Contents

Intended audience ........................................................................................................... 6
How this manual is organized .......................................................................................... 6
Related documentation .................................................................................................... 6
Technical support ............................................................................................................ 7

Overview of Skybox Firewall Assurance ...................................................................... 8
Skybox platform ............................................................................................................... 8
Highlights of Skybox Firewall Assurance ....................................................................... 10
Basic architecture .......................................................................................................... 11

Data collection ................................................................................................................ 12
Quick reference for data collection ................................................................................. 12
Using the wizard for online import .................................................................................. 14
Using the wizard for import from the file system ............................................................. 15
Viewing and validating imported firewalls ..................................................................... 16
Working with tasks .......................................................................................................... 18
Using the Operational Console ....................................................................................... 18
Using tasks for data collection ....................................................................................... 19

Policy compliance ......................................................................................................... 21
Rule Compliance .............................................................................................................. 21
Rule Compliance overview .............................................................................................. 22
Viewing Rule Compliance ................................................................................................. 22
Viewing the violating firewalls for a Rule Check .............................................................. 23
Customizing a Rule Policy ................................................................................................. 24
Exceptions ....................................................................................................................... 28

Access Compliance ...................................................................................................... 30
Workflow for Access Compliance ..................................................................................... 31
Classifying the network interfaces into zones ................................................................. 32
Structure of the Access Policy tree .................................................................................... 34
Access Compliance and violation management ............................................................... 39
PCI DSS support in Skybox Firewall Assurance .............................................................. 46
Customizing an Access Policy ......................................................................................... 47

Configuration Compliance ............................................................................................ 56
Configuration Compliance overview ................................................................................ 57
Viewing Configuration Compliance per firewall ............................................................. 58
Viewing the analyzed firewalls for a Configuration Check ............................................... 58
Viewing violations in the configuration file ....................................................................... 59
Customizing a Configuration Policy ................................................................................ 61
Detecting vulnerability occurrences on network devices ................................................. 69
Optimization and cleanup ................................................................. 71
  Shadowing and redundancy analysis ............................................... 71
  Setting up shadowing and redundancy ......................................... 72
  Working with shadowed and redundant rules ................................ 72
Rule usage analysis ........................................................................... 75
  Rule usage analysis in Skybox ...................................................... 76
  Setting up rule usage analysis ...................................................... 76
  Working with rule usage data ....................................................... 77

Change tracking ............................................................................... 85
  Change tracking overview .......................................................... 85
  Setting up change tracking .......................................................... 86
  Viewing changes ......................................................................... 88
    Changing the tracking period ..................................................... 89
  Viewing the history of an access rule .......................................... 90
  Change Tracking reports ............................................................. 90
  Recovering lost changes ............................................................. 91
  Reviewing and reconciling changes .......................................... 92
    Setting up change review and reconciliation ............................ 92
    Reviewing the changes ............................................................ 93
    Prerequisite for change reconciliation ..................................... 94
    Coverage of changes ............................................................... 95
    Reconciling changes ............................................................... 95

Rule review and recertification ....................................................... 98
  Overview of rule review and recertification ................................. 98
  Reviewing a rule ....................................................................... 99
  Business attributes ................................................................. 100
    Adding custom business attributes ....................................... 101
  Recertification ......................................................................... 101
  Starting the recertification process manually ............................. 102
  Automatic update of next review dates ..................................... 102
    Creating rule review policies .................................................. 103
    Initializing the last certification date ....................................... 103
  Automatic ticket creation for rules needing review .................... 103
    Creating new rule recertification ticket policies ....................... 104

Intrusion prevention systems ......................................................... 105
  Viewing IPS information .......................................................... 105
    Viewing IPS information with vulnerability occurrences .......... 106
    Viewing IPS information without vulnerability occurrences .......... 108

Auditing firewalls on a continuous basis ...................................... 109
  Triggered collection and analysis .............................................. 109
  Task sequences ....................................................................... 110
    Creating task sequences ....................................................... 110
    Creating triggered collection and analysis task sequences .......... 111
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Viewing and editing task sequences</td>
<td>112</td>
</tr>
<tr>
<td>Task groups</td>
<td>113</td>
</tr>
<tr>
<td>Scheduling tasks and task sequences</td>
<td>113</td>
</tr>
<tr>
<td>Monitoring task results</td>
<td>114</td>
</tr>
<tr>
<td>Triggers</td>
<td>115</td>
</tr>
<tr>
<td>Creating triggers</td>
<td>116</td>
</tr>
</tbody>
</table>

**Advanced topics**                                                                 | 117  |
| Reports                                                                 | 117  |
| Access Checks reports                                                 | 117  |
| Access Compliance reports                                             | 118  |
| Firewall Assurance reports                                            | 122  |
| Firewall Changes reports                                              | 124  |
| Change Tracking reports                                               | 126  |
| NERC Compliance reports                                               | 128  |
| PCI Firewall Compliance reports                                       | 129  |
| Exporting model data                                                  | 131  |
| Searching for access rules                                            | 132  |
| Extended search                                                       | 133  |
| Search formats                                                        | 134  |
| Other ways to import data offline                                     | 135  |
| Change tracking utility                                               | 135  |
| Using the change tracking utility                                     | 136  |
| Troubleshooting                                                       | 137  |
| Cisco configuration diffs                                             | 137  |
| Addresses behind network interfaces                                   | 138  |
| Multi-zone interfaces                                                 | 142  |
| Overview of multi-zone interfaces                                     | 142  |
| Using multi-zone interfaces                                           | 143  |
Preface

Intended audience

The Skybox Firewall Assurance User’s Guide explains how to work with Skybox Firewall Assurance. Use this document in conjunction with:

- Skybox Installation and Administration Guide, which explains Skybox installation, and various configuration and maintenance tasks
- Skybox Firewall Assurance Getting Started Guide, which explains how to use the various features of Skybox Firewall Assurance, using predefined data

The intended audience is any user of Skybox Firewall Assurance, especially a user who manages firewall compliance.

How this manual is organized

This manual includes the following chapters:

- Overview of Skybox Firewall Assurance (on page 8)
- Data collection (on page 12)
- Policy compliance (on page 21)
- Optimization and cleanup (on page 71)
- Change tracking (on page 85)
- Rule review and recertification (on page 98)
- Intrusion prevention systems (on page 105)
- Auditing firewalls on a continuous basis (on page 109)
- Advanced topics (on page 117)

Related documentation

The following documentation is available for Skybox Firewall Assurance:

- Skybox Firewall Assurance Getting Started Guide

Other Skybox documentation includes:

- Skybox Installation and Administration Guide
- Skybox Reference Guide
- Skybox Developer’s Guide
- Skybox Release Notes
- Skybox Change Manager User’s Guide

The entire documentation set (in PDF format) is available here

You can access a comprehensive Help file from any location in the Skybox Manager by using the Help menu or by pressing F1.
Technical support

You can 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.

When opening a case, you need the following information:

- Your contact information (telephone number and email address)
- Skybox version and build numbers
- Platform (Windows or Linux)
- Problem description
- Any documentation or relevant logs

You can compress logs before attaching them by using the Pack Logs tool (see Packing log files for technical support, in the Skybox Installation and Administration Guide).
Chapter 1

Overview of Skybox Firewall Assurance

This chapter is an overview of Skybox Firewall Assurance.

