Application Notes for Configuring Avaya VPNremote™ Phone with Juniper Secure Services Gateway using Policy-Based IPSec VPN and XAuth Enhanced Authentication – Issue 1.0

Abstract

These Application Notes describe the steps for configuring the Juniper Secure Services Gateway 520 Security Platform with a policy-based IPSec VPN and XAuth enhanced authentication to support the Avaya VPNremote™ Phone. The sample configuration presented in these Application Notes utilizes a shared IKE Group ID to streamline the VPN configuration and management, IP Network Region segmentation to logically group and administer VPNremote Phones and NAT-T for IPSec traversal of Network Address Translation devices.
TABLE OF CONTENTS

1. INTRODUCTION ................................................................................................................................................. 3
   1.1. HIGHLIGHTS .................................................................................................................................................. 3

2. NETWORK TOPOLOGY ........................................................................................................................................... 4

3. EQUIPMENT AND SOFTWARE VALIDATED ............................................................................................................ 7

4. CONFIGURE JUNIPER SSG 520 ........................................................................................................................... 7
   4.1. ACCESS SSG 520 ......................................................................................................................................... 7
   4.2. CONFIGURE JUNIPER SSG ETHERNET INTERFACES .................................................................................. 8
   4.3. IP ADDRESS POOL .................................................................................................................................. 11
   4.4. ROUTES ...................................................................................................................................................... 12
   4.5. LOCAL USER CONFIGURATION .................................................................................................................. 14
   4.6. LOCAL USER GROUP CONFIGURATION ..................................................................................................... 17
   4.7. VPN ............................................................................................................................................................ 19
   4.8. XAUTH CONFIGURATION .......................................................................................................................... 24
   4.9. H.323 ALG ............................................................................................................................................... 26
   4.10. SECURITY POLICIES ................................................................................................................................. 26

5. AVAYA VPNREMOTE PHONE CONFIGURATION .................................................................................................. 28
   5.1. VPNREMOTE PHONE FIRMWARE ................................................................................................................ 28
   5.2. CONFIGURING AVAYA VPNREMOTE PHONE ........................................................................................... 28

6. EXTREME 3804 CONFIGURATION ....................................................................................................................... 30
   6.1. ADD IP ROUTE TO VPN IP ADDRESS POOL NETWORK ........................................................................... 30

7. AVAYA COMMUNICATION MANAGER CONFIGURATION ....................................................................................... 31
   7.1. VPNREMOTE PHONE CONFIGURATION .................................................................................................... 31
   7.2. IP CODEC SETS CONFIGURATION ............................................................................................................. 31
   7.3. IP NETWORK MAP CONFIGURATION ....................................................................................................... 32
   7.4. IP NETWORK REGIONS CONFIGURATION .................................................................................................. 33

8. VERIFICATION STEPS .......................................................................................................................................... 34
   8.1. VPNREMOTE PHONE QTEST ....................................................................................................................... 34
   8.2. VPNREMOTE PHONE IPSec STATS ............................................................................................................ 35
   8.3. JUNIPER SSG DEBUG AND LOGGING ....................................................................................................... 35
   8.4. OVERLAPPING NETWORK ADDRESSES .................................................................................................... 37

9. CONCLUSION ......................................................................................................................................................... 37

10. DEFINITIONS AND ABBREVIATIONS ............................................................................................................... 37

11. REFERENCES ....................................................................................................................................................... 38

APPENDIX A: SSG 520 A CLI CONFIGURATION .................................................................................................. 39
1. Introduction

These Application Notes describes the steps for configuring the Juniper Secure Services Gateway 520 security appliance to support the Avaya VPNremote™ Phone.

The Avaya VPNremote™ Phone is a software based Virtual Private Network (VPN) client integrated into the firmware of an Avaya IP Telephone. This enhancement allows the Avaya IP Telephone to be plugged in and used seamlessly over a secure VPN from any broadband Internet connection. The end user experiences the same IP telephone features as if they were using the phone in the office. Avaya IP Telephone models supporting the Avaya VPNremote Phone firmware are the 4610SW, 4620SW, 4621SW, 4622SW and 4625SW.

Release 2 of the Avaya VPNremote Phone extends the support of head-end VPN gateways to include Juniper security platforms. The configuration steps described in these Application Notes utilize a Juniper Secure Services Gateway (SSG) model 520. However, these configuration steps can be applied to Juniper NetScreen and ISG platforms using the ScreenOS version specified in Section 3.

1.1. Highlights

The sample network provided in these Application Notes implements the following features of the Juniper SSG 520 and Avaya VPNremote Phone:

- **Policy-Based IPSec VPN**
  The policy-based VPN feature of the Juniper SSG allows a VPN Tunnel to be directly associated with a security policy as opposed to a route-based VPN being bound to a logical VPN Tunnel interface. Because no network exists beyond a VPN client end-point, policy-based VPN tunnels are a good choice for VPN end-point configurations such as with the Avaya VPNremote Phone.

- **XAuth User Authentication**
  The XAuth protocol enables the Juniper SSG to authenticate the individual users of the VPNremote Phone. The XAuth user authentication is in addition to the IKE IPSec VPN authentication. The IKE and XAuth authentication steps of the Avaya VPNremote Phone are as follows:

**Step 1. Phase 1 negotiations:** the Juniper SSG authenticates the Avaya VPNremote Phone by matching the IKE ID and Pre-SharedKkey sent by the Avaya VPNremote Phone. If there is a match, the Juniper SSG XAuth process begins.
Step 2. **XAuth**: the Juniper SSG XAuth server prompts the Avaya VPNremote Phone for user credentials (username and password). If the Avaya VPNremote Phone is configured to store user credentials in flash memory, the Avaya VPNremote Phone responds to the Juniper SSG with the stored credentials without user involvement. Otherwise the Avaya VPNremote Phone displays a prompt for username and password to be manually entered.

Step 3. **Phase 2 negotiations**: Once the XAuth user authentication is successful, Phase 2 negotiations begin.

- **XAuth Dynamic IP Address Assignment**
  The XAuth protocol enables the Juniper SSG appliance to dynamically assign IP addresses from a configured IP Address pool range. The assignment of IP address ranges to Avaya VPNremote Phones enables Avaya Communication Manager to map the Avaya VPNremote Phones into IP Network Regions.

- **Shared IKE Group ID**
  The shared IKE ID feature of the Juniper SSG appliance facilitates the deployment of a large number of dialup IPSec VPN users. With this feature, the security device authenticates multiple dialup VPN users using a single group IKE ID and preshared key. Thus, it provides IPSec protection for large remote user groups through a common VPN configuration. XAuth user authentication must be used when implementing Shared IKE Group ID.

- **IP-Network-Region Segmentation**
  A common deployment for the Avaya VPNremote Phones is in a home network environment with limited bandwidth. The G.729 codec is recommended for such bandwidth constrained environments. Avaya Communication Manager IP Network Regions allow IP endpoints to be logically grouped together to apply unique configuration settings, including the assignment of specific codecs.

2. **Network Topology**

The sample network implemented for these Application Notes is shown in Figure 1. Three office locations are included, a “Main Campus” and three “Remote Offices”.

The **Main Campus** consists of two Juniper SSG 520’s, named “SSG 520 A” and “SSG 520 B”, functioning as perimeter security devices and IPSec VPN head-ends. The Avaya S8710 Media Server and Avaya G650 Media Gateway are also located at the Main Campus. The Main Campus is mapped to **Network Region 1** in Avaya Communication Manager.
Remote SOHO Office A consists of two Avaya VPNremote Phones connected to a Netgear broadband router. The Netgear router is configured as a firewall with NAT enabled as well as a local DHCP server. The VPNremote phones in Remote Office A are configured to use SSG 520 A for IPSec tunnel termination. SSG 520 A assigns an IP address to the VPNremote Phones mapped to Network Region 2 in Avaya Communications Manager.

