# Important Information

## Check Point R80
For more about this release, see the R80 home page

## Latest Version of this Document
Download the latest version of this document

To learn more, visit the Check Point Support Center

## Feedback
Check Point is engaged in a continuous effort to improve its documentation.

Please help us by sending your comments
mailto:cp_techpub_feedback@checkpoint.com?subject=Feedback on VPN Pre-R80 Security Gateways with R80 Security Management Administration Guide.

## Searching in Multiple PDFs
To search for text in all the R80 PDF documents, download and extract the complete R80 documentation package

Use **Shift-Control-F** in Adobe Reader or Foxit reader.

To search for all text in the R77 PDF documents, download and extract the R77 documentation package

## Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>31 March 2016</td>
<td>First release of this document</td>
</tr>
</tbody>
</table>
About this Guide

In This Section:
R80 SmartConsole Toolbars ................................................................. 6

This guide explains how to manage backward compatible (R77.xx and lower) Security Gateways with the R80 SmartConsole.

This guide shows only the updated procedures. To learn more about earlier features, see the R77 documentation http://supportcontent.checkpoint.com/documentation_download?ID=26770.

R80 SmartConsole Toolbars

Global Toolbar (top left of R80 SmartConsole)

<table>
<thead>
<tr>
<th>Description and Keyboard Shortcut</th>
</tr>
</thead>
<tbody>
<tr>
<td>The main R80 SmartConsole Menu</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>The Objects menu.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Also leads to the Object Explorer Ctrl+E</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Install policy on managed gateways</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ctrl+Shift+Enter</td>
</tr>
</tbody>
</table>

Navigation Toolbar (left side of R80 SmartConsole)

<table>
<thead>
<tr>
<th>Description and Keyboard Shortcut</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gateway configuration view</td>
</tr>
<tr>
<td>Ctrl+1</td>
</tr>
</tbody>
</table>

| Security Policies Access Control view |
| Security Policies Threat Prevention view |
| Ctrl+2 |

<table>
<thead>
<tr>
<th>Logs &amp; Monitor view</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ctrl+3</td>
</tr>
</tbody>
</table>

| Manage & Settings view - review and configure the Security Management Server settings |
| Ctrl+4 |
### Command Line Interface Button (left bottom corner of R80 SmartConsole)

<table>
<thead>
<tr>
<th>Description and Keyboard Shortcut</th>
</tr>
</thead>
</table>
| Open a command line interface for management scripting and API
| F9 |

### What's New Button (left bottom corner of R80 SmartConsole)

<table>
<thead>
<tr>
<th>Description and Keyboard Shortcut</th>
</tr>
</thead>
<tbody>
<tr>
<td>Open a tour of the R80 SmartConsole</td>
</tr>
</tbody>
</table>

### Objects and Validations Tabs (right side of R80 SmartConsole)

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Objects</td>
</tr>
<tr>
<td>Validations</td>
</tr>
</tbody>
</table>

#### Objects
- Manage security and network objects

#### Validations
- Validation warnings and errors

### System Information Area (bottom of R80 SmartConsole)

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Task List</td>
</tr>
<tr>
<td>Server Details</td>
</tr>
<tr>
<td>Connected Users</td>
</tr>
</tbody>
</table>

#### Task List
- Management activities, such as policy installation tasks

#### Server Details
- The IP address of the Security Management Server

#### Connected Users
- The administrators that are connected to the Security Management Server
Introduction to VPN

In This Section:

- Migrating from Traditional Mode to Simplified Mode ................................................... 8
- Configuring a Meshed Community Between Internally Managed Gateways ............................. 8
- Configuring a Star VPN Community ..................................................................................... 9
- Confirming a VPN Tunnel Successfully Opens ......................................................................... 10
- VPN with External Security Gateways Using Certificates .................................................... 10
- VPN with External Security Gateways Using Pre-Shared Secret ........................................... 11
- Authorizing Firewall Control Connections in VPN Communities ............................................ 12

Migrating from Traditional Mode to Simplified Mode

To migrate from Traditional Mode VPN to Simplified Mode:

1. On the Global Properties > VPN page, select one of these options:
   - Simplified mode to all new Firewall Policies
   - Traditional or Simplified per new Firewall Policy
2. Click OK.
3. From the R80 SmartConsole Menu, select Manage policies.
   The Manage Policies window opens.
4. Click New.
   The New Policy window opens.
5. Give a name to the new policy and select Access Control.
   In the Security Policy Rule Base, a new column marked VPN shows and the Encrypt option is no longer available in the Action column. You are now working in Simplified Mode.

Configuring a Meshed Community Between Internally Managed Gateways

To configure an internally managed VPN meshed community:

1. Install and configure the Security Gateways.
2. In R80 SmartConsole, double click on the Security Gateway object.
3. In the General Properties page:
   a) Enter the gateway Name.
   b) Enter the IPv4 Address or IPv6 Address (or both).
   c) In the Network Security tab, Select IPsec VPN.
   d) Click Communication and establish trusted communication with the Gateway.
4. In the **Network Management** page, click **Get Interfaces**.
   a) After the interfaces show in the table, click **Edit** to open the **Interface** window.
   b) In the **Interface** window, define the general properties of the interface and the topology of the network behind it.

5. In the **Network Management** > **VPN Domain** page, define the VPN domain one of:
   - **All IP Addresses behind the Gateway based on Topology information**
   - **Manually defined** as an address range, a network, or a group that can be a combination of address ranges, networks, and even other groups.

   (In a primary backup MEP configuration, leave the backup encryption domain empty.)

   The network Security Gateway objects are now configured, and need to be added to a VPN community.

   **Note** - There is nothing to configure on the **IPsec VPN** page, regarding certificates, because internally managed Security Gateways automatically receive a certificate from the internal CA.

6. Open the **Object Explorer** (Ctrl+E), and select **VPN Communities**.
   a) Click **New** > **VPN Communities** > **Meshed Community**.
      The **New Meshed Community** window opens.
   b) In the **Encrypted Traffic** page, select **Accept all encrypted traffic** if you need all traffic between the Security Gateways to be encrypted. If not, then create appropriate rules in the Security Policy Rule Base that allows encrypted traffic between community members (step 7).
   c) On the **Gateways** page, add the Security Gateways created in step 1.

   A VPN tunnel is now configured.

   You can also configure these options: **Encryption**, **Shared Secret**, and **Advanced**.

7. If you did not select **Accept all encrypted traffic** in the **Encrypted Traffic** page of the Community, build an access control policy, for example:

```
<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>VPN</th>
<th>Services &amp; Applications</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>Any</td>
<td>Meshed community</td>
<td>Any</td>
<td>Accept</td>
</tr>
</tbody>
</table>
```

   Where "Meshed community" is the VPN community you have just defined.

### Configuring a Star VPN Community

A star VPN community is configured in much the same way as a meshed community, the difference being the options on the **Star Community** window:

- On the **VPN Routing** page - Select **To center only**.
- On the Gateways page:
  - **Central Gateways** - Add the central Security Gateways.
  - **Central Gateways** - Select **Mesh central Security Gateways** if you want the central Security Gateways to communicate.
  - **Satellite Gateways** - Add the satellite Security Gateways.
Confirming a VPN Tunnel Successfully Opens

To make sure that a VPN tunnel has successfully opened:

1. Edit the VPN rule and Select Log as the Track option.
2. Open Logs & Monitor and click a new tab.
3. From the bottom of the window, click Tunnel and User Monitoring. Check Point SmartView Monitor opens.
4. Click the gateway to see IPsec VPN traffic and tunnels opened. A successful connection shows encrypt, decrypt and key install logs.

Alternatively, search for VPN in R80 SmartConsole to see the relevant logs:

1. Open SmartView Monitor and see that VPN tunnels are up.

VPN with External Security Gateways Using Certificates

To configure VPN using certificates, with the external Security Gateways as satellites in a star VPN Community:

1. Obtain the certificate of the CA that issued the certificate for the peer VPN Security Gateways, from the peer administrator. If the peer Security Gateway is using the ICA, you can obtain the CA certificate using a web browser from:

   http://<IP address of peer Security Gateway or Management Server>:18264

2. In R80 SmartConsole, define the CA object for the CA that issued the certificate for the peer (see “Enrolling with a Certificate Authority” on page 16).
3. Define the CA that will issue certificates for your side if the Certificate issued by ICA is not appropriate for the required VPN tunnel.

You may have to export the CA certificate and supply it to the peer administrator.

4. Define the Network Object(s) of the Security Gateway(s) that are internally managed. In particular, be sure to do the following:
   - In the General Properties page of the Security Gateway object, select IPsec VPN.
   - In the Network Management page, define the Topology.
   - In the VPN Domain page, define the VPN Domain. If it does not contain all the IP addresses behind the Security Gateway, define the VPN domain manually by defining a group or network of machines and setting them as the VPN Domain.

5. If the ICA certificate is not appropriate for this VPN tunnel, then in the IPsec VPN page, generate a certificate from the relevant CA (see “Enrolling with a Certificate Authority” on page 16).

6. Define the Network Object(s) of the externally managed Security Gateway(s).
   - If it is not a Check Point Security Gateway, define an Interoperable Device: In Object Explorer click New > Network Object > More > Interoperable Device.
   - If it is a Check Point Security Gateway, define an Externally Managed VPN Gateway: In Object Explorer, click New > Network Object > Gateways and Servers > More > Externally Managed VPN Gateway.
7. Set the various attributes of the peer Security Gateway. In particular, be sure to do the following:
   - For an Externally Managed Check Point Security Gateway: In the General Properties page of the Security Gateway object, select IPsec VPN.
   - Define the Topology.
   - Define the VPN Domain using the VPN Domain information obtained from the peer administrator. If the VPN Domain does not contain all the IP addresses behind the Security Gateway, define the VPN domain manually by defining a group or network of machines and setting them as the VPN Domain.
   - For an Externally Managed Check Point Security Gateway: In the IPsec VPN page, define the Matching Criteria. Specify that the peer must present a certificate signed by its own CA. If feasible, enforce details that appear in the certificate as well.

8. Define the Community.

   These details assume that a Star Community is used, but you can also use a Meshed Community. If you are working with a Meshed community, ignore the difference between the Central Security Gateways and the Satellite Security Gateways.
   - Agree with the peer administrator about the various IKE properties and set them in the Encryption page and the Advanced page of the community object.
   - Define the Central Security Gateways. These are usually the internally managed ones. If no other Community is defined for them, decide whether or not to mesh the central Security Gateways. If they are already in a Community, do not mesh the central Security Gateways.
   - Define the Satellite Security Gateways. These are usually the external ones.

