How To Install Third Party SSL Certificates for the IPsec VPN Software Blade

14 April 2015

Check Point
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.
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=16641)
To learn more, 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>14 April 2015</td>
<td>Changed document title. Formerly: How To Install Third Party SSL Certificates</td>
</tr>
<tr>
<td></td>
<td>Fixed Trusting a Third-party Certificate Authority (on page 6). GoDaddy certificates are supported.</td>
</tr>
<tr>
<td>7 May 2012</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 Install Third Party SSL Certificates for the IPsec VPN Software Blade).

Objective

This document explains how to create and install a third party SSL Certificate for the IPsec VPN Software Blade on a Check Point Firewall.

Supported Versions

- NGX R65 (up to HFA 70)
- R70
- R71

Note - If you need to install an SSL Certificate on a Connectra gateway (R62 or R66), refer to the Connectra R66 Administration Guide (http://supportcontent.checkpoint.com/documentation_download?ID=8393) (LM or CM) for instructions, as the configuration steps described below do not support Connectra Gateway SSL Certificates.

Supported Operating Systems

- All Operating Systems, Configuration is done through SmartDashboard.

Supported Appliances

- All appliances running the supported versions.

Before You Start

Related Documents and Assumed Knowledge

- Before doing the steps in this document, it is recommended that you perform a Database Revision. This will let you revert to a previous configuration if necessary.

Impact on Environment and Warnings

- No change will take effect on the Firewall until after you install the policy on a gateway.
Installing a Third Party SSL Certificate with Check Point Firewall

To install and use a third party SSL Certificate with a Check Point firewall gateway, you need to:

- Trust a third party Certificate Authority
- Install an Intermediate CA (for Verisign and some other vendors)
- Obtain a valid SSL Certificate from a third (includes generating a Certificate Signing Request (CSR), sending the CSR to the third party, installing the certificate and installing the policy)

**Note:** If you need to install an SSL Certificate on a Connectra gateway, refer to the Connectra Administration Guide (http://supportcontent.checkpoint.com/documentation_download?ID=8393) for instructions, as the GUI does not support Connectra Gateway SSL Certificates properly.

In this section:

- Trusting a Third-party Certificate Authority ................................................................. 6
- Installing an Intermediate CA........................................................................................ 9
- Obtaining a Certificate from a 3rd-party Certificate Authority ......................................... 11

**Trusting a Third-party Certificate Authority**

To trust a third party Certificate Authority:

Examples of third party SSL Certificates are: Verisign, Entrust and Digicert.

The firewall needs to "trust" the third party Certificate Authority (CA). In order for the firewalls to trust a particular CA, you must define both Root CA and any Intermediate CA’s inside of the SmartConsole Smart Dashboard. The procedure below explains how to establish this trust and then how to obtain a certificate from that third party authority.

You will create the Trusted CA and install the Root CA from your third party.
**Installing a Third Party SSL Certificate with Check Point Firewall**

**Note:** It is always recommended to talk with your third party CA to ensure that you have the correct CA certificate.

1. Log in to SmartDashboard.

2. From the Servers and OPSEC Applications tab > Servers > Trusted CAs, select New CA > Trusted to add the top level root CA first.

3. Add the appropriate label in the Name field and select OPSEC PKI as the Certificate Authority type.

4. Select the OPSEC PKI tab. In the "Retrieve CRL From" section, make sure that only "HTTP Server(s)" is selected, and then inside the "Certificate" section, click Get to insert the root CA certificate.

5. Browse to where you saved the root certificate. Check Point supports DER or PEM encoded certificates. Select the Root Certificate only, not a chain. They can have a .crt, .cer or similar extension.
6. Click **Open**. 
A view of the imported certificate appears.

7. Verify the serial number or thumbprint and click OK to Accept the CA certificate.
8. The Root CA object appears as shown.
Installing an Intermediate CA

Notes:

- If you are using a third party like Verisign that uses an Intermediate CA, then you must install that Intermediate CA as described in this section. If not, continue to the Obtaining a Certificate from a Third Party Certificate Authority section.

Verisign has 16 different Intermediate CA certificates that are available, see: https://knowledge.verisign.com/support/ssl-certificates-support/index?page=content&id=AR657&actp=LIST

- It is always recommended to talk with your third party CA to ensure that you have the correct CA.

