How To Troubleshoot VPN Issues in Site to Site

29 December 2010
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=11841
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>12/29/2010</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 Troubleshoot VPN Issues in Site to Site ).
## 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 Troubleshoot VPN Issues in Site to Site</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>Troubleshooting VPN issues in Site to Site</td>
<td>6</td>
</tr>
<tr>
<td>New Installation Checklist</td>
<td>6</td>
</tr>
<tr>
<td>Failed Upgrade to R70</td>
<td>11</td>
</tr>
<tr>
<td>Issue:</td>
<td>11</td>
</tr>
<tr>
<td>Issue:</td>
<td>11</td>
</tr>
<tr>
<td>Issue:</td>
<td>11</td>
</tr>
<tr>
<td>Issue:</td>
<td>11</td>
</tr>
<tr>
<td>Previously Working Installations</td>
<td>12</td>
</tr>
<tr>
<td>Issue:</td>
<td>12</td>
</tr>
<tr>
<td>Issue:</td>
<td>12</td>
</tr>
<tr>
<td>Issue:</td>
<td>12</td>
</tr>
<tr>
<td>Issue:</td>
<td>12</td>
</tr>
<tr>
<td>Completing the Procedure</td>
<td>13</td>
</tr>
<tr>
<td>Verifying</td>
<td>13</td>
</tr>
</tbody>
</table>
How to Troubleshoot VPN Issues in Site to Site

Objective
This document provides troubleshooting steps for site to site connections with Check Point gateways. It addresses site to site VPN troubleshooting in simplified mode only.

Supported Versions
- R65, R70

Supported OS
- SecurePlatform, Windows

Supported Appliances
- All gateway appliances

Before You Start

Related Documentation and Assumed Knowledge
- Basic understanding of network and security concepts/terminology. For example: IPSec, TCP/IP, routing, firewall, etc.
- VPN administration guides:
  - R70:
    - http://supportcontent.checkpoint.com/documentation_download?id=8751
    - http://supportcontent.checkpoint.com/documentation_download?id=8751
  - R65:
    - http://supportcontent.checkpoint.com/documentation_download?id=7261
    - http://supportcontent.checkpoint.com/documentation_download?id=7261

Impact on the Environment and Warnings
- Be aware that changing VPN configuration on the management and installing the changes on the security gateways may effect currently established VPN tunnels. Check carefully if the change you are applying, is related to live VPN tunnels.
- It is advised to make all changes during a maintenance window.
Troubleshooting VPN issues in Site to Site:

In this section

- New Installation Checklist
- Failed Upgrade to R70
- Previously Working Installations

New Installation Checklist

Note: The steps in this section are relevant only for new installations, not for an existing one that has previously worked.

If your configuration:

- Stopped working after being upgraded to R70, please skip to: Failed Upgrade to R70 (on page 10)
- Worked before, please skip to: Previously Working Installations (on page 11)

To verify that settings have been setup correctly:

1. Verify both gateways are in the same community:

![Image of the Meshed Community Properties window showing Participating Gateways with two selected gateways: Corporate Cluster 1 and Remote-1-gw]
2. If the gateway is externally managed, verify the following:
   
   a) If shared secret is used, verify that it is properly entered on both sides:

   b) If a certificate is used, verify that the certificate authority is properly defined:
c) Verify that tunnel settings in the VPN community (negotiation times, encryption algorithms, data hashing algorithms) are the same on both ends:
New Installation Checklist

Troubleshooting VPN issues in Site to Site: Page 9
3. Verify gateway encryption domain and topology are properly set:

If the issue is still not resolved, contact the Check Point Support Center.
Failed Upgrade to R70

After upgrading previous version of Check Point gateway/SmartCenter to R70 and above, several manually edited configuration files are returned to their default settings, thus causing some VPN configurations to malfunction.