9. Click OK and publish the changes.

10. Define the relevant access rules in the Security Policy.

11. Add the Community in the VPN column, the services in the Service & Applications column, the desired Action, and the appropriate Track option.

12. Install the Access Control Policy.

VPN with External Security Gateways Using Pre-Shared Secret

The configuration instructions require an understanding of how to build a VPN (see “Introduction to VPN” on page 8).

To configure a VPN using pre-shared secrets, with the external Security Gateways as satellites in a star VPN Community:

1. Define the Network Object(s) of the Security Gateways that are internally managed. In particular, be sure to:
   - In the General Properties page of the Security Gateway object, in the Network Security tab, select IPsec VPN.
   - In the Network Management page, define the Topology.
   - In the Network Management > VPN Domain page, define the VPN Domain. If it does not contain all the IP addresses behind the Security Gateway, define the VPN domain manually by defining a group or network of machines and setting them as the VPN Domain.
2. Define the Network Object(s) of the externally managed Security Gateway(s).
   • If it is not a Check Point Security Gateway, define an Interoperable Device: In Object Explorer click New > Network Object > More > Interoperable Device.
   • If it is a Check Point Security Gateway, define an Externally Managed VPN Gateway: In Object Explorer, click New > Network Object > Gateways and Servers > More > Externally Managed VPN Gateway.

3. Set the various attributes of the peer Security Gateway. In particular, make sure to configure:
   • In the Topology page, define the Topology and the VPN Domain using the VPN Domain information obtained from the peer administrator.
   • If the VPN Domain does not contain all the IP addresses behind the Security Gateway, define the VPN domain manually by defining a group or network of machines and setting them as the VPN Domain.

4. Define the Community.
   The following details assume that a Star Community was chosen, but a Meshed Community is an option as well. If you are working with a Mesh community, ignore the difference between the Central Security Gateways and the Satellite Security Gateways.
   • Agree with the peer administrator about the various IKE properties and set them in the Encryption page and the Advanced page of the community object.
   • Define the Central Security Gateways. These will usually be the internally managed ones. If there is no another Community defined for them, decide whether or not to mesh the central Security Gateways. If they are already in a Community, do not mesh the central Security Gateways.
   • Define the Satellite Security Gateways. These will usually be the external ones.

5. Publish the changes.

6. Agree on a pre-shared secret with the administrator of the external Community members. Then, in the Shared Secret page of the community, select Use only Shared Secret for all external members. For each external peer, enter the pre-shared secret.

7. Define the relevant access rules in the Access Control Policy. Add the Community in the VPN column, the services in the Services & Applications column, the desired Action, and the appropriate Track option.

8. Install the Security Policy.

Authorizing Firewall Control Connections in VPN Communities

Check Point Nodes communicate with other Check Point Nodes by means of control connections. For example, a control connection is used when the Security Policy is installed from the Security Management Server to a Security Gateway. Also, logs are sent from Security Gateways to the Security Management Server across control connections. Control connections use Secure Internal Communication (SIC).

Control connections are allowed using Implied Rules in the Access Control Rule Base. Implied Rules are added to or removed from the Access Control Rule Base, by selecting or clearing options in the Firewall page of the R80 SmartConsole Global Properties.
Multiple Entry Point for Site to Site VPN

In This Section:
- Configuring Explicit MEP ................................................................. 13
- Configuring Implicit First to Respond ............................................. 13
- Routing Return Packets .................................................................. 15
- Configuring IP Pool NAT ................................................................. 15

Configuring Explicit MEP

Explicit MEP is only available in Site-to-Site Star VPN communities where multiple central Security Gateways are defined.

To configure MEP:
1. Open the Star Community object and go to the MEP page.
2. Select Enable center gateways as MEP.
3. Select an entry point mechanism:
   - First to respond
   - By VPN domain
   - Random selection
   - Manual priority list
   If you select By VPN domain or Manually set priority list, in the Advanced, section choose First to respond or Random selection to resolve how more than one Security Gateway with equal priority should be selected.
   If you select Manually set priority list, click Set to create a series of MEP rules.
4. Select a Tracking option, if required.

Configuring Implicit First to Respond

When more than one Security Gateway leads to the same (overlapping) VPN domain, they are in a MEP configuration. The first Security Gateway to respond is chosen. To configure first to respond, define that part of the network that is shared by all the Security Gateways into a single group and assign that group as the VPN domain.

Before you start, make sure that Load Distribution is not enabled:
1. In R80 SmartConsole, go to Menu > Global Properties > VPN > Advanced.
2. Clear the Enable load distribution for Multiple Entry Points option.

To configure First to Respond MEP:
1. For each Security Gateway in the VPN domain, run vpn overlap_encdom.
2. In R80 SmartConsole, create a host group and assign all these Security Gateways to it.
3. In each Security Gateway object go to the Network Management > VPN Domain page,
4. Select Manually defined.
5. Select the host group of MEP gateways that you defined in step 2.
6. Click OK.

Configuring Implicit Primary-Backup

Configure the VPN Domain that includes the Primary gateway and another domain that includes only the backup gateway. Configure each gateway as either the Primary gateway or a backup gateway.

To configure the primary gateway:
1. Open Global Properties window > VPN > Advanced, select Enable Backup Gateway.
2. In the Object Explorer, click New > Network Group and create a group of gateways to act as backup gateways.
3. Edit the Primary gateway object and open the IPsec VPN page.
4. Select Use Backup Gateways, and select the group of backup gateways.
   This gateway is the primary gateway for this VPN domain.
5. For each backup gateway, make a VPN domain that does not include IP addresses that are in the Primary VPN domain or the other backup domains.
   If the backup gateway already has a VPN domain, you must make sure that its IP addresses do not overlap with the other VPN domains.
   a) Create a group of IP addresses not in the other domains, or a group that consists of only the backup gateway.
   b) In the backup network object, go to the Network Management > VPN Domain section, select Manually defined.
   c) Select the group.
6. Click OK.
7. Install the policy.

Configuring Implicit Load Distribution

To configure implicit MEP for random gateway selection:
1. Click Menu > Global Properties.
2. Open the VPN > Advanced page.
3. Select Enable load distribution for Multiple Entry Point configurations (Site to Site connections).
4. Define the same VPN domain for all the gateways:
   a) Create a group of the gateways.
   b) In each gateway network object, go to the Network Management > VPN Domain page, and select Manually defined.
   c) Select the group.
5. Click OK.
6. Install the Access Control Policy.
Routing Return Packets

To make sure return packets are routed correctly, the MEP Security Gateway can make use of either:

- IP pool NAT (static NAT) or
- Route Injection Mechanism. For more information on RIM, see Configuring RIM in a Star Community (on page 27)

Configuring IP Pool NAT

To configure IP pool NAT for site to site VPN:

1. In Menu > **Global Properties**, open the **NAT** page, and click **Enable IP Pool NAT**.
2. Set tracking options for address exhaustion and for address allocation and release.
3. For each Security Gateway, create a network object that represents the IP pool NAT addresses for that Security Gateway. The IP pool can be a network, group, or address range. For example:
   - Open the **Object Explorer** (Ctrl+E) and click **New > Network Object > Address Range > Address Range**. The **New Address Range** window opens.
   - On the **General** tab, enter the first IP and last IP of the address range.
   - Click **OK**.
4. On the Security Gateway object where IP pool NAT translation is performed, in the **NAT > IP Pool NAT** page, select either
   - **Allocate IP Addresses from**, and select the address range you created, OR
   - **Define IP Pool addresses on Security Gateway interfaces**. If you choose this option, you need to define the IP Pool on each required interface, in the **Interface Properties** window, **IP Pool NAT** tab.
5. In the **IP Pool NAT** page, select either (or all):
   - **Use IP Pool NAT for VPN clients connections**
   - **Use IP Pool NAT for Security Gateway to Security Gateway connections**
   - **Prefer IP Pool NAT over Hide NAT**
6. Click **Advanced...**
   - Decide after how many minutes unused addressees are returned to the IP pool.
   - Click **OK** twice.
7. Edit the routing table for each internal router, so that packets with an IP address assigned from the NAT pool are routed to the appropriate Security Gateway.
Public Key Infrastructure

In This Section:

- Enrolling with a Certificate Authority ................................................................. 16
- Manual Enrollment with OPSEC Certified PKI .................................................... 16
- Trusting an Externally Managed CA ................................................................. 17
- Trusting an OPSEC Certified CA ........................................................................ 17
- Certificate Revocation (All CA Types) ............................................................... 18

Enrolling with a Certificate Authority

A certificate is automatically issued by the ICA for all internally managed entities that are VPN capable. That is, after the administrator has selected IPsec VPN in the Network Security tab of the General Properties page for network objects.

The process for obtaining a certificate from an OPSEC PKI or External Check Point CA is identical.

Manual Enrollment with OPSEC Certified PKI

To create a PKCS#10 Certificate Request:

1. Create the CA object [see “Trusting an OPSEC Certified CA” on page 17].
2. Open the IPsec VPN tab of the relevant Network Object.
3. In the Certificate List field click Add.
   The Certificate Properties window is displayed.
4. Enter the Certificate Nickname
   The nickname is only an identifier and has no bearing on the content of the certificate.
5. From the CA to enroll from drop-down box, select the direct OPSEC CA/External Check Point CA that will issue the certificate.
   Note - The list displays only those subordinate CA’s that lead directly to a trusted CA and the trusted CAs themselves. If the CA that issues the certificate is a subordinate CA that does not lead directly to a trusted CA, the subordinate CA will not appear in the list.
6. Choose the appropriate method for Key Pair creation and storage.
7. Click Generate.
   The Generate Certificate Properties window is displayed.
8. Enter the appropriate DN.
   The final DN that appears in the certificate is decided by the CA administrator.
   If a Subject Alternate Name extension is required in the certificate, check the Define Alternate Name check box.
   Adding the object IP as Alternate name extension can be configured as a default setting by selecting in Menu > Global Properties > Advanced > Configure > Certificates and PKI properties, the options:
   add_ip_alt_name_for_opsec_certs
add_ip_alt_name_for_ICA_certs
The configuration in this step is also applicable for Internal CAs.

