Application Notes for Configuring a Site-to-Site VPN Tunnel Between Avaya Small Office and NetScreen 5XT, and a Dynamic VPN Tunnel Between Avaya Small Office and NetScreen-Remote Client - Issue 1.0

Abstract

These Application Notes present a sample configuration for NetScreen 5XT and NetScreen-Remote Client working with Avaya Small Office and Avaya PhoneManager in an IPSec VPN environment.
1. Introduction

These Application Notes describe the VPN configurations among the NetScreen 5XT security device, NetScreen-Remote client, and Avaya Small Office 2.0. The Avaya Small Office and the NetScreen 5XT are configured to provide a site-to-site IPSec Tunnel between Site A and Site B, and the NetScreen-Remote client is configured to set up a dynamic IPSec tunnel between the PC on Site C and the Small Office on Site A to support Avaya PhoneManager. Figure 1 displays the network configuration used for verification.

Figure 1: Network Configuration
Table 1 lists IP addresses and subnet mask for devices used in those tests.

<table>
<thead>
<tr>
<th>Device</th>
<th>Interface</th>
<th>IP Address/Mask</th>
<th>Gateway</th>
</tr>
</thead>
<tbody>
<tr>
<td>Small Office</td>
<td>LAN 1 (Private)</td>
<td>200.1.1.1/24</td>
<td></td>
</tr>
<tr>
<td></td>
<td>LAN 2 (Public)</td>
<td>110.1.1.1/24</td>
<td></td>
</tr>
<tr>
<td>NetScreen 5XT</td>
<td>Ethernet 1 (Private)</td>
<td>70.1.1.1/24</td>
<td>90.1.1.2</td>
</tr>
<tr>
<td></td>
<td>Ethernet 2 (Public)</td>
<td>90.1.1.1/24</td>
<td></td>
</tr>
<tr>
<td>NetScreen –Remote Client</td>
<td>NIC on PC</td>
<td>115.1.1.100/24</td>
<td>115.1.1.1</td>
</tr>
<tr>
<td>Cajun P330R</td>
<td>Vlan1 (to Small Office)</td>
<td>110.1.1.2/24</td>
<td>110.1.1.1</td>
</tr>
<tr>
<td></td>
<td>Vlan90 (to NetScreen 5XT)</td>
<td>90.1.1.2/24</td>
<td>90.1.1.1</td>
</tr>
<tr>
<td></td>
<td>Vlan115 (to Site C)</td>
<td>115.1.1.1/24</td>
<td></td>
</tr>
</tbody>
</table>

Table 1: IP Address/Mask Assignment

2. Equipment and Software Validated

Table 2 shows equipment and software used for the sample configuration provided:

<table>
<thead>
<tr>
<th>Equipment</th>
<th>Software</th>
</tr>
</thead>
<tbody>
<tr>
<td>Avaya Small Office</td>
<td>2.0</td>
</tr>
<tr>
<td>Avaya S8300 Media Server running Communication Manager Software</td>
<td>2.0</td>
</tr>
<tr>
<td>Avaya 4620 IP Telephone</td>
<td>2.0</td>
</tr>
<tr>
<td>Avaya PhoneManager</td>
<td>2.0.13</td>
</tr>
<tr>
<td>Avaya P333R Stackable Switch</td>
<td>4.0.8</td>
</tr>
<tr>
<td>Avaya P333T Stackable Switch</td>
<td>4.0.17</td>
</tr>
<tr>
<td>NetScreen 5XT</td>
<td>5.0.r3.0</td>
</tr>
<tr>
<td>NetScreen-Remote</td>
<td>10.0.0 (Build 10)</td>
</tr>
</tbody>
</table>

