

Usage guide

Firesectm

Firewall Rule base Analysis Tool

PCI DSS Compliance



Comprehensive rule base analysis for medium to large enterprise environments

The large picture – Automation of rule base analysis

- Simplified analysis of large rule sets
- Removes redundancy
- Compares rule sets
- Groups common rules
- Searches for vulnerable rule patterns
- Analyses security

in Full Version

Supported Firewalls

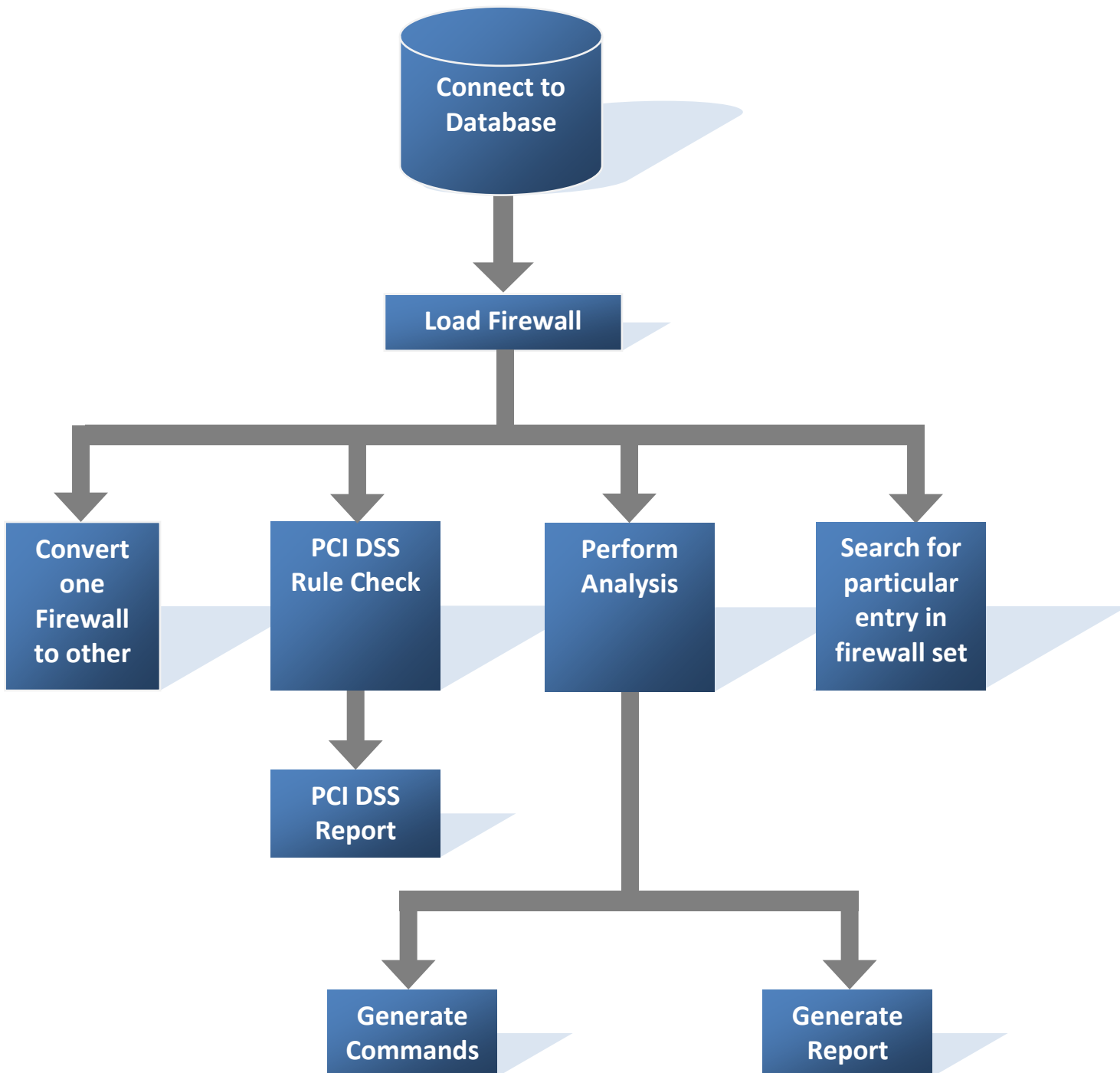
Netscreen
Cyberguard
Cisco PIX
Generic rule sets

