

Stonylake Firewall Reporter

Version 4.1.0

User Guide

© Copyright 2004



TABLE OF CONTENTS

1.	WHAT'S NEW	1
2.	OVERVIEW	1
	<i>System Requirements</i>	2
	<i>Supported Firewalls</i>	2
	<i>Supported Browsers</i>	3
3.	INSTALLATION	4
	<i>Overview</i>	4
	<i>Trial version</i>	6
	<i>Quick Installation Steps</i>	6
	<i>Installation on Windows</i>	7
4.	INSTALLATION ON LINUX	9
5.	CONFIGURATION.....	11
	<i>Overview</i>	11
	<i>Details</i>	11
	<i>Firewall Configurations</i>	14
	<i>IIS and Apache Web Servers</i>	26
	<i>Other Settings</i>	26
6.	USING SFR	27
	<i>Starting and Stopping SFR</i>	27
	<i>Viewing Reports</i>	28
	<i>Summary Screen</i>	29
	<i>Server time</i>	29
	<i>Admin Settings</i>	29
	<i>Printing a Report</i>	30
	<i>Help</i>	30
	<i>'About' Box</i>	30
	<i>Reports for a single or group of firewalls</i>	31
	<i>Report Settings</i>	31
	<i>Generating a Report</i>	34
	<i>Understanding Reports</i>	34
	<i>Interacting with Reports</i>	35
7.	SFR CONTROL CENTER.....	37
	<i>Licensing</i>	38
	<i>Database</i>	39
	<i>Services</i>	40
	<i>System</i>	41
	<i>Auditors</i>	42
	<i>Firewall Groups</i>	43
	<i>User Groups</i>	44

<i>Destination Groups</i>	44
<i>SLE (SFR Logging Engine)</i>	45
<i>Processors</i>	47
8. ANOMALY DETECTION SYSTEM.....	53
<i>Average values calculation</i>	53
<i>Configuration</i>	53
<i>Rules</i>	54
<i>Suggested Rules</i>	54
<i>ADS Password</i>	55
<i>Available List of Services</i>	55
<i>Initial Operation</i>	55
<i>Memory Usage</i>	55
9. PERMANENT LICENSE KEY.....	56
<i>How to Obtain</i>	56
10. UNINSTALL.....	56
11. TROUBLESHOOTING.....	56
<i>System Checks</i>	56
<i>Error Log Files</i>	57
<i>Common Problems and Solutions</i>	57
12. TECHNICAL SUPPORT.....	60

1. WHAT'S NEW

In Version 4.1.0

1. Support for Remote Data Processors

In Version 4.0.2

1. Support for PIX 7.x
2. Changes in startup scripts
3. Minor Bug Fixes in error handling

In Version 4.0.1

1. Support for file processing for PIX.
2. Support for Check Point™ LEA authenticated connection
3. Option for Check Point™ LEA debugging mode
4. Changes pertaining to non-English locale
5. Changes pertaining to connections between SFR and MSDE
6. Improvements in stopping SFR services on Windows
7. Enhancements to un-installation process.

2. OVERVIEW

Stonylake Firewall Reporter (SFR) is a browser-based application for reporting firewall traffic statistics in real time. The application provides standard reports that are configurable via user-selected criteria. Selection and navigation are achieved through a simple interface using standard tools.

Stonylake Firewall Reporter comes in two editions -

Standard Edition: Suitable for firewalls having a small traffic load, this edition has a limitation of supporting only the MSDE 2000 database with a maximum storage capacity of 2GB. Additionally, it can log data from one firewall only and some features are not available in the Standard Edition.

Enterprise Edition: Suitable for all capacities of firewalls, this edition supports multiple, mixed set of firewalls simultaneously from a single, centrally installed and managed system. This edition supports MS SQL Server 2000 and PostgreSQL 7.x databases.

A pure Java application, SFR can be installed on any operating system that supports Java. Firewalls are configured to send their logs via Syslog to SFR where they are analyzed and consolidated. MSDE, MS SQL Server or PostgreSQL databases are used to store the consolidated logs in the Enterprise and MSDE in the Standard Edition. In both editions,

the software can be installed on one single machine or distributed over a group of machines.

Reports, as well as the SFR Control Center - the utility for system management are both browser based.

System Requirements

Given below are the **minimum** system requirements to operate SFR. These configurations will support a 100 firewall-user base. For more firewall users, machines having more memory and higher processor speeds will be necessary.

Windows XP/Windows 2003/ Windows 2000/Red Hat Linux 9/Fedora Core3

Dedicated Application server

512 MB RAM
1.1 GHz processor
5 MB free hard drive space for SCC, IRE, SLE
100 MB free hard drive space for temp log files
20 MB free hard drive space for Tomcat
65 MB free hard drive space for JDK

Dedicated Database server

512 MB RAM
1.1 GHz processor
10.0 GB free hard drive space
MSDE 2000 (for Standard Ed), MS SQL Server 2000 or PostgreSQL 8.0

Single application-database server

768 MB RAM
1.5 GHz processor
10.0 GB free hard drive space
IIS/Apache Web Servers (optional)
MSDE 2000 (for Standard Ed), MS SQL Server 2000 or PostgreSQL 8.0

Supported Firewalls

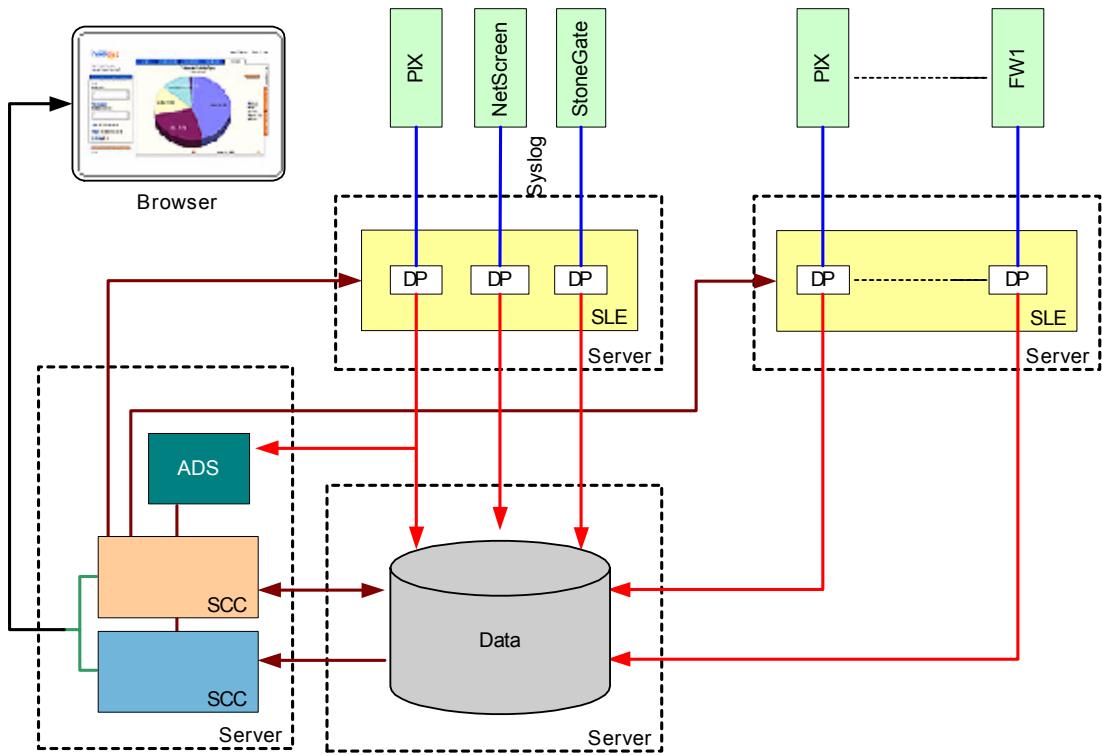
1. Cisco PIX 5.x, 6.x, 7.x
2. Check Point™ FireWall-1® 4.1, NG FP3, NGAI
3. NetScreen Firewall Appliance OS 3.x, OS 4.x, OS 5.x
4. StoneGate 2.x
5. SonicWall 6.4.2
6. Cisco IOS
7. Cisco FWSM

8. Symantec (Raptor) 7.0

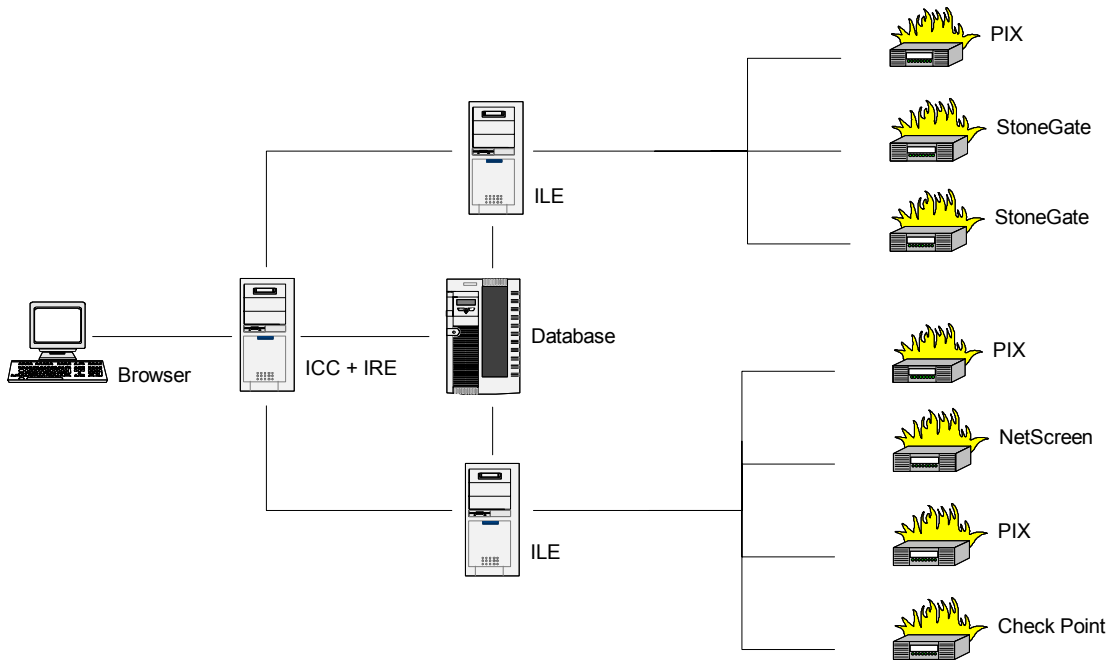
Supported Browsers

The following browsers are supported

1. MS Internet Explorer version 5.0 for Windows or later.
2. Netscape version 7.0 for Windows or later.
3. Fire Fox
4. Any browser supporting Sun Java Plugin ver 1.4.1_01



DistributedArchitecture



Distributed Architecture - Physical diagram

Trial version

SFR comes with a built in 30 day trial license that is activated the first time the application runs; there is no need to enter any license key. In trial mode, only log data that is less than 48 hours old is stored on a continuous basis and logging of new data stops after 30 days. A 30-day fully functional, unrestricted license for evaluation purposes is available to qualified users on request.

Quick Installation Steps

1. **Decide on the architecture** for deploying SFR – single machine or distributed. For a distributed architecture, decide what components go on each machine.
2. **Install SFR** On Windows, launch the SFR install program by running `sfr400winsetup.exe` where 400 indicates a version number 4.0.0. Choose what components you want to install – all components are required except the LEA Client, which is needed only for Check Point™. Finish the installation program. For Linux follow the instructions provided with the package.
3. **Restart Tomcat** Open the Windows Services Panel and stop the Tomcat service. Then start Tomcat from `C:\Program Files\SFR\jakarta-tomcat-5.5.0\bin\startup.bat`
4. **Open SCC** Launch URL `http://server-ip:8080/sfr/admin.html` to configure SFR (refer the chapter titled Configuration for details). This URL will launch the SCC (SFR Control Center)
5. **Database Settings** Specify Database type and the database server IP address; provide database user id and password. Click Apply.
6. **Reload SCC** Refresh browser to reload SCC. The default password to access the SCC is *stonylake*. The SCC will now show the default SLE and Data Processor
7. **Processor Settings** Expand the SCC tree to display the default SLE and Processor. Review Processor settings and change as necessary. Click Apply.
8. **Specify Log Origin ID** In Processor Settings, specify the IP address of the source of the firewall logs. This will be the IP address of the firewall in most cases.
9. **Assign License** In Processor Settings, click the License button and assign an available license.
10. **Start Processor** Right click Processor node and choose Start Processor. (Requires that SLE be started prior as a service or from `c:\program files\sfr\SLE\bin\sle.bat`)
11. **Configure firewall** to send logs to the SLE.
12. **View reports** at `http://server-ip:8080/sfr`
13. **Configure ADS** Launch URL `http://server-ip:8080/ads`. Enter the email address to send the ADS alerts and set up the Rules.
14. **Start ADS Service** Stonylake Firewall Reporter (ADS Service) for the monitoring to commence.

Remote Processor:

1. Install the RSLE (Remote SLE)

2. Edit and adjust remotesle.ini in the \SFR\rsle\conf\ folder
3. Configure a corresponding central Processor (refer Processor Settings above)
4. Start the remote logging engine RSLE by running rsle.bat

Installation on Windows

Installation for Windows is done using the SFR for Windows installation program. It is recommended that all defaults offered in the install program be accepted. The install program offers the option of selectively installing the following components.

SFR Server (SCC–SRE)
SFR Logging Engine (SLE)
Anomaly Detection System (ADS)
LEA Client (required only for Check Point™)

Note that the database server will have to be installed separately and in advance. MSDE 2000 is available in the MSDE folder of the installation package. The database itself will get installed automatically when SFR is activated.

