Abstract

These Application Notes describe the steps to configure the Check Point VPN-1 Power/UTM to support IPSec tunnel termination and Extended Authentication (XAUTH) authentication of the Avaya VPNremote Phone.
1. Introduction

These Application Notes describe the steps to configure the Check Point VPN-1 Power/UTM product to support IPSec tunnel termination and Extended Authentication (XAUTH) authentication of the Avaya VPNremote Phone.

The Avaya VPNremote Phone is a software based IPSec Virtual Private Network (VPN) client integrated into the firmware of an Avaya 4600 Series IP Telephone. This capability allows the Avaya IP Telephone to be plugged in and used over a secure IPSec VPN from any broadband Internet connection. End users experience the same IP telephone features as if they were using the telephone in the office. Avaya IP Telephone models supporting the Avaya VPNremote Phone firmware include the 4610SW, 4620SW, 4621SW, 4622SW and 4625SW.

Release 2 of the Avaya VPNremote Phone firmware, used in these Application Notes, extends the support of head-end VPN gateways to include the Check Point gateway. The configuration steps described in these Application Notes utilize a Check Point Secure Platform with VPN-1 Power/UTM product which from here on is generally referred to as Check Point.

The Avaya VPNremote Phone utilizes the Internet Key Exchange (IKE) protocol, XAUTH for IPSec tunnel establishment and authentication with the Check Point gateway. XAUTH allows security gateways to perform user authentication in a separate phase after the IKE authentication phase 1 exchange is complete. After user authentication is successful, the VPN router sends an IP address from a pre-configured IP Address to the Avaya VPNremote Phone.
1.1. Avaya VPNremote Phone Startup Events

The steps shown in Figure 1 below describe the high level events that take place during the startup of an Avaya VPNremote Phone. The focus of these Application Notes is on the configuration of the Avaya VPNremote Phone and the Check Point functioning as the IPSec VPN head-end.

1. Avaya VPNremote Phone establishes an IPSec VPN tunnel upon boot up with the designated IPSec VPN head-end.

2. Avaya VPNremote Phone initiates a TFTP, HTTP, or HTTPS session with the phone configuration file server for configuration file download. (46vpnuprgade.scr, 46vpnsettings.txt, 46xxsettings.txt)

3. Avaya VPNremote Phone registers with Avaya Communication Manager and is ready for service.

Figure 1: Avaya VPNremote Phone Startup Events
2. Network Topology

The sample network implemented for these Application Notes is shown in Figure 2. The Corporate IP Network location contains the Check Point Secure Platform functioning as perimeter security device and VPN head-end. The Avaya S8710 Servers and Avaya G650 Media Gateway are also located at the Corporate IP Network. The Corporate IP Network is mapped to IP Network Region 1 in Avaya Communication Manager.

The Avaya VPNremote Phones are located in the public network and configured to establish an IPSec tunnel to the Public IP address of the Check Point gateway. The Check Point gateway will assign IP addresses to the Avaya VPNremote Phones. The assigned IP addresses, also known as the inner addresses, will be used by the Avaya VPNremote Phones when communicating inside the IPSec tunnel and in the private corporate network to Avaya Communication Manager.

Avaya Communication Manager maps the Avaya VPNremote Phones to the appropriate IP Network Region using this inner IP address and applies the IP Network Region specific parameters to the Avaya VPNremote Phone. In these Application Notes, the G.729 codec with three 10ms voice samples per packet is assigned to the Avaya VPNremote Phones.

![Figure 2: Network Diagram](image)

©2007 Avaya Inc. All Rights Reserved.
3. Equipment and Software Validated

Table 1 lists the equipment and software/firmware versions used in the sample configuration provided.

<table>
<thead>
<tr>
<th>Equipment</th>
<th>Software Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Avaya S8710 Servers with Avaya G650 Media Gateway</td>
<td>Avaya Communication Manager 4.0.1 (R014x.00.1.731.2)</td>
</tr>
<tr>
<td>Avaya 4610SW IP Telephones</td>
<td>R2.3.2 – Release 2 (a10bVPN232_1.bin)</td>
</tr>
<tr>
<td>Check Point NGX Secure Platform with VPN-1 Power/UTM product</td>
<td>R65</td>
</tr>
<tr>
<td>Linksys BEFSR41v4</td>
<td>Firmware 1.04.05</td>
</tr>
</tbody>
</table>

Table 1 – Equipment Version Information

4. Check Point NGX Secure Platform Configuration

4.1. Log In and Global Setting

These Application Notes assume the Check Point gateway has been configured with basic IP connectivity and is connected to the network. The Check Point gateway depicted in Figure 2 has been configured with IP address 192.168.1.190 as its internal and management IP address. All configuration presented in these Application Notes are performed from the SmartDashboard application running on a management workstation (not shown in Figure 2).

