Sample Avaya {VPN}remote Pocket PC Wireless VPN Configuration using Shared IKE ID (Preshared Keys) with a NetScreen 208 Gateway - Issue 1.0

Abstract

The sample configuration provided in these Application Notes demonstrates the use of the shared IKE ID with pre-shared key feature on a NetScreen 208 gateway over an 802.11b wireless LAN to Avaya {VPN}remote Pocket PC clients equipped with Avaya IP Softphone Pocket PC.
1. Introduction

The sample configuration provided in these Application Notes demonstrates the use of the Shared IKE ID with pre-shared key feature on a NetScreen 208 gateway over an 802.11b wireless LAN to Avaya VPNetwork PPC clients equipped with Avaya IP Softphone PPC (Figure 1). The NetScreen 208 gateway is capable of authenticating multiple Avaya™ VPNetwork Pocket PC (PPC) clients using a single IKE ID and preshared key. This allows a large number of VPNetwork users to be grouped together while sharing a common VPN configuration.

The NetScreen gateway authenticates each Avaya VPNetwork PPC client during Phase 1 negotiations by first matching the common IKE ID and preshared key that each client sends to the gateway. If a match occurs in Phase 1, the NetScreen 208 gateway uses XAuth to authenticate each individual user between Phase 1 and Phase 2 IKE negotiations. If the VPNetwork remote user name and password match during the XAuth challenge, Phase 2 negotiations begin. If a match occurs in Phase 2, the VPNetwork PPC client then acquires a seat license from a predetermined Avaya™ WebLM licensing server, which is depicted on the private side of the VPN in the sample configuration provided.

Note: The Avaya WebLM Server is only required for validating Avaya VPNetwork PPC seat licenses when third party gateways such as those offered by Cisco, Netscreen, or Checkpoint are implemented. It is not required when Avaya™ Security Gateways are deployed.

1.1. Requirements

The following rules must be adhered to when using the Shared IKE ID with pre-shared key feature of the NetScreen 208 gateway to authenticate VPNetwork PPC clients using the sample network provided:

- The IKE ID must be an e-mail address
  Example demonstrated: engineers@avaya.com
- A single pre-shared key is specified for all users in a group
  Example demonstrated: secret
- XAuth must be used to authenticate each individual user
  Example demonstrated:
  
  `username=axim5/password=1234`
  
  `username=compaqppc/password=5678`
Figure 1: Wireless VPN Configuration using Shared IKE ID and Pre-Shared Key
2. Equipment and Software Validated
The following equipment and software were used for the sample configuration provided:

<table>
<thead>
<tr>
<th>Equipment</th>
<th>Software</th>
</tr>
</thead>
<tbody>
<tr>
<td>Avaya S8300 Media Server with Avaya G700 Media Gateway</td>
<td>Communication Manager 1.3</td>
</tr>
<tr>
<td>Avaya Wireless AP-3 Access Point</td>
<td>v2.0.0(269)</td>
</tr>
<tr>
<td>Avaya VPNremote Pocket PC Client</td>
<td>v1.1.24</td>
</tr>
<tr>
<td>Avaya IP Softphone Pocket PC Client</td>
<td>R2.0</td>
</tr>
<tr>
<td>Avaya 4620 IP Telephones</td>
<td>R1.8</td>
</tr>
<tr>
<td>Avaya P333R Stackable L3 Switch</td>
<td>v4.0.9</td>
</tr>
<tr>
<td>Avaya WebLM Web-based License Manager</td>
<td>R2.0 (with 100 client licenses)</td>
</tr>
<tr>
<td>NetScreen 208 Gateway</td>
<td>ScreenOS 5.0.0 r1.0</td>
</tr>
<tr>
<td>Dell AXIM X5 Pocket PC</td>
<td>PocketPC 2003</td>
</tr>
<tr>
<td>Netgear MA701 802.11b Wireless CF Card</td>
<td>v2.0</td>
</tr>
<tr>
<td>Compaq 3850 Pocket PC with CF Expansion Pack</td>
<td>PocketPC 2002</td>
</tr>
<tr>
<td>Linksys WCF11 Wireless Network CF Card</td>
<td>v1.2</td>
</tr>
</tbody>
</table>

3. Configure the NetScreen 208 Gateway
The following steps assume that the NetScreen 208 gateway has a factory default configuration, and the administrator has chosen to assign initial IP addressing using the command line interface (CLI) via the console port.