SFR Server

The SFR Server consists of the SCC (SFR Control Center) and the SRE (SFR Reporting Engine). They run in the context of the Tomcat Servlet Engine. On Windows NT/Windows 2000, SFR Server can be run as a background service or in the foreground by running C:\Program Files\SFR\jakarta-tomcat-5.5.0\bin\startup.bat

SLE

The SLE (SFR Logging Engine) can be installed on an independent machine or co-located with another component. After the basic installation of an instance of the SLE, it can be run as a background service or from C:\Program Files\SFR\sle\bin\sle.bat

ADS

The ADS (Anomaly Detection System) module is typically installed on the SFR Server machine. After installation it can be run as a background service or from C:\Program Files\SFR\ads\bin\ads.bat

Database Server

Important - the SFR install program does not have a built in option to install any of the supported Database Servers. MSDE 2000 is the only database server provided in a separate folder with the package and has to be installed separately. Installation packages for MS SQL Server 2000 or PostgreSQL 7.x can be obtained from Microsoft and Postgresql.org respectively.

On Windows NT/Windows 2000/Windows XP, the MSDE database server can be started as a background service and must be set to start automatically. If you choose to use an instance of SQL Server that is already installed, MSDE should not be installed. For the SFR database to install successfully, availability of MSDE, MS SQL Server or PostgreSQL is a prerequisite.

SFR Database

SFR uses one single database named ifr. This database is automatically created by the SFR software when it first connects to a database server. Updates to an existing database are also similarly implemented by newer versions of SFR software.

LEA Client

The LEA client is a Windows program and is needed for SFR to work with the Check Point™ firewall. It installs as a service in the \lea folder on Windows NT 4.0/Windows 2000/Windows XP. It can be installed on the firewall machine, SFR server machine (Windows only) or a separate standalone machine.

4. INSTALLATION ON LINUX

SFR Server

On a Red Hat Linux 9.0 machine extract `sfr400lnxsetup.tar` to `/opt`. The `sfr` directory will contain all the components of SFR except the database.

PostgreSQL Database

PostgreSQL 8.0 should be installed to standards listed in the PostgreSQL documentation. PostgreSQL should be configured to allow connections over port TCP 5432 (this is the default).

1. Certain parameters have to be set in the `postgres.conf` file for required database performance. The parameters and their values are given below:

```
tcpip_socket = true
max_connections = 150
port = 5432
sort_mem = 5242 # keep this 2% of RAM, expressed in KB. The value shown
here is for 256 MB
shared_buffers = 16384 # formula: (RAM/2)*1024/8 where RAM is in MB. Each
buffer is 8KB, allocate half the RAM
fsync = false
enable_seqscan = false
enable_sort=false

wal_buffers = 64
wal_debug = 1
checkpoint_timeout = 120

log_timestamp = true
log_pid = true
```

2. Adjust the `SHMMAX` value for Linux. This value expressed in bytes should be about 1 MB greater than the `shared_buffers` value. For example, if `shared_buffers` = 16384, then `shmmax` should be set to 135266304. On Linux enter:

```
$ echo 135266304 >/proc/sys/kernel/shmmax
```

3. Edit the `pg_hba.conf` file located in the `PGDATA` directory and list the real IP addresses of the SCC and SLE machines for access to the database.

Database Installation

Ensure that a user account named postgres is set up with a blank password and the database cluster has been initialized using the initdb command. Refer to the PostgreSQL documentation for explanations of these requirements.

SFR uses one single database named ifr. This database is automatically created by the SFR software when it first connects to a database server. Updates to an existing database are also similarly implemented by newer versions of SFR software.

5. CONFIGURATION

Overview

SFR minimum configuration consists of the following steps.

1. Start the SFR Server.
2. Choose the edition to activate.
3. Set database type, location and other settings.
4. Add one or more SLEs in the SCC
5. Edit the SLE configuration file if necessary.
6. Configure one or more Data Processors for each SLE.
7. Configure one or more Remote SLE. Configure the remotesle.ini file.
8. Configure the firewall to send logs to the SFR server or the Remote SLE.

Refer to Section 7, SFR Control Center for screen shots and more details on each step.

Details

Start SFR Server

In a Windows environment, the SFR Server is started by starting the Stonylake Firewall Reporter(Apache Tomcat 5.5) service. In Linux, run `\opt\sfr\jakarta-tomcat-5.5.0\bin\startup.sh`.

Activate Edition

After starting the SFR Server, launch a browser and open `http://sfr_server_ip:8080/SFR/admin.html` where `sfr_server_ip` is the ip addresses of the machine where the SFR Server is installed. If you see a gray box, refresh the browser 2-3 times till you get the SCC screen. Choose the appropriate edition as desired. Note that this dialog is offered only once when the system is started for the first time. **To change to a different edition will require a complete reinstallation.**

The Standard Edition allows reporting on only one firewall at a time; the Enterprise Edition allows multiple firewalls of different types to be reported on. The Standard Edition supports MSDE 2000 database server; the Enterprise Edition additionally support MS SQL Server 2000 and PostgreSQL 7.x.

30 day trial licenses are activated on Edition Activation.

Database

After choosing the edition, the SCC loaded in the browser with the database settings page open. Choose the appropriate database and fill in the required settings of location (IP address or FQDN), database port and security settings for accessing the database. Before clicking the “Apply” button ensure that the database server is running and accessible.

After clicking the Apply button, the refresh the browser to fully reload the SCC navigation tree. The default password to login to the SCC is *stonylake*.

License Information

Each firewall requires a license for reporting. SFR Standard Edition comes with a built-in 30-day trial license that is activated the first time the application runs. SFR Enterprise Edition comes with 3 built-in 30-day licenses. In demo mode, log data that is more than 48 hours old is automatically deleted during maintenance. When you buy the software, a permanent license key is provided; this license key is required to be entered in the SCC.

Define SLE in the SCC

A default SLE (SFR Logging Engine) definition using IP address 127.0.0.1 is created when you initialize the application.

An SLE can be deleted if required by right clicking the SLE node and choosing Delete SLE. To add an SLE, right click the SLEs node and choose to add a New SLE. You can have several SLEs in the system but you can have only one SLE on any one machine. Each SLE can contain one or more Data Processors, one for each firewall.

The SLE Com Port is the TCP port that the SLE listens on for communications from the SCC. The default value of 7878 for each SLE need not be changed.

SLE Component Configuration

After defining the SLE in the SCC, the SLE component itself has to be configured. The configuration is stored in a file named SLE.ini with the SLE component. The file is located in the conf folder of the SLE installation. (c:\program files\sfr\sle\conf\sle.ini)

Edit the sle.ini file to specify the IP address of the SCC and the TCP port to use by the SLE for communication with the SCC. This will be the port that the SCC is listening on (check SCC Com Port in SCC System Settings) the default for which is TCP 7879; this need not be changed.

For the first time, start the SLE by running `..\sle\bin\sle.bat` on Windows or `../sle/bin/sle.sh` on Linux. Informational messages in the SLE window will indicate error conditions, possible causes and solutions or successful running. SLE errors are written to log files located at `...\sfr\shared\logs\sle.log.x`

Once the SLE has been configured and working satisfactorily, it can be run as a background service.

Data Processors

A default Processor is created in the context of the default SLE when you initialize the application.

Expand the Processor node and change as necessary.

Syslog port will typically be (UDP) 514. Origin IP address will typically be the firewall's IP address. Check Point™ and Stonegate require special considerations as outlined below.

In case of **Check Point™**, it is the LEA Client that will send the logs to an SLE. The LEA Client sends one Syslog stream for each FireWall-1® Module. The Origin IP in Processor Settings will be the IP address of the LEA Client. Syslog port will be unique for each data stream coming from the LEA client and will be the same as defined in lea.conf

In case of **StoneGate**, it is the Log Server that sends the logs to an SLE. From among all the Data Processors configured for StoneGate, one Data Processor in the SLE is picked by the system to capture the single stream sent by the Log Server. This processor then segregates the data into temp files in accordance with the configuration of each StoneGate Data Processor. Thus all Data Processors for StoneGate are given the same Syslog Port- the UDP port on which the Log Server sends the logs. Additionally, the firewall (node) IP address has to be defined in each Data Processor in the Origin IP field for Syslog segregation.

Define Network IDs as appropriate for identifying the subnets of internal sources.

Click the Assign License button and assign an available license to this processor.

Click Apply to save the settings.

Navigate the Processor branch of the tree to Misc. and optionally define any additional internal IP addresses. Enable Remote Processor if there will be a corresponding Remote Processor. Click Apply to save the settings.

Finally, after ensuring that all the settings for the Data Processor are effective after having clicked the Apply button, right click on the Data Processor node and choose Start Processor.

Remote Data Processors

SFR supports Remote Data Processors. This feature is useful where the firewall is in a remote location such as a branch office and it is not practical to transport the firewall logs to the central SFR server in real time. In this configuration, the RSLE (Remote SLE) is installed at the branch office and the branch office firewall's logs are directed to it. The RSLE is configured using the remotese.ini file to receive, partially process and send the partially processed logs in a compressed archive format to a corresponding Data Processor configured in the central SFR server for consolidation, storage and reporting. Every Remote Processor must have a corresponding Data Processor in the central SFR server.

Firewall Configurations

Each firewall requires to be configured to send its logs to the SFR server. All supported firewalls except Check Point™ send logs via Syslog. Check Point™ uses its LEA client-server system to send the logs.

Cisco PIX firewall

SFR can report on the Cisco PIX firewall using one of two methods – File Processing or Syslog.

Using file processing:

Refer to the PIX documentation to configure the PIX. On the PIX, set the logging level to Informational and include the time stamp on the logs.

Log files generated by the firewall are processed in SFR by copying them into a receiving folder named after the firewall in the SFR folder structure. For example, log files from a firewall named PixLondon will need to be copied to a folder named C:\Program Files\SFR\SLE\incoming\PixLondon\. A separate script or process will have to be used to copy the logs files into the SFR receiving folder.

The log files must be named in the following format: logfile.yyyymmdd[-n] For example,

```
logfile.20050614  
logfile.20050614-1  
logfile.20050614-2
```

To use SFR more effectively, the firewall log files should be switched more frequently.

Using Syslog:

In this method, the PIX is configured to directly send its log data over Syslog to SFR. The PIX can be configured using one of two methods. (Refer to the PIX documentation for detailed instructions.)

Using the PDM (PIX Device Manager) Interface:

Click on the System Properties tab. Navigate to the Logging/Logging Setup node in the Categories panel on the left hand side of the screen. Check Enable Logging in the Logging Setup screen on the right hand side. Navigate to the Logging/Syslog node in the Categories panel on the left hand side of the screen. In the Syslog screen on the right hand side set the following values:

```
Syslog: LOCAL4(20)  
Level: Informational  
Include Timestamp: Check  
Number of messages allowed to be queued: 500
```

Click the Add button to add a Syslog Server. In the 'Add Syslog Server' screen that is displayed, set the following values:

Interface: 'inside' if the SLE that contains the Data Processor for processing the logs has an internal IP address and 'outside' if it is an external address
IP address: IP address of the SLE that contains the Data Processor for processing the logs.
Protocol: UDP
Port: The UDP port that the dedicated Data Processor is listening on (any port number other than 514 will have to be greater than 1024)

Using the command line interface:

Add the following commands to the PIX configuration:

```
logging host [interface] [SLE IP Address] (e.g. logging host inside 192.168.1.10)
logging trap 6
logging on
```

Check Point™ FireWall-1® (4.1, NG and AI)

Each FW1 node sends its logs to the Check Point™ Management Station (LEA Server) that must be configured to connect and send those logs to the LEA Client that can be installed anywhere but generally installed with SFR. The LEA Client is provided with SFR and must be installed specifically for SFR to report Check Point™ logs.

The communication between the Management Station (Lea Server) and the Lea Client can be clear or encrypted and/or authenticated with configuration required at both, the Management Station and at the Lea Client.

There entire configuration can be viewed as consisting of two parts – configuring communication between the Lea Client and SFR, and configuring communication between LEA Server and Lea Client:

LEA Client – SFR Configuration

LEA Client must be configured to correctly filter the logs and send them on to the designated Data Processors:

In the lea.conf file found in the \SFR\lea folder on the machine hosting the LEA Client, define the ip address and connection port of the Check Point™ Management Station. Then for every FireWall-1® node, define its Host Name, IP address, the IP address of the SLE/Data Processor and the port that it is listening on. Detailed instructions are and examples are given in the file itself. For example:

```
# [SFR Logging Configuration]
# FIREWALL_NAME FIREWALL_IP_ADDRESS SFR_IP_ADDRESS PORT
SFR= CPNG 192.168.1.2 127.0.0.1 515
```

LEA Server – LEA Client configuration

If necessary, add a rule to the FireWall-1® Security Policy with the following values to allow communication between the LEA Client and FireWall-1® Management Station:

Source = your LEA Client host (create one first if necessary) or the Local Net.

Destination = the FireWall-1[®] host
Service = Fw1_lea (TCP port 18184)
Action = Accept

Decide what type of connection you wish to establish between the Lea Server and Lea Client and follow the appropriate section below:

Connections to VPN-1[®]/FireWall-1[®] version 4.1

- **Clear connection**

On the VPN-1[®]/FireWall-1[®] machine, in \$FWDIR/conf/fwopsec.conf set:

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

then execute:

```
fwstop  
fwstart
```

On the LEA Client machine, in lea.conf file set:

```
lea_server ip_address <vpn-1-fw-1_ip_address>  
lea_server port 18184
```

Start the LEA application, execute:

```
lea
```

- **Default connection(auth_opsec)**

On the VPN-1[®]/FireWall-1[®] machine, in \$FWDIR/conf/fwopsec.conf set:

```
lea_server auth_port 18184
```

then execute:

```
fwstop  
fw putkey -opsec <lea_application_ip_address>  
fwstart
```

On the LEA Application machine, in lea.conf file:

```
lea_server ip_address <vpn-1-fw-1_ip_address>  
lea_server auth_port 18184  
lea_server auth_type auth_opsec
```

then execute:

```
opsec_putkey <vpn-1-fw-1_ip_address>
```

This will create a file called "**authkeys.C**" which will be used for authentication. Make sure this file is accessible to the LEA application. The OPSEC™ infrastructure will look for this file in the directory that the environment variable "OPSECDIR" specifies. If OPSECDIR is not set or the file is not available in the directory, it will look for the file in the current working directory. If the "**authkeys.C**" file cannot be accessed, the authentication will fail and the communication between the OPSEC™ application and VPN-1®/FireWall-1® will not be initialized.

