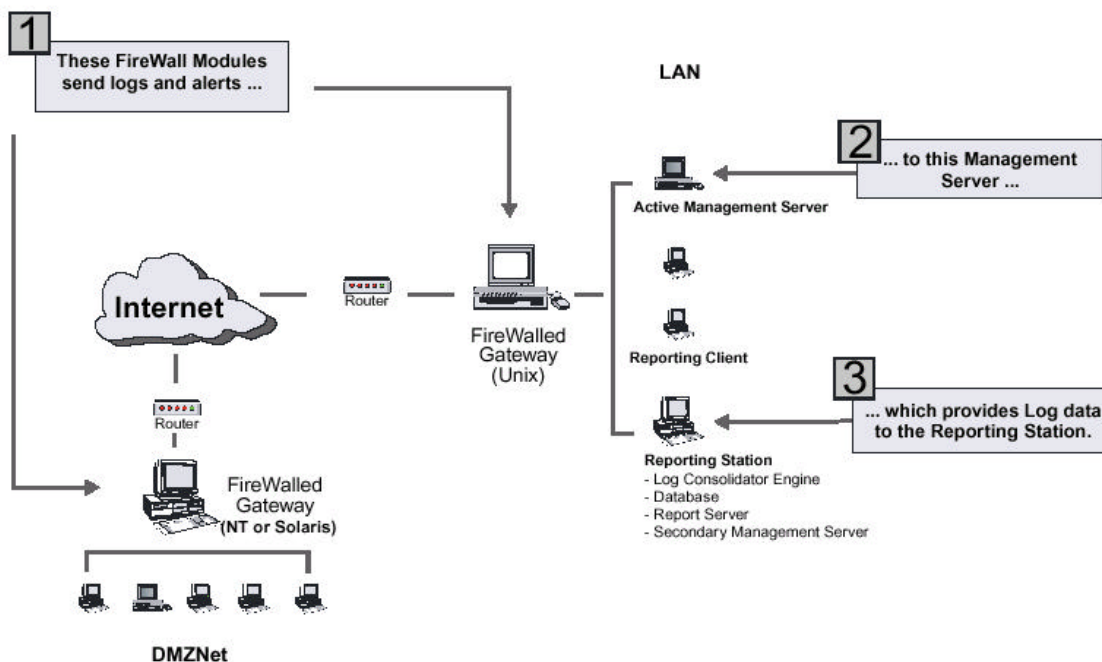


Configuring the Standalone Reporting Module

Authored By: Vladimir Sokol
Date: May 22, 2000
Purpose: To describe and document how to configure the Standalone Reporting Module
Configuration
Credits: Rakefet Ackerman, Sanjit Shah
Version: 1.0

Configuring Standalone Reporting Module

Reporting Module components including Reporting Server are installed on a separate machine from the active FireWall-1 Management Server. An additional FireWall-1 Management Server dedicated to the Reporting Module system is passive — it does not manage a Security Policy for FireWall-1 Modules.



This configuration is appropriate for organizations that do not want to install the Reporting Server components on the same machine as the active FW-1 Management Server that maintains and installs the Security Policy.

All FireWall Modules send log and alert data to the active FW-1 Management Server *only*. The secondary (passive) Management Server does not receive log messages. The active FW-1 Management Server collects log events and creates *.log and *.alog files in the \$FWDIR/log directory. The Log Consolidator Engine on the Reporting Station (which is installed on the machine with the passive FW-1 Management Server) retrieves log data from the active Management Server according to the Consolidation Policy.

Reporting Station Components

The following components are installed on the Reporting Station:

1. Reporting Server (includes the Log Consolidator Engine, the Report Server and the Database)
2. FireWall-1 Management Server
3. Reporting Client can be installed on the Reporting Station or on a separate machine.

Things to Consider:

- A license for the passive FW-1 Management Server is supplied with the Reporting Module license.
- Communication between the Active FireWall-1 Management Server and the Reporting Station must be enabled.
- Files on the Active FireWall-1 Management Station must be manually copied to the Reporting Station whenever FireWall-1 object databases are updated.

