y

## 7.6. Avaya Communication Manager “status station”

The Avaya Communication Manager “status station” command, run from the SAT, can be used to verify the current status of an administered station. The **Service State: in-service/off-hook** shown on **Page 1**, abridged below, indicates the IP Softphone with extension 50006 is participating in an active call.

```
status station 50006
```

GENERAL STATUS		Page 1 of 6
<b>Administered Type: 4620</b>	<b>Service State: in-service/off-hook</b>	
Connected Type: N/A	TCP Signal Status: connected	
<b>Extension: 50006</b>		
Port: S00012	Parameter Download: complete	

**Page 4**, abridged below, displays the audio status of an **active call between two IP Softphones**. The highlighted fields shown below indicate the following:

- **Other-end IP Addr** value is from the Juniper SA-4000 IP Address Pool indicating the call is with another SSL VPN connected IP Softphone.
- **Audio Connection Type: ip-direct** indicates audio RTP packets are going direct between IP Softphone via the SA-4000.
- Both stations are in **Network Region 6**.
- **G.729A** codec is being used.

status station 50006				Page 4 of 6	
AUDIO CHANNEL					
Port: S00012					
Switch		IP		IP	
Port		Other-end IP Addr :Port		Set-end IP Addr:Port	
G.729A	Audio:	192.168. 1. 71	:2048	192.168. 1. 70	:2048
Node Name:					
Network Region:		6		6	
Audio Connection Type: ip-direct					

**Page 4**, abridged below, displays the audio status of an **active call between a IP Softphone and a Main Campus IP Telephone**. The highlighted fields indicate the following:

- **Other-end IP Addr** value indicates the call is with an IP telephone at the main campus.
- **Audio Connection Type: ip-direct** indicates audio RTP packets are going direct between IP Softphone via the SA-4000.
- Call is between Network Region 1 and Network Region 6.
- **G.711mu-law** codec is being used.

status station 50006				Page 4 of 6	
AUDIO CHANNEL					
Port: S00012					
Switch		IP		IP	
Port		Other-end IP Addr	:Port	Set-end IP Addr	:Port
G.711MU	Audio:	192.168. 1. 60	:2512	192.168. 1. 70	:2048
Node Name:					
Network Region:		1		6	
Audio Connection Type: ip-direct					

## 8. Troubleshooting

This section provides some useful tools for troubleshooting.

### 8.1. Juniper SA-4000 Logs

The Juniper SA-4000 provides several logging capabilities.

#### 8.1.1. User Access

To access the User Access log click **System > Log/Monitoring > User Access > Log** from the left navigation menu of the SA-4000.

The screen below shows the User Access log from the sample configuration illustrating user “avayauser1” starting an SSL VPN session, being successfully authenticated by the “System Local” authentication server and starting a Network Connect session.

**Logs**

Events | **User Access** | Admin Access | NC Packets | Sensors | Client Logs | SNMP | Statistics

Log | Settings | Filters

View by filter: Standard:Standard (default) Show 200 items

Edit Query:

Update Reset Query Save Query...

Save Log As... Clear Log Save All Logs

**Filter:** Standard (default)  
**Date:** Oldest to Newest  
**Query:**  
**Export Format:** Standard

Severity	ID	Message
Info	JAV20021	2007-03-23 11:54:32 - ive - [111.2.2.70] Root::avayauser1(Users)[Avaya Sopftphone Users] - Connected to TUN-VPN port 443
Info	NWC23464	2007-03-23 11:54:32 - ive - [111.2.2.70] Root::avayauser1(Users)[Avaya Sopftphone Users] - Network Connect: Session started for user with IP 192.168.1.70
Info	AUT22670	2007-03-23 11:54:31 - ive - [111.2.2.70] Root::avayauser1(Users)[Avaya Sopftphone Users] - Login succeeded for avayauser1/Users from 111.2.2.70.
Info	AUT24326	2007-03-23 11:54:31 - ive - [111.2.2.70] Root::avayauser1(Users)[] - Primary authentication successful for avayauser1/System Local from 111.2.2.70

### 8.1.2. Network Connect

A Network Connect logging filter must first be created before Network Connect packets are written to the log. To access the Network Connect Logging Filters page, click **Users > Resource Policies > Network Connect > Logging** from the left navigation menu of the SA-4000. The Network Connect Logging Filters page is displayed as illustrated below. Make note of the warning message displayed on this page.

Resource Policies >  
**Network Connect Logging Filters**

Access | Logging | NC Connection Profiles | Split-tunneling Networks

Show policies that apply to: All roles [v] Update

**Warning**  
NC Packet Logging could significantly degrade performance, and should only be used for Troubleshooting.

New Policy... Duplicate Delete... [up] [down] Save Changes

Policies	Action	Resources	Applies to role

A Network Connect logging filter policy defines which Network Connect packets to show in the log and to which users the filter applies.

The steps below create a new Network Connect Logging Filter Policy illustrating the values used in the sample configuration. The sample configuration creates a new Policy called “NC Filter – ASU – ALL” which includes all Network Connect packets for Avaya Softphone Users.

1. Click **New Policy**.
2. In the **Name** and **Description** fields, enter descriptive text for this Network Connect Logging Filter Policy

Network Connect Logging Filters >  
**New Policy**

\* Name: NC Filter - ASU - ALL Required: Label to reference this policy.

Description: Show all NC packets for Avaya Softphone Users

3. Under **Resources**, enter the matching criteria for Network Connect packets. A resource of **\*:\*** means match on all.