Start the LEA application, execute:

```
lea
```

- **ssl_opsec connection**

On the VPN-1®/FireWall-1® machine, in \$FWDIR/conf/fwopsec.conf set:

```
lea_server auth_type ssl_opsec
```

then execute:

```
fwstop  
fw putkey -opsec -ssl <lea_application_ip_address>  
fwstart
```

On the LEA Application machine, in lea.conf file:

```
lea_server ip_address <vpn-1-fw-1_ip_address>  
lea_server auth_port 18184  
lea_server auth_type ssl_opsec
```

then execute:

```
opsec_putkey -ssl <vpn-1-fw-1_ip_address>
```

This will create a file called "**sslkeys.C**". The same rules as "**authkeys.C**" given above apply to this file.

Start the LEA application, execute:

```
lea
```

Connections to VPN-1®/FireWall-1® NG

- **Clear connection**

On the VPN-1®/FireWall-1® machine, in \$FWDIR/conf/fwopsec.conf set:

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

then execute:

```
cpstop
cpstart
```

On the LEA Application machine, in lea.conf file:

```
lea_server ip_address <vpn-1-fw-1_ip_address>
lea_server port 18184
```

Start the LEA application, execute:

```
lea
```

- **Default connection(sslca)**

On the VPN-1[®]/FireWall-1[®] machine, FW-1 policy:

- create a new OPSEC[™] Application Object with the following details:
 - Name: leaclient
 - Vendor: User Defined
 - Server Entities: None
 - Client Entities: LEA
- initialize Secure Internal Communication (SIC) for recently created OPSEC[™] Application Object and enter (and remember) the activation key.
- write down the DN of the recently created OPSEC[™] Application Object. This is your Client Distinguished Name, which you need later on.
- open the object of your FW-1 management server and write down the DN of that object. This is the Server Distinguished Name, which you will need later on.
- add a rule to the policy to allow the port defined above as well as port 18210/tcp (FW1_ica_pull. The port 18210/tcp can be shut down after the communication between leaclient and the FW-1 management server has been established successfully.
- install the policy

in \$FWDIR/conf/fwopsec.conf either all LEA Server values must be commented out or set as follows:

```
lea_server auth_type sslca
lea_server auth_port 18184
```

then execute:

```
cpstop
cpstart
```

On the LEA Application machine, in lea.conf file:

```
lea_server ip_address <vpn-1-fw-1_ip_address>
lea_server auth_port 18184
```

```
lea_server auth_type sslca
lea_server opsec_entity_sic_name "cn=cp_mgmt,o=test..7ck5tf"
opsec_sic_name "CN=leaclient,o=test..7ck5tf"
opsec_sslca_file opsec.p12
```

then execute:

```
opsec_pull_cert -h <vpn-1-fw-1_ip_address> -p <activation key> -n
leaclient
```

Start the LEA application, execute:

```
lea
```

- **ssl_opsec connection**

On the VPN-1®/FireWall-1® machine, in \$FWDIR/conf/fwopsec.conf set:

```
lea_server auth_type ssl_opsec
```

then execute:

```
cpstop
fw putkey -opsec -ssl <lea_application_ip_address>
cpstart
```

Configuration of FW-1 policy:

- create a new OPSEC™ Application Object with the following details:
 - Name: leaclient
 - Vendor: User Defined
 - Server Entities: None
 - Client Entities: LEA
- initialize Secure Internal Communication (SIC) for recently created OPSEC™ Application Object and enter (and remember) the activation key.
- write down the DN of the recently created OPSEC™ Application Object. This is your Client Distinguished Name, which you need later on.
- open the object of your FW-1 management server and write down the DN of that object. This is the Server Distinguished Name, which you will need later on.
- add a rule to the policy to allow the port defined above as well as port 18210/tcp (FW1_ica_pull. The port 18210/tcp can be shut down after the communication between leaclient and the FW-1 management server has been established successfully.
- install the policy

On the LEA Application machine, in lea.conf file:

```
lea_server ip_address <vpn-1-fw-1_ip_address>
lea_server auth_port 18184
lea_server auth_type ssl_opsec
lea_server opsec_entity_sic_name "cn=cp_mgmt,o=test..7ck5tf"
opsec_sic_name "CN=leaclient,O=test..7ck5tf"
```

then execute:

```
opsec_putkey -ssl <vpn-1-fw-1_ip_address>
```

Start the LEA application, execute:

```
lea
```

How to re-issue a SIC certificate

opsec_pull_cert is used to get SIC certificate which is needed for authentication communication with the LEA server in Check Point™ NG, such as sslca, ssl_opsec, etc., but it works once per certificate.

After you successfully pull a certificate, you are unable to re-issue a SIC certificate for the same OPSEC™ Application object. If you want to re-issue, you have to edit the OPSEC™ application object.

Go to Manage->OPSEC™ Applications.
Select OPSEC™ application object, which is leaclient here, and Click Edit.
Click Communication, and you should observe that current state of the trust is "Trust established".
Click Reset. Now, the state of trust changes into the "Un-initialized" trust state.

You have to re-install the security policy in order to update the CRL list. You must install the security policy to all modules. You are prompted to enter an activation key that you specify must also be used in the module configuration, which is used to pull the SIC certificate in the module that is running LEA client.

After you input your activation key twice, and click Initialize. Now the state of trust becomes "Initialized but trust not established".

On the box, which runs lea, you run an opsec_pull_cert as follows:

```
opsec_pull_cert -h host -n object-name -p activation-key
```

where host is the host name or ip of the Check Point™ management server ;
object-name is the name of the OPSEC™ application set in the OPSEC™ Application Properties dialog, using leaclient here;
activation-key is the one-time-password, which is entered in the Communication dialog during the setup of the OPSEC™ Application;
cert_file is the name of certificate file, which is used to store the SIC certificate. The default is opsec.p12;

dn_file is the name of a file, which stores sic name, i.e. DN (Certificate DN, i.e., full distinguished name).

For example:

```
opsec_pull_cert -h 192.168.0.63 -n leaclient -p abc123
```

The full entity sic name is:

CN=leaclient,O=cp.stonylakesolutions.com 4ytqbw

Certificate was created successfully and written to "opsec.p12".

This command puts the SIC certificate in the directory set in the %OPSECDIR% environment variable. Otherwise, it is saved in the same folder where you run opsec_pull_cert. The certificate is saved in a file called opsec.p12. where CN=leaclient,O= cp.stonylakesolutions.com 4ytqbw is the SIC name of the OPSEC™ application, which stands for your box that runs lea.

Afterwards, the state of the trust changes to Trust established from Initialized but trust not established.

Extended URL information

By default the Check Point™ firewall does not capture extended URL information. To capture extended urls, in the FireWall-1® Policy manager first setup a Resource named URL if you don't already have one. Then add a rule for http and ftp services using "Add with Resource" when setting the Service parameters and choose the resource named URL. If you already have a rule for the services, all you have to do is change it use the URL Resource. For more information refer to your Check Point™ documentation.

Reporting account (bytes) information:

Ensure that for every rule in the FireWall-1® Security Policy that you want account information (bytes) about has its 'Track' value set to Accounting. This will capture the number of bytes, source, destination and other accounting information. This is normally done for rules pertaining to allowed services.

Rules that block access will not allow the 'Track' value to be set to accounting; for such rules the 'Track' value should be set to 'Long'.

NetScreen Firewall Appliance (OS 3.x)

In the firewall Administration screen, click on "Admin", and then "Syslog" tab in the top row. Then set the following values in the syslog settings screen:

1. Enable Syslog Messages - Yes (checked).
2. Enable Syslog VPN Encryption - No (unchecked).
3. Include Traffic Log - Yes (checked).

4. Syslog Host Name - Enter the IP address of the computer running the SLE and Processor that will process the firewall logs.
5. Syslog Host Port - The UDP port number that the dedicated Processor is listening on.
6. Enable WebTrends Messages - No (unchecked)
7. All other fields should be left at their default values.
8. Click on "Log" in the menu on the left hand side and then click on the "Settings" tab in the top row.
9. For the Syslog, check all Log Severity Levels from Emergency through Information. Keep Debugging Level unchecked.
10. Apply the Settings.

NetScreen Firewall Appliance (OS 5.x, 4.x.)

In the firewall Administration screen, navigate to Configuration | Report Settings | Syslog. Then set the following values in the Syslog settings screen:

1. Enable Syslog Messages - Yes (checked).
2. Include Traffic Log - Yes (checked).
3. Syslog Host Name - Enter the IP address of the computer running the SLE and Processor that will process the firewall logs.
4. Syslog Host Port – The UDP port number that the dedicated Processor is listening on.
5. All other fields should be left at their default values.
6. Apply the Settings.

Next, navigate to Home | Configuration | Report Settings | Log Settings. For Syslog, check Severity Levels from Emergency through Informational. Keep Debugging unchecked. Apply the settings.

StoneGate 2.x

StoneGate log server must be configured to send log data to SFR. This is done as follows (Refer to the StoneGate documentation for detailed and optional steps):

1. Stop the log server.
2. Modify the LogServerConfiguration.txt with the following values –
SYSLOG_SERVER_ADDRESS=IP address of the SLE containing the Processors that will process the logs (for all firewalls)
SYSLOG_PORT=UDP port that the dedicated Processor is listening on.
SYSLOG_MESSAGE_PRIORITY=6

3. For every rule in the Policy, from the rule's logging options –
 - enable logging
 - set Log Level to 'Stored'
 - set Connection Closing to Log Accounting Information
 Note that logging every rule may have an adverse effect on the log server.
4. Restart the log server

SonicWall

In the firewall Administration screen navigate to the Log | Log Settings screen.

Scroll down to the Syslog Servers section and add the IP address and port (default of 514) of the SLE that contains the Processor set up to process the SonicWall logs.

Scroll down further to the Categories section. In the Log sub-section enable the following parameters at the minimum:

Blocked Web Sites	Dropped TCP
Blocked Java	Dropped UDP
User Activity	Dropped ICMP
Attacks	

Cisco IOS Router

Configuration of the Cisco IOS Router for reporting consists of the following tasks to be completed:

1. Enable timestamps for logging using date-time and local time:


```
service timestamps log datetime localtime
```
2. Verify/set correct time on the device


```
sh clock
clock timezone
clock summer-time
clock set
```
3. Enable audit logs to be sent using syslog


```
ip audit notify log
```
4. Enable CBAC audit trail messages


```
ip inspect audit-trail
```
5. Set logging level


```
logging trap informational
```
6. Enable syslog to be sent to the SLE that contains the Processor set up to process the logs

```
logging 192.168.1.22 (replace 192.168.1.22 with your SLE
address)
```

7. Set interface for source address in log messages, for example,
`logging source-interface Ethernet0`
8. Enable logging of each access rule for example,
`access-list 110 permit ip 192.168.1.0 0.0.0.255 any log`

Symantec (Raptor) firewall:

Symantec does not provide event logs in real time via syslog or other protocol. Log files generated by the firewall are processed by copying them to a specific folder in the SFR folder structure. For example, log files from a firewall named SRLondon will need to be copied to a folder named C:\Program Files\SFR\SLE\incoming\SRLondon\

The screenshot shows the 'Processor Settings' window. It contains the following fields and controls:

- Name:** Symantec-London (text input), Processor ID: 3 (text label)
- Description:** (empty text input)
- License:** None (text input), Assign License... (button)
- Firewall Type:** Symantec 7.0 (dropdown menu)
- Firewall Name:** SRLondon (text input), Receiving folder for log files: ifr/file/incoming/SRLondon/ (text label)
- Network ID:** (text input with dots), Subnet Mask: (text input with dots), Add (button), Remove (button)

A separate script or process will have to be used to copy the logs files into the SFR receiving folder.

To use SFR more effectively, the firewall log files should be switched more frequently.

Finish Configuration

The basic configuration is complete once you have finished the steps outlined in the previous section. At this point the SFR Server and SLE should be running. Informational messages on the SCC (Tomcat window) and SLE consoles indicate whether everything is working correctly. If the firewall is sending logs, the SLE should be receiving and processing them.

For example, on the SCC console you will see:

```
*****
SFR Firewall Reporter
Stonylake Solutions
*****

*****
SFR Control Center
Edition: Standard
Host ID: KU7357
Version: 4.0.0
Lic Type: Eval.
Expires: 2004 12 02
Started: 2:00 PM Nov 05, 2004
*****

*****
* NOTE: If you close this command prompt window, *
* the SFR Server will shut down. *
*****

*****
* WARNING:Firewall log data older than 48 hrs will *
* be deleted for Processors running Demo Licenses *
*****

[08:43:07] Starting SFR Control Center ver 4.0.0 ...

[08:43:09] SFR is ready ...
```

For an SLE running a Processor for Cisco PIX you will see:

```
*****
SFR Firewall Reporter
Stonylake Solutions
*****

*****
SFR Logging Engine
Version: 4.0.0
Started: 2:00 PM Nov 05, 2004
*****

*****
* NOTE: If you close this command prompt window, *
* the SFR Logging Engine will shut down. *
*
* On Windows, SLE can be installed as a service *
* and run in the background *
*****
```

```
*****
*****
* WARNING:Firewall log data older than 48 hrs will *
* be deleted for Processors running Demo Licenses *
*****

[11/05/2004 14:00:39 EST] Starting SFR Logging Engine ver 4.0...

[11/05/2004 14:00:40 EST] Connecting to SCC at 127.0.0.1 on TCP port
7879 ...

[11/05/2004 14:00:43 EST] Downloaded configuration

[11/05/2004 14:00:46 EST] Loading Processor ID 1 named PIX for Pix 6.x
on port 514, license expiring never

[11/05/2004 14:00:46 EST] PIX: waiting for logs on port 514
```

To view SFR reports point your browser to http://sfr_server_IP_address:8080/sfr

If the SFR Server (Tomcat) has been started in the foreground you might want to stop it and restart it as a service. Refer to the Tomcat documentation for running Tomcat as a service.