1. Start a HyperTerminal session to the Console port.
   - Bits per second **9600**
   - Data bits **8**
   - Parity **None**
   - Stop bits **1**
   - Flow control **None**

2. Enter a valid username and password.

3. Assign the Trust and Untrust Security Zones to specific Ethernet interfaces.

   ns208-> **set interface ethernet1 zone trust**
   ns208-> **set interface ethernet3 zone untrust**
4. Assign IP addresses to each Ethernet interface and enable management on the Trust side. Save the configuration.

```
ns208-> set interface ethernet1 ip 135.8.21.1/24
ns208-> set interface ethernet1 manage-ip 135.8.21.254
ns208-> set interface ethernet1 manage web
ns208-> set interface ethernet3 ip 110.110.110.1/24
ns208-> save
```

5. Log in to the NetScreen web management interface on the private side using a valid user name and password in the **Admin Name** and **Password** fields and click **Login**.

6. Define all protected network Addresses.

Navigate to **Objects** → **Addresses** → **List** → **New**, enter the following and click **OK**: See **Figure 2**.

- **Address Name**: 10.0.10.0/24
- **IP/Netmask**: (select), 10.0.10.0/24
- **Zone**: (select) **Trust**

![Address Window](image)

**Figure 2: Address Window**

Navigate to **Objects** → **Addresses** → **List** → **New**, enter the following and click **OK**: Figure not shown.

- **Address Name**: 135.8.21.0/24
- **IP/Netmask**: (select), 135.8.21.0/24
- **Zone**: (select) **Trust**
7. Define a Virtual IP Address Pool for the VPN remote PPC clients (Figure 3).

Navigate to **Objects → IP Pools → New**, enter the following and click **OK**:

- IP Pool Name: `xauthppcuser`
- Start IP: `101.101.101.1`
- End IP: `101.101.101.254`

![IP Address Pool Window](image)

**Figure 3: IP Address Pool Window**
8. Define the Shared IKE User to be used by all clients for Phase 1 negotiations (Figure 4).

Navigate to **Objects → Users → Local → New**, enter the following and click **OK**:

- **User Name**: Remote_Engineers
- **Status**: (select) Enable
- **IKE User**: (select)
- **Number of Multiple Logins with same ID**: 100
- **Simple Identity**: (select)
- **IKE Identity**: engineers@avaya.com

**Note**: The Number of Multiple Logins with same ID field indicates the number of simultaneous client logins that can be made using the IKE ID engineers@avaya.com for Phase 1 negotiations. This number should correspond with the number of VPNremote PPC client seat licenses available on the Avaya WebLM licensing server.

![Auth/IKE/L2TP/XAuth User](image_url)

---

**Figure 4: Shared IKE ID User Profile Window**
9. Define a user group and add the Shared IKE ID User to the group (Figure 5).

Navigate to Objects → Users → Local Groups, enter the following and click OK:

Group Name: R_E
Under ← Available Members → : (select) Remote_Engineers
Click the Left Pointing Arrows (<<)

Note: When more than 1 login using the same IKE ID is allowed, NetScreen requires that the Shared IKE ID user be defined in a group. In this example, up to 100 simultaneous logins are being allowed using engineers@avaya.com. Therefore, the shared IKE User must be added to a group.

![Figure 5: User Group Window](image-url)
Define the XAuth Users to be used by each client individually for authentication (Figure 6).

Navigate to **Objects** → **Users** → **Local** → **New**, enter the following and click **OK**:

- **User Name:** axim5
- **Status:** (select) Enable
- **XAuth User:** (select)
- **User Password:** 1234
- **Confirm Password:** 1234
- **IP Pool:** (select) xauthppcuser

Navigate to **Objects** → **Users** → **Local** → **New**, enter the following and click **OK**:

- **User Name:** compaqppc
- **Status:** (select) Enable
- **XAuth User:** (select)
- **User Password:** 5678
- **Confirm Password:** 5678
- **IP Pool:** (select) xauthppcuser

![Figure 6: XAuth User Profile Window](image-url)
11. Define the VPN Gateway to be used by the clients (Figure 7).