9. Click **OK**.
The public key and the DN are then used to DER-encode a PKCS#10 Certificate Request.

10. After the Certificate Request is ready, click **View**.
The Certificate Request View window appears with the encoding.

11. Copy the whole text in the window and deliver it to the CA.
The CA administrator must now complete the task of issuing the certificate. Different CAs provide different ways of doing this, such as an advanced enrollment form (as opposed to the regular form for users). The issued certificate may be delivered in various ways, for example email. After the certificate has arrived, it needs to be stored:

   a) In **Object Explorer** (Ctrl+E), go to the **Servers** category and select the CA object.
   b) Open the OPEC PKI tab, click **Get** and browse to the location in which the certificate was saved.
   c) Select the appropriate file and verify the certificate details.
   d) Close object and save.

### Trusting an Externally Managed CA

An externally managed CA is the ICA of another Security Management Server. The CA certificate has to be supplied and saved to disk in advance. To establish trust:

1. In **Object Explorer** (Ctrl+E), click **New > Server > More > Trusted CA**.
The Certificate Authority Properties window opens.
2. Enter a **Name** for the CA object
3. Go to the **OPSEC PKI** tab and click **Get...**
4. Browse to where you saved the peer CA certificate and select it.
The certificate details are shown. Verify the certificate’s details. Display and validate the SHA-1 and MD5 fingerprints of the CA certificate.
5. Click **OK**.

### Trusting an OPSEC Certified CA

The CA certificate has to be supplied and saved to the disk in advance.

*Note* - In case of SCEP automatic enrollment, you can skip this stage and fetch the CA certificate automatically after configuring the SCEP parameters.

The CA’s Certificate must be retrieved either by downloading it using the CA options in the Certificate Authority object, or by obtaining the CA’s certificate from the peer administrator in advance.

Then define the CA object according to the following steps:

1. In **Object Explorer** (Ctrl+E), click **New > Server > More > Trusted CA or Subordinate CA**.
The Certificate Authority Properties window opens.
2. Enter a **Name** for the CA object.
3. On the **OPSEC PKI** tab:
   - For automatic enrollment, select **automatically enroll certificate**.
   - From the **Connect to CA with protocol**, select the protocol used to connect with the certificate authority, either SCEP, CMPV1 or CMPV2.
   
   **Note** - For entrust 5.0 and later, use CMPV1

4. Click **Properties**.
   - If you chose SCEP as the protocol, in the **Properties for SCEP protocol** window, enter the CA identifier (such as example.com) and the Certification Authority/Registration Authority URL.
   - If you chose cmpV1 as the protocol, in the **Properties for CMP protocol - V1** window, enter the appropriate IP address and port number. (The default port is 829).
   - If you chose cmpV2 as the protocol, in the **Properties for CMP protocol -V2** window, decide whether to use direct TCP or HTTP as the transport layer.
   
   **Note** - If Automatic enrollment is not selected, then enrollment will have to be performed manually.

5. Choose a method for retrieving CRLs from this CA.
   - If the CA publishes CRLs on HTTP server choose **HTTP Server(s)**. Certificates issued by the CA must contain the CRL location in an URL in the **CRL Distribution Point** extension.
   - If the CA publishes CRL on LDAP server, choose **LDAP Server(s)**. In this case, you must define an LDAP Account Unit as well. See the **Security Management Server Administration Guide** for more details about defining an LDAP object.
   
   Make sure that **CRL retrieval** is checked in the **General** tab of the **LDAP Account Unit Properties** window.
   
   Certificates issued by the CA must contain the LDAP DN on which the CRL resides in the CRL distribution point extension.

6. Click **Get**.

7. If SCEP is configured, it will try to connect to the CA and retrieve the certificate. If not, browse to where you saved the peer CA certificate and select it.
   
   VPN reads the certificate and displays its details. Verify the certificate’s details. Display and validate the SHA-1 and MD5 fingerprints of the CA certificate.

8. Click **OK**.


**Certificate Revocation (All CA Types)**

To remove the certificate:

1. Open the **IPsec VPN** tab of the relevant Security Gateway.

2. In the Repository of **Certificates Available to the Gateway**, select the appropriate certificate and click **Remove**.
Traditional Mode VPNs

In This Section:
- Editing a Traditional Mode Policy ................................................................. 19
- Configuring VPN between Internal Gateways with ICA Certificates ............... 19
- Configuring VPN between Internal Gateways with Third Party CA Certificates 20

Editing a Traditional Mode Policy

An existing Traditional Mode policy will open in Traditional Mode.

To start a new Traditional Mode policy:
1. Open the Global Properties window, VPN page.
2. Select one of these options:
   - Traditional mode to all new Firewall Policies
   - Traditional or Simplified per new Firewall Policy
3. Install the Access Control policy.

If you selected Traditional or Simplified per new Firewall Policy:
1. From the R80 SmartConsole Menu, select Manage policies (Ctrl+O).
   The Manage policies window opens.
2. Click New
   The New Policy window opens.
3. Give the new policy a name.
4. Select the Policy types.
5. Select VPN Traditional mode.
6. Click OK.
   In the new Policy Rule Base, one of the available Actions is Encrypt.

Configuring VPN between Internal Gateways with ICA Certificates

To define the Security Gateways:
1. For each Security Gateway that is to be part of the VPN define a Check Point Security Gateway object. In the In Gateways & Servers view, click New > Gateway.
2. In the General Properties page of the Check Point Security Gateway object, select IPsec VPN.
3. In the Communication window, establish Trusted Communication.
4. In the Network Management page, define the IP address, network mask, and Anti-Spoofing for every Security Gateway interface
5. In the Network Management > VPN Domain page, define the VPN Domain, select either:
   - All IP Addresses behind Security Gateway based on Topology information or
   - Manually defined. Either select an existing network or group from the drop-down list or create a new group of machines or networks by clicking New...
6. In the IPsec VPN page, Repository of Certificates Available to the Gateway, Add a certificate issued by the ICA.

7. Still on the IPsec VPN page, click Traditional mode configuration. The Traditional mode IKE properties window opens.
   - In the Support authentication methods area, select Public Key Signatures. To specify that the Security Gateway will only use certificates issued by the ICA, click Specify and select the ICA.
   - Select IKE Phase 1 encryption and data integrity methods or accept the checked defaults.

Configuring VPN between Internal Gateways with Third Party CA Certificates

To define the Security Gateways:

1. For each Security Gateway that is to be part of the VPN define a Check Point Security Gateway object. In the In Gateways & Servers view, click New > Gateway.
2. In the General Properties page of the Check Point Security Gateway object, select IPsec VPN.
3. In the Communication window, establish Trusted Communication.
4. In the Network Management page, define the IP address, network mask, and Anti-Spoofing for every Security Gateway interface
5. In the Network Management > VPN Domain page, define the VPN Domain. select either:
   - All IP Addresses behind Security Gateway based on Topology information or
   - Manually defined. Either select an existing network or group from the drop-down list or create a new group of machines or networks by clicking New...
6. In the IPsec VPN page, Repository of Certificates Available to the Gateway, Add a certificate issued by the certificate authority (see “Enrolling with a Certificate Authority” on page 16) defined in step 1.
7. Still on the IPsec VPN page, click Traditional mode configuration. The Traditional mode IKE properties window opens.
   - In the Support authentication methods area, select Public Key Signatures. To specify that the Security Gateway will only use certificates issued by the ICA, click Specify and select the CA.
   - Select IKE Phase 1 encryption and data integrity methods or accept the checked defaults.
8. Repeat step 2 to step 7 for each Security Gateway taking part in the VPN.
Site to Site Solutions for Different Deployments

In This Section:

Configuring VPN Routing for Security Gateways through R80 SmartConsole ..........21
Enabling Route Based VPN ..........................................................................................22
Configuring Tunnel Features .......................................................................................24
Permanent Tunnels ......................................................................................................24
Configuring RIM in a Star Community .......................................................................27
Enabling the RIM_inject_peer_interfaces flag ...........................................................27
Enabling Wire Mode on a VPN Community .................................................................28
Enabling Wire Mode on a Specific Security Gateway ..................................................28
Configurable Objects in a Direction .............................................................................28
Configuring Directional VPN Within a Community .....................................................29
Configuring Directional VPN Between Communities ................................................29
Configuring On Demand Links ....................................................................................29
Configuring Link Selection and ISP Redundancy ........................................................30
VPN Community Object - Encryption Settings .............................................................30

Configuring VPN Routing for Security Gateways through R80 SmartConsole

For simple hubs and spokes (or if there is only one Hub), the easiest way is to configure a VPN star community in R80 SmartConsole:

1. On the Star Community window, in the:
   a) Center Gateways section, select the Security Gateway that functions as the "Hub".
   b) Satellite Gateways section, select Security Gateways as the "spokes", or satellites.

2. On the VPN Routing page, Enable VPN routing for satellites section, select one of these options:
   - To center and to other Satellites through center - This allows connectivity between the Security Gateways, for example if the spoke Security Gateways are DAIP Security Gateways, and the Hub is a Security Gateway with a static IP address.
   - To center, or through the center to other satellites, to internet and other VPN targets - This allows connectivity between the Security Gateways as well as the ability to inspect all communication passing through the Hub to the Internet.

3. Create an appropriate Access Control Policy rule.
4. NAT the satellite Security Gateways on the Hub if the Hub is used to route connections from Satellites to the Internet.

The two Dynamic Objects (DAIP Security Gateways) can securely route communication through the Security Gateway with the static IP address.
Configuring the 'Accept VPN Traffic Rule'

In R80 SmartConsole:
1. Double click on a Star or Meshed Community.
2. On the Encrypted Traffic page, select Accept all encrypted traffic.
3. In a Star community, choose between accepting encrypted traffic on Both center and satellite gateways or Satellite gateways only.
4. Click OK.

Enabling Route Based VPN

If you configure a Security Gateway for Domain Based VPN and Route Based VPN, Domain Based VPN takes precedence by default. To force Route Based VPN to take priority, you must create a dummy (empty) group and assign it to the VPN domain.

To force Route-Based VPN to take priority:
1. In the Gateways & Servers view, edit a Check Point Security Gateway.
2. Go to the Network Management > VPN Domain page.
3. Select Manually define.
5. Enter a Name and click OK.

Configuring VTIs in a Clustered Environment

After configuring the VTIs on the cluster members, you must configure in the R80 SmartConsole the VIP of these VTIs.