In this chapter

Skybox platform ................................................................. 8
Highlights of Skybox Firewall Assurance ............................... 10
Basic architecture ............................................................... 11

Skybox platform

Skybox™ Security arms security professionals with the broadest platform of solutions for security operations, analytics and reporting. By integrating with more than 100 networking and security technologies organizations are already, the Skybox Security Suite merges data silos into a dynamic network model of your organization’s attack surface, giving comprehensive visibility of public, private and hybrid IT environments. Skybox provides the context needed for informed action, combining attack vector analytics and threat-centric vulnerability intelligence to continuously assess vulnerabilities in your environment and correlate them with exploits in the wild. This makes the accurate prioritization and mitigation of imminent threats a systematic process, decreasing the attack surface and enabling swift response to exposures that truly put your organization at risk.
Skybox arms security leaders with a comprehensive cybersecurity management platform to address the security challenges of large, complex networks. The Skybox Security Suite breaks down data silos to build a dynamic network model that gives complete visibility of an organization’s attack surface and the context needed for informed action across physical, multi-cloud and industrial networks. We leverage data by integrating with 120 security technologies, using analytics, automation and advanced threat intelligence from the Skybox Research Lab to continuously analyze vulnerabilities in your environment and correlate them with exploits in the wild. This makes the prioritization and mitigation of imminent threats an efficient and systematic process, decreasing the attack surface and enabling swift response to exposures that truly put your organization at risk. Our award-winning solutions automate as much as 90 percent of manual processes and are used by the world’s most security-conscious enterprises and government agencies, including Forbes Global 2000 companies. For more information visit the Skybox Security website.
The Skybox Security Suite includes:

- **Skybox Vulnerability Control**: Powers threat-centric vulnerability management by correlating intelligence on vulnerabilities in your environment, the surrounding network and security controls and exploits in the wild focusing remediation on your most critical threats.

- **Skybox Threat Manager**: Consolidates threat intelligence sources and prioritizes advisories in the context of your attack surface, automatically analyzing the potential impact of a threat and providing remediation guidance.

- **Skybox Firewall Assurance**: Brings multi-vendor firewall environments into a single view and continuously monitors policy compliance, optimizes firewall rule sets and finds attack vectors that others miss.

- **Skybox Network Assurance**: Analyzes hybrid environments end to end across physical, virtual and cloud – even operational technology – networks, illuminating complex security zones, access paths and policy compliance violations.

- **Skybox Change Manager**: Ends risky changes with network-aware planning and risk assessments, making firewall changes a secure, consistent process with customizable workflows and automation.

- **Skybox Horizon**: Visualizes an organization’s unique attack surface and indicators of exposure (IOEs), giving threat-centric insight to critical risks, visibility across an entire organization or down to a single access rule and metrics to track risk reduction over time.

The products share common services, including modeling, simulation, analytics, reporting, and automated workflow management.

**Highlights of Skybox Firewall Assurance**

Skybox Firewall Assurance is most often used to automate firewall audits, but you can use it to test policy compliance on other types of forwarding devices, as well.

**Highlights**

- **Comprehensive detection of security threats and compliance risks**
  - Imports, combines and normalizes firewall data automatically from multiple vendors.
  - Highlights access policy violations and provides root cause analysis.
  - Identifies rule conflicts and misconfigurations.
  - Reveals vulnerabilities on firewalls.

- **Next-generation firewall management**
  - Supports next-generation access and rule compliance at the user and application level.
  - Provides configuration analysis and reporting on intrusion prevention system (IPS) blades.
  - Provides comprehensive visibility and real-time reporting.
Chapter 1  Overview of Skybox Firewall Assurance

- Highlights the impact of firewall risks on your attack surface
- Shows the relation between firewalls and zones on an interactive map
- Reports on firewall ruleset audits and automates change tracking
- Incorporates compliance metrics and configuration analysis

▷ Firewall optimization and cleanup
- Automates rule recertification to streamline rulesets and ensure compliance
- Monitors firewalls continuously to eliminate security gaps
- Targets redundant, hidden and obsolete rules for cleanup and optimization

Basic architecture

The Skybox platform consists of a 3-tiered architecture with a centralized server (Skybox Server), data collectors (Skybox Collectors), and a user interface (Skybox Manager). Skybox can be scaled easily to suit the complexity and size of any infrastructure.

For additional information, see the Skybox architecture topic in the *Skybox Installation and Administration Guide*. 

Skybox version 8.5.600
Chapter 2

Data collection

The 1st step in analyzing firewalls using Skybox is to add their data to the Skybox database. You can collect firewall data online (by connecting to the firewall) (see page 14) or import it offline (by importing saved configuration files from the file system) (see page 15). Reimport data each time that there are changes to the firewall configuration, including new or deleted access rules or changes to existing access rules.

Note: Data for Palo Alto Networks firewalls includes IPS signatures and should also be reimported each time changes are made to the signatures.

You can import data from firewalls interactively (using a wizard) or by using a Skybox task that you can schedule to run at regular intervals.

For additional information about collection of data from many types of devices, see the Quick reference for data collection chapter in the Skybox Reference Guide.

In this chapter

Quick reference for data collection ........................................ 12
Using the wizard for online import......................................... 14
Using the wizard for import from the file system ..................... 15
Viewing and validating imported firewalls............................... 16
Working with tasks .............................................................. 18

Quick reference for data collection

The Add Firewalls Wizard enables you to import firewall configurations to Skybox for analysis.

Use the wizard to:

➢ Connect directly to the firewall or router ( ), or device management system ( ) and collect configuration data.
   For this method, you must know firewall details, see Using the wizard for online import (on page 14).

➢ Import saved device configuration files ( ).
For this method, you must save copies of the necessary configuration files on your file system, see Using the wizard for import from the file system (on page 15).

The firewall and router types available from the wizard and their requirements are listed in the following table.

<table>
<thead>
<tr>
<th>Device</th>
<th>Data source</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Check Point FireWall-1</td>
<td>The OPSEC API gets configurations remotely from a FireWall-1 Management Server</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>The following files are required:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• objects_5_0.C: The network objects</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• rulebases_5_0.fws: The rulebase</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The following files are optional:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• install_statuses.C: The statuses</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> If the Check Point configuration contains several policies, install_statuses.C is mandatory.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• vsx_objects.C: The VSX device objects</td>
</tr>
<tr>
<td></td>
<td></td>
<td>You also need the name of the active policy on each firewall module and the ifconfig and netstat –rnv output from each firewall module.</td>
</tr>
<tr>
<td>Cisco IOS</td>
<td></td>
<td>• The IP address of the router</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• A user name and password to access the router</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The following files are required:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• run.txt: The IOS configuration</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• (Optional) route.txt: Dump of the IOS routing table</td>
</tr>
<tr>
<td>Cisco Nexus</td>
<td></td>
<td>• The IP address of the router</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• A user name and password to access the router</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The following files are required:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• run.txt: The Nexus configuration</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• (Optional) route.txt: Dump of the Nexus routing table</td>
</tr>
<tr>
<td>Cisco PIX/ASA/FWS M</td>
<td></td>
<td>• The IP address of the firewall</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• SSH or Telnet access to the firewall</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• An admin user with level 5 privileges</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The following files are required:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• run.txt: The PIX/ASA/FWSM configuration</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• (Optional) route.txt: Dump of the PIX/ASA/FWSM routing table</td>
</tr>
<tr>
<td>Fortinet FortiGate</td>
<td></td>
<td>• The IP address of the firewall</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• SSH or Telnet access to the firewall</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• A user name and password to access the firewall</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The following files are required:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• config.txt: The FortiGate configuration</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• (Optional) route.txt: Dump of the FortiGate routing table</td>
</tr>
</tbody>
</table>
### Device Data Source and Requirements