Remote Home Office B consists of a single Avaya VPNremote Phone connected to a Linksys broadband router. The Linksys router is configured as a firewall with NAT enabled as well as a local DHCP server. The VPNremote phone in Remote Office B is configured to use SSG 520 A for IPSec tunnel termination. SSG 520 A assigns an IP address to the VPNremote Phone mapped to Network Region 2 in Avaya Communication Manager.

Remote Home Office C consists of a single Avaya VPNremote Phone connected to a Dlink broadband router. The Dlink router is configured as a firewall with NAT enabled as well as a local DHCP server. The VPNremote phone in Remote Office C is configured to use SSG 520 B for IPSec tunnel termination. SSG 520 B assigns an IP address to the VPNremote Phone mapped to Network Region 3 in Avaya Communication Manager.

Table 1 summarizes the Network Region IP address mappings.

<table>
<thead>
<tr>
<th>Network Region</th>
<th>IP Address Range</th>
<th>Juniper SSG</th>
<th>Office</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>192.168.1.0 /24</td>
<td>-</td>
<td>Main</td>
</tr>
<tr>
<td>2</td>
<td>50.50.100.0 /24</td>
<td>A</td>
<td>Remote SOHO Office A</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Remote Home Office B</td>
</tr>
<tr>
<td>3</td>
<td>50.50.130.0 /24</td>
<td>B</td>
<td>Remote Home Office C</td>
</tr>
</tbody>
</table>

Table 1 – Network Region Mappings
Figure 1: Physical Network
3. Equipment and Software Validated

Table 2 lists the equipment and software/firmware versions used in the sample configuration provided.

<table>
<thead>
<tr>
<th>Device Description</th>
<th>Versions Tested</th>
</tr>
</thead>
<tbody>
<tr>
<td>Avaya S8710 Media Server</td>
<td>Avaya Communication Manager R3.0.1 (R013x.00.1.346.0)</td>
</tr>
<tr>
<td>Avaya G650 Media Gateway</td>
<td>-</td>
</tr>
<tr>
<td>TN2312BP IPSI</td>
<td>FW 22 (HV 6)</td>
</tr>
<tr>
<td>TN799DP C-LAN</td>
<td>FW 16 (HV 1)</td>
</tr>
<tr>
<td>TN2302AP IP MedPro</td>
<td>FW 108 (HV 12)</td>
</tr>
<tr>
<td>Avaya 4610SW IP Telephones</td>
<td>R2.3.2 – Release 2 (a10bVPN232_1.bin)</td>
</tr>
<tr>
<td>Avaya 4620SW IP Telephones</td>
<td>R2.3.2 – Release 2 (a20bVPN232_1.bin)</td>
</tr>
<tr>
<td>Avaya 4621SW IP Telephones</td>
<td>R2.3.2 – Release 2 (a20bVPN232_1.bin)</td>
</tr>
<tr>
<td>Avaya 4625SW IP Telephones</td>
<td>R2.5.2 – Application (a25VPN252_1.bin)</td>
</tr>
<tr>
<td>Juniper Networks SSG 520</td>
<td>ScreenOS 5.4.0r1.0</td>
</tr>
<tr>
<td>Extreme Alpine 3804</td>
<td></td>
</tr>
<tr>
<td>Netgear Broadband Router – RP614v3</td>
<td>Firmware – V6.0NA 09/03/04</td>
</tr>
<tr>
<td>D-Link Broadband Router – DL-604</td>
<td>Firmware – 3.51 11/22/04</td>
</tr>
<tr>
<td>Linksys Broadband Router – BEFSR41 Ver4</td>
<td>Firmware – v1.04.05 07/20/05</td>
</tr>
</tbody>
</table>

Table 2 – Equipment and Software Validated

4. Configure Juniper SSG 520

Two Juniper SSG 520’s are included in the sample configuration as described in Section 2. The primary difference in the configuration between these Juniper SSG 520s is IP address assignment and IP Pool address range. For brevity purposes, only the steps for configuring one of the SSG’s, SSG 520 A, is covered in these Application Notes.

The configuration steps utilize the Web User Interface (WebUI) of the Juniper SSG 520. The entire Juniper SSG 520 system CLI configuration is provided as a reference in Appendix A.

4.1. Access SSG 520

1. From a serial connection to the Console port of the Juniper SSG, log in and access the Command Line Interface using a Terminal Emulation application such as Windows HyperTerm. Execute the following commands to configure the Juniper SSG Ethernet interface 0/0. This enables access to the Juniper SSG WebUI.

```
SSG520-> set interface ethernet0/0 ip 192.168.1.199/24
SSG520-> set interface ethernet0/0 ip manageable
```
2. From a web browser, enter the URL of the Juniper SSG WebUI management interface, https://<IP address of the SSG>, and the following login screen appears. Log in using a user name with administrative privileges.

   ![Login Screen](image)

3. The Juniper SSG WebUI administration home page appears upon successful login. Note the ScreenOS Firmware Version in the Device Information section.

   ![Device Information](image)

4.2. Configure Juniper SSG Ethernet Interfaces

The Juniper SSG 520 has four build-in Ethernet interfaces, Ethernet 0/0 – Ethernet 0/3. The steps below configured Ethernet 0/0 to a Trust security zone facing the internal corporate network and Ethernet 0/2 to an Untrust security zone facing the public internet. The Avaya VPNremote Phone will interact with Ethernet 0/2 when establishing an IPSec Tunnel.

Configure Ethernet 0/0:

1. From the left navigation menu, select Network > Interfaces. The Network Interfaces List screen appears. The IP address is already populated for Ethernet0/0 from the basic configuration of Section 4.1. Select Edit for Ethernet 0/0 to configure additional parameters.
2. From the Ethernet 0/0 properties page, configure the highlighted fields shown below. All remaining fields can be left as default. Select OK to save.

Ethernet 0/0 connects to the private corporate network making it a trusted interface. It is placed in the Trust security zone of the Juniper SSG. The Service Options selected and enabling Manageability are related to the interface being in the Trust zone.
Configure Ethernet 0/2 Interface:

1. From the Network Interfaces List screen, select **Edit** for Ethernet 0/2

<table>
<thead>
<tr>
<th>Name</th>
<th>IP/Netmask</th>
<th>Zone</th>
<th>Type</th>
<th>Link</th>
<th>PPPoE</th>
<th>Configure</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet0/0</td>
<td>192.168.1.199/24</td>
<td>Trust</td>
<td>Layer3</td>
<td>Up</td>
<td>-</td>
<td>Edit</td>
</tr>
<tr>
<td>ethernet0/1</td>
<td>172.16.254.118/24</td>
<td>MGT</td>
<td>Layer3</td>
<td>Up</td>
<td>-</td>
<td>Edit</td>
</tr>
<tr>
<td>ethernet0/2</td>
<td>0.0.0.0/0</td>
<td>Untrust</td>
<td>Layer3</td>
<td>Up</td>
<td>-</td>
<td>Edit</td>
</tr>
<tr>
<td>ethernet0/3</td>
<td>0.0.0.0/0</td>
<td>HA</td>
<td>Layer3</td>
<td>Down</td>
<td>-</td>
<td>Edit</td>
</tr>
<tr>
<td>vlan1</td>
<td>0.0.0.0/0</td>
<td>VLAN</td>
<td>Layer3</td>
<td>Down</td>
<td>-</td>
<td>Edit</td>
</tr>
</tbody>
</table>

2. From the Ethernet 0/2 properties page, configure the highlighted fields shown below. All remaining fields can be left as default. Select **OK** to save.

