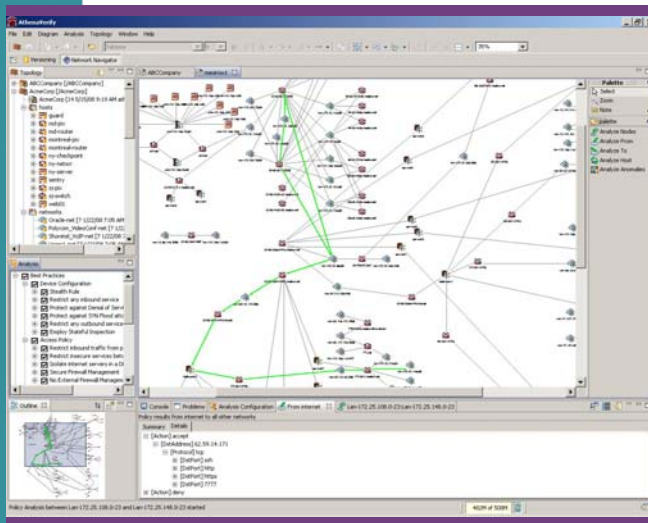


# Firewall Configuration Complexity

## *Seriously Simplified by Athena Security*

### Athena Security

Athena provides comprehensive analysis tools for managing and simplifying firewall configuration complexity. We make this possible by revealing the precise relationship between firewall rules and network services in a single device or across an entire network. Developed to address the operational needs of network engineers, Athena's products provide safe, offline analysis with the strength, attention to detail, scale and flexibility necessitated by companies of all sizes.



### Verify's Network Analysis

AthenaVerify provides a detailed/transparent view of packet flow through the network. At the core, is the ability to precisely evaluate network access paths between any pair of hosts in the network, or between a host and a remote network or the Internet. This evaluation is done off-line and does not involve any introduction of spurious packets into the network. Similarly, firewall ACL, NATting, and routing rules can be analyzed with respect to usage in enforcing policy and removing unneeded rules.

### Assess Network Policies

Using AthenaVerify, the network group can evaluate best practices and implement policies that result in improved security, commensurate with business needs. Risk is measured by the degree to which best practices are implemented in the network. As policies deviate, risk profile increases. This is an automatic quantification of policy compliance using an objective and repeatable framework for measurement.

### Manage Change Impact

AthenaVerify also provides features to support network architecture, configuration and policy change modeling/management. It takes into account the interdependencies of network devices and the policy access paths for all possible connections. It is the only commercially available solution that layers on top the ability to model the impact of a configuration change on best practices and regulatory compliance controls.

### Security for Network Operators

AthenaVerify addresses network security via tight network policies that reduce reliance on the application layer to enforce security. Athena does not utilize application vulnerability data that is typically associated with fulfilling patch management requirements. Rather, the network's security posture is specified by a set of best practices that cover good network architecture, device configuration, and network policy.

### The Key to Firewall Management

AthenaVerify predicts how any rule change will impact service availability when multiple configurations work together to form a complex network.

## AthenaVerify Key Capabilities

<b>Path-Based Policy Analysis</b>	Graphical display of access paths that traverse all security devices across the network
<b>Best Practices Evaluation</b>	Based on guidelines and recommendations from sources such as NSA, NIST, SANS, Neohapsis, ISACA, ITIL...
<b>Risk Scoring</b>	Evaluates deviation from Best Practices and calculates a risk score aggregated for all network nodes
<b>Compliance Scoring</b>	Explicit correlation of Best Practices to control elements in compliance frameworks and regulations
<b>Attack Simulation</b>	Analyze potential attack paths and exposures based on library of threat scenarios
<b>Configuration Change Modeling</b>	Models the effects of changes on security policy
<b>Role-Based Reporting</b>	Pre-defined business and technical reports tailored for executives, auditors and network operators
<b>Agent-less Analysis</b>	Completely offline simulation of network behavior
<b>Firewall Audit</b>	Integrated view of the effects of ACLs, routing and NATs on layer 3 and 4 devices across the network

### Benefits

- Includes all functionality of Athena FirePAC
- A quantifiable assessment of network exposures based on the configuration data embedded in infrastructure devices
- A holistic evaluation of network device configuration changes and the impact on business policy
- Support for networks containing heterogeneous multi-vendor devices



Athena Security 650 Warrenville Road, Suite 100, Lisle, Illinois 60532  
tel (630) 353-1900 • fax (630) 353-1901

## Technical Specifications

### Requirements

- 2.0 GHZ dual-core CPU
- 4 Gb RAM
- 500 Mb free disk space
- Windows 2000, XP, or Vista (Windows 2000 requires download of GDI+ graphics library)
- Java Runtime Environment (JRE) 5.0

### Firewalls

Provides support for analyzing stateful filtering rules, NAT configurations, anti-spoofing rules, implicit rules, IPSec VPN configurations.

- Cisco PIX firewall
- Cisco ASA firewall
- Juniper Netscreen firewall
- Checkpoint FireWall – 1 NGX
- Secure Platform firewall
- Nokia IPSO firewall
- Crossbeam firewall

### Routers and Switches

Provides support for filtering rules, NAT configurations, policy routing, IPSec VPN configurations.

- Cisco IOS
- Cisco Catalyst

### Device Access Method

Provides support for various communication protocols to retrieve device configurations.

- SSH2
- Telnet

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