<table>
<thead>
<tr>
<th>Device</th>
<th>Data Source</th>
<th>Requirements</th>
</tr>
</thead>
</table>
| Juniper Junos            |             | • The IP address of the firewall  
                          |             | • SSH or Telnet access to the firewall  
                          |             | • A user name and password to access the firewall  
                          |             | The following files are required:  
                          |             |   • config.txt: The Junos configuration  
                          |             |   • (Optional) route.txt: Dump of the Junos routing table  
| Juniper NetScreen        |             | • The IP address of the firewall  
                          |             | • SSH or Telnet access to the firewall  
                          |             | • A user name and password to access the firewall  
                          |             | The following files are required:  
                          |             |   • config.txt: The NetScreen configuration  
                          |             |   • (Optional) route.txt: Dump of the NetScreen routing table  
| Nortel Passport          |             | • The IP address of the router  
                          |             | • SSH or Telnet access to the router  
                          |             | • A user name and password to access the router  
                          |             | The following files are required:  
                          |             |   • run.txt: The Nortel configuration  
                          |             |   • (Optional) route.txt: Dump of the Nortel routing table  
| Palo Alto Networks       |             | • The name or IP address of the firewall  
                          |             | • A user name and password to access the firewall  
                          |             | The following files are required:  
                          |             |   • config.xml: The Palo Alto configuration and system information  
                          |             |   • (Optional) route.txt: Dump of the Palo Alto Networks routing table  

### Using the wizard for online import

*To import a firewall by connecting to the firewall*

1. Click \(\text{Add Firewall}\).
2. Select a firewall type, select the **Import from Firewall** method, and click **Next**.
3. Fill in the necessary connection and authentication fields, as described in the following topics in the Skybox Reference Guide:
   - Check Point FireWall-1
   - Cisco IOS
   - Cisco PIX/ASA/FWSM
   - Cisco Nexus
   - Fortinet FortiGate
   - Juniper Junos
   - Juniper NetScreen
Chapter 2  Data collection

- Nortel Passport
- Palo Alto Networks

4 Click **Next**.

5 Click **Start Import**.

After the import finishes, you can see the status of the import and any warning messages.

**Note:** If the import fails, click the link to the details log to see whether the reason for the failure is explained there. Go back to the details of the import (that is, the firewall type and the properties) and make corrections.

6 Click **Next**.

7 In the Select Firewalls screen, from the list of imported firewalls, select the firewalls that you want to add to Skybox (other firewalls are lost). Existing firewalls are automatically updated.

**Note:** The number of firewalls that you can include in the model is limited by your Skybox license.

8 Click **Next**.

9 (Optional) Use the Scheduling screen to specify whether this import is to run on a regular basis by creating a Skybox task to run on a specific schedule:
   a. Select **Add this import as a scheduled task**.
   b. (Optional) Change the name of the task.
   c. Select a schedule for the task.

10 Click **Next**.

In the Finish screen, you can see the added and updated firewalls.

By default, all new and updated firewalls are analyzed for Rule Compliance and shadowed and redundant rules when the wizard finishes.

11 Click **Finish**.

**Using the wizard for import from the file system**

Before importing firewall data from configuration files, prepare the files as explained in the following sections in the Skybox Reference Guide:

- Check Point firewalls from FireWall-1 Management Servers
- Check Point firewalls from Provider-1 CMAs
- Check Point Firewalls from Security Management
- Cisco IOS routers
- Cisco Nexus routers
- Cisco PIX/ASA/FWSM firewalls
- Fortinet FortiGate firewalls
- Juniper Junos firewalls
To import a firewall’s configuration files

1. Click Add Firewall.
2. Select a firewall type, select the Import configuration files method, and click Next.
3. Specify the location of the files to import.
4. For Check Point firewalls only, fill in the additional fields:
   - (Optional) Modules List: Type a comma-separated list of the names of the specific firewalls (modules) to import.
   - Rulebase: Specify the policy (rulebase) to import:
     - Use active policy: If you select a statuses file (in the Statuses field), import the active policy as specified in that file. Otherwise, import the most recently edited policy as specified in the objects file.
     - Use Specific Policy: The name of the policy to import.
5. Click Next.
6. In the Import Firewall Configuration screen, click Start Import.
   The status of the import and any warning messages are displayed.

Note: If the import fails, click the link to the details log to see whether the reason for the failure is explained there. Go back to the details of the import (that is, the firewall type and the other properties) and make corrections. If the import fails again, contact Skybox Professional Services.

7. Click Next.
8. In the Select Firewalls screen, from the list of newly imported firewalls, select the firewalls that you want to add to Skybox (other firewalls are lost). Existing firewalls are automatically updated.

Note: The number of new firewalls that you can include in the model is limited by your Skybox license.

9. Click Next.

   In the Finish screen, you can see the added and updated firewalls.

   By default, all new and updated firewalls are analyzed for Rule Compliance and shadowed and redundant rules when the wizard finishes.

10. Click Finish.

Viewing and validating imported firewalls

After you import a firewall, validate that it was imported correctly and completely.
1 Confirm that the import succeeded:
   • For an existing device, look at the import time at the top-right of the
device’s summary page reflects the time of the current import, rather than
that of a previous import.
   • For a new device (a device that was imported for the 1st time), check
whether the imported device is now listed in the All Firewalls tree.
   If the firewall is part of a firewall management system, it is listed
underneath that server rather than directly under All Firewalls.

2 Check that the network interfaces were imported correctly: at the top of the
device’s summary page, click **Firewall Map.** You can see all the network
interfaces and the networks to which they are connected.

   ![Firewall Map (Main Router)](image)

   Close the map when you are finished.

3 Make sure that the routing rules were imported correctly:
   a. Right-click the device and select **Routing Rules.** Check that the routing
rules were imported (that is, Skybox contains a list of routing rules for this
device.)
   b. Use a sample routing rule to confirm that it was imported correctly: take a
routing rule that exists on the device and try to find its logical match in the
routing rules in Skybox.

   **Note:** A correctly imported set of routing rules (or access rules) logically
matches the set of rules on the device. However, some individual rules
might not be modeled in the same way that they are in the device.

4 Make sure that the access rules were imported correctly:
   a. Right-click the device and select **Access Rules.** Confirm that the access
rules were imported.
b. Take an access rule that exists on the device and try to find its logical match in the access rules in Skybox.

For Palo Alto Networks firewalls, make sure that the IPS rules were imported correctly:

a. In the Table pane, right-click the device and select **Manage IPS Rule Groups**.

b. Double-click each rule group to view its rules.

c. Verify that the rules appear in the Skybox Vulnerability Dictionary (that is, a check mark appears in the **Dictionary** column of the table).

d. If many of the rules are not in the Vulnerability Dictionary, you might be using an outdated version of the Dictionary.
   
   – For information about updating your Vulnerability Dictionary, see the Dictionary updates chapter in the Skybox Installation and Administration Guide.

e. Verify that the rule groups of the device in Skybox match the rules groups of the actual device.

### Working with tasks

When importing multiple firewalls, it is usually more efficient to work with Skybox tasks and task sequences than to use the Add Firewalls Wizard.

The following sections describe how to work with tasks and explain which tasks you can use for data collection.

#### USING THE OPERATIONAL CONSOLE

You manage Skybox tasks in the Operational Console. Skybox tasks include importing data from external sources, analyzing data, generating reports, and creating tickets.

*To use the Operational Console*

1. On the toolbar, click **Operational Console**.
   
The GUI of the Operation Console is set up the same way as the main GUI, with a tree on the left and a workspace on the right.

2. Navigate to **Tasks > All Tasks** to see a list of existing tasks.

*To run a task manually*

> Select the task and click **Launch**.

*To modify an existing task*

1. Select the required task.

2. Double-click the task to open its Properties dialog box.
   
   You can modify the task and **create a schedule for it** (see page 113).
To create a task

› Click New Task.

Task sequences

You can create task sequences, which group tasks together in a specific order. This is useful when you have several tasks that must run at the same time or consecutively. For example, you can update all the firewalls at a location at specific intervals and then analyze the updated firewalls. For additional information, see Task sequences (on page 110).

USING TASKS FOR DATA COLLECTION

Tasks enable you to schedule collection and other system activities to run as frequently as necessary.

The tasks that are used by the wizard to collect firewall data can be configured separately to run on a regular basis. There are also tasks for collecting data (both online and offline) from other firewalls and devices, and from management systems.