Navigate to **VPNs → AutoKey Advanced → Gateway → New**, enter the following and click **Advanced**:

- **Gateway Name**: `engineering_gateway`
- **Security Level**: (select) **Custom**
- **Dialup User Group**: (select)
  - **Group**: (select) **R_E**
- **Preshared Key**: `secret`

![VPN Gateway Window](image)

**Figure 7: VPN Gateway Window**
12. Define the Advanced VPN Gateway parameters to be used by the clients (Figure 8).

Enter the following and click **Return** then **OK**:

- **Phase 1 Proposal**: (select) **pre-g2-3des-sha**
- **Mode (Initiator)**: (select) **Aggressive**
- **XAuth Server**: (select)
- **Local Authentication**: (select)
- **Allow Any**: (select)

**Note:** The Phase 1 proposal used above was picked for demonstration purposes only. Any phase 1 proposal supported both by NetScreen and VPNremote PPC may be used. The Mode must be Aggressive for client authentication. This allows VPN users to be identified by usernames instead of being restricted to IP address identification, as is the case for Main mode.

---

![Gateway Advanced Window](image-url)
13. Define the VPN that will be used to secure client data over the wireless LAN (Figure 9).

Navigate to **VPNs -> AutoKey IKE -> New**, enter the following and click **Advanced**:

- **VPN Name:** engineering_VPN
- **Security Level:** (select) **Custom**
- **Predefined:** (select) engineering_gateway
- Click **Advanced**

![VPN Window](image)

**Figure 9: VPN Window**
14. Define the Advanced VPN Gateway parameters to be used by the clients (Figure 10).

Enter the following and click **Return** then **OK**:

- Phase 2 Proposal: (select) **nopfs-esp-3des-sha**
- Bind to: (select) **Tunnel Zone, Untrust-Tunnel**

**Note:** The Phase 2 proposal used above was chosen for demonstration purposes only. Any phase 2 proposal supported by both NetScreen and VPNremote PPC may be used. The VPN tunnel must be bound to the un-trusted interface using the Tunnel Zone drop-down menu.

---

**Figure 10: VPN Advanced Window**
15. Define static routes to all trusted networks (Figure 11).

Navigate to **Network** → **Routing** → **Routing Entries** → **New**, enter the following and click **OK**:

Network Address/Netmask: *10.0.10.0/255.255.255.0*
Gateway: (select)
Interface: (select) *ethernet1*
Gateway IP Address: *135.8.21.200*

![Figure 11: Route Window](image-url)
16. Define static routes to all un-trusted networks (Figure 12).

Navigate to Network → Routing → Routing Entries → (trust-vr) New, enter the following and click OK:

- Network Address/Netmask: **0.0.0.0/0**
- Gateway: (select)
- Interface: (select) **ethernet3**
- Gateway IP Address: **110.110.110.254**

![Route Window](image)

**Figure 12: Route Window**
17. Define policies for encrypting traffic between clients and all trusted networks.

Navigate to **Policies** → (From: Untrust, To: Trust) **New**, enter the following and click **OK**: See **Figure 13**.

Source Address:
- Address Book Entry: (select), **Dial-Up VPN**

Source Address:
- Address Book Entry: (select), **135.8.21.0/24**

Action: (select) **Tunnel**

Tunnel VPN: (select) **engineering_VPN**

![Policy Window](image)

**Figure 13: Policy Window**
Navigate to **Policies →** (From: Untrust, To: Trust) **New**, enter the following and click **OK**:  
See **Figure 14**.

Source Address:  
Address Book Entry: (select), **Dial-Up VPN**
Source Address:  
Address Book Entry: (select), **10.0.10.0/24**
Action: (select) **Tunnel**
Tunnel VPN: (select) **engineering_VPN**

![Policy Window](image-url)

**Figure 14: Policy Window**
4. Configure the VPNremote Pocket PC (PPC) Client

The following steps can be generalized for any Pocket PC running VPNremote PPC.

1. Open the VPNremote PPC client and load the VPN profile wizard (Figure 15).

   Navigate to Start → VPNremote for Pocket PC and click Advanced.

   ![Figure 15: VPNremote PPC v1.1.24 Main Page]
   
   Select the Profile Manager tab and click Add (Figure 16).

   ![Figure 16: Profile Manager]
18. Configure the VPN profile to connect to the NetScreen 208 gateway.

