## Contents

### Chapter 1  
**Getting Started**
- Introduction ...................................................................................................... 7
- Installing .......................................................................................................... 8
- Enabling Endpoint Connectivity........................................................................... 9

### Chapter 2  
**Endpoint Connect**
- Introduction .................................................................................................... 11
  - Why Endpoint Connect?............................................................................... 11
  - Capabilities ................................................................................................ 12
  - Installation and Use .................................................................................... 14
  - Administration ............................................................................................ 14
- Configuring the Gateway Using SmartDashboard ................................................. 15
  - Obligatory Settings.................................................................................. 15
  - Endpoint Connect Advanced Settings....................................................... 20
- Manually Configuring the Gateway for Endpoint Connect .................................... 25
- Configuring Optional Endpoint Connect Settings ................................................. 26
  - Link Selection and MEP ........................................................................... 26
  - Hub Mode ................................................................................................. 27
  - Secure Configuration Verification............................................................ 29
  - Authentication Time-out ........................................................................ 29
  - Working with RSA Hard and Soft Tokens ............................................... 31
  - Configuring Logging Options for Client Users ......................................... 32
  - Disabling CAPI Authentication .................................................................. 32
  - Disabling DNS-based Geo-Cluster Name Resolution ................................... 33
  - NAT Traversal .......................................................................................... 34
  - Smart Card Removal Detection .................................................................... 35
  - Tunnel Idleness ........................................................................................ 35
- Using the Packaging Tool ................................................................................. 38
Chapter
Getting Started

In This Chapter:

Introduction  page 7
Installing  page 8
Enabling Endpoint Connectivity  page 9

Introduction

HFA40 for R65 gateways delivers Connectra NGX R66 remote client enhancements to NGX R65 gateways and SmartCenter servers, for example Endpoint Connect. Endpoint Connect is Check Point's new lightweight remote access client. Providing seamless, secure (IPSec) VPN connectivity to corporate resources, the client works transparently with VPN-1 and Connectra gateways.
Installing

To install:

1. On SmartCenter server, install the Connectra plug-in:
   Connectra NGX R66 CD2 Plug-in.iso.

2. On the VPN-1 NGX R65 gateway, install HFA40.

While it is recommended to install both, it's also possible to install just HFA40 on the gateway without updating the SmartCenter server database schema with the Connectra NGX R66 plug-in. To configure Endpoint Connect properties, a file on the gateway has to be manually edited. See “Manually Configuring the Gateway for Endpoint Connect” on page 25 for more information.
Enabling Endpoint Connectivity

To enable Endpoint Connect connectivity with the gateway:

1. Open **GuiDBedit**, and connect to SmartCenter server, as shown in Figure 1-1:

**Figure 1-1** GuiDBedit

![GuiDBedit](image)

2. On the **Tables** tab, select **Network Objects**.

3. In the **Object Name** window, select the object that represents the R65 gateway.
   (cpmodule in Figure 1-1).

4. In the **Field Name** table:
   a. Locate the **vpn_clients_settings_for_gateway**
   b. Select the row and right-click
   c. Select **Edit**, and click **OK** to confirm the setting.
   d. Locate the **endpoint_vpn_client_settings_for_gateway** property
Enabling Endpoint Connectivity

e. Select the row and right-click
f. Select Edit and click OK to confirm the setting.
g. Select the `endpoint_vpn_connectivity_method` property
h. Select Edit and change the value to IPSEC.
i. Select the `endpoint_vpn_enable` property
j. Select Edit and change the value to True.
k. Save changes.
l. Exit GuiDBEdit.

5. Open SmartDashboard.
   You will be prompted to download a new version of SmartDashboard.

6. Using the new SmartDashboard, configure the gateway for Endpoint connectivity. (See “Configuring the Gateway Using SmartDashboard” on page 15)

7. Install the policy.
Chapter 2
Endpoint Connect

In This Chapter:

- **Introduction** page 11
- **Configuring the Gateway Using SmartDashboard** page 15
- **Manually Configuring the Gateway for Endpoint Connect** page 25
- **Configuring Optional Endpoint Connect Settings** page 26
- **Using the Packaging Tool** page 38

This chapter explains how to configure the VPN-1 gateway to work with Endpoint Connect.