The SLE can also be run as a background service once everything has been configured satisfactorily.

IIS and Apache Web Servers

Optionally you may want to use IIS or Apache to serve browser requests for SFR. Instructions on configuring Apache or IIS to work with Tomcat are given in the Config Reference | Connectors | AGP section of the Tomcat documentation.

Other Settings

There are several other parameters in the in Admin Settings that you should review and set to suit your preference.

6. USING SFR

Starting and Stopping SFR

Starting SFR means (a) starting the SFR Server that consists of the SCC and SRE and, (b) starting the SLEs. The database server must be running and accessible for SFR to start.

SFR Server can be started in one of two ways - on Windows, running C:\Program Files\SFR\jakarta-tomcat-5.5.0\bin\startup.bat or starting the Stonylake Firewall Reporter(Apache Tomcat 5.5) service. The service may be set to start automatically.

When the server is started from startup.bat, the server process runs in a normal dos console window. Caution: this console window should not be closed as closing it will shut down the SFR Server immediately.

SFR Server can be stopped by running C:\Program Files\SFR\jakarta-tomcat-5.5.0\bin\shutdown.bat if started via startup.bat or by stopping the service if started as a service.

SLE can be started in one of two ways - C:\Program Files\SFR\sle\bin\sle.bat or in Windows NT/2000/Linux starting the SLE service. The service may be set to start automatically.

When the server is started from startup.bat the server process runs in a console window. Caution: this console window should not be closed as closing it will shut down the SLE immediately.

The SLE can be stopped by closing the console window or in Windows NT/2000/Linux stopping the service.

Linux Options for sle.sh and ads.sh

1. run in console:
./sle.sh console
./ads.sh console
2. start the sle and ads in the backgroud:
./sle.sh start
./ads.sh start
3. stop the sle and ads:
./sle.sh stop
./ads.sh stop

4. restart the sle and ads:
./sle.sh restart
./ads.sh restart
5. show the status of the sle and ads
./sle.sh status
./ads.sh status
6. kill the sle and ads:
./sle.sh dump
./ads.sh dump

Viewing Reports

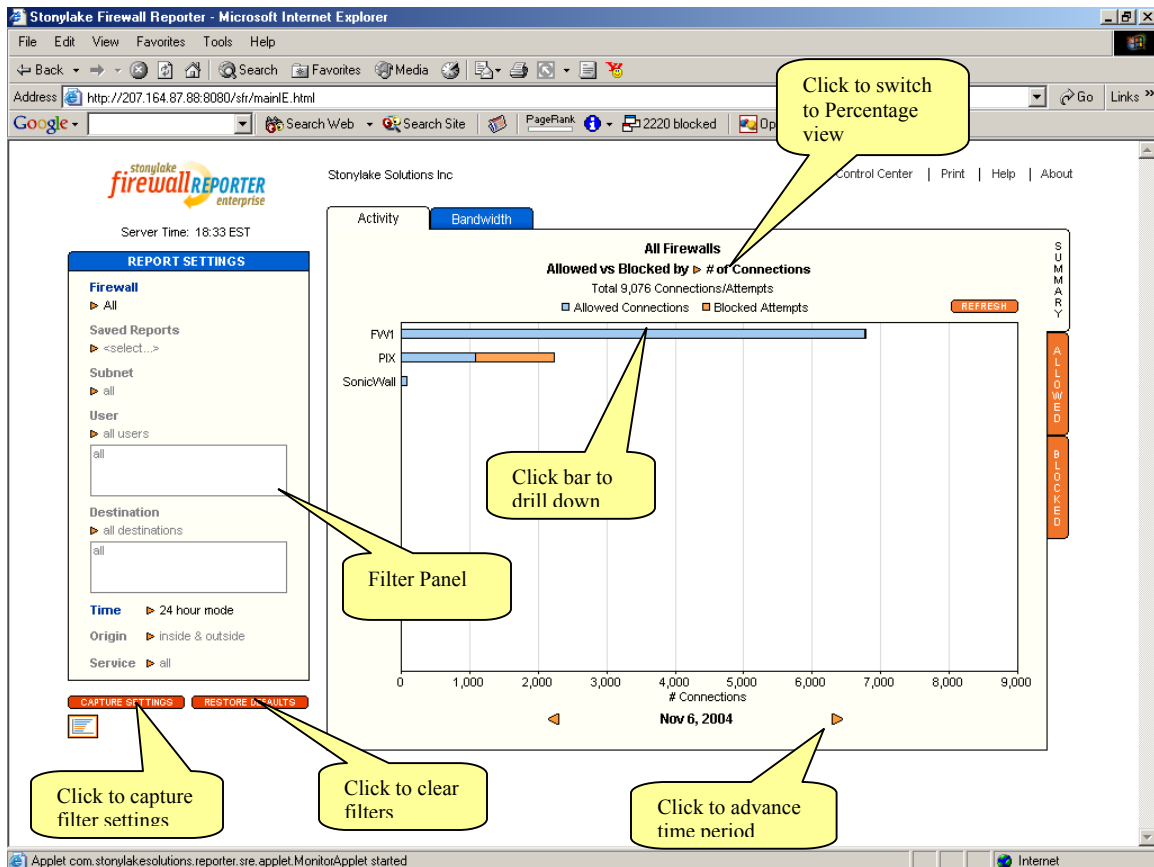
To view reports you need a Java enabled web browser that can connect to the SFR server. A java applet (called the SFR applet) displays the reports. Open a browser and enter the URL set up by your administrator (default URL is <http://servername:8080/SFR>) in the address field of the browser. You will be required to login using your login ID and password. The built-in userid is 'admin' and password is 'stonylake' without the quotes.

The SFR applet is made up of a tabbed report area and a Report Settings panel that is used to set report selection criteria.

Summary Screen

The Summary screen is the first to be displayed on loading the SFR applet showing summary reports for Activities and Bandwidth for all firewalls in the Enterprise Edition. In the Standard Edition, the reports are for only the one firewall that is currently active.

The Activities Report can be switched between absolute number of connections and a percentage view.



Server time

This is the time on the server machine on which the SFR Server application is running.

Admin Settings

To modify administration settings, click "Admin Settings" on the top right hand corner of the application window. This opens a password dialog box. See Modifying Admin Settings for more detailed instructions.

Printing a Report

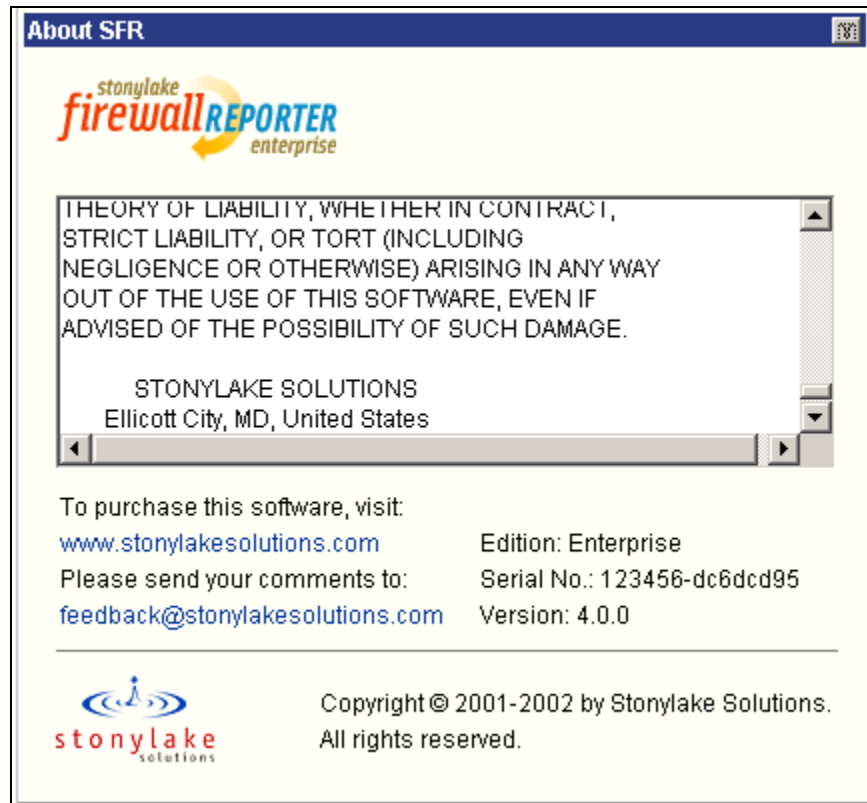
To print out a report, click "Print" on the top right hand corner of the application window. This opens a printable version of the report in another web browser window. Press Ctrl+P to print. (Note: this feature requires a color depth of 24 bits or less. Refer to your operating system manual for instructions to change the color depth.) You can also save the printable report image using your browser's controls and use it in an email message.

Help

To view the help file, click "Help" on the top right hand corner of the application window. This opens a new web browser window containing a printable version of the help contents.

'About' Box

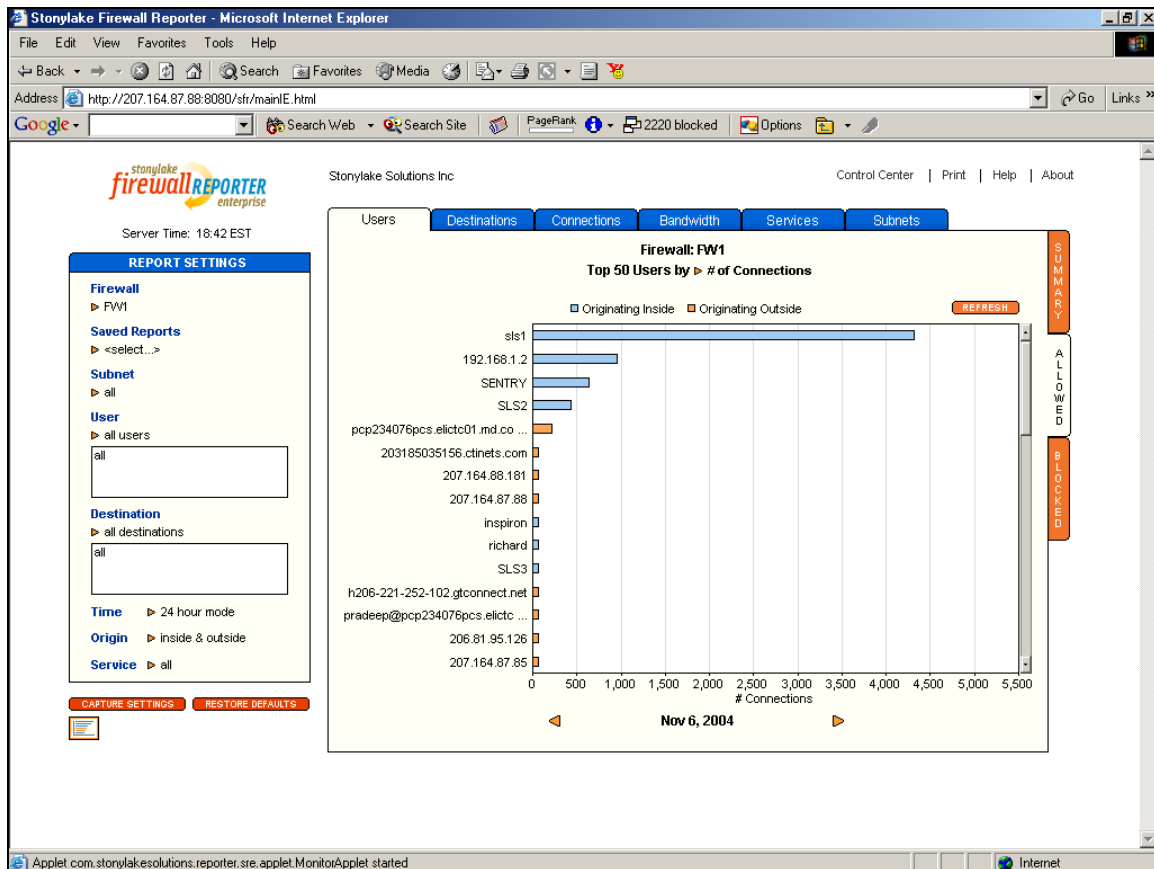
Click the SFR logo to find out about your version of SFR and serial number of the installation. You will need this information when you call in for technical support.



Reports for a single or group of firewalls

Detailed reports for a single firewall can be viewed by selecting the firewall in the Report Settings panel or by clicking the specific bar in the Summary Report screen.

Reports for a group of firewalls can be viewed by choosing the group in the Report Settings panel. The group must be predefined by the administrator in the SFR Control Center.



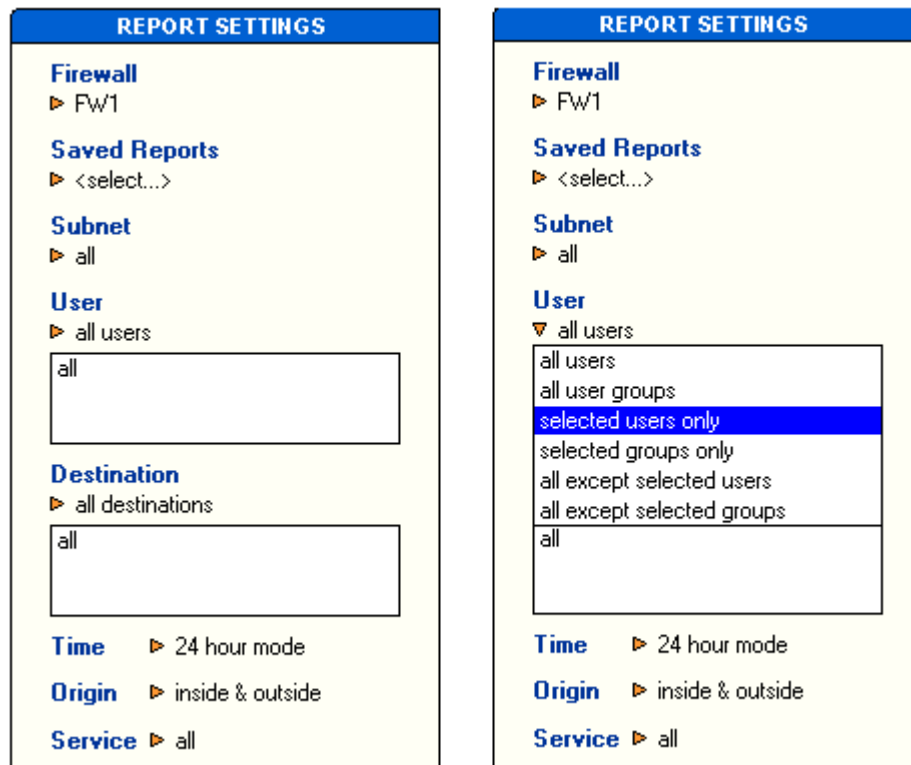
The firewall report screen provides eleven kinds of reports – six in the ‘Allowed’ category and five in the ‘Blocked’ category.