Information about importing data from directly supported firewalls is available in the Tasks part of the Skybox Reference Guide.

You can use the following generic file import tasks to import configuration data from other supported device types.

› **Import – Directory**: Import configuration files of multiple devices from multiple directories on the Server or the Collector
  - For information about these tasks, see the Import directory tasks topic in the Skybox Reference Guide.

› **Import – Basic**: Import configuration files of selected devices into the model, where the files are located on the local machine
  - For information about these tasks, see the Basic file import tasks topic in the Skybox Reference Guide.

Note: We recommend that you use Import – Directory tasks whenever possible, rather than Import – Basic.

Refer to the Skybox website for a list of supported devices.

Importing configuration data of other firewalls

You can import firewall types that do not have device-specific tasks and whose configurations are not supported directly by the generic import tasks. These firewalls are supported by running a script that converts the configuration of the firewalls to Skybox’s Integration XML (iXML) format, and then importing the iXML file using an offline file import task.
Running groups of tasks

In addition to setting up a schedule for a single task, you can run multiple tasks using Skybox task sequences. Most data collection tasks involve task sequences. For example, you might want to update several firewalls; analyze them for policy compliance, shadowed and redundant rules, and access rule changes; and then generate automatic reports. For information about creating task sequences, see Task sequences (on page 110).
Chapter 3

Policy compliance

Skybox checks each firewall for:

› Rule Compliance: Whether the firewall’s access rules comply with specific syntactic rules (for example, whether any of the firewall’s Allow rules contain “Any” in their source, destination, or services)
› Access Compliance: Whether the access enabled by the firewall’s access rules is in accordance with a standard (NIST 800-41 or PCI DSS) or organization-specific Access Policy
› Configuration Compliance: Whether there are weaknesses in the firewall’s configuration (for example, the default account uses the default password or the version of the firewall is outdated)

We recommend that you start by examining Rule Compliance and Configuration Compliance. Afterwards, you can move on to Access Compliance, which requires that you select a policy and map the firewall’s interfaces to it.

In this chapter

Rule Compliance ................................................................. 21
Access Compliance ........................................................... 30
Configuration Compliance ................................................. 56

Rule Compliance

Rule Compliance involves comparing the existing access rules of a firewall to a list of syntactic Rule Checks that consist of basic standards for access rules. For example:

› “Any” must not appear as the source, destination, or service of any access rule that defines permitted traffic
› The number of ports accessible using 1 access rule must be limited to a maximum of 1024

This set of syntactic checks is a Rule Policy.

Skybox checks the access rules of each firewall for compliance with the Rule Policy and shows which access rules violate the policy.
RULE COMPLIANCE OVERVIEW

Skybox comes with an out-of-the-box Rule Policy (Standard) that is applied to all firewalls.

<table>
<thead>
<tr>
<th>Rule Policies</th>
<th>Standard v2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anti-Spoofing IS not Configured (Check Point) (5 FWs)</td>
<td>Any in Destination (10 FWs)</td>
</tr>
<tr>
<td>Any in Service (10 FWs)</td>
<td>Any in Two Fields (11 FWs)</td>
</tr>
<tr>
<td>Any in Three Fields (4 FWs)</td>
<td>Bidirectional Rules</td>
</tr>
<tr>
<td>Deny Rules Not Logged (3 FWs)</td>
<td>Disabled Rules (3 FWs)</td>
</tr>
<tr>
<td>High Risk Application</td>
<td>Missing Explicit Deny Rule (6 FWs)</td>
</tr>
<tr>
<td>Missing Stealth Rule (7 FWs)</td>
<td>Risky Ports - Clear Text Passwords (9 FWs)</td>
</tr>
<tr>
<td>Risky Ports - Vulnerable Services (4 FWs)</td>
<td>Symmetric Rules (1 FWs)</td>
</tr>
<tr>
<td>Too Many Ports (2 FWs)</td>
<td>Too Many Rules in Section</td>
</tr>
<tr>
<td>Too Many IP's in Destination (1 FWs)</td>
<td></td>
</tr>
</tbody>
</table>

The policy includes:

- Standard best practice Rule Checks
- Checks relating to missing access rules (for example, “Is the ACL missing an explicit Any-Any Deny rule?”)
- Checks relating to the interaction between access rules (for example, “Are there bidirectional rules (that is, 2 rules with opposite source and destination but with the same service) in the ACL?”)

You can control the set of Rule Checks in the Rule Policy; see Customizing a Rule Policy (on page 24).

VIEWING RULE COMPLIANCE

Rule Compliance should be analyzed after firewalls are imported. You can either use a task of type Analysis – Policy Compliance or select the All Firewalls node in the Firewall Assurance tree and click Analyze on the toolbar. Analysis is done for Rule Compliance, Access Compliance and Configuration Compliance.

To view Rule Compliance

1. In the tree, select the desired firewall.
2. In the workspace, look at the Rule Compliance pane (in the Policy Compliance section).
   
   You can see whether the firewall is compliant with the Rule Policy and how many access rules violated the Rule Policy.
3 Click the link to view the Violating Rules.

The Violating Rules tab lists the access rules in the firewall that violate the Rule Policy.

If you also select Access Policy (above the list of rules), you can see the access rules that violate the Rule Policy and the Access Policy.

4 Click the Rule Compliance tab.

You can see the Rule Checks applied to the firewall and their pass/fail status. When you select a Rule Check, you can see its details in the Details pane or view its violating access rules.

Analyzing Rule Compliance after firewall updates

When you import a firewall using the wizard (as you did in the import tutorial), Rule Compliance is analyzed. When firewalls are updated using Skybox tasks, run an Analysis – Policy Compliance task to analyze Rule Compliance.

Note: If a firewall was not analyzed for some reason or if you accidentally cleared the compliance results, reanalyze compliance; right-click the Policy Compliance node of the firewall and select Analyze Compliance.

VIEWING THE VIOLATING FIREWALLS FOR A RULE CHECK

For each Rule Check, you can see the violating firewalls and then view the violating access rules for each firewall.
To view violating firewalls for a Rule Check

1. In the Tree pane, expand the Rule Policies node and select the desired Rule Check.

2. In the Table pane, click the Analyzed Firewalls tab.

You can see the firewalls that violated the selected Rule Check. In the Details pane, you can see the violating access rule.

CUSTOMIZING A RULE POLICY

Rule Policies are displayed under the Rule Policies node in the Firewall Assurance tree. The predefined Rule Policy is named Standard.

You can make the following changes:

- Create a Rule Policy or import a Rule Policy from a file
- Export a Rule Policy
- Customize the predefined Rule Policy (or a Rule Policy that you created or imported) by:
  - Modifying Rule Checks
  - Changing the limit or other properties of specific Rule Checks (see page 25)
  - Adding and deleting Rule Checks
  - Enabling and disabling Rule Checks

Rule Policies

- To make changes to an existing Rule Policy or to export it, right-click the Rule Policy.
- To create or import a Rule Policy, right-click the Rule Policies node.

Rule Checks

- To make changes to an existing Rule Check, right-click the Rule Check.
- To add a Rule Check, right-click the Rule Policy node and select New Rule Check.
Some Rule Checks might not be relevant for all firewalls; to disable (or enable) any Rule Check for a specific firewall, right-click the Rule Check in the Rule Compliance tab of the firewall and select Disable Rule Check in this Firewall (or Enable Rule Check in this Firewall).

**Exporting and importing Rule Policies**

You can export Rule Policies and reimport them later as necessary. This is useful when:

- You are working with multiple Servers and want to copy the policy between them.
- Skybox is upgraded and there are changes to the predefined Rule Policy.
  
  The predefined policy is not upgraded automatically. Rather, the new policy is available as an import so that you can look at both policies and select the policy that better meets your organization’s requirements.
- You want to make changes to the policy; exporting generates a backup file.