Table 2: Equipment and Software Used in Testing

3. Site-to-Site IPSec Tunnel between the Small Office and the NetScreen 5XT

3.1. Configure the NetScreen 5XT

The site-to-site VPN tunnel between the NetScreen 5XT and Avaya Small Office is configured based on the following parameters:
<table>
<thead>
<tr>
<th></th>
<th>Authentication</th>
<th>Encryption</th>
<th>Hash</th>
<th>Key Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phase 1 (IKE)</td>
<td>Pre-shared key</td>
<td>Triple DES</td>
<td>SHA</td>
<td>2</td>
</tr>
<tr>
<td>Phase 2 VPN</td>
<td>Triple DES</td>
<td>SHA</td>
<td>N/A</td>
<td></td>
</tr>
</tbody>
</table>

A route-based VPN tunnel is used in this configuration. Route-based VPN is a feature in NetScreenOS where the endpoint of a VPN tunnel is seen as a network interface instead of a policy. From a routing standpoint, a route-based VPN behaves similarly to other point-to-point WAN technologies like Frame Relay or ATM.

```
******  Set up service for H.323 signaling protocol  *********

set service "Q931" protocol tcp src-port 1-65535 dst-port 1720-1720
  timeout 2160
set service "ras" protocol udp src-port 1-65535 dst-port 1719-1719
  timeout 2160

******  Setup login name and password  *********

set hostname ns5XT
set admin name "NetScreen"
set admin password "NetScreen"
set admin auth timeout 10

****  Create the physical interfaces and assign them to zones  ***********

set interface e1 zone Trust
set interface e1 route
set interface e1 ip 70.1.1.1/24

set interface e2 zone Untrust
set interface e2 route
set interface e2 ip 90.1.1.1/24

****  Create the virtual tunnel interface, which is the virtual tunnel endpoint.  ****
****  Assign the tunnel interface into the "trust" zone.  ****

set interface tunnel.1 zone Trust
set interface tunnel.1 route
set interface tunnel.1 ip unnumbered interface e1
```
***** Define the security gateway parameters for phase 1 proposal using 3DES-SHA1 *****
***** and bind it to the outgoing interface Ethernet2. *****

set ike gateway Small-Office-gw address 200.1.1.1 outgoing-interface e2 preshare netscreen proposal pre-g2-3des-sha

***** Define the VPN parameters for phase 2 proposal using 3DES-SHA1. Configure *****
***** the firewall to copy DiffServ QoS bits from the original packets into the *****
***** IP header of the encrypted packets. Bind the tunnel to the outgoing interface *****

set vpn Small-Office-vpn gateway Small-Office-gw idletime 0 proposal g2-esp-3des-sha
set vpn Small-Office-vpn monitor
set vpn Small-Office-vpn df-bit copy
set vpn Small-Office-vpn bind interface tunnel.1

***** Define the local and remote network, and the service for traffic to *****
***** be encrypted by the tunnel. *****

set vpn Small-Office-vpn proxy-id local-ip 70.1.1.0/24 remote-ip 200.1.1.0/24 any

***** Set route into the VPN tunnel for the remote network. *****

set route 110.1.1.0/24 gateway 90.1.1.2
set route 200.1.1.0/24 interface tunnel.1
4. Configure the Avaya Small Office
This section describes the steps necessary to configure the Small Office working with the NetScreen 5XT.

4.1. Configure the Avaya Small Office Parameters
The Avaya Small Office is configured using the IP Office Manager application. The LAN 1 interface is used for protected network connectivity, while the LAN 2 interface is used for public network connectivity.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 1.   | **Configuring interface LAN1**  
Using the IP Office Manager, browse the configuration tree and select **System Configuration** and click the **LAN1** tab. |
|      | • Set **IP Address** to 200.1.1.1 and **IP Mask** to 255.255.255.0.  
• Leave the **Primary Trans. IP Address** field blank  
• Leave the **Enable NAT** box unchecked  
• For the **DHCP Mode**, select **Disabled**. In the described configuration, static IP addresses are assigned to devices at all sites. |
### Step 2

**Configuring interface LAN2**

Click the **LAN2** tab.

