Abstract

These Application Notes describe the setup and configuration of a dynamic IPSec VPN Tunnel between Check Point VPN-1 SecureClient and Check Point Next Generation (NG) VPN-1/Firewall-1 to support Avaya Communication Manager and Avaya IP Softphone. Avaya S8500 Media Server and Avaya G650 Media Gateway are used in the Application Notes. The configuration can be used for other Avaya Media Servers (S8700, S8300) and Avaya Media Gateways (G600, G350, G700, MCC1, SCC1, and CMC1).
1. Introduction

Check Point VPN client software bundles two client products - SecuRemote and SecureClient. Users have the option to install either of them during the software installation. Even though both clients provide authentication and encryption for remote users, compared to the SecuRemote, the SecureClient provides the following additional functionality:

- Adding a personal firewall capability to the SecureClient (Desktop Security)
- Creating a virtual adapter on the client and receiving a virtual IP address from the Check Point VPN/Firewall (OfficeMode)
- Secure Configuration Verification

These Application Notes focus on a dynamic IPSec VPN Tunnel configuration between Check Point SecureClient and Check Point NG VPN/Firewall (Feature Pack 3) to carry VoIP traffic for Avaya Communication Manager and Avaya IP Softphone. The procedures needed to configure the SecureClient to work with VPN communities through IP NAT will also be covered. Refer to the appropriate administration documentation for Avaya Communication Manager and Avaya IP Softphone configuration. Avaya S8500 Media Server and Avaya G650 Media Gateway are used in the Application Notes. The configuration can be used for other Avaya Media Servers (S8700, S8300) and Avaya Media Gateways (G600, G350, G700, MCC1, SCC1, and CMC1). Figure 1 represents the sample network configuration for verification.
Note: An IP address pool 80.1.1.0 (OfficeMode Network) will be created on the Check Point Firewall for SecureClient to use. The IP addresses in Table 1 were used for the configuration shown in Figure 1.

<table>
<thead>
<tr>
<th>Device Name</th>
<th>IP Address</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Avaya S8500 Media Server with G650 Media Gateway</td>
<td>10.1.1.85</td>
<td>Default Gateway is 10.1.1.1</td>
</tr>
<tr>
<td>• IPSI</td>
<td>10.1.1.11</td>
<td></td>
</tr>
<tr>
<td>• C-Lan</td>
<td>10.1.1.12</td>
<td></td>
</tr>
<tr>
<td>• MedPro</td>
<td>10.1.1.13</td>
<td></td>
</tr>
<tr>
<td>Avaya IP Softphone PC 1</td>
<td>211.1.1.80</td>
<td>Default Gateway is 211.1.1.1</td>
</tr>
<tr>
<td>Avaya IP Softphone PC 2</td>
<td>211.1.1.81</td>
<td>Default Gateway is 211.1.1.1</td>
</tr>
<tr>
<td>Check Point NG VPN / Firewall</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Public</td>
<td>134.1.10.1</td>
<td>Default Gateway is 134.1.10.2</td>
</tr>
<tr>
<td>Private</td>
<td>10.1.1.50</td>
<td></td>
</tr>
<tr>
<td>Cisco 3745 FastEthernet0/0</td>
<td>134.1.10.2</td>
<td></td>
</tr>
<tr>
<td>T1</td>
<td>200.1.1.1</td>
<td></td>
</tr>
<tr>
<td>Cisco 2691 Fastether0/0 T1</td>
<td>211.1.1.1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>200.1.1.2</td>
<td></td>
</tr>
</tbody>
</table>
2. Equipment and Software Validated

Table 2 shows the software/firmware versions used during the verification:

<table>
<thead>
<tr>
<th>Devices</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Avaya S8500 Media Server with Avaya G650 Media Gateway</td>
<td>R012x.00.0.219.0</td>
</tr>
<tr>
<td>Avaya 4620 IP Telephone</td>
<td>1.81</td>
</tr>
<tr>
<td>Avaya IP Softphone</td>
<td>4.1.3.6</td>
</tr>
<tr>
<td>Check Point VPN-1 / Firewall-1</td>
<td>NG with FP 3</td>
</tr>
<tr>
<td>Check Point VPN-1 SecureClient NG with Application Intelligence</td>
<td>R54, Build number: 132</td>
</tr>
<tr>
<td>Cisco 3745 Router</td>
<td>IOS 12.2.(15T)</td>
</tr>
<tr>
<td>Cisco 2691 Router</td>
<td>IOS 12.3.(2T)</td>
</tr>
<tr>
<td>Cisco Catalyst 6509 Switch</td>
<td>Cat OS 7.5(1)</td>
</tr>
<tr>
<td>Cisco Catalyst 2948 Switch</td>
<td>IOS V.12.0 (25)W5(27)</td>
</tr>
</tbody>
</table>

