# Firewall Operations & Security Management with FirePAC 5.0

**Product Datasheet**

***FirePAC 5.0 is a suite of integrated tools that use patented security analytics to deliver industry leading firewall risk and operations management capabilities.***

***The suite comprises of separately licensable components, each of which performs a distinct task to support the operations, audit or optimization of a firewall. The suite works off a common framework and is powered by an analytics engine that models firewall behavior to provide complete simulation of traffic flows through the device.***

## Multiple ways to connect to devices

FirePAC 5.0 comes fitted with interfaces to network configuration management systems like SolarWinds Orion NCM and also has direct connectivity to devices to access firewall configuration data. It can also work in a pure offline mode where configuration data is made available via the file system.

## Simple user interface

FirePAC 5.0 is a Windows application built using the Java programming language. The user interface is intuitive and requires little or no training before first use. Firewall configurations from different firewall brands are normalized for easy viewing and do not require users to be aware of the native formats. Multiple firewalls can be analyzed simultaneously.

## Firewall best practices at your fingertips

FirePAC 5.0 comes with a built-in catalog of security checks that is based on advisories collected from security agencies like the SANS Institute and NIST. These checks investigate whether a firewall has security risks caused by overly permissive rules and rules that allow dangerous services. You can create your own custom security check catalogs by configuring checks based on business and network policies specific to your own environment. The security checks in the catalog can be run any time to determine the security posture of the firewall and also scheduled on a continuous basis.

## Elaborate and actionable reports

FirePAC 5.0 reports are delivered in both PDF and Excel spreadsheet formats. They are elaborate, detailed and highly actionable. They pin-point failures and drill down into the causes of failure to identify the specific rules that are responsible. Reports provide information on firewall complexity, security audit failures, rule usage and optimization, compliance to standards, policy differences across configuration versions and traffic flows through a firewall.

## Affordable

FirePAC 5.0 components are individually licensable. This means that users buy only the features and capabilities they require and not the whole platform. Athena specializes in best-in-class point tools for firewall analysis, audit and operations and provides them on an integrated platform that ensures user investments are never obsolete.

**IT Managers**

- Monitor Policy Compliance
- Measure Operational Effectiveness

**Network Architecture Groups**

- Visualize Network Access Policy
- Validate Network Paths After Changes

**Firewall Engineers**

- Approve Changes
- Monitor Impact of Changes on Traffic

**Network Engineers**

- Determine Optimal Changes
- Troubleshoot Service Availability and Routing Issues

**Project Teams**

- Migrate Firewall Platforms

### Technical Specifications

- Requires a Windows 2000 (or later) operating system with Java Runtime 5.0 (or later).
- Uses Microsoft Internet Explorer 6.0 SP1 (or later) or Firefox 2.0 (or later) and PDF reader for reading HTML/PDF reports.
- Runs on any Intel Pentium-compatible 2 GHz or faster machine and requires 2GB of memory (RAM) and 5GB of temp disk space besides25MB for every firewall report.
- Supports firewalls Cisco PIX/ASA/FWSM, Juniper Netscreen and Check Point.

# Firewall Operations & Security Management with FirePAC 5.0

## PRIMARY FIREPAC TOOLS

### Rule/Object Cleanup

Rule and Object Cleanup analyzes the redundancy levels in the configuration of a firewall and provides cleanup and optimization information to ensure maximum security and manageability of the firewall. Rule usage information, when provided, allows unused rules to be removed and rule order to be changed for best performance.

### Security Audit

Security Audit provides the user an automated audit mechanism to evaluate firewalls for non-compliances. It runs the checks in the security check catalog automatically using firewall interface definitions set by the user and provides a report on those checks that did not pass. The security audit report is a detailed report that describes every failure and its reason down to the rule (ACL or NAT) that is responsible for it. This represents highly actionable information that can be addressed immediately by network staff. Security audits can be performed in a matter of minutes and do not require any manual intervention.

### PCI Report Card

The PCI Report covers all PCI-DSS control items that deal with the firewall and provides comprehensive information on failures, down to the rules that cause them.

### Rule Tracker

Rule Tracker is a secure rule documentation management system that ensures complete documentation coverage. Rules that require documentation updates are automatically identified when changes are made to the rule or when the rule is changed in position within the rule base. An easy spreadsheet interface allows a group of individuals to collaborate. Rule Tracker associates rule comments with the semantics of a rule and within the context of the overall firewall policy. When firewall policy or the semantics of a rule changes, the documentation of the affected rule is automatically invalidated and will be flagged for refresh.

### Change Advisor

Change Advisor automates the change process, taking advantage of Athena's core technology for understanding how packets would traverse the network, based on connectivity, routing and the firewall devices involved in the change request. When presented to the network engineer, this analysis result shows precisely where in the network the packet will travel, which devices along the path will need to be modified to allow the requested service, and even which rules in those devices need to be changed.

### Impact Monitor

Change Monitor has built in scheduling that allows firewall configurations to be collected directly from devices on a routine basis at a desired interval and to run a monitoring task on every change to a firewall configuration. It reports on rule changes, traffic flow variances and security audit failures caused by the rule changes and emails the reports to specified users.

### Firewall Migration

Firewall Migration provides policy equivalence matching across firewall device types to validate migration results. The identified policy differences can help migration teams to quickly address the problems and to fix and revalidate the new device policies until they converge with the old. Firewall Migration provides the basis for a systematic process to execute the migration and reduces the emphasis on testing. This allows migration projects to be in greater control and to execute to a defined timeline.

### Object Standardization

Object Standardization offers a process driven, systematic approach, assisted by automation, to unify and standardize object definitions and usage across an entire network. Its semantic engine recognizes unique names across any number of firewalls and understands semantic equivalences and differences in objects without relying on names. Using a user supplied naming standard and objects definitions, and guided by a user map between the new standard and the old names, regenerates rules for every firewall in the inventory using the new standardized names and automatically compensates for differences with the old objects.