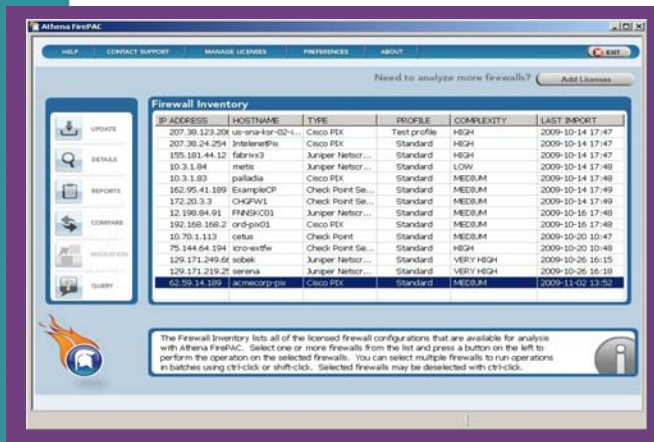


# Firewall Security Management

## Seriously Simplified by Athena Security

### FirePAC's Firewall Analysis

Athena FirePAC is a low cost, easy to use, offline security analytics tool for any Cisco, Check Point™ or Juniper Netscreen firewall. It comprehensively analyzes your firewall configurations using extensive checks for security risks to critical hosts, identifies problem rules in the configuration, determines redundant and unused rules/objects, and summarizes the services allowed by the rule base. Over 300 companies use Athena products to eliminate the vulnerabilities, non-compliances and errors in firewall infrastructure.



### Security Policy Checks

Athena FirePAC partitions the firewall interfaces into security zones and evaluates the traffic that is allowed between these zones. The analysis provided by FirePAC identifies risks to critical hosts based on overly permissive rules or rules allowing dangerous services. Users can define their own custom security zones and create new checks or customize existing checks to reflect unique business requirements. FirePAC restricts flagged ACL and NAT rules to only those that are applicable to the defined security check. It takes into account what networks are reachable from each interface in the firewall based on routing and anti-spoof settings to provide a more precise risk analysis. This ensures that users do not waste time looking at the rules that are not important. FirePAC understands different firewall brands and their unique handling of

data traffic. This makes it possible for any auditor to assess firewall security without having to understand the exact syntax of a particular firewall implementation.

### Rule Cleanup and Optimization

Athena FirePAC automates the cleanup and optimization of firewall configurations. Using FirePAC, administrators can isolate more rules for removal than any other solution. FirePAC performs a thorough analysis of the rule dependencies to identify every possible opportunity for removing rules that are covered by one or more preceding or succeeding rules. Whether your firewall has a few hundred or thousands of rules, FirePAC will reduce your maintenance burden by at least 10-30%. Using firewall logs and access list hit counts, Athena FirePAC also identifies most used rules and unused rules/objects, and identifies an optimized rule order that improves performance. Because FirePAC comprehensively understands how rule changes impact firewall behavior, following FirePAC's recommendations for cleanup and optimization will never disrupt critical business services.

### Object and Rule Search

Athena FirePAC lets users search and browse all objects in a vendor neutral tabular format by object name, address or service content. In a single search, users can view all references to the object including parent and child relationships. This makes clear how any change to an object would impact other objects in the firewall. FirePAC rule search allows users to cut through objects with multiple levels of membership hierarchies to pinpoint the services and addresses allowed or denied by a rule.

### Advanced Query

FirePAC's advanced query can be used to identify all the ACL, NAT, VPN and routing rules that act on any traffic that is of interest to the user. By specifying a single address, users can understand all access to a server from external and internal zones. Unlike other tools, issuing a separate query with the public address is not required.

## Policy Comparison

FirePAC shows change in traffic flow through the firewall resulting from changes to the firewall rules. It can be used to model the effect of a change before it is deployed to the network, or after, to verify that the rules implement a given security policy correctly. With FirePAC's compare feature, users can break out of the never ending cycle of test-repair-test. It takes any configuration revision and analyzes the behavioral differences against the original. With policy comparison users can:

- Determine what IP addresses might be at increased risk or what services are allowed by new versions of the configuration.
- Use it to make sure that the changes that were made produce the desired policy.
- Verify policy equivalence when rationalizing objects groups before migrating to Cisco CSM or Netscreen NSM.
- Isolate the rules that were responsible for the differences in the actual verses expected behavior.

FirePAC also provides support for migrating Cisco PIX/ASA/FWSM to Check Point configurations. Cisco and Check Point firewall have different device architectures and hence any migrations need to be performed carefully without leaving any gaps. FirePAC analyzes Cisco and migrated Check Point configurations, identifies all gaps, and suggests remedies to make the policies equivalent.

## NCM Integration to SolarWinds Orion

Using these products together, engineers have a comprehensive firewall change management solution that also detects how rule changes impact dataflow through the firewall.

## PCI DSS 1.2 Compliance

FirePAC identifies the specific rules that cause PCI control items to fail. The reachability analysis, based on routing and anti-spoof settings, is the only way to achieve a consistent and true assessment of firewall security.

## Technical Specifications

### Minimum Software:

- Windows 2000 Professional, Windows 2000 Server, Windows XP Professional SP2 (or later), Windows 2003 Server SP1 (or later)
- Java Runtime Environment (JRE) 5.0 and 6.0
- Microsoft Internet Explorer 6.0 SP1 (or later) or Firefox 2.0 (or later) or PDF reader for reading HTML/PDF reports

### Minimum hardware requirements:

- Intel Pentium-compatible 2 GHz or faster
- 1 GB memory (RAM) (2 GB RAM recommended).
- 1 GB of drive space (and 5GB of temp space, up to 25MB of disk space for each firewall reports).

### FirePAC provides full support for:

- Cisco PIX/ASA/FWSM firewalls
- Netscreen firewalls
- Check Point™ firewalls

[www.athenasecurity.net](http://www.athenasecurity.net)



Athena Security 1 East 22<sup>nd</sup> Street, Suite 107, Lombard, Illinois 60148  
tel (630) 629-0600 • fax (630) 629-2429