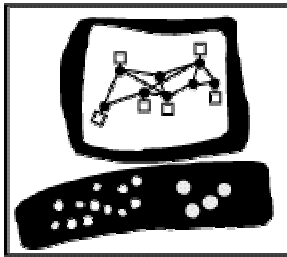


CHECK POINT™
Software Technologies, Inc.



We Secure the Internet.

OPSEC Certification Technical Note

Log Export API (LEA) Next Generation Architecture

August 2001



1. Introduction

OPSEC™ certified products using the Log Export API (LEA) interface certified with FireWall-1™ or VPN-1™ versions 4.1 and before will need to be re-certified with the new Next Generation (NG) architecture.. Due to architectural changes that provide powerful new features and the natural evolution of the API, the LEA Server in NG will not be backwards compatible with LEA clients built with previous versions of the OPSEC SDK. All Check Point customers using the new NG product will require an NG compatible version of your product for interoperability.

Please review the following scenarios to see if your product integration with LEA matches one and follow the appropriate actions provided. If none of the scenarios match your LEA integration, please contact your OPSEC Alliance Manager.

Scenario 1 – Current shipping release is OPSEC certified, need to test NG compatibility

Using LEA Interface	YES
OPSEC certified product version is the same as your current release	YES
Application was built using OPSEC SDK v4.1.2 or before	YES

Please re-submit your application for OPSEC NG certification as soon as possible. **The certification fee will be waived until the last business day of December 2001.** The certification will test your current version for compatibility with our new NG products. Once verified as compatible with NG, we will designate your product as “NG Compatible.”

Scenario 2 – Current shipping release is not OPSEC certified, need to certify!

Using LEA Interface	YES
Current released version is OPSEC certified	NO
Application using OPSEC SDK v4.1.2 or before	YES

Please submit your non-certified current release for OPSEC certification with the appropriate certification submission document and fee. Your current release needs to be OPSEC certified and will be tested for NG compatibility. Once certification is complete, we will include you in our “NG Compatible” listing.

Scenario 3 – Submit NG OPSEC SDK compiled application with new features

Using LEA Interface	YES
Application using OPSEC SDK v4.1.2 or before	YES
Would like to re-compile using the new NG OPSEC SDK adding new application functionality with LEA	YES

Please submit your application for OPSEC NG certification with the certification fee. Once certified the application will be clearly noted on our web site as “NG Certified” and your certification listing will be updated noting your new LEA features. Note that the NG compiled version will only function with NG released products, not prior versions. Please submit early, you will want to publicize your new LEA features to our customers and resellers.

Scenario 4 – New LEA integration partner, first certification!

Using LEA Interface	YES
Developing a new LEA integrated application solution	YES

Please use the OPSEC SDK NG. All previous bug fixes have been rolled into this release. The SDK NG also has many new powerful features that you can take advantage of in your application. Upon completion of QA testing, submit your application for OPSEC certification with the completed certification submission forms and fee. Once certified, your application will be noted as “NG Certified” on our OPSEC web site. Note that the NG compiled version will only function with NG released products, not prior versions.

Again, if your product does not fit any of the above scenarios, please contact your OPSEC Alliance Manager for clarification.

2. LEA Server Changes in FireWall-1 and VPN-1 NG Releases

The sections below review changes in the LEA Server for FireWall-1 and VPN-1 NG product releases. Please see the OPSEC SDK NG documentation for complete information on new LEA features and other APIs in the OPSEC SDK NG. This document focuses on changes to the LEA API so partners can quickly review them and certify their products with minimal effort for NG.

2.1 Field Changes

Field in 4.1	Field in NG	Comments
Sys_msgs	Sys_message:	Name change
ISAKMP Log:	IKE Log:	Name change (changed in 4.1 SP 3)

SPI:		Manual IPSec not available in NG, therefore the field is no longer available
Negotiation Id:	CookieI CookieR	<p>“Negotiation Id:” is the concatenation of CookieI and CookieR, separated by a dash.</p> <p>There are no changes in the content, only in the meaning of the field. If the dash is there, it’s in IKE phase 1, if not, it’s IKE phase 2.</p> <p>In FireWall-1/VPN-1 4.1 SP3 and above, the content will be in the msgid field rather than in Negotiation ID:</p>
Product	Product	Content changed from “FW1” or “FG” to have the names of all the relevant products concatenated, separated with a “\n”.

2.2 File Access Changes

2.2.1 File Extension Completion

In some situations the 4.1 LEA Server associated log files with extensions. For example, opening a file named “fw” would result in the opening of “fw.log” in LEA_NORMAL_FILENAME mode, and “fw.alog” in LEA_ACCOUNT_FILENAME mode.

The NG LEA Server will only open files with exact filenames.

When a LEA session is opened in some modes like “LEA_FIRST_NORMAL_FILEID” or “LEA_CURRENT_ACCOUNT_FILEID” where the filename is inferred from the logtrack, the LEA Server will open the appropriate file.

2.2.2 Files with “.alog” extension

FireWall-1 and VPN-1 NG releases does not store the account information in a separate log file. So the “.alog” files do not exist.

2.3 Content Changes

In FireWall-1 and VPN-1 v4.1, alerts in the alerts dictionary appear inside square brackets with a leading exclamation mark (e.g. “![mailalert]”). In the new release, alerts have been simplified (e.g. “mailalert”).

The “product” field in FireWall-1 and VPN-1 v4.1 always contained “VPN-1 & FireWall-1” for Check Point log records, and perhaps other values in log records

written by vendors using the ELA interface. In NG, more than one Check Point product might want to give an opinion about a single connection. Therefore more than one value might exist in a single field, separated by new lines.

For example, “VPN-1 & FireWall-1\nFloodgate-1\n...”.

*** End of Document ***