Using the keyboard located in the lower right corner, enter the following in profile page 1/6 (Figure 17) and click the Next arrow:

Profile Name: **ns208**
Gateway Type: (select) **NETSCREEN**
Gateway Address: **110.110.110.1**
Auth Method: (select) **XAUTH**
User Name: **axim5**
IKE ID: **engineers@avaya.com**
Preshared secret: **secret**

![Figure 17: Profile Wizard Page 1/6](image-url)
Using the keyboard located in the lower right corner, enter the following in profile page 2/6 *(Figure 18)* and click the Next arrow:

- Encryption Alg: (select) **3DES**
- Hash Alg: (select) **SHA1**
- DH Group: (select) **2**

![Figure 18: Profile Wizard Page 2/6](image-url)
Using the keyboard located in the lower right corner, enter the following in profile page 3/6 (Figure 19) and click the Next arrow:

Encryption Alg: (select) 3DES
Hash Alg: (select) HMAC_SHA
AH / ESP: (select) ESP
PFS: (select) NO

![Profile Wizard (3/6)](image)

Figure 19: Profile Wizard Page 3/6
Using the keyboard located in the lower right corner, enter the private networks located on the Trust side of the NetScreen 208 gateway in profile page 4/6 (Figure 20) and click the Next arrow:

- **IP Address:** 135.8.21.0
- **Mask:** 255.255.255.0
- **Click Add**
- **IP Address:** 10.0.10.0
- **Mask:** 255.255.255.0
- **Click Add**

![Figure 20: Profile Wizard Page 4/6](image-url)
Leave the Network Config drop-down menu set to **AUTO**, on profile page 5/6 (**Figure 21**), and click the Next arrow:

![Figure 21: Profile Wizard Page 5/6](image)

Use the keyboard located in the lower right corner to match the parameters on profile page 6/6 shown below, then click **OK** (**Figure 22**):

- **Enable Split Tunnel**: (uncheck)
- **License Server**: [http://135.8.21.51/WebLM/LicenseServer](http://135.8.21.51/WebLM/LicenseServer)

![Figure 22: Profile Wizard Page 6/6](image)
5. Configure the P333R Switch

The following steps can be generalized for most configurations.

1. Start a HyperTerminal session to the embedded P330 switch via the console port.
   - Bits per second 9600
   - Data bits 8
   - Parity None
   - Stop bits 1
   - Flow control None

2. Enter a valid user name and password.

3. Configure the port VLANs.

   P330-1(super)# set port vlan 135 1/1-2
   P330-1(super)# set port vlan 10 1/3-5

4. Enter the router configuration mode.

   P330-1(super)# session router
   Router-1(super)# configure
   Router-1(configure)#

5. Configure the Virtual LANs that are to be associated with each router interface.

   Router-1(configure)# set vlan 10 name vlan10
   Router-1(configure)# set vlan 135 name vlan135

6. Provision the router interfaces for each Virtual LAN.

   Router-1(configure)# interface vlan10
   Router-1(config-if:vlan10)# ip address 10.0.10.1 255.255.255.0
   Router-1(config-if:vlan10)# ip vlan name vlan10
   Router-1(config-if:vlan10)# ex
   Router-1(configure)# interface vlan135
   Router-1(config-if:vlan135)# ip address 135.8.21.200 255.255.255.0
   Router-1(config-if:vlan135)# ip vlan name vlan135
   Router-1(config-if:vlan135)# exit

7. Create a static route destined for the client virtual IP address pool using the NetScreen 208 gateway trust IP interface as the next hop address. Save the configuration.

   Router-1(configure)# ip route 101.101.101.0 255.255.255.0 135.8.21.1 1
   Router-1(configure)# copy running-config startup-config

Note: If this static route is not added, VPNremote PPC tunnel traffic will have no return route and connectivity between the clients and the trusted networks will fail.
6. Configure the Media Server
The following steps can be generalized for most configurations

1. Configure Codec Set 1 with G.711MU default settings (Figure 23).

   ```
   change ip-codec-set 1
   Codec Set: 1
   Audio Codec: G.711MU
   Silence Suppression: n
   Frames Per Pkt: 2
   Packet Size(ms): 20
   ```

   Figure 23: IP Codec Set Form

2. Prepare Region 1 for use specifically for IP Telephones using Codec Set 1 (Figure 24).

   ```
   change ip-network-region 1
   Region: 1
   Name: IP Hardphone Region
   Location: 
   AUDIO PARAMETERS
   Codec Set: 1
   UDP Port Range
   Min: 2048
   Max: 3029
   DIFFSERV/TOS PARAMETERS
   Call Control PHB Value: 34
   Audio PHB Value: 46
   AUDIO RESOURCE RESERVATION PARAMETERS
   RSVP Enabled? n
   802.1P/Q PARAMETERS
   Call Control 802.1p Priority: 7
   Audio 802.1p Priority: 6
   Inter-region IP-IP Direct Audio: yes
   ```

   Figure 24: IP Network Region Form
3. Prepare Region 2 for use specifically for IP Softphones using Codec Set 1 (Figure 25).