1. From the Check Point management workstation, log into the SmartDashboard application using an appropriate User Name and Password.
2. Configure the Global Properties of the Check Point gateway. The Global Properties screen can be accessed via **Policy → Global Properties** in the top main menu as shown below.

![Global Properties Screen](image)

The IKE Phase 1 is set to use 3DES for encryption, MD5 for data integrity, and Diffie-Hellman Group 1 for hashing. A screen capture of these setting is shown below. Other encryption, authentication, and hashing algorithm are also supported by Avaya VPN remote Phones and may be used.

![VPN - IKE (Phase 1) Screen](image)
The IPSEC Phase 2 is set to use 3DES for encryption, and MD5 for data integrity. A screen capture of these settings is shown below.
4.2. Define Networks

1. Two networks (Avaya–Voip and VPN-phone_DHCP) are defined in the sample configuration. These networks are used to create firewall policy and IP address assignment of the Avaya VPNremote Phone. Below are the screen captures showing the Avaya-Voip and the VPN-phone_DHCP networks.
4.3. Define VPN User and Group

1. Each individual Avaya VPNremote phone is assigned a user name and password for the purpose of VPN authentication. As a way to facilitate the identification of an Avaya VPNremote phone user, the sample network uses the phone extension number and the user name as a VPN user ID. For example the user ID 50015-andy is for Avaya VPNremote phone with extension 50015 for user andy.

2. Below are screen captures showing the properties for the user 50015-andy that have been changed. All fields that are not shown are left at their default setting. Each Avaya VPNremote phone user must be defined in Check Point gateway.
3. A group called Avaya-voip is used to logically group all Avaya VPN remote phone users together within Check Point gateway. Make sure all AvayaVPN remote phone user IDs are assigned to this group.

4.4. Configure Check Point VPN

1. Configure additional firewall specific settings by double clicking on the desire firewall in the left menu. A Check Point Host window as shown in Step 2 will be displayed. voip-fw is the name of the Check Point VPN-1 Power/UTM gateway used in our sample network.
2. Make sure the **VPN** product is selected for the firewall.

3. The **Default_Protection** profile is used as the **SmartDefense** profile in the sample network.
4. Make sure the RemoteAccess VPN Community is selected to participate in VPN.

5. Select the firewall’s external interface IP address for the **Selected address from topology table**. For the sample network the external interface IP is 140.2.2.2
6. Check the **Allow SecureClient to route traffic through this gateway** option. This option will instruct the VPN client to send all outbound traffic through the tunnel to this firewall.
7. Select **Offer Office Mode to group** for the **Avaya-voip** group created in **Section 4.2, Step 1** and select to use **Manual (using IP pool)** using the **VPN-phone_DHCP** network defined in **Section 4.2, Step 1**.

8. Make sure **Check Point Password** is selected under the Enabled Authentication Schemes.
4.5. Configure Check Point Security Policy

1. The following screen captures show the security policy defined in Check Point for the VPNremote phone and the Avaya_RTP service. The policy is designed to allow any IP address belonging to the VPN-phone_DHCP network to any address for Avaya_RTP, H323-any, and H323_ras services to pass through. Both the H323_any and H323-ras services are pre-defined services within Check Point. The Avaya_RTP service is defined as any UDP traffic between ports 2048-2999.

<table>
<thead>
<tr>
<th>No</th>
<th>NAME</th>
<th>SOURCE</th>
<th>DESTINATION</th>
<th>VPN</th>
<th>SERVICE</th>
<th>ACTION</th>
<th>TRACK</th>
<th>INSTALL ON</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Avaya VPNremote phone</td>
<td>Any</td>
<td>Any</td>
<td>Any Traffic</td>
<td>Any</td>
<td>accept</td>
<td>None</td>
<td>Policy Targets</td>
</tr>
<tr>
<td>2</td>
<td></td>
<td>VPN-phone_DHCP</td>
<td>Any</td>
<td>Any</td>
<td>Any Traffic</td>
<td>H323_any</td>
<td>accept</td>
<td>Log</td>
</tr>
<tr>
<td>3</td>
<td></td>
<td>Any</td>
<td>Any</td>
<td>Any Traffic</td>
<td>Any</td>
<td>drop</td>
<td>None</td>
<td>Policy Targets</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. Refer to [1] and [2] 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 1, 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 a TFTP/HTTP/HTTPS server or locally on the phone. These Application Notes utilize the local phone configuration method. Refer to [1] and [2] for details on a 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 telephone screen as shown below.

