How To Troubleshoot VPN Issues with Endpoint Connect

26 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=11810
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>12/26/2010</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 with Endpoint Connect ).
Contents

Important Information.................................................................3
How To Troubleshoot VPN Issues with Endpoint Connect ..................5
  Objective .................................................................................5
  Supported Versions ..................................................................5
  Supported OS .........................................................................5
  Supported Appliances .............................................................5
Before You Start ........................................................................5
  Related Documentation and Assumed Knowledge .........................5
  Impact on the Environment and Warnings ..................................6
New Installation Checklist................................................................7
  Step 1 - Checking GW Readiness .............................................7
  Step 2 - Checking GW Configuration .........................................9
Previously Working Installations..................................................15
  Problem Types: ........................................................................15
  Error Upon Connection ............................................................15
  Issues Covered: .........................................................................15
  Issue: .....................................................................................15
    Potential Solution: ...............................................................15
  Issue: .....................................................................................15
    Potential Solution: ...............................................................15
  Issue: .....................................................................................16
    Potential Solution: ...............................................................16
  Issue: .....................................................................................16
    Potential Solution: ...............................................................16
  Connectivity Stability – Disconnecting ........................................16
  Issue: .....................................................................................16
    Potential Solution: ...............................................................16
  Issue: .....................................................................................17
    Potential Solution: ...............................................................17
  Connection Takes Too Long ......................................................17
  Issue: .....................................................................................17
    Potential Solution: ...............................................................17
Completing the Procedure ..........................................................17
Verifying .....................................................................................18
How To Troubleshoot VPN Issues with Endpoint Connect

Objective

The objective of this document is to describe troubleshooting steps for Endpoint Connect VPN client. This document shall assist in troubleshooting connectivity and/or performance issue with Check Point VPN client – Endpoint Connect.

Supported Versions

- R65 HFA 40 and above

Supported OS

- Windows 2000 Professional 32-bit with SP1-4
- Windows XP Home & Professional 32-bit, with or without SP1-3
- Windows Vista 32-bit and 64-bit, with or without SP1
- Windows 7 32-bit and 64-bit, Premium or Enterprise

Supported Appliances

- All Check Point supported appliances.

Before You Start

Related Documentation and Assumed Knowledge

This document assumes that the reader has reviewed the following Endpoint Connect Admin Guides:

- NGX R65.4 Endpoint Connect Admin Guide
  http://dl3.checkpoint.com/paid/72/CP_NGX_R65.4_(HFA40)_Endpoint_Connect_AdminGuide.pdf?HashKey=1273927113_171cc1d38ce54391418044700c7aae36&xtn=.pdf

- NGX R66 HFA01 Endpoint Connect User Guide

It is also assumed that the reader has a basic understanding of networking and VPN terminology: encryption domain, IPsec, etc.
Impact on the Environment and Warnings

- N/A
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 has worked before, please skip to Previously Working Installations.

To verify that EndPoint connect has been setup correctly:

- Carry out Steps 1 and 2 in this section.
- If the issue is still not resolved, contact Check Point Support Center

Step 1 - Checking GW Readiness

To check gateway readiness:

1. Verify that the version installed on the gateway and Smart Center is NGX R65 HFA 40 at least.
2. Make sure Connectra plug-in is installed on the Smart Center - Connectra_NGX_R66_CD2_Plug-in. (not relevant for R70 and above)

If you do not wish to install Connectra plug-in, or you use R70, you can manually edit the data base to add Endpoint Connect features:

To configure these properties you need to manually:
Edit the trac_client_1.ttm file on the gateway.

To manually configure the gateway for Endpoint Connect:

a) Open $FWDIR/conf/trac_client_1.ttm for editing.

Note - On Windows, use notepad to edit the file. Wordpad and other word processors alter the file formatting. All the settings for Endpoint Connect features (smartcard removal, tunnel idleness, location awareness and so on) are found in this file.

b) Enable those features relevant for your deployment.

c) Save and close the file.

d) Install a policy or run: cpstop, cpstart.
3. Make sure that the relevant database changes were performed using GuidbEdit:
   a) Open GuidbEdit, and connect to SmartCenter server
   
   b) In the **Tables** tab, select **Network Objects**.
   
   c) In the **Object Name** window, select the object that represents the gateway.
   
   d) In the **Field Name** table:
      (i) Locate the **vpn_clients_settings_for_gateway**
      (ii) Select the row and right-click
      (iii) Select **Edit**, and click OK to confirm the setting
      (iv) Locate the **endpoint_vpn_client_settings_for_gateway** property
         
         **Enabling Endpoint Connectivity**
         
         (v) Select the row and right-click
         
         (vi) Select **Edit** and click OK to confirm the setting.
         