**Introduction**

Endpoint Connect is Check Point's new lightweight remote access client. Providing seamless, secure (IPSec) VPN connectivity to corporate resources, the client works transparently with Connectra R66 and VPN-1 NGX R65 gateways.

**Why Endpoint Connect?**

With their requirement to repeatedly reconnect and authenticate to the corporate gateway, traditional IPSec clients can be slow and cumbersome. Even SSL VPNs with their explicit login requirements through a browser, are a less than optimal solution for highly mobile laptop users.
Capabilities

Providing a highly secured, low footprint VPN technology with advanced security scanning capabilities, Endpoint Connect uses intelligent Auto-Connect and roaming technologies to facilitate seamless and transparent interaction with the gateway at the perimeter of the corporate network.

Designed for corporate users who prefer to use their native desktop to launch business applications rather than the Connectra SSL portal, Endpoint Connect users do not have to authenticate each time they connect. Through interface roaming technologies, client users are always connected to the resources available behind the gateway. As corporate users move around, an auto connect mode discovers whether users are outside of a secure environment, and implements the best way to connect, using either NAT-T or Visitor Mode. In practical terms, if client users outside of the internal network open their mail programs a connection is transparently established to the mail server behind the gateway. If client users have mapped drives to servers on the internal network, those mapped drives remain functional even as users roam in and out of the network.

Note - While Endpoint Connect can reside on the same host with SecureClient or Endpoint Security, users should avoid connecting with the two VPN clients to the same network at the same time

Capabilities

Resident on the users desktop or laptop, Endpoint Connect provides various capabilities for connectivity, security, installation and administration.

Connectivity

• Network Layer Connectivity
  An IPSec VPN connection to the gateway for secure encrypted communication. If the network connection is lost, the client seamlessly reconnects without user intervention.

• Intelligent Auto detect and connect
  Whenever the gateway or client’s location changes, Endpoint Connect autodetects the best method to establish a connection, using either NAT-T or Visitor mode, intelligently auto-switching between the two modes as necessary.

• Smart location awareness
  Endpoint Connect intelligently detects whether it is inside or outside of the VPN domain (Enterprise LAN), and automatically connects or disconnects as required.
Capabilities

- **Proxy detection**
  Proxy servers between the client and the gateway are automatically detected, authenticated to, and replaced when no longer valid.

- **Transparent Network and Interface Roaming**
  If the IP address of the client changes, for example if the client is using a wireless connection then physically connects to a LAN that is not part of the VPN domain, interface roaming maintains the logical connection.

- **Multiple Sites**
  Endpoint Connect connects to any one of a number of user defined gateways.

- **Dead Gateway Detection**
  If the client fails to receive an encrypted packet within a specified time interval, it sends a special “tunnel test” packet to the gateway. If the tunnel test packet is acknowledged, then the gateway is active. If number of tunnel test packets remain unacknowledged, the gateway is considered inactive or dead.

- **Dialup Support**

**Security**

- **Full IPSec VPN**
  Internet Key Change (version 1) support for secure authentication.

- **Support for strong authentication schemes** such as:
  a. Username and passwords (including cached passwords)
  b. SecurID
  c. Challenge-Response
  d. CAPI software and hardware tokens

- **Certificate enrollment, renewal, and auto Renewal**

- **Tunnel idleness Detection**

- **Smartcard Removal Detection**

- **Hub Mode**
  Increases security by routing all traffic, such as traffic to and from the Internet, through the gateway, where the traffic can be inspected for malicious content before being passed to the client.

