## Contents

### The Common Criteria Evaluated Configuration

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Overview</td>
<td>9</td>
</tr>
<tr>
<td></td>
<td>The Certification Challenge</td>
<td>9</td>
</tr>
<tr>
<td></td>
<td>Reference Material</td>
<td>10</td>
</tr>
<tr>
<td>2</td>
<td>Evaluated Configuration</td>
<td>11</td>
</tr>
<tr>
<td></td>
<td>Administrator-defined User Parameters</td>
<td>11</td>
</tr>
<tr>
<td></td>
<td>User Authentication Schemes</td>
<td>11</td>
</tr>
<tr>
<td></td>
<td>Single-Use Password Authentication</td>
<td>12</td>
</tr>
<tr>
<td></td>
<td>Remote Access Virtual Private Networks (VPNs)</td>
<td>12</td>
</tr>
<tr>
<td>3</td>
<td>Security Guidelines</td>
<td>13</td>
</tr>
</tbody>
</table>

### User Authentication

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>Telnet Authentication</td>
<td>17</td>
</tr>
<tr>
<td></td>
<td>Welcome Message</td>
<td>17</td>
</tr>
<tr>
<td></td>
<td>User Identification and Authentication</td>
<td>17</td>
</tr>
<tr>
<td></td>
<td>Authentication Failure Handling</td>
<td>18</td>
</tr>
<tr>
<td></td>
<td>Connection to Destination Server</td>
<td>18</td>
</tr>
<tr>
<td></td>
<td>Inactive Session Termination</td>
<td>18</td>
</tr>
<tr>
<td></td>
<td>Error Messages</td>
<td>19</td>
</tr>
<tr>
<td></td>
<td>Examples</td>
<td>20</td>
</tr>
<tr>
<td>5</td>
<td>FTP Authentication</td>
<td>22</td>
</tr>
<tr>
<td></td>
<td>Welcome Message</td>
<td>22</td>
</tr>
<tr>
<td></td>
<td>User Identification and Authentication</td>
<td>22</td>
</tr>
<tr>
<td></td>
<td>Connection to Destination Server</td>
<td>24</td>
</tr>
<tr>
<td></td>
<td>Error Messages</td>
<td>25</td>
</tr>
<tr>
<td></td>
<td>Examples</td>
<td>28</td>
</tr>
</tbody>
</table>
CHAPTER 6  SSL Network Extender  
SSL Network Extender Download................................. 31
Establishing the SSL VPN Session............................... 32

CHAPTER 7  SecureClient Mobile  
SecureClient Mobile Installation ................................... 35
Establishing the SecureClient Mobile Session............... 36

CHAPTER 8  Other VPN Clients  
IPSec VPN Clients...................................................... 37
The Common Criteria Evaluated Configuration
The Certification Challenge

"Common Criteria for Information Technology Security Evaluation" (CCITSE) usually referred to as the "Common Criteria" (CC) is an evaluation standard for a multi-national marketplace. The uses of Common Criteria include:

- For consumers:
  - To find requirements for security features that match their own risk assessment.
  - To shop for products that have ratings with those features.
  - To publish their security requirements so that vendors can design products that meet them.

- For developers:
  - To select security requirements that they wish to include in their products.
  - To design and build a product in a way that can prove to evaluators that the product meets requirements.
  - To determine their responsibilities in supporting and evaluating their product.
Check Point VPN-1 Power/UTM NGX R65 provides a broad range of services, features and capabilities. The Security Target (ST) makes a set of claims regarding the product's security functionality, in the context of an evaluated configuration. The claimed security functionality is a subset of the product's full functionality. The evaluated configuration is a subset of the possible configurations of the product, established according to the evaluated configuration guidance.

This document describes the security functions and interfaces available to the non-administrative users of NGX R65. The security functions and interfaces that are visible at the user interfaces are authentication for FTP and Telnet, as well as the download and use of the SSL Network Extender client.

**Reference Material**

The evaluated configuration is described in:
- *Check Point VPN-1 Power/UTM NGX R65 Security Target*

The user interfaces and security functions relating to the SSL Network Extender client are described in detail in:
CHAPTER 2

Evaluated Configuration

In This Chapter

Administrator-defined User Parameters  page 11
User Authentication Schemes  page 11
Single-Use Password Authentication  page 12

Administrator–defined User Parameters

The Administrator defines the different terms under which users can operate, such as:

- The services users are allowed to use
- How users are authenticated

User Authentication Schemes

Users sending or receiving information through the evaluated configuration can be authenticated by either:

- Setting up a VPN rule that requires a remote access VPN tunnel to be used by the user for sending information through the evaluated configuration
  or
- Configuring a Security Server to require single-use password authentication using an authentication server in the IT environment.
User Authentication is available for the services Telnet and FTP. Using SSL Network Extender and SecureClient Mobile, users can use an authenticated secure channel for all IP-based protocols.