Note – Both the active Management Server and the secondary Management Server must be FireWall-1 Version 4.0 SP-2 or higher (Windows NT version 4.1 or higher) or FireWall-1 Version 4.0 SP-6 (Solaris) or FireWall-1 Version 4.1 SP-1 (Solaris), and the same version.

Configuring the Reporting Station

Before you begin, you must decide if Log data from the active Management Station is transferred to the Reporting Station in standard or authenticated mode. Authenticated mode requires a key exchange between the Management Station and the Reporting Station.

Configuration Overview

On the Active Management Server

1. Modify `$FWDIR/conf/fwopsec.conf`
2. Perform "fw putkey" on the Management Server with the Reporting Station IP Address
3. Allow a rule for the Reporting Station to talk with the Management Server.

On the Reporting Station

1. Validate the configuration of the "lc_rt_lea.conf" file on the Reporting Station
2. Perform "opsec_putkey.exe" on the Reporting Station with the Management Server IP Address
3. Copy the following files from the Management Station to the Reporting Module:
 - `$FWDIR/conf/objects.C`
 - `$FWDIR/conf/fwauth.NDB`
4. Enable LEA communication between the active Management Station and Firewallled Reporting Station in the Security Policy if Firewall Module is installed on the Reporting Station.
5. Allow remote Reporting GUI access to the Reporting Server if necessary.
6. Allow Administrator permission – in 4.1 Reporting Tool and Log Consolidation specific permissions, in 4.0 FW-1 user permissions are used.
7. Allow GUI client access – the clients' working station IP must be defined on the Reporting stations, to be permitted to work.

On the Active Management Server

1. The file `$FWDIR/conf/fwopsec.conf` includes a configuration line for a LEA (Log Export API) server. A LEA server sends FireWall-1 log events to a LEA client for processing. In this case, the LEA server is the active FireWall-1 Management Server, and the LEA client is the Reporting Station.

You must configure the LEA server line in one of the following ways:

For Standard Communication:

```
lea_server port 18184
```

For Authenticated Communication:

```
lea_server auth_port 18184
```

If you modify the `$FWDIR/conf/fwopsec.conf` file you must stop and then restart the FireWall-1 service. You can stop and restart the FireWall-1 service using the Windows Control Panel's Services dialog.

2. If you are using authenticated communication, then you must supply a password that will be used to authenticate control connections between the active Management Server and the Reporting Station.

In the `$FWDIR/bin` directory, enter the following command:

```
fw putkey -opsec <IP or name of Reporting Station>
```

You will be prompted to enter a password of at least 6 characters. You will later use this password when you configure authenticated communications on the Reporting Station host.

3. In the FireWall-1 Security Policy, you must allow the Reporting Station to communicate with the active Management Server using the FireWall-1 LEA service. Define a rule similar to the following:

Source	Destination	Service	Action	Track	Install On
 ReportingStation	 Active_Management	 FW1_Jea	 accept	 Short	 Gateways

On the Reporting Station

1. The `lc_rt_lea.conf` specifies the configuration of the LEA server. By default, this file is located in the following directory on the Reporting Station:

```
C:\Program Files\Check Point\Reporting Server\Log Consolidator Engine\conf
```

You must modify the `lea_server port` line in this file to support the communication mode you defined on the active Management Server:

For Standard Communication:

```
lea_server port 18184
```

For Authenticated Communication:

```
lea_server auth_port 18184
```

2. On the `lea_server ip` line, change the IP address of the LEA server to the IP address of the active Management Server:

```
lea_server ip <IP of active management server>
```

If you are using authenticated control communications, then perform the following steps:

1. Make sure the FireWall-1 service is running on the Reporting Station machine. To start the FireWall-1 service, enter the `fwstart` command on the Reporting Station. You can also start the service using the Windows Control Panel.
2. The `opsec_putkey.exe` file is located by default in the following directory on the Reporting Station:

```
C:\Program Files\Check Point\Reporting Server\Log Consolidator Engine\bin
```

Execute this file with the name or IP address of the active Management Server as the parameter. You will be prompted for a password. You must use the same password you used when you issued the `fw putkey` command on the active Management Server. You will receive a message notifying you whether the `fw putkey` command succeed or failed.