You can export a single Rule Policy or all policies in your Rule Policies folder. The result of the export is always a single file.

When you import policies from a file, each selected Rule Policy from the file is saved separately in the selected folder. Multiple policies with the same name are saved separately; they are not merged.

**To export Rule Policies**

1. Right-click the Rule Policies folder or a specific Rule Policy and select Export Rule Policy.

2. In the Export Rule Policy dialog box:
   a. (Optional) Change the name or type of the output file.
   b. If you want the policy saved on the Manager machine as well, select Save copy to a local directory and select the directory.

   This can be useful if you want to copy the policy to another Server.
   c. Click OK.

**To import Rule Policies**

1. Right-click the Rule Policies folder and select Import Rule Policy.

2. In the Import Rule Policy dialog box, select the file to load and the Rule Policies in the file that you want to import.

   To use a file from a local directory (rather than a file on the Server machine), click Upload.

3. Click OK.

**Rule Check types**

This section explains the different types of Rule Checks in Skybox and describes the fields that you can customize when creating a new Rule Check.

When editing an existing Rule Check, you can change the name, description, and severity only.
Antispoofing is not Configured

Rule Checks of this type verify that antispoofing is not configured on Check Point firewalls. Enabling antispoofing is a security best practice and helps prevent source IP addresses that are not part of the permitted IP address space from entering the protected network. Spoofing source IP addresses can be part of a DoS or other type of attacks.

There are no fields to customize in these Rule Checks.

Note: These Rule Checks are only run on Check Point firewalls.

Any in Allow Rules

Rule Checks of this type verify that “Any” is not used in Allow rules. Permitting “Any” in fields opens potential access that might not be intended and bypasses the security purpose of the firewall; limit access to those IP addresses and services required for business purposes and block all other IP addresses.

When creating a Rule Check of this type, you define which fields of the access rules are checked for the presence of “Any”.

Bidirectional Rules

Rule Checks of this type verify that there are no bidirectional access rules. A rule is bidirectional if another rule in the rulebase permits access to the same service in the opposite direction—from destination to source. Because of the stateful nature of firewalls, it is usually sufficient to define access in a single direction (from the client to the server). If any bidirectional rules exist, check them to verify that they are required and to understand the purpose that they serve in the security model of the firewall.

There are no fields to customize in these Rule Checks.

Disabled Rules

Rule Checks of this type test for disabled access rules. By default, violations of these checks have Info severity only, and do not impact the compliance metrics.

There are no fields to customize in these Rule Checks.

Field Content

Rule Checks of this type validate the content and format of text fields (for example, description and comments) in an access rule.

You can customize the following fields in these Rule Checks:

- **In Field**: Specifies which field in the access rules to check: Description, Original Rule Text, or Original Rule ID
- **Operator**: The operator to use when checking access rules
- **Expression**: The string or regular expression to check using the Operator
- **Include Deny Rules**: Specifies whether to also check Deny rules
- **Firewall Type**: The type of firewall whose fields are checked

Missing Explicit Deny-All Rule

Rule Checks of this type verify the existence of an explicit Deny Any/Any, or ‘cleanup’, rule in the rulebase of firewalls that do not add an implied Deny rule to the end of access lists. It is a good security practice to add such a rule to deny all access that is not explicitly permitted.
There are no fields to customize in these Rule Checks.

**Missing Stealth Rule**

Rule Checks of this type verify that the access list of each Check Point firewall includes a stealth rule, which is an access rule that does not permit any communication to the firewall from unauthorized sources. A stealth rule is a security practice that helps to protect the firewall from attacks. No exceptions are permitted on Rule Checks of this type.

There are no fields to customize in these Rule Checks.

Note: These Rule Checks are only run on Check Point firewalls.

**Risky Applications**

Rule Checks of this type test for applications, source zones, and destination zones that are vulnerable to attacks. It is a good security practice to limit access to these entities to essential access only.

You can customize the following fields in these Rule Checks:

- **Applications**
- **Source Zones**
- **Destination Zones**

Entities must be comma-separated.

**Risky Ports**

Rule Checks of this type test for services (ports) which are vulnerable to attacks. It is a good security practice to limit access to these services to essential access only.

When creating a Rule Check of this type, specify:

- Services to check (services must be comma-separated.)
- Whether to include rules that have Any in their Service field

**Symmetric Rules**

Rule Checks of this type test for the presence of symmetric rules. A rule is symmetric if its source field and its destination field are identical (but are not Any). Because of the stateful nature of firewalls, it is not usually necessary to have symmetric rules in the rulebase. Check these rules to verify that they are required and to see what purpose they serve in the security model of the firewall.

There are no fields to customize in these Rule Checks.

**Too Many IP Addresses**

Rule Checks of this type test for IP address ranges in the source or destination that enable overly permissive access to the protected network. It is good security practice to limit access to the protected network to only the required IP addresses, rather than specify a network range.

When creating a Rule Check of this type, specify:

- **In Field**: The fields to check: Source, Destination, or both
- **Limit**: The maximum number of IP addresses that permit access (Class B, Class C, or Specific Number)
Specified Number: If Specific Number was selected in the Limit field, enter the number here

Too Many Ports
Rule Checks of this type check for access rules that permit access to an excessive number of ports. It is a good security practice to limit access to the protected network to only the required ports.

When creating a Rule Check of this type, you specify the maximum number of ports to permit in Allow rules (when Any is not used).

Too Many Rules in Section
Rule Checks of this type check for sections that contain too many rules. It is a good security practice to limit the number of rules in a section.

When creating a Rule Check of this type, you specify the maximum number of rules to permit in a section.

Unlogged Rules
Rule Checks of this type test for the presence of access rules that are not logged. It is a good security practice to log all explicit Deny rules for tracking and auditing purposes, and it is often advisable to log other types of access rules as well. By default, violations of these checks have Info severity only, and do not impact the compliance metrics.

When creating a Rule Check of this type, you must specify the rule action (that is, the type of access rules to check).

Exceptions
Rule Checks can have multiple violations, where each violation is a single access rule that violates the Rule Check.

In some cases, these violating rules should be labeled as exceptions to the Rule Checks—they should not be reported as violations and should not affect the status of the Rule Check. When a violating rule is to be labeled as an exception, you create an exception for it. You can create exceptions from the following locations:

- Specific firewall > Policy Compliance > List of violating access rules in the Table pane
- Specific firewall > Policy Compliance > Rule Compliance tab (with the desired Rule Check selected) > Violating Rules tab in the Details pane
- Rule Policies > Specific Rule Policy > Specific Rule Check > Analyzed Firewalls tab (with the desired firewall selected) > Violating Rules tab of the Details pane
To create an exception from a Rule Policy violation

1. In the Table pane or the Details pane, right-click the desired access rule and select **Mark as Exception**.

   The Rule Check scope of the exception in the New Rule Exception dialog box varies according to where you are when you open the dialog box; it is either a specific Rule Check or **All Rule Checks** and any relevant Access Checks. If there were any Access Checks violated, they will also be included in the scope of the exception.
   
   - For information about the properties of exceptions, see **Properties of exceptions** (on page 30).

2. You can narrow or widen the scope of the exception.

3. By default, the exception expires when the access rule is modified. You can change the expiration to a specific date.

   After the exception expires, the violation reappears.

4. Click **OK**.

**Exception expiration**

There are 2 ways in which Rule Policy exceptions can expire:

- **Rule Modification**: When the access rule (for which the exception was created) is modified
- **Date Expiration**: According to a specific date

After an exception expires, the violation reappears. Sometimes an exception is required even after it expires. For example, if an access rule was modified, but it still violates the Rule Check.

To reactivate an exception

1. Open the Rule Exception Properties dialog box for the expired rule.

2. You can change the expiration method or expiration date.

   **Note**: If the expiration method is **Access Rule Modification**, you must clear and then reselect the check box to ‘set’ the change.