**Single-Use Password Authentication**

The evaluated configuration supports the use of authentication servers in the IT environment for user authentication via single-use passwords. The RADIUS and SecurID protocols are supported for this purpose.

The Telnet, FTP, and SSL Network Extender interfaces support the use of the RADIUS and SecurID protocols for sending the user-supplied single-use password to an external authentication server.

**Remote Access Virtual Private Networks (VPNs)**

The evaluated configuration allows users to establish Virtual Private Network tunnels with Check Point VPN-1 Power/UTM gateways. The user connects to the gateway, authenticates using a certificate or single-user password, verifies the gateway’s fingerprint, and a secure session is established, automatically tunneling all network traffic between the user’s workstation and the gateway’s encryption domain.

Check Point remote access VPN solutions include SecureClient: an IPSec VPN client application, SSL Network Extender: a downloadable thin client invoked from a standard Web browser that provides a SSL VPN, and SecureClient Mobile: a SSL VPN implementation for mobile phones. All of these solutions are supported by the evaluated configuration.
CHAPTER 3

Security Guidelines

This section lists some basic security guidelines:

- **Logging In from a Secure Device:** You should not attempt to log in from an insecure device, such as a public terminal or a computer belonging to a friend. Even if the person owning the computer is trustworthy, the computer may not be, due to having been infected with malicious code.

- **Follow Client Operating System Security Guidance:** Remote access VPN client software is dependent on the underlying operating system to provide a protected domain of execution and cryptographic support for the establishment of VPN tunnels. Read and follow your operating system’s security guidance documentation, to ensure that your VPN client software is running in a protected environment.

- **Authentication Credential Handling:** Protect your authentication credentials, and do not allow others to use them. Your credentials authenticate you to the system, and if others gain access to these credentials, they may impersonate you in order to gain unauthorized access to computer resources.

- **Logging Out:** When you log out of the system and leave the device that you used for access (such as a terminal or a workstation with terminal emulation), you must ensure that you have not left information on the screen, or within an internal buffer that can be accessed by another user. Safe options include completely shutting down the client software used for access, powering down a hardware terminal, or clearing the scrollback buffer by switching among virtual terminals, in addition to clearing the visible screen area.
User Authentication
CHAPTER 4

Telnet Authentication

In This Chapter

Welcome Message  page 17
User Identification and Authentication  page 17
Authentication Failure Handling  page 18
Connection to Destination Server  page 18
Inactive Session Termination  page 18
Error Messages  page 19
Examples  page 20

Welcome Message

When the TCP session is established, the Telnet security server sends a welcome message, as configured by the administrator.

User Identification and Authentication

1. After the welcome message(s) is sent to the client, the Telnet security server prompts you for a username. (The Telnet security server does not accept a username longer than 256 characters.)
2. Then, once the username has been entered, you are prompted for a password.
3. When authentication succeeds, the Telnet security server sends you the following message: "User *user* authenticated by mechanism", where *user* is the username, and mechanism is either "SecurID" or "RADIUS authentication".

4. After successful authentication, if no information flow control rules match *user* or any of his group memberships, an error message will be displayed and the connection will be terminated.

**Authentication Failure Handling**

When a password authentication failure occurs, the Telnet security server prompts you for a username and password, again. This is allowed to occur within the same connection a preset number of times, *x*. After *x* failures, the connection is terminated by the security server.

**Connection to Destination Server**

Upon successful connection to the destination server, the Telnet security server sends you a “Connected to *host*” message (where *host* is replaced by the destination server’s hostname, or IP address).

