

## Holistic View of Network Access and Policy Compliance

The numbers and variety of network devices used by organizations today make it extremely difficult and labor intensive to validate compliance with network access policies. An additional factor is the lack of a centralized and accurate definition for such policies. Network operations teams easily become overwhelmed by both the number and diversity of controls and policies due to complexity and resource dependence.

Skybox's Network Compliance Auditor automates the process of collecting network and security devices configurations and validating them against network policies in a non-intrusive way. In addition, it discovers policy violations, displays root cause, and calculates compliance status. Compliance calculations may take place multiple times in a single day, or ad hoc as network or security device configurations change. Automated weekly or monthly compliance reports may be delivered to the network administrator's mailbox.

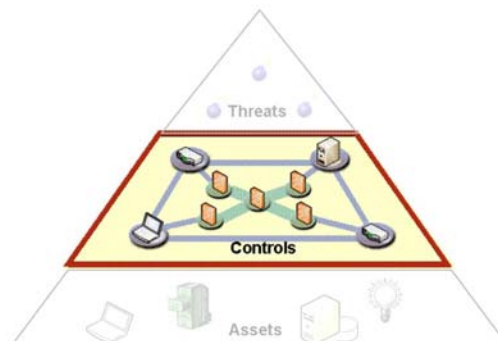
## Business Problem

- Lack of centralized, well-maintained definition of network access policies
- Complex network with a high rate of change
- Multi-vendor firewalls and routers each with unique management interfaces
- Infrequent compliance monitoring and reports due to time-consuming processes
- Inability to understand access permissions/routes from all points on network
- Difficult to map complex access rules to policies
- Root cause of access violations are impossible to determine
- Unidentifiable network security and availability exposures

## Value Proposition

The Network Compliance Auditor helps organizations quickly discover the root cause of access policy violations while simultaneously reducing the resources required for network policy compliance. The ability to document and maintain network access policies is simplified, while up-to-the-minute network mapping helps management visualize the entire network from a centralized point.

When combined with Skybox Security's Firewall Compliance Auditor, the Network Compliance Auditor provides CIOs and network operations teams a completely proactive network and firewall compliance assurance solution.



## Why Skybox Security?

*"One version of the truth."*  
- Reuters

*"Risk exposure window is reduced by 95%."*  
- USAID

*"Allows us to carry out a measurable, repeatable, and predictable risk assessment and mitigation planning process."*  
- EGG Bank

*"By visualizing threats quickly and efficiently, we realized a full ROI in a year and a 300% ROI in three years."*  
- Credit Suisse

*"We now have more answers than questions."*  
- Barclays Capital

*"Once you have it, you realize you can't live without it."*  
- Standard Chartered Bank

*"Skybox could completely change the vulnerability assessment landscape and become the dominant vendor in the world."*  
- Forrester

## Why Should You Care?

- Rapidly discover root cause of access policy violations
- Reduce resources required for network policy compliance
- Document and maintain network access policies
- Provide up-to-date network mapping and visualization

# Network Compliance Auditor

## Key Features

- Normalized network modeling and visualization
- Support for most major network devices and firewall types: Check Point, Cisco, ISS, Juniper, Nortel, Symantec
- Network and Firewall Configuration Management: AlterPoint, Check Point Provider-1, Cisco Works, HP NAS, Juniper NSM
- Holistic network access simulation
- Network access policy management
- Out-of-the-box best practice policy
- Customizable access policy (security and availability)
- Root cause analysis for access violations
- Compliance metrics and reporting

## Benefits

- Central repository of network policies and compliance status
- Audit network access policies in minutes—not days/weeks
- Ensure balance with network security and availability requirements
- Significant time and labor reduction
- When combined with Skybox Firewall Compliance Auditor, provides comprehensive network security compliance support

## How It Works

Implementation of Skybox Security's Network Compliance Auditor is a five step process that will ultimately optimize the visibility and productivity of existing security layers.

**Step 1: Normalized Network Model**—Device configurations are imported into the system from NCCM, file repositories, or directly from the device; access control rules and interfaces are normalized using ACL, NAT and routing tables; networks and devices are mapped into zones to simplify the interface.

**Step 2: Access Policy**—An out-of-the-box best practice policy bundle is provided; rules and policy are customized to the corporate policy; source and destination is specified by zones allowing for scalable policy management.

**Step 3: Policy Compliance Analysis**—Policy compliance analysis is automated using Skybox's access simulation technology; reports automatically provide metrics with the current status of compliance percentage; a drill down of the violations that impede compliance is generated; root cause of violations and their details is obtained; information on how rules match with access is generated.

**Step 4: Interactive Access Analyzer**—An interactive model is used to analyze the access paths, creating a "virtual trace route"; trouble-shooting capability allows the user to assess network security and availability problems.

**Step 5: Report Generation**—Reports are generated and presented in either custom or template form as either a PDF, HTML, or RTF file; the scope and details of each report is completely customizable to your needs; reports can be generated on an ad hoc basis or continuously through regularly scheduled intervals delivered via email.