in Trial Version

Supported Firewalls

Only default logs provided with the setup

Firesec™ Architecture



Steps to run FireSec

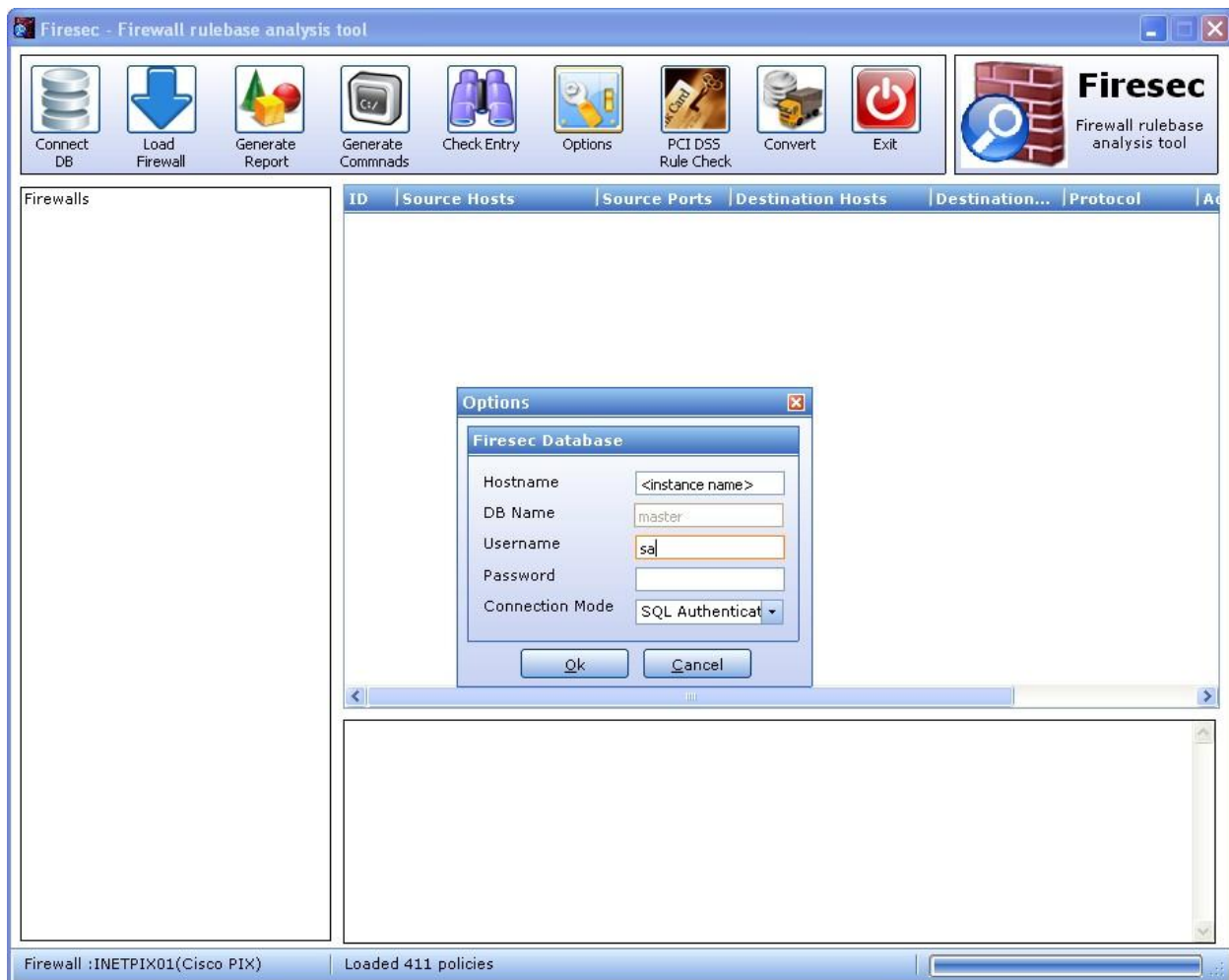
Prerequisites:

SQL Server instance running on local or any remote system to store & analyze the rules set

Following are the two simple steps to use FireSec

Step 1: For the first run of FireSec, it prompts for the login credentials of the SQL server. Click Connect DB menu to connect to the database. The login credentials can also be changed later using the Option menu in the toolbar.