- **Visitor Mode**
When the client needs to connect through a gateway that limits connections to port 80 or 443, encrypted (IPSec) traffic between the client and the gateway is tunneled inside a regular TCP connection.

**Installation and Use**

- **Small footprint**
- **Offline and Web deployment**
  
  Endpoint Connect is easily distributed through the gateway.
- **Automatic upgrades**
  
  Endpoint Connect upgrades are automatic, transparent to the user, and do not require administrator privileges or a client reboot.
- **Site and Create New Site connection wizards**
  
  For quickly configuring connections to corporate resources.
- **CLI Scripting**
  
  For automation and internal testing, and use as an embedded “headless” client.
- **OPSEC API**
  
  Available for embedded applications, Endpoint Connect is also designed to be part of specialized customer integrations and deployments, for example, organizations that build their own corporate presence applications that require VPN components. The client's intelligent auto-detect and disconnect features make it ideal for remote unmanned devices that need multiple High Availability options, such as embedded Windows ATMs. For such scenarios, Endpoint Connect offers a native Command Line Interface and OPSec API for configuration and monitoring, as well as the ability to be installed and run as a service.

**Administration**

- **Unified Central Management**
- **Advanced User Management**
- **Unified updates**
- **Regulatory Compliance with Advanced Monitoring, Logging and Reporting**
  
  DLL version numbers collected in a special file for troubleshooting purposes.
Configuring the Gateway Using SmartDashboard

In This Section:

Obligatory Settings page 15
Endpoint Connect Advanced Settings page 20

Obligatory Settings

In SmartDashboard:

1. Open the General Properties window for the gateway.
2. Enable VPN:

3. On the Topology page, create a VPN domain:
4. On the **VPN > VPN Advanced** page, enable NAT Traversal:
See “NAT Traversal” on page 34 for additional information.

5. On the **Remote Access** Page, enable Visitor Mode:

6. On the **Remote Access > Office Mode** page enable Office Mode and configure the appropriate settings:
Enable Office Mode when the remote client may be working with an IP address that clashes with an IP address on the network behind the gateway. When working with Office Mode, Endpoint Connect takes an Office IP address from the same reserved pool of IP addresses as SecureClient Mobile or SSL Network Extender.

7. On the Remote Access > SSL Clients page enable SSL clients:
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):**
Endpoint Connect Advanced Settings

1. In **Global Properties > Remote Access > Endpoint Connect**, open the advanced settings:

The window is divided into four sections:

- **Authentication Settings**
- **Connectivity Settings**
- **Security Settings**
- **Configuration and Version Settings**
**Authentication Settings**

Use the settings in this section to configure password caching, and how often the user needs to re-authenticate. If you do not open this window and configure options, then the client’s default value takes affect:

**Table 2-1**  Default Authentication values

<table>
<thead>
<tr>
<th>Option</th>
<th>SmartDashboard default value</th>
<th>Endpoint Connect default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable password caching</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Cache password for</td>
<td>1440 (minutes)</td>
<td>1440</td>
</tr>
<tr>
<td>Reauthenticate user every</td>
<td>480 (minutes)</td>
<td>480</td>
</tr>
</tbody>
</table>

**Connectivity Settings**

Use the settings in this section to determine connect and disconnect options. **Connect mode** covers whether the user should manually connect each time, the user is always connected, or whether the decision can be made on the client side. If the decision is left to the client, the user can select the Enable Always Connect option on the Settings tab of the site properties window.

