



We Secure the Internet.

OPSEC SDK Support of InterSpect 2.0

September 28, 2004



In This Document

<i>Introduction</i>	page 1
<i>Supported OPSEC services</i>	page 1
<i>LEA</i>	page 2
<i>ELA</i>	page 2
<i>SAM</i>	page 3
<i>Configuration</i>	page 3

Introduction

This document summarizes the OPSEC SDK support on InterSpect 1.5. It lists the OPSEC services that are supported on InterSpect, and offers instructions about configuring an OPSEC application.

The OPSEC SDK referred to in this document is OPSEC SDK NG FP3. There is currently no OPSEC SDK that supports additional InterSpect features.

This document contains important information. Please review this information before using the OPSEC SDK with InterSpect.

Up-to-date information about OPSEC SDK can be found at: <http://www.opsec.com/>

Latest Hot-Fix of the OPSEC SDK NG FP3 can be found at:
http://www.checkpoint.com/techsupport/ng/fp3_hotfix.html

Up-to-date information about InterSpect can be found at:
<http://www.checkpoint.com/products/enterprise/interspect.html>

Supported OPSEC services

The following OPSEC services are supported on InterSpect 1.5:

- LEA
- SAM

-
- ELA

LEA

InterSpect supports all VPN-1/FireWall-1 LEA features.

In addition the following new actions were added to InterSpect.

TABLE 1 New Action Types supported on InterSpect

Action	Meaning
Bypass	The connection was allowed without inspection of the configured network and application-level attacks.
Inspect	The connection was inspected and was not blocked.
Quarantine	The host that generated the connection was quarantined.
Block	The attack was blocked.
Monitor	The attack was logged instead of blocked.

ELA

InterSpect supports all the VPN-1/FireWall-1 ELA features.

The new action types listed in Table 1 can be sent with ELA. Although these actions are not defined in the SDK, they can be sent with ELA API by using their corresponding numerical values, specified in the following table.

TABLE 2 Numerical Values of New InterSpect Actions for ELA

Action	Meaning
Bypass	30
Inspect	31
Quarantine	32
Block	33
Monitor	34

The numeric values listed in Table 2 can be sent as the logfield argument of *ela_log_add_field* or *ela_log_add_raw_field*.

For example, the following call will add a quarantine action to the log:
ela_log_add_raw_field(log, "action" , ELA_VT_STRING, NULL, "32");

SAM

InterSpect supports all the VPN-1/FireWall-1 SAM features.

Configuration

In InterSpect, OPSEC applications can only be configured from the command line.

Configuration requires the following 3 basic steps:

- 1 Allowing the OPSEC services to connect to the InterSpect machine, both for configuration and operation.
- 2 Configuration of the OPSEC application in the InterSpect database by using the Roaming Administrator utility.
- 3 Pulling a certificate for the application.

Steps 2 and 3 may be done implicitly by the OPSEC application, as part of its installation procedure.

These steps are the same as the configuration steps required for VPN-1/FireWall-1, when configured from command-line.

Step 1: Allow OPSEC services on InterSpect

In order to connect to the InterSpect machine with the different OPSEC services, the ports listed in the following table (Table 3) must be allowed:

TABLE 3 Ports Required for OPSEC Applications

Port	Service	Comment
18183	SAM	
18184	LEA	
18187	ELA	
18191	RoamAdmin	For remote configuration of an OPSEC application
18210	CA	For pulling a certificate for the OPSEC application

To allow the ports listed in Table 3 edit the *implied_rules.def* file, located in *\$FWDIR/lib* directory.

The port numbers must be added to the ports list belonging to the `mgmt_tcp_port_list` attribute.

