

Network Security Compliance

The disparate nature of point products, each with its own unique function and interface, has become an obstacle to managing IT security controls and network access policies. The processes associated with understanding network security compliance is often labor-intensive and time-consuming due to the difficulty of mapping thousands of complex security controls to network access policies. These barriers often result in mis-configured network devices that increase network exposure and non-compliance.

Designed specifically for network operation and engineering teams, Skybox Assure's product line streamlines and simplifies network security compliance. Analyzing complex rules and conducting firewall audits takes only minutes, sporadic information is converted into actionable information, simplifies documentation of regulatory compliance (PCI, FISMA, etc.), while network access and connectivity are continuously analyzed.

By using Skybox Assure, network operations can move from an error-prone configuration management process to one that is disciplined, auditable and error-free. Each Skybox Assure product can be deployed individually or collectively to address a specific problem.

Key Features

- Automated configuration analysis
- Automated firewall compliance audit
- Rule usage analysis and optimization
- Network access policy compliance and reporting
- Network access analysis—discover policy violations and root cause
- Process automation—customizable to organization's workflow processes
- Consolidation—all data sources viewable from central source
- Configuration change assurance
- Access simulation and what-if analysis
- Regulatory compliance alignment and documentation (PCI, FISMA, etc.)

Benefits

- Visualize, understand, and predict access and policy exposures
- Audit network policies and firewalls in just minutes
- Shorten time to compliance
- Assure control effectiveness—prioritize changes based on business impact
- Analyze impact of proposed changes—reduce human and configuration error
- Make accurate and confident decisions
- Generate meaningful compliance measurements
- Lower operational cost through elimination of manual processes

Sample Usages of Skybox Assure

On-Demand and Automated Firewall Compliance Audit

•
Control Compliance Documentation

•
Network Access Policy Compliance

•
Discover Compliance Violations

•
Optimize Rule-base Through Rule Usage Analysis

•
Regulatory Compliance—PCI, FISMA, etc.

•
Framework Compliance—ISO 17799, COBIT

•
Change Validation Before Deployment

•
Predict Impact of Configuration Changes

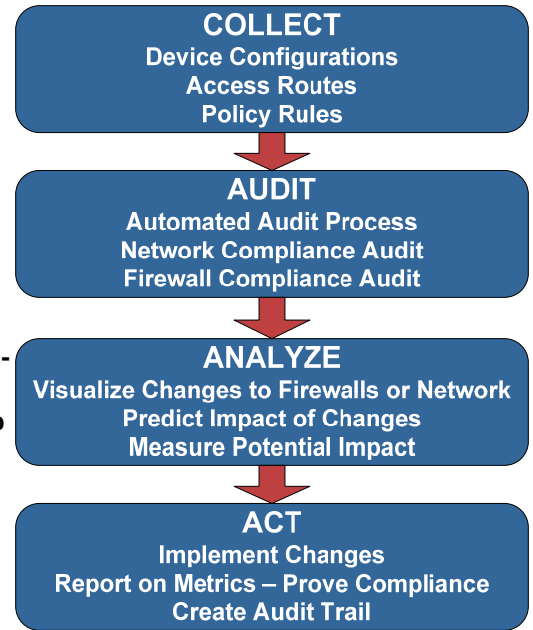
Why Should You Care?

- Maximize Existing Network and Firewall Investments Without Disruption of Live Environment
- Audit All Production Firewalls in Minutes
- Assure Control Effectiveness by Optimizing Complex Rules
- Quickly & Easily Demonstrate Compliance with Regulatory Requirements

Audit and Compliance Reporting

Skybox Assure offers an extensive package of reporting capabilities, including pre-defined and customizable reports. Reports are available for a broad range of audiences, including IT auditors, compliance officers, security professionals, operations teams and upper management. Report contents range from details about access routes and comparisons of rule-sets over time to high-level summaries suitable for evaluating policy compliance and resource allocation. Historical trending data is also available to help management measure the effectiveness of its team or to demonstrate compliance to the auditors.

Reports can be viewed online or exported to PDF, HTML or RTF.



Skybox Assure Product Line

Firewall Compliance Auditor	Network Compliance Auditor
On-demand firewall compliance audit	Network access policy management
What-if analysis: access policy—change prediction—access path analysis	Root cause analysis for policy violations
Rule usage analysis and optimization	Normalized network modeling and map visualization
Access policy compliance—customizable	Compliance metrics and reporting capabilities
Violation root cause analysis	Holistic network access simulation

Deployment Architecture

Skybox Secure is based upon a three-tiered architecture with a centralized server, one or more data collectors and two distinct management interfaces. It can be scaled to suit the complexity and size of any organization.

- **Server**—Merges all collected data and maintains an up-to-date model of the network environment.
- **Collector**—Deployed in various network segments, where it automatically discovers and collects vulnerability and network configuration data. The process is fully automated and centrally controlled.
- **Manager**—Provides a well-structured workspace for security teams where data from across the organization is analyzed, measured and acted upon.