If you do not open this window, then default values apply:

**Table 2-2**  Default Connectivity values

<table>
<thead>
<tr>
<th>Option</th>
<th>SmartDashboard default value</th>
<th>Endpoint Connect default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connect mode</td>
<td>Client decide</td>
<td>Yes</td>
</tr>
<tr>
<td>Location Aware Connectivity</td>
<td>Client decide</td>
<td>Yes</td>
</tr>
<tr>
<td>Disconnect when no connectivity to network</td>
<td>Client decide</td>
<td>No</td>
</tr>
<tr>
<td>Disconnect when device is idle</td>
<td>Client decide</td>
<td>No</td>
</tr>
</tbody>
</table>

**Location Aware Connectivity**

Endpoint Connect intelligently detects whether it is inside or outside of the VPN domain (Enterprise LAN), and automatically connects or disconnects as required. When the client is detected within the internal network, the VPN connection is terminated. If the client is in **Always-Connect** mode, the VPN connection is established again when the client exits.
Configuring Location Aware Connectivity

To configure Location Aware Connectivity:

a. Select Yes from the drop-down box and click Configure....

The Location Awareness Settings window opens:

b. Select the criteria by which the client determines whether it is within the internal network:

- Client can access its defined domain controller
- Client connection arrives from within the following network

If necessary, click Manage to define a new Simple Group, Group With Exclusion, or Network.

c. Click Advanced....
The **Location Awareness - Fast Detection of External Locations** window opens:

Use these options to identify external networks. For example, create a list of wireless networks or DNS suffixes that are known to be external. Or cache (on the client side) names of networks that were previously determined to be external. Selecting one or more of these options enhances the performance of location awareness.

**Security Settings**

Use the settings in this section to determine whether or not traffic to and from Endpoint Connect is routed through the gateway, and therefore subject to content inspection.

- If the system administrator decides to **Route all traffic through gateway**, all outbound traffic on the client is encrypted and sent to the gateway but only traffic directed at site resources is passed through; all other traffic is dropped.
- If this option is **not** selected, only traffic directed at site resources is encrypted and sent to the gateway. All other outbound client traffic passes in the clear.
• For the gateway to act as a hub for content inspection of all inbound and outbound client traffic, regardless of destination, the administrator needs to define a network application that includes the range: 0.0.0.1 > 255.255.255.254.

If you do not open this window, then default values apply:

Table 2-3  Default Security Settings

<table>
<thead>
<tr>
<th>Option</th>
<th>SmartDashboard default value</th>
<th>Endpoint Connect default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Route all traffic through gateway</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Configuration and Version Settings**

Use the settings in this section to configure how the client is upgraded. The upgrade procedure remains transparent to the user, and does not require administrator privileges on the endpoint or a reboot after the upgrade is complete.

If you do not open this window, then default values apply:

Table 2-4  Default configuration and version settings

<table>
<thead>
<tr>
<th>Option</th>
<th>SmartDashboard default value</th>
<th>Endpoint Connect default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client upgrade mode</td>
<td>ask user</td>
<td>do not upgrade</td>
</tr>
</tbody>
</table>

2. Save the policy.
Manually Configuring the Gateway for Endpoint Connect

If you choose to install HFA40 on the VPN-1 gateway without installing the NGX R66 plug-in on the SmartCenter server, then SmartDashboard cannot be used to configure Endpoint Connect — the database schema has not been updated with the appropriate endpoint properties. 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:

1. 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.

2. Enable those features relevant for your deployment.

3. Save and close the file

4. Install a policy or run: `cpstop`, `cpstart`.

For other manual configurations, see:

- “Configuring Logging Options for Client Users” on page 32
- “Disabling CAPI Authentication” on page 32
- “Disabling DNS-based Geo-Cluster Name Resolution” on page 33
- “Disabling DNS-based Geo-Cluster Name Resolution” on page 33
- “Smart Card Removal Detection” on page 35
Configuring Optional Endpoint Connect Settings

In This Section:

- Link Selection and MEP
- Hub Mode
- Secure Configuration Verification
- Working with RSA Hard and Soft Tokens
- Configuring Logging Options for Client Users
- Disabling CAPI Authentication
- Disabling DNS-based Geo-Cluster Name Resolution
- NAT Traversal
- Smart Card Removal Detection
- Tunnel Idleness

If you are considering migrating SecureClient users to Endpoint Connect, then read the following sections before reaching a decision. There are a number of important differences between SecureClient and Endpoint Connect. For example:

- SecureClient supports link selection and multiple entry points. The current release of Endpoint Connect accomplishes MEP through the use of a DNS server for configured for DNS-based Geo-cluster name resolution.

