How To Setup a Remote Access VPN
Important Information

Latest Software
We recommend that you install the most recent software release to stay up-to-date with the latest functional improvements, stability fixes, security enhancements and protection against new and evolving attacks.

Latest Documentation
The latest version of this document is at:
http://supportcontent.checkpoint.com/documentation_download?ID=12227
For additional technical information, visit the Check Point Support Center (http://supportcenter.checkpoint.com).

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>5/9/2011</td>
<td>First release of this document</td>
</tr>
</tbody>
</table>

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 How To Setup a Remote Access VPN).
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Important Information</td>
<td>3</td>
</tr>
<tr>
<td>How To Setup a Remote Access VPN</td>
<td>5</td>
</tr>
<tr>
<td>Objective</td>
<td>5</td>
</tr>
<tr>
<td>Supported Versions</td>
<td>5</td>
</tr>
<tr>
<td>Supported OS</td>
<td>5</td>
</tr>
<tr>
<td>Supported Appliances</td>
<td>5</td>
</tr>
<tr>
<td>Before You Start</td>
<td>5</td>
</tr>
<tr>
<td>Related Documentation and Assumed Knowledge</td>
<td>5</td>
</tr>
<tr>
<td>Impact on the Environment and Warnings</td>
<td>5</td>
</tr>
<tr>
<td>Setting Up Remote Access</td>
<td>6</td>
</tr>
<tr>
<td>Configuring Users and a Users Group</td>
<td>20</td>
</tr>
<tr>
<td>Creating Access Rules</td>
<td>26</td>
</tr>
<tr>
<td>Completing the Procedure</td>
<td>27</td>
</tr>
<tr>
<td>Verifying the Procedure</td>
<td>27</td>
</tr>
</tbody>
</table>
How To Setup a Remote Access VPN

Objective

This document covers the basics of configuring remote access to a Check Point firewall. It does not cover all possible configurations, clients or authentication methods. There are individual documents on advanced configurations such as multiple entry point (MEP), using active directory or radius and for each of the individual clients that can be used to connect.

Supported Versions

- NGX R60, R62, R65, R70, R71

Supported OS

- Any

Supported Appliances

- Any

Before You Start

Related Documentation and Assumed Knowledge

- General Firewall functionality
- VPN Admin Guide

Impact on the Environment and Warnings

- Configuration document, no impact
Setting Up Remote Access

To set up a remote access VPN:

1. In the General Properties window of your Security Gateway, make sure that the IPSec VPN checkbox is marked.

2. If the checkbox is not already marked, mark it and click OK. The following message is displayed:
Your security gateway object should now have a key symbol on the bottom right:

3. If you are using SecureClient and have desktop policy server license and want to use the desktop policy server, then mark the Policy Server checkbox under IPSec VPN.
4. Open the VPN tab on the gateway object. In the “This module participates in the following VPN Communities” section click Add and add the RemoteAccess community in the window that pops up.

5. Click OK. The RemoteAccess community should now be visible in the “This module participates in the following VPN Communities” section.
6. Click **Traditional mode configuration...** The Traditional mode IKE properties window is displayed.

![Traditional mode IKE properties window]

7. Make sure that the Exportable for SecuRemote/SecureClient checkbox is marked.
8. Click **OK**.
9. In the Link Selection section of the VPN tab on the gateway object, select the appropriate setting for link selection. This determines how the remote client determines what IP address to connect to. The Help button provides information on what each setting means.

In this example we are going to use Main address, which is the IP listed in general properties of the gateway object.

**Note** – Make sure that the “Main IP” listed in General Properties is not a Private IP address, as that is what IP address that the server will expect traffic on.
10. Open the Topology tab of the Gateway object. Click **Set domain for Remote Access Community**.

The default option uses the same VPN domain used for site-to-site VPN for the gateway. For most setups you can use the default here.

If you require a separate Remote Access VPN domain, click **Set** and put in the network or group you wish to use. For this example we will use the default setting.
Impact on the Environment and Warnings

### Setting Up Remote Access

#### Check Point Gateway - Corporate gw

**Topology**

<table>
<thead>
<tr>
<th>Name</th>
<th>IP Address</th>
<th>Network Mask</th>
<th>Topology</th>
</tr>
</thead>
<tbody>
<tr>
<td>eth0</td>
<td>143.100.75.1</td>
<td>255.255.255.0</td>
<td>External</td>
</tr>
<tr>
<td>eth1</td>
<td>172.16.2.1</td>
<td>255.255.255.0</td>
<td>This Network</td>
</tr>
<tr>
<td>eth2</td>
<td>172.16.1.1</td>
<td>255.255.255.0</td>
<td>Undefined</td>
</tr>
<tr>
<td>eth3</td>
<td>10.1.0.1</td>
<td>255.255.255.0</td>
<td>This Network</td>
</tr>
<tr>
<td>eth4</td>
<td>10.2.0.1</td>
<td>255.255.255.0</td>
<td>This Network</td>
</tr>
</tbody>
</table>

#### VPN Domain per Remote Access Community

For Remote Access Community traffic, set an alternative VPN Domain for this Gateway:

<table>
<thead>
<tr>
<th>Community</th>
<th>VPN Domain</th>
</tr>
</thead>
<tbody>
<tr>
<td>RemoteAccess</td>
<td>Same as Gateway</td>
</tr>
</tbody>
</table>

[Diagram of Check Point Gateway interface showing settings and topology options]
11. Open the Remote Access tab of the gateway object.