Report Settings

Report Settings or Filters define the selection criteria for each report. There are six different types of report settings or filters that can be set: Firewall, User, Destination, Time, Origin, and Service. Every report that is generated is specific to the Report Settings or filters that are current.

To view pre-configured reports, click on Saved Reports in the Report Settings panel. Then select a report from the drop down list. Pre-configured reports are set up from the SCC.

- **Saved Reports:** Each Saved Report is a set of pre-configured report filter settings that, when used, generate a report. Saved Reports are set up from the SCC and are available for use from the Report Settings panel.
- **Subnet:** The subnet for each internal source can be identified if the network information is provided and subnet resolution is turned on in the SCC. Reports can be viewed by subnets that can further be drilled down to the user level.
- **User:** A user is the machine located behind a firewall (inside) or outside that initiates a connection through the firewall. A group is a group of users that share a certain set of characteristics (e.g. the group "Sales" could contain all sales people in the company). You can view reports on "all users" (default), "all user groups", "selected users only", "selected groups only", "all except selected users", or "all except selected groups". To change the User setting click on the current User setting and choose from the drop down list. From the dialog box that may follow select a list of users from the list of available users and/or available groups.



You can create and/or modify global groups of users (sources), or destinations, from the SCC.

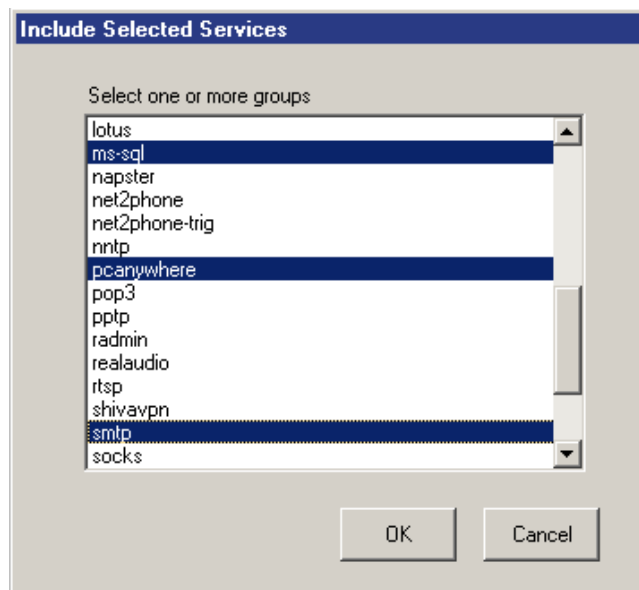
- **Destination:** A destination is the location a user connects to or tries to connect to. A destination group is one that shares a certain set of characteristics (e.g. the group "Music" could contain music sharing sites such as "Jobs"). You can view reports on "all destinations" (default), "selected destinations only", "selected groups only", "all except selected destinations", or "all except selected groups".

To change the Destination setting, click on the current Destination setting and choose from the drop down list. From the dialog box that may follow type in a list of destinations or choose from the list of available groups.

- **Time:** You can specify the time interval for which the report is to be generated. By default, the time interval for a report is set to the "24 hour mode" ("today"). The other time intervals are "current 5 minutes", "this hour", "this week", "this month", "this year", or specify another time interval by selecting "other".

Once a report for a given time interval is generated, a report for the previous or the next time interval can be generated by clicking on the back/forward arrows located below the chart.

- **Origin:** The origin is where an action is initiated, from inside the firewall or outside the firewall. You can view reports on connections from "inside", "outside", or both "inside & outside" (default).
- **Service:** You can view reports on different Services (default is "all"), such as "ftp" (file transfer), "http" (Web) and "smtp" (email). SFR comes pre-configured with a list of well-known Services. You can add your own Services and edit existing ones from the SCC. Refer to the "Admin Settings" section of the help file for more details. In addition, the Services drop down list contains two special selections. First, the "other ports" selection allows you to view activity based on all ports that are not pre-defined. Second, the "multiple..." selection allows you to select more than one pre-defined port to filter by. For example, you can select SMTP and POP3 to view all email related activity. Shown below is the multiple services selection screen.



You can revert to the default Report Settings by choosing Restore Defaults from the Saved Reports setting.

Generating a Report

A default set of twelve tabbed reports is generated every time you launch SFR. The default set of reports is based on a default set of filters.

To generate a new set of reports simply define new Report Settings. Whenever any of the Report Settings/filters are changed, SFR immediately begins generating a new report. If you follow up a filter change with another change before the report is generated, the previous report generation is cancelled and a report generation based on the new Report Settings is immediately started.

Understanding Reports

SFR provides a set of thirteen reports. These are organized into three main categories – Summary, Allowed and Blocked.

Summary

This category contains summary reports on Activity (Allowed Vs Blocked Connections) and Bandwidth (originating inside Vs outside) by firewall.

Allowed

This category contains reports on successful connections made through the firewall.

Blocked

This category contains reports on attempts denied by the firewall.

Clicking on an appropriate orange colored category tab on the right hand side and then clicking a blue report tab at the top can bring any one of the ten reports up.

Services Report

In the Services Report, you may see a slice of the pie chart labeled as Misc. This represents all activities that are each less than 2% of the total pie. As an extreme example, if there is extensive ports scan for a selected 5-minute interval, it is possible that you could see Misc. as an 80% slice. Clicking on the Misc. slice drills down to a report showing all the ports that formed the Misc. group (not available in the Standard Edition)

Interacting with Reports

Click to Select

In the Allowed-Users and Blocked-Sources report, when a bar is clicked the "User" filter will change to filter by the corresponding user/source.

In the Services report, when a section of the chart is clicked the "Activity" filter will automatically change to filter by the corresponding port. This is useful when you want to filter by ports that are not defined in your activity list.

Click to Launch URL

In the Allowed-Destinations and Blocked-Destinations report, when a bar is clicked the "Destination" filter will automatically change to filter by the corresponding destination. When the bar label is clicked, a separate browser window is launched with the associated URL.

Click to Drill Down

In the Allowed-Connections, Allowed-Bandwidth, and Blocked-Attempts reports, clicking a bar will generate a new report for that time interval and the next finer time scale level. For example, if the report is showing bars for every day of the month, clicking a bar will generate a detailed report for that day and time interval by the hour.

In the Services Report, clicking on the Misc slice drills down to a report showing all the ports that formed the Misc. group (Not available in Standard Edition)

Capture Report Settings (Snapshots)

Before you generate a second set of reports based on another set of filters, you can capture the settings of the current report so you can return to it without having to re-enter all the settings.

To capture the current report settings, click "Capture Report Settings". Your filter settings will be saved and an icon will appear. If you hover your mouse over the icon, a tool tip will display the associated filter settings. Click the icon to regenerate that report.

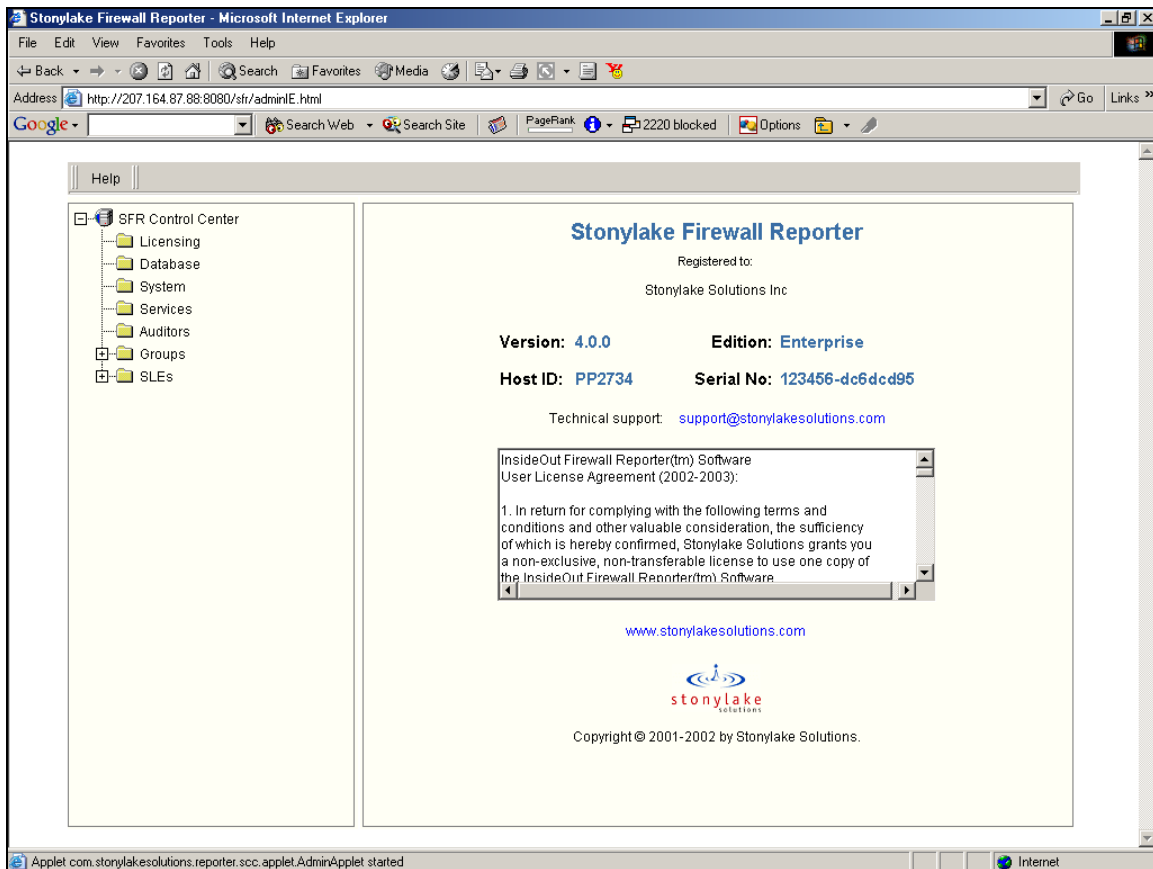
Note: Snapshots use browser cookies to save information; this allows you to restore a snapshot in a new browser session even after a current browser is closed. However, due to cookie size limitations, reports that use large filters (for example, a large list of selected users) may exceed the size limit. In that case, the report settings captured will be available only for that session. You have the option of replacing an existing snapshot with the new one or to use pre-configured reports. Please consult the section Admin Settings | Other Tab | Reports in this help file for more information on pre-configured reports.

Refreshing a Report

You can refresh a report to reflect the most current data and user activities. Click the "Refresh" button. SFR will regenerate the report.

7. SFR CONTROL CENTER

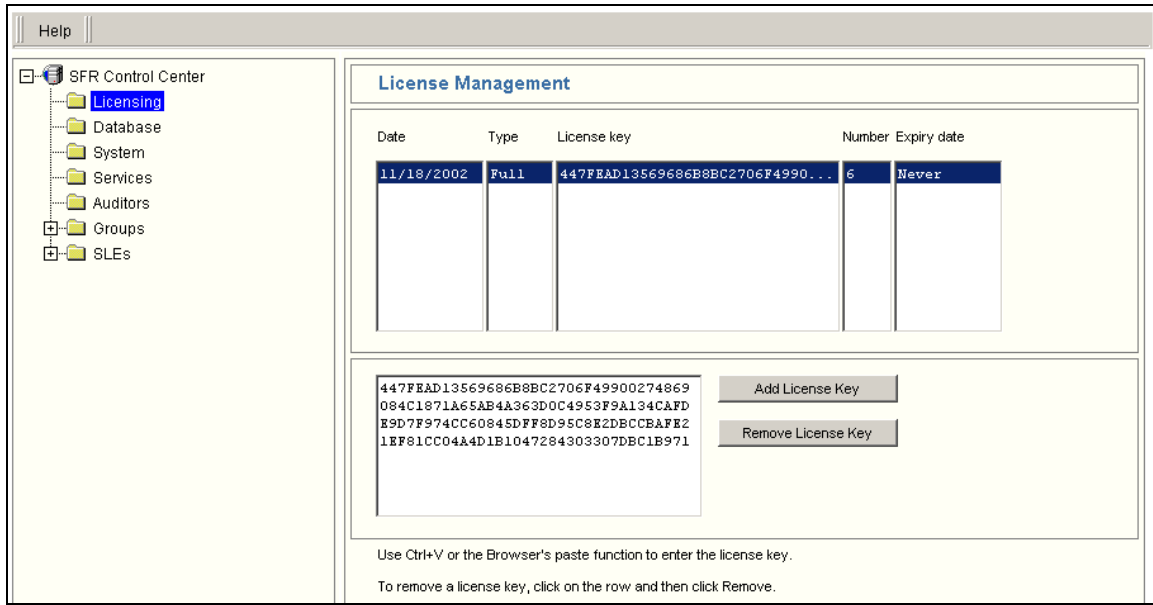
The SCC screen can be accessed from the main SFR browser window by clicking the Admin Settings hyperlink located at the top right hand corner. It can also be accessed at <http://servername/SFR/admin.html> The Admin Settings screen access is controlled by a password; the **default password** is stonylake. In case you lose the password, call technical support for a new password that will override and clear the earlier password.