Link Selection and MEP

Link Selection

Because remote sites are defined on the client according to a single IP address or resolvable (DNS) name, Link Selection is not supported. Endpoint Connect ignores SecureClient link selection settings.

Multiple Entry Points

If a site implements gateways in a cluster (load sharing) or primary-backup/first to respond (high availability) configuration, it is important that the client performs DNS resolution each time it connects to the site. Providing:

- A site is defined by a DNS resolvable name rather than IP address
The DNS server is configured for DNS-based Geo-Cluster name resolution then Multiple Entry Point (MEP) for gateway redundancy can be implemented by the DNS server.

See “Disabling DNS-based Geo-Cluster Name Resolution” on page 33 for related information.

Hub Mode

Hub mode is configured in two places:

1. In Global Properties > Remote Access > Endpoint Connect:

   ![Endpoint Connect configuration settings]

   The options are:

   - Not to route all the traffic through the gateway
   - To route all traffic through the gateway
Hub Mode

- Route according to the Endpoint client configuration. If the client configuration is the determining factor, see the client's **Settings** tab for a particular site:

![Settings tab](image)

2. On the **Gateway > Remote Access** page:

![Remote Access tab](image)

Select **Allow SecureClient to route traffic through the gateway**. The setting applies equally to Endpoint Connect.
Secure Configuration Verification

While SecureClient uses the SCV settings configured in Global Properties, no SCV enforcement occurs for Endpoint Connect. This means that for Endpoint Connect you must bypass SVC for none SecureClient traffic by creating an exception:

1. Open Global Properties > Remote Access > Secure Configuration Verification
2. Select Apply Secure Configuration Verification on Simplified mode Security Policies
3. Click Exceptions
4. In the Secure Configuration Verification Exceptions window select Do not apply Secure Configuration Verification on SSL client connections:

Authentication Time-out

These settings for the gateway determine how long the remote client's password remains valid, which is equal to the frequency of IKE phase 1. By default, IKE authentication is valid for one day. If you do not want to accept the IKE default, set a different value here in Global Properties > Remote Access > Authentication Timeout.
The client timeout is read from the Endpoint Connect Settings in **Global Properties > Remote Access**.
Working with RSA Hard and Soft Tokens

If SecurID is used for authentication, you must manage the users on RSA’s ACE management server. ACE manages the database of RSA users and their assigned hard or soft tokens. The client contacts the site’s gateway. The gateway contacts the ACE Server for user authentication information. This means:

- Remote users must be defined as RSA users on the ACE Server.
- On the gateway, SecurID users must be placed in a group with an external user profile account that specifies SecurID as the authentication method.

For remote users to successfully use RSA’s softID:

1. Create a remote users group on the Ace Server
2. Distribute the SDTID token file (or several tokens) to the remote users “out of band”.
3. Instruct remote users on how to import the tokens.
Configuring Logging Options for Client Users

The Options window, Advanced tab of the client enables users to send log using their default mail client. Administrators can:

- Define an email address for these log files by modifying the `send_client_logs` attribute in `$FWDIR/conf/trac_client_1.ttm` on the gateway.

```
:send_client_logs {
  :gateway {
    :default ("email@example.com")
  }
}
```

- If an email address is not defined in `trac.client_1.ttm`, clicking Collect Logs in the Options > Advanced window collects all the client logs into a single CAB file, which the user can save and then send to the network administrator as an attachment.

Disabling CAPI Authentication

Endpoint Connect supports user authentication through the use of PKCS#12 certificates. A PKCS#12 certificate can be accessed directly or imported to the CAPI store and accessed from there.

