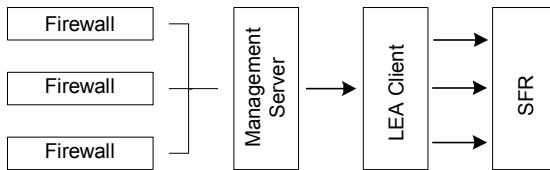


Overview

Stonylake Firewall Reporter uses the LEA Client component to connect to the Check Point firewall to receive logs. Logs are generated at the Check Point Firewall Module and by default, are continuously sent to the Check Point Management Server. The Management Server contains a component called LEA Server. The LEA Client connects to the LEA Server using TCP 18184 to receive firewall logs. The LEA Client then sends them on to SFR Logging Engine (SLE) using UDP.



Lea.conf configuration:

Edit the c:\program files\sfr\lea\lea.conf file. There are two sections in the file that need editing.

```
# [LEA Server Configuration]
lea_server ip 192.168.1.3 (this is the Management Server IP address)
lea_server port 18184
```

```
# [SFR Logging Configuration]
# FIREWALL_NAME FIREWALL_IP_ADDRESS ILE_IP_ADDRESS PORT
CPNG-NY          192.168.1.1          127.0.0.1      514
CPNG-SF          192.168.1.2          127.0.0.1      515
```

In the example above, 192.168.1.3 is the IP address of the Management Server that manages two Checkpoint Firewall Modules – one named CPNG-NY with IP address 192.168.1.1 and the other named CPNG-SF with IP address 192.168.1.2.

NOTE: Firewall Name above is case sensitive.

The LEA Client receives the logs on one single connection with the LEA Server but sends the data to the ILE using a separate UDP stream for each Firewall Module. In the example above, two UDP streams are used to send the log data to the ILE.

To determine the correct values for Firewall_Name and Firewall_IP_Address, first ensure that the Lea Server values are correct and that the necessary modifications are made to the fwopsec.conf and Policy. Then run the LEA client by executing lea.exe. The LEA client should connect and will display possible values. For example, if CPNG-NY is not specified correctly you will see:

```
Ignoring Data From [CPNG-NY]
Ignoring Data From [CPNG-NY]
...
```

The correct value can also be determined from the Checkpoint Log Viewer. It will be the value of the field named Origin.

Running the LEA Client:

The LEA Client can be run in the foreground by executing lea.exe. When the LEA Client is correctly configured, a stream of log data will be seen in the lea.exe window. Once the LEA Client is working satisfactorily, it can be run as a Windows service. The LEA Client is installed as

Management Server Configuration

1. Create a rule in the Security Policy if necessary to permit connections on TCP 18184 from the LEA Client (also the Firewall Reporter) machine to the Management Server.

Source = your LEA Client host (create one first if necessary) or the Local Net.
 Destination = the Management Server
 Service = Fw1_lea (TCP port 18184)
 Action = Accept

2. On the Check Point Management Server, open the file named fwopsec.conf found in the \$FWDIR\conf folder of the Check Point installation and locate the lines:

```
#lea_server auth_port 18184
#lea_server port 0
```

Change the lines to read as follows:

```
lea_server port 18184
lea_server auth_port 0
```

If the lines are missing, add them to the file.

Note that *auth_port* is changed to *port* and vice versa.

Reboot the Management Server.

3. By default Check Point FireWall-1 does not capture extended URL information. To capture extended URLs, first setup a Resource named URL. Then add (or modify) rules for http and ftp services using the "Add with Resource" option for the Service parameters choosing the resource named URL.
4. For every rule in the Security Policy that you want reports on the bandwidth utilized by that rule, set its 'Track' value to 'Accounting'.