In R80 SmartConsole:
1. In the Gateways & Servers view, edit the Check Point Cluster.
2. In Network Management window, click Get Interfaces.
   The VTIs are shown in the Topology column as Point to point.
   Interfaces are members of the same VTI if these criteria match:
   • Remote peer name
   • Remote IP address
   • Interface name
3. Configure the VTI VIP. Select the interface and click Edit. Edit the interface in the General page of the interface object.
4. Click OK and install policy.

Configuring Anti-Spoofing on VTIs

In R80 SmartConsole:
1. In the Gateways & Servers view, edit a Check Point Security Gateway.
2. Go to the Network Management page.
3. Click Get Interfaces to read the interface information on the Security Gateway computer.
4. Select an interface, and click Edit.
5. In the Topology section of the General page, click Modify.
6. In the **IP Addresses behind peer Security Gateway that are within reach of this interface** section, select:
   - **Not Defined** to accept all traffic.
   - **Specific** to choose a particular network. The IP addresses in this network will be the only addresses accepted by this interface.

7. In the **Perform Anti-Spoofing based on interface topology** section, select **Don’t check packets from** to ensure Anti-Spoofing checks do not take place for addresses from certain internal networks coming into the external interface. Define a network object that represents those internal networks with valid addresses, and from the drop-down list, select that network object.
   
   Objects selected in the **Don’t check packets from** drop-down menu are disregarded by the Anti-Spoofing enforcement mechanism.

8. Under **Spoof Tracking** select **Log**, and click **OK**.

### Configuring Unnumbered VTIs

Working with unnumbered interfaces eliminates the need to assign two IP addresses per interface (the local IP, and the remote IP Address), and the need to synchronize this information among the peers.

If the VPN Tunnel Interface is unnumbered, local and remote IP addresses are not configured. This interface is associated with a proxy interface from which the virtual interface inherits an IP address. Traffic initiated by the Security Gateway and routed through the virtual interface will have the physical interface’s IP Address as the source IP.

Unnumbered interfaces are supported for Gaia and IPSO (3.4 and higher) platforms.

**Note** - IPSO platform supports unnumbered VTIs in a VRRP HA configuration, active-passive mode only.

**To configure unnumbered VTIs for IPSO:**

1. Log into IPSO Network Voyager.
2. Click **Configuration**.
3. Click **Interface Configuration**.
4. On the next page, click **FWVPN Tunnel**.
5. On the **FWVPN Tunnel Configuration** page, enter the name of the Security Gateway you want to connect to in the **Peer GW Object Name** field.
6. Select a proxy interface from the **Proxy** drop down menu.
7. Click **Apply**.
   
   The new interface shows on the **FWVPN Tunnel Configuration** page.

**To configure unnumbered VTIs for Gaia:**

1. In Gaia WebUI, select **Interface Management > Network Interfaces**.
2. Click **Add > VPN Tunnel**.
3. In the **Add/Edit** window that opens, configure these parameters:
   - **VPN Tunnel ID** - an integer from 1 to 99, and Gaia automatically adds **vpnt** prefix to the Tunnel ID
• **Remote Peer Name** - alpha-numeric Peer ID, as defined for the Remote Peer Name in the VPN community. You must define the two peers in the VPN community before you define the VTI.

• **VPN Tunnel Type** - select **Unnumbered**

• **Local Address** - leave empty for unnumbered VTI

• **Remote Address** - leave empty for unnumbered VTI

• **Physical Device** - the name of the local peer interface (the loopback interface can also be configured as the local peer interface)

### Configuring Tunnel Features

To configure Tunnel Management options:

1. In R80 SmartConsole, click **Object Explorer** (Ctrl+E)

2. Click **New > VPN Community** and choose **Star Community** or **Meshed community**.

3. Click **Tunnel Management** and configure the tunnel settings:
   - Permanent Tunnels
   - Tracking Options
   - VPN Tunnel Sharing

### Permanent Tunnels

In the **Star Community** or **Meshed community** object, on the **Tunnel Management** page, select **Set Permanent Tunnels**. These are the options:

- **On all tunnels in the community**
- **On all tunnels of specific Security Gateways**
- **On specific tunnels in the community**

To configure all tunnels as permanent, select **On all tunnels in the community**. Clear this option to terminate all Permanent Tunnels in the community.

To configure on all tunnels of specific Security Gateways:

1. Select **On all tunnels of specific gateways** and click **Select Gateways**.

   The **Select Gateway** window is displayed.

   To terminate Permanent Tunnels connected to a specific Security Gateway, highlight the Security Gateway and click **Remove**.

2. To configure the Tracking options for a specific Security Gateway, highlight a Security Gateway and click **Gateway Tunnel Properties**.

To configure on specific tunnels in the community:

1. Select **On specific tunnels in the community** and click **Select Permanent Tunnels**.

   The **Select Permanent Tunnels** window opens.

2. Double click in the white cell that intersects the Security Gateways where a permanent tunnel is required.

   The **Tunnel Properties** window is displayed.
3. Click **Set these tunnels to be permanent tunnels**.
   To terminate the Permanent Tunnel between these two Security Gateways, clear **Set these tunnels to be permanent tunnels**.

4. Click **OK**.

**Advanced Permanent Tunnel Configuration**

In R80 SmartConsole:

1. Click **Menu > Global Properties**.
   The **Global Properties** window shows.

2. Select **Advanced > Configure**.
   The **Advanced configuration** window shows.

3. Click **VPN Advanced Properties > Tunnel Management** to see the five attributes that may be configured to customize the amount of tunnel tests sent and the intervals in which they are sent:
   - **life_sign_timeout** - Set the amount of time the tunnel test runs without a response before the peer host is declared 'down.'
   - **life_sign_transmitter_interval** - Set the time between tunnel tests.
   - **life_sign_retransmissions_count** - When a tunnel test does not receive a reply, another test is resent to confirm that the peer is 'down.' The Life Sign Retransmission Count is set to how many times the tunnel test is resent without receiving a response.
   - **life_sign_retransmissions_interval** - Set the time between the tunnel tests that are resent after it does not receive a response from the peer.
   - **cluster_status_polling_interval** - (Relevant for HA Clusters only) - Set the time between tunnel tests between a primary Security Gateway and a backup Security Gateway. The tunnel test is sent by the backup Security Gateway. When there is no reply, the backup Security Gateway will become active.

**DPD Responder Mode**

In this mode the Check Point gateway sends the IKEv1 DPD Vendor ID to peers from which the DPD Vendor ID was received.

**To enable DPD Responder Mode:**

1. Run on each gateway:
   
   ```
   ckp_regedit -a SOFTWARE/CheckPoint/VPN1 forceSendDPDPayload -n 1
   ```

2. Enable the `keep_IKE_SAs` property in GuiDBedit to prevent a problem where the Check Point gateway deletes IKE SAs:
   
   a) In **R80 SmartConsole**, go to **Menu > Global Properties > Advanced > Advanced Configuration > VPN advanced properties > VPN IKE properties**.
   
   b) Change `keep_IKE_SAs` to **true**.

**To disable DPD Responder Mode:**

1. Run on each gateway:

   ```
   ckp_regedit -d SOFTWARE/CheckPoint/VPN1 forceSendDPDPayload
   ```
**Note** - Enable the `keep_IKE_SAs` property in GuiDBedit to prevent a problem where the Check Point gateway deletes IKE SAs. The DPD mechanism is based on IKE SA keys. In some situations, the Check Point gateway deletes IKE SAs and a peer, usually a 3rd Party gateway, sends DPD requests without response and concludes that the Check Point gateway is down. The peer can then delete the IKE and IPsec keys, which causes encrypted traffic from the Check Point gateway to be dropped by the remote peer.

**Permanent Tunnel Mode Based on DPD**

DPD can monitor remote peers with the permanent tunnel feature. All related behavior and configurations of permanent tunnels are supported.

To configure DPD for a permanent tunnel, the permanent tunnel must be in the VPN community. After you configure the permanent tunnel, configure Permanent Tunnel mode Based on DPD. There are different possibilities for permanent tunnel mode:

- **tunnel_test (default)** - The permanent tunnel is monitored by tunnel test (as in earlier versions). It works between Check Point gateways only. Keepalive packets are always sent.

- **dpd** - The active DPD mode. A peer receives DPD requests at regular intervals (10 seconds). DPD requests are only sent when there is no traffic from the peer.

- **passive** - The passive DPD mode. Peers do not send DPD requests to this peer. Tunnels with passive peers are monitored only if there is IPsec traffic and incoming DPD requests.

  **Note:** To use this mode for only some gateways, enable the `forceSendDPDPayload` registry key on Check Point remote peers.

To enable DPD monitoring:

On each VPN gateway in the VPN community, configure the `tunnel_keepalive_method` property, in GuiDBedit. This includes 3rd Party gateways. (You cannot configure different monitor mechanisms for the same gateway).

1. In GuiDBedit, go to Network Objects > network_objects > <gateway> > VPN.
2. For the Value, select a permanent tunnel mode.
3. Save.
4. Install policy on the gateways.

**Optional Configuration**

- **IKE Initiation Prevention** - By default, when a valid IKE SA is not available, a DPD request message triggers a new IKE negotiation. To prevent this behavior, set the property `dpd_allowed_to_init_ike` to `false`.
  Edit the property in GuiDBedit under Network Objects > network_objects > <gateway Name> > VPN.

- **Delete IKE SAs for dead peer** - Based on RFC 3706, a VPN gateway has to delete IKE SAs from a dead peer. This functionality is enabled, by default.
  To disable this feature, set the `DPD_DONT_DEL_SA` environment variable to `0`:

  - To do this temporarily, run:
    ```
    cpstop
    export DPD_DONT_DEL_SA=0
    cpstart
    ```
To do this permanently:

(i) Add this line to the $CPDIR/tmp/.CPprofile.sh file:

   DPD_DONT_DEL_SA=0 ; export DPD_DONT_DEL_SA

(ii) Reboot

Note: To re-enable the feature, remove the DPD_DONT_DEL_SA environment variable.

Configuring RIM in a Star Community

1. Open the Star Community > Tunnel Management page.

2. In the Permanent Tunnels section, select Set Permanent Tunnels. The following Permanent Tunnel modes are then made available:

   • On all tunnels in the community
   • On all tunnels of specific Security Gateways
   • On specific tunnels in the community

When choosing tunnels, keep in mind that RIM can only be enabled on tunnels that have been configured to be permanent (see "Configuring Tunnel Features" on page 24). On all tunnels in the community must be selected if MEP is enabled on the community.

