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=11938
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>2/6/2011</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 Configure OCSP ).
How To Configure OCSP

Objective
This document describes how to configure VPN-1 Power/UTM to use OCSP

Supported Versions
- VPN-1 NGX up to R71

Supported OS
- All

Supported Appliances
- Any running VPN-1 Power/UTM NGX or later

Before You Start

Related Documentation
- VPN Admin Guide

Assumed Knowledge
- How to configure Certificate based authentication

Impact on the Environment and Warnings
OCSP performs a real-time check of the certificate status, which means as soon as a certificate is revoked; it will immediately be recognized by the gateway as being revoked. This differs from the default behavior of CRL checking. CRLs are cached by default. Depending on the configuration, there can be a lag between when the certificate was actually revoked by the Certificate Authority, and when the gateway actually recognizes that the certificate has been revoked.

OCSP does not cache any data. A request will be sent from the gateway to the OCSP responder each time the gateway needs to check the status of a certificate. This could have a performance impact under some circumstances if the amount of data being sent between the gateway and OCSP responder is excessive.

One major benefit to using OCSP over CRLs is that a VPN outage can occur under some circumstances if the CRL list grows too large. This potential problem is eliminated when using OCSP.
Configuring OCSP

Note – This procedure assumes you have already configured a Trusted Root Certificate Authority object, and the VPN is already functioning using certificates issued by this CA.

In this section:

- Creating an OCSP Server Object 7
- Configuring the New OCSP Server 10
- Formatting the Certificate 11
- Configuring the Trusted Root CA Object 13
Creating an OCSP Server Object

To create an OCSP Server object:
1. Run GuiDBedit and connect it to the SmartCenter server.
2. Navigate to: +Managed Objects -> servers.
3. Right-click in the upper right-hand pane and click: New...

4. In the Create Object window from the Class pull-down menu, select OCSP_server.

5. In the Object: text box type a name for the object (Example: myOCSPserver).

6. Click OK and the object will be created.
Configuring the New OCSP Server

To configure the OCSP server object you just created:

1. Using GuiDBedit, in the upper-right hand pane click the OCSP server object you just created. Its attributes are displayed in the lower pane.
2. Double-click the Value column in the url field and enter the URL of the OCSP server supplied by the Certificate Authority vendor being used. Click **OK**.*

   **Note** – this should be a standard URL such as: http://someocsp.someCAvendor.com.

3. Double-click the Value column in the Certificate field and enter the OCSP server’s certificate data (Base64 encoded DER format).
Formatting the Certificate

Note – when viewed in an ASCII viewer, a Base64 encoded DER certificate starts with "-----BEGIN CERTIFICATE-----" and ends with "-----END CERTIFICATE-----", containing the certificate data in the middle.

To format a Base64 encoded DER certificate:

1. Open the certificate file in ASCII editor and delete all line breaks, to turn the data into a single, long, line.
2. Open the entire string (including "-----BEGIN CERTIFICATE-----" and "-----END CERTIFICATE-----") and paste the data into the Value field.

Click OK.

The OCSP Server object is now fully configured.
Configuring the Trusted Root CA Object

To configure the relevant Trusted Root CA object to use the OCSP server:

1. In the upper-right hand pane of GuiDBedit, click the relevant Root CA object.

2. In the lower pane, double-click the Value column of the OCSP_servers field, and select the OCSP server you just created.
3. Double-click the Value column of the "OCSP_validation" field and set it to true.

4. Save the changes in GuiDBedit by clicking: File -> Save All.

5. Close GuiDBedit.

6. Open the SmartDashboard and install the Security Policy.

   Note – CRLs will not be fetched for a CA for which OCSP validation has been configured. OCSP responses are not cached.
Completing the Procedure

- Open the SmartDashboard and install the Security Policy.

Verifying the Procedure

- Enable logging on the rule that allows the VPN-1 gateway to communicate with the OCSP responder (May be an implied rule or explicit rule) and verify that the gateway is communicating with the OCSP responder every time a certificate is validated by the gateway.

- A more conclusive way to verify that OCSP is working is to enable a VPN debug as such:
  - `vpn debug on OCSP=5`
    This will cause the VPN daemon to write OCSP debug prints to `$FWDIR/log/vpnd.elg`
  - To turn off the debug run:
    `vpn debug off`