**Inactive Session Termination**

An inactive Telnet session will be terminated after 15 minutes.
## Error Messages

<table>
<thead>
<tr>
<th>Condition</th>
<th>Message</th>
<th>Side Effects</th>
</tr>
</thead>
<tbody>
<tr>
<td>Communication failure with SecurID server</td>
<td>Access denied – wrong user name or password</td>
<td>Authentication failure</td>
</tr>
<tr>
<td>Communication failure with RADIUS server</td>
<td>Access denied – wrong user name or password</td>
<td>Authentication failure</td>
</tr>
<tr>
<td>Unsuccessful SecurID or RADIUS authentication</td>
<td>Access denied – wrong user name or password</td>
<td>Authentication failure</td>
</tr>
<tr>
<td>Unknown username</td>
<td>Access denied – wrong user name or password</td>
<td>Authentication failure</td>
</tr>
<tr>
<td>Username greater than 256 characters is specified</td>
<td></td>
<td>Connection is closed</td>
</tr>
<tr>
<td>Invalid RADIUS user</td>
<td>Invalid username in RADIUS authentication</td>
<td>Authentication failure</td>
</tr>
<tr>
<td>User database entry restricts the authenticated user from operating at the current time</td>
<td>Your login is restricted to <em>from</em> <em>to</em></td>
<td>Connection is closed</td>
</tr>
<tr>
<td>User database entry restricts the authenticated user from operating on the current day of the week</td>
<td>Your login is not allowed for <em>day</em> <em>day</em></td>
<td>Connection is closed</td>
</tr>
<tr>
<td>No User Auth rules match the user or any of his group memberships (after successful I&amp;A)</td>
<td>Access denied by FW-1</td>
<td>Connection is closed</td>
</tr>
<tr>
<td>Unable to connect to the destination server</td>
<td>Connection to <em>host</em> failed</td>
<td>Connection is closed</td>
</tr>
</tbody>
</table>
Examples

Telnet Authentication

In the example below, the user is prompted to enter his User Name and Password and is successfully authenticated:

![Telnet Authentication Example](image-url)
Wrong User Name

In the example below, access is denied because of wrong User Name and Password:
FTP Authentication

Welcome Message

1. When a control connection is established from the client to the FTP security server, the FTP security server will send you the following greeting message: "Check Point FireWall-1 Secure FTP server running on host", where host is replaced by the Check Point VPN-1 Power/UTM NGX R65 appliance host name, or IP address.
2. If no message is specified, the FTP security server sends you a new line.

User Identification and Authentication

After the welcome message, the FTP security server will prompt you for a username.
When the User Authentication mode is active, the FTP security server will expect one of the following inputs on the control channel:

- USER user@fw_user@host
- USER fw_user@host
- USER fw_user

fw_user is the user identifier in the evaluated configuration user database, user is the user name on the destination server, and host is the destination server host. host is ignored. (When using the first format, fw_user may contain the '@' separator character.)

If user is omitted, the FTP security server attempts to use fw_user for both the destination server and the evaluated configuration user database.

1. Once the user has been identified, this additional user security attribute (the fw_user user identity) is associated with the connection.
2. The FTP security server will expect you to enter a password.
   Supported formats are:
   - PASS password@fw_password
   - PASS password

Where fw_password is used for authentication to the evaluated configuration, and password is the destination server’s password. (When using the first format, password may contain the '@' separator character.)

1. If fw_password is omitted, the FTP security server will prompt for it. The evaluated configuration sends fw_user and fw_password to the RADIUS or SecurID server for validation.
2. As an alternative, the FTP security server may be configured to first prompt for a user and password to be sent to the destination server, and then for a user and password for authenticating to the evaluated configuration.
3. In the Remote Access VPN mode, the FTP security server does not require the user to perform additional identification and authentication. The client's USER and PASS commands will be forwarded to the destination server.
4. Once the user has been authenticated via the initial identification and authentication exchange, the FTP security server will allow the user to send additional USER and PASS commands to the destination server.

Connection to Destination Server

Upon successful connection to the destination server, the evaluated configuration will send you the following message: “Connected to host. Logging in...” (host is the destination server’s hostname, or IP address). The actual code will be determined later according to the server’s return code from the login process. The original message accepted from the server is then sent to you.
## Error Messages

