Skybox Firewall Assurance

Product Tour

8.0.600

Revision 11
About Skybox Security, Inc.

Skybox gives security management and operations the tools they need to eliminate attack vectors and safeguard business data and services every day. With unparalleled visibility and context-aware intelligence of the attack surface, Skybox solutions drive effective vulnerability and threat management, firewall management and continuous compliance monitoring.

Established in 2002, Skybox is a privately held company with worldwide sales and support teams serving an international customer base of Global 2000 enterprises and government agencies.

Contact information

Contact Skybox using the form on our website or by emailing info@skyboxsecurity.com.

Customers and partners can contact Skybox technical support via the Skybox support portal.
Skybox Firewall Assurance Product Tour

Redundant Rules.........................................................................................26

Optimization and Cleanup: Rule Usage.........................................................27
  Unused Rules............................................................................................28
  Rule Usage ...........................................................................................29
  Critical Rule Information.........................................................................30

Zone to Zone Access Policy Compliance ...................................................31
  Access Policies: Violating Rules...............................................................32

Reports.....................................................................................................34
  Reports: Output ....................................................................................35

Change Tracking.......................................................................................37
  Viewing Changes ...................................................................................38
  All Changes..........................................................................................39
  Side-by-Side Changes............................................................................40

Product Tour Conclusion..........................................................................41
Chapter 1

Overview

This chapter provides a short overview of Skybox® and Skybox Firewall Assurance.

Summary of Skybox Security Suite

The Skybox Security Suite is a proven, award–winning security management platform with an attack surface visualization layer and a portfolio of 5 security analytics modules for vulnerability and threat management and security policy management. The Suite gives operational teams continuous visibility of the attack surface, enabling them to eliminate attack vectors and respond to security threats and incidents in minutes.

The foundation of the Skybox platform provides an integrated process for data collection, modeling, simulation and reporting on an enterprise scale for holistic insight to IT security and operations.

The remainder of this document focuses exclusively on the Network Security Management portion of the Skybox solution.
Skybox Architecture: Modeling and Simulation Technology

The basis of the Skybox architecture is the model, which can be viewed in Skybox as a network map. This model is made up of Layer 3 devices (firewalls, routers, load balancers, and IPSs) and is useful for a variety of functions. The data for the model consists of device configuration data, and routing tables containing static and dynamic routes. This data is collected in a variety of ways, depending on the device. Data can be collected from the device directly using protocols like SSH, or it can be collected from a specific vendor management platform like Cisco’s CSM, or even from 3rd-party configuration managers like HPE Network Automation.

The data is collected in an automated, continuous fashion using a scheduled-task-based system. The frequency of collection can be anything from once a year down to syslog event-triggered real-time collection. We find that most organizations are happy with once a day collection.

Skybox provides its analysis using several related models—Live, What If, and Forensics—and several different workspaces. The models and workspaces enable users to run analysis over time, providing access path troubleshooting, compliance with policy, change verification, and reconciliation of all network security devices. In this product tour, you use a demo model that already exists within the product and consists of several preloaded firewalls and other network devices.
Introduction to Network Security Management

Continuous validation that your network and systems are correctly and securely configured is necessary to ensure uptime and maintain compliance. Automated analysis and secure change management processes provide a strong foundation to:

- **Increase security and availability**: Identify and close security gaps such as configuration errors to reduce risk and avoid downtime
- **Increase productivity, reduce management costs**: Automate firewall and device change management to reduce management time and focus scarce resources on key initiatives
- **Gain visibility and control**: Enhance visibility and oversight of your firewall and network device management processes
- **Show compliance**: Validate and document that security controls and change processes comply with corporate, industry, and government regulations

![Diagram showing model network, analyze firewalls, monitor compliance, manage rule life cycle]

Security Policy Management Products

**Skybox Firewall Assurance**

Skybox Firewall Assurance completely automates firewall management tasks across different firewall vendors and complex rulesets. It readies your network for action by continuously verifying that firewalls are clean, optimized and working effectively. Firewall Assurance extends beyond firewall rule checks, analyzing possible traffic between network zones to find hidden risk factors, flagging unauthorized changes, and finding vulnerabilities on firewalls.
Identify security policy violations and platform vulnerabilities to reduce your attack surface
Visualize how network traffic can flow through your firewalls to troubleshoot access issues
Clean and optimize firewall rulesets to maintain top firewall performance
Manage traditional, next-generation, virtual, and cloud-based firewalls with a single consistent and efficient process

Skybox Network Assurance
Skybox Network Assurance provides total network visibility in the context of your network devices and security controls, showing how they work together — or leave you exposed. With Network Assurance, you can find potential attack vectors, check correct implementation of security zone policies or troubleshoot the root causes of network outages.