- Set **IP Address** to 110.1.1.1 and **IP Mask** to 255.255.255.0.
- Leave the **Primary Trans. IP Address** field blank
- Leave the **Enable NAT** box unchecked
- For the **DHCP Mode**, select **Disabled**
- Click **OK** when done.

![System Configuration Dialog](image)

<table>
<thead>
<tr>
<th>System</th>
<th>LAN1</th>
<th>LAN2</th>
<th>DNS</th>
<th>Voicemail</th>
<th>Telephony</th>
<th>Gatekeeper</th>
<th>LDAP</th>
<th>SMTP</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>110.1.1.1</td>
<td>Number Of DHCP IP Addresses</td>
<td>200</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP Mask</td>
<td>255.255.255.0</td>
<td>DHCP Mode</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Firewall Profile</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Primary Trans. IP Address</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Step</td>
<td>Description</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| 3.   | **Configuring default gateway**  
Using the IP Office Manager, browse the configuration tree and select **IP Route**.  
- Leave **IP Address** and **IP Mask** fields blank  
- Enter **110.1.1.2** (IP address of P333R interface) as gateway IP address  
- Select **LAN2** as **Destination**  
- Click **OK** when done. |

[Image of IP Route configuration screen]

| 4.   | **Configuring IPSec Tunnel**  
Using the IP Office Manager, browse the configuration tree and select **Tunnel**.  
- Move the mouse in the right side of configuration panel. Right click the mouse and select **New** to add a new tunnel  
- Click **IP Sec** as **Tunneling Type**  
- Click **OK** when done |
5. **Configuring IPSec tunnel for local and remote networks**

   Click the **Main** tab and enter the information as shown in figure below.

   Note the following:
   - Network 200.1.1.0 is the protected network behind the Small Office on Site A
   - Gateway address 110.1.1.1 is the Small Office’s LAN2 IP address
   - Network 70.1.1.0 is the protected network behind the NetScreen 5XT on Site B
   - Gateway address 90.1.1.1 is the IP address of the NetScreen 5XT’s public interface

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td><strong>Configuring IPSec tunnel for local and remote networks</strong></td>
</tr>
</tbody>
</table>

Click the **Main** tab and enter the information as shown in figure below.

<table>
<thead>
<tr>
<th>Configuration Tree</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Tunnel Name</th>
<th>Local Account Name</th>
<th>Remote Account Name</th>
<th>Local Gateway</th>
</tr>
</thead>
<tbody>
<tr>
<td>SiteA-B</td>
<td></td>
<td></td>
<td>110.1.1.1</td>
</tr>
</tbody>
</table>

Remote Configuration:
- **IP Address**: 70.1.1.0
- **IP Mask**: 255.255.255.0
- **Gateway**: 90.1.1.1

![Diagram of configuration settings](image.png)
### Step 6: Configuring the IKE Policies (phase 1)

- Click the IKE Policies tab
- Enter the password in the **Shared Secret** field
- Re-enter the password in the **Confirm Password** field
- Select **ID Prot** (Main mode) in the **Exchange Type** field
- Select **3DES CBC** in the **Encryption** field
- Select **SHA** in the **Authentication** field
- Select **Group 2** in the **DH Group** field
- Select **Seconds** in the **Life Type** field
- Type **28800** in the **Life** field