Because Ethernet0/2 is in the Untrust zone and not configured as manageable, all service options are disabled.
4.3. IP Address Pool

The XAuth protocol enables the Juniper SSG to dynamically assign IP addresses from a configured IP Address pool range to IPSec clients such as the Avaya VPNremote Phone. Controlling the assignment of IP address ranges to Avaya VPNremote Phones enables Avaya Communication Manager to map the Avaya VPNremote Phones into IP Network Regions as described in Section 7.4.

The following steps create the IP Address Pool:

1. From the left navigation menu, select **Objects > IP Pools**.  
   On the IP Pools list page, select **New**.

2. From the IP Pools Edit page, populate the highlighted fields shown below then select **OK** to save.

   The **IP Pool Name** is a descriptive name for this IP Pool. Once configured, this name will appear in the **IP Pool Name** drop-down menu of Section 4.8.

   Ensure the IP address range does not conflict with addresses used throughout the corporate trusted network.

   ![IP Pool Configuration](image)

3. The IP Pools list page displays the new address pool entry.

<table>
<thead>
<tr>
<th>Name</th>
<th>Start IP</th>
<th>End IP</th>
<th>In use</th>
<th>Configure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote-User-IP</td>
<td>50.50.100.1</td>
<td>50.50.100.100</td>
<td>0</td>
<td>Edit, Remove</td>
</tr>
</tbody>
</table>
4.4. Routes

The sample configuration requires two new route entries be added to the Juniper SSG routing table, one specifying the default route and one specifying the network address range entered for the IP Address Pool in Section 4.3. Although several routing options exist in the Juniper SSG platform, static routes are used for this sample configuration.

4.4.1. Configure Default Route

1. From the left navigation menu, select Network > Routing > Destination

The Route Entries screen similar to the one below appears.

Select trust-vr from drop down menu then New
2. Configure the highlighted fields shown below. All remaining fields can be left as default. Select OK to save.

The 0.0.0.0/0 network indicates the default route when no other matches existing in the routing table. The route is going to the next hop out interface Ethernet 0/2 to the public internet.
4.4.2. Configure Route to IP Pool Address range

1. From the Route Entries screen, select trust-vr from the drop down menu then select New.

2. Configure the highlighted fields shown below. All remaining fields can be left as default. Select OK to save.

The IP Address / Netmask is the network used for the IP Address Pool in Section 4.3. The Gateway IP Address specifies the next hop route of the Trusted corporate network, the Extreme 3804 L2/L3 switch in the sample configuration. See Section 6 for information on the Extreme 3804 switch.

4.5. Local User Configuration

The sample configuration includes two different user types; IKE users and XAuth users.

IKE users are typically associated with a device such as the Avaya VPNremote Phone and are used to authenticate the actual device during the establishment of the IPSec tunnel.

XAuth users are remotely authenticated users who access a head-end security gateway via an AutoKey IKE VPN tunnel. Whereas the authentication of IKE users is actually the authentication of an individual’s device, Avaya VPNremote Phone, the authentication of XAuth users is the authentication of the individual themselves.
4.5.1. IKE User

The following steps create an IKE user to be used by Avaya VPNonRemote Phones for IKE authentication.

1. From the left navigation menu, select **Objects > User > Local > New**. Configure the highlighted fields shown below. All remaining fields can be left as default. Select **OK** to save.

   The **Number of Multiple Logins with Same ID** parameter specifies the number of end-points that can concurrently establish IPSec tunnels using this identity. This number must equal or exceed the number of Avaya VPNonRemote Phones accessing this Juniper SSG.

   **IKE Identity**, combined with a Pre-Shared Key, is used to identify the end-point when an initial IKE Phase one dialog begins. The format of the IKE Identity used is of an email address. As described in Section 5.2, the Group Name field of the Avaya VPNonRemote Phone must match this IKE Identity string. vpnphone@avaya.com is used in these Application Notes however any email address string can be used.

```
Auth/IKE/L2TP/XAuth User

- User Name: vpnphone-ike
- Status: Enable

- IKE User
- Simple Identity
- IKE ID Type: AUTO
- Number of Multiple Logins with Same ID: 100
- IKE Identity: vpnphone@avaya.com

- Use Distinguished Name For ID

- Authentication User: User Password
- XAuth User: Confirm Password

- L2TP User
```

2. The local Users list page displays the new IKE user:

```
<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Group</th>
<th>Status</th>
<th>Identity</th>
<th>Configure</th>
</tr>
</thead>
<tbody>
<tr>
<td>vpnphone-ike</td>
<td>IKE</td>
<td>-</td>
<td>Enabled</td>
<td><a href="mailto:vpnphone@avaya.com">vpnphone@avaya.com</a></td>
<td>Edit, Remove</td>
</tr>
</tbody>
</table>
```
4.5.2. XAuth Users

Three XAuth user accounts, owen, garrett, and evan are created in the sample configuration for users of the Avaya VPNIphone. The following steps create a user account for owen. Follow the same steps to create accounts for garrett and evan.

The XAuth server of the Juniper SSG provides the authentication of these users. The users of the Avaya VPNIphone will need to be supplied with their user name and password. Users will be prompted on the phone display to enter this information as the Avaya VPNIphone establishes the IPSec tunnel or the password can be stored the VPNIphone flash memory, see Section 5.2 for additional detail.

1. From the left navigation menu, select Objects > User > Local > New.
   Configure the highlighted fields shown below. All remaining fields can be left as default. Select OK to save.

Follow the same steps for each additional user.
2. The local Users list page displays the new XAuth users:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Group</th>
<th>Status</th>
<th>Identity</th>
<th>Configure</th>
</tr>
</thead>
<tbody>
<tr>
<td>evan</td>
<td>XAuth</td>
<td>-</td>
<td>Enabled</td>
<td>-</td>
<td>Edit</td>
</tr>
<tr>
<td>garrett</td>
<td>XAuth</td>
<td>-</td>
<td>Enabled</td>
<td>-</td>
<td>Edit</td>
</tr>
<tr>
<td>owen</td>
<td>XAuth</td>
<td>-</td>
<td>Enabled</td>
<td>-</td>
<td>Edit</td>
</tr>
<tr>
<td>vpnphone-ike</td>
<td>IKE</td>
<td>-</td>
<td>Enabled</td>
<td><a href="mailto:vpnphone@avaya.com">vpnphone@avaya.com</a></td>
<td>Edit</td>
</tr>
</tbody>
</table>

4.6. Local User Group Configuration

User groups have the benefit of being able to create one policy for the user group and that policy automatically applies to all members of a group. This eliminates the need to create policies for each individual user.

The sample configuration includes two different types of User Groups: IKE and XAuth. The IKE users and XAuth users created in Section 4.5 must now be added to an IKE Group and an XAuth Group respectively.

4.6.1. IKE User Group

1. From the left navigation menu, select **Objects > User > Local Groups > New**.

Enter a descriptive **Group Name**. Select the vpnphone-ike user name from the **Available Members** column on the right. Select the << icon to move the user name to the **Group Members** column on the left. Select **OK** to save.
2. The Local Groups list page displays the new IKE group:

<table>
<thead>
<tr>
<th>Group Name</th>
<th>Group type</th>
<th>Members</th>
<th>Configure</th>
</tr>
</thead>
<tbody>
<tr>
<td>vpnphone-grp</td>
<td>ike</td>
<td>vpnphone-ike</td>
<td>Edit, Remove</td>
</tr>
</tbody>
</table>

### 4.6.2. Xauth User Group

1. From the left navigation menu, select **Objects > User > Local Groups > New.**

Enter a descriptive **Group Name.** Select the owen, garrett and evan user names from the **Available Members** column on the right. Select the **<<** icon to move the user name to the **Group Members** column on the left. Select **OK** to save.