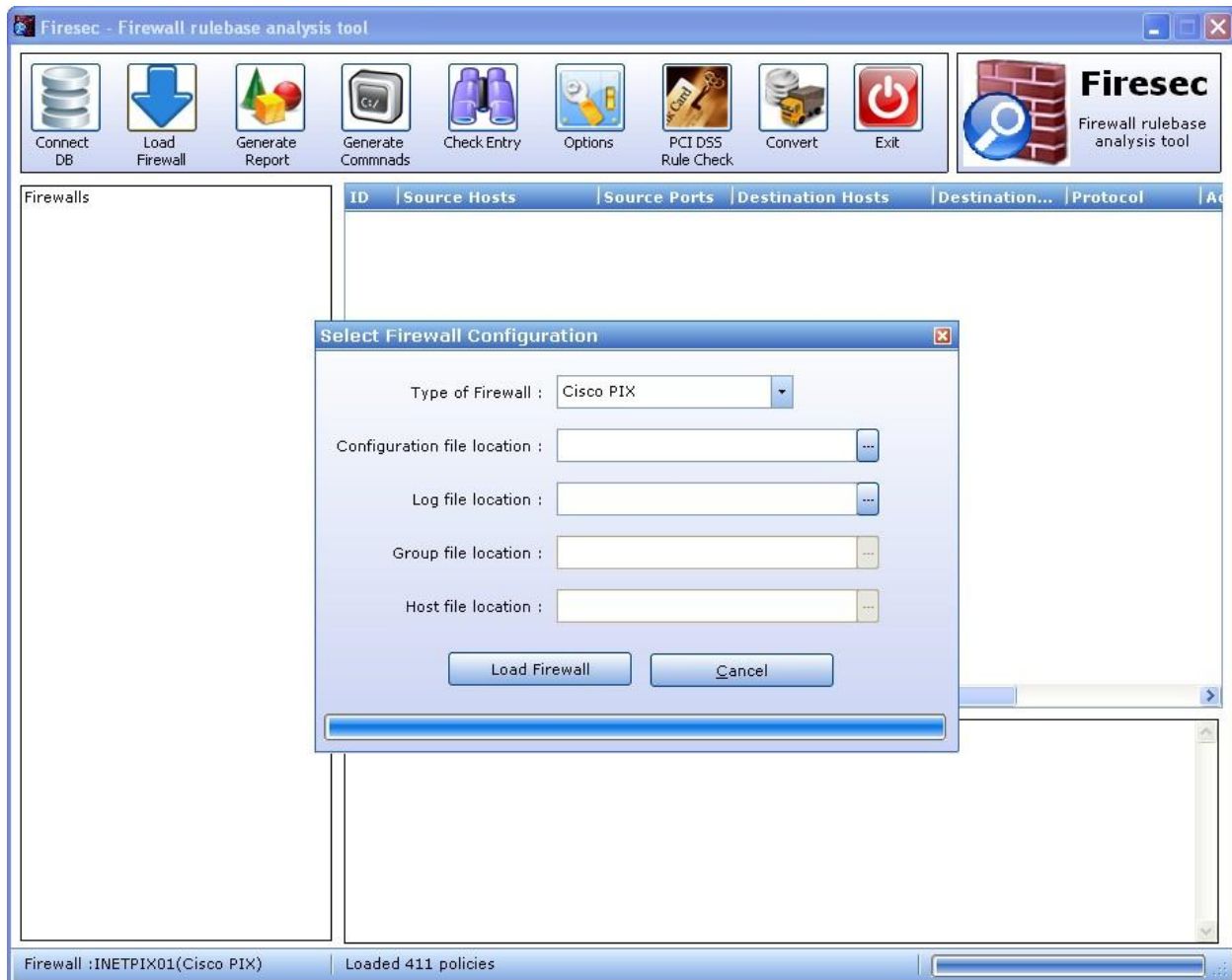
Screenshot:



Connecting to Database

Step 2: Once connected, use the Load firewall menu to load the config & the log file of the firewall.