3. Click **Activate**.

**Exception management**

You can view, modify, and delete existing exceptions using the Exceptions dialog box. You can export the list of exceptions to a CSV file.

**Note**: You can only add new exceptions as explained in the preceding section (by selecting a specific access rule and, optionally, also a specific Rule Check).

You can manage Rule Policy exceptions in the following ways:

- Right-click the **Policy Compliance** node of a firewall and select **Exceptions**.

  The dialog box lists all exceptions for the selected firewall. Click the **Rule Policy Exceptions** tab to view these exceptions.
Right-click the Rule Policies node and select Exceptions.
The dialog box lists all Rule Policy exceptions.

Properties of exceptions

The properties of exceptions are described in the following table.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall Name</td>
<td>(Read-only) The name of the firewall with which this exception is associated.</td>
</tr>
<tr>
<td>Violating Rule#</td>
<td>(Read-only) The original rule ID of the access rule with which this exception is associated. If there is no original rule ID, the violating rule number is shown.</td>
</tr>
<tr>
<td>Rule Policy Scope</td>
<td>The Rule Checks with which this exception is associated.</td>
</tr>
<tr>
<td>Access Policy Scope</td>
<td>The Access Checks with which this exception is associated.</td>
</tr>
<tr>
<td>Max. Severity</td>
<td>(Read-only) The maximum severity of all the violations of the access rule associated with this exception.</td>
</tr>
<tr>
<td>Expiration</td>
<td>Specifies when the exception expires. By default, the exception expires when the access rule is modified; you can select a specific date. <strong>Note:</strong> After the exception expires for either reason, the violation reappears.</td>
</tr>
<tr>
<td>Tag</td>
<td>Enables you to categorize the exception according to your organization’s requirements; use this field to search for the exception.</td>
</tr>
<tr>
<td>Ticket ID</td>
<td>(Read-only) If the exception was created by approving risk in Change Manager, this is the ID of the relevant ticket.</td>
</tr>
<tr>
<td>Comment</td>
<td>Enables you to add comments.</td>
</tr>
<tr>
<td>Comment History</td>
<td>(Read-only) A listing of added user comments.</td>
</tr>
</tbody>
</table>

Access Compliance

*Access Compliance* simulates the traffic that can pass through a firewall by examining its access rules. It checks access between the network interfaces of individual firewalls. Access Compliance enables you to audit your firewall access rules based on PCI, NIST, or specific organizational guidelines, to see whether the traffic in your organization is in accordance with the selected guidelines.

You can analyze compliance on a continuous basis to monitor changes in firewall policy as they occur. Monitoring and reporting tools are provided so that you can assess the overall status of compliance.
WORKFLOW FOR ACCESS COMPLIANCE

The following is the basic workflow for using Skybox Firewall Assurance to verify Access Compliance:

1. Select the Access Policy for each firewall (right-click the firewall’s Policy Compliance node and select Manage Access Policy) and map its network interfaces to the appropriate zone.

   - For information about zones, see Classifying the network interfaces into zones (on page 32).

2. (Recommended) Review the Access Policy and modify it to match your organization.

   One area that might need modifying in the predefined policy is the definition of the limits in Limited Access Checks. For example, in the Limited SMTP Access Check, access from External zones is limited to 5 mail servers in the DMZ; if your organization has more than 5 accessible mail servers, change this limit.

   For additional information, see Policy customization (on page 47).

   **Note:** You can review and modify the policy after analysis. In this case, some access violations found the 1st time might be caused by Access Checks that do not match your organization’s network and policy.

3. Navigate to the main node for the Access Policy and click Analyze on the toolbar.

   Skybox applies the Access Policy to the firewall, checking the traffic between the interfaces.
4 Review the results of the analysis to see whether the firewall is compliant with the Access Policy. If it is non-compliant, check which access rules are causing the problems.

- For information about these results, see **Access Compliance and violation management** (on page 39).

5 Make all necessary changes (see **Handling policy violations** (on page 45)).

6 Generate and send **Access Compliance reports** (see page 118) as necessary.

### CLASSIFYING THE NETWORK INTERFACES INTO ZONES

You can apply an Access Policy to a firewall by selecting the Access Policy and then mapping the firewall's network interfaces to the zones used in that policy. A zone is a way of grouping network interfaces that have the same trust level. For example, map the network interface of a firewall that leads to the DMZ network to the DMZ zone and map network interfaces leading to the internet and other external networks to the External zone. You can then check compliance of this firewall with the selected Access Policy.

The predefined Access Policies for NIST use the following zones:

- **External**: A public network located outside your organization. External networks can usually only access the DMZ network, which serves as a neutral zone between the external network and the internal network. Assume communication from this side is untrusted.

- **Partner**: Partner or B2B networks located outside your organization. Partner networks usually have limited access to DMZ networks and to the internal assets of your organization.

- **DMZ**: A network located between a trusted internal network and an untrusted external network. The DMZ contains devices accessible to the external network using various protocols, including HTTP (web), FTP, SMTP (email), and DNS.

- **Internal**: A trusted network located inside your organization, which contains internal assets.

The predefined Access Policy for PCI DSS uses the following zones:

- **PCI_Cardholder Data Environment**
- **PCI_DMZ**
- **PCI_Internet**: For interfaces to outbound traffic to the internet. Assume communication from this side is untrusted.
- **PCI_Partners**
- **PCI_Untrusted_Wireless**
To check whether your firewall is compliant with an Access Policy, you must select the Access Policy and map each network interface of the firewall to the appropriate zone.

Note: Use the firewall map to see the network to which each interface is connected. This can help you to understand which network interfaces map to which zones.

To select an Access Policy for a firewall and map its interfaces to zones

1. In the Firewall Assurance tree, right-click the Policy Compliance node of the desired firewall and select Manage Access Policy.
2. In the Manage Access Policy dialog box, select the desired Access Policy.
3. Select each network interface in turn, and click Mark as Zone. Change or add the zone type. (The zone name is optional.)

Note: Alternatively, you can map the network interfaces to zones using the firewall map (right-click the interface in the map and select Mark as Zone).

4. To check traffic to or from a network interface, select the interface and click Access from Interface or Access to Interface.
   - For information about these results, see Access Analysis.
5. Click OK.
STRUCTURE OF THE ACCESS POLICY TREE

Each predefined Access Policy is divided into folders according to the type of access to be tested.

- Access Policies
  - Public Access Policies (52%)
    - NIST 800-41 & Application (55%)
      - NIST External Access (35%)
      - NIST Partner Access (84%)
      - NIST DMZ Access (62%)
      - NIST Internal Access (49%)
      - NIST Internal Cloud Access
    - NSX Access Queries
    - AWS Access Queries
    - Azure Access Queries
  - PCI DSS V3.2 Policy (31%)
    - 1.1 Firewall Configuration Standards (41%)
    - 1.2 Restrict Untrusted Access to Cardholder Data Environment (42%)
    - 1.3 Restrict Access from Internet to Cardholder Data Environment (18%)
    - 1.4 Install Personal Firewalls for Mobile Devices [N/A]
    - 1.5 Firewall Security Policies and Operational Procedures [N/A]

Each folder contains a set of policy sections that define the relationships between different zones.

- NIST External Access (35%)
  - NIST-External to Partner (100%)
  - NIST-External to DMZ (9%)
  - NIST-External to Internal (41%)
Each policy section includes a source, a destination, and Access Checks that define the access between them. The Access Checks define the access that is permitted between the source and destination zones of the policy section: access that must be blocked completely and access that can be permitted in some limited way.