         (vii) Select the **endpoint_vpn_connection_method** property
         
         (viii) Select **Edit** and change the value to **IPSEC**
         
         (ix) Select the **endpoint_vpn_enable** property
         
         (x) Select **Edit** and change the value to **True**
         
         (xi) Save changes
         
         (xii) Exit GuidbEdit
   
   e) Open SmartDashboard.
      You will be prompted to download a new version of SmartDashboard.
   
   f) Using the new SmartDashboard, configure the gateway for Endpoint connectivity.
   
   g) Install policy.
Step 2 - Checking GW Configuration

To check the gateway configuration:
Verify the configuration below (required for Endpoint Connect clients to work properly):
1. In SmartDashboard, open the **General Properties** window for the gateway.
2. Enable VPN:
   - For version R65:
   - For version R70:
3. On the **Topology** page, create a VPN domain:

4. On the **VPN > VPN Advanced** page, enable NAT Traversal:
5. On the **Remote Access** page, enable Visitor Mode:

![Remote Access settings](image)

6. On the **Remote Access > Office Mode** page enable Office Mode and configure the appropriate settings:

![Office Mode settings](image)

7. On the **Remote Access > SSL Clients** page enable SSL clients:
   
   For version R65:
Step 2 - Checking GW Configuration

For version R70:
8. Endpoint Connect does not support the DES encryption algorithm. If you have a gateway configured to support only the DES encryption algorithm, then reconfigure the settings in Global Properties > Remote Access VPN-IKE (phase1):
Previously Working Installations

Problem Types:
- Error upon connection
- Connectivity stability – disconnecting
- Connection takes too long

Error Upon Connection

Issues Covered:
- Endpoint Connect error: "Connection failed: Failed to download topology"
- Endpoint connect fails to connect to the gateway with error: "Page Not Found"
- Endpoint Connect fails to connect with error: "Client Encryption: No proposal chosen"

Issue:
- Endpoint Connect error: "Connection failed: Failed to download topology"

Potential Solution:
Symptoms:
Endpoint Connect fails to connect to the VPN-1 gateway with error: "Connection failed: Failed to download topology"
IKE Main Mode, Connect Mode, and Quick Mode complete successfully, then the client sends a phase1 delete message to the VPN-1 gateway.

Cause:
User is authenticating with a pre-shared secret.

Solution:
Endpoint Connect fails to download topology if the user authenticates with an IKE pre-shared secret. This issue is under investigation.

Workaround: Configure the user object with a Check Point password under the "Authentication" tab and remove the pre-shared secret under the "Encryption" tab.

Issue:
- Endpoint Connect fails to connect to the gateway with error: "Page Not Found"

Potential Solution:
Symptoms:
When trying to connect to the gateway with Endpoint connect, the connection fails with the message: "page not found" although that port is allowed by the gateway policy.
Cause:

Webui is enabled on port 443
If you run the command:

```
netstat -nap| grep 443
```
You will see that the `cp_http_server` process is running on that port:

```
tcp 0 0 0.0.0:443 0.0.0:* LISTEN 3611/cp_http_server
```

Endpoint Connect uses port 443 in order to authenticate the users during the IKE negotiation therefore the webui port needs to be changed.

Solution:

Change the webui port using the command:

```
# webui enable [put a different port number here]
```
or disable the webui using the command:

```
# webui disable
```

Then, verify that `VPND` runs on that port with the command:

```
# netstat -nap | grep 443
```

Issue:

- Endpoint Connect fails to connect with error: "Client Encryption: No proposal chosen"

Potential Solution:

Symptoms:

When trying to establish a VPN tunnel using Endpoint Connect client, the client says "Authentication succeeded" and right after that "Connection Failed: The user is not defined properly."

SmartView Tracker shows main mode completion and then shows an IKE failure error: "reason: Client Encryption: No proposal chosen".

Cause:

Phase 2 encryption settings were set for DES.

Endpoint Conenct requires strong encryption, changing it for 3DES solves the issue.

Solution:

Change settings as above, no fix is required.

Connectivity Stability – Disconnecting

Issue:

- Disconnection/reconnection of Endpoint Connect every 20 seconds

Potential Solution:

Symptoms:

You are able to establish a tunnel, but 20 seconds after the connection, the Endpoint received a reconnection notification.

- The configuration in both the Endpoint side and the gateway side seems correct, tunnel idleness parameters were not configured in client side and are correct in server side.
- 10 seconds after the disconnections, the tunnel is established again.
Issue:

Cause:
This is a misconfiguration of the gateway (not a bug).

Solution:
In Global Properties >> Firewall, under the Firewall Implied Rules section, check the “Accept Control Connections” option.

Issue:

- When DHCP server is used to provide Office Mode IPs, Endpoint Connect client disconnects after 15 minutes

Potential Solution:
See sk43615 http://supportcontent.checkpoint.com/solutions?id=sk43615

Connection Takes Too Long

Issue:

- Endpoint Connect takes 30 seconds to connect.

Potential Solution:

Symptoms:
- In some cases EPC take longer time to establish VPN connection to the gateway as the VNA takes more time to load.

Cause:
The OM IP assignment has been delayed.

Solution:
A new attribute was added to allow the administrator to control the time the client waits for the OM assignment before it assigns it statically. (The IP is still received from the gateway but the difference is the way the IP is assigned in the VNA).
After installing the client build that supports it, add the following lines on the gateway:

```plaintext
$FWDIR/conf/trac_client_1.ttm
:neo_static_ipassignment_timeout {
    :gateway {endpoint_vpn_Static_ipassignment_timeout
        :default (1)
    }
}
```

In this example the VNA will get an IP after 1 second. (Before that attribute has been added, the default value was 30 seconds).

Completing the Procedure

- Install a policy, to verify all changes are implemented on the gateway.
Verifying

- Connectivity can be verified by pinging/trying to access a resource in the internal network.