Screenshot:



Before loading

ID	Source Hosts	Source Ports	Destination Hosts	Destination...	Protocol
1	any		any	42	UDP
2	any		any	42	TCP
3	any		any	5554	TCP
4	any		any	9996	TCP
5	any		4000	any	UDP
6	22.118.100.78/32		any	any	ICMP
7	any		any	1434	UDP
8	any		any	6129	TCP
9	dialup/22		dialup/24	any	ICMP
10	Dailup_user/23		intranet	80	TCP
11	any		idl	80	TCP
12	any		HASimc01	25	TCP
13	any		HASimc02	25	TCP
14	any		HASimc04	25	TCP
15	any		22.118.128.154/32	25	TCP
16	any		WAS	21	TCP
17	Dailup_user/23		cache	8080	TCP

Firewall : INETPIX01(Cisco PIX) | Loaded 411 policies

After Loading

Methodology for obtaining the log and configuration files

Before beginning with the firewall analysis, the following must be in place:

Cisco PIX: For the Cisco PIX firewall you will need the following:

1. Output of the “sh config” command.
2. Output of the “sh access-list” command.
3. Halt all changes to be made to the firewall 48 hours prior to the rollout window.

Cyberguard: For the Cyberguard firewall you will need the following:

1. Exported configuration of the Cyberguard.
2. Results from the log analysis script on the Cyberguard logs.
3. Halt all changes to be made to the firewall 48 hours prior to the rollout window.

Cyberguard-Knightstar: For the Cyberguard-Knightstar firewall you will need the following:

1. Exported configuration of the Cyberguard-Knightstar.
2. Results from the log analysis script on the Cyberguard-Knightstar logs.
3. Exported Group configuration of the Cyberguard-Knightstar.
4. Exported Host configuration of the Cyberguard-Knightstar.
5. Halt all changes to be made to the firewall 48 hours prior to the rollout window.

Netscreen: For the Netscreen firewall you will need the following:

1. Exported configuration of the Netscreen.
2. Results from the log analysis script on the Netscreen logs.
3. Halt all changes to be made to the firewall 48 hours prior to the rollout window.

Log Analysis

Cisco PIX

The log analysis process for the PIX firewall simply requires the output of the “show access-list” command to be obtained

Cyberguard

Navigate to the directory where the logs are being stored.

If the logs are in zipped format:

```
$ zcat *.log.* | perl cgloganalysis.pl -n <FW Name or IP address> | sort -n | uniq > output.log
```

If the logs are in unzipped format

```
$ cat *.log | perl cgloganalysis.pl -n <FW Name or IP address> | sort -n | uniq > output.log
```

Netscreen

Navigate to the directory where the logs are being stored.

If the logs are in zipped format:

```
$ zcat *.log.* | perl nsloganalysis.pl -n <FW Name or IP address> | sort -n | uniq > output.log
```

If the logs are in unzipped format

```
$ cat *.log | perl nsloganalysis.pl -n <FW Name or IP address> | sort -n | uniq > output.log
```

Once the firewall config is loaded, you can do the following analysis on the firewall configuration loaded

1) Normalization

Reads the firewall configuration and normalizes it into a standardized database format. Both rules and firewall objects are fed into the FireSec database for analysis.

2) Traffic analysis

FireSec comes with standard firewall log parsing scripts, which will chew through giga bytes of logs, and retrieve the relevant packet information. The output from the log parsing scripts is read by the tool to check against the rule sets and remove those, which were not being used.

3) Rule Analysis

FireSec supports following types of rules analysis

- ❑ **Log Analysis** – Studies have shown that for most firewalls the actual traffic that passes through them uses up only a small subset of the actual rules. Therefore, traffic log analysis for the firewalls helps to determine which rules are actually being used, and which are not. This is the first and most important step in the firewall analysis.
- ❑ **Shadow rules** – two or more rules which match the same traffic, but perform opposite actions
- ❑ **Grouped rules** – Certain rules have the same source address, and the same destination addresses, but different destination ports. These rules can be grouped by creating an object group for the combined ports of the rules, and retaining only one rule from the set and dropping all the others. For instance, the following rules can be grouped together:

```
access-list outside_access_in permit udp host aaa-router host aaa-server eq radius-acct
```

```
access-list outside_access_in permit udp host aaa-router host aaa-server eq radius
```

In this case, both the rules have the same source IP address (aaa-router), the same destination IP address (aaa-server), but different destination ports (radius-acct and radius). Thus, these two rules can be grouped together by creating a new object group, say new_group_1, with radius and radius-acct added to it, and dropping the second rule and replacing the destination port in the first rule with this new object group.

