

Firesec™

Firewall Configuration Analysis Tool

PCI DSS Compliance

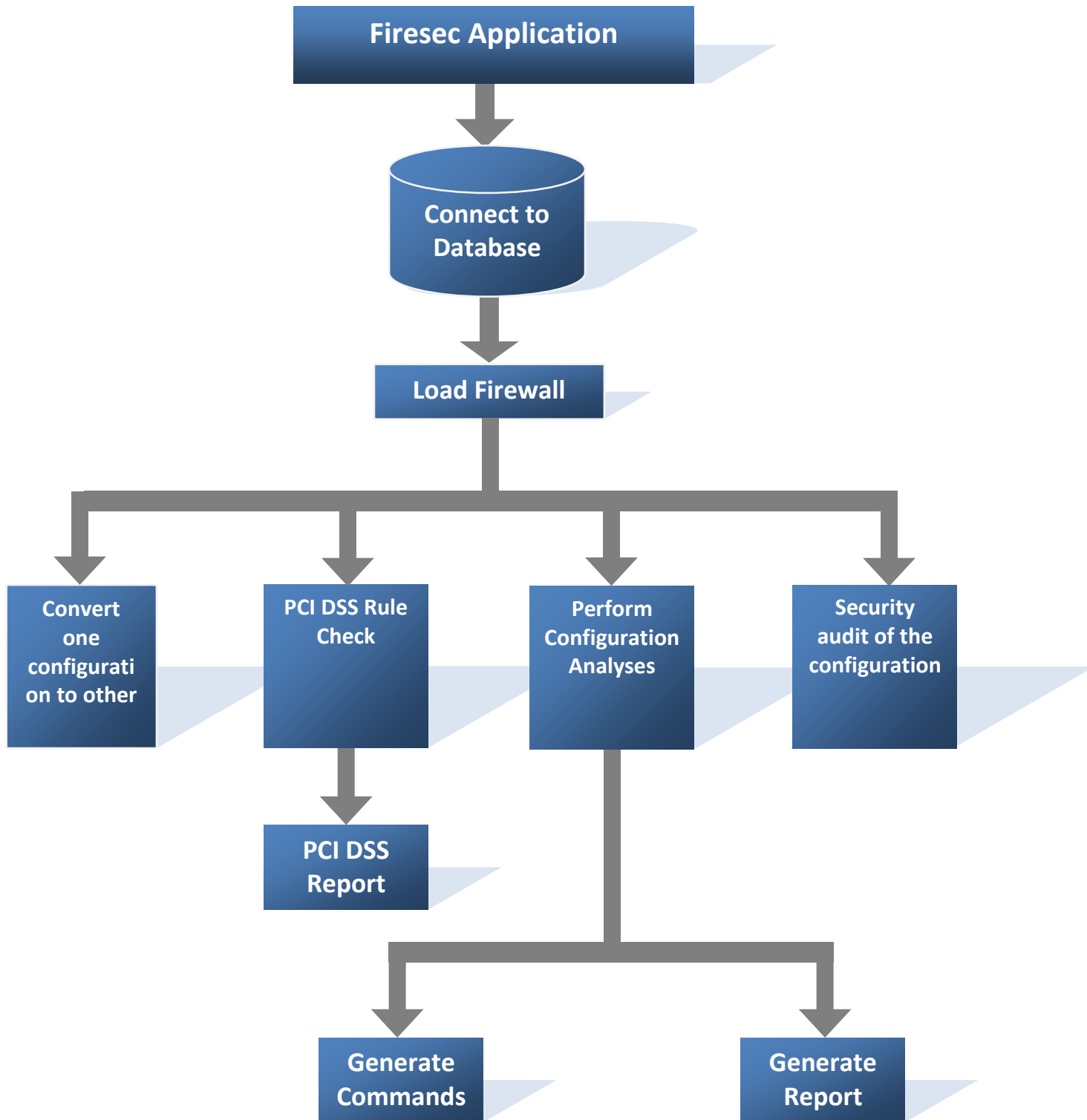


Comprehensive firewall configuration analysis for medium to large enterprise environments