3. Configure the Check Point NG VPN/Firewall

Launch the Check Point Configuration menu by selecting Start ➔ Programs ➔ Check Point SMART Clients ➔ SmartDashboard NG FP3. The main menu is displayed in Figure 2.
3.1. Create group and User for SecureClient

Since it is required to specify the user group under the Authentication branch when the Policy Server is selected, create a user group first.
• From the top menu bar of Figure 2, select Manage → Users → New → Group and create a new group (for example interop) as shown in Figure 3.

• Click OK

![Group Properties - interop](image)

Figure 3 Creating User Group

Follow the following steps to create a new user for SecureClient.

• Click Manage → Users and Administrators…
• Click button New… as shown in Figure 4
Figure 4: Creating New User

- Click the **General** tab, and Enter **user1** in the **Login Name** field and click **OK** as shown in Figure 5

![Figure 4: Creating New User](image)

Figure 5: Creating New User (Continued)

- Click the **Authentication** tab
- Select **VPN-1 & firewall-1 Password**
- Click **Enter Password...** as shown in Figure 6

![Figure 5: Creating New User (Continued)](image)
Enter **123456** as password
- Click **OK** as shown in **Figure 7**

![Figure 6: Configuring User Authentication](image)

**Figure 7: Configuring User Password**
- Click the **Encryption** tab
- Check **IKE** and click **Edit...** as shown in **Figure 8**
• Click **Authentication** tab in **Figure 9**
• Click **Password (Pre-shared secret)**: and enter **123456** in the **Password** field as shown in **Figure 9**
Figure 9: Configuring Password for User Authentication

- Click the **Encryption** tab
- Select **Defined in the Remote Access VPN page of the Global Properties window** as shown in Figure 10
- Click **OK**
• Click the Groups Tab
• Highlight the icon Interop and click the Add> button to add user1 to this group as shown in Figure 11
3.2. Create a New Policy for SecureClient

Create a new policy by selecting **File → New…** from **Figure 2** and providing the following information as shown in **Figure 12**.
• New Policy Package Name: remote
• Check Security and Address Translation
• Click Simplified mode
• Click Desktop Security
• Click OK

![New Policy Package](image)

Figure 12: Configure a New Policy

3.3. Configure Protected Network and OfficeMode Network (IP Pool)

3.3.1. Configure the Protected Network
The protected network is IP network 10.1.1.0 /24 as indicated in Figure 1. This network will be defined as an encryption domain behind the Check Point Firewall. The following configurations are applied to Figure 13.
• Select the **Network Objects** → **Networks** from the **Network Objects** tree in **Figure 2**
• Using the right mouse button, select **New Network**
• Create a Trusted Network by providing the following information:
  o Name **S8500-CM**
  o Network Address **10.1.1.0**
  o Net Mask **255.255.255.0**
  o Click the Broadcast address button **Included**
  o Click **OK**

![Network Properties - S8500-CM](image)

**Figure 13: Configuring Protected Network Property**

### 3.3.2. Configure OfficeMode Network (IP Pool for SecureClient)

The OfficeMode network is an IP address pool that the Check Point Firewall will use to push the IP address to the SecureClient during the VPN setup. Use the same procedures above to create an OfficeMode network. The 80.1.1.0 / 24 network is used for this configuration as shown in **Figure 14**.
Figure 14: Creating an IP Pool for SecuClient

**Note:** Do not make this network as part of the VPN encryption domain. The IP addresses from this pool are only used by SecuClients to communicate with the Check Point Gateway. The 10.1.1.0 network is the protected network, and must be in the VPN encryption domain.

- Click **OK** when done as shown in **Figure 14**.

### 3.4. Configure the Check Point Gateway

In these Application Notes, the Check Point Gateway Object is created with name **win2k-1**.

Follow the following steps to access the Check Point Gateway’s properties menu:

- Expand folder **Check Point ➔ win2k-1** from the **Network Objects** tree in **Figure 2**
• Double click on the Gateway Object **win2k-1**. The screen is displayed as shown in **Figure 15**.

Notice that the IP Address on the general tab is the external IP address of the gateway, this is important for OfficeMode. Also, make sure the **VPN-1 Pro** and **SecureClient Policy Server** products are checked under “Check Point Products”.

**Figure 15: Configuring Check Point Gateway Property**

Define the VPN domain as shown in **Figure 16**.