1. Select Enable Route Injection Mechanism (RIM).

2. Click Settings...

   The Star Community Settings window opens

   Decide if:

   • RIM should run automatically on the central or satellite Security Gateways [Gaia, SecurePlatform, or IPSO only].
   • A customized script should be run on central or satellite Security Gateways whenever a tunnel changes its states (goes up or down).

   You can also configure the tracking options.

3. If a customized script is run, edit custom_rim [.sh or .bat] script in the $FWDIR/Scripts directory on each of the Security Gateways.

Enabling the RIM_inject_peer_interfaces flag

To enable the RIM_inject_peer_interfaces flag:

1. In R80 SmartConsole, click Menu > Global Properties.

2. Go to Advanced > Configure.

   The Advanced Configuration window opens

3. Click VPN Advanced Properties > Tunnel Management.

4. Select RIM_inject_peer_interfaces.

5. Click OK.
Enabling Wire Mode on a VPN Community

1. In R80 SmartConsole, open the Object Explorer, select the VPN community to be configured and click Edit.
2. Open the Wire Mode page.
3. To enable Wire Mode on the community, select Allow uninspected encrypted traffic between Wire mode interfaces of the Community members.
4. To enable Wire Mode Routing, select Wire Mode Routing - Allow members to route uninspected encrypted traffic in VPN routing configurations.

Enabling Wire Mode on a Specific Security Gateway

1. In R80 SmartConsole, open the Gateways & Servers view, select the relevant Security Gateway and click Edit.
2. Open the IPsec VPN > VPN Advanced page.
3. To enable Wire Mode on the Security Gateway, select Support Wire Mode (and Wire mode routing...)
4. Click Add to include the interfaces to be trusted by the selected Security Gateway.
5. Select Log Wire mode traffic to log wire mode activity.

Configurable Objects in a Direction

The table shows all the objects that can be configured in a direction, including three new objects created for Directional VPN:

<table>
<thead>
<tr>
<th>Name of Object</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote Access</td>
<td>Remote Access community</td>
</tr>
<tr>
<td>Site2SiteVPN</td>
<td>Regular Star/Mesh community</td>
</tr>
<tr>
<td>Any Traffic</td>
<td>Any traffic</td>
</tr>
<tr>
<td>All_GwToGw</td>
<td>All gateway to gateway traffic</td>
</tr>
<tr>
<td>All_Communities</td>
<td>All communities</td>
</tr>
<tr>
<td>External_clear</td>
<td>For traffic outside the VPN community</td>
</tr>
<tr>
<td>Internal_clear</td>
<td>For traffic between local domains within the community</td>
</tr>
</tbody>
</table>

**Note**: Clear text connections originating from the following objects are not subject to enforcement:
- Any Traffic
- External_clear
- Internal_clear

There is *no limit* to the number of VPN directions that can be configured on a single rule. In general, if you have many directional enforcements, consider replacing them with a standard bidirectional condition.
Configuring Directional VPN Within a Community

To configure Directional VPN within a community:

1. In the Global Properties > VPN > Advanced page, select Enable VPN Directional Match in VPN Column.
2. In the VPN column of the appropriate rule, select Directional Match Condition. The New Directional Match Condition window opens.
3. In the Traffic reaching from drop-down box, select the object for Internal_clear (the source).
4. In the Traffic leaving to drop-down box, select the relevant community object (the destination).
5. Add another directional match in which the relevant community object is both the source and destination. This allows traffic from the local domain to the community, and within the community.
6. Click OK.

Configuring Directional VPN Between Communities

To configure Directional VPN between communities:

1. In the Global Properties > VPN > Advanced page, select Enable VPN Directional Match in VPN Column.
2. In the VPN column of the appropriate rule, select Directional Match Condition. The New Directional Match Condition window opens.
3. In the Traffic reaching from drop-down box, select the source of the connection.
4. In the Traffic leaving to drop-down box, select the destination of the connection.
5. Click OK.

Configuring On Demand Links

You can enable On Demand Links only if you enabled Route Based Probing. Configure On Demand Links commands in GuiDBedit, the Check Point Database Tool.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>use_on_demand_links</td>
<td>Enables on-demand links. The default is FALSE. Change to TRUE.</td>
</tr>
<tr>
<td>on_demand_metric_min</td>
<td>Defines the minimum metric level for an on-demand link. This value must be equal to or higher than the configured minimum metric.</td>
</tr>
<tr>
<td>on_demand_initial_script</td>
<td>The name of the on-demand script, which runs when all not-on-demand routes stop responding. Put the script in the $FWDIR/conf directory.</td>
</tr>
<tr>
<td>on_demand_shutdown_script</td>
<td>This script is run when the failed links become available. Put the script in the $FWDIR/conf directory.</td>
</tr>
</tbody>
</table>
If you do not want to use GuiDBedit, you can configure the `use_on_demand_links` and `on_demand_metric_min` commands in R80 SmartConsole:

1. In R80 SmartConsole, click **Menu > Global Properties > Advanced > Configure**.
2. In **VPN Advanced Properties**, click **Link Selection**.
3. Click **use_on_demand_links** to enable On Demand Links.
4. Set the minimum metric level for an On Demand Link next to the `on_demand_metric_min` command.

### Configuring Link Selection and ISP Redundancy

Configure Link Selection and ISP Redundancy in the **Other > ISP Redundancy** page of the Gateway object.

### VPN Community Object - Encryption Settings

IPv6 automatically works with IKEv2 encryption only. The option that you select here, applies to IPv4 traffic.

To configure a VPN Community object:

1. In R80 SmartConsole, click **Open Object Explorer** (Ctrl+E).
2. From the navigation tree, click **VPN Communities**.
3. Double-click the VPN Community object.
   The Community object window opens and shows the **Gateways** page.
4. From the navigation tree, click **Encryption**.
5. Configure the settings.
6. Click **OK** and publish the changes.

#### Encryption Method

- **Encryption Method** - For IKE phase I and II.
  - **IKEv2 only** - Only support encryption using IKEv2. Security Gateways in this community cannot access peer gateways that support IKEv1 only.
  - **Prefer IKEv2, support IKEv1** - If a peer supports IKEv2, the Security Gateway will use IKEv2. If not, it will use IKEv1 encryption. This is recommended if you have a community of older and new Check Point Security Gateways.
  - **IKEv1 only** - IKEv2 is not supported.

#### Encryption Suite

- **Use this encryption suite** - Select the methods negotiated in IKE phase 2 and used in IPSec connections. Select and choose the option for best interoperability with other vendors in your environment.
  - **VPN-A** or **VPN B** - See RFC 4308 for more information.
  - **Suite-B GCM-128 or 256** - See RFC 6379 for more information.
- **Custom encryption suite** - If you require algorithms other than those specified in the other options, select the properties for IKE Phase 1, including which **Diffie-Hellman group** to use. Also, select properties for IKE Phase 2.
Note - Suite-B GCM-128 and 256 encryption suites are supported on R71.50 gateways and from R75.40 gateways.

If there is a Dynamic IP Gateway inside the community, R77.30 (or lower) community member gateways that respond to its IKE negotiation, use the configuration defined in Global Properties > Remote Access > VPN -Authentication and Encryption.

More

- **Use aggressive mode** (Main mode is the default) - Select only if the peer only supports aggressive mode. This is only supported with IKEv1.
- **Use Perfect Forward Secrecy**, and the **Diffie-Hellman group** - Select if you need extremely high security.
- **Support IP compression** - Select to increase throughput.

**VPN Community Object - Advanced Settings**

Configure these options in the VPN Community object Advanced page:

**IKE (Phase 1)**

When to renegotiate the IKE Security Associations.

**IKE (Phase 2)**

When to renegotiate the IPsec security associations. This sets the expiration time of the IPsec encryption keys.

**NAT**

**Disable NAT inside the VPN community** - Select to not apply NAT for the traffic while it passes through IPsec tunnels in the community.

**Reset**

Reset all VPN properties to the default.
Configuring Remote Access VPN

In This Section:

Defining a Remote Access Community .................................................................32
Configuring the Security Gateway for a Remote Access Community ................32
Defining Access Control Rules ...............................................................................33
Enabling a User Certificate ....................................................................................33
Enabling Hybrid Mode and Methods of Authentication ........................................34
Using a Pre-Shared Secret ......................................................................................34
Configuring RADIUS Objects ...............................................................................35
Modifying Encryption Properties for Remote Access VPN .................................37

This section includes procedures and explanations for configuring Remote Access VPN. For configuration specific to Endpoint Security VPN, Check Point Mobile for Windows, and SecuRemote, see the Remote Access Clients Administration Guide.

Defining a Remote Access Community

To define the VPN Remote Access community and its participants:

1. From the Objects Bar, click VPN Communities.
   The Remote Access window opens.
3. On the Participating Gateways page, click the Add button and select the Security Gateways that are in the Remote Access Community.
4. On the Participating User Groups page, click the Add button and select the group that contains the Remote Access users.
5. Click OK.
6. Publish the changes.

Configuring the Security Gateway for a Remote Access Community

Make sure that the VPN Software Blade is enabled before you configure the Remote Access community.

To configure the Security Gateway for Remote Access:

1. In R80 SmartConsole, click Gateways & Servers and double-click the Security Gateway. The gateway window opens and shows the General Properties page.
2. From the navigation tree, click IPsec VPN. The page shows the VPN communities that the Security Gateway is participating.
3. To add the Security Gateway to a community:
   a) Click Add.
   b) Select the community.
   c) Click OK.
4. From the navigation tree, click Network Management > VPN Domain.
5. Configure the VPN Domain.
6. Configure the settings for Visitor Mode ["Proxy Replacement for the Security Gateway” on page 50].
7. From the navigation tree, click VPN Clients > Office Mode.
8. Configure the settings for Office Mode [“IP Pool Configuration” on page 39].
   Note - Office Mode support is mandatory on the Security Gateway side.
9. Click OK and publish the changes.

**Defining Access Control Rules**

Access control is a layer of security not connected with VPN. The existence of a remote access community does not mean that members of that community have free automatic access to the network. Appropriate rules need to be created in the Access Control Policy Rule Base blocking or allowing specific services.