      ![DHCP * to program]

      When the * key is pressed, several configuration parameters are presented such as the phone’s IP Address, the Call Server’s 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, e.g., 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 to enter the VPN Options menu.
2. The VPN configuration options menu is displayed. For detailed description of each VPN configuration option, refer to [1] and [2].

The configuration values of one of the VPN remote Phones used in the sample configuration are shown in Table 2 below.

**Note:** The values entered below are case sensitive.

Press the ► hard button on the telephone to access the next screen of configuration options. Phone models with larger displays (e.g., 4621SW) will present more configuration options per page.

<table>
<thead>
<tr>
<th>Configuration Options</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server:</td>
<td>140.2.2.2</td>
<td>IP address of the Check Point external interface.</td>
</tr>
<tr>
<td>User Name:</td>
<td>50017-sherman</td>
<td>User created in Section 4.3.</td>
</tr>
<tr>
<td>Password:</td>
<td>********</td>
<td>Must match user password entered in Section 4.3.</td>
</tr>
<tr>
<td>Password Type:</td>
<td>Save in Flash</td>
<td>User is not prompted at phone boot up.</td>
</tr>
<tr>
<td>VPN Start Mode:</td>
<td>BOOT</td>
<td>IPSec tunnel dynamically starts on Phone power up.</td>
</tr>
<tr>
<td>IKE Over TCP</td>
<td>Auto</td>
<td></td>
</tr>
<tr>
<td>Encapsulation</td>
<td>4500-4500</td>
<td>This default value enables NAT traversal.</td>
</tr>
<tr>
<td>Syslog Server:</td>
<td>-</td>
<td>Server used for logging. Default is blank.</td>
</tr>
<tr>
<td>IKE Parameters:</td>
<td>DH1-3DES-MD5</td>
<td>Must match Security Association (SA) proposals from Section 4.1, Step 2.</td>
</tr>
<tr>
<td>IKE ID Type:</td>
<td>KEY-ID</td>
<td></td>
</tr>
<tr>
<td>Diffie-Hellman Grp</td>
<td>1</td>
<td>Can be set to “Detect” to accept VPN Concentrator settings (in this configuration, the Check Point firewall).</td>
</tr>
<tr>
<td>Encryption Alg:</td>
<td>3DES</td>
<td>Can be set to “Any” to accept VPN Concentrator settings.</td>
</tr>
<tr>
<td>Authentication Alg:</td>
<td>MD5</td>
<td>Can be set to “Any” to accept VPN Concentrator settings.</td>
</tr>
<tr>
<td>IKE Xchg Mode:</td>
<td>Identity Protected</td>
<td></td>
</tr>
<tr>
<td>IKE Config Mode:</td>
<td>Enable</td>
<td></td>
</tr>
<tr>
<td><strong>Configuration Options</strong></td>
<td><strong>Value</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>-----------------</td>
<td>---------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>IPSec Parameters:</td>
<td>DH1-3DES-MD5</td>
<td>Must match SA proposals from <a href="#">Section 4.1, Step 2</a>.</td>
</tr>
<tr>
<td>Encryption Alg:</td>
<td>3DES</td>
<td>Can be set to “Any” to accept VPN Concentrator settings.</td>
</tr>
<tr>
<td>Authentication Alg:</td>
<td>MD5</td>
<td>Can be set to “Any” to accept VPN Concentrator settings.</td>
</tr>
<tr>
<td>Diffie-Hellman Grp</td>
<td>1</td>
<td>Can be set to “Detect” to accept VPN Concentrator settings.</td>
</tr>
<tr>
<td>Protected Net:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remote Net #1:</td>
<td>0.0.0.0/0</td>
<td>Access to all private nets.</td>
</tr>
<tr>
<td>Connectivity Check:</td>
<td>First Time</td>
<td>Test initial IPSec connectivity.</td>
</tr>
<tr>
<td>Copy TOS:</td>
<td>Yes</td>
<td>Maintain phone Type Of Service (TOS) setting on Corporate Network for QoS.</td>
</tr>
<tr>
<td>QTest</td>
<td>Enable</td>
<td>Can be either “Enable” or “Disable” to allow user access to QTest feature.</td>
</tr>
</tbody>
</table>