- **NIST-External to DMZ (9%)**
  - Limited DNS Access: (5 Dest IPs) (0%)
  - Limited HTTP Access: (50 Dest IPs) (0%)
  - Limited SMTP Access: (5 Dest IPs) (0%)
  - Limited VPN Access: (5 Dest IPs) (0%)
  - Block ICMP Echoing Messages (50%)
  - Block Login Services (0%)
  - Block Miscellaneous (0%)
  - Block RPC and NFS (0%)
  - Block Small Services (0%)
  - Block Trojan and Worm Ports (0%)
  - Block Windows NetBIOS (0%)
  - Block X-Windows (0%)
  - Block Audio Streaming Applications (100%)
  - Block Video Streaming Applications (0%)
  - Block Gaming Applications (100%)
  - Block Email Applications (0%)
  - Block Social-Networking Applications (0%)
  - Block File-Sharing Applications (0%)
  - No Access - non-specified services (0%)
  - Limited Access - Services (10 ports) (0%)

### The PCI DSS V3.2 Policy

The folders of the **PCI DSS V3.2 Policy** correspond directly to the hierarchy of sections in PCI DSS Requirement 1. If you make changes to the hierarchy of this policy or if you create your own PCI policy, see **Mapping PCI policy folders** (on page 55) for information about teaching Skybox how the policy folders of your PCI policy correspond to the sections of PCI DSS Requirement 1.

### Policy sections

The source and destination of a policy section are defined by their scope. The scope of the source specifies the source points for access analysis; the scope of the destination specifies the destination points for access analysis. Usually, the source and destination are zone types, but they can be specific network interfaces.
To view the properties of a policy section

Right-click the policy section in the Access Policies tree and select **Properties**.

A policy section includes a source, a destination, and Access Checks of various types: **Limited Services**, **Risky Services to Block**, **All Other Services**, **Number of ports per destination IP**, and **Application Access Checks**. Some policy sections (for example, those that block all access between the source and the destination) have only 1 Access Check.

**Access Checks in a policy section**

An **Access Check** is a way to monitor access between 2 points.

The Access Checks in a policy section are grouped into several types:

- **Service Access Checks** test access between the source and the destination over specific protocols (services):
  - **Limited Services**: Services (protocols) that are limited to a specific number of IP addresses (to prevent excessive permissions)
  - **Risky Services to Block**: Services that are blocked completely
• **All Other Services**: Services that are not specified by the previous 2 sets and whose access is defined manually

If the **Limited Services** and **Risky Services to Block** Access Checks cover all services, there cannot be an **All Other Services** Access Check.

• **Number of ports per destination IP**: Limits the number of ports that can be accessed for each destination IP address

  ▶ **Application Access Checks** test to make sure that there is no access between the source and the destination over specific applications.

  Note: Application Access Checks are only tested on next-generation firewalls (NGFWs) (for example, Palo Alto Networks and FortiGate firewalls).

**Limited Services Access Checks**

These checks can limit the number of destination IP addresses or the number of source IP addresses.

▶ When the limit is on destination IP addresses, Skybox counts and limits the number of accessible destinations. For example, “Permit access to up to 5 mail servers.”

▶ When the limit is on source IP addresses, Skybox counts and limits the number of addressing sources. For example, “Permit access to my management network from up to 20 addresses.”

When limiting access by IP addresses, the limit can be specified as any of the following:

▶ A specific number of IP addresses that must not be exceeded for each service. For example, “No more than 5 SMTP servers in each DMZ zone may be accessible from an External zone.” If there are 6 or more SMTP servers in the DMZ that are accessible from an External zone through the firewall, the firewall is not compliant with the Access Check.

▶ A list of networks or devices in the destination that are permitted from the source through the firewall. If other networks or firewalls are accessible, the tested firewall is not compliant with the Access Check.

▶ Some limit: Not all IP addresses are accessible for each service, although no specific numeric limit or list of permitted entities is set. For example, “HTTP traffic between External zones to the DMZ must be filtered.” If all IP addresses in the DMZ are accessible via HTTP through the firewall, it is non-compliant.

  This type of limit is useful for making sure that there are no Any-Any rules in the tested firewall.

**Number of ports per destination IP Access Checks**

When limiting access by destination ports, the limit can be specified as:

▶ A specific number of ports that must not be exceeded for each destination IP address. For example, “No more than 5 ports on any DMZ server may be available to an External zone.”
Some limit: For each destination device (that is, for each destination IP address), some ports are inaccessible from the source, although no specific numeric limit is set. If all ports on even 1 destination IP address are accessible, the tested device is non-compliant.

Access tests

Each Access Check in a policy section is divided into separate access tests, where each test checks access (and compliance) from a specific source to a specific destination. The entities in the source and destination of the policy section control the breakdown of the Access Check into access tests: each entity in the source or destination is considered a separate source or destination instance and a separate access test is created from each source instance to each destination instance.

In this way, you can define an Access Policy using zone types, but analyze the access using actual network interfaces that are added to and deleted from the zone types dynamically when firewalls and network interfaces are added and removed.

When you select an Access Check in the tree, you can see these tests in the All Access Tests tab of the workspace.

Policy sections that use zones

When the source or destination is a zone type, each network interface of that zone type is used as a separate source or destination to create the tests. As each test focuses on a specific route in the network, you can examine the results of access testing on each route in detail.

For example, a firewall is imported to Skybox with the following interfaces:

- NI1 and NI2: Marked as External zones
- NI3 and NI4: Marked as DMZ zones

For a policy section with Source = External zones and Destination = DMZ zones, the following tests are created for each Access Check in the policy section:

- NI1 to NI3
- NI1 to NI4
- NI2 to NI3
- NI2 to NI4

Policy sections that use a specific list of sources or destinations

When there is a specific list of sources or destinations in a policy section, those network interfaces are used to create the tests for each Access Check.

For example, for a policy section with Source = NI_Partner1, NI_Partner2 (each of which connects a firewall to a specific partner network) and Destination = NI_Users1, NI_Users2 (connecting to user networks in your organization), the following access tests are created for each Access Check in the policy section:

- NI_Partner1 to NI_Users1
Chapter 3  Policy compliance

› NI_Partner1 to NI_Users2
› NI_Partner2 to NI_Users1
› NI_Partner2 to NI_Users2

Note: Tests are created only for firewalls whose network interfaces match those in the policy section.

**Access tests when using multiple firewalls**
Compliance is tested only between network interfaces on the same firewall. If you are testing compliance for many firewalls at the same time, no cross-firewall access tests are created.

To test for access between 2 separate firewalls, use Skybox Network Assurance.

**Viewing and managing access tests**
You can view and manage access tests per firewall (in the All Firewalls tree) or by Access Check.

Even before the results of a firewall or Access Check are analyzed, you can see a list of the access tests for the selected firewall (or Access Check) in the All Access Tests tab of the Table pane. After analysis, each access test has a compliance indicator (pass or fail) instead of a question mark and you can view a list of non-compliant tests for the Access Check in the Violations tab. Results are displayed per test in the Access Results pane.

Review the list of access tests before you analyze compliance. If the list of tests is not what you expected, this could mean that the Access Check is not defined correctly or that you did not mark the zone types of the network interfaces correctly.

Reminder: To view the zone types for a firewall’s network interfaces, select the firewall under the All Firewalls node of the Firewall Assurance tree, right-click the Policy Compliance node and select Manage Access Policy, and look in the Zone Type column.

**Disabling access tests**
When you view the access tests, you might see tests that should not be analyzed. You can disable these tests. If you disable an analyzed test, its analysis results are erased.

*To disable or enable a test*

› Right-click the test in the All Access Tests tab of the Table pane and select Disable or Enable.

Disabled tests are listed in a light gray font in all tables that list access tests and violations.

**ACCESS COMPLIANCE AND VIOLATION MANAGEMENT**
This section explains how to verify that the firewall being audited complies with your organization’s Access Policy and how to view and handle policy violations.
Reviewing compliance metrics

After compliance is analyzed for a firewall, you can view an overview of its compliance on the Summary page (in the tree, select the firewall).