2. The Local Groups list page displays the new XAuth group:

<table>
<thead>
<tr>
<th>Group Name</th>
<th>Group type</th>
<th>Members</th>
<th>Configure</th>
</tr>
</thead>
<tbody>
<tr>
<td>remoteuser-grp</td>
<td>xauth</td>
<td>evan, garrett, owen</td>
<td>Edit, Remove</td>
</tr>
<tr>
<td>vpnphone-grp</td>
<td>ike</td>
<td>vpnphone-ike</td>
<td>Edit, Remove</td>
</tr>
</tbody>
</table>
4.7. VPN

Setting up the VPN tunnel encryption and authentication is a two-phase process.

- Phase 1 covers how the Avaya VPNNremote Phone and the Juniper SSG will securely negotiate and handle the building of the tunnel.
- Phase 2 sets up how the data passing through the tunnel will be encrypted at one end and decrypted at the other. This process is carried out on both sides of the tunnel.

Table 3 provides the IKE Proposals used in the sample configuration including the proposal name used by the Juniper SSG.

<table>
<thead>
<tr>
<th>Phase</th>
<th>Encryption/ Authentication Method</th>
<th>Diffie-Hellman Group</th>
<th>Encryption Algorithm</th>
<th>Hash Algorithm</th>
<th>Life Time (sec)</th>
<th>SSG Proposal Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>P1</td>
<td>Pre-Shared Key</td>
<td>2</td>
<td>3DES</td>
<td>MD5</td>
<td>28800</td>
<td>pre-g2-3des-md5</td>
</tr>
<tr>
<td>P2</td>
<td>ESP</td>
<td>2</td>
<td>AES128</td>
<td>SHA-1</td>
<td>3600</td>
<td>g2-esp-aes128-sha</td>
</tr>
</tbody>
</table>

Table 3 – IKE P1 /P2 Proposals
4.7.1. AutoKey IKE Gateway Configuration - Phase 1

1. From the left navigation menu, select **VPNs > AutoKey Advanced > Gateway**. Select **New**. Configure the highlighted fields shown below. All remaining fields can be left as default.

   Provide a descriptive **Gateway Name**. Selecting **Custom Security Level** provides access to a more complete list of proposals available on this Juniper SSG. Selecting **Dialup User Group** associates the **Group vpnphone-grp** created in **Section 4.6** to this IKE gateway.

   Enter an ASCII text string for a **Preshared Key** that will match the text entered on the Avaya VPNremote Phone.

   **Outgoing Interface** is the interface which terminates the VPN tunnel.

   Select **Advanced** to access additional configuration options.

   ![Gateway Configuration Interface](image-url)

2. Configure the highlighted fields shown on the next page. All remaining fields can be left as default. Select **Return** to complete the advanced configuration, and then **OK** to save.

   Select **Security Level** of Custom and the appropriate **Phase 1 Proposal** from the drop down menu. Refer to **Table 3 – IKE P1 / P2 Proposals**.
**Aggressive Mode** must be used for end-point negotiation such as the Avaya VPN remote Phone.

**Enable NAT-Traversal** allows IPSec traffic after Phase 2 negotiations are complete to traverse a Network Address Translation (NAT) device. The Juniper SSG first checks if a NAT device is present in the path between itself and the Avaya VPN remote Phone. If a NAT device is detected, the Juniper SSG uses UDP to encapsulate each IPSec packet.
3. Because the IKE group was selected in Step 1 above, a pop-up window similar to the one below is displayed as a reminder to enable the XAuth server. Section 4.8 provides the XAuth server configuration. Select OK.

![XAuth Server Configuration Reminder](image)

4. The AutoKey Advanced > Gateway list page displays the new gateway.

<table>
<thead>
<tr>
<th>Name</th>
<th>Peer Type</th>
<th>Address/ID/User Group</th>
<th>Local ID</th>
<th>Security Level</th>
<th>Configure</th>
</tr>
</thead>
<tbody>
<tr>
<td>vpnuphone-gw</td>
<td>Dialup</td>
<td>vpnuphone-gp</td>
<td></td>
<td>Custom</td>
<td>Edit, Xauth, Remove</td>
</tr>
</tbody>
</table>

4.7.2. AutoKey IKE VPN Tunnel Configuration - Phase 2

1. From the left navigation menu, select VPNs > AutoKey IKE. Select New. Configure the highlighted fields shown below. All remaining fields can be left as default.

Provide a descriptive **VPN Name**. Selecting **Custom Security Level** provides access to a more complete list of proposals available on the Juniper SSG. Select **Predefined** for Remote Gateway and the select the Remote Gateway name entered in Section 4.7.1, *vpuphone-gw*, from the drop-down menu.

Select **Advanced** to access additional configuration options.
2. Configure the highlighted fields shown below. All remaining fields can be left as default. Select **Return** to complete the advanced configuration, and then **OK** to save.

Select **Security Level** of Custom and the appropriate **Phase 2 Proposal** from the drop down menu. Refer to **Table 3 – IKE P1 / P2 Proposals**.

**Replay Protection** protects the encrypted IPSec traffic from man-in-the-middle replay attacks by including a sequence number with each IKE negotiation between the IKE endpoints.

**Bind to None** uses the outgoing interface, Ethernet 0/2, for all VPN tunnel traffic.

<table>
<thead>
<tr>
<th>Security Level</th>
<th>Predefined</th>
<th>Standard</th>
<th>Compatible</th>
<th>Basic</th>
<th>User Defined</th>
<th>Custom</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phase 2 Proposal</td>
<td>g2-esp-aes128-sha</td>
<td>None</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Replay Protection

Transport Mode

**Bind to**

<table>
<thead>
<tr>
<th>Tunnel Interface</th>
<th>None</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tunnel Zone</td>
<td>Untrust-Tun</td>
</tr>
</tbody>
</table>

Proxy-ID

Local IP / Netmask

Remote IP / Netmask

Service

VPN Group

VPN Monitor

Source Interface
default

Destination IP

Optimized

Rekey

Return Cancel
3. The **AutoKey IKE** list page displays the new IKE VPN:

<table>
<thead>
<tr>
<th>Name</th>
<th>Gateway</th>
<th>Security</th>
<th>Monitor</th>
<th>Configure</th>
</tr>
</thead>
<tbody>
<tr>
<td>vpnphone-vpn</td>
<td>vpnphone-gw</td>
<td>Custom</td>
<td>On</td>
<td>Edit</td>
</tr>
</tbody>
</table>

### 4.8. XAuth Configuration

The Juniper SSG has a “local” XAuth server integrated within the ScreenOS operating system. Alternatively, an external Radius server can be used.

These Application Notes implement the “local” ScreenOS XAuth server. The following steps configure the default and IKE gateway specific settings of the local XAuth server.

#### 4.8.1. XAuth Server Defaults

1. From the left navigation menu, select **VPNs > AutoKey Advanced > XAuth Settings**. Configure the highlighted fields shown below. All remaining fields can be left as default. Select **Apply** when complete.