Visualize and understand your network and interactions of network devices and controls
Analyze network path between any source and destination — including the cloud — to uncover access issues and attack vectors
Stay secure and compliant by checking security zones, routers and switches for security violations
Troubleshoot in a virtual model to avoid disrupting network services

Skybox Change Manager
Skybox Change Manager ends risky changes with network-aware planning and risk assessment that keep your network secure and in continuous compliance with policies. Change Manager incorporates customizable workflows and provides comprehensive management of rule lifecycles to automate change processes.

Evaluate proposed firewall changes for compliance violations and exposed vulnerabilities
Accurately identify firewalls that need to be changed using complete network context
Translate change requests to a detailed plan for quick, error-free implementation
Automate and optimize rule lifecycle management
Customize workflows to match organizational needs
Verify that changes were completed as intended

Note: Skybox Change Manager is beyond the scope of this guide.
Chapter 2

Launching Firewall Assurance

This section explains how to launch Firewall Assurance.

Skybox Start Menu

1. Install the software. Refer to the Installation Guide for step-by-step instructions on how to install Skybox.

2. Choose **Skybox** from the **Skybox Start** menu.
Skybox Login Screen

Log in with the following credentials:
- User: skyboxview
- Password: skyboxview

Note: If this is your 1st time logging in to Skybox, it might take several minutes to start. In the lower left you see Connecting to server until the server starts.

License Management

At this point, you must add your Skybox license.
- Click Manage License.
Adding the License File

Click **Update License** and navigate to the location where you saved the license file. The file is named `license.xml`.
Chapter 3

Welcome Page

The Welcome Page is displayed when you open Firewall Assurance. It provides the following useful links:

- **Load demo model**: Loads the preconfigured network model that ships with the software, which you use during this product tour
- **Add new firewalls**: Enables you to add new firewalls. When using the trial version, you can add up to 5 of your own firewalls
- **Open Change Manager**: Opens Skybox Change Manager in your default browser
- **Getting Started Guide**: Opens the Getting Started Guide, which provides a more in-depth look into Firewall Assurance. After going through this trial guide, consult the Getting Started Guide to learn more
- **On-line help**: Opens the on-line help for all Skybox products

To load the demo model you will use during this product tour

▷ Click **Load demo model**.
Chapter 4

Firewall Assurance: Dashboard Summary Page

Once the demo model is loaded, the All Firewalls summary page is displayed in the workspace. This is the main page for Skybox Firewall Assurance where you can see summaries of the various types of information that Skybox has about your firewalls.

You are going to look at the 3 major use cases of Firewall Assurance: policy compliance, optimization and cleanup, and change management. The 1st steps are policy analysis and compliance, and optimization and cleanup of firewall rulesets. Once the network is in compliance, Skybox helps keep it there by utilizing Firewall Assurance’s change tracking functionality and Change Manager.
Chapter 5

Firewall Assurance Topology Map

Firewall Assurance models each firewall so that you can visualize your entire firewall topology.

1. In the tree on the left, select **dev FW**.
2. Click **Firewall Map** on the toolbar.
Chapter 6

Firewall Map: Mark as Zone

A zone is a way of grouping network interfaces that have the same trust level, such as DMZ, External, or Internal. You can work within the map to mark interfaces as zones, or view and easily make changes to their properties.

1. Right-click an interface and select **Mark as Zone**.
2. Look at the zones available in the Zone Type field without selecting any.
3. Click **Cancel**.
4. Close the map.
Skybox Firewall Assurance provides 3 types of policy compliance: Configuration Compliance, Access Compliance, and Rule Compliance.

Configuration Compliance defines how well a device is in compliance with best practice standards, which are based on CIS benchmarks and NIST standards.

- In the tree on the left, select **Configuration Policies > Standard v7 > 1.4 Cisco FW Standard Policy**.

In the workspace, you see the out-of-the-box Configuration Checks that Skybox provides to analyze each Cisco firewall configuration in the modeled network. The Configuration Checks are based on NIST standards.

Skybox includes checks for many different firewall vendors: including Juniper NetScreen and Junos, Cisco, Palo Alto Networks, and Check Point. Additional checks can easily be added and are fully customizable.
1. In the table, highlight **1.4.69 SNMP "public" community string – prohibited**. Right-click it and select **Properties**.

Here you see the details of this SNMP Configuration Check and that it consists of a regular expression that checks whether the string is found. In this Configuration Check, if the specified string is found, it is a violation of the policy. In other Configuration Checks, such as those that end in **– required**, if the string is not found it is a violation of the policy.

2. Close the Properties dialog box.
Analyzed Firewalls

In the workspace, click **1.4.69 SNMP "public" community string – prohibited**, and then click the **Analyzed Firewalls** tab.