Thus the revised configuration would look like

```
object-group service new_group_1 udp  
port-object eq radius
```

```
port-object eq radius-acc  
access-list outside_access_in permit udp host aaa-router host aaa-server object-group  
new_group_1
```

- ❑ **Redundant rules** – Often new rules are created on the firewall, which process traffic that some other rule already processes. Thus this rule is never processed, or even if it is processed, there is already some other rule that processes the same traffic. For instance, the following two rules of a Cisco PIX firewall are redundant:

```
access-list outside_access_in permit tcp host webserver1 host intranet eq www  
access-list outside_access_in permit tcp any host intranet eq www
```

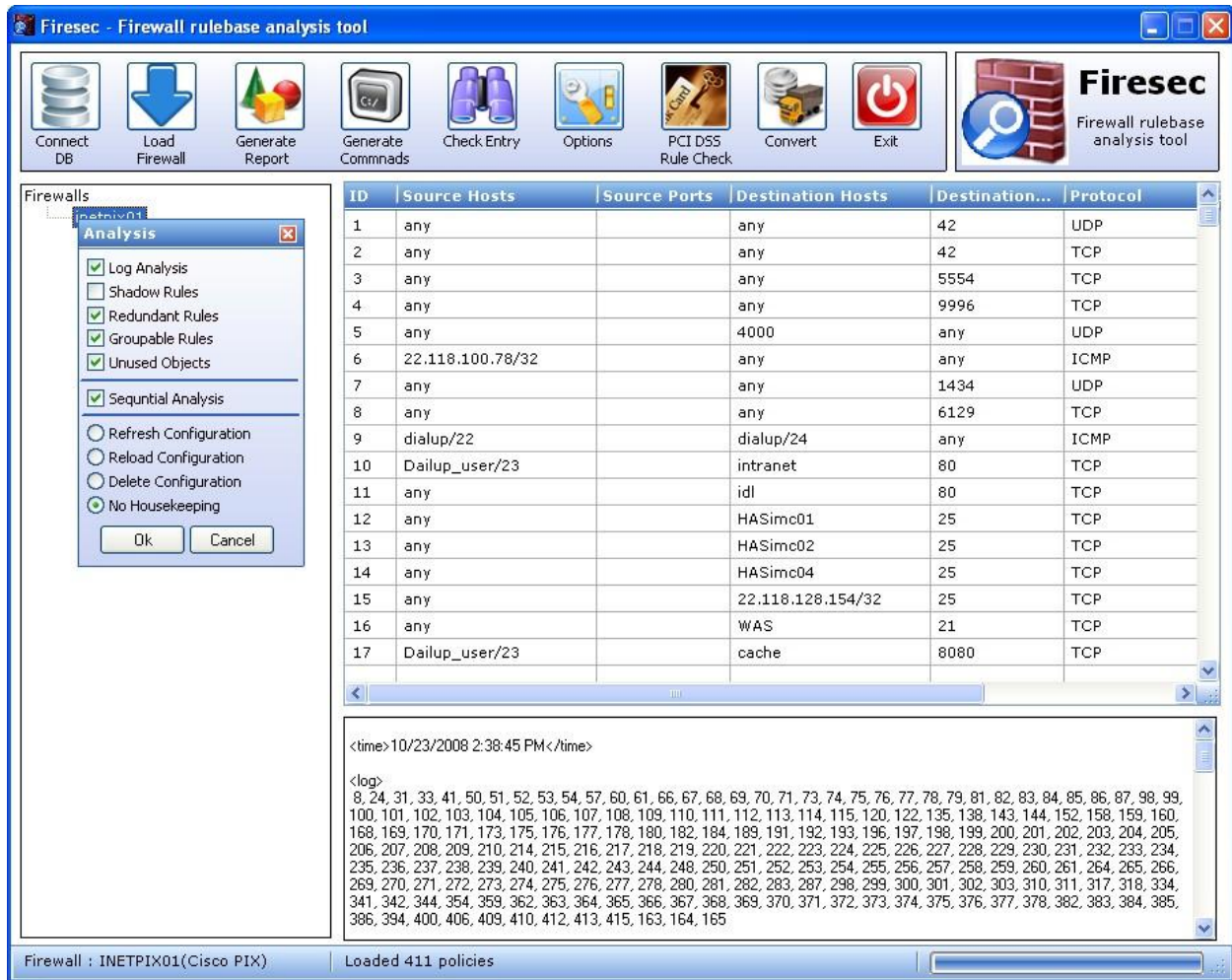
The first rule allows the host “webserver1” access to port 80 on the host “intranet”. The second rule allows any source access to the host “intranet” on port 80. Therefore, the first rule is a *subset* of the second rule, and so it can be removed.