   Select the **IP Pool Name** created in **Section 4.3** from the drop down menu. This defines the IP Address range used when IP addresses are dynamically assigned to the Avaya VPN remote Phone by the XAuth server during IKE setup. DNS and WINS IP addresses are also dynamically assigned by the XAuth server.
4.8.2. Enable XAuth Authentication for AutoKey IKE gateway

1. From the left navigation menu, select **VPNs > AutoKey Advanced > Gateway**. The list page displays the IKE gateway created in Section 4.7.1 as shown below.

   Select **Xauth** under the **Configure** column for the vpnphone-gw IKE gateway.

<table>
<thead>
<tr>
<th>Name</th>
<th>Peer Type</th>
<th>Address/ID/User Group</th>
<th>Local ID</th>
<th>Security Level</th>
<th>Configure</th>
</tr>
</thead>
<tbody>
<tr>
<td>vpnphone-gw</td>
<td>Dialup</td>
<td>vpnphone-grp</td>
<td>-</td>
<td>Custom</td>
<td>Edit Xauth Remove</td>
</tr>
</tbody>
</table>

2. Configure the highlighted fields shown below. All remaining fields can be left as default. Select **OK** when complete to save settings.
4.9. H.323 ALG

1. From the left navigation menu, select Configuration > Advanced > ALG > Configure. Un-check the H323 check box to globally disable the H.323 Application Layer Gateway.

![Application Layer Gateway]

Basic MGCP H323 SIP SCCP

4.10. Security Policies

1. From the left navigation menu select Policies. Any currently configured security policies are displayed.

Create a security policy for traffic flowing from the Untrust zone to the Trust zone. On the top of the Policies page select Untrust on the From drop-down menu and Trust on the To drop-down menu. Select the New button on top right corner of page to create the new security policy.

![Security Policies]

List 10 per page

From: Untrust  To: All zones

From Untrust To Trust, total policy: 4

<table>
<thead>
<tr>
<th>ID</th>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td>Any</td>
<td>Any</td>
<td>ANY</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Any</td>
<td>Any</td>
<td>ANY</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Any</td>
<td>Any</td>
<td>ANY</td>
<td></td>
</tr>
</tbody>
</table>
2. Configure the highlighted fields shown below. All remaining fields can be left as default. Select OK when complete to save settings. Enter a descriptive policy Name to easily identify this policy in the policy list and logs.

Selecting Dial-Up VPN from the Source Address drop down menu and Any from the Destination Address defines the VPN tunnel as the traffic originator.

Selecting Tunnel from the Action field drop down menu indicates the action the SSG will take against traffic that matches the first three criteria of the policy: Source Address, Destination Address, and Service. All matching traffic will be associated with a particular VPN Tunnel specified in the Tunnel field.

Selecting vpnphone-vpn from the Tunnel VPN drop down menu associates the VPN remote Phone VPN tunnel to the Action.

Check the Modify matching bidirectional VPN policy to have the SSG create a matching VPN policy for traffic flowing in the opposite direction.
4. The Policies list page displays the new Dial-Up VPN policy:

<table>
<thead>
<tr>
<th>ID</th>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
<th>Options</th>
<th>Configure</th>
<th>Enable</th>
<th>Move</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Dial-Up VPN</td>
<td>Any</td>
<td>ANY</td>
<td>![Image]</td>
<td></td>
<td>Edit, Clone, Remove</td>
<td>✔</td>
<td>![Image]</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ID</th>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
<th>Options</th>
<th>Configure</th>
<th>Enable</th>
<th>Move</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Any</td>
<td>Dial-Up VPN</td>
<td>ANY</td>
<td>![Image]</td>
<td></td>
<td>Edit, Clone, Remove</td>
<td>✔</td>
<td>![Image]</td>
</tr>
</tbody>
</table>

5. Avaya VPNremote Phone Configuration

5.1. VPNremote Phone Firmware

The Avaya VPNremote Phone firmware must be installed on the phone prior to the phone being deployed in the remote location. See *VPNremote for the 4600 Series IP Telephones Release 2.0 Administrator Guide* for details on installing VPNremote Phone firmware. The firmware version of Avaya IP telephones can be identified by viewing the version displayed on the phone upon boot up or when the phone is operational by selecting the *Options* hard button ➔ *View IP Settings* soft button ➔ *Miscellaneous* soft button ➔ *Right arrow* hard button. The Application file name displayed denotes the installed firmware version.

As displayed in Table 2 – Equipment and Software Validated, VPNremote Phone firmware includes the letters *VPN* in the name. This allows for easy identification of firmware versions incorporating VPN capabilities.

5.2. Configuring Avaya VPNremote Phone

The Avaya VPNremote Phone configuration can be administered centrally from an HTTP/TFTP server or locally on the phone. These Application Notes utilize the local phone configuration method. See Section 11 *VPNremote for the 4600 Series IP Telephones Release 2.0 Administrator Guide* for details on centralized configuration.

1. There are two methods available to access the VPN Configuration Options menu from the VPNremote Phone.

   a. **During Telephone Boot:**

   During the VPNremote Phone boot up, the option to press the * key to enter the local configuration mode is displayed on the telephones screen as shown below.

   ```
   DHCP
   * to program
   ```

   When the * key is pressed, several configuration parameters are presented such as the phones IP Address, the Call Servers IP Address, etc. Press # to accept the current settings or set to an appropriate value. The final configuration option displayed is the VPN Start Mode...
option shown below. Press the * key to enter the VPN Options menu.

VPN Start Mode: Boot
*=Modify #=OK

b. During Telephone Operation:

While the VPNremote Phone is in an operational state, i.e. registered with Avaya Communication Manager, press the following key sequence on the telephone to enter VPN configuration mode:

Mute-V-P-N-M-O-D-# (Mute-8-7-6-6-6-3-#)

The follow is displayed:

VPN Start Mode: Boot
*=Modify #=OK

Press the * key and the VPN Options menu to enter the VPN Options menu.

2. The following VPN configuration options are displayed. The settings highlighted below are from the VPNremote Phone of user owen. For detailed description of each VPN configuration option, see Section 11 VPNremote for the 4600 Series IP Telephones Release 2.0 Administrator Guide.

<table>
<thead>
<tr>
<th>Server:</th>
<th>100.2.2.100 (Public Eth2 address of SSG A)</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Name:</td>
<td>owen</td>
</tr>
<tr>
<td>Password:</td>
<td>xxxxx (Must match XAuth user password entered in Section 4.5.2)</td>
</tr>
<tr>
<td>Group Name:</td>
<td><a href="mailto:vpnphone@avaya.com">vpnphone@avaya.com</a></td>
</tr>
<tr>
<td>Group PSK:</td>
<td>xxxxx (Must match PreShared Key entered in Section 4.7.1)</td>
</tr>
<tr>
<td>VPN Start Mode:</td>
<td>BOOT</td>
</tr>
<tr>
<td>Profile: Modify:</td>
<td>Juniper Xauth with PSK (Press Profile softbutton to access)</td>
</tr>
</tbody>
</table>

Press the ► hard button to access next screen with the following VPN configuration options.

| Password Type: | Save in Flash (User not prompted at phone boot) |
| Encapsulation: | 4500-4500 |
| Syslog Server: | |
| IKE Parameters: | DH2-ANY-ANY |
| IKE ID Type: | USER-FQDN |
| Diffie-Hellman Group: | 2 |
| Encryption Alg: | Any |
| Authentication Alg: | Any |
| IKE Xchg Mode: | Aggressive |
| IKE Config Mode: | Enable |
| IPSec Parameters: | DH2-ANY-ANY |
| Encryption Alg: | Any |
From the telephone keypad, press the telephone ➤ hard button to access the next screen with the following VPN configuration options.