Table 2 – VPNremote Phone Configuration
1. The VPNremote Phone can interoperate with several VPN head-end vendors. The VPNremote Phone must be told which VPN head-end vendor will be used so the appropriate protocol dialogs can take place. This is done by setting the **VPN Configuration Profile** on the VPNremote Phone.

Press the **Profile** soft button at the bottom of the VPNremote Phones display while in the VPN Options mode. The **VPN Configuration Profile** options, shown below, are displayed. If a Profile other than Cisco is already chosen, press the **Modify** soft button to display the following list:

- Avaya Security Gateway
- Cisco Xauth with Certs
  - 
  - 
  - Checkpoint
- Juniper Xauth with Certs

Press the button aligned with the **Checkpoint** profile option. Then press the **Done** soft button.

When all VPN configuration options have been set, press the **Done** soft button. The following is displayed. Press # to save the configuration and reboot the phone.

```
Save new values ?
*=no  #=yes
```

6. **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 already been completed.

As shown in **Figure 2**, Avaya VPNremote Phones are assigned to IP Network Region 5 using ip-network-map in Avaya Communication Manager based on IP address range of the VPN Concentrator IP Address Pool. IP Network Region 5 is then assigned to a codec set configured with the G.729 codec. The Corporate IP Network is assigned to IP Network Region 1 using the G.711 codec.

6.1. **VPNremote Phone Administration**

An Avaya VPNremote Phone is administered the same as other H.323 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 H.323 Avaya IP telephones located locally on the corporate LAN once the VPN tunnel has been established.
For additional information regarding the administration of Avaya Communication Manager, refer to [3].

6.2. IP Codec Sets Configuration
Use the `change ip-codec-set n` command to configure IP Codec Set parameters where n is the IP Codec Set number. Configure the highlighted fields shown below. All remaining fields can be left at the default values.

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

```
change ip-codec-set 1

IP Codec Set
Codec Set: 1

Audio Codec  Silence Suppression  Frames Per Pkt  Packet Size(ms)
1: G.711MU     n         2        20
```

2. Use the `change ip-codec-set 2` command to define a codec set for the G.729 (30ms) codec as shown below.

```
change ip-codec-set 2

IP Codec Set
Codec Set: 2

Audio Codec  Silence Suppression  Frames Per Pkt  Packet Size(ms)
1: G.729      n         3        30
```
3. Use the list ip-codec-set command to verify the codec assignments.

```
list ip-codec-set

IP CODEC SETS
Codec  Codec 1     Codec 2     Codec 3     Codec 4     Codec 5
Set
  1    G.711MU
  2    G.729
  3
  4
```

6.3. IP Network Map Configuration

Use the change ip-network-map command to define the IP address to Network Region mapping for VPNremote Phones.

```
change ip-network-map

IP ADDRESS MAPPING

From IP Address  (To IP Address or Mask)  Region  VLAN  Extension
10.10.10.01 10.10.10.254 24 5 n
. . . . . . . . 24 5 n
. . . . . . . . 24 5 n
. . . . . . . . 24 5 n
```
6.4. IP Network Regions Configuration

Use the `change ip-network-region n` command to configure IP Network Region parameters where n is the IP Network Region number. Configure the highlighted fields shown below. All remaining fields can be left at the default values.

**Intra-region IP-IP Direct Audio** and **Inter-region IP-IP Direct Audio** determine the flow of RTP audio packets. Setting these fields to “yes” enables the most efficient audio path to be taken. **Codec Set 1** is used for IP Network Region 1 as described in **Section 6.2**.

![IP Network Region Configuration](image)

Page 3 of the IP-Network-Region form, shown below, defines the codec set to use for intra-region and inter-region calls. Avaya VPNremote Phones are mapped to Region 5. Calls within IP Network Region 1 use Codec Set 1 (G.711MU) while calls between IP Network Region 1 and IP Network Region 5 use Codec Set 2 (G.729).

![IP Network Region Configuration](image)
Use the `change ip-network-region 5` command to configure IP Network Region 5 parameters. Configure the highlighted fields shown below. All remaining fields can be left at the default values.