The common issues are described below:

**Issue:**
- `vpn_route.conf` – setting are not passed correctly to the upgraded SmartCenter/gateway.

**Potential Solution:**
- The file needs to be modified again. You can use the same syntax used in R65. If file modification issues are encountered, refer to sk31021 (http://supportcontent.checkpoint.com/solutions?id=sk31021)

**Issue:**
- You would like to exclude specific address from encryption domain (like peer GW IP), and you are using R70 or above – user.def is irrelevant in this case under R70.

**Potential Solution:**
- In SmartCenter Server add the following lines at the end of the file:

  ```
  $FWDIR/lib/crypt.def:
  #define NON_VPN_TRAFFIC_RULES \
  (dst=x.x.x.x)
  ```

  The address ‘x.x.x.x’ is the IP address of the remote peer which should be excluded from the VPN-1 gateway's remote encryption domain.
  
  Push the policy to VPN-1 gw

  Check that there are proper NAT rules for hide-NATing the internal source addresses when accessing the remote peer address in clear from the VPN-1 site (e.g. NAT rule with src=internal net, dst=x.x.x.x -> src=hide behind fw external address, dst=origin)

**Issue:**
- `user.def` – previous modifications done in R65 in user.def that set max_subnet_per_range are not saved.

**Potential Solution:**
- The change in R70 must be applied in user.def.NGX_FLO. Policy installation must be performed afterwards.

**Issue:**
- VPND crashes or causes very high CPU consumption in R70 when using manually modified ipassigmet.conf.

**Potential Solution:**
- sk41786 (http://supportcontent.checkpoint.com/solutions?id=sk41786)
Previously Working Installations

To troubleshoot VPN issues on a previously working installation:

- Initiate VPN connectivity attempt by sending traffic from one site to another.
- Review SmartView tracker for potential errors. Based on that, review the common issues and their troubleshooting steps listed below:

**Issue:**

- Site to site VPN connections between VPN-1 Power/UTM Security Gateways, configured as Center Gateways in Star VPN Community, not being encrypted.

**Potential Solution:**


**Issue:**

- Site-to-site VPN using certificates issued by the ICA (Internal Certificate Authority) fails with error

**Potential Solution:**


**Issue:**

- After upgrade to R70 site to site VPN fails with "authentication error" message in SmartView tracker.

**Potential Solution:**

- Shared secret did not move in the upgrade process. Redefine the shared secret for the peer gateway.

**Issue:**

- Traffic is dropped inside a VPN tunnel with the error: "packet should not have been decrypted".

**Potential Solution:**

- Consider the following scenario:

  GW1======VPN======GW2
  ||
  ||
  Mgmt1 mgmt2

  On gateway 1, traditional policy is installed which encrypts all services from GW1 encryption domain to GW2 encryption domain. On gateway 2 simplified policy installed to allow encrypted traffic between the two gateways, however in the community settings there are several excluded services configured.

  The excluded services that are encrypted by GW1 are in the excluded services on GW2, hence the error "packet should not have been decrypted”. GW2 thinks that this packet shoud have come in clear and not encrypted.

  To fix this - take the relevant service out of the excluded services so that the configuration matches what is configured on GW1.
Issue:

- VTI error "encryption failure: Clear text packet should be encrypted"

Potential Solution:

- Edit the $FWDIR/conf/vpn_route.conf file on the SmartCenter, and declare each gateway's local domain to itself.

Example:

Suppose you have two gateways or clusters with VTI tunnels configured. One is named "satellite" and the other is named "center"

Create two groups. One group will contain all of the "satellite" internal networks that participate in the tunnel, and the other group will contain all of the "center" internal networks that participate in the tunnel.

Call these groups: "center_nets" and "satellite_nets"

Configure vpn_route.conf as such:

```
# destination router install_on

center_nets center center
satellite_nets satellite satellite
```

- In case the suggested steps fail to resolves the issue:
  Refer to sk34467 (http://supportcontent.checkpoint.com/solutions?id=sk34467)
  Gather the troubleshooting information described in the SK, and contact Check Point support.

Completing the Procedure

- After each Smart Dashboard modification, push the policy.

Verifying

- Ensure you can communicate between the sites both ways.