How To Setup a Site-to-Site VPN with a Remotely Managed Check Point Gateway

2 February 2011
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=11928
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>1/31/2011</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 Site-to-Site VPN with a Remotely Managed Check Point Gateway).
# 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 Site-to-Site VPN with a Remotely Managed Check Point Gateway</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>Setup Procedure</td>
<td>6</td>
</tr>
<tr>
<td>Creating an ICA Certificate</td>
<td>6</td>
</tr>
<tr>
<td>Setting up Your VPN</td>
<td>7</td>
</tr>
<tr>
<td>Defining Your VPN Domains</td>
<td>12</td>
</tr>
<tr>
<td>Example</td>
<td>13</td>
</tr>
<tr>
<td>Completing the Procedure</td>
<td>16</td>
</tr>
<tr>
<td>Verifying</td>
<td>16</td>
</tr>
</tbody>
</table>
How To Setup a Site-to-Site VPN with a Remotely Managed Check Point Gateway

Objective
This guide shows you how to set up a simple site-to-site VPN with another Check Point gateway, which is not managed by the same management server.

Supported Versions
- R55, R60, R61, R62, R65, R70, R71

Supported OS
- All

Supported Appliances
- All

Before You Start

Related Documentation and Assumed Knowledge
- Network of the remote site
- Negotiation properties you will use

Impact on the Environment and Warnings
- Ensure you have a good understanding of your topology, as mis-configuring a VPN can cause major communication issues on your network.
Creating an ICA Certificate

1. In the General Properties window of your Security Gateway, ensure that the IPSec VPN check box is marked.

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

The next step is to set up your VPN.

**Setting up Your VPN**

Once an ICA certificate has been created, you are ready to setup the VPN.

**To setup your VPN:**

1. Create an object to represent the peer gateway. In the left-hand panel select Network Objects and right-click and select:
   
   New > Others > Interoperable Device
2. A properties dialog popup is displayed. For now, give the gateway a name, IP address, and description (optional).

![Properties dialog popup](image1)

3. From the IPSec VPN tab in your SmartDashboard, right-click in the open area on the top panel and select:
   **New Community > Star.**

![SmartDashboard](image2)

4. The Star Community Properties popup is displayed. In the first window, give your VPN community a name:

![Community Properties](image3)

5. Select Center Gateways on the left. Click Add below the empty box and select your local Check Point gateway object. Click **OK.**

![Gateway selection](image4)
6. Select Satellite Gateways on the left. Click Add below the empty box and select the peer gateway object. Click OK.

7. Select VPN Properties on the left. You can change the Phase 1 and Phase 2 properties here. Take note of the values you select because the peer will need to match these values.
8. Select Tunnel Management on the left. Here, you can define how you want the tunnel to be setup. The recommended tunnel sharing method is: One VPN tunnel per subnet pair. This will share your network on either side of the VPN. Selecting this makes the phase 2 negotiation smooth and requires less tunnels to be built for the VPN. If you need to restrict access over the VPN, you can do that later through your security rulebase.

9. Expand Advanced Settings on the left and select Shared Secret. Mark the Use only Shared Secret for all External members check box. Select your peer gateway in the list below and click Edit to edit the shared secret. Remember this secret as your peer will need it to set up the VPN on the other end.
10. Select Advanced VPN Properties on the left. Here, you can modify the more advanced settings regarding phase 1 and 2. Keep note of these values. It is also a good idea to mark the Disable NAT inside the VPN community check box, as then you can access resources behind your peer gateway using their real IP addresses, and vice versa.

11. Click OK on the VPN community properties dialog to exit back to the SmartDashboard. You may see the following message:

12. Click Yes to continue. Now you can see your VPN community defined:
The next step is to address the VPN domain setup.

**Defining Your VPN Domains**

If you have not already done so, create network objects to represent your local networks and your peer's networks that they will be sharing.

**To create network objects for the peer:**

1. Right-click on Networks under the Network Objects list in the left-hand panel and click Network to define a new network.
   In the following image, create a network to represent your peer's internal network that they will be sharing with the previously defined local network:

2. If you or your peer are sharing more than one network over the tunnel, create groups to represent each side's VPN domain. Under the Network Objects list in the left-hand panel, right-click Groups, select Groups > Simple Group...
Example:

This example is for only sharing one network, so the group will only have one object included, but you can put as many networks in this group as you would like to share. It is important to not add groups within a group as this can impact performance.

- Make sure the group is "flat".
- Give your group a meaningful name, such as: "Local_VPN_Domain".

**To create a group to represent your peer's shared networks:**

- Click OK once you have added all of your local networks and then repeat the procedure to create a group to represent your peer's shared networks.
To set the VPN domains for each of the gateways:

1. Open the properties for your local Check Point gateway object. Select Topology on the left. In the VPN Domain section, mark the Manually defined check box, and from the drop-down list, select your Local VPN domain group object.

2. Click OK to save the object and open the properties for the peer gateway and select the group/network that represents its VPN domain:

3. Click OK to complete the peer gateway configuration.
To create a rule for the traffic:

Now, you have both objects setup for VPN and you have defined your community. You need to create a rule for the traffic. Here is where you should restrict access if required.

1. Decide where in your rulebase you need to add your VPN access rule and right click the number on the rule just above where you want it and select: **Add Rule > Below**.

In this example, we are allowing any service across the tunnel in both directions.
2. You should also explicitly set the VPN community in the VPN column on your rule. To do this, right-click the Any Traffic icon in the VPN column and select: Edit Cell.... Select the option button for “Only connections encrypted in specific VPN Communities” and click Add. Select your VPN community (created in the above steps) and click OK and then OK again.

Now, your rule should show the VPN community in the VPN column.

Completing the Procedure

- Install the policy to your local Check Point gateway. The VPN is now setup.
- Once the remote side has setup their VPN to match, you should have secure communication with their site.

Verifying

- Verify that you can initiate and receive secure communication with the remote site.