- ❑ **Unused Objects** - Once all the rules that can be removed have been removed, a number of firewall objects would be found which are no longer in use. These objects also consume resources, and should be removed

4) House Keeping

FireSec also gives you flexibility to reload, refresh & delete a particular configuration in case of any changes made or introduced in the configuration of the firewall.

Screenshot:



Analysis Options

5) Reporting

Once done with the analysis of your choice you can then view the report using the “Generate Report” menu in the toolbar.

Firewall Rulebase Analysis Report

Copyright © Network Intelligence (I) Pvt. Ltd.

Results of analysis carried out for:

Firewall	inetpix01
Type	Cisco PIX
Date	10/23/2008 2:38:45 PM

Statistics on the analysis:

Rules category	Number dropped	Percentage
Log analysis	200	48.66 %
Redundant	5	1.216 %
Grouped	18	4.379 %
Unused objects	32	7.785 %

Results of log analysis

The following policies can be dropped based on log analysis

Top

Overview of the analysis

Results of log analysis

The following policies can be dropped based on log analysis

ID	Source Hosts	Destination Hosts	Services	Action
8	any	any	6129	deny
24	any	edirectory1	80	permit
31	dialup/24	inetlog02	161	permit
33	dialup/22	22.118.128.78/32	53	permit
41	any	22.118.128.25/32	80	permit
50	22.118.128.20/32	any	443	permit
51	22.118.128.25/32	any	443	permit
52	ABCNet	BSC	8080	permit
53	any	22.118.128.152/32	80	permit
54	any	22.118.128.152/32	443	permit
57	any	symantec1	25	permit
60	any	22.118.128.95/32	80	permit
61	ipass	22.118.128.158/32	577	permit
	ipass	22.118.128.68/32	23	permit
	26.239.102.125/32	22.118.128.68/32	any	permit
	26.239.111.125/32	cache1-out	any	permit
	26.239.108.125/32	22.118.128.68/32	any	permit
	26.239.110.125/32	any	any	permit
	26.239.105.125/32	cache1-out	any	permit
	26.239.104.125/32	22.118.128.68/32	any	permit
	26.239.101.125/32	any	radius:radius-acct	permit
	26.239.99.125/32	22.118.128.66/32	radius:radius-acct	permit
	26.239.98.125/32	22.118.128.67/32	radius:radius-acct	permit
	26.239.109.125/32	cisco-tac	23	permit
	26.239.103.125/32	172.20.238.77/32	1521	permit
	26.239.107.125/32	172.20.238.77/32	1521	permit
	8.22.202.21/32	ibill	515	permit
77	ebill	inetlog02	22	permit
78	22.118.128.224/28	22.118.128.169/32	22	permit
79	22.247.15.77/32	22.118.128.66/32	radius	permit
81	22.118.128.226/32	22.118.128.66/32	radius-acct	permit
82	22.118.128.226/32	any	any	deny
83	22.234.153.202/32			

Results of log analysis

Note: If you mouse hover on the group name or a single host or service group or a single service name then it will create a callout which contains all the member/s of that group or host (See figure above). This will help the analyst while analyzing the firewall.

Results of redundant analysis

The first policy is a subset of the second one

ID	Source Hosts	Destination Hosts	Services	Action
37	escr4466_s	escr4466_d	1645:1646	permit
124	escr-4466_s1	escr-4466_d	1645:1646	permit
ID	Source Hosts	Destination Hosts	Services	Action
38	escr4466_s	escr4466_d	radius:radius-acct	permit
125	escr-4466_s1	escr-4466_d	radius:radius-acct	permit
ID	Source Hosts	Destination Hosts	Services	Action
94	scr2160_d	22.118.128.164/32	mask-reply	permit
97	22.118.136.54/32	22.118.128.164/32	mask-reply	permit
ID	Source Hosts	Destination Hosts	Services	Action
37	escr4466_s	escr4466_d	1645:1646	permit
124	escr-4466_s1	escr-4466_d	1645:1646	permit
ID	Source Hosts	Destination Hosts	Services	Action
312	22.118.128.176/32	12.151.162.110/32	443	permit
325	escr4979_s	12.151.162.110/32	443	permit