• Select **General Properties ➔ Topology**
• Click **Manually Defined** for VPN Domain and select **S8500-CM** as the trusted network.
• Click **OK**
Figure 16: Configuring VPN Domain

Select Remote Access to configure the OfficeMode properties as show in Figure 17.

- Click Offer Office Mode to group and use the drop-down button to select the Interop group
• Click Manual (using IP pool) and use the drop-down button to select Office-Mode-Network
• Click OK as shown in Figure 17

![Figure 17: Configuring Remote Access (OfficeMode)](image)

Select Authentication to configure authentication properties as shown in Figure 18.

• Check VPN-1 & Firewall-1 Password
- Select **Interop** in the **Users** field and click **OK**

**Figure 18: Configuring VPN Authentication Property**
3.5. Configure Remote Access Community (RAC)

The Check Point VPN/Firewall object needs to be configured as a member of the RAC. To do this, click on the **VPN Manager** tab in the SmartDashboard and double click the **RemoteAccess** icon to open the RAC property form as show in **Figure 19**.

![Figure 19: Configuring Remote Access Community](image-url)
• Add the gateway object **win2k-1** to the **Participating Gateways** window as shown in Figure 20.

**Figure 20: Adding the Gateway to Remote Access Community**
- Add the **Interop** group to the **Participating User Groups** as shown in **Figure 21**
- Click **OK**

**Figure 21: Adding User Group in Remote Access Community**
3.6. Configure the Rulebases

When using “Simplified Mode” policies, there is no Client Encrypt in the action column. There is no “Encrypt” action either. The encryption properties are configured via the community or under global properties. The rule sets for policy remote are created as shown in Figure 22.

Figure 22: Configuring Rules for SecureClient
As shown in Figure 23, click the Desktop Security-remote tab to configure the Inbound and Outbound Rules for SecureClient. The inbound rules control traffic going inbound to the client. The outbound rules control traffic originating from the client. With these defined inbound rules, the internal network is allowed to communicate to the users with encrypted traffic and all other traffic gets dropped. With these outbound rules, the remote users are allowed to communicate to the internal network with encrypted traffic and to go anywhere else without encryption.

Figure 23: Configuring Inbound and Outbound Rules

Note: Both the inbound and outbound rules defined in Figure 23 are pushed to the SecureClients once they are authenticated by the Check Point Firewall.

3.7. Configure Encryption Properties for Remote Access Users

The authentication and encryption parameters of the tunnel used between the SecureClient and the Check Point VPN/Firewall are presented below.

- Phase 1 Proposal (Define the Encryption and Authentication Algorithm for IKE):
  - Preshared Secret
  - Encryption Algorithm – 3DES
  - Authentication Algorithm – SHA1
  - Diffie-Hellman Group – 2
• Phase 2 Proposal (Define the Algorithm for data Encryption and Authentication):
  o No Compression
  o No Perfect Forward Secrecy
  o AH/ESP – ESP Trailer
  o Encryption Algorithm – 3DES
  o Authentication Algorithm – HMAC-SHA1

The encryption properties can be configured globally for all remote users. This is done under the Policy ➔ Global Properties ➔ Remote Access menu in the SmartDashboard as shown in Figure 24.
Configure **VPN – Basic** properties as shown in **Figure 25**.

---

**Figure 25: Configuring Basic VPN Property for SecureClient**
Configure **VPN – Advanced** properties as shown in **Figure 26**.

![VPN - Advanced Configuration](image)

**Figure 26: Configuring Advanced VPN Property for SecureClient**
4. Configure the Check Point VPN SecureClient
The following steps can be used to configure the SecureClient software.

4.1. SecureClient Site Configuration
Once the SecureClient software has been installed on the PC or laptop, a login site needs to be created. The configuration is shown in Figure 27.

- From the SecureClient window, click on Sites ➔ Create New… and enter the IP address 134.1.10.1 in the Name / IP: field as shown in Figure 27.
  **Note:** The IP address is the external IP address of the Check Point Firewall.
- Click OK

![Figure 27: Creating A New Site](image-url)
Figure 27: Create A New Site (Continued)

After clicking **OK** from Figure 27, the Authentication screen pops up as shown in Figure 28. Enter user name **user1** and password **123456** and click **OK**.

Figure 28: Authenticating User
4.2. Configure the SecureClient Mode to Support OfficeMode

Transparent Mode is selected as a default for the SecureClient. Since the OfficeMode is only supported in Connect Mode, the Client Mode needs to be changed to **Connect Mode**.