#### Configuration Tree

```
+--- BOOTP (1)
  +--- Operator (4)
  |     +--- System OCE 007014994 (5)
  |     +--- Line (5)
  |     +--- Control Unit (3)
  |     +--- Extension (16)
  |     +--- User (18)
  |     +--- Hunt Group (1)
  |     +--- Shortcode (59)
  |     +--- Service (0)
  |     +--- RAS (1)
  |     +--- Incoming Call Route (2)
  |     +--- WAN Port (0)
  |     +--- Directory (0)
  |     +--- Time Profile (0)
  |     +--- Firewall Profile (1)
  |     +--- IP Route (5)
  |     +--- Least Cost Route (0)
  |     +--- License (5)
  |     +--- Account Code (0)
  |     +--- Wireless 802.11b (1)
  |     +--- User Restriction (1)
  |     +--- Logical LAN (0)
  |     +--- Tunnel (3)
  |         +--- SiteA-B
  |         +--- SiteC-a
  |         +--- Remote-Client
  +--- Auto Attendant (0)
  +--- E911 System (1)
```

#### Tunnel Name Table

<table>
<thead>
<tr>
<th>Tunnel Name</th>
<th>Remote Account Name</th>
<th>IPSec Policies</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Main  | IKE Policies  | IPSec Policies  |
|-----------|---------------|-----------------|

- **Shared Secret**: 
- **Confirm Password**: 
- **Exchange Type**: ID Prot
- **Encryption**: 3DES CBC
- **Authentication**: SHA
- **DH Group**: Group 2
- **Life Type**: Seconds
- **Life**: 28800
7. **Configuring the IPSec Policies (phase II)**

- Click the **IPSec Policies** tab
- Select **ESP** in the **Protocol** field
- Select **3DES** in the **Encryption** field
- Select **HMAC SHA** in the **Authentication** field
- Select **Seconds** in the **Life Type** field
- Type **3600** in the **Life** field
- Click OK when done
8. **Configuring line options**

Using the IP Office Manager, browse the configuration tree and select **Line**.

- Enter **06** in the **Line Number** field
- Enter description in **Telephone Number** field (optional)
- Enter **6** as **Incoming Group** and **Outgoing Group ID**
- Enter **20** as voice and data channels as shown in figure below

---

**Configuration Tree**

**IP Line Options**

<table>
<thead>
<tr>
<th>Line Number</th>
<th>Telephone Number</th>
<th>Number Of Channels</th>
<th>Data Channels</th>
</tr>
</thead>
<tbody>
<tr>
<td>06</td>
<td></td>
<td>30</td>
<td>20</td>
</tr>
</tbody>
</table>

**Outgoing Channels**

<table>
<thead>
<tr>
<th>Outgoing Channels</th>
<th>TEI</th>
</tr>
</thead>
<tbody>
<tr>
<td>20</td>
<td>0</td>
</tr>
</tbody>
</table>

**Voice Channels**

<table>
<thead>
<tr>
<th>Voice Channels</th>
<th>TEI</th>
</tr>
</thead>
<tbody>
<tr>
<td>20</td>
<td>0</td>
</tr>
</tbody>
</table>

**Incoming Group ID**

<table>
<thead>
<tr>
<th>Incoming Group ID</th>
<th>International Prefix</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>00</td>
</tr>
</tbody>
</table>

**Outgoing Group ID**

<table>
<thead>
<tr>
<th>Outgoing Group ID</th>
<th>International Prefix</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>00</td>
</tr>
</tbody>
</table>

**National Prefix**

<table>
<thead>
<tr>
<th>National Prefix</th>
<th>Prefix</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Step</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>9.</td>
<td>Click the <strong>VoIP</strong> tab to enter H.323 trunk configuration.</td>
</tr>
</tbody>
</table>

- In the **Gateway IP Address** field, enter **70.1.1.5**. This is the IP address of the S8300 Media Server at Site B.
- In the **Compression Mode** field, select **G.711 ULAW 64K**.
- In the **H.450 Mode** field, select **H.450**.
- The **Silence Suppression** box may remain unchecked.
- Select the **Enable Faststart** checkbox.
- Leave the **Fax Transport Support** box unchecked.
- Leave the **Local Hold Music** box unchecked.
- Leave the **Local Tones** box unchecked.
- Leave the **Out of Band DTMF** unchecked.
- Select the **Allow Direct Media Path** checkbox.
- Leave the **Voice Networking** box unchecked.
- Click **OK** when done.
10. Configuring the Shortcode

Configure the shortcode so that the Small Office will route the calls to S8300 Media Server using the H.323 trunk defined in Step 8.