<table>
<thead>
<tr>
<th>change ip-network-region 5</th>
<th>Page 1 of 19</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Region:</strong> 5</td>
<td></td>
</tr>
<tr>
<td>Location:</td>
<td>Authoritative Domain:</td>
</tr>
<tr>
<td><strong>Name:</strong> VPNphones-CheckPoint</td>
<td></td>
</tr>
<tr>
<td>MEDIA PARAMETERS</td>
<td></td>
</tr>
<tr>
<td><strong>Codec Set:</strong> 2</td>
<td>Intra-region IP-IP Direct Audio: yes</td>
</tr>
<tr>
<td>UDP Port Min: 2048</td>
<td>Inter-region IP-IP Direct Audio: yes</td>
</tr>
<tr>
<td>UDP Port Max: 3028</td>
<td>IP Audio Hairpinning? y</td>
</tr>
</tbody>
</table>

Page 3 defines the codec set to use for intra-region and inter-region calls. Avaya VPNremote Phones are mapped to Region 5. Calls within IP Network Region 5, i.e., a VPNremote Phone calling another VPNremote Phone, use Codec Set 2 (G.729). Calls between IP Network Region 5 and IP Network Region 1 will also use Codec Set 2 (G.729).

<table>
<thead>
<tr>
<th>change ip-network-region 5</th>
<th>Page 3 of 19</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Inter Network Region Connection Management</strong></td>
<td></td>
</tr>
<tr>
<td>src</td>
<td>dst</td>
</tr>
<tr>
<td>-----</td>
<td>-----</td>
</tr>
<tr>
<td>5</td>
<td>1</td>
</tr>
<tr>
<td>5</td>
<td>2</td>
</tr>
<tr>
<td>5</td>
<td>3</td>
</tr>
<tr>
<td>5</td>
<td>4</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
</tr>
</tbody>
</table>
7. Verification

7.1. VPNremote Phone IPSec Statistics

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 (with √ icon). From the telephone keypad, press the ► hard button until the VPN Status… option appears. Select VPN Status… The VPN statistics of the active IPSec tunnel will be displayed. Use the ► hard button to access the next screen. Press the Refresh soft button to update the displayed statistics.

The list below shows the statistics from the VPNremote phone used in the sample configuration.

<table>
<thead>
<tr>
<th>VPN Status…</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>PKT S/R</td>
<td>47/39</td>
</tr>
<tr>
<td>FRAG RCVD</td>
<td>0</td>
</tr>
<tr>
<td>Comp/Decomp</td>
<td>0/0</td>
</tr>
<tr>
<td>Auth Failures</td>
<td>0</td>
</tr>
<tr>
<td>Recv Errors</td>
<td>0</td>
</tr>
<tr>
<td>Send Errors</td>
<td>0</td>
</tr>
<tr>
<td>Gateway</td>
<td>140.2.2.2</td>
</tr>
<tr>
<td>Outer IP</td>
<td>192.168.2.204</td>
</tr>
<tr>
<td>Inner IP</td>
<td>10.10.10.4</td>
</tr>
<tr>
<td>Gateway Version</td>
<td>UNKNOWN</td>
</tr>
<tr>
<td>Inactivity</td>
<td>0</td>
</tr>
<tr>
<td>Timeout</td>
<td></td>
</tr>
<tr>
<td>DH1-3DES-MD5-60 mins</td>
<td></td>
</tr>
</tbody>
</table>
7.2. Check Point Logging

The active VPN sessions to Check Point can be viewed by initiating the SmartView Tracker program from the management workstation.

1. The following screen capture shows a successful connection of a VPN remote phone onto Check Point. Log entries 2-7 show an IPSec tunnel negotiated for the VPN remote phone user 50017-sherman and log entries 8-9 show the VPN remote phone registering with Avaya Communication Manager.

2. The following screen capture shows the log entries of a call being established between 50017-sherman and 50015-andy. Notice that media traffic is shuffled between the two VPN remote phones in log entry 7.

3. The screen capture below shows the log of a conference call initiated from 50017-sherman to 50015-andy and 50016-rich.
8. Troubleshooting

This section offers some common configuration mismatches between the VPN remote Phone and the VPN Concentrator to assist in troubleshooting. The key events of the logs are highlighted in bold.