If, for security reasons, you do not wish users to authenticate using certificates within the CAPI store:

1. On the gateway, open the `$FWDIR/conf/trac_client_1.ttm` file for editing.
2. Modify the `enable_capi` attribute to FALSE.

```python
enable_capi {
  :gateway {
    :map {
      :false (false)
      :true (true)
      :client_decide (client_decide)
    }
    :default (true)
  }
}
```

By default, the value is TRUE.
Modify the `:default (true)` line.
Disabling DNS-based Geo-Cluster Name Resolution

Each time Endpoint Connect connects to the VPN-1 or Connectra gateway, the client performs, by default, DNS name resolution. For a deployment consisting of a single gateway, there is no need to perform DNS resolution every time — the first time the client connects, it caches the IP address of the gateway and reuses it on each subsequent connect operation. In this kind of deployment, the default behavior of the client can be safely modified.

To prevent the gateway from performing name resolution each time Connect connects:

1. On the gateway, open the $FWDIR/conf/trac_client_1.ttm file for editing.
2. Modify the enable_gw_resolving attribute to FALSE:

   ```
   :enable_gw_resolving (
     :gateway (  
       :map (  
         :false (false)  
         :true (true)  
         :client_decide (client_decide)  
       )  
       :default (true)  
     )  
   )
   ```

   By default, the value is TRUE.
   Modify the :default (true) line.

However, in a deployment consisting of multiple gateways, for example in a cluster (load sharing) or primary-backup (high availability) configuration, it is important that the client performs DNS resolution each time it connects to the site. Based on geographical proximity or the load-sharing requirements of the gateway, the DNS server might return to the client a different IP address each time: the IP address of the nearest available gateway. This IP address may not be the same as the IP address cached during the first connect operation. Resolving DNS names each time:

- Enables DNS to be used for High availability (the IP address of the backup gateway is returned when the primary fails to respond)
- Adds to the client a functionality similar to MEP (Multiple Entry Points)

**Note** - This is not a regular cluster environment, as the two or more gateways are not synchronized.
NAT Traversal

When a remote user initiates a VPN (IPSec encrypted) session with the gateway, during the initial negotiation, both gateway and remote client attempt to detect whether the traffic between them passed through a NAT device.

For a number of reasons NAT is incompatible with IPSec:

- IPSec assures the authenticity of the sender and the integrity of the data by checking to see that the data payload has not been changed in transit. A NAT device alters the IP address of the remote client. The Internet Key Exchange (IKE) protocol used by IPSec embeds the client’s IP address in its payload, and this embedded address, when it reaches the gateway, will fail to match the source address of the packet, which is now that of the NAT device. When addresses don’t match, the gateway drops the packet.

- TCP and UDP checksums in the TCP header are sometimes used to verify the packet’s integrity. The checksum contains the IP addresses of the remote client and gateway, and the port numbers used for the communication. IPSec encrypts the headers with the Encapsulating Security Payload (ESP) protocol. Since the header is encrypted, the NAT device cannot alter it. This results in an invalid checksum. The gateway again rejects the packet.

The Endpoint Connect Client resolves these and other NAT related issues by using NAT-Traversal (NAT-T) as a way of passing IPSec packets through the NAT device.

On the gateway, default ports are:

- Internet Key Exchange (IKE) - User Datagram Protocol (UDP) on port 500
  
  **Note** - only IKEv1 is supported

- IPsec NAT-T - UDP on port 4500

- Encapsulating Security Payload (ESP) - Internet Protocol (IP) on 50

If a NAT device is detected during the initial negotiation, communication between gateway and client switches to UDP port 4500. Port 4500 is used for the entire VPN session.