The main page of the SCC shows the **Host ID, Version, Edition and Serial Number** of the installation. The Host ID is a unique identifier of the machine on which the SCC is installed. Licenses are tied to the Host ID.

Licensing

Licenses can be added or removed from the License Management screen. To add a license, **paste** the license key into the single large text box and click Add License Key. To remove an existing license, click on the license and click on Remove License Key.



Date	Type	License key	Number	Expiry date
11/18/2002	Full	447FEAD13569686B8BC2706F4990...	6	Never

447FEAD13569686B8BC2706F49900274869
084C1871A65AB4A363D0C4953F9A134CAFD
E9D7F974CC60845DFF8D95C8E2DBCCBAFE2
1EF81CC04A4D1B1047284303307DBC1B971

Add License Key

Remove License Key

Use Ctrl+V or the Browser's paste function to enter the license key.

To remove a license key, click on the row and then click Remove.

Only additional Licenses of the same Edition and with the identical Organization name and Host ID can be added.

Standard Edition can have only one license key with only one Data Processor license at any time. Enterprise Edition can have more than one license keys, each containing one or more Data Processor licenses.

To be able to add a permanent license to the Standard Edition, any existing demo license keys must be removed prior to adding the permanent license key.

Database

The screenshot shows the 'SFR Control Center' interface with a 'Database Settings' panel. The left sidebar contains a tree view with folders for Licensing, Database (highlighted), System, Services, Auditors, Groups, and SLEs. The main panel has a title bar 'Help' and a 'Database Settings' section. The settings are as follows:

Field	Value
Database Type:	MS SQLServer
Database IP / FQDN:	127.0.0.1
Database Port:	1433
Database Login ID:	sa
Database Password:	[Hidden]
Database Connection Pool:	
Initial Connections:	5
Incremental Connections:	5
Max Connections:	50

An 'Apply' button is located at the bottom of the settings panel.

Database Type: Choose from MSDE, MS SQL Server or PostgreSQL. In the Standard Edition only MSDE is supported.

Database IP/FQDN: The IP address or FQDN of the database server.

Database Port: The TCP port number to use to connect to the database server. Default for MSDE and MS SQL Server is 1433; default for PostgreSQL is 5432

Database Login ID: The login ID with administrative privileges to the ifr database.

Services

SFR comes with several predefined standard services. Add, Remove, Edit Services from this screen.

The screenshot shows the SFR Services Management interface. On the left is a navigation tree with the following items: SFR Control Center, Licensing, Database, System, Services (highlighted in blue), Auditors, Groups, and SLEs. The main area is titled "Services Management" and contains the following controls:

- New Services:** A text input field followed by an "Add" button.
- Existing Services:** A list box containing "auth", "bootpc", "bootps", and "citrix", with a "Remove" button to its right.
- Services reported by CheckPoint:** A text input field.
- Port No:** A radio button and a text input field.
- Port Range:** A radio button, a ">Add" button, and a "Remove" button.
- From:** A text input field.
- To:** A text input field.
- Protocol:** A dropdown menu currently set to "TCP".
- Ports:** A large empty rectangular box.
- Protocols:** A large empty rectangular box.

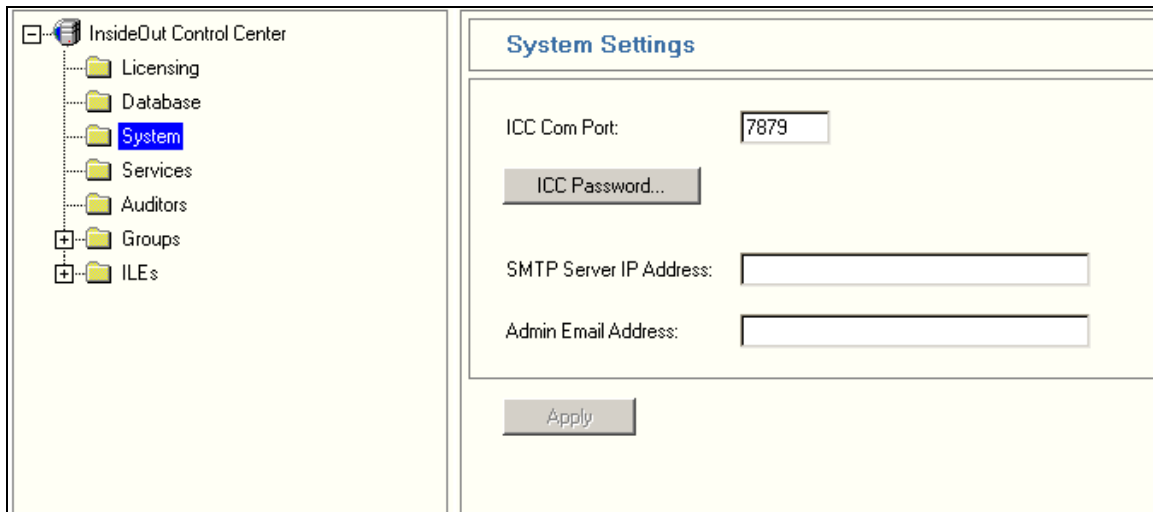
An "Apply" button is located at the bottom of the main content area.

System

Define system wide settings in this screen.

SCC Com Port: is the TCP port that the SCC listens for communications from the SLE and IRE. Default value is 7879.

SMTP Server: is the mail server to use to send system error notifications to the Admin Email Address to be provided. Ensure that the mail server will permit the SCC to send SMTP messages.



The screenshot shows the 'System Settings' configuration window. On the left is a tree view of the 'InsideOut Control Center' with folders for Licensing, Database, System (selected), Services, Auditors, Groups, and ILEs. The main area contains the following settings:

- ICC Com Port:
- ICC Password...:
- SMTP Server IP Address:
- Admin Email Address:

An 'Apply' button is located at the bottom of the settings area.

Auditors

Define here, end users (auditors) and their access rights to view reports for specific firewalls.

The built-in user named *admin* cannot be deleted. The **default password** for *admin* is SFR. It is suggested that this password be changed at the first opportunity.

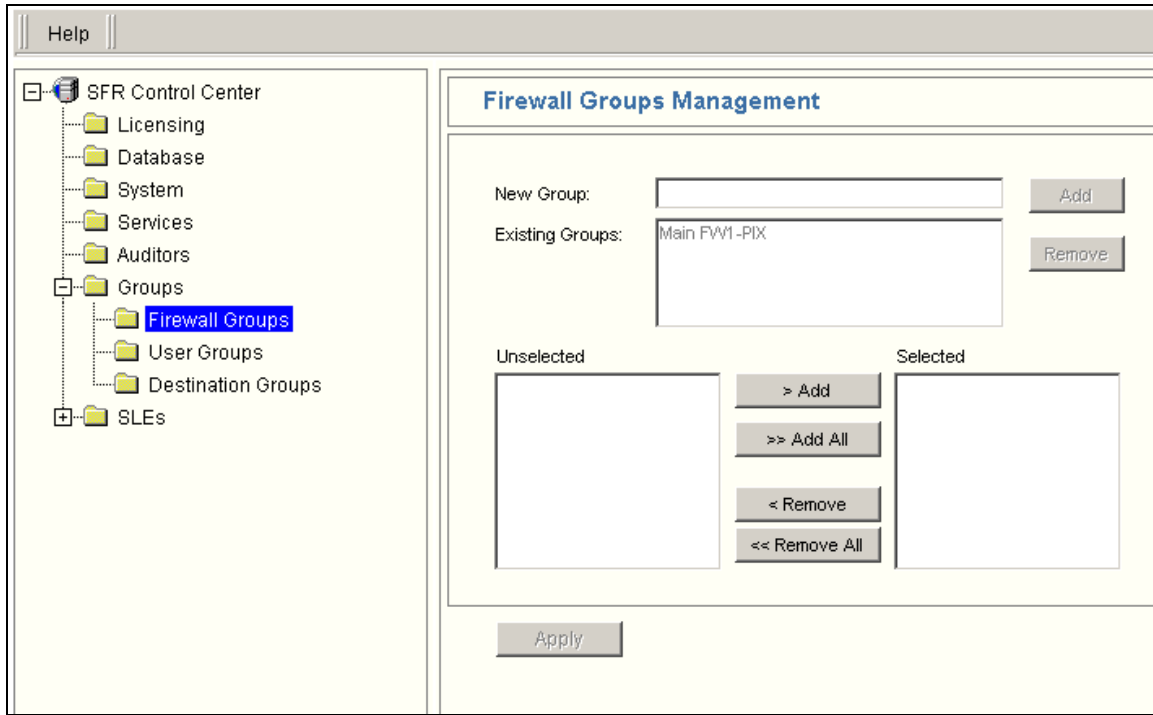
The screenshot shows the 'Auditors Management' interface within the SFR Control Center. On the left is a navigation tree with 'Auditors' selected. The main area is divided into three sections:

- New Auditor:** Includes input fields for name and password, and buttons for 'Add', 'Remove', and 'Change Password'.
- Existing Auditors:** A list box containing 'admin' and 'bob'.
- Firewall Management:** Contains instructions to click on an existing auditor to manage firewalls. It features two sets of list boxes: 'Available Firewalls' and 'Available Firewall Groups' on the left, and 'Allowed Firewalls' and 'Allowed Firewall Groups' on the right. Arrows indicate the direction of adding and removing items.

At the bottom, there is a section for 'Firewalls & Groups' with a list box containing 'PIX', 'FW1', 'CPNG', 'NetScreen', and 'StoneGate', and an 'Allowed Auditors' list box. An 'Apply' button is located at the bottom center.

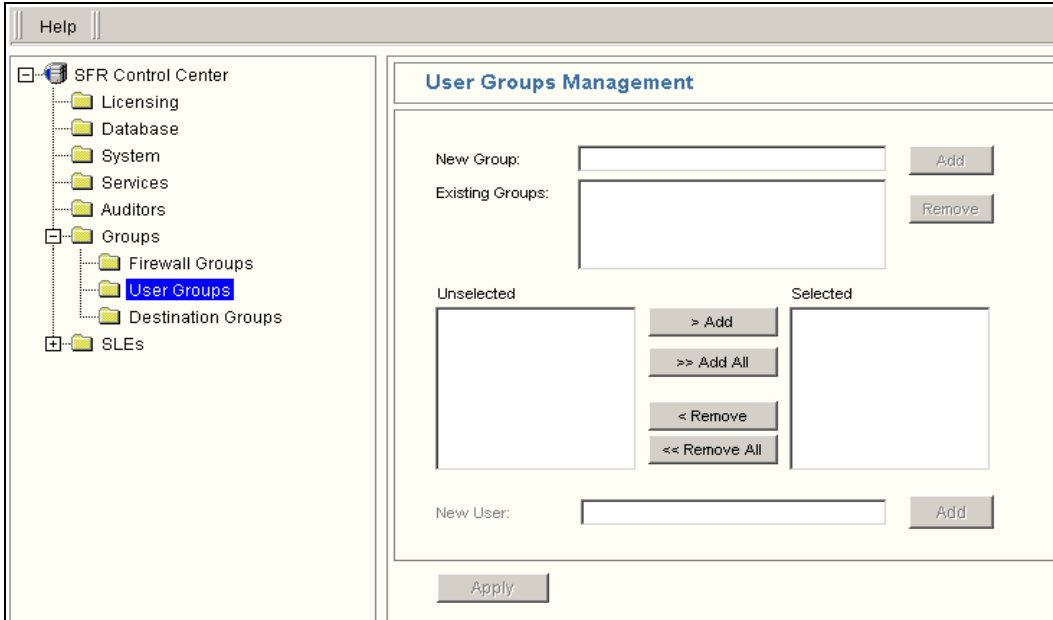
Firewall Groups

Define firewall groups from this screen.



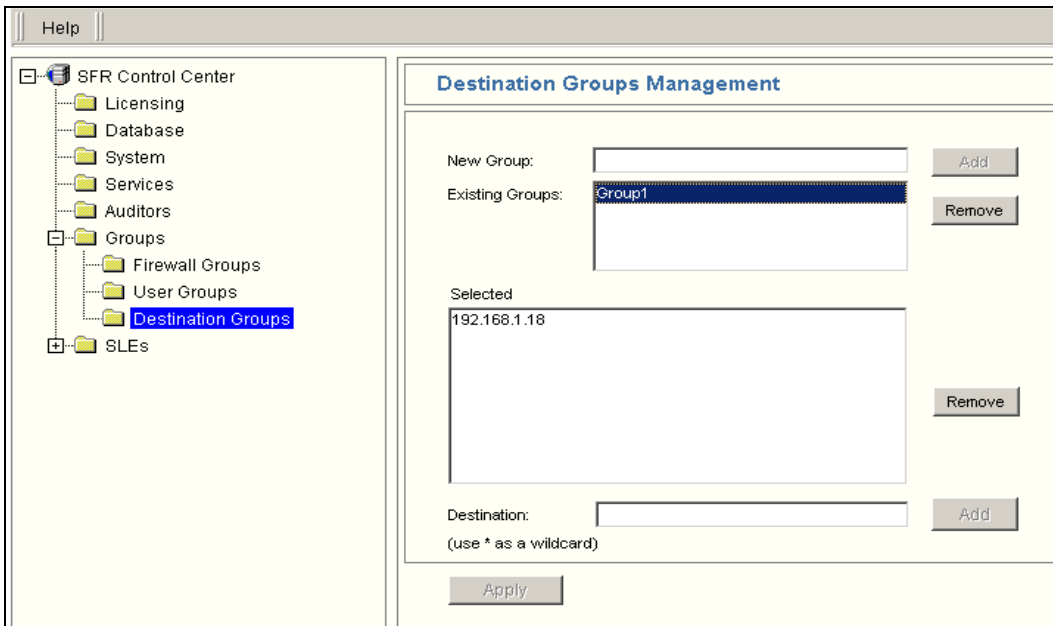
User Groups

Set up User Groups from this screen. Available list of users is dynamically updated at maintenance time. Note that no users will be displayed until the maintenance procedure has run at least once.