The large picture – automation of rule base analysis

- ❧ Security audits of access control lists
- ❧ PCI DSS compliance review of firewall configurations
- ❧ Simplified analysis of large rule sets
- ❧ Analyses security
- ❧ Removes redundancy
- ❧ Compares rule sets
- ❧ Group's common rules
- ❧ Searches for vulnerable rule patterns
- ❧ Create secured access control lists

Firesec Architecture



Key Benefits

Reduce Cost

Firesec has helped customers reduce their firewall configurations by more than 50% - lesser rules, lesser objects, and therefore lower consumption of available firewall resources. This helps you delay upgrading your firewalls, and helps you maximize the return on investments made on your current firewalls.

Secure Configuration

The security check feature of Firesec helps you scan your entire configuration for rules that contain dangerous ports and access to sensitive servers. Just feed in the IP address, and Firesec will search for that IP address, subnets containing the IP address, object groups that contain that IP address or subnets containing that IP address. Similarly, feed in a port number, and Firesec will search not just for that specific port number, but ranges that contain that port number, as well as object groups that contain that port or such ranges. What would normally take a few hours, can now be completed in a matter of minutes – a comprehensive firewall security audit.

Achieve Compliance

A number of regulations and standards such as ISO 27001 and PCI DSS focus heavily on network segregation and secure firewall configurations. Firesec comes with a specific PCI DSS compliance module that focuses on achieving compliance with this standard. It also helps organizations comply with security standards and requirements flowing from ISO 27001, Sarbanes-Oxley, HIPAA and others.

Increase Manageability

With reduced firewall rule sets, lesser objects, and a more cohesive set of policies, your firewalls suddenly become easily manageable. Once the analysis and clean up is completed, you'll know for sure that what remains is exactly the configuration that is needed on your firewall, and absolutely nothing else. All unused, redundant, shadowed rules and objects will be analyzed and removed.

For more information on Firesec

Visit <http://www.niiconsulting.com/products/firesec.html>

Download a trial version at http://www.niiconsulting.com/products/trial/Firesec_Trial.exe

Key Features



No.	Source	Destination	Service	Action	Track	Install On	Time
1	Any	FWall	Any	reject	Alert	Gateways	Any
2	localhost	FTPServer	Any	accept	Short	Gateways	Any
3	localhost	FTPServer	ftp	accept	Long	Gateways	Any
4	Any	MailServer	smtp	accept	Short	Gateways	Any
5	Any	HTTPServer	http	accept	Short	Gateways	Any
6	Managers@Any	FTPServer	telnet	User Auth	Long	Gateways	Any
7	Any	Any	Any	reject	Long	Gateways	Any

Challenges with large rule sets

In large infrastructures, the firewall rule bases can expand to an extent where they are simply UNMANAGEABLE. Analyses have shown that in any firewall, a large majority of the rules are NEVER USED.¹ In addition, large rule bases create inconsistencies in terms of REDUNDANT² and shadowed rules³. Large rule bases also prevent efficient security audits since insecure or VULNERABLE RULES could get missed during an analysis of a large set of rules

Finally, large rule bases result in PERFORMANCE BOTTLENECKS (packets having to traverse hundreds or thousands of rules to find a match) and resource crunches (number of objects or groups exceeds maximum allowable limits)



No.	Source IP	Destination IP	Service	Rule Action	Status
5	ANY	4000	ANY	deny	E
6	22.118.100.78/32	ANY	ANY	deny	E
9	22.118.128.0/32	22.118.128.0/32	ANY	permit	E
11	ANY	22.118.128.131/32	180	permit	E
23	ANY	22.118.128.130/32	180	permit	C
27	22.118.130.0/32	22.118.128.87/32	ANY	deny	C
29	22.118.133.49/32	22.118.128.100/32	ANY	permit	D
41	ANY	22.118.128.25/32	180	permit	L

Searches for vulnerable rule patterns

Conducting a security audit of a firewall configuration can often be a daunting task. Numerous rules to be verified, within each rule object groups to be checked, members of each of these groups to be verified. Simply searching in a text editor for vulnerable patterns is a faulty process, and can lead to insecure rules continuing to be present in the firewall configuration.

