14 July 2015

Endpoint Security VPN for Mac

E80.61

Release Notes
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.

Check Point E80.61
For more about this release, see the E80.61 home page http://supportcontent.checkpoint.com/solutions?id=sk105123.

Latest Version of this Document
Download the latest version of this document http://supportcontent.checkpoint.com/documentation_download?ID=40525.
To learn more, visit the Check Point Support Center http://supportcenter.checkpoint.com.

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 Endpoint Security VPN for Mac E80.61 Release Notes).

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>14 July 2015</td>
<td>Updated build number for this release (&quot;Build Numbers&quot; on page 9)</td>
</tr>
<tr>
<td>31 March 2015</td>
<td>First release of this document</td>
</tr>
</tbody>
</table>
Introduction

Check Point offers multiple enterprise-grade VPN clients to fit a wide variety of organizational needs. The Remote Access VPN stand-alone clients provide a simple and secure way for endpoints to connect remotely to corporate resources over the Internet, through a VPN tunnel, and are managed in SmartDashboard.

See Remote Access Clients Comparison (on page 6) for a detailed feature comparison of different E80.61 clients.

This release of Endpoint Security VPN for Mac supplies improved stability and bug fixes.

Supported Upgrades

Upgrade to this release from Endpoint Security VPN for Mac E75 and higher.

You can upgrade FROM this release TO Endpoint Security Suite E80.61 and higher for more Endpoint Security blades and functionality.

Migrating from SecureClient

Endpoint Security VPN for Mac is not compatible with SecureClient for Mac. You must uninstall SecureClient before you install Endpoint Security VPN.
## Remote Access Clients Comparison

<table>
<thead>
<tr>
<th>Feature</th>
<th>Endpoint Security VPN for Windows</th>
<th>Check Point Mobile for Windows</th>
<th>SecuRemote</th>
<th>Endpoint Security VPN for Mac</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Client Purpose</strong></td>
<td>Secure connectivity with desktop firewall &amp; compliance checks</td>
<td>Secure connectivity &amp; compliance checks</td>
<td>Basic secure connectivity</td>
<td>Secure connectivity with desktop firewall</td>
<td></td>
</tr>
<tr>
<td><strong>Replaces Client</strong></td>
<td>SecureClient NGX R60 Endpoint Connect R73</td>
<td>Endpoint Connect R73</td>
<td>SecuRemote NGX R60</td>
<td>SecureClient for Mac</td>
<td></td>
</tr>
<tr>
<td><strong>IPSEC VPN Tunnel</strong></td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>All traffic travels through a secure VPN tunnel.</td>
</tr>
<tr>
<td><strong>Security Compliance Check (SCV)</strong></td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td></td>
<td>Monitor remote computers to confirm that the configuration complies with organization's security policy.</td>
</tr>
<tr>
<td><strong>Integrated Desktop Firewall</strong></td>
<td>✔</td>
<td></td>
<td>✔</td>
<td></td>
<td>Integrated endpoint firewall centrally managed from a Security Management Server</td>
</tr>
<tr>
<td><strong>Split Tunneling</strong></td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>Encrypt only traffic targeted to the VPN tunnel.</td>
</tr>
<tr>
<td><strong>Hub Mode</strong></td>
<td>✔</td>
<td></td>
<td>✔</td>
<td></td>
<td>Pass all connections through the gateway.</td>
</tr>
<tr>
<td><strong>Dynamic Optimization of Connection Method</strong></td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>When NAT-T connectivity is not possible, automatically connect over TCP port 443 (HTTPS port).</td>
</tr>
</tbody>
</table>