Destination Groups

Set up destination groups from this screen



SLE (SFR Logging Engine)

Right click the ILEs node to add a New SLE configuration. Every SLE configuration is uniquely identified by the IP address of the machine hosting the SLE component and is needed for an SLE to run.

The SLE configuration additionally defines one or more Data Processors. Each Processor is a process established by the SLE component to process log data from one specific firewall.

The screenshot displays the SFR Control Center interface. On the left is a tree view with the following structure:

- SFR Control Center
 - Licensing
 - Database
 - System
 - Services
 - Auditors
 - Groups
 - Firewall Groups
 - User Groups
 - Destination Groups
 - SLEs
 - 127.0.0.1** (selected)
 - Processor-PIX
 - Processor-FW1
 - Processor-CPNG
 - Processor-NetScreen
 - Processor-StoneGate
 - Processor-SonicWall

On the right is the 'SLE(SFR Logging Engine) Settings' configuration panel:

SLE(SFR Logging Engine) Settings	
Disk Capacity:	N/A
Used Space:	N/A
Free Space:	N/A
IP Address:	<input type="text" value="127.0.0.1"/>
SLE Com Port:	<input type="text" value="7878"/>
Maximum records per temp log file:	<input type="text" value="50000"/>
<input type="radio"/> Save raw log in database	<input checked="" type="radio"/> Save raw log to file
Create raw log file every:	<input type="text" value="24"/> hours
Delete raw log older than:	<input type="text" value="3 Month"/>

An 'Apply' button is located at the bottom of the settings panel.

IP Address: defines the IP address of the machine that hosts the SLE.

When an SLE component starts up, it first connects to the SCC and receives its configuration based on its IP address and sets itself up accordingly. The SLE does not run when a configuration is not available.

SLE Com Port: is the TCP port that the SLE must open to receive communications from the SCC.

Maximum records per temp log file: Log records are stored temporarily in files before being written to database. This parameter holds the number of records per temporary log file. Increasing the number of records per file increases the size of the file and accordingly the risk associated with file corruption. Keeping a lower number of records per file increases the number of files and frequency of their creation and deletion.

Files are deleted as they are processed. When an SLE is stopped, it notes the last record processed and then when restarted, it resumes processing any pending temporary files starting from the last processed record.

Create Raw Log file every: This option is not available in the Standard Edition.

Raw Logs are written to files. Define here how frequently to open a new raw log file. Each Processor's Raw Log files are stored in a sub-folder named after the Processor ID in the rawlogs folder of each SLE installation.

Delete Raw Log Files older than: Define here how frequently - daily, weekly, or monthly (1 to 6 months) to delete raw log files. A separate process must be used to archive the raw log files if needed.

To Delete an SLE configuration, right click the SLE node and choose Delete SLE. When an SLE configuration is deleted, the licenses associated with each Processor defined in the SLE are returned to the System.

Processors

Each firewall requires a unique Processor for processing its logs. Each Processor runs within the context of an SLE. A Processor might also have a Remote Processor counterpart.

To set up a Processor, choose an SLE that will run the Processor. Right click the SLE in the SCC tree and choose New Processor; then define the settings for the Processor.

A Processor can be Started and Stopped manually from the SCC tree. Right click the Processor node to Start/Stop. Optionally the Processor can be set to start automatically when the SLE component starts.

The screenshot shows the SFR Control Center interface. On the left is a tree view of the SCC structure, including SLEs, Groups, and Services. The 'Processor-PIX' node under the '127.0.0.1' SLE is selected. The main area displays the 'Processor Settings' dialog box with the following fields and options:

- Name:** PIX (Processor ID: 1)
- Description:** CISCO PIX firewall
- License:** Full - Expiring Never (Assign License... button)
- Firewall Type:** Pix 6.x (dropdown)
- Syslog Port No.:** 514 (Origin ID: 192.168.1.1)
- Network ID:** 192.168.1.0 (Subnet Mask: 255.255.255.0) (Add/Remove buttons)
- Logging Enabled
- Raw Logs Enabled
- Start Automatically
- Ignore Port 53, 137, 138, 139
- Resolve subnet when logging
- Resolve Internal IP Addresses when logging
- Resolve External IP Addresses when logging
- Apply** button

Name: The user-friendly name of the Processor. This name will be used in all Reports for the associated firewall.

Description: A description of the associated firewall.

License: The license that has been assigned to the Processor. Each Processor requires a license to be able to run. Click on the License button to assign, reassign or delete a license.

Firewall Type: Define a firewall type from the list of available options.

Syslog Port Number: Define the **UDP port number** that the Processor listens on for logs coming from the firewall. The protocol is UDP, which cannot be changed. The default port is 514.

The Syslog Port Number value for a Processor must be unique in the context of its SLE and the firewall must be configured to use the same port number to send logs for the Processor to work correctly.

In case of Check Point™, it is the LEA Client that would send the logs to an SLE. The LEA Client sends one Syslog stream for each FireWall-1® Module.

In case of StoneGate, it is the Log Server that sends the logs to an SLE. From among all the Data Processors configured for StoneGate, one Data Processor in the SLE is picked by the system to capture the single stream sent by the Log Server. This processor then segregates the data into temp files in accordance with the configuration of each StoneGate Data Processor. Thus all Data Processors for StoneGate are given the same Syslog Port- the UDP port on which the Log Server sends the logs. Additionally, the firewall (node) IP address is defined in each Data Processor for Syslog segregation.

Firewall Name: This is applicable only for Symantec (Raptor) firewall. This name is the basis for naming the receiving folder for log files.

Origin IP: Used to specify the IP address of the source of logs, usually the firewall. For Check Point™ it will be the IP address of the LEA Client. For Stonegate it will be the IP address of the Node.

Network ID and Subnet Mask: Define the network ids and the subnet masks for subnet resolution.

Logging Enabled: Logging to the database can be enabled or disabled. By default logging is enabled. In case of an evaluation copy this option is disabled upon the expiration of the evaluation license.

Raw Logs Enabled: Logging Raw Logs to the database can be enabled or disabled. By default logging is disabled. In the case of an evaluation copy, this option is disabled upon the expiration of the evaluation license.

Start Automatically: Check to start the Processor automatically when the SLE starts.

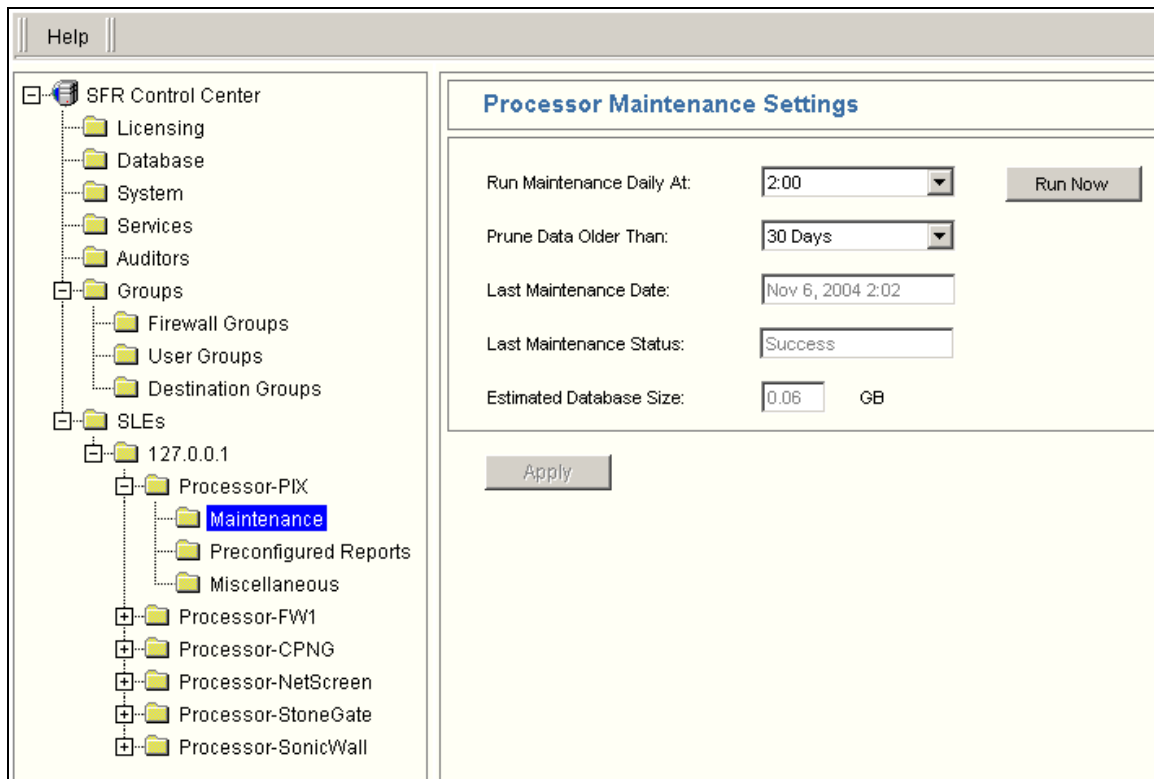
Ignore Port 53, 137, 138, 139, 445: Traffic on ports 53, 137, 138, 139, 445 is generally denied in a typical firewall configuration. While any traffic on port 137 is popularly

considered risky, not all traffic is harmful. Numerous denials logged for port 137 may be due to name resolution calls. To avoid construing these instances as hacker attacks, you have the option of ignoring logs related to port 53, 137, 138, 139, 445. By default this option is enabled.

Resolve External/Internal IP addresses when Logging: By default, IP addresses are resolved to machine names. Turning this off will decrease the processing load. Keeping this on will create new network traffic for address resolution.

Resolve Subnet when Logging: This is applicable only if the local network is divided into one or more subnets. It requires the network information to be filled out. Reports by subnet are useful in many ways – for example, determine bandwidth utilization by subnets or use of different subnets by roaming/laptop users

Maintenance



The screenshot shows the SFR Control Center interface. On the left is a tree view of the system structure, including folders for Licensing, Database, System, Services, Auditors, Groups, SLEs, and various Processor folders like Processor-PIX, Processor-FW1, Processor-CPNG, Processor-NetScreen, Processor-StoneGate, and Processor-SonicWall. The 'Maintenance' folder under Processor-PIX is selected. On the right is the 'Processor Maintenance Settings' panel. It contains the following fields and controls:

- Run Maintenance Daily At: 2:00 (dropdown menu) with a 'Run Now' button.
- Prune Data Older Than: 30 Days (dropdown menu).
- Last Maintenance Date: Nov 6, 2004 2:02 (text field).
- Last Maintenance Status: Success (text field).
- Estimated Database Size: 0.06 GB (text field).
- An 'Apply' button at the bottom.

Run Maintenance Daily At: Set the time for daily database maintenance. Database maintenance entails the archiving and pruning of old records, the re-indexing and compacting of the associated tables for improved performance, preparing future tables, rebuilding views, updating the summary tables and updating the list of unique users. Reports cannot be generated when the maintenance process is running. A typical maintenance procedure takes approximately twenty (20) minutes to complete. Though reports cannot be generated during maintenance, logging of new data will continue.

Note: configurations using MS SQL Server should not schedule any database maintenance tasks from MS SQL Server manager for the SFR database as these are done by the SFR Maintenance task. Only backups of the database and transaction log files need to be done externally.

Run Now: allows you to run the maintenance process on demand.

Prune Data Older Than: Specify the age of the log and raw log records that will be deleted (the default is 60 days). Deletion occurs during the daily maintenance process. The data should be archived as required prior to pruning.

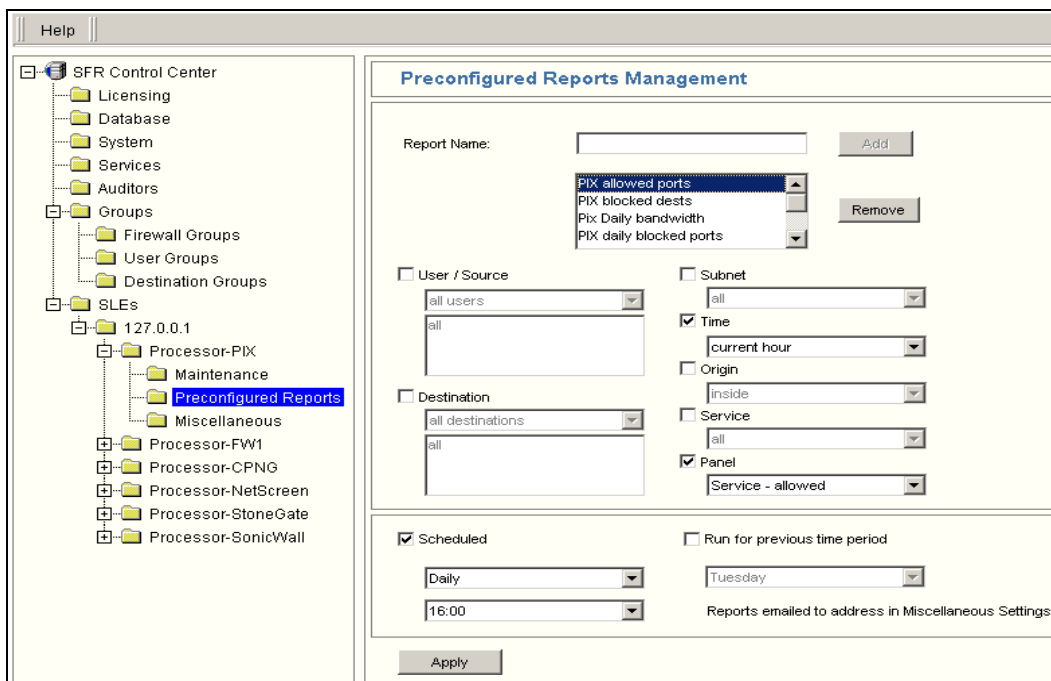
Last Maintenance Date: Displays the date and time that the last maintenance procedure was completed.

Last Maintenance Status: Displays the status - Success or Failure - of the last maintenance procedure. SFR can be set to alert the administrator in case of maintenance failures. Errors encountered in the maintenance procedure are logged to the Jakarta log files in the C:\Program Files\SFR\shared\logs\ folder.