1. Create an Intermediate CA object. From the Servers and OPSEC applications tab > Servers > Trusted CAs > New CA, select Trusted.

2. Add the appropriate label for the Intermediate CA in the Name field.

3. Select the OPSEC PKI tab and click Get to obtain the Intermediate CA certificate.

4. Browse to where you have saved the Intermediate root certificate, same as before. Select the Policy Certificate only, not a chain.
5. Click **Open**. A view of the imported certificate appears.

![Certificate Authority Certificate View](image)

6. Click **OK** to save the CA object. You should now see Root CA and Intermediate CA objects.

![Certificate Management](image)
Obtaining a Certificate from a 3rd-party Certificate Authority

After you define the third party Certificate Authorities and they are trusted by the gateway/cluster object you can request and obtain a certificate from them. Requesting a certificate is a multi-step process. You need to issue a Certificate Signing Request (CSR), submit it to a trusted third party CA for signing, and then import the signed certificate back into the firewall.

1. Select the Network Objects tab and edit the Check Point gateway/cluster object.

2. Select VPN and click Add to add a certificate to the Repository of Certificates available to the Gateway.

3. Enter a name in the Certificate Nickname field (this is for your reference) and select what Certificate Authority will sign your CRS. You select the third party CA that you installed above.

**Note:** If this is for Verisign, use the INTERMEDIATE CA and not the ROOT CA.
4. Click **Generate** to start the process of creating a CSR.
5. Click **Yes** in the warning that appears. If you make a mistake, delete the CSR request and start over.

![Generate Certificate Request window]

6. In the Generate Certificate Request window, enter DN information. Refer to previous SSL Certificate information for this data. Do not select "Define Alternate Names".

   ![Generate Certificate Request window]

   If this is a new SSL Certificate request, the general format for DN is as follows:

   - **CN**=sitename.domain.com (if gateway name, it has to match exactly!) OR *.domain.com for a Wildcard certificate
   - **OU**=Group name (ex. IT Operations)
   - **O**=Company Name
   - **L**=Location/City information
   - **ST**=State (DO NOT USE "s=")
   - **C**=Country (ex. US)

   These values are separated by a comma. Not all of these values are needed, you need just the cn=sitename or gateway name as a minimum.

   (Example: CN=sitename.domain.com,OU=IT Operations, O=Company Name, L=City, ST=State, C=US)

   **Note 1**: Check Point does not support the standard E= or S= attribute. If needed, use ST= instead of S= or E=.

   **Note 2**: If an extra "," is needed in the name, use "\" to skip the comma. Example: O=Company Name\, Inc.

7. Click **OK** to generate a CSR.
8. Click **OK** in the created successfully message. Now you have an entry for a certificate and you need to submit the CSR to the third party.

![Certificate request created successfully]

9. To sign the request, click **View**. The Certificate Request View appears.

![Certificate Request View]

10. Click **Save to a File**... This lets you save this to a text file that you can then send to your third party.
Alternatively:
Click **Copy to Clipboard** and paste this on the third party web site that requests the signing certificate.

11. When you get the file back from the third party, save the file, and then go back to the Gateway properties window > VPN > select the certificate, and click **Complete**.

12. Select the signed CSR and click **Open**.

13. Review the details of the certificate.

14. Now the certificate is installed. When you click **OK** and install the policy, the SSL certificate will be installed on the gateway.

Note: If you need to install an SSL Certificate on a Connectra gateway, please refer to the Connectra Administration Guide (http://supportcontent.checkpoint.com/documentation_download?ID=8393) for instructions, as the GUI does not support Connectra Gateway SSL Certificates.
Verifying

When you view the SSL certificate, it will no longer be generated by the SmartCenter server, but by the third party server that you used.
Index

B
Before You Start • 5

I
Impact on Environment and Warnings • 5
Important Information • 3
Installing a Third Party SSL Certificate with
   Check Point Firewall • 5
Installing an Intermediate CA • 8

O
Objective • 5
Obtaining a Certificate from a 3rd-party
   Certificate Authority • 11

R
Related Documents and Assumed Knowledge •
   5

S
Supported Appliances • 5
Supported Operating Systems • 5
Supported Versions • 5

T
Trusting a Third-party Certificate Authority • 6

V
Verifying • 14