**Note** - NAT-T packets (or the packets of any other protocol) need to return to the client through the same interface they came in on. While the recommended deployment is to place the gateway in a public DMZ with a single interface for all traffic, it is also possible to deploy with inbound and outbound interfaces, the default route being the outbound route towards the Internet. Endpoint Connect only connects to the Connectra gateway’s default outbound interface.
Smart Card Removal Detection

If remote users authenticate through a Smart Card, and the smart card or smart reader is removed from the USB port, the client detects that the certificate is no longer available and disconnects from the site. A VPN tunnel has disconnected. Smart card was removed message is displayed to the user. To configure this behavior:

On the gateway:
1. Open $FWDIR/conf/trac_client_1.ttm for editing.
2. Locate the line:
   ```
   :disconnect_on_smartcard_removal ( 
   :gateway ( 
   :default (client_decide) 
   )
   )
   ```
3. Replace “Client_decide” with either TRUE or FALSE. If leave the decision to the client, then on the client:
   a. Open %programfiles%\checkpoint\endpoint\connect\trac.defaults for editing.
   b. Locate the line:
   ```
   :disconnect_on_smartcard_removal STRING false GW_USER 0
   ```
   c. Replace false with true
   d. Save and close the file

Tunnel Idleness

A number of organizations may have specific security requirements, such that an open VPN tunnel should be transporting work-related traffic to the site at all times. An idle or inactive tunnel should be shut down. (Stay-alive packets or “noise” such as NetBios Broadcasts to port 83 or DNS broadcasts to port 137 are not considered “work related”. A mail program such as OUTLOOK performing a send-receive operation every five minutes would be considered work-related, and the tunnel kept open.)

For this reason, a tunnel idleness interval can be configured in accordance with the company’s security policy.

Tunnel idleness can be set either in the gateway policy or on the client.
Tunnel Idleness

**Configuring Tunnel Idleness on the Client**

1. Open for editing:
   
   %programfiles%\checkpoint\endpoint connect\trac.defaults.

2. Locate the line:

   tunnel_idleness_timeoutINT 0 GW_USER 0

3. Replace INT 0 with a value. For example INT 20 will shut down an inactive
   VPN tunnel after twenty minutes. INT 0 means no tunnel idleness. The feature
   is switched off.

   This setting is only enforced if no policy regarding tunnel idleness is set on the
   gateway. Otherwise, the gateway policy set by SmartCenter server is enforced.

**Configuring Tunnel Idleness on the Server**:

1. Connect to the SmartCenter server using GuiDBedit.

2. Open the **Global Properties > properties > firewall_properties object**:
3. Configure the following parameters:

- `disconnect_on_idle`
- `do_not_check_idleness_on_icmp_packets`
- `do_not_check_idleness_on_these_services`

By listing services, you effectively include the associated port numbers. For example, if NetBios is entered as the service, then port 83 is not monitored for tunnel idleness.

- `enable_disconnect_on_idle`
- `idle_timeout_in_minutes`
Using the Packaging Tool

Set a value such as 30, for thirty minutes.

Note - If you enter a value for idle_timeout_in_minutes, then enable_disconnect_on_idle must also be set to TRUE.

4. Save and install a policy.

Using the Packaging Tool

Endpoint Connect supports a special administration mode that enables the creation of preconfigured packages. The administrator opens one instance of the client, configures all settings then saves the client as an .msi package for further distribution to end point users.

To create a preconfigured package:

1. Open the Endpoint Connect client in administration mode:
   - Click on AdminMode.bat file in c:\Program Files\Checkpoint\Endpoint Connect, or:
   - From a command prompt, run: c:\Program Files\Checkpoint\Endpoint Security\trgui.exe /admin

2. Right-click the client icon in the system tray, and select VPN Options.
   The VPN Options window opens showing the administration tab:
3. Using the options on the Site and Advanced tabs, configure:
   • Site definitions
   • Authentication method
   • Logging
   • Proxy server settings
   • Always-connect mode
   • VPN tunneling

4. On the Administration tab:
   a. Select a folder for the new package
   b. Decide whether to override the previous configuration when upgrading
   c. Click Generate to create the .msi package in the designated folder.

5. Distribute this package to Endpoint Connect users.
Using the Packaging Tool