

Firesec™

Firewall Analysis Solution

The Challenge

Growing & Complex **FIREWALL RULE BASE**

Configuration **CHANGE MANAGEMENT** on **FIREWALLS**

COMPLIANCE To PCI DSS, ISO27001 & SOX

Background

“permit ip any any”

This surprisingly insecure rule was found configured on an internal firewall during one of our routine security audits for an enterprise customer. Investigation revealed that this rule had been in place for over 2 years to resolve some troubleshooting issues before a critical go-live event.

Even more surprisingly, these sorts of issues routinely crop up at the network security layer. The growing **complexity of networks**, increasing **pressure from regulators** and **business’ expectations** of faster turnaround on such changes results in firewall configurations getting **bloated and highly insecure**. Often changes get introduced **without proper documentation and authorization** – leading to headaches when it comes to security reviews and PCI DSS compliance. And of course, the network becomes as

Why Firesec™ ?

Here are some signs that tell you

whether you’ve got a problem or not:

Do you have a way to confirm that all your firewalls adhere to the stated firewall configuration standards?

Are you 100% sure that all changes to firewalls are made not only with all proper authorizations but also do not violate any of your configuration standards?

Are you fully compliant to PCI DSS requirement ?

Do you have a way to analyse the impact of firewall rule changes to the rest of your network?

Do you have the capability to visualize what your network really looks like and trace the accessibility from a system in one segment to another one?

Are your firewall configurations fully optimized – with little or no redundancy, no unused rules, and no unused objects?

Supported Firewalls



Firesec™

Benefits

The key benefits of Firesec® are:

In-built change management workflow. Administrators get a single interface from which to simulate rules (from an access control what-if scenario) as well as ensure policy compliance

Firewall risk levels in real-time. Configurations are pulled on a periodic basis and risk scores are shown against pre-defined and customizable policies that are aligned to PCI DSS, CIS Benchmarks, Cisco benchmarks, etc.

PCI DSS Compliance Workflow. Get complete compliance to PCI DSS Requirement for firewalls and routers

Support for multifarious devices. We support Cisco, Palo Alto, Fortinet, Juniper, Cyberguard, Checkpoint out of the box

Firewall optimization. Find out unused rules, unused objects, redundant and shadow rules, and rules which can be grouped for easier manageability

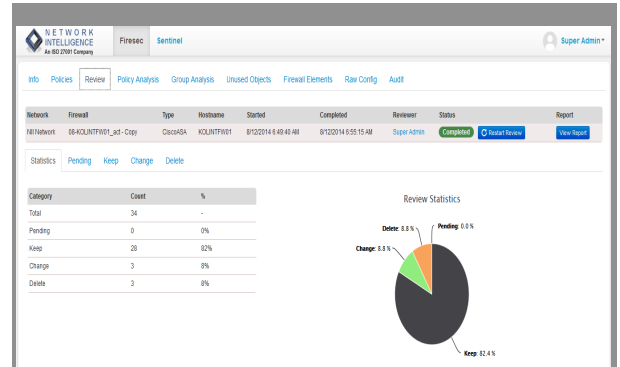
Configuration List. Interface to add, delete the config and to view the statics of the Firewall which shows number of shadow, redundant, groupable, disabled, insecure and unused objects.

Policies. Firesec allows comparison of Policies with the previous configuration added.

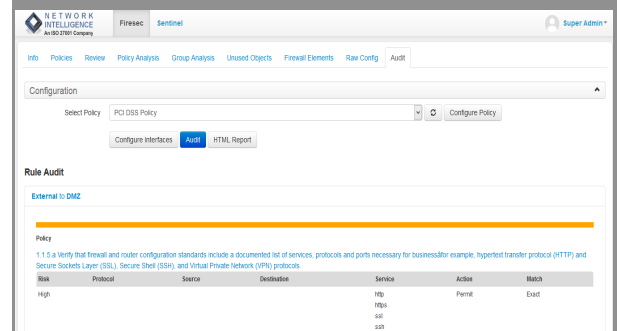
Policy Analysis. Firesec does rule base analysis and finds shadow rules, redundant rules, unused rules, insecured access rules, large subnets and critical ports.

Group Analysis. Firesec does group analysis and finds source grouping, destination grouping, service grouping and protocol grouping.