Results of redundant analysis

Results of group analysis

The following policies can be grouped together

ID	Source Hosts	Destination Hosts	Services	Action
30	any	ebill	group_30	permit
88	any	ebill	81	permit
89	any	ebill	449	permit
ID	Source Hosts	Destination Hosts	Services	Action
39	22.118.128.225/32	22.118.128.67/32	group_39	permit
55	22.118.128.225/32	22.118.128.67/32	radius	permit
ID	Source Hosts	Destination Hosts	Services	Action
40	any	22.118.128.20/32	group_40	permit
42	any	22.118.128.20/32	443	permit
ID	Source Hosts	Destination Hosts	Services	Action
90	any	22.118.128.110/32	group_90	permit
91	any	22.118.128.110/32	80	permit
126	any	22.118.128.110/32	11001	permit
ID	Source Hosts	Destination Hosts	Services	Action
92	any	22.118.128.91/32	group_92	permit
93	any	22.118.128.91/32	443	permit
ID	Source Hosts	Destination Hosts	Services	Action
183	cache1-out	any	group_183	permit
308	cache1-out	any	443	permit

Results of group analysis

Results of objects analysis

The following objects can be dropped

Objects
no object-group service escr3240_p
no object-group service escr5723_p1
no object-group service escr7197_p
no object-group service escr8764_p1
no object-group service escr8793_p1
no object-group service escr9313_p
no object-group service escr9313_p1
no object-group service Internet-MIS
no object-group service scr05-01-1581_p
no object-group service scr05-01-1685_p
no object-group service scr2160_p
no object-group network escr2129_d
no object-group network escr2129_s
no object-group network escr2689_d
no object-group network escr2689_s
no object-group network escr3240_d
no object-group network escr4466_d
no object-group network escr4466_s
no object-group network escr7197_d
no object-group network escr7880_s
no object-group network escr8241_d
no object-group network escr8384_s
no object-group network escr9313_d
no object-group network escr9313_s
no object-group network escr9332_s
no object-group network ipass
no object-group network scr05-01-1581_s
no object-group network scr05-01-1685_d
no object-group network scr05-01-1685_s

Results of objects analysis

Firewall Rule base Analysis Report

Other prominent features of FireSec are

The analysis part is now complete. All the rules which could have been dropped have been removed. All objects have also been removed. Now, automatic commands can be generated to reconfigure the firewalls. In the case of Cisco PIX and Netscreen where CLI is supported, it simply requires you to copy-paste the output into the command interface. In the case of Cyberguard, the reconfiguration must be done manually.

Note: In all cases, please take a backup of the current configuration

There are two approaches for modifying the firewall configuration:

Approach I: Instead of dropping the rules, which are not needed, simply change their “action” value to “deny”. As a result, when traffic arrives, which meets the rule’s parameters, the traffic is denied, and the logs reflect, which rule affected the traffic. This rule needs to then be reinserted into the rule base. This process can be monitored for a period of one week. All rules, which have mistakenly been dropped (primarily from log analysis), will show up immediately.

If this approach is adopted, then select the radio button “Deny & Drop” and click on “Generate Commands”. This will generate commands to convert all the rules that are to be dropped to action = deny.



Approach II: Directly drop all the rules, which are not required. This can be done after **Approach I**. This results in a completely clean configuration, since all rules which were to be dropped have now been removed. For this, select the radio button “Drop only”, and click on “Generate Commands”.



Generating Drop only Commands for Firewalls

Check Entry

In large rulesets, security analysis can be faulty since not all vulnerable rules might get identified. FRAT enables a quick analysis of the rulebase by looking out for patterns among the rules, which could be either specific IP ranges, subnets, ports, or port ranges.

When you want to check for a specific IP's or a set of IPs against all other rules the destination IPs text area is left blank. This helps you compare against all rules, remaining rules & dropped rules.

Eg: In the screenshot below we have check for ip 22.118.128.0/24 against all rules.

No	Source IP	Destination IP	Service	Rule Acti...	Status
1	any	any	u42	deny	E
2	any	any	t42	deny	E
3	any	any	t5554	deny	E
4	any	any	t9996	deny	E
5	any	4000	uany	deny	E
6	any	any	u1434	deny	E
7	any	22.118.128.131/32	t80	permit	E
8	any	22.118.128.135/32	t25	permit	E

Checking for specific IP's or set of IP's against all rules

Compare Firewall configuration.

FireSec also provides intelligent comparison of rule sets belonging to two or more firewalls. The rule sets can be loaded for not just textual (string) comparison but for similarity between rules based on IP addresses, ports and deny.

Comparing Firewalls based on IP addresses, ports and deny