Estimated Database Size: displays the approximate size of the database determined during the last Maintenance run.

Pre-configured Reports

This feature is available only in the Enterprise Edition. Pre-configured reports can be set up for conveniently generating Reports with a single click. Each Pre-configured report can be defined using any combination of the filter settings.



Scheduled Reports

This feature is available only in the Enterprise Edition. A Pre-configured report can be scheduled for daily or weekly run for automatic generation and delivery via email.

Optionally, the scheduled report can be generated for a previous period. For example, a pre-configured report using a time setting of “This week” can be used to generate a Scheduled Report for “Last Week” by checking the “Run for Previous Time Period” option.

All Reports generated by Scheduled Reports are stored in SFR and available at <http://server:8080/SFR/schedule/index.html>

Miscellaneous Settings

The screenshot shows the SFR Control Center interface. On the left is a tree view with the following structure:

- SFR Control Center
 - Licensing
 - Database
 - System
 - Services
 - Auditors
 - Groups
 - SLEs
 - 127.0.0.1
 - Processor-PIX
 - Maintenance
 - Preconfigured Reports
 - Miscellaneous
 - Processor-2

The main content area is titled "Miscellaneous Settings" and contains the following configuration options:

- Email Address same as System Email Address
- Email Address:
- Refusals Alert Threshold:
- Alert in case of Maintenance Failure
- Standard internal IP addresses:
 - 10.0.0.0 to 10.255.255.255
 - 172.16.0.0 to 172.31.255.255
 - 192.168.0.0 to 192.168.255.255
- Additional Internal IP addresses:
 - Start IP:
 - End IP:
 -
 -
- Remote Process Remote IP Address:
- Transfer logs every hour(s)
- Transfer logs every Mega Bytes
-

Refusals Alert Threshold: Set the refusals alert threshold to None, Low (5 refusals/min), Medium (15 refusals/min) (default) or High (50 refusals per minute). An email alert is sent on breaching the threshold.

Alert in case of Maintenance Failure: Enable (default) or disable email alerts on Database Maintenance failures.

Additional Internal IP Addresses: Define here additional IP addresses that are considered internal.

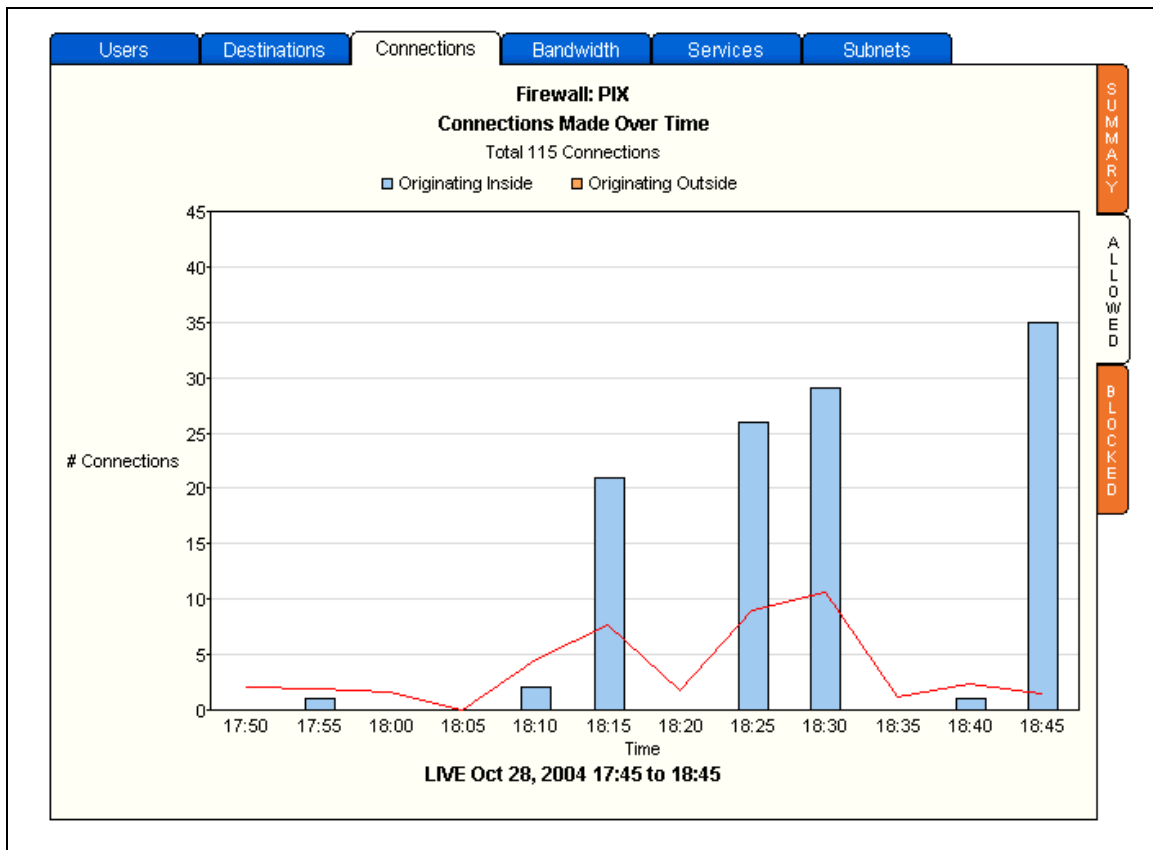
Remote Process: Enable to specify this processor to be the master for a Remote Processor.

Remote IP Address: Define here the IP address of the Remote Processor that the SLE will connect to communicate. It could be a public IP address mapped to the Remote Processor host machine or it could be a private IP address on the remote network.

Transfer Logs: Specify here how often the log file from the Remote Processor must be transferred to the central processing facility.

8. ANOMALY DETECTION SYSTEM

The Anomaly Detection System (ADS) module detects anomalies between current values and historical averages in real time and sends out email alerts containing numerical values and graphical snapshot of the trailing one-hour statistics.



Average values calculation

The starting historical average values are calculated whenever the system starts. Thereafter the average values are updated continuously with fresh data as it comes in. An average value is always the moving average for the trailing one-hour for same time period and same weekdays for the previous four weeks. For example, the average for the one hour between 3.15 pm to 4.15 pm on a Tuesday will be calculated using the data for the past four Tuesdays between 3.15pm to 4.15 pm.

Configuration

Launch URL <http://server-ip:8080/ads> to configure the Anomaly Detection System. Enter the email address that the alerts should be sent to and set up the Rules.

Rules

Rules can be set up to monitor any combination of one or more IP addresses and one or a group of services. Furthermore, a rule can be set to monitor attempts, connections or bandwidth.

Alerts sent by the ADS can be one three categories:

Category 1 Alert is sent when the moving 1 hr total of any of the Activities Monitored goes above the threshold for 10 minutes.

Category 2 Alert is sent when the moving 1 hr total of any of the Activities Monitored goes above the threshold for 5 minutes.

Category 3 Alert is sent instantly when the moving 1 hr total of any of the Activities Monitored goes above the threshold

Shown below is a typical rule:

Processor: PIX

Host name or IP: all

Services: all

The Services listed above are defined in the SFR Control Center

Activity Monitored: connections bandwidth attempts

Category 1 Alert: Threshold: 50 % above avg Wait: Minimum 60 minutes between alerts

Category 2 Alert: Threshold: 30 % above avg Wait: Minimum 15 minutes between alerts

Category 3 Alert: Threshold: 150 % above avg Wait: Minimum 30 minutes between alerts

Save Cancel

Suggested Rules

Rules will vary from organization to organization depending on organization policy and focus of interest. A good starting point would be to set up 3 rules – one to monitor connections, the second to monitor bandwidth and the third to monitor attempts. Set the threshold on each to 50%, minimum wait between alerts to 60 minutes and enable Category 1 alert. A final rules set up will need a lot of fine-tuning of the parameters in correlation with the historical data.

Other suggested activities to monitor:

1. Bandwidth on SMTP. An alert could indicate a compromised email server or host.

2. Bandwidth on FTP.
3. Attempts and Connections on all services and all hosts. An alert could indicate an attack or early warning of an outbreak of a new virus.

ADS Password

The password to access the ADS Control Center is the same as the one used to access the SFR Control Center. Any changes made to the SCC password are effective on the ADS immediately.

Available List of Services

The services listed in the ADS for monitoring are maintained from the SFR Control Center. For a new service to show up in ADS, it must be added in the SFR Control Center.

Initial Operation

When the system is started after installation, the database at first is blank. Accordingly the average values will be zero for at least the first week. The alerts will however still work if enabled in accordance with the Rule parameters. Best results from ADS will be apparent only after a week of SFR operation.

Memory Usage

Memory usage for ADS is directly proportional to the number of Rules setup. Moreover, the entire ADS module is operated in memory. Accordingly, sufficient physical memory availability is critical and should be provided for proper ADS operation.

9. PERMANENT LICENSE KEY

SFR comes with built in 30 day trial licensing. Standard Edition comes with one license each good for one firewall. The Enterprise Edition comes with three licenses good for three firewalls.

In Trial mode, only data less than 48 hours is stored. A permanent license key is required to continue operating the software beyond 30 days and for not deleting the data.

How to Obtain

1. Launch the SFR Control Center (SCC). The Host ID for your machine is displayed prominently on the main screen.
2. Alternatively, the Host ID is also displayed on the console when the SFR server starts.
3. If you are placing a Purchase Order, Host ID information has to be submitted along with the Company, Contact and payment information.
4. When you receive the permanent license key from Stonylake Solutions, in the SCC tree navigate to the "License" node and enter the new license information.

10. UNINSTALL

In an MS Windows environment run the uninstall program `unwise.exe` found in the root folder of SFR. Note that this will not uninstall the database.

To uninstall in a Linux environment, simply delete the SFR directory and its contents.

11. TROUBLESHOOTING

System Checks

General

1. Is the database server running?
2. Is the correct database userid and password specified in the SCC?

SCC

1. Is Tomcat running as a service as well as via `startup.bat`? Only one instance must run.
2. Has an edition been activated – `http://server_ip:8080/SFR/admin.html`
3. Is the Processor assigned a valid license?
4. Has a valid Origin IP been specified.

5. Is the SLE running? (c:\program files\sfr\SLE\bin\sle.bat)

SLE

1. Is the IP address defined for the SCC in the SLE.ini file correct?
2. Has the SLE Service already started in the background and you are trying to start another instance via sle.bat?
3. Is the SLE defined in the SCC?
4. Is another vendor's syslog server running on the machine? Shut it down.

Firewall

1. Stonegate – is the Origin ID defined correctly in the Processor? This is the IP address of the firewall node.
2. Check Point™ NG FP3 – automatic log file switch results in no logs being received by the LEA Client. To resolve this problem on a Windows platform, run a scheduled task using the command 'fw logswitch' instead of the feature built in Check Point™.
3. Check Point™ error – “unable to contact the Certificate Authority on the management station, please make sure the certificate authority daemon is running”. To resolve this problem add the following line to fwopsec.conf

```
lea_server auth_port 0
```

Error Log Files

If you are having some issues with getting the SFR server to run, or your browser to load the applets, there are a few log files you can look at that may help you out. If you are still having problems, you will need these files when you reach Technical Support. The files are located at C:\Program Files\SFR\shared\logs

Common Problems and Solutions

1. Tomcat does not start when you run startup.bat
 - Tomcat may have already started as a service. Stop the service and then try running startup.bat
2. Applet does not load
 - Possible reason – Java virtual machine not enabled.
Solution - In Internet Explorer Menu, navigate to Tools | Internet Options | Advanced Tab. Locate and check Java (Sun): Use Java [version] for (applet) or locate Microsoft VM and check Java Console and JIT Compiler.

If the Java Virtual Machine is missing, download and install the Java (Sun) Plugin available at <http://java.sun.com/getjava/>

3. SLE does not run – starts and quits because no configuration available
 - Verify that the SCC address is correctly specified in sle.ini. Ensure that SCC is running.
4. LEA is consuming 99% processor power
 - Probably the LEA service is running in the background and in addition the LEA client is run as a foreground process. Run only one instance.
5. Records are being written to the database extremely slowly
 - Name resolution has been turned on and DNS for the SLE machine(s) is not configured correctly. When name resolution is turned on for any processor, the processor queries the DNS or hosts (both internal and external) for their names. If the DNS server does not have the information and the host is not reachable, the processor waits till it times out. This time out for every record slows down the process. Test the speed by turning off name resolution. If this is the problem then DNS and the network has to be adjusted.
 - If it is a high load in excess of 100,000 logs per day on MSDE then switch to SQL Server. MSDE is far slower compared to SQL Server.
6. Some IP addresses are not resolved
 - Verify that DNS and name resolution replies are allowed back in by the firewall to reach the IFR machine. These responses are on port 53 (TCP and UDP) and some on port 137 or 445.
 - All IP addresses do not have a reverse entry available in DNS servers and do not respond to reverse name queries even though the corresponding URL resolves to an IP address. IFR caches all address resolution answers in memory that is flushed to a file called 'cache' in the \SLE\temp folder when you stop the SLE. If wrong answers are suspected to have been cached, the cache can be cleared - delete the cache file and run a command `c:\>ipconfig /flushdns`. After this, start SLE again. Cached records have a ttl of 28800 secs (8 hours)
7. Increased NetBios traffic to SFR
 - This traffic is due to address resolution queries sent by SFR on a Windows platform to remote hosts. NetBios queries are the last option by default on Windows 2000 or later. These can be turned off from My Computer | Manage | System Tools | Device Manager (View, Show Hidden Devices | Non-Plug

and Play Drivers | NetBios over TCPIP – right click Disable. Note that this will adversely affect accessing shares over the local network.

12. TECHNICAL SUPPORT

Search the knowledge base at <http://www.stonylakesolutions.com>

By email: Email your question to support@stonylakesolutions.com

Phone: Call toll free (866) 757 0852 from within North America or +1 (416) 929 0343 internationally.

Please have your log files handy when you reach our Technical Support (see the Troubleshooting section).