For example, the following line will allow all OPSEC ports:

```
mgmt_tcp_port_list = { 22, 443, CPML_PORT, CP_reporting, CPRID_PORT, 18183, 18184, 18187, 18191, 18210};
```

Important Points to Remember

- The machines that need to access the ports listed in Table 3 should connect to the InterSpect machine through the management interface.
- Only the OPSEC ports that will be used should be configured. For example if LEA is not used, the LEA port (18184) should not be added.
- The RoamAdmin and CA ports should only be opened during the configuration stage. Once the OPSEC application is configured they may be removed from the list.
- The RoamAdmin port should only be configured if configuration is performed from a remote location. If RoamAdmin is executed locally, the addition of the RA port to the list of open ports is not required.
- The CA port should only be configured if the OPSEC application is installed on a remote host and uses SSLCA authentication and encryption methods.

Once the `implied_rules.def` is ready, the configuration must be committed.

The configuration is committed by installing the InterSpect policy with the following command: `fwm load $FWDIR/conf/Amazonas.W`

To remove any of these ports:

- 1 Remove the ports from the `implied_rules.def` file
- 2 Re-install the policy

Step 2: Application Configuration

The OPSEC application must be configured in the InterSpect database, by using the RoamAdmin utility. This utility is distributed with the OPSEC SDK.

Information about the RoamAdmin utility can be found in `RA_NG_FP3.pdf`. This file is part of OPSEC NG FP3 documentation and can be found at:

http://www.checkpoint.com/techsupport/ng/fp3_updates.html#docs

The use of RoamAdmin is disabled by default and must therefore be enabled. To do this, use the Database Tool (`GuiDBedit`), which is located in the installation directory of SmartDashboard for InterSpect. In the **Tables** tab, go to the **Global Properties** table, edit the `firewall_properties` object, and change the value of the `allow_remote_ra` field to `true`.

This utility can be executed either locally (on the InterSpect machine) or from a remote host. If executed from a remote host, the RA port must be enabled (See TABLE 3)

The use of RoamAdmin is disabled by default and therefore must be enabled. This can be done using the following dbedit command:

```
modify properties firewall_properties allow_remote_ra true
```

The following steps should be performed in order to configure an OPSEC application:

1.1 Register the OPSEC Application's Host Machine

Register the OPSEC application using the `RoamAdmin addnet` command. Refer to the *Register Target Host* section in the *RA* document.

Note - the `-mgmt` option should be given the InterSpect management interface IP.

1.2 Configure the OPSEC Product

All OPSEC products defined in VPN-1/FireWall-1 NG with Application Intelligence exist in the InterSpect database.

The list of OPSEC products is kept in the products table of the database.

`$FWDIR/bin/queryDB_util` can be used for viewing the list.

For example:

```
>queryDB_util
```

```
Enter Server name: localhost
```

```
Please enter a query: -t products
```

If a product does not exist in the list it can be added using the `RoamAdmin addprod` command. Refer to the *Register OPSEC Product* section of the *RA* documentation for additional information.

2.3 Configure the OPSEC Application

Add the OPSEC application of a given product and attach it to a host machine with the `RoamAdmin addapp` command.

Refer to the *Register OPSEC Application Object* section of the *RA* documentation for additional information.

2.4 Generate a Certificate

When generating a certificate for the OPSEC application, run the `RoamAdmin gencert` command.

Refer to the *Generate Certificate* section of the *RA* documentation for additional information.

Note - The OPSEC application configuration must be applied by installing the InterSpect policy. This can be done either from the command-line with the following command: `fwmm load $FWDIR/conf/Amazonas.w` or by activating the settings in the InterSpect SmartDashboard application.

Step 3: Certificate Retrieval

The certificate generated with the `RoamAdmin gencert` command can be retrieved with the `opsec_pull_cert` utility. This utility is distributed with the OPSEC SDK.

Refer to the *Pulling Certificate* section in the `OPSEC_NG_FP3.pdf` for additional information.

This document is part of the *OPSEC FP3* documentation found at:

http://www.checkpoint.com/techsupport/ng/fp3_updates.html#docs