The screenshot shows a window titled "Resources". Below the title bar, it says "Specify the resources for which this policy applies, one per line." There is a text input field labeled "\* Resources:" containing the text "\*: \*". To the right of the input field, there is a list of examples: "Examples: tcp://\*:1-1024", "tcp://\*:80,443", "udp://10.10.10.0/24:\*", and "icmp://10.10.10.10/255.255.255.255 10.10.10.0/24".

4. Under **Roles**, select the user group (User Roles) for which the policy applies.

The screenshot shows a window titled "Roles". Below the title bar, there are three radio buttons: "Policy applies to ALL roles", "Policy applies to SELECTED roles" (which is selected), and "Policy applies to all roles OTHER THAN those selected below". Below the radio buttons, there are two text input fields: "Available roles:" and "Selected roles:". The "Available roles:" field contains the text "Users". The "Selected roles:" field contains the text "Avaya Softphone Users". Between the two input fields, there are two buttons: "Add ->" and "Remove".

5. All remaining fields may be left at default values. Click **Save Changes** when finished.

To access the Network Connect log click **System > Log/Monitoring > NC Packets > Log** from the left navigation menu of the SA-4000.

The screen below shows the Network Connect log from the sample configuration illustrating the Network Connect packets containing the Avaya IP Softphone H.323 RAS message (port 1720) exchange with the C-LAN interface of the Avaya G650 Media Gateway.

## Logs

Events
User Access
Admin Access
**NC Packets**
Sensors
Client Logs
SNMP
Statistics

Log
Settings
Filters

View by filter: Standard:Standard (default) Show 200 items

Edit Query:

Update
Reset Query
Save Query...

Save Log As...
Clear Log
Save All Logs

**Filter:** Standard (default)  
**Date:** Oldest to Newest  
**Query:**  
**Export Format:** Standard

Severity	ID	Message
Info	NWC23475	2007-03-23 11:59:11 - ive - [111.2.2.70] Root::avayauser1(Users)[Avaya Softphone Users] - TCPpkt: PROT=TCP DESTIP=192.168.1.10 SRCPORT=33298 DSTPORT=1720 WINDOW=64195 ACK
Info	NWC23475	2007-03-23 11:59:11 - ive - [111.2.2.70] Root::avayauser1(Users)[Avaya Softphone Users] - TCPpkt: PROT=TCP DESTIP=192.168.1.70 SRCPORT=1720 DSTPORT=33298 WINDOW=8172 ACK PSH
Info	NWC23475	2007-03-23 11:59:11 - ive - [111.2.2.70] Root::avayauser1(Users)[Avaya Softphone Users] - TCPpkt: PROT=TCP DESTIP=192.168.1.10 SRCPORT=33298 DSTPORT=1720 WINDOW=64343 ACK PSH
Info	NWC23475	2007-03-23 11:59:11 - ive - [111.2.2.70] Root::avayauser1(Users)[Avaya Softphone Users] - TCPpkt: PROT=TCP DESTIP=192.168.1.70 SRCPORT=1720 DSTPORT=33298 WINDOW=8172 ACK PSH
Info	NWC23475	2007-03-23 11:59:11 - ive - [111.2.2.70] Root::avayauser1(Users)[Avaya Softphone Users] - TCPpkt: PROT=TCP DESTIP=192.168.1.10 SRCPORT=33298 DSTPORT=1720 WINDOW=64492 ACK PSH
Info	NWC23475	2007-03-23 11:59:11 - ive - [111.2.2.70] Root::avayauser1(Users)[Avaya Softphone Users] - TCPpkt: PROT=TCP DESTIP=192.168.1.70 SRCPORT=1720 DSTPORT=33298 WINDOW=8320 ACK PSH
Info	NWC23475	2007-03-23 11:59:11 - ive - [111.2.2.70] Root::avayauser1(Users)[Avaya Softphone Users] - TCPpkt: PROT=TCP DESTIP=192.168.1.70 SRCPORT=1720 DSTPORT=33298 WINDOW=8320 ACK
Info	NWC23475	2007-03-23 11:59:11 - ive - [111.2.2.70] Root::avayauser1(Users)[Avaya Softphone Users] - TCPpkt: PROT=TCP DESTIP=192.168.1.10 SRCPORT=33298 DSTPORT=1720 WINDOW=64641 ACK PSH

## 9. Conclusion

The Avaya IP Softphone combined with the Juniper Networks Secure Access SSL VPN appliance provides a secure and reliable solution for remote worker telephony over a broadband Internet connection. The Juniper Network Connect client demonstrated interoperability with the Avaya IP Softphone application and provided a comparable level of performance for voice packets, while in ESP mode, as a traditional IPSec VPN connection.

## 10. References

Avaya Application Notes and additional resources can be found at the following web address <http://www.avaya.com/gcm/master-usa/en-us/resource/>. Avaya Product Support web site can be found at the following web address <http://support.avaya.com/>.

- [1] *Administrators Guide for Avaya Communication Manager*,  
Doc ID: 03-300509
- [2] *Juniper Networks Secure Access Administration Guide – Instant Virtual Extranet Platform – Release 5.4*
- [3] *Juniper Networks Secure Access Quick Start Guide*
- [4] *Juniper Networks WSAM and Network Connect Error Messages – Release 5.4*
- [5] *Juniper Networks Secure Access Client Side Changes Guide – Release 5.4*
- [6] **RCF 2406** – IP Encapsulating Security Payload (ESP)  
<http://www.ietf.org/rfc/rfc2406.txt>

---

**©2007 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)