<table>
<thead>
<tr>
<th>Condition</th>
<th>Code</th>
<th>Message</th>
<th>Side Effects</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client does not send a 'USER' command on the control connection within 60 seconds of connection establishment</td>
<td>202</td>
<td>'USER' command expected</td>
<td>Connection is closed</td>
</tr>
<tr>
<td>Client sends command other than 'USER' after connection establishment</td>
<td>202</td>
<td>'USER' command expected</td>
<td>Connection is closed</td>
</tr>
<tr>
<td>Username longer than 256 characters</td>
<td></td>
<td>User name too long</td>
<td>Connection is closed</td>
</tr>
<tr>
<td>Client sends a USER command not followed by a username</td>
<td></td>
<td>no arg to 'USER' command</td>
<td>User may retry entering a user name</td>
</tr>
<tr>
<td>Prompt for user password in Remote Access VPN mode</td>
<td>331</td>
<td>(not authenticated): Enter server password</td>
<td>None</td>
</tr>
<tr>
<td>No User Auth rules match the user or any of his group memberships (after identification)</td>
<td></td>
<td>connection not allowed by rule base</td>
<td>Connection is closed</td>
</tr>
<tr>
<td>User enters newline as password</td>
<td></td>
<td>you can use 'quote password' or Account command ('ACCT')</td>
<td>User may retry entering a password</td>
</tr>
<tr>
<td>Authentication failure</td>
<td>421</td>
<td>aborted</td>
<td>Connection is closed</td>
</tr>
<tr>
<td>User database entry has expired</td>
<td></td>
<td>Login expired on fix_date.</td>
<td>Connection is closed</td>
</tr>
<tr>
<td>User database entry restricts the authenticated user from operating at the current time</td>
<td></td>
<td>Your login is restricted to from to</td>
<td>Connection is closed</td>
</tr>
<tr>
<td>User database entry</td>
<td></td>
<td>Your login is not allowed</td>
<td>Connection is closed</td>
</tr>
<tr>
<td><strong>Condition</strong></td>
<td><strong>Code</strong></td>
<td><strong>Message</strong></td>
<td><strong>Side Effects</strong></td>
</tr>
<tr>
<td>------------------------------------------------------------------------------</td>
<td>----------</td>
<td>------------------------------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>restricts the authenticated user from operating on the current day of the week</td>
<td></td>
<td>for day <em>day</em></td>
<td>closed</td>
</tr>
<tr>
<td>Intersection with user database restricts authenticated user from accessing the destination server or from doing so from the presumed source address</td>
<td>421</td>
<td>You are not allowed to perform ftp to this destination</td>
<td>Connection is closed</td>
</tr>
<tr>
<td>FTP security server timeout (<em>au_connect_timeout</em>, default 10 seconds) in connecting to destination server</td>
<td>413</td>
<td>Connection to <em>host</em> failed</td>
<td>Connection is closed</td>
</tr>
<tr>
<td>Invalid FTP server reply</td>
<td>413</td>
<td>Unsupported server reply. Aborted</td>
<td>Connection is closed</td>
</tr>
<tr>
<td>Authentication to the destination server fails</td>
<td>421</td>
<td>aborted</td>
<td>Connection is closed</td>
</tr>
<tr>
<td>Unauthorized command</td>
<td>505</td>
<td>Command was blocked. Contact admin.</td>
<td>Command blocked</td>
</tr>
<tr>
<td>Unknown command</td>
<td>505</td>
<td>Security Server forbids unknown commands. Contact admin.</td>
<td>Command blocked</td>
</tr>
<tr>
<td>Command denied by resource rule</td>
<td>550</td>
<td>Security server forbids that action on this file</td>
<td>Command blocked</td>
</tr>
<tr>
<td>Command exceeds maximum command length (2047 bytes)</td>
<td>505</td>
<td>Command too long. Contact admin.</td>
<td>Command blocked</td>
</tr>
<tr>
<td>Unable to establish the data connection to the evaluated configuration</td>
<td>550</td>
<td>data connection establishment failed</td>
<td>None</td>
</tr>
<tr>
<td>Unable to connect data connection to the</td>
<td>550</td>
<td>data connection failure</td>
<td>None</td>
</tr>
<tr>
<td>Condition</td>
<td>Code</td>
<td>Message</td>
<td>Side Effects</td>
</tr>
<tr>
<td>--------------------------------------------------------</td>
<td>------</td>
<td>----------------------------------------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td>destination</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unable to send data</td>
<td>550</td>
<td>failed to write data</td>
<td>None</td>
</tr>
<tr>
<td>Data received in the wrong direction (i.e. when the evaluated configuration does not expect the client to send data)</td>
<td>550</td>
<td>Data on wrong direction</td>
<td>Connection is closed</td>
</tr>
<tr>
<td>Failure to listen on the data port</td>
<td>550</td>
<td>accept data connection failed</td>
<td></td>
</tr>
<tr>
<td>Error reading from sending side</td>
<td>550</td>
<td>data read error</td>
<td>Connection is closed</td>
</tr>
<tr>
<td>Unexpected termination of data connection</td>
<td>550</td>
<td>io error</td>
<td></td>
</tr>
<tr>
<td>Receiving side unexpectedly terminated</td>
<td>550</td>
<td>dst_dataconn ended unexpectedly</td>
<td></td>
</tr>
<tr>
<td>Memory allocation failure</td>
<td>425</td>
<td>Security server is out of memory</td>
<td>Connection is closed</td>
</tr>
<tr>
<td>Tracking failure</td>
<td>550</td>
<td>Security server failure(track)</td>
<td>Connection is closed</td>
</tr>
</tbody>
</table>
Examples

