



Skybox® Firewall Assurance

PCI Compliance, Change Assurance, Ruleset Optimization

Skybox Firewall Assurance allows IT operations or security managers to quickly assess their firewall compliance status in a fraction of the time of manual audits, reducing firewall maintenance and compliance costs. Customers can visualize and pinpoint potential risk exposures that need immediate attention, including conflicting firewall rules and misconfigurations, and track historical changes in access rules and objects.

Using Firewall Assurance, IT teams can also validate planned network changes to avoid human error and the misconfigurations that could result in security or compliance exposures.

Visibility

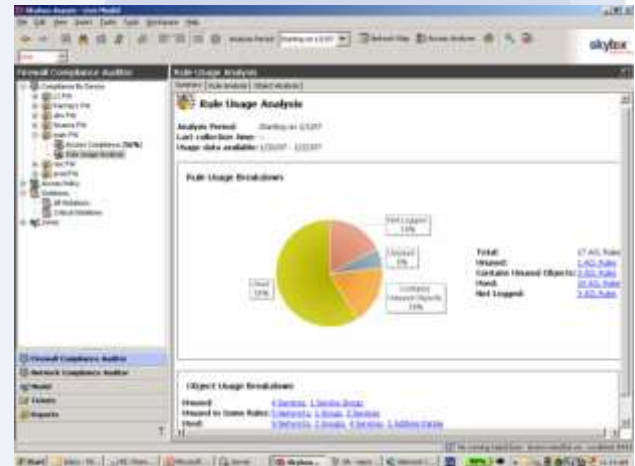
Firewall Assurance collects information from multiple firewalls, normalizes the data, and analyzes compliance with industry best practices or custom-tailored policies. A visual map of the firewall topology is generated. Redundant, shadowed, and obsolete rules can quickly be found and remediated to optimize and simplify firewall rulesets.

On-demand Audits

Audit reports and compliance scorecards are instantly available and can be provided to compliance auditors and management to document compliance status. These provide tangible evidence of firewall compliance with security policies and regulations. Firewall Assurance reports are designed to support PCI DSS v1.2 and other compliance requirements.

Change Assurance

Firewall Assurance helps organizations validate firewall changes in advance, finding access issues and other potential problems before they impact the network. In addition, change tracking capabilities maintain a history of firewall rule modifications. Additional workflow capabilities are provided through the optional Change Manager module, or by using the Skybox API for custom integration with 3rd party change tools. A web service application enables access and policy analysis integration with external workflow applications. Using these capabilities, systems can avoid downtime and potential availability issues that would normally result from human or configuration errors.



Rule ID	Name	Action	Status	Source	Target	Priority	Created	Modified
1	Deny All	Deny	Active	*	*	1	2008-01-01	2008-01-01
2	Allow HTTP	Allow	Active	192.168.1.0/24	192.168.1.0/24	2	2008-01-01	2008-01-01
3	Deny All	Deny	Active	*	*	3	2008-01-01	2008-01-01
4	Allow HTTPS	Allow	Active	192.168.1.0/24	192.168.1.0/24	4	2008-01-01	2008-01-01
5	Deny All	Deny	Active	*	*	5	2008-01-01	2008-01-01
6	Allow SSH	Allow	Active	192.168.1.0/24	192.168.1.0/24	6	2008-01-01	2008-01-01
7	Deny All	Deny	Active	*	*	7	2008-01-01	2008-01-01
8	Allow Telnet	Allow	Active	192.168.1.0/24	192.168.1.0/24	8	2008-01-01	2008-01-01
9	Deny All	Deny	Active	*	*	9	2008-01-01	2008-01-01
10	Allow FTP	Allow	Active	192.168.1.0/24	192.168.1.0/24	10	2008-01-01	2008-01-01
11	Deny All	Deny	Active	*	*	11	2008-01-01	2008-01-01
12	Allow SMTP	Allow	Active	192.168.1.0/24	192.168.1.0/24	12	2008-01-01	2008-01-01
13	Deny All	Deny	Active	*	*	13	2008-01-01	2008-01-01
14	Allow POP3	Allow	Active	192.168.1.0/24	192.168.1.0/24	14	2008-01-01	2008-01-01
15	Deny All	Deny	Active	*	*	15	2008-01-01	2008-01-01
16	Allow IMAP	Allow	Active	192.168.1.0/24	192.168.1.0/24	16	2008-01-01	2008-01-01
17	Deny All	Deny	Active	*	*	17	2008-01-01	2008-01-01
18	Allow DNS	Allow	Active	192.168.1.0/24	192.168.1.0/24	18	2008-01-01	2008-01-01
19	Deny All	Deny	Active	*	*	19	2008-01-01	2008-01-01
20	Allow NTP	Allow	Active	192.168.1.0/24	192.168.1.0/24	20	2008-01-01	2008-01-01



Key Features

- Broadest support for all firewall vendors, including Check Point, Cisco, Fortinet, Juniper, McAfee, Symantec and others
- Out-of-the-box best practice policies based on PCI DSS and NIST standards
- Change tracking shows historical changes made to access rules and objects
- Side-by-side comparison of past, present, and future firewall configurations
- Firewall access path analysis
- Rule usage analysis and optimization
- Customizable access policy: violation discovery, root cause analysis and management
- Automated access compliance analysis
- What-if analysis to virtually check planned firewall changes
- Rule compliance – run checks on rules (any, disabled, risk port, etc.) and view by firewall level or policy level
- Audit reports and compliance metrics
- Optional Change Manager module adds full workflow capabilities for firewall change control

Supported Operating Systems

Windows 7, Windows Server 2008, Windows Server 2003 (32/64 bit)
 XP Professional SP2 or higher, Vista
 Red Hat Enterprise Linux v.4 (32/64 bit), v.5 (64 bit)
 CentOS

Minimum Hardware Requirements*

Memory: 4GB RAM
 CPU: 2.8 GHz
 Storage: 20GB

Supported Devices—Network Devices

Check Point VPN-1, Firewall-1 and Provider-1
 Fortinet Fortigate 2.x, 3.x
 Nokia Appliances running Check Point FW-1/VPN-1
 McAfee Firewall Enterprise (Sidewinder) G2, V.6
 Cisco routers running Cisco IOS 11.x, 12.x; Cisco PIX, ASA, FWSM
 Juniper Netscreen, SSG, ISG running ScreenOS 4.x, 5.x, 6.x, and
 Network and Security Manager (NSM)
 Symantec SGS

Supported Devices—Management Systems

Cisco Works

* = Request additional information based on your specific needs.



Skybox Advantages

- Easily track historical changes to rules and objects
- Maintain and demonstrate firewall compliance easily
- Find and remediate potential security issues quickly
- Optimize firewall rulesets and reduce configuration errors
- Drastically reduce the amount of time required for firewall management