8.1. Incorrect User Name

- **VPN remote Phone display:**
  Initial display shows the following:
  
  Enter Username and Password
  
  After a short period of time with no input (5 minutes), the display shows the following:
  
  IKE Phase 1 no response

Press the **More** soft button to display the following:

Invalid password OR user name

Error Code: 3997698:0

Module: IDEDcfg:430

- **VPN Router Event Log:**

![Record Details](image)
8.2. Incorrect User Password

- VPNremote Phone display:
  Initial display shows the following:

After a short period of time with no input (5 minutes), the display shows the following:
Invalid PSK or Group Password

Press the More soft button to display the following:
Invalid password OR user name
Error Code: 3997698:0
Module:IDECFG:430

- VPN Router Event Log:
8.3. Mismatched Phase 1 Proposal

- **VPNremote Phone display:**

  IKE Phase1 no response

  Press the **More** soft button to display the following:
  
  Error Code: 3997700:0  
  Module:IDMPD:142

  Press the **Next** soft button to display the following:
  
  Error Code: 3997700:0  
  Module:IDMPD:459

- **VPN Router Event Log:**

  ![Record Details]

  Number: 34
  Date: 31Aug2007
  Time: 14:21:30
  Product: VPN-1 Power/UTM
  Interface: daemon
  Origin: voip-fw
  Type: Log
  Action: Reject
  Protocol: 
  Source: 100.2.2.32
  Destination: voip-fw
  Rule: 
  User: 
  Information: IKE: Main Mode Failed to match proposal: Transform: 3DES, MD5, Group 2 (1024 bit)
  Reason: Wrong value for: Encryption Algorithm
  Encryption Scheme: IKE
  IKE Initiator Cookie: 924af75a7b32e49
  Reject Reason: IKE failure
  Subproduct: VPN
  VPN Feature: IKE
  VPN Peer Gateway: 100.2.2.32
8.4. Mismatched Phase 2 Proposal

- **VPN Remote Phone display:**
  
  IKE Phase 2 no response

  Press the **More** soft button to display the following:
  
  IKE Phase1 send notify
  Error Code: 39977698:14
  Module: NOTIFY:444

  Press the **Next** soft button to display the following:
  
  IKE Phase2 no response
  Error Code: 39977000:0
  Module: IKECFG:1184

- **VPN Router Event Log:** (some non-relevant log entries removed for brevity)

![Record Details](image-url)
### No IP Pool Addresses Available

- **VPNremote Phone display:**
  
  ![VPN remote phone display](image)

- **VPN Router Event Log:**

  ![VPN router event log](image)

<table>
<thead>
<tr>
<th>Number</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date</td>
<td>31Aug2007</td>
</tr>
<tr>
<td>Time</td>
<td>14:51:43</td>
</tr>
<tr>
<td>Product</td>
<td>VPN-1 Power/UTM</td>
</tr>
<tr>
<td>Interface</td>
<td>voip-fw</td>
</tr>
<tr>
<td>Type</td>
<td>Log</td>
</tr>
<tr>
<td>Action</td>
<td>Reject</td>
</tr>
<tr>
<td>Source</td>
<td>100.2.2.32</td>
</tr>
<tr>
<td>Destination</td>
<td></td>
</tr>
<tr>
<td>Rule</td>
<td></td>
</tr>
<tr>
<td>User</td>
<td>50017-sherman</td>
</tr>
</tbody>
</table>
| Information | MAC: 00-04-0D-E4-37-79  
OM: -IP pool full  
om_method: IP pools |
| Encryption Scheme | IKE |
| Reject Reason | IKE failure |
| Subproduct | VPN |
| VPN Feature | OfficeMode |

![Record Details](image)
8.6. Graceful Reboot of VPNremote Phone

- VPNremote Phone display:
  
  Rebooting...

- VPN Router Event Log:

  ![Record Details]

  ![Record Details]
9. Conclusion
The Avaya VPNNremote Phone combined with Check Point VPN-1 Power/UTM gateway provides a secure solution for remote worker telephony over any broadband Internet connection. The Avaya VPNNremote Phone XAUTH implementation for Check Point VPN-1 Power/UTM demonstrated successful interoperability with the Check Point NGX.

10. References

Avaya Application Notes and Resources Web Site:

Avaya Product Support Web Site:
http://support.avaya.com/japple/css/japple?PAGE=Home


Check Point Product Support Web Site:
http://www.checkpoint.com/support/technical/documents