- Open **Tools** and select **Configure Client Mode...** as shown in **Figure 29**

![Figure 29: Configuring Client Mode](image)

- Select **Connect Mode** and click **OK** as shown in **Figure 30**
- Stop and restart the SecureClient application for this change to take effect

![Figure 30: Selecting Connect Mode](image)
After the SecureClient starts, click **Properties…** as shown in **Figure 31** to access the **Configure Connection Profile** screen as shown in **Figure 32**.

![VPN-1 SecureClient Connection](image)

**Figure 31: Accessing SecureClient Profile Configuration**
• Check the box **Logon to Policy Server**
• Check the box **Support Policy Server High Availability:**
• Click button **Advanced...** as shown in **Figure 32**

![Figure 32: Configuring SecureClient Profile](image-url)
Configure the OfficeMode and NAT support as shown in Figure 33.

- Check the box Support Office Mode
- Check the box Connectivity enhancements to configure the options for NAT traversal
- Click OK

![Advanced Settings dialog box]

**Figure 33: Configuring Office Mode and NAT Property**

### 5. Configure Port NAT (PNAT) on Cisco 2691 Router

This section describes how to configure the Cisco 2691 router as a PNAT device to translate IP addresses for IP Softphones. It also verifies that SecureClient can pass through PNAT and establish an IPSec Tunnel with the Check Point Firewall. The router is configured to perform Port NAT, translating the IP addresses from 211.1.1.0 (Private) to 200.1.1.10 (Public IP Address). In these Application Notes, both IP Softphones’ IP addresses are translated to 200.1.1.10. The PNAT configuration for the Cisco 2691 router is shown below:

```plaintext
interface FastEthernet0/0.5
  encapsulation dot1Q 5
  ip address 211.1.1.1 255.255.255.0
  ip nat inside --- enable NAT for private side

interface Serial0/0.1 point-to-point
  bandwidth 1540
  ip address 200.1.1.2 255.255.255.0
  ip nat outside --- enable NAT for public side
```
6. Verification Steps

- Use the SecureClient login status screen to show the client connection status as shown in Figure 34 and Figure 35.

Figure 34: SecureClient Connection Status
• Click the **Details** tab from Figure 34 to display the information shown in Figure 35.

**Note:** The client’s IP address is 211.1.1.81 and Assigned IP address is 80.1.1.3. In the NAT environment, the IP address 211.1.1.81 is translated to 200.1.1.10, however the assigned IP address 80.1.1.3 is unchanged. The IP address 80.1.1.3 is the address known to Communication Manager.

![VPN-1 SecureClient Connection Status](image)

**Figure 35: SecureClient Connection Details**
• Click the SecureClient Diagnostics link from Figure 34 to display the diagnostics information shown in Figures 36 and 37.

Figure 36: SecureClient Connection Status
The following verification steps are executed without PNAT.

- Launch both IP Softphones to log into the S8500 Media Server and verify both phones are registered with the S8500 Media Server.
- Make a call from IP Softphone 1 to IP Phone 1 and verify the voice quality.
- Make a call from IP Softphone 1 to IP Softphone 2 and verify the voice quality. (Note the IP direct is not supported because both IP Softphones are using IP addresses from IP Pool (80.1.1.0 network). These IP addresses are on public side of Check Point Gateway. There is no policy to encrypt traffic from same source to same destination.)
- Make a call from IP Softphone 1 to Digital phone 1 and conference IP Softphone 2 in. Verify that all three phones are in the conference and the voice quality is good.

The following verification steps are executed via PNAT.

- Enable NAT on router 2691 and repeat the four tests above. Verify that the PCs IP addresses have been NATed and the calls are successful.
• **Figures 38 – 40** show the login status of the IP Softphone 1 and the call status between IP Softphone 1 and IP phone 1 from the S8500 Server.

![Image of IP phone and software interface]

**Figure 38: Accessing Login Status from IP Softphone**

![Login Status dialog box]

**Figure 39: IP Software Login Status Detail**

**Note:** The Local IP Address used by the IP Softphone is 80.1.1.3, which is an address assigned by Office-Mode-Network (IP Pool).
Figure 40 shows the result of command **status station 30030** (IP Softphone 1) from the S8500 Media Server SAT.

![Figure 40: Station Status for IP Softphone 1](image)

7. Conclusion

With proper configuration, the Check Point SecureClient works with Avaya Communication Manager and Avaya IP Softphone in a NATed or non-NATed environment. Avaya S8500 Media Server and Avaya G650 Media Gateway are used in the Application Notes. The configuration can be used for other Avaya Media Servers (S8700, S8300) and Avaya Media Gateways (G600, G350, G700, MCC1, SCC1, and CMC1).