If authentication is successful, the `authkeys.C` file is created. Copy this file to the `\Log Consolidator Engine\conf` directory on the Reporting Station.

If authentication is not successful, the FireWall-1 service may not be running, or you may have entered the wrong password.

- If the FireWall-1 service is stopped, restart the FireWall-1 service.
- If you used the wrong password, reenter the password using the `fw putkey` command.

Before you retry the password, it is recommended to delete the `authkeys.C` file on the Reporting Station and the `opsec_authkeys.C` file on the active Management Server.

Copying and Updating Directories

You must copy the following files from the active Management Server to the `$FWDIR/conf` directory on the Reporting Station:

```
$FWDIR/conf/objects.C
$FWDIR/conf/fwauth.NDB
```

Warning – These files must be copied to the Reporting Station each time FireWall-1 object and user definitions are modified on the active Management Server.

If a FireWall Module is Installed on the Reporting Station

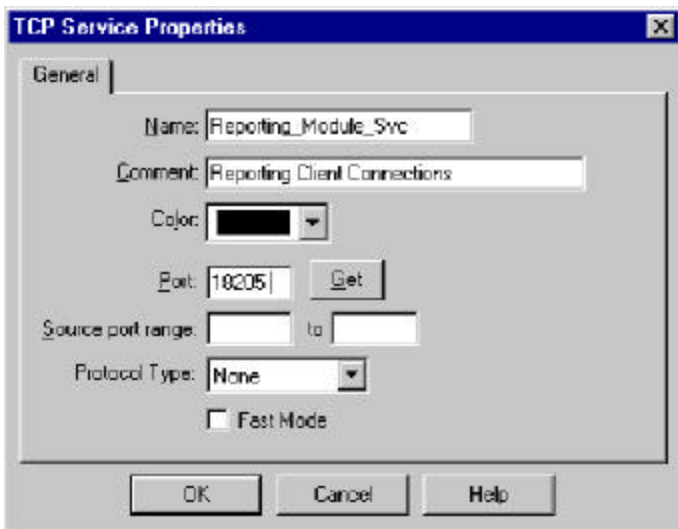
If there is a FireWall Module installed on the Reporting Station, you must enable LEA communications between the active Management Station and the FireWalled Reporting Station in the FireWall-1 Security Policy. Define a rule which allows the FW1_lea service between the Reporting Station and the active Management Station and the FireWalled Reporting Station.

Source	Destination	Service	Action	Track	Install On
ReportingStation	Active_Management	FW1_Lea	accept	Short	Gateways

Allowing Access From Remote Reporting Clients

If you have remote Reporting Tool GUI clients, the FireWall-1 Security Policy must allow these remote clients to connect to the Reporting Station.

1. In the FireWall-1 Rule Base, define a TCP service on port 18205



Port 18205 is the default port used for communications with the Reporting Server.

This port is listed in the `Reporting Client\RTClient.conf` file (on the GUI client) in the following line:

```
RT_SRV_PORT = "18205"
```

This port is also listed in the `Reporting Server\RTServer.conf` file (on the Reporting Station) in the following line:

```
RT_SERVERPORT = "18205"
```

If you change the port number of the Reporting Server in the above configuration files, you must also update the Reporting service properties in the FireWall-1 Rule Base.

2. Define a rule that allows Reporting service connections between the remote client and the Reporting Station.

Source	Destination	Service	Action	Track	Install On
RemoteReportClient	ReportingServer	ReportingService	accept	Short	Gateways

Define the FireWall-1 Administrators and GUI clients that are allowed to use the remote Client with the Reporting Station.