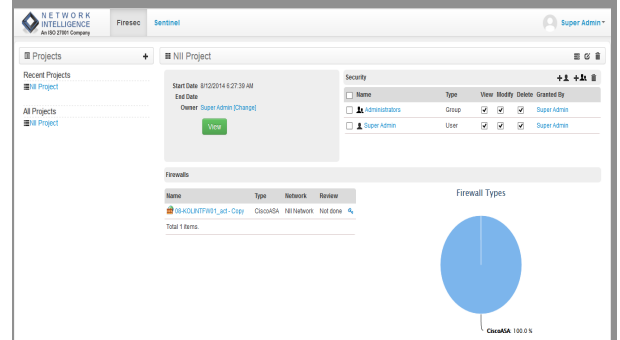
Firewall Elements. Firesec does firewall elements analysis and find Interface, access list, Object group, Network object, service object. Compare the firewall elements with respect to the previous configuration and highlights new, modified, removed firewall elements.



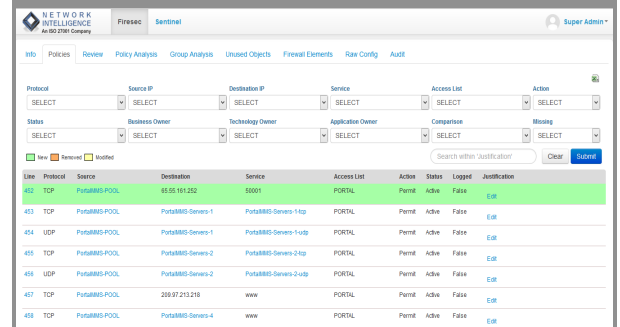
Review Statistics & Change Management Workflow



PCI DSS Policy Compliant



Support Multifarious Firewalls



Comparison of Policies

Firesec™

The Ultimate Firewall Analysis & Configuration Management Solution

Firesec is a comprehensive solution for firewall rule base analysis in medium to large enterprise environments. It addresses the problems inherent with large rule sets and helps purge and update a rule base as per network requirements. Firesec provides multiple functions such as removing redundant rules, grouping similar rules, and searching for vulnerable rule patterns.

Hardware requirements:

Hardware requirements:

- Server with 8 GB RAM,
- Dual Core processor,
- 500 GB HDD

Software requirements:

- Windows 2012 or later with IIS as the web server
- .NET Framework,
- MS SQL Database

Supported Firewall & Network Devices

- Cisco ASA, Cisco PIX, Juniper, JunOS, Fortinet, Palo Alto, Checkpoint, Cyberguard and Many more
- Cisco Routers, Cisco Switches, HP ProCurve Switches

Firesec™

About NETWORK INTELLIGENCE (I) PVT. LTD

Network Intelligence, incorporated in 2001, is a committed and well-recognized provider of services, solutions and products in the IT Governance, Risk Management, and Compliance space. Our professionals have made a mark for themselves with highly satisfied clients all across the globe supported by our offices in India and the Middle East. As an ISO 27001-certified company ourselves, we are strongly positioned to understand your needs and deliver the right answers to your security and compliance requirements. We have won accolades at numerous national and international forums and conferences. Our work truly speaks for itself and our clients are the strongest testimony to the quality of our services!

Testimonials

“NII has greatly assisted Batelco in its effort to structure its information security management framework. The NII consultants were true experts in their own domains and helped us align the processes and technology on the basis of ISO 27001. They customized their approach to suit Batelco’s requirements and executed the various phases of our Information Security Project in a timely and professional manner.”

Ahmed H.G. Ali - Manager, Information Security,

“We have been working with NII since 2005 to conduct audits and reviews of various aspects of Information Technology within the Bank. We consider them one of our key reference subject matter experts that we continue to rely on for the audit of our IT environment. They have gained respect of both ARR and IT in all the reviews”

Ibrahim Al-Gomllas

Lead Auditor, ARR, Samba

NETWORK INTELLIGENCE (I) PVT. LTD.

204, Old Nagardas Road,
Near Andheri Subway,
Andheri (E), Mumbai 400 069
India

Phone: ++91-22-2839-2628
Fax: +91-22-2837-5454
E-mail:
info@niiconsulting.com

NETWORK INTELLIGENCE (I) PVT. LTD.

Pratik Samant
(Head-MEA Operations)
P.O. Box 122074, SAIF Zone,
Sharjah, U.A.E.

Phone: +971-561-181-669
Fax: +91-22-2837-5454
E-mail:
pratik.samant@niiconsulting.com