Wrong User Name

In the example below, authentication to the destination server fails, and the return code is 421:
Remote Access VPN
SSL Network Extender

In This Chapter

SSL Network Extender Download  page 31
Establishing the SSL VPN Session  page 32

SSL Network Extender Download

The SSL Network Extender client software must be installed on the user workstation for the user to be able to establish SSL VPN tunnels with a VPN-1 Power/UTM gateway. The software may be preinstalled by the workstation administrator, or it may be downloaded by the user from the gateway, using a standard Web browser. If the software has already been installed on your workstation, you may skip this section and continue to the Establishing the SSL VPN Session section.

Check Point VPN-1 Power/UTM gateways that have been configured to support SSL Network Extender provide a SSL Network Extender portal, accessed using the https protocol. For example, if your gateway’s name is “gateway.mycompany.com”, you can access the portal using your Web browser by entering “https://gateway.mycompany.com/” in the browser’s address bar.

The precise user experience will depend on your choice of browser and its configuration. The SSL Network Extender portal pages use Javascript to identify the browser platform and automatically download the client software packaged either as an ActiveX control or a trusted Java applet.
Depending on your security settings, the browser may request user confirmation for accessing the portal and for installing the client software. If automatic installation does not complete successfully, you may also download the SSL Network Extender client software package and install it manually on your workstation.

In order to prevent another Web server from impersonating your gateway portal and fooling you into downloading malicious software, it is imperative that you verify that the https session was indeed established with the intended gateway before acknowledging any security-related prompts. Most browsers will do this verification automatically, and provide appropriate feedback (e.g. Microsoft Internet Explorer will display a closed lock icon).

### Establishing the SSL VPN Session

After the SSL Network Extender client software is installed on the user’s workstation, access to the gateway’s SSL Network Extender portal will automatically pop up a login window in the browser.

If certificate-based authentication has been configured on the gateway, the browser will look for an applicable certificate in the user’s browser’s certificate store, and use it to establish the SSL VPN session. Depending on browser configuration, the user may be prompted to select a certificate to be used to authenticate to the gateway, and may be prompted to provide a password to approve use of the certificate for authentication.

If password-based authentication has been configured, the browser will prompt the user to enter a user name and password. If you are using a SecurID token for authentication, click the **Click for using SecurID** button and enter user name, password, and the SecurID-generated one-time code.
If the login fails, a “Wrong user name or password” or “Authentication failed” message will be displayed.

If this is the first time the user is connecting to this gateway from this user workstation, or if the gateway’s certificate has been updated, the SSL Network Extender client will pop up a gateway verification window, displaying the gateway’s identification and a certificate fingerprint. Compare the two displayed values to secure values that must be provided by the gateway administrator (e.g. in an email). If there is a mismatch, you must cancel the session and contact the administrator for assistance.
After both user and gateway have been mutually authenticated, the SSL Network Extender client software will reconfigure the user workstation’s operating system to route network traffic whose destination is inside the gateway’s encryption domain through a secure SSL VPN channel. The SSL Network Extender window shows the connection status, and the time remaining until the user is required to re-authenticate. The user may also manually disconnect the connection.
SecureClient Mobile

In This Chapter

SecureClient Mobile Installation  page 35
Establishing the SecureClient Mobile Session  page 36

SecureClient Mobile Installation

SecureClient Mobile is a Check Point SSL VPN resident client that provides SSL VPN functionality on mobile platforms such as cell phones and PDAs running Windows Pocket PC and Windows Mobile operating systems.

The SecureClient Mobile software must be installed on the user’s mobile device for the user to be able to establish SSL VPN tunnels with a VPN-1 Power/UTM gateway. The software may be downloaded by the user from the gateway, using a standard Web browser. Follow the directions provided above in the SSL Network Extender Download section for downloading the software. Run the client software package on the mobile device to install the software.
Establishing the SecureClient Mobile Session

Once installed on your mobile device, SecureClient Mobile provides behavior similar to that of the SSL Network Extender client, optimized for the mobile device user interface.