1. Create a rule in the Security Access Control Rule Base that deals with remote access connections.
2. Right-click the cell in the VPN column, and select Specific VPN Communities.
3. Click the add button for each community that you are adding to the rule.
4. Close the VPN community window.
5. Define Services & Applications and Actions.
6. Publish the changes and install the policy.

   For example, to allow remote access users to access the organization’s SMTP server, called SMTP_SRV, create the following rule:

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>VPN</th>
<th>Service</th>
<th>Action</th>
<th>Track</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>SMTP_SRV</td>
<td>Remote_Access_Community</td>
<td>SMTP</td>
<td>Accept</td>
<td>Log</td>
</tr>
</tbody>
</table>

**Enabling a User Certificate**

To enable a user certificate:

1. In R80 SmartConsole, from the Objects Bar click Users > Users.
2. Create a new user or double-click an existing user.
   The User Properties window opens.
3. From the navigation tree, click Encryption.
4. Click Edit.
   The IKE Phase 2 Properties window opens.
5. Click the Authentication tab and make sure that Public key is selected.
6. Click **OK**.
7. Publish the changes.

**For Internally Managed Users**

When a user is deleted, their certificate is automatically revoked. Certificates can be disabled or revoked at any time.

If the certificate is already active or was not completed by the user, you can revoke it by clicking **Revoke** in the **Certificates** tab of the **User Properties** window.

**Enabling Hybrid Mode and Methods of Authentication**

Hybrid mode allows the Security Gateway and remote access client to use different methods of authentication.

**To enable Hybrid Mode:**

1. From Menu, click **Global Properties**.
2. From the navigation tree, click **Remote Access > VPN Authentication**.
3. In the **Support authentication methods** section, click **Support Legacy Authentication for SC (hybrid mode), L2TP (PAP), and Nokia clients (CRACK)**.
4. Click **OK**.
5. Publish the changes.

**Defining User Authentication Methods in Hybrid Mode**

**To define the Hybrid Mode authentication for a user:**

1. From the Objects Bar, double-click the user. The **User Properties** window opens.
2. From the navigation tree, click **Authentication**.
3. Select the **Authentication Scheme**.
4. Configure the necessary settings.
5. Click **OK**.
6. Publish the changes.
7. Give these credentials to the user.

**Using a Pre-Shared Secret**

When using pre-shared secrets, the remote user and Security Gateway authenticate each other by verifying that the other party knows the shared secret: the user's password.

**To enable authentication with pre-shared secrets:**

1. From Menu, click **Global Properties**.
2. From the navigation tree, click **Remote Access > VPN Authentication**.
3. In the **Support authentication methods** section, select **Pre-Shared Secret (For SecuRemote / SecureClient users)**.
4. Click **OK**.
5. Configure the Authentication settings for each applicable user:
   a) From the Objects Bar, double-click the user. 
      The **User Properties** window opens.
   b) From the navigation tree, click **Encryption**.
   c) Select **IKE** and click **Edit**. 
      The **IKE Phase 2 Properties** window opens.
   d) From the Authentication tab, click **Password (Pre-Shared Secret)**.
   e) Enter and **Confirm** the **Password (Pre-shared secret)**.
   f) Click **OK**.
6. Publish the changes.
7. Give the password to the user.

### Configuring RADIUS Objects

**To create a new RADIUS host object:**

1. In R80 SmartConsole, the **Objects** tab, click **New > Host**. 
   The **New Host** window opens.
2. Enter the **Object Name** and the **IP Address** of the new RADIUS host object, and click **OK**.
3. Publish the changes.

**To configure the RADIUS server object settings:**

1. In R80 SmartConsole, the **Objects** tab, click **New > More > Server > More > RADIUS**. 
   The **RADIUS Server Properties** window opens.
2. Configure new server properties:
   - Enter the **Name** of the RADIUS server object.
   - Select the RADIUS **Host** object.
   - Select the **Service - RADIUS** (on port 1645) or **NEW-RADIUS** (on port 1812 service).
     **Note** - The default setting is **RADIUS**, but the RADIUS standards group recommends using **NEW-RADIUS**, because port 1645 can conflict with the datametrics service running on the same port.
   - Enter the **Shared Secret** that you configured on the RADIUS server
   - Select the version - **RADIUS Ver. 1.0 Compatible** (RFC 2138 compliant) or **RADIUS Ver. 2.0 Compatible** (RFC 2865 compliant)
   - Select the peer authentication **Protocol - PAP** or **MS-CHAP v2**
   - If you use more than one RADIUS authentication server, select the **Priority**
3. Click **OK**.
4. Publish the changes.
To configure a Security Gateway to use RADIUS authentication:

1. In R80 SmartConsole, go to the **Gateways & Servers** view, right-click a Security Gateway object and select **Edit**.
2. In the gateway property window that opens, select **Other > Legacy Authentication**.
3. In the **Enabled Authentication Schemes** section, select **RADIUS**.
4. Click **OK**.

To define a RADIUS user group:

1. In R80 SmartConsole, the **Objects** tab, click **New > More > Users > User Group**.
   The **New User Group** window opens.
2. Enter the name of the group in this format: **RAD_<group_name>**.
   Make sure the group is empty.
3. Click **OK**.
4. Publish the changes and install the policy.

To configure RADIUS authentication settings for users:

1. Create new user profiles -
   • For users with Security Gateway user accounts - in R80 SmartConsole, go to the **Objects** tab and click **New > More > User > User**.
   • For users without Security Gateway user accounts, open the SmartDashboard - go to **Users > External User Profile > New External User Profile > Match all users** (or **Match by domain**). If you support more than one external authentication scheme, set up External User Profiles with the **Match By Domain** setting.
   The **User Properties** window opens.
2. In the **General Properties** tab, configure these settings:
   • Enter a **User Name** for the RADIUS server. (When configuring **Match all users** as an External User Profile, the name "**generic*" is automatically assigned)
   • Set the **Expiration Date**.
3. In the **Authentication** tab, configure these settings:
   • Select **RADIUS** from the **Authentication Scheme** drop-down list
   • From the **Select a RADIUS Server or Group of Servers** drop-down menu, select the RADIUS object that you configured earlier
4. Click **OK**.

To complete the RADIUS authentication configuration:

1. In R80 SmartConsole, create the required Access Control rules to allow access to users authenticated through the RADIUS server.
2. Verify that communication between the firewall and the server is not NATed in the Address Translation Rule Base.
3. Save the changes.
4. Close all R80 SmartConsole windows.
5. On the Security Management Server, use GuiDBedit to change the value of the **add_radius_groups** attribute from **false** to **true**.
6. Save and then close GuiDBedit.
7. Open R80 SmartConsole.
8. Install the policy.
9. On the RADIUS server, edit the RADIUS users to include a class RADIUS attribute on the users Return list that corresponds to the user group that they access.

To use a different attribute instead of the class attribute:
1. Close all R80 SmartConsole windows and clients.
2. On the Security Gateway, use GuiDBedit to modify the value of the firewall_properties attribute radius_groups_attr to the new RADIUS attribute.
3. Save.
5. Open R80 SmartConsole.
6. Install the policy.
7. On the RADIUS server, make sure that you use the same RADIUS attribute on users’ Return lists that corresponds to the Firewall user group that they access.

Modifying Encryption Properties for Remote Access VPN

The encryption properties of the users participating in a Remote Access community are set by default. If you must modify the encryption algorithm, the data integrity method and/or the Diffie-Hellman group, you can either do this globally for all users or configure the properties per user.

To modify the user encryption properties globally:
1. From Menu, click Global Properties.
2. From the navigation tree, click Remote Access > VPN- Authentication and Encryption.
3. From the Encryption algorithms section, click Edit.
   The Encryption Properties window opens.
4. In the IKE Security Association (Phase 1) tab, configure the applicable settings:
   - Support encryption algorithms - Select the encryption algorithms that will be supported with remote hosts.
   - Use encryption algorithms - Choose the encryption algorithm that will have the highest priority of the selected algorithms. If given a choice of more than one encryption algorithm to use, the algorithm selected in this field will be used.
   - Support Data Integrity - Select the hash algorithms that will be supported with remote hosts to ensure data integrity.
   - Use Data Integrity - The hash algorithm chosen here will be given the highest priority if more than one choice is offered.
   - Support Diffie-Hellman groups - Select the Diffie-Hellman groups that will be supported with remote hosts.
   - Use Diffie-Hellman group - SecureClient users utilize the Diffie-Hellman group selected in this field.
5. Click OK and publish the changes.
To configure encryption policies for specified users:

2. From the Encryption algorithms section, click Edit.
3. In the Encryption Properties window, click the IPSEC Security Association (Phase 2) tab.
4. Clear Enforce Encryption Algorithm and Data Integrity on all users.
5. Click OK and close the Global Properties window.
6. For each user:
   a) From the Objects Bar, double-click the user.
   b) From the navigation tree, click Encryption.
   c) Click Edit.
      The IKE Phase 2 Properties window is displayed.
   d) Click the Encryption tab.
   e) Click Defined below.
   f) Configure the Encryption Algorithm and Data Integrity.
   g) Click OK and close the User Properties window.
7. Publish the changes and install the policy.
Office Mode

In This Section:

- IP Pool Configuration ................................................................................................... 39
- DHCP Configuration ..................................................................................................... 40
- Use First Office Mode IP. ............................................................................................... 41
- Office Mode - Using a RADIUS Server ......................................................................... 41

IP Pool Configuration

Make sure that all the internal routers are configured to route all the traffic destined to the internal address space you had reserved to Office Mode users through the Security Gateway.

To deploy the basic Office Mode using IP pools:

1. From the Objects Bar click New > Network.
   The New Network window opens.
2. In the General tab, set the IP address pool range:
   a) Enter a Name for the network.
   b) In Network Address enter the first IP address.
   c) In Net Mask enter the subnet mask according to the required amount of IP addresses (entering 255.255.255.0, for example, will designate all 254 IP addresses from 10.130.56.1 to 10.130.56.254 for Office Mode addresses.)
   d) Click OK and publish the changes.
3. Click Gateways & Servers and double-click the Security Gateway.
   The gateway window opens and shows the General Properties page.
4. From the navigation tree, click VPN Clients > Office Mode.
5. Configure these settings:
   - In the Office Mode Method section, from Allocate IP from network select the IP Pool network object
   - Optional Parameters > IP lease duration - Enter the number of minutes that the IP address is used by the remote host
   - To allow routing to be done after the encapsulation of Office Mode packets, click Support connectivity enhancement for gateways with multiple external interfaces
   - To check that Office Mode packets are not spoofed, click Perform Anti-Spoofing on Office Mode addresses
6. Click OK and publish the changes.
7. If you completed configuring the settings for Office Mode, install the policy.
To specify which WINS and DNS servers Office Mode users can use:

**Note** - WINS and DNS servers should be set on the Security Management Server only when IP pool is the selected method.