This tab gives you information about how you’re doing on the specific policy. You can see which firewalls are analyzed by this configuration check. This goes according to which firewalls match the policy: in this case, Cisco firewalls.
In the tree on the left, click **Configuration Policies** to view the high-level dashboard screen.
Chapter 8

Rule Compliance

Skybox analyzes Rule Compliance—checking firewall access rules against a set of best practice guidelines (a Rule Policy). Included with Skybox is a predefined Rule Policy with which firewall access rules must comply. Skybox checks the access rules of each firewall for compliance with the Rule Policy and shows which access rules violate the policy. Rule Compliance analysis provides a starting point for understanding how much protection is offered by a firewall’s access rules.

> In the tree, select **Rule Policies > Standard v2 > Any in Two Fields**.

This rule checks for overly permissive rules with the value “Any” in at least 2 fields. You can see that 13 firewalls failed this check, meaning that 13 firewalls in the model have access rules that have the value “Any” in at least 2 fields. The **Analyzed Firewalls** tab shows which firewalls and which rules.
Chapter 9

Optimization and Cleanup: Shadowed and Redundant Rules

Shadowing and redundancy is based on a logical analysis of the firewall’s ACL to find access rules that can never be reached or that can be removed without changing the behavior of the firewall. Knowing how to correctly remove or change these rules enables you to optimize the firewall ruleset and enables easier compliance with standards.

1. In the tree, click **All Firewalls**.

2. The **Summary** tab is a dashboard view displaying results for all firewalls. In this tab, under **Optimization and Cleanup**, click **Firewalls by Shadowed/Redundant Rules**.
Shadowed Rules

In the main_FW row, the 4 in the Shadowed Rules column means that 4 rules are shadowed in this firewall. Click this link to see a list of the shadowed rules.

Details of Shadowed Rules

In the workspace, you see the 4 shadowed firewall rules in the top pane. When you select a shadowed rule, the bottom pane lists the selected rule underneath the rule which shadows (covers) it.

Click Explain.
Explanation of Shadowing

Note: Close the warning dialog box that appears.

In the **Causes Shadowing** box, click the arrows to expand the source, destination, and service.

Here you can see an explanation of how Rule 13 is shadowed by Rule 4. They have the same source, but the destination and service of Rule 13 are a subset of those in Rule 4—any traffic that would be stopped by Rule 13 has already been stopped by Rule 4; Rule 13 is not necessary.
Chapter 10

ACL Editor

→ Right-click the selected shadowed rule in the bottom pane and select **Open in ACL Editor**.
Viewing in the ACL Editor

The Access Control List Editor shows the details of the firewall’s access rules.

1. Double-click rule 13 to see its details.
2. When you are finished, click **Cancel** to close the rule’s properties, and then close the ACL Editor.
Chapter 11

Redundant Rules

You can view redundant rules in the same manner that you view shadowed rules.

- Click the **Redundant Rules** tab in the workspace.
Chapter 12

Optimization and Cleanup: Rule Usage

In Skybox Firewall Assurance, you can use a process named *rule usage analysis* to streamline the optimization of access rules and to help you identify unused rules and objects.

1. In the tree, select **All Firewalls > main_FW**.
2. In the workspace, click **Unused Rules**.
Unused Rules

The **Rule Usage** tab (currently displayed) contains usage information about the access rules that make up this firewall. The **Object Usage** tab contains usage information about the firewall objects used in the firewall's access rules.

Expand each usage type in the workspace to see the details.

- **Unused**: Rules that had no hits or object hits.
- **Used**: Rules that had hits and all objects referenced in the rule had hits.
- **Unused Objects**: Rules that had hits, but some objects referenced in the rule had no hits.
- **Unloggable**: Rules that cannot be logged. These are implicit rules and rules entered manually in Skybox.
- **Not Logged**: Rules for which logging is disabled on the firewall.

The value in the **Hit Count** column of the unused rule is **0**. Rules in the **Used** and **Contains Unused Objects** groups have hit counts greater than **0**.
Chapter 12  Optimization and Cleanup: Rule Usage

Rule Usage

You see that there are 2 rules that have a (Critical) icon in the Actual Rule Usage column, and that the actual rule usage for these rules is 0.01%. The Actual Rule Usage column shows the lowest usage level of the Source, Destination, and Service fields.
Critical Rule Information

Select the 1st Critical rule.

In the bottom pane, you can see the actual usage for the access rule, split according to its dimensions (source, destination, and service). By investigating the details of rules that are overly permissive you can identify addresses or ports that are truly needed, and consider changing the rule to reflect this. For example, you can see that only 3 services were actually used, even though the value of the Services field in this access rule is Any.
Chapter 13

Zone to Zone Access Policy Compliance

Zone to zone Access Policies help administrators describe common security policies such as “Never permit the DMZ to send Telnet data to any of the servers in my data center”. For a large, wide-spread network this can be very complex. To validate a single policy, it might be necessary to perform a large number of access checks to fully vet adherence to the policy.