Using the IP Office Manager, browse the configuration tree and select **Shortcode**.

- Enter 4xxxx in the **Short Code** field
- Enter . in the **Telephone Number** field
- Enter 06 in the **Line Group** field
- Select **Dial** in the **Feature** field
- Click **OK** when done.

![Shortcode Configuration](image-url)
Step 11. **Configuring a user**
In Small Office, every extension must be associated with a user. The following example shows how to configure a PhoneManager user using extension 50001.

Using the IP Office Manager, browse the configuration tree and select **User**.

- Enter information in the fields as shown below.

![User Configuration Screen](image-url)
<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 12.  | • Click the **Telephony** tab  
      • Select **VoIP** from the **Phone Manager Type** field  
      • Leave other parameters as default  
      • Click **OK** when done. |
### Step 13: Configuring an extension

Using the IP Office Manager, browse the configuration tree and select **Extension**.

- Right click **Extension** and select **Add**
- **Extension ID 8001** is assigned by Small Office, leave it unchanged
- Enter **50001** in the field of **Extension**
- Configure and select other parameters as shown in the figure below

#### IP Extension 50001

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extension ID</td>
<td>8001</td>
</tr>
<tr>
<td>Extension</td>
<td>50001</td>
</tr>
<tr>
<td>Caller Display Type</td>
<td>CRI</td>
</tr>
</tbody>
</table>

- **Equipment Classification**
  - Quiet Headset
  - Paging Speaker
  - Standard Telephone
  - IVR Port

- **Flash Hook Pulse Width**
  - **Use System Defaults**
  - **Minimum Width**: 2 (Unit: 10ms)
  - **Maximum Width**: 50 (Unit: 10ms)

- **Message Waiting Lamp Indication Type**: None

- **Reset Volume After Calls**: unchecked

![IP Extension 50001 Configuration](image)
<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 14.  | • Select the **VoIP** tab  
      • Configure and select other parameters as shown in the figure below  
      • Click **OK** when done. |

**IP Extension 50001**

<table>
<thead>
<tr>
<th>IP Address</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Voice Pkt. Size</td>
<td>160</td>
<td></td>
</tr>
<tr>
<td>Compression Mode</td>
<td>0.711 ULAW 8K</td>
<td></td>
</tr>
<tr>
<td>MAC Address</td>
<td>000000000000</td>
<td></td>
</tr>
</tbody>
</table>

- Silence Suppression  
- Enable Faststart  
- Fax Transport Support  
- Local Hold Music  
- Local Tones  
- Enable RSVP  
- Out Of Band DTMF  
- Allow Direct Media Path

| OK | Cancel | Help |

<table>
<thead>
<tr>
<th>15.</th>
<th><strong>Save changes to the Small Office</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Under the Manager File Menu item, select <strong>Save</strong>. At the <strong>Send Config to</strong> dialog box, click the <strong>immediately</strong> reboot mode radio button and press <strong>OK</strong>.</td>
</tr>
<tr>
<td></td>
<td>• If the Small Office Server IP address has been changed, update the PC address and reset the Manager “preferences” setting under the File menu before reconnecting.</td>
</tr>
</tbody>
</table>
5. Remote IPSec Tunnel between the Avaya Small Office and the NetScreen-Remote Client

This section describes the steps necessary to configure the Avaya Small Office and the NetScreen-Remote client to establish a remote IPSec tunnel.