*Note: The table columns are marked with ✔ to indicate availability across different clients.*
<table>
<thead>
<tr>
<th>Feature</th>
<th>Endpoint Security VPN for Windows</th>
<th>Check Point Mobile for Windows</th>
<th>SecuRemote</th>
<th>Endpoint Security VPN for Mac</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multi Entry Point (MEP)</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️ Manual</td>
<td>✔️</td>
<td>Client seamlessly connects to an alternative site when the primary site is not available.</td>
</tr>
<tr>
<td>Secondary Connect</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td></td>
<td>End-users can connect once and get transparent access to resources, regardless of their location.</td>
</tr>
<tr>
<td>Office Mode IP</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td></td>
<td>Each VPN client is assigned an IP from the internal office network.</td>
</tr>
<tr>
<td>Back Connection Protocols</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td></td>
<td>Support protocols where the client sends its IP to the server and the server initiates a connection back to the client using the IP it receives. These protocols include: Active FTP, X11, some VoIP protocols.</td>
</tr>
<tr>
<td>Auto Connect and Location Awareness</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td></td>
<td>Intelligently detect if the user is outside the internal office network, and automatically connect as required. If the client senses that it is inside the internal network, the VPN connection is terminated.</td>
</tr>
<tr>
<td>Roaming</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td></td>
<td>Tunnel and connections remain active while roaming between networks.</td>
</tr>
<tr>
<td>Always Connected</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td></td>
<td>VPN connection is established whenever the client exits the internal network.</td>
</tr>
<tr>
<td>Feature</td>
<td>Endpoint Security VPN for Windows</td>
<td>Check Point Mobile for Windows</td>
<td>SecuRemote Endpoint Security VPN for Mac</td>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-----------------------------------</td>
<td>--------------------------------</td>
<td>----------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Secure Domain Logon (SDL)</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>VPN tunnel and domain connectivity is established as part of Windows login allowing GPO and install scripts to execute on remote machines.</td>
<td></td>
</tr>
<tr>
<td>Split DNS</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>Resolves internal names with the SecuRemote DNS Server configuration.</td>
<td></td>
</tr>
<tr>
<td>Hotspot Detection and Registration</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>Makes it easier for users to find and register with hot spots to connect to the VPN through local portals (such as in hotels or airports).</td>
<td></td>
</tr>
<tr>
<td>Secure Authentication API (SAA)</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>Allows third party-extensions to the standard authentication schemes. This includes 3-factor and biometrics authentication.</td>
<td></td>
</tr>
</tbody>
</table>
System Requirements

Read all requirements carefully.

Client Requirements

Endpoint Security VPN E80.61 can be installed on these Mac platforms in 32 and 64 bit:

- Mac OS X 10.6 Snow Leopard
- Mac OS X 10.7 Lion
- Mac OS X 10.8 Mountain Lion
- Mac OS X 10.9 Mavericks
- Mac OS X 10.10 Yosemite

VPN Gateway Requirements

For the most up-to-date list of supported operating systems, server and gateway requirements, see: sk67820 http://supportcontent.checkpoint.com/solutions?id=sk67820.

Build Numbers

The build number for this release is: 860100101

Installation and Configuration

Before you install this release, make sure that you have supported gateways, and if necessary, a required Hotfix.

If Visitor mode is configured on port 443 and WebUI is enabled on the gateway, the WebUI must listen on a port other than 443. Otherwise, Endpoint Security VPN cannot connect.

Installing the Client

Install the client on a supported Mac platform booted in 64-bit or 32-bit mode. Get all files from sk105123 (http://supportcontent.checkpoint.com/solutions?id=sk105123).

To install Endpoint Security VPN for Mac on a client computer:

1. Download the Endpoint Security VPN for Mac E80.61 - Disc Image file to the client computer.
2. Double-click the file.
   After the disk image mounts to the file system, a Finder window opens with the contents of the package.
3. Double-click the Endpoint_Security_VPN.pkg file to start the installation.
4. Follow the on-screen instructions.
Uninstalling the Client

If necessary, you can uninstall the Endpoint Security VPN client.

To install Endpoint Security VPN for Mac from a client computer:

   After the disk image mounts to the file system, a Finder window opens with the contents of the package.
2. Double-click the Uninstaller to start the uninstall process.
3. Do the on-screen instructions.