12. Mark the following checkboxes according to your system’s requirements:
   - **Allow SecureClient to route traffic through this gateway**
     If you want remote access clients to route traffic not meant for this gateway’s remote access VPN domain (for example, to the Internet) through the gateway.
   - **Support NAT traversal mechanism (UDP encapsulation)**
     Required for clients that are behind a hidden NAT device.
   - **Support Visitor Mode**
     If you are using SSL Network extender(SNX), SecureClient mobile or Endpoint Connect.

   **Note** – Click Help for detailed information on the meaning of each option.
13. Open the Remote Access tab of the gateway object and select the Office Mode tab. Office mode allows you to provide a unique IP address from which the remote access client will be sending. This allows you to prevent any overlap between the physical IP address of the remote access client and your Remote Access VPN domain.

**Note** – The default Office mode IP network is 172.16.10.0 /24. You have to ensure that the Office Mode Network is NOT already used inside of your network. If it is, you have to use/create a network not already used. The range selected for the office mode IP pool should not overlap with your internal networks or your Remote Access VPN domain.

14. Select the user group to which you are going to offer Office Mode. In this example Office Mode is offered to all users.
15. Chose the method to use to give out the office mode IP addresses. In this example the gateway assigns them manually via an IP pool defined on the gateway. You can also use a DHCP server to assign the IP addresses.

16. If you are using the IP Pool, click on **Optional Parameters** to configure DNS and WINS information to be sent to the client with its IP address.

17. Click **OK** to close the Optional Parameters button.
18. Open the Remote Access tab of the gateway object and select the VPN Clients tab.

19. If you are using SSL Network Extender or SecureClient Mobile mark those checkboxes.

20. If you are using Check Point Abra, mark the USB-1 checkbox.

21. Click OK to save the changes and close the object.
22. In SmartDashboard go to Policy->Global Properties. In the Firewall Implied Rules section make sure that the Accept control connections and Accept Remote Access control connections checkboxes are both marked.
23. In SmartDashboard go to Policy->Global Properties->Remote Access. There are a number of settings here but for this document we are concerned with VPN – IKE (Phase 1) and VPN – IKE (Phase 2).
24. Select the Encryption Algorithm and Data Integrity methods you want to support for your remote access users.

**Note** – You can select several for Phase 1, but only one the Encryption Algorithm and one Data Integrity method for Phase 2.
Configuring Users and a Users Group

To configure some users:
1. In SmartDashboard Select the Users tab. Then go to Users->New User->Standard_User.
2. Supply a login name for the user.

3. On the authentication tab select Check Point Password and then enter and confirm the password for the user.
To configure a remote access users group:

1. In SmartDashboard on the Users and Administrators tab, go to User Groups->New Group

![SmartDashboard screen showing the process of configuring a remote access users group.]

2. Give the group a descriptive name and put the required users in this group.

![Group Properties window showing the process for adding users to the group.]

1. Name: remote_users
2. Comment: 
3. Color: 
4. View: All
5. Not in Group:
   - Clientless-vpn-user
   - Customers
   - L2TP-vpn-user
   - Mobile-vpn-user
   - Partners
   - URL-bypass-group

6. In Group:
   - John

OK  Cancel  Help
To edit the remote access VPN community:

1. In SmartDashboard from the Manage menu, select VPN Communities.

2. Select the Remote Access community.
3. In the Remote Access Community make sure that your gateway shows in the Participating Gateways tab.
4. In the Participating User Groups tab select the group for which you want to allow remote access.

5. Click OK to exit and save the Remote Access VPN community.
Creating Access Rules

Now we need to create rules to allow the remote access users access to the permitted internal networks.

To create a security rule:
1. From SmartDashboard in the source column, right-click and select Add User Access.
2. Select the user group you put into the remote access community participating user groups.
3. In the DESTINATION select the network or group of networks in your Remote Access VPN domain to which you want to allow your users access.
4. In the VPN column select the Remote Access VPN community.
5. In the SERVICE column select the services you want to allow to remote access users.
6. In the ACTION column select accept.

When done the rule should look similar to this.
Completing the Procedure

Install the policy to gateway.

Verifying the Procedure

Verify you are able to make a remote access connection, get an Office Mode IP (if applicable) and access internal resources.