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication Alg:</td>
<td>Any</td>
</tr>
<tr>
<td>Diffie-Hellman Group:</td>
<td>2</td>
</tr>
<tr>
<td>Protected Net:</td>
<td>0.0.0.0/0</td>
</tr>
<tr>
<td>Remote Net #1:</td>
<td>0.0.0.0/0</td>
</tr>
</tbody>
</table>

When the VPN configuration options have been set, press the Done softbutton. The following is displayed. Select # to save the configuration and the reboot phone.

Save new values ?
* = no  # = yes

6. Extreme 3804 Configuration

The focus of these Application Notes is on the configuration of the Juniper SSG and Avaya VPNremote Phone. Therefore, the network infrastructure configuration is not described. However, the addition of route entries for the IP Pool Addresses defined in Section 4 in the private corporate network is required.

6.1. Add IP Route to VPN IP Address Pool network

Although the Extreme 3804 supports several dynamic routing protocols, static routes have been utilized these Application Notes. The config iproute add CLI command is used to add the static route entries for the IP Pool Address ranges defined in the Juniper SSG A and Juniper SSG B. The sh iproute command confirms the two new entries are in the route table.

* Alpine3804:4 # config iproute add 50.50.100.0 / 24 192.168.1.199
* Alpine3804:4 # config iproute add 50.50.130.0 / 24 192.168.1.196

* Alpine3804:11 # sh iproute

<table>
<thead>
<tr>
<th>Ori Destination</th>
<th>Gateway</th>
<th>Mtr</th>
<th>Flags</th>
<th>VLAN</th>
<th>Duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>*s 50.50.100.0/24</td>
<td>192.168.1.198</td>
<td>1</td>
<td>UG---S-um--</td>
<td>voice</td>
<td>0d:0h:00m:18s</td>
</tr>
<tr>
<td>*s 50.50.130.0/24</td>
<td>192.168.1.196</td>
<td>1</td>
<td>UG---S-um--</td>
<td>voice</td>
<td>0d:0h:00m:18s</td>
</tr>
</tbody>
</table>
7. Avaya Communication Manager Configuration

All the commands discussed in this section are executed on Avaya Communication Manager using the System Access Terminal (SAT). This section assumes that basic configuration on Avaya Communication Manager has been already completed.

7.1. VPNremote Phone Configuration

An Avaya VPNremote Phone is configured the same as other IP telephones within Avaya Communication Manager. Even though the Avaya VPNremote Phone is physically located outside of the corporate network, the Avaya VPNremote Phone will behave the same as other Avaya IP telephones located locally on the corporate LAN once the VPN tunnel has been established.

For additional information regarding Avaya Communication Manager configuration, see the Administrator Guide for Avaya Communication Manager.

7.2. IP Codec Sets Configuration

These Application Notes utilize the G.711 codec for the Main Campus location (Network Region 1) and the G.729 codec (3 Frames Per Pkt 30ms) for the Remote Office locations with Avaya VPNremote Phones deployed. The high compression of the G.729 codec accommodates the limited bandwidth of the remote office WAN connection (i.e. DSL or Cable).

For more information on configuring codecs, please see Setting WAN Bandwidth Limits between Network Regions section of the Administrators Guide for Avaya Communication Manager.