1. Create a DNS server object.
   a) From the Objects Bar click New > Host.
   b) In the General page, enter the Object Name and IP address settings.
   c) In the Servers page, click DNS Server.
   d) Click OK.

2. Create a WINS server object.
   a) From the Objects Bar click New > Host.
   b) In the General page, enter the Object Name and IP address settings.
   c) Click OK.

3. Publish the changes.

4. Click Gateways & Servers and double-click the Security Gateway.
   The gateway window opens and shows the General Properties page.

5. From the navigation tree, click VPN Clients > Office Mode.

6. Click Optional Parameters.

7. For the DNS and WINS Servers, click Primary and select the server.

8. Click OK and publish the changes.

9. Install the Policy.

**DHCP Configuration**

To configure Office Mode with a DHCP server:

1. On your DHCP server’s configuration, make sure that you have designated an IP address space for Office Mode users (e.g., 10.130.56.0).

2. From the Objects Bar click New > Host.

3. Configure the settings for the name, IP address, and subnet mask.

4. Click OK and publish the changes.

5. Double-click the Remote Access gateway.
   The gateway window opens and shows the General Properties page.

6. From the navigation tree, click VPN Clients > Office Mode.

7. Configure these settings:
   - Click Automatic (use DHCP)
   - From Use specific DHCP server, select the DHCP server
   - In Virtual IP address for DHCP server replies, enter an IP address from the sub network of the IP addresses which are designated for Office Mode usage.

   Office Mode supports DHCP Relay method for IP assignment, so you can direct the DHCP server as to where to send its replies. The routing on the DHCP server and that of internal routers must be adjusted so that packets from the DHCP server to this address are routed through the Security Gateway.
• Optional: In the Additional IP addresses for Anti-Spoofing, select the network object you have created with the IP address range you have set aside for Office Mode on the DHCP server.

8. Click OK and publish the changes.

To create a new network object for Office Mode on the DHCP server:

1. From the Objects Bar click New > Network.
   The New Network window opens.
2. In Network Address enter the first address that is used (e.g. 10.130.56.0).
3. In Net Mask enter the subnet mask according to the amount of addresses that is used.
   For example, the IP address 255.255.255.0 designates that all 254 IP addresses from 10.130.56.1 until 10.130.56.254 are set aside for remote host Office Mode addresses on the DHCP server.
4. Click OK and publish the changes.
5. Install the Access Control policy.
6. Make sure that all the internal routers are configured to route all the traffic destined to the internal address space you had reserved to Office Mode users through the Security Gateway.
   For example, in the example above it is required to add routes to the class C sub network of 10.130.56.0 through the Security Gateway’s IP address.
7. Make sure that the remote access clients are also configured to use Office Mode.

Use First Office Mode IP

To configure all gateways to work in Office Mode:

1. From Menu, click Global Properties.
2. From the navigation tree, click Remote Access > VPN - Advanced.
3. In the Office Mode section, click Use first allocated Office Mode IP address for all connections to the Security Gateways of the site.
4. Click OK and publish the changes.

Office Mode - Using a RADIUS Server

To configure the RADIUS server to allocate IP addresses:

1. From the Objects Bar, click Servers > RADIUS.
2. Right-click the RADIUS server and select Edit.
   The RADIUS Server Properties window opens.
3. Click the Accounting tab.
5. Select the service the RADIUS server uses to communicate with remote users.
6. Click OK and publish the changes.
To configure the RADIUS server to perform authentication for remote users:

1. In R80 SmartConsole, click **Gateways & Servers** and double-click the Security Gateway. The gateway window opens and shows the **General Properties** page.

2. From the navigation tree, click **VPN Clients > Office Mode**.

3. In the **Office Mode Method** section, click **From the RADIUS server used to authenticate the user**.

4. Click **OK** and publish the changes.
Configuring the Gateway to Support the SSL Network Extender

**Note** - If the Mobile Access blade is active on a Security Gateway, SSL Network Extender works through Mobile Access and not IPsec VPN. In this case, SSL Network Extender must be configured through the Mobile Access blade. If you already had SSL Network Extender configured on an IPsec VPN Security Gateway and then you enable the Mobile Access blade, you must reconfigure SSL Network Extender for the Mobile Access blade.

Configure each Security Gateway that uses SSL Network Extender. When the Mobile Access Software Blade is enabled, SSL Network Extender is enabled as a Web client.

To configure the SSL Network Extender settings for a Security Gateway:

1. In R80 SmartConsole, click **Gateways & Servers** and double-click the Security Gateway. The gateway window opens and shows the **General Properties** page.
2. If Mobile Access is enabled:
   a) From the navigation tree, click **Mobile Access**.
   b) When **Web** is selected, SSL Network Extender is enabled.
3. From the navigation tree, click **VPN Clients**.
4. Click **SSL Network Extender**.
5. From **The gateway authenticates with this certificate**, select the certificate that is used to authenticate to all SSL clients.
6. Click **OK** and publish the changes.

Configuring SSL Network Extender

To configure the settings for SSL Network Extender connections:

1. From Menu, click **Global Properties**.
2. Select **Remote Access > SSL Network Extender**.
3. Select the user authentication method, employed by the SSL Network Extender, from the drop-down list. The options are:
   - **Certificate** - The system authenticates the user only with a certificate.
   - **Certificate with enrollment** - The system authenticates the user only with a certificate. Enrollment is allowed.
If the users do not have a certificate, they can enroll using a registration key that they previously received from the administrator.

- **Legacy** - [Default setting] The system authenticates the user with the **Username** and **Password**.
- **Mixed** - The system tries to authenticate the user with the certificate. If the user does not have a valid certificate, the system tries to authenticate the user with the **Username** and **Password**.

**Load Sharing Cluster Support**

The SSL Network Extender provides Load Sharing Cluster Support. When the client connects to the cluster, all its traffic will pass through a single Security Gateway. If that member Security Gateway fails, the client reconnects transparently to another cluster member and resumes the session.

**To provide Load Sharing Cluster Support:**

1. In R80 SmartConsole, click **Gateways & Servers** and double-click the cluster object.
   The cluster window opens and shows the **General Properties** page.
   **Note** - A Load Sharing Cluster must have been created before you can configure use of sticky decision function.
2. From the navigation tree, click **ClusterXL and VRRP**.
3. Make sure that **Load Sharing** is selected.
4. In the **Advanced Settings** section, click **Use Sticky Decision Function**.
5. If you are using Office Mode, configure these settings:
   a) From the navigation tree, click **VPNClients > Office Mode**.
   b) In the Office Mode Method section, make sure that **Automatic (using DHCP)** is NOT selected.
      Only the **Manual (using IP pool)** method is supported.
6. Click **OK** and publish the changes.
Remote Access Solutions for Different Deployments

In This Section:

- Configuring Desktop Security - Server Side ............................................................... 45
- Configuring Office Mode and L2TP Support ................................................................. 46
- Configuring the CA to Issue Certificates [L2TP] .......................................................... 46
- Configuring SCV - Server Side ..................................................................................... 47
- Configuring Client to Client Routing .......................................................................... 47
- Multiple External Interfaces ........................................................................................ 48
- Configuring Directional VPN with Remote Access Communities .............................. 48
- Authentication Timeout Interval .................................................................................. 49
- Configuring the SecuRemote DNS Server .................................................................. 49
- Proxy Replacement for the Security Gateway.............................................................. 50

Configuring Desktop Security - Server Side

To enable the gateway to be a Policy Server for Desktop Security:

1. Click Gateways & Servers and double-click the Security Gateway.
   The gateway window opens and shows the General Properties page.
3. Click OK and publish the changes.

To activate the Desktop Security policy:

1. Click Security Policies and open the Manage Policies window (CTRL + T).
2. Click the All icon.
3. Select the policy that you want to edit and click Edit.
   The policy window opens.
5. Click OK and publish the changes.

To configure the Desktop Policy rules:

1. Click Security Policies and from the navigation tree click Access Control > Desktop.
2. Click Open Desktop Policy in SmartDashboard.
   SmartDashboard opens and shows the Desktop tab.
3. Configure the inbound rules. Using the Rules>Add Rule menu item, you can add rules to the policy.
   In inbound rules, the SecureClient (the desktop) is the destination, and you can specify the users to which the rule is to be applied.
4. Configure the outbound rules.
   In outbound rules, the SecureClient (the desktop) is the source, and you can specify the users
   to which the rule is to be applied.
5. Click **Save** and close SmartDashboard.
6. Publish the changes and install the policy.
   Make sure that you install the Advanced Security policy on the Security Gateways and the
   Desktop Security policy on your Policy Servers.

### Configuring Office Mode and L2TP Support

**To configure L2TP support:**

1. Configure Office Mode (on page 39).
2. Click **Gateways & Servers** and double-click the Security Gateway.
   The gateway window opens and shows the **General Properties** page.
3. From the navigation tree, click **VPN Clients > Remote Access**.
4. Click **Support L2TP**.
5. Select the **Authentication Method** for the users:
   - To use certificates, choose **Smart Card or other Certificates (encryption enabled)**.
   - To use a username and a shared secret (password), choose **MD5-challenge**.
6. For **Use this certificate**, select the certificate that the Security Gateway presents in order to
   authenticate itself to users.
7. Click **OK** and publish the changes.

### Configuring the CA to Issue Certificates (L2TP)

**To configure the CA with the ICA Management Tool:**

1. Run the ICA Management tool:
2. Change the property **IKE Certificate Extended Key Usage** property to the value 1, to issue
   Security Gateway certificates with the "server authentication" purpose.
3. Change the property **IKE Certificate Extended Key Usage** to the value 2 to issue user
   certificates with the "client authentication" purpose.
   If you are using an OPSEC certified CA to issue certificates, use the **DBedit** command line or
   **GuiDBedit**, the graphical Database Tool to change the value of the global property
   **cert_req_ext_key_usage** to 1. This causes the Security Management Server to request a
   certificate that has purposes [Extended Key Usage extension] in the certificate.