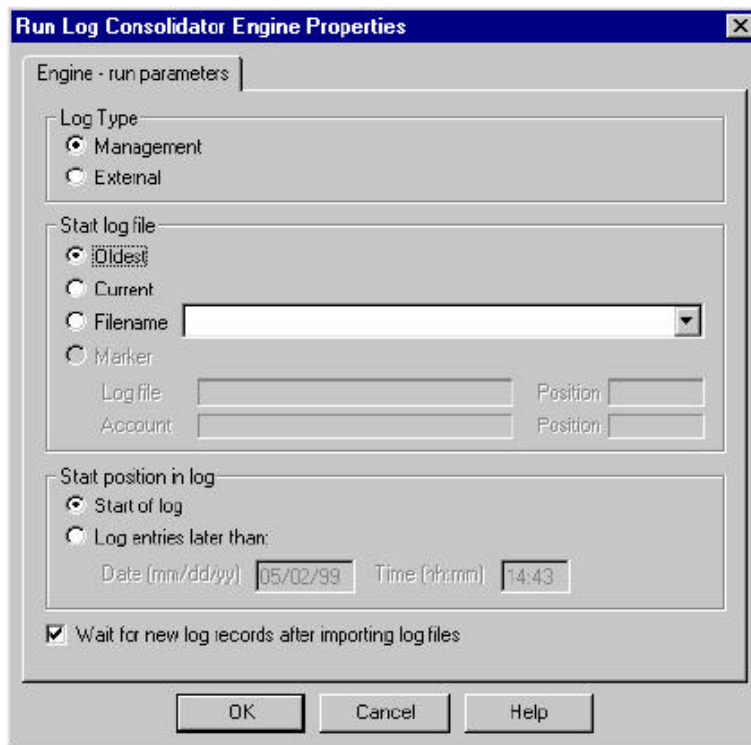
Installing the Consolidation Policy

Log File Types

When you install a Log Consolidator Policy, you can choose to process one of two Log Types:

■ **Management** — Log files generated and maintained by the FireWall-1 Management Station. In the configuration shown, this is the active FW-1 Management Station.

■ **External** — External logs are log and accounting files copied to the active Management Server from another machine. These logs are copied to the `$FWDIR/log` directory of the active Management Server from either a FireWall Module or another logging station.



Processing Management Logs

It is recommended to process Management logs in the following situation:

- the active Management Server collects log data from the FireWall Modules on a continual basis
- you want to use a background process to load logged events online — the Log Consolidator Engine processes new log events as they are recorded in the log file.

When you install a Log Consolidator policy, you configure the Log Consolidator Engine to process Management logs.

Processing External Logs

In order to consolidate logs from external logging stations, you must:

1. Copy log files (`*.log`) and their corresponding account log files (`*.alog`) from each logging station to the `$FWDIR/log` directory on the passive Management Server. The passive Management Server is on the same machine as the Reporting Server components.

There is no automatic mechanism for copying log files. Log files must be copied manually. It is recommended rename the log files to indicate they are from an external location (for example, `04May_extlogs4.log`, `04May_extlogs4.alog`).

2. Copy the following files from the logging station to the `$FWDIR/conf` directory on the passive Management Server.:

```
$FWDIR/conf/objects.C  
$FWDIR/conf/fwauth.NDB
```

The above files must be copied in order to maintain synchronization between object databases on the logging stations and object databases on the passive Management Server. These files are used for resolving IP Addresses before going to DNS, and network object resolution before the consolidation step. For example, in case the Log

Consolidation policy includes group, the objects database is used to extract the list of IP's this rule is effective for. Also, these files are used for the network object resolving for reporting. In case the report criteria includes for example a group, it makes use of the objects database to extract the items for which the report is effective

3. Install the Log Consolidator Policy. When you install the Log Consolidator Policy, you must choose the log type and log file that will be processed. Files copied to the Reporting Station from other logging stations are processed as external logs.