Note: Intra-region IP-IP Direct Audio is disabled for the IP Softphone Region because the VPN policy will not allow the IP Softphone PPC clients to establish direct audio connections with each other using their Virtual IP Addresses. In order for two protected IP Softphone PPC users to communicate with one another, each must tunnel back to the Media Gateway first.

![change ip-network-region 2]

### Figure 25: IP Network Region Form

4. Configure the IP Network Map feature to force IP Telephones and IP Softphones to be assigned to specific regions (Figure 26).

![change ip-network-map]

### Figure 26: IP Address Mapping Form
5. Change IP Network Region 2 page 2 of 3 such that IP Codec Set 1 is used for Inter-Region calling between Regions 1 and 2 (Figure 27).

![Figure 27: IP Network Region 2 (Page 2 of 3) Form]

**7. Verification Steps**

The following steps can be used to validate the configuration.

**7.1. Log VPNremote PPC Client Into VPN Tunnel**

1. Verify that the VPNremote PPC client can connect to the public interface of the NetScreen 208 gateway. This may require that the NetScreen firewall policies be modified if ICMP was previously blocked. Open the VPNremote PPC client. Navigate to Tools → Ping Utility (Figure 28).

![Figure 28: VPNremote PPC v.1.1.24 Main Menu]
2. Using the keyboard located in the lower right corner, enter Untrust (ethernet3) IP address of the NetScreen 208 gateway in the Host field (e.g. 110.110.110.1) and click Ping (Figure 29).

![Figure 29: Ping Utility](image)

3. Log in the VPN User. From the Profile drop-down menu select ns208. Enter 1234 in the Password field and click Connect (Figure 30).

![Figure 30: Log In AXIM 5 User](image)
4. Observe that a VPN tunnel has been connected (Figure 31). Click Advanced.

![Figure 31: VPNremote PPC Connected Window](image1)

5. Verify that two Security Associations (one for each network) have been created. Select one of the SAs and click Details (Figure 32).

![Figure 32: VPNremote PPC Secure Connection Window](image2)
6. Verify that the expected IKE and IPsec parameters have been negotiated for the SA being observed (Figure 33). Click Tools.

![Figure 33: VPNremote PPC Secure Connection Session Window](image1)

7. Using the keyboard located in the lower right corner enter the IP address of the protected Media Server in the Host field (e.g. **10.0.10.102**) and click Ping (Figure 34). This establishes that the tunnel is up and routing is working as expected.

![Figure 34: VPNremote PPC Ping Utility Window](image2)
If the user gets the following message, the WebLM server is inaccessible, the WebLM server is not configured properly, or the URL request is incorrectly formatted for the WebLM server in the Profile Wizard (Figure 35).

![VPNremote v1.1](image)

**Figure 35: License Failure**

7.2. Inspect NetScreen Log during VPNremote PPC Authentication

Things to look for in the log output (Figure 36):

1. Aggressive mode negotiations from VPNremote PPC are acknowledged.
2. Shared IKE ID "engineers@avaya.com" is used for Phase 1 negotiations
3. After completing Phase 1 the XAuth login of user "axim5" completes challenge.
4. Two Phase 2 Security Associations (SAs) are created, one for each private network.