**To configure the CA with R80 SmartConsole:**

1. Click **Gateways & Servers** and double-click the Security Gateway.
   The gateway window opens and shows the **General Properties** page.
2. From the navigation tree, click **IPsec VPN**.
3. In the **Repository of Certificates Available to the Gateway** section, click **Add**.
4. The **Certificate Properties** window opens.
5. Configure the settings for the certificate and click **OK**.
6. Select the certificate and click View.
7. Make sure that the Extended Key Usage Extension appears in the certificate.
8. From the navigation tree, click **VPN Clients > Remote Access**.
9. In the **L2TP Support** section, select the new certificate.
10. Click **OK** and publish the changes.

### Configuring SCV - Server Side

To configure SCV settings in Global Properties:

1. From Menu, click **Global Properties**.
2. From the navigation tree, click **Remote Access > Secure Configuration Verification (SCV)**.
3. Configure the settings:
   - **Apply Secure Configurations on Simplified Mode** - Specifies if SCV is applied to all remote access rules in the simplified policy mode.
   - **Upon Verification failure** - Specifies the action that is performed when the client fails one or more SCV checks. The options are to **Block** the client’s connection or to **Accept** it and send a log about the event.
   - **Basic configuration verification on client’s machine** - Specifies whether SecureClient performs SCV checks to determine if the policy is installed on all network interfaces cards on the client’s desktop, and if only TCP/IP protocols are installed on these interfaces.
   - **Configurations Violation Notification on client’s machine** - Specifies if a log record is saved on the Security Management Server machine indicating that a remote user is not verified by SCV (this is a general indication, without a specification of a certain SCV check the user’s desktop had failed).

4. Click **OK** and publish the changes.

### Configuring Client to Client Routing

R80 SmartConsole includes a default object for Office Mode IP addresses, **CP_default_Office_Mode_addresses_pool**. You can use the default object, or create a new one for your network.

To create a new Office Mode IP address object:

1. In R80 SmartConsole, click **Objects > Object Explorer** (Ctrl+E).
2. Click **New > Network**.
3. Enter the **Name**, **IP address** and **Net mask**.
4. Click **OK** and publish the changes.

To configure VPN routing for remote access clients with the VPN domain:

1. Create a network group, click **New > Network Group**.
2. Add these settings:
   - **VPN domain**
   - **Office Mode range**
   - **Encryption domain settings**
3. Click **OK** and publish the changes.
4. Click **Gateways & Servers** and double-click the Security Gateway. The gateway window opens and shows the **General Properties** page.
5. From the navigation tree, click **Network Management > VPN Domain**.
6. Click **Manually defined**.
7. Select the new network group.
8. Click **OK** and publish the changes. The remote clients must connect to the site and perform a site update before they can communicate with each other.

**Multiple External Interfaces**

To use multiple external interfaces with Remote Access clients:

1. Open R80 SmartConsole.
2. Click **Gateways & Servers** and double-click the Security Gateway. The gateway window opens and shows the **General Properties** page.
3. From the navigation tree, click **VPN Clients > Office Mode**.
4. In the **Multiple Interfaces** section, select **Support connectivity enhancement for gateways with multiple external interfaces**.
5. Click **OK**.
6. Install policy on the gateway.

**Configuring Directional VPN with Remote Access Communities**

To configure Directional VPN with Remote Access communities:

1. From Menu, click **Global Properties**.
2. From the navigation tree, click **VPN > Advanced**.
3. Click **Enable VPN Directional Match in VPN Column**.
4. Click **OK** and publish the changes.
5. Go to **Security Policies > Access Control Policy**.
6. Right-click the VPN cell for the rule, and select **Directional Match Condition**. The **New Directional Match Condition** window opens.
7. Configure the directional VPN:
   - From **Traffic reaching from**, select the source of the connection
   - From **Traffic leaving to**, select the connection’s destination
8. Click **OK** and publish the changes.
9. Install the policy.
Authentication Timeout Interval

For Connect Mode, the countdown to the timeout begins from the time that the Client is connected.

To specify the length of time between re-authentications:

1. From Menu, click Global Properties.
2. From the navigation tree, click Remote Access.
3. In the Authentication Timeout section, configure the setting:
   • Use default value
   • In Validation timeout every, enter the number of minutes between re-authentications
4. Click OK and publish the changes.

Configuring the SecuRemote DNS Server

Names in the domain that correspond to the rule that the SecuRemote DNS Server resolves. All other names are resolved by the SecuRemote client’s default DNS server.

To configure the object for the SecuRemote DNS Server:

1. In R80 SmartConsole, click Open Object Explorer (Ctrl+E).
2. Click New > Server > More > SecuRemote DNS.
   The SecuRemote DNS Properties window opens.
3. In the General tab, configure these settings:
   • Name of the SecuRemote DNS Server
   • Select the Host object for this server
4. In the Domains tab, click Add.
5. In Domain Suffix, enter the value that the SecuRemote DNS Server resolves to the internal names. For example, checkpoint.com
6. Configure the settings for the Domain Match Case.
   • Select Match only *.suffix to specify that the maximum number of labels resolved is 1.
     For example, if Domain Suffix is checkpoint.com and Match only *.suffix is selected, then the SecuRemote DNS Server resolves www.checkpoint.com and sample.checkpoint.com. It does not resolve www.internal.checkpoint.com
   • Select Match up to…labels preceding the suffix to increase the number of labels to be matched.
     For example, if Domain Suffix is checkpoint.com and Match up to…labels preceding the suffix is selected and set to 3, then the SecuRemote DNS Server used to resolves www.checkpoint.com and www.internal.checkpoint.com. It does not resolve www.internal.inside.checkpoint.com
7. Click OK and close the SecuRemote DNS Properties window.
8. Publish the changes.
Proxy Replacement for the Security Gateway

To configure the Security Gateway to support Visitor Mode:

1. From Menu, click **Global Properties**.
2. From the navigation tree, click **Advanced**.
3. In the **Advanced Configuration** page, click **Configure**.
   The **Advanced Configuration** window opens:
4. From the navigation tree, click **VPN Advanced Properties > Remote Access VPN**.
5. Select one of these options:
   - **ie_proxy_replacement** - When selected, Windows proxy replacement is always performed, even if Visitor Mode is not enabled
   - **ie_proxy_replacement_limit_to_tcpt** - When selected, the proxy replacement is only when Visitor Mode is enabled
### Index

**A**
- About this Guide • 6
- Advanced Permanent Tunnel Configuration • 25
- Authentication Timeout Interval • 49
- Authorizing Firewall Control Connections in VPN Communities • 12

**C**
- Certificate Revocation (All CA Types) • 18
- Configurable Objects in a Direction • 28
- Configuring a Meshed Community Between Internally Managed Gateways • 8
- Configuring a Star VPN Community • 9
- Configuring Anti-Spoofing on VTIs • 22
- Configuring Client to Client Routing • 47
- Configuring Desktop Security - Server Side • 45
- Configuring Directional VPN Between Communities • 29
- Configuring Directional VPN with Remote Access Communities • 48
- Configuring Directional VPN Within a Community • 29
- Configuring Explicit MEP • 13
- Configuring Implicit First to Respond • 13
- Configuring Implicit Load Distribution • 14
- Configuring Implicit Primary-Backup • 14
- Configuring IP Pool NAT • 15
- Configuring Link Selection and ISP Redundancy • 30
- Configuring Office Mode and L2TP Support • 46
- Configuring On Demand Links • 29
- Configuring RADIUS Objects • 35
- Configuring Remote Access VPN • 32
- Configuring RIM in a Star Community • 27
- Configuring SCV - Server Side • 47
- Configuring SSL Network Extender • 43
- Configuring the 'Accept VPN Traffic Rule' • 22
- Configuring the CA to Issue Certificates [L2TP] • 46
- Configuring the Gateway to Support the SSL Network Extender • 43
- Configuring the SecuRemote DNS Server • 49
- Configuring the Security Gateway for a Remote Access Community • 32
- Configuring Tunnel Features • 24
- Configuring Unnumbered VTIs • 23
- Configuring VPN between Internal Gateways with ICA Certificates • 19
- Configuring VPN between Internal Gateways with Third Party CA Certificates • 20
- Configuring VPN Routing for Security Gateways through R80 SmartConsole • 21
- Configuring VTIs in a Clustered Environment • 22
- Confirming a VPN Tunnel Successfully Opens • 10

**D**
- Defining a Remote Access Community • 32
- Defining Access Control Rules • 33
- Defining User Authentication Methods in Hybrid Mode • 34
- DHCP Configuration • 40
- DPD Responder Mode • 25

**E**
- Editing a Traditional Mode Policy • 19
- Enabling a User Certificate • 33
- Enabling Hybrid Mode and Methods of Authentication • 34
- Enabling Route Based VPN • 22
- Enabling the RIM_inject_peer_interfaces flag • 27
- Enabling Wire Mode on a Specific Security Gateway • 28
- Enabling Wire Mode on a VPN Community • 28
- Enrolling with a Certificate Authority • 16

**F**
- For Internally Managed Users • 34

**I**
- Important Information • 3
- Introduction to VPN • 8
- IP Pool Configuration • 39

**L**
- Load Sharing Cluster Support • 44

**M**
- Manual Enrollment with OPSEC Certified PKI • 16
- Migrating from Traditional Mode to Simplified Mode • 8
- Modifying Encryption Properties for Remote Access VPN • 37
- Multiple Entry Point for Site to Site VPN • 13
- Multiple External Interfaces • 48

**O**
- Office Mode • 39
- Office Mode - Using a RADIUS Server • 41

**P**
- Permanent Tunnel Mode Based on DPD • 26
- Permanent Tunnels • 24
- Proxy Replacement for the Security Gateway • 50
- Public Key Infrastructure • 16
R
R80 SmartConsole Toolbars • 6
Remote Access Solutions for Different Deployments • 45
Routing Return Packets • 15

S
Site to Site Solutions for Different Deployments • 21
SSL Network Extender • 43

T
Traditional Mode VPNs • 19
Trusting an Externally Managed CA • 17
Trusting an OPSEC Certified CA • 17

U
Use First Office Mode IP • 41
Using a Pre-Shared Secret • 34

V
VPN Community Object - Advanced Settings • 31
VPN Community Object - Encryption Settings • 30
VPN with External Security Gateways Using Certificates • 10
VPN with External Security Gateways Using Pre-Shared Secret • 11