Based on either specific IP ranges, subnets, ports, or port ranges, FireSec enables a quick and very comprehensive analysis of the rule base to identify vulnerable rules, and rules that violate corporate firewall standards and policies.



PCI DSS Rule Check

Firesec™ is an advanced firewall configuration analysis tool, which helps you answer the following questions:

1. What traffic is allowed on to my card holder database?
2. Are there any rules that permit traffic from my internal IP addresses to the Internet?
3. Have I opened up risky ports such as Telnet (TCP 23), FTP (TCP 21), RDP (TCP 3389) to any of my servers?
4. What traffic is allowed between my internal IP addresses and my DMZ?
5. Do I have any rules which contradict each other (Shadow rules)?
6. Do I have rules, which are no longer in use (Unused Rules)?
7. Do I have rules, which are subsets of each other (Redundant Rules)?

¹ Analysis of Firewall Policy Rules using Data Mining, <http://www.mnlab.cs.depaul.edu/mnlab/pubs/noms06-mining.pdf#search=%22Analysis%20of%20Firewall%20Policy%20Using%20Data%20Mining.pdf%22>

² Two or more rules in the same rule base which process the same types of packets

³ Two rules which process exactly the same type of packets but one rule permits them, while the other rule disallows them



Solution from FireSec

FireSec automates the analysis process, and use a multi-pronged approach to rationalize the rule base to the maximum extent possible with the help of

- Traffic analysis to determine rules which have not been used
- Rules analysis to determine Redundant rules, Shadow rules, Group(able) rules
- Configuration analysis to determine objects which can be dropped
- Security analysis can also be automated by formalizing the configuration and searching for vulnerable rule patterns or critical hosts or port ranges



Simplified Analysis of large rule sets

FireSec traverses through the length and breadth of the firewall's rule set to rationalize rules individually and collectively.

Groups Common Rules

Intelligence built into FireSec helps group rules based on common values – source and destination IP address, source and destination ports, and deny/ permit criteria.



Compares rule sets

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/permit

Removes Redundancy

FireSec removes any duplication in the rule set reducing resource consumption to while analyzing packets.



Generates Commands

FireSec reduces the effort of repeating the process by generating commands required to clean up the configuration. The user may choose to first set the rules to “deny” in order to monitor traffic that might still be using those rules, or may choose to simply drop the rules from the database.

Supported Firewall

Following is the list of supported firewalls:

System Requirements	Version
Cisco PIX	All
Cisco ASA	All
Netscreen	All
Cyberguard	All
Cyberguard-Knightstar	All

Minimum System Requirement

Following is the list pre-requisites for Firesec:

System Requirements	Minimum
Operating System	Microsoft Windows XP Professional, Microsoft Windows Server 2003, Microsoft Windows Server 2000, Microsoft Windows Vista.
Browser	Internet Explorer 6.0 or higher
Processor	1GHz or higher.
RAM	512MB
Disk space	150MB free disk space
Networking	Network connection to application
Back End Database	Microsoft SQL Server 2000 SP4, Microsoft SQL Server 2005, Microsoft SQL Server 2005 Express Edition, or MSDE 2000 SP4

Contact Us

Network Intelligence (India) Pvt. Ltd.
#204, Ecospace, Awadh Narayan Tiwari Road,
Andheri (East), Mumbai - 400069.
Maharashtra, India
Ph: +91-22-2839-2628
+91-22-4005-2628
Fax: +91-22-2837-5454

P.O. Box 122074, SAIF Zone, Sharjah, United Arab Emirates
Ph: +971 506925128

#17, Building 160, Block 326, Manama, P.O. Box 75298,
Kingdom of Bahrain.
Ph: +973 39593057