Automatic Upgrade from the Gateway

You can configure your Security Gateway to automatically upgrade Remote Access VPN clients the next time that they connect. When this occurs, the Security Gateway downloads the applicable package to the client. Endpoint users must have administrator permissions to install an upgrade.

You can have packages for different versions of the VPN client for Windows and Mac OS X on your Security Gateway at the same time. For example, you can have E75.01 for Mac and E75.20 for Windows at the same time.

To set up a gateway to automatically install client upgrades:

2. Rename the Endpoint_Security_VPN.pkg, Endpoint_Security_VPN.pkg.signature and ver.ini files to TRAC.pkg, TRAC.pkg.signature and trac_ver_osx.txt respectively.
3. Upload these files to this directory on the gateway:
   $FWDIR/conf/extender/CSHELL
   - For version R71.x only, copy the TRAC.pkg and TRAC.pkg.signature files also to:
     $CVPNDIR/htdocs/SNX/CSHELL.
4. On a non-Windows gateway, run:
   - chmod 750 TRAC.pkg
   - chmod 750 TRAC.pkg.signature
   - chmod 750 trac_ver_osx.txt
5. In SmartDashboard, go to Policy >Global Properties >Remote Access >Endpoint Connect.
6. Select one of these Client upgrade mode options:
   - Do not upgrade - This option disables automatic upgrades from the gateway. Automatic upgrades are not available for endpoint users.
   - Ask user - The user receives a prompt and can install immediately or at a later time.
     If the user does not install the upgrade immediately, the prompt will show again in one week.
   - Always upgrade - The new package installs silently without user intervention. The user receives a notification once the upgrade completes successfully.
7. Install the policy.
Installing the Endpoint Security VPN Hotfix

If you have R71.30 and higher or R75 and higher installed on a gateway, Security Management Server, or Multi-Domain Server, it can support Endpoint Security VPN. It is not necessary to install a Hotfix. See the System Requirements section of the Release Notes for exact details.

For earlier supported gateway versions, install the Hotfix http://supportcontent.checkpoint.com/solutions?id=sk67820.

Install the Endpoint Security VPN E80.61 Hotfix on gateways or standalone, self-managed gateway deployments. In a Multi-Domain Security Management environment install the Hotfix on the Multi-Domain Server.

Before you install the Hotfix:

This Hotfix has possible conflicts with other installed Hotfixes. If you can, it is safest to uninstall all Hotfixes installed on the Security Management Server or gateways. See Uninstalling a Hotfix ("Uninstalling this Hotfix" on page 12). If you cannot uninstall a Hotfix, contact Check Point Technical Support.

To install the Hotfix on a Security Gateway or Security Management Server:

1. Download the Hotfix.
3. Run the Hotfix:
   - On SecurePlatform, Disk-based IPSO, and Solaris:
     a) tar -zxvf <name_of_file>.tgz
     b) ./UnixInstallScript
   - On Windows platforms: double-click the installation file and follow the instructions.

To install the Hotfix on a Multi-Domain Server:

2. Download the Endpoint Security VPN Hotfix to the Multi-Domain Server.
3. Run the Hotfix on SecurePlatform and Solaris:
   a) tar -zxvf <name_of_file>.tgz
   b) ./UnixInstallScript
4. Follow the on-screen instructions.
5. Reboot the Multi-Domain Server.
Uninstalling this Hotfix

If you need to uninstall a Hotfix, use this procedure.

To uninstall a Hotfix from a gateway:

1. Go to the installation directory: `cd /opt/CPsuite-\textit{version}/`
   - For example, the installation directory on an R70.40 gateway is: `/opt/CPsuite-R70/`
2. Run: `/\textit{uninstall}_{\textit{name\_of\_original\_Hotfix\_file}}`
   - The name of the Hotfix is different for gateway version and for Hotfix functionality.
3. Enter `y` at the prompt.
4. Reboot the Security Gateway.

Known Limitations and Resolved Issues

For known limitations that apply to this release, see sk105124

For issues resolved in this release, see sk105125