5.1. Configure the Avaya Small Office

The Avaya Small Office is configured as a VPN tunnel gateway for NetScreen-Remote Client. To support a generic VPN installation package and avoid user specific configuration on the VPN client, the user should be configured to authenticate with a password, either maintained locally on the firewall or on a RADIUS server.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 1.   | **Configuring IPSec Tunnel**  
   Using the IP Office Manager, browse the configuration tree and select **Tunnel**.  
   - Move the mouse in the right side of configuration panel. Right click the mouse and select **New** to add a new tunnel  
   - Click **IP Sec** as **Tunneling Type**  
   - Click **OK** when done |
2. **Configuring local and remote networks for the tunnel**

Click the **Main** tab and enter the information as shown in figure below.

Note the following:

Under the Local Configuration:
- Network 200.1.1.0 is the protected network behind the Small Office on Site A
- Gateway address 110.1.1.1 is the Small Office’s LAN2 IP address

Under the Remote Configuration:
- Network 115.1.1.0 is the protected network in Site C
- Gateway address 115.1.1.100 is the IP address of the PC on which the NetScreen-Remote client resides
<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.</td>
<td><strong>Configuring the IKE Policies (phase I)</strong></td>
</tr>
<tr>
<td></td>
<td>- Click the <strong>IKE Policies</strong> tab</td>
</tr>
<tr>
<td></td>
<td>- Enter the password in the <strong>Shared Secret</strong> field</td>
</tr>
<tr>
<td></td>
<td>- Re-enter the password in the <strong>Confirm Password</strong> field</td>
</tr>
<tr>
<td></td>
<td>- Select <strong>Aggressive</strong> in the <strong>Exchange Type</strong> field</td>
</tr>
<tr>
<td></td>
<td>- Select <strong>3DES CBC</strong> in the <strong>Encryption</strong> field</td>
</tr>
<tr>
<td></td>
<td>- Select <strong>SHA</strong> in the <strong>Authentication</strong> field</td>
</tr>
<tr>
<td></td>
<td>- Select <strong>Group 2</strong> in the <strong>DH Group</strong> field</td>
</tr>
<tr>
<td></td>
<td>- Select <strong>Seconds</strong> in the <strong>Life Type</strong> field</td>
</tr>
<tr>
<td></td>
<td>- Type <strong>3660</strong> in the <strong>Life</strong> field</td>
</tr>
</tbody>
</table>

**Configuring the IPSec Policies (phase II)**
<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 4.   | - Click the **IPSec Policies** tab  
      - Select **ESP** in the **Protocol** field  
      - Select **3DES** in the **Encryption** field  
      - Select **HMAC SHA** in the **Authentication** field  
      - Select **Seconds** in the **Life Type** field  
      - Type **3600** in the **Life** field  
      - Click **OK** when done |

![](image)

5. **Save changes to the Small Office**

- Under the Manager File Menu item, select **Save**. At the **Send Config to** dialog box, click the **immediately** reboot mode radio button and press **OK**.
- If the IP Office Server IP address has been changed, update the PC address and reset the Manager “preferences” setting under the File menu before reconnecting.
5.2. Configure the NetScreen-Remote Client

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 1.   | **Configuring client connection**  
  - Launch the NetScreen Remote client by selecting Start → Programs → NetScreen-Remote → Security Policy Editor.  
  - Right click the folder My Connections and select Add → Connection. Name the new connection as Netscreen Testing.  
  - Select Secure for Connection Security  
  - Select IP Subnet for ID Type  
  - Enter 200.1.1.0 in the field Subnet and 255.255.255.0 in the field Mask  
  - Select All in the Protocol field and Secure Gateway Tunnel in the Connect using field. Check the Connect using box.  
  - Select IP Address in the field ID Type and enter 110.1.1.1 (IP Address of the Small Office LAN2 interface) as the tunnel endpoint IP Address. |

![Security Policy Editor - NetScreen-Remote](image)
<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 2.   | **Configuring the tunnel mode**  
• Highlight the Security **Policy** and select **Aggressive Mode** |

![Security Policy Editor - NetScreen-Remote](image)