Use the `change ip-codec-set 1` command to define the G.711 codec as shown below.

```
change ip-codec-set 1

IP Codec Set

Codec Set: 1

<table>
<thead>
<tr>
<th>Audio Codec</th>
<th>Silence Suppression</th>
<th>Frames Per Pkt</th>
<th>Packet Size(ms)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1: G.711MU</td>
<td>n</td>
<td>2</td>
<td>20</td>
</tr>
<tr>
<td>2:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3:</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```
Use the `change ip-codec-set 2` command to define the G.729 codec as shown below.

<table>
<thead>
<tr>
<th>IP Codec Set</th>
</tr>
</thead>
<tbody>
<tr>
<td>Codec Set: 2</td>
</tr>
<tr>
<td><strong>Audio Codec</strong></td>
</tr>
<tr>
<td>1: G.729</td>
</tr>
<tr>
<td>2:</td>
</tr>
<tr>
<td>3:</td>
</tr>
</tbody>
</table>

Use the `list ip-codec-set` command to verify the codec assignments.

<table>
<thead>
<tr>
<th>IP CODEC SETS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Codec 1</strong></td>
</tr>
<tr>
<td>Set</td>
</tr>
<tr>
<td>1 G.711MU</td>
</tr>
<tr>
<td>2 G.729</td>
</tr>
<tr>
<td>3 G.711MU</td>
</tr>
<tr>
<td>4 G.711MU</td>
</tr>
</tbody>
</table>

### 7.3. IP Network Map Configuration

Use the `change ip-network-map` command to define the IP addresses mapped to Network Region 2 and 3 as shown below. Refer to Table 1 – Network Region Mappings and Figure 1: Physical Network in Section 2.

<table>
<thead>
<tr>
<th>IP ADDRESS MAPPING</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>From IP Address</strong></td>
</tr>
<tr>
<td>50.50.100.1</td>
</tr>
<tr>
<td>50.50.130.1</td>
</tr>
<tr>
<td>. . . . . . . . . .</td>
</tr>
</tbody>
</table>
7.4. IP Network Regions Configuration

Use the `change ip-network-region 1` command to configure Network Region 1 parameters. Configure the highlighted fields shown below. All remaining fields can be left as default.

Select a descriptive name for **Name**. **Intra-region** and **Inter-region IP-IP Direct Audio** determines the flow of RTP audio packets. Setting to yes enables the most efficient audio path be taken. **Codec Set 1** is used for Network Region 1 as described in **Section 7.2**.

<table>
<thead>
<tr>
<th>Region: 1</th>
<th>Location: 1</th>
<th>Authoritative Domain: avaya.com</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name: Main Campus</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MEDIA PARAMETERS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Codec Set: 1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Intra-region IP-IP Direct Audio: yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Inter-region IP-IP Direct Audio: yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>UDP Port Min: 2048</td>
<td></td>
<td></td>
</tr>
<tr>
<td>UDP Port Max: 3327</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DIFFSERV/TOS PARAMETERS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP Audio Hairpinning? y</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Call Control PHB Value: 46</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Audio PHB Value: 46</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Video PHB Value: 26</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Inter-region IP-IP Direct Audio: yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Codec Set: 1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Inter-region IP-IP Direct Audio: yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>UDP Port Min: 2048</td>
<td></td>
<td></td>
</tr>
<tr>
<td>UDP Port Max: 3327</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DIFFSERV/TOS PARAMETERS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RTCP Reporting Enabled? y</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Call Control PHB Value: 46</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Audio PHB Value: 46</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Video PHB Value: 26</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AUDIO RESOURCE RESERVATION PARAMETERS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RSVP Enabled? n</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Page 3 of the IP-Network-Region form defines the codec set to use for intra-region and inter-region calls. Avaya VPNremote Phones are mapped to Region 2 or 3. Calls within IP Network Region 1 use Codec Set 1 (G.711MU) while calls from IP Network Region 1 to IP Network Region 2 or 3 use Codec Set 2 (G.729).
Use the `change ip-network-region 2` command to configure Network Region 2 parameters. Configure the highlighted fields shown below. All remaining fields can be left as default.

![_table](image)

Page 3 defines the codec set to use for intra-region and inter-region calls. All calls from IP Network Region 2 will use the G.729 codec as defined by the IP Codec Set in Section 7.2

![_table](image)

Follow these same steps for configuring IP Network Region 3.

### 8. Verification Steps

#### 8.1. VPNremote Phone Qtest

Using a feature of the Avaya VPNremote Phone called **Quality test** or **Qtest**, the VPNremote Phone can test the network connection to the VPN head-end gateway to characterize the voice quality an end user is likely to experience.

Once the Avaya VPNremote Phone establishes an IPSec tunnel, registers with Avaya Communication Manager and becomes functional, enter the Avaya VPNremote Phone VPN configuration mode as described in Section 5.2. Select the **Qtest** softbutton to enter the Qtest menu. Select the **Start** softbutton to start Qtest. Note the reported statistics to determine the network connection quality.
8.2. VPNremote Phone IPSec stats

Once the Avaya VPNremote Phone establishes an IPSec tunnel, registers with Avaya Communication Manager and becomes functional, from the telephone keypad, press the OPTIONS hard button (✓ icon). From the telephone keypad, press the telephone ▶ hard button to access the next screen. Select the VPN Status… option. There are two screens of IPSec tunnel statistics displayed. Use the ▶ hard button to access the next screen. Press the Refresh softbutton to update the displayed statistics.

8.3. Juniper SSG Debug and Logging

From the Juniper SSG WebUI, select Reports > System Log > Event Log Level: - information from the left navigation menu.

The Juniper SSG System Log shown below contains the IKE Phase1, IKE Phase2 and XAuth events logged as an Avaya VPNremote Phone establishes an IPSec tunnel. The screen below shows the events of a single Avaya VPNremote Phone successfully establishing a tunnel.

<table>
<thead>
<tr>
<th>Date / Time</th>
<th>Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2006-09-11 23:37:46</td>
<td>info</td>
<td>IKE&lt;2,2,2,2&gt;: Phase 2 msg ID &lt;5363B21&gt;: Completed negotiations with SPI &lt;50163a2&gt;, tunnel ID &lt;32912&gt;, and lifetime &lt;3600&gt; seconds &lt;0&gt; KB.</td>
</tr>
<tr>
<td>2006-09-11 23:37:46</td>
<td>info</td>
<td>IKE&lt;2,2,2,2&gt;: Phase 2 msg-id &lt;5363B21&gt;: Completed for user <a href="mailto:vpmphone@avaya.com">vpmphone@avaya.com</a>.</td>
</tr>
<tr>
<td>2006-09-11 23:37:47</td>
<td>info</td>
<td>IKE&lt;2,2,2,2&gt;: Received initial contact notification and removed Phase 1 SAs.</td>
</tr>
<tr>
<td>2006-09-11 23:37:47</td>
<td>info</td>
<td>IKE&lt;2,2,2,2&gt;: Received initial contact notification and removed Phase 2 SAs.</td>
</tr>
<tr>
<td>2006-09-11 23:37:47</td>
<td>info</td>
<td>IKE&lt;2,2,2,2&gt;: Received a notification message for DOI &lt;1&gt; &lt;24578&gt; &lt;INITIAL-CONTACT&gt;.</td>
</tr>
<tr>
<td>2006-09-11 23:37:47</td>
<td>info</td>
<td>IKE&lt;2,2,2,2&gt;: Phase 2 msg ID &lt;5363B21&gt;: Responded to the peer's first message from user <a href="mailto:vpmphone@avaya.com">vpmphone@avaya.com</a>.</td>
</tr>
<tr>
<td>2006-09-11 23:37:47</td>
<td>info</td>
<td>IKE&lt;2,2,2,2&gt;: XAuth login was passed for gateway &lt;vpmphone-gw&gt;, username &lt;garrett&gt;, retry: 0, Client IP Addr:50.50.100.1, JPPool name: &lt;Remote-User-IP&gt;, Session-Timeout: &lt;0&gt;, IKE-Timeout: &lt;0s&gt;.</td>
</tr>
<tr>
<td>2006-09-11 23:37:46</td>
<td>info</td>
<td>IKE&lt;2,2,2,2&gt;: XAuth login was refreshed for username &lt;garrett&gt; at &lt;50.50.100.1/255.255.255.255&gt;.</td>
</tr>
<tr>
<td>2006-09-11 23:37:46</td>
<td>info</td>
<td>IKE&lt;2,2,2,2&gt;: Phase 1: Completed Aggressive mode negotiations with a &lt;28800&gt; second lifetime.</td>
</tr>
<tr>
<td>2006-09-11 23:37:46</td>
<td>info</td>
<td>IKE&lt;2,2,2,2&gt;: Phase 1: Completed for user <a href="mailto:vpmphone@avaya.com">vpmphone@avaya.com</a>.</td>
</tr>
<tr>
<td>2006-09-11 23:37:46</td>
<td>info</td>
<td>IKE&lt;2,2,2,2&gt;: Phase 1: IKE responder has detected NAT in front of the remote device.</td>
</tr>
<tr>
<td>2006-09-11 23:37:45</td>
<td>info</td>
<td>IKE&lt;2,2,2,2&gt;: Phase 1: Responder starts AGGRESSIVE mode negotiations.</td>
</tr>
</tbody>
</table>
From the Juniper SSG CLI, the ScreenOS **debug ike basic** and **debug ike detail** commands are useful for troubleshooting ISAKMP (IKE) tunnel setup (e.g., detect mis-matched proposals, can't find gateway, etc.).

The **get ike cookies** command is also useful in getting status on existing IKE negotiations by displaying the completed IKE Phase 1 negotiations as shown below.

No active Phase 1 Security Associations:

```
SSG520-> get ike cookies
Active: 0, Dead: 0, Total 0
```

One active Phase 1 Security Association:

```
SSG520-> get ike cookies
Active: 1, Dead: 0, Total 1

1017182f/0006, 2.2.2.2:32831->100.2.2.100:4500, PRESHR/grp2/AES192/SHA,
xchg(4) (vpnphone-gw/
grp6/usr13)
resent-tmr -65536 lifetime 300 lt-recv 86400 nxt_rekey 44 cert-expire 0
responder, err cnt 0, send dir 1, cond 0x0
nat-traversal map:
  keepalive frequency 5 sec
  nat-t udp checksum disabled
  local pri ip 100.2.2.100
  local pri ike port 4500
  local pub ip 0.0.0.0
  local pub ike port 0
  remote pri ip 0.0.0.0
  remote pri ike port 4500
  remote pub ip 2.2.2.2
  remote pub ike port 32831
  internal ip 0.0.0.0
  internal port 0
  natt proto 17
ike heartbeat              : disabled
ike heartbeat last rcv time: 0
ike heartbeat last snd time: 0
XAUTH status: 100
DPD seq local 0, peer 0