The precise user experience will depend on your choice of device and its configuration. Sample screen captures are depicted below.

Follow the directions given in the Establishing the SSL VPN Session section above for establishing and monitoring the SecureClient Mobile session.
CHAPTER 8

Other VPN Clients

In This Chapter

IPSec VPN Clients page 37

IPSec VPN Clients

Check Point provides a range of end point security products that provide remote access VPN capabilities compatible with VPN-1 Power/UTM, including Check Point SecureClient, Check Point Integrity SecureClient, and Check Point Endpoint Security. These clients are supported by the evaluated configuration, but they are not considered part of it. In particular, a Check Point VPN-1 Power/UTM gateway does not provide these clients as downloadable packages. The user must ensure that client software is securely delivered and installed on the user’s workstation or mobile phone, prior to using the client for establishing remote access VPN connections.

As described in the previous chapter, it is the user’s responsibility to verify that the client is connecting to a valid gateway, by comparing the gateway’s certificate’s identify and fingerprint with known values received from a trusted source.
THIRD PARTY TRADEMARKS AND COPYRIGHTS

Entrust is a registered trademark of Entrust Technologies, Inc. in the United States and other countries. Entrust’s logos and Entrust product and service names are also trademarks of Entrust Technologies, Inc. Entrust Technologies Limited is a wholly owned subsidiary of Entrust Technologies, Inc. FireWall-1 and SecuRemote incorporate certificate management technology from Entrust.

Verisign is a trademark of Verisign Inc.

The following statements refer to those portions of the software copyrighted by University of Michigan. Portions of the software copyright © 1992-1996 Regents of the University of Michigan. All rights reserved. Redistribution and use in source and binary forms are permitted provided that this notice is preserved and that due credit is given to the University of Michigan at Ann Arbor. The name of the University may not be used to endorse or promote products derived from this software without specific prior written permission. This software is provided “as is” without express or implied warranty. Copyright © Sax Software (terminal emulation only).

The following statements refer to those portions of the software copyrighted by Carnegie Mellon University.

Copyright 1997 by Carnegie Mellon University. All Rights Reserved.

Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of CMU not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission. CMU DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, IN NO EVENT SHALL CMU BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS; WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

The following statements refer to those portions of the software copyrighted by The Open Group.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE OPEN GROUP BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

The following statements refer to those portions of the software copyrighted by The OpenSSL Project. This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT "AS IS" AND ANY * EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The following statements refer to those portions of the software copyrighted by Eric Young. THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. Copyright © 1998 The Open Group.

The following statements refer to those portions of the software copyrighted by Jean-Ioup Gailly and Mark Adler. This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software. Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.

2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.

3. This notice may not be removed or altered from any source distribution.

The following statements refer to those portions of the software copyrighted by the Gnu Public License. This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version. This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details. You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 675 Mass Ave, Cambridge, MA 02139, USA.

The following statements refer to those portions of the software copyrighted by Thai Open Source Software Center Ltd and Clark Cooper Copyright (c) 2001, 2002 Expat maintainers. Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the Software), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions: The above copyright
notice and this permission notice shall be included in all copies or substantial portions of the Software. THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.


Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at http://www.apache.org/licenses/LICENSE-2.0

The curl license

COPYRIGHT AND PERMISSION NOTICE

Copyright (c) 1996 - 2004, Daniel Stenberg, <daniel@haxx.se> All rights reserved.

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization of the copyright holder.

The PHP License, version 3.0

Copyright (c) 1999 - 2004 The PHP Group. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, is permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The name "PHP" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact group@php.net.
4. Products derived from this software may not be called "PHP", nor may "PHP" appear in their name, without prior written permission from group@php.net. You may indicate that your software works in conjunction with PHP by saying "Foo for PHP" instead of calling it "PHP Foo" or "phpfoo"
5. The PHP Group may publish revised and/or new versions of the license from time to time. Each version will be given a distinguishing version number. Once covered code has been published under a particular version of the license, you may always continue to use it under the terms of that version. You may also choose to use such covered code under the terms of any subsequent version of the license published by the PHP Group. No one other than the PHP Group has the right to modify the terms applicable to covered code created under this License.
6. Redistributions of any form whatsoever must retain the following acknowledgment: "

This product includes PHP, freely available from <http://www.php.net/>".

THIS SOFTWARE IS PROVIDED BY THE PHP DEVELOPMENT TEAM "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE PHP DEVELOPMENT TEAM OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.