- **Network Security Policy**
  - My Connections
    - Netscreen testing
    - My Identity
    - Security Policy
      - Authentication (Phase 1)
      - Key Exchange (Phase 2)
    - Other Connections

- **Security Policy**
  - Select Phase 1 Negotiation Mode
    - Main Mode
    - Aggressive Mode
    - Use Manual Keys
  
  - Enable Perfect Forward Secrecy (PFS)
    - Diffie-Hellman Group 2
  
  - Enable Replay Detection
3. **Configuring client identity**
   - Expand the **Netscreen testing** folder and select **My Identity**
   - Select **Any** in the **Name** field under the **Internet Interface**
   - Leave other fields as default
   - Click **Pre-Shared Key** under **My Identity**

   - Click **Enter Key** and type key in the field
   - Click **OK** when done
4. **Configuring phase 1 proposal**

- Expand folder **Security Policy → Authentication (Phase 1) → Proposal 1**
- Select **Pre-Shared Key** under **Authentication Method**
- Select **Triple DES** for **Encrypt Alg**, and **SHA-1** for **Hash Alg**
- Select **Unspecified** for **SA Life**, and **Diffie-Hellman Group 2** for **Key Group**
5. **Configuring phase 2 proposal**
   - Expand folder Security Policy → Key Exchange (Phase 2) → Proposal 1
   - Select Unspecified for SA Life, and None for Compression
   - Check the box Encapsulation Protocol (ESP)
   - Select Triple DES for Encrypt Alg, and SHA-1 for Hash Alg
   - Select Tunnel for Encapsulation

6. **Saving the configuration**
   - From the main menu, select File → Save.
   
   Or

   - Click the floppy disk icon from the tool bar.
6. Configure the Avaya PhoneManager

This section describes the steps necessary to configure the PhoneManager connecting to the Small Office via a remote VPN tunnel.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td><strong>Configuring PhoneManager</strong></td>
</tr>
<tr>
<td></td>
<td>• Launch Avaya PhoneManager by selecting Start → Programs → IP Office → PhoneManager from the PC where the PhoneManager is installed.</td>
</tr>
<tr>
<td></td>
<td>• Configure the PhoneManager to use Small Office as a Call Server by selecting Configure → PBX….</td>
</tr>
</tbody>
</table>

![Phone Manager interface](image)
- In the field **UserName**, select **Ext50020** (previously created from the Small Office)
- In the field **Password**, Enter the password previously defined
- In the field **PBX Address**, enter the Small Office’s private interface IP Address 200.1.1.1
- Click **Login >>** to log into Small Office
2. To set codec preferences for the PhoneManager, select Configure ➔ Preferences …
   • Highlight the codec and move it up or down by clicking the up or down button
   • Check the box Enable FastStart
   • Click OK when done

7. Verification Steps

The following verification steps can be used to verify correct system operation:
   • Make a call from the IP telephone on site A to the digital telephone on site B, and verify the voice quality is good.
   • Use an Ethernet sniffer to decode the VoIP packets on the public side, and verify that the packets are encapsulated with IPSec header.
   • Launch the NetScreen-Remote client and verify that the remote VPN tunnel is up between the NetScreen-Remote client and the Small Office.
   • Launch the PhoneManager and verify that the PhoneManager can register with the Small Office successfully through the IPSec tunnel.
   • Make a call from the PhoneManager on site C to the IP telephone on site A, and verify that the voice quality is good.
• Make a call from digital telephone on site A to the PhoneManager on site C. While the calls is up, conference the IP Telephone at site B and verify that all three parties are in the conference, and the voice quality is good.

8. Conclusion
These Application Notes describe the configuration steps necessary to allow Avaya Small Office and Avaya PhoneManager to work with NetScreen 5XT security device and NetScreen-Remote client. All configurations described have been tested and all test cases have been successfully completed.

9. Additional References
For Avaya IP Office related configuration information, visit http://support.avaya.com/