SSG520->
```
8.4. Overlapping Network Addresses
During the writing of these Application Notes problems were observed if the private IP address range of the residential router is the same as the private IP address range within the corporate network. In the sample network configuration of these Application Notes, 192.168.1.0 /24 is the private corporate network. The following characteristics occur if the residential router uses the same 192.168.1.0 /24 IP network on the private side of the NAT:

The IPSec tunnel is successfully established from the Avaya VPNremote Phone to the Juniper SSG and the VPNremote phone is assigned a dynamic IP address from the Juniper SSG IP Address pool. However, the VPNremote phone is not able to access the corporate TFTP/HTTP server or Avaya Communication Manager H.323 GateKeeper and goes into “discover mode”.

Changing the private network IP range at the residential router to a range not matching the private corporate network corrects the problem.

9. Conclusion
The Avaya VPNremote Phone combined with Juniper ScreenOS security appliances; SSG, NetScreen and ISG, provide a secure solution for remote worker telephony over any broadband internet connection.

10. Definitions and Abbreviations
The following terminology is used throughout this document.

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>CLAN</td>
<td>Control LAN</td>
</tr>
<tr>
<td>IKE</td>
<td>Internet Key Exchange (An IPSec control protocol)</td>
</tr>
<tr>
<td>ISAKMP</td>
<td>Internet Security Association and Key Management Protocol</td>
</tr>
<tr>
<td>IPSec</td>
<td>Internet Protocol Security</td>
</tr>
<tr>
<td>IPSI</td>
<td>IP Services Interface</td>
</tr>
<tr>
<td>MD5</td>
<td>Message Digest 5</td>
</tr>
<tr>
<td>MEDPRO</td>
<td>Media Processor</td>
</tr>
<tr>
<td>NAT</td>
<td>Network Address Translation</td>
</tr>
<tr>
<td>PFS</td>
<td>Perfect Forward Secret</td>
</tr>
<tr>
<td>Phase 1</td>
<td>IKE negotiations used to create an ISAKMP security association.</td>
</tr>
<tr>
<td>Phase 2</td>
<td>IKE negotiations used to create IPSec security associations.</td>
</tr>
<tr>
<td>RTP</td>
<td>Real-Time Transport Protocol</td>
</tr>
<tr>
<td>SA</td>
<td>Security Association</td>
</tr>
<tr>
<td>SHA-1</td>
<td>Secure Hash Algorithm 1.</td>
</tr>
<tr>
<td>VPN</td>
<td>Virtual Private Network</td>
</tr>
</tbody>
</table>
11. References

1. **Juniper Networks: Concepts & Examples ScreenOS Reference Guide; Volume 5: Virtual Private Networks** *Release 5.4.0, Rev. A*
   
   [http://www.juniper.net/techpubs/software/screenos/screenos5.4.0/CE_v5.pdf](http://www.juniper.net/techpubs/software/screenos/screenos5.4.0/CE_v5.pdf)

2. **Secure Services Gateway (SSG) 500 Series Hardware Installation and Configuration Guide** *ScreenOS Version 5.4.0*
   

   
   [http://juniper.net/training/jnbooks/configuring_nscn_firewalls.html](http://juniper.net/training/jnbooks/configuring_nscn_firewalls.html)

4. Avaya VPNremote Phone documentation and software download.
   

5. **Avaya Administrators Guide for Communication Manager**
   

6. Additional Avaya Application Notes and Resources are available,
   
Appendix A: SSG 520 A CLI Configuration

```plaintext
set clock timezone 0
set vrouter trust-vr sharable
set vrouter "untrust-vr"
exit
set vrouter "trust-vr"
unset auto-route-export
exit
unset alg h323 enable
set auth-server "Local" id 0
set auth-server "Local" server-name "Local"
set auth default auth server "Local"
set auth radius accounting port 27911
set admin name "netscreen"
set admin password "nKVUM2rwMUzPcrkG5sWlHdCtqkAibn"
set admin user "interop" password "nANqEgr5A3pAcWOEfs6NpNBteXJxQn" privilege "all"
set admin http redirect
set admin auth timeout 30
set admin auth server "Local"
set admin format dos
set zone "Trust" vrouter "trust-vr"
set zone "Untrust" vrouter "trust-vr"
set zone "DMZ" vrouter "trust-vr"
set zone "VLAN" vrouter "trust-vr"
set zone "Untrust-Tun" vrouter "trust-vr"
set zone "Trust" block
set zone "Trust" tcp-rst
set zone "Trust" asymmetric-vpn
set zone "Untrust" block
set zone "Untrust" tcp-rst
set zone "Untrust" asymmetric-vpn
set zone "MGT" block
set zone "DMZ" tcp-rst
set zone "VLAN" block
set zone "VLAN" tcp-rst
set zone "Untrust" screen tear-drop
set zone "Untrust" screen syn-flood
set zone "Untrust" screen ping-death
set zone "Untrust" screen ip-filter-src
set zone "Untrust" screen land
set zone "V1-Untrust" screen tear-drop
set zone "V1-Untrust" screen syn-flood
set zone "V1-Untrust" screen ping-death
set zone "V1-Untrust" screen ip-filter-src
set zone "V1-Untrust" screen land
set interface "ethernet0/0" zone "Trust"
set interface "ethernet0/1" zone "MGT"
set interface "ethernet0/2" zone "Untrust"
unset interface vlan1 ip
set interface ethernet0/0 ip 192.168.1.199/24
set interface ethernet0/0 nat
set interface ethernet0/1 ip 172.16.254.118/24
set interface ethernet0/1 route
```
set interface ethernet0/2 ip 100.2.2.100/30
set interface ethernet0/2 route
unset interface vlan1 bypass-others-ipsec
unset interface vlan1 bypass-non-ip
set interface ethernet0/0 ip manageable
unset interface ethernet0/2 ip manageable
unset interface ethernet0/0 manage snmp
set interface ethernet0/0 manage mtrace
unset interface vlan1 manage mtrace
unset flow no-tcp-seq-check
set flow tcp-syn-check
set console timeout 15
set pki authority default scep mode "auto"
set pki x509 default cert-path partial
set address "Trust" "0.0.0.0/0" 0.0.0.0 0.0.0.0
set address "Trust" "0.0.0.0/0.0.0.0" 0.0.0.0 0.0.0.0
set user "evan" uid 4
set user "evan" type xauth
set user "evan" password "rY27/4vQeNnFM9MsszyCnjHNzgpnDvp01Lg=="
unset user "evan" type auth
set user "evan" "enable"
set user "garrett" uid 3
set user "garrett" type xauth
set user "garrett" password "Gx7kdqYVNa70FRs0CoCF8Cto1Dnz3cum1g=="
unset user "garrett" type auth
set user "garrett" "enable"
set user "owen" uid 2
set user "owen" type xauth
set user "owen" password "xOfx89OCNyMQJ/sPQ1CWUlrvHGngirErgg=="
unset user "owen" type auth
set user "owen" "enable"
set user "vpnphone-ike" uid 1
set user "vpnphone-ike" ike-id u-fqdn "vpnphone@avaya.com" share-limit 100
set user "vpnphone-ike" type ike
set user "vpnphone-ike" "enable"
set user-group "remoteuser-grp" id 3
set user-group "remoteuser-grp" user "evan"
set user-group "remoteuser-grp" user "garrett"
set user-group "remoteuser-grp" user "owen"
set user-group "vpnphone-grp" id 1
set user-group "vpnphone-grp" user "vpnphone-ike"
set ike respond-bad-spi 1
unset ike ikeid-enumeration
unset ipsec access-session enable
set ipsec access-session maximum 5000
set ipsec access-session upper-threshold 0
set ipsec access-session lower-threshold 0
set ipsec access-session dead-p2-sa-timeout 0
unset ipsec access-session log-error
unset ipsec access-session info-exch-connected
unset ipsec access-session use-error-log
set xauth default ippool "Remote-User-IP"
set xauth default dns1 192.168.1.30
set url protocol websense
exit
set monitor cpu 100
set nsmgmt bulkcli reboot-timeout 60
set ssh version v2
set ssh enable
set config lock timeout 5
set snmp port listen 161
set snmp port trap 162
set vrouter "untrust-vr"
exit
set vrouter "trust-vr"
unset add-default-route
set route 0.0.0.0/0 interface ethernet0/2 gateway 100.2.2.1 preference 20 permanently
set route 50.50.100.0/24 vrouter "untrust-vr" preference 20 metric 1
exit
set vrouter "untrust-vr"
exit
set vrouter "trust-vr"
exit