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IKE&lt;110.110.110.151&gt; Phase 2 msg ID &lt;00000bb3&gt;: Completed negotiations with SPI &lt;4545bc27&gt;, tunnel ID &lt;32773b&gt;, and...</td>
</tr>
<tr>
<td>IKE&lt;110.110.110.151&gt; Phase 2 msg-id &lt;00000bb3&gt;: Completed for user <a href="mailto:engineers@avaya.com">engineers@avaya.com</a>.</td>
</tr>
<tr>
<td>IKE&lt;110.110.110.151&gt; Phase 2 msg ID &lt;000000029&gt;: Completed negotiations with SPI &lt;4545bc26&gt;, tunnel ID &lt;32777&gt;, and...</td>
</tr>
<tr>
<td>IKE&lt;110.110.110.151&gt; Phase 2 msg-id &lt;000000029&gt;: Completed for user <a href="mailto:engineers@avaya.com">engineers@avaya.com</a>.</td>
</tr>
<tr>
<td>IKE&lt;110.110.110.151&gt; Phase 2 msg ID &lt;000000bb3&gt;: Responded to the peer's first message from user &lt;<a href="mailto:engineers@avaya.com">engineers@avaya.com</a>...</td>
</tr>
<tr>
<td>IKE&lt;110.110.110.151&gt;: Received initial contact notification and removed Phase 1 SAs.</td>
</tr>
<tr>
<td>IKE&lt;110.110.110.151&gt;: Received initial contact notification and removed Phase 2 SAs.</td>
</tr>
<tr>
<td>IKE&lt;110.110.110.151&gt;: Received a notification message for DOI &lt;11&gt; &lt;24576&gt; NOTIFY_INITIAL_CONTACT&gt;.</td>
</tr>
<tr>
<td>IKE&lt;110.110.110.151&gt; Phase 2 msg ID &lt;000000029&gt;: Responded to the peer's first message from user &lt;<a href="mailto:engineers@avaya.com">engineers@avaya.com</a>...</td>
</tr>
<tr>
<td>IKE&lt;110.110.110.151&gt;: XAuth login was passed for gateway &lt;engineering_gateway&gt;, username &lt;axim5&gt;, retry: 0.</td>
</tr>
<tr>
<td>IKE&lt;110.110.110.151&gt; Phase 1: Completed Aggressive mode negotiations with a &lt;28860&gt;:second lifetime.</td>
</tr>
<tr>
<td>IKE&lt;110.110.110.151&gt; Phase 1: Completed for user <a href="mailto:engineers@avaya.com">engineers@avaya.com</a>.</td>
</tr>
<tr>
<td>IKE&lt;110.110.110.151&gt; Phase 1: Responder starts AGGRESSIVE mode negotiations.</td>
</tr>
</tbody>
</table>

All logged events or alarms were cleared by admin netscreen.

**Figure 36: NetScreen 208 Gateway Log Trace**
7.3. Place Test Calls using Softphone PPC

1. Enter the following and click **Log In** (**Figure 37**):

   - Extension: 44005
   - Password: 1234
   - Server IP: 10.0.10.102

   ![Figure 37: Log In Window for IP Softphone PPC](image)

   **Figure 37:** Log In Window for IP Softphone PPC

2. Verify log in. Notice VPN override indicates the Virtual IP address assigned to the VPN remote PPC client (**Figure 38**). Place test calls.

   ![Figure 38: IP Softphone PPC with Phone Skin Loaded](image)

   **Figure 38:** IP Softphone PPC with Phone Skin Loaded
7.4. Communication Manager Call Traces

1. Enter `list trace station 44005` from the SAT (Figure 39). Place a call between x44005 and x44003. Notice that the call is Inter-region between 1 and 2 using G.711MU between the IP Telephones IP address and Virtual IP Address of the VPNremote PPC client.

```
list trace station 44005

LIST TRACE

time            data
05:54:14     active station    44005 cid 0x99
05:54:14     G711MU ss:off ps:20 rn:2/1 101.101.101.1:2048 10.0.10.103:2262
05:54:19     dial 44003
05:54:19     ring station    44003 cid 0x99
05:54:19     G711MU ss:off ps:20 rn:1/1 10.0.10.121:2618 10.0.10.103:2264
05:54:23     active station    44003 cid 0x99
05:54:23     G711MU ss:off ps:20 rn:2/1 101.101.101.1:2048 10.0.10.121:2618
05:54:30     idle station    44003 cid 0x99
```

Figure 39: List Trace Form

2. Enter `list trace station 44850` from the SAT (Figure 40). Place a call between x44850 and x44005. Even through this is an Intra-region call, the call is routed back to the Media Gateway VoIP because Intra-region IP-IP Direct Audio was disabled for Region 2.

```
list trace station 44850

LIST TRACE

time            data
06:02:16     active station    44850 cid 0xa7
06:02:16     G711MU ss:off ps:20 rn:2/1 101.101.101.2:2048 10.0.10.103:2294
06:02:22     dial 44005
06:02:22     ring station    44005 cid 0xa7
06:02:22     G711MU ss:off ps:20 rn:2/1 101.101.101.1:2048 10.0.10.103:2296
06:02:52     active station    44850 cid 0xa7
06:03:49     idle station    44850 cid 0xa7
```

Figure 40: List Trace Form

8. Conclusion

Connectivity between all Avaya VPNremote PPC clients and the NetScreen 208 gateway over a wireless LAN can be achieved using the guidelines demonstrated in these Application Notes. In addition, Avaya IP Softphone PPC may also be used in conjunction with the VPN tunnel demonstrated to provide secure IP telephony in a wireless environment. The steps described in these Application Notes can be generalized for most configurations.