Skybox starts by defining different zones mapped to the PCI DSS and NIST policies; several zones are associated with each, including external, internal, and DMZ. The policies themselves describe what kind of traffic is permitted between any 2 zones.

▶ In the tree, select **Access Policies > Public Access Policies > NIST 800-41 Policy > NIST Internal Access > NIST- Internal to DMZ > Block Login Services.**

In the workspace, you can see what kind of traffic is or is not permitted between the Internal and DMZ zones. When these policies are applied to your model, Administrators can see specific violations of these policies in your organization.
Access Policies: Violating Rules

1. With **Block Login Services** still selected in the tree, click the **Violations** tab at the top of the workspace.

2. In the bottom set of tabs, click the **Violating Rules** tab.
   
   You see a rule on main_FW that is causing violations of this policy.

Compliance information is captured in several dashboards at each level of the tree. In each dashboard you can see the percentage of compliance, and the violating rules and severity.

▶ In the tree, select **Public Access Policies**.
You can access the summary screens and the dashboard summaries in report format.
Skybox reports can be generated in several different formats including PDF, HTML, and CSV.

1. On the bottom left hand side click the Reports icon ( ).
   Note: If your screen is big enough, the icon is part of the list under Firewall Assurance and Network Assurance.

2. In the tree, select Firewall Compliance > Firewall Access Compliance.

3. Click Generate.

4. Select the Generate in the foreground option and click OK.
Reports: Output

Firewall Access Compliance

The Firewall Compliance report presents detailed information about firewall-level Access Policy compliance.

The report provides compliance metrics for the selected firewalls and detailed information on all violating access rules and violations found for each firewall in the scope.

The report helps you understand the compliance status of your policy as applied to each of the specified firewalls, and identify problematic access configuration in your firewalls.

1 Summary
2 Firewall: main_FW
   2.1 Violating Access Rules for firewall main_FW
3 Firewall: dev FW
4 Firewall: PA 2020/vsys1
   4.1 Violating Access Rules for firewall PA-2020/vsys1
5 Firewall: vCloudRoster_10.6.0.16
6 Firewall: PA 2020/vsys2
7 Firewall: finance FW
8 Firewall: L2 FW
9 Firewall: noc FW
10 Firewall: NSX edge 5.0
11 Firewall: Partner1 FW
12 Firewall: US_ECE01
   12.1 Violating Access Rules for firewall US_ECE01
13 Firewall: US_ECE02
   13.1 Violating Access Rules for firewall US_ECE02
14 Firewall: vlab-cisco
   14.1 Violating Access Rules for firewall vlab-cisco
15 Firewall: prod FW
   15.1 Violating Access Rules for firewall prod FW
16 Report Properties

Generated by Skybox | 11/15/18
Scroll through the PDF report that was generated. Contained in this report is summary information, and detailed information for the firewalls and the rules violated. These reports can be generated and emailed to multiple recipients using Skybox tasks.
Chapter 15

Change Tracking

The change tracking feature analyzes changes that occur in firewall access rules and objects, including the user who made each change, and the timestamp. By selecting a specific tracking period, you can view all changes in the access rules and firewall objects that occurred during this time period.

1. Underneath the tree, switch back to Firewall Assurance.
2. In the tree, right-click All Firewalls, and select Change Tracking > Change Tracking Period.
3. In the dialog box that appears, select All Available from the drop-down list; click OK. This sets the GUI to show all firewall changes.
4. Click Yes in the popup that says “This change will affect all firewalls in the model. Do you want to continue?”
Viewing Changes

By tracking observed changes on firewalls, Skybox adds risk awareness to the change management process. As firewall configurations are retrieved, they are compared with the previous configuration, and changes are pulled out and delineated.

1. In the tree, select **All Firewalls**, and click the Summary Tab at the top of the workspace.
2. Look at Change Tracking at the bottom of the workspace.
3. You can see the number of total changes. To view all changes click the link.
Look at the **All Changes** tab (which is open).

You can see a list of rules that were added, changed, or deleted. In the bottom pane, you can see information about the selected change. The **Change Summary** tab (open) shows metadata about the change. In a real model, you can see who made each change; in the demo model, the **Changed by** field is empty.
Side-by-Side Changes

1. Click the 1st entry in the table whose change type is **Changed**
   
   Note: If there are changed objects (in addition to changed rules), they are easier to see; click the 1st object whose change type is **Changed**.

2. In the bottom pane, click **Change Details**.
   You can see the before and after details of this recent change to the firewall.
Chapter 16

Product Tour Conclusion

This concludes the product tour guide for Firewall Assurance. To view a more detailed demo or to request a guided demo, contact your local sales team or send an email to info@skyboxsecurity.com