At the top, you can see the overall Access Compliance status for the selected firewall. Under that, there is a link specifying the number of violating rules and a list of the top violating policy sections.

Click the link to open the Violating Rules tab. If it is clear from the list of violating access rules that only a small number of them caused most of the violations, you can drill down directly into those access rules (see page 40). Otherwise, in the Access Compliance tab, review the policy sections 1-by-1 (see page 40), starting with the top violating sections.

Reviewing the violating access rules

Sometimes, many violations are caused by a single access rule. It is easy to view the list of violations and decide whether to fix the access rule or whether the policy is incorrectly defined.

The Violating Rules tab shows all the violating access rules of the firewall.

- If you sort the list by number of violations, you can see which access rules cause the most violations. The Details pane lists the attributes of the 1st access rule or the selected access rule, and the list of violations that it causes.
- If you sort the list by source or destination, you can review the access rules with wider exposure before those that specify only 1 network or asset.

When you select an access rule, the Details pane includes a tab listing the violations for that access rule and a tab with read-only information about the access rule. When you select a violation, the Details pane shows detailed information about the selected violation.

For additional information about violations, see Viewing violations (on page 41).

Viewing the policy sections

The Access Compliance tab of each firewall shows all policy sections in the Table pane. You can see the compliance percentage of this firewall against each policy section and how many violations there are. When you select a policy section, the Details pane lists the violating access rules for the selected policy section and the access tests that were run.

You can click the link of any policy section with violations to view more details about the violating access rules and the violations of that policy section.
Viewing violations

A violation is an access test that was analyzed and found to be non-compliant—the amount of access between the source and the destination of the access test does not match the expected access (of the Access Check).

For each violation, you can see the following tabs in the Details pane:

› **Details**: Details about the access test (Access Check information with the source and destination of this specific instance).

› **Violation Explanation**: An explanation of why this access test (that is, this violation) does not comply with the Access Check.

For example:

| On the device main_FW, too many destination ports are accessible in the destination int2809 (DMZ). |
| The limit in the Access Check specifies that no more than 10 destination ports should be accessible for each IP address in the destination. The following IP addresses exceeded the limit by being accessible on too many destination ports: |
| 192.170.1.96-192.170.1.111 - accessible on 197119 destination ports |
| 192.170.33.0-192.170.36.255 - accessible on 197119 destination ports |

› **Access Results**: The entities that violate the Access Check

Note: When you select a compliant test, you might need to make changes to display actual entities.

› **Exceptions**: A list of exceptions specified for this access test

› **Comments** and **History**

Viewing access results

The **Access Results** tab of the Details pane contains a *results tree* that displays the access results of the selected test. You can expand the tree to view the entities enabling or blocking access: network interfaces, IP address ranges, and services.

To view access results for an access test

1. Do one of the following in the Firewall Assurance tree:
   - Select the Access Check in the Access Policies tree and then select the violation or test in the **Violations** tab or **All Access Tests** tab of the Table pane.
   - Select the **Policy Compliance** node of the firewall and select an Access Check:
     - In the **Violating Rules** tab, select the relevant access rule and click the link of the Access Check in the Details pane.
     - In the **Access Compliance** tab, click the link of the relevant Access Policy section in the Table pane and then, in the **Violating Rules** tab, select the relevant access rule and click the link of the Access Check in the Details pane.
   - Select a node under **Access Policies > Access Policy Violations** and then select a violation in the Table pane.
2 Click the **Access Results** tab in the Details pane and expand the results tree.

The entities are displayed and grouped according to the type of Access Check and the compliance results. For example, for violations, the default view is **Accessible Destinations**; for a successful access test, the default view is **Blocked Destinations**.

You can change the information in the results tree by changing the value of the **Show** field:

- **Accessible Destinations**: Destinations accessible from the specified source point
- **Sources Accessing the Destination**: Source points that have access to the specified destination
- **Blocked Destinations**: Destinations that cannot be reached from the specified source point (because they are blocked)
- **Blocked Sources**: Source points that do not have access to the specified destination (because they are blocked)

Note: The content of each view depends on the display filters (see page 42) that you select.

When destinations are displayed, you can expand a destination asset node to see accessible or blocked services on that asset. When source points are displayed, you can expand a destination network node to see the gateways that enable or block access.

**Display filters**

The toolbar at the top of the **Access Results** tab of the Details pane contains the following display filters:

- **Show**: Specifies the type of entities to display:
  - **Accessible Destinations**: The accessible destinations when using the specified services
  - **Blocked Destinations**: The destinations for which there are blocked routes from the source when using the specified services
  - **Sources Accessing the Destination**: The assets that can access the selected destination when using the specified services
  - **Blocked Sources**: The assets for which there are blocked routes to the destination when using the specified services

Note: When blocked sources or destinations are displayed in the results tree, all names in the tree are italicized.
Group By: Toggles between grouping the entities displayed in the results
tree by their services or by their network interfaces

Authentication:
- No: Unauthenticated traffic
- Yes: Authenticated traffic
- N/A: All traffic, whether authenticated or unauthenticated

Save Results:
- Save Results as XML: Saves the currently displayed access results as
  an XML file
- Save Results as CSV: Saves the currently displayed access results as
  a CSV file

Mark as Exception: Marks a specific entity (network, network interface, or
service) as an exception to the Access Check (policy exception), so that it is
not analyzed

Show Access Route: The Access Route Details dialog box displays all access
routes for the selected entity in the results tree

What If: Runs a comparison between access in the current model (usually
Live) and access in another model (usually What If)

Viewing the Access Route
The Access Route shows all potential routes through which access from the
source to the destination is possible for a selected entity.
**To view the Access Route**

1. In the results tree, select an IP address range or port range.
2. Click **Show Access Route**.

   The Access Route Details dialog box displays every potential route for the selected entity.

![Access Route Details](image)

Each Access Route shows how many routes are available from a specific source to a specific destination through the firewall; multiple routes are displayed after the other. For each route:

 › The Source is described.
   If the source point is a subset of the source specified in the Source field, the source IP address ranges are listed.

 › Address translation rules (if any) and access rules on the firewall that enables the access are listed in a table.
   Rules are shown with their direction, rule number, ruleset name, and rule action. Click the link in a rule to open the Access Control List Editor for easy viewing of the rule.

 › The Destination is described.
   Asset name, IP address, service type and port number are displayed.

For inaccessible (blocked) routes, the source is displayed, followed by the access rule in the firewall that blocks the route. For additional information about inaccessible routes, see **Inaccessible entities** (on page 45).
Inaccessible entities

Sometimes, an access rule blocks access between the source network interface and the destination network interface. The rule might block access to all IP address ranges behind the destination network interface or only to some of them.

Use the Show Blocked Destinations filter to discover which IP address ranges behind the destination network interface are blocked.

To view additional information

1. From the Show field on the toolbar, select Blocked Destinations.
   The results tree changes to display the blocked routes.
2. In the results tree, select the entity for which you want to see the blocking rule.
3. On the toolbar, click Show Access Route.
   The Access Route Details dialog box displays the selected routes; the table for each route shows the access rule on the device that blocks access.

![Access Route Details dialog box]

Note: The value in the Detail Level field is irrelevant when checking access for single devices; there is always only 1 blocking rule.

4. Click the link on the access rule to view the rule in the Rule Match Details dialog box.

Handling policy violations

Policy violations (noncompliant tests) might indicate any of the following:
A problem in the firewall’s ACL
For example, a change was made to a firewall that exposes database server to the access from new networks. The access rule must be fixed to prevent this exposure.

The Access Check is not defined correctly and must be fixed
For example, the “Block Login Services” Access Check includes the SSH protocol. However, in your organization, SSH is permitted. You can edit the Access Check and delete SSH from the list of blocked login services.
A similar situation can occur with “Limited Number of Services” Access Checks; you might want to change the limit from 10 to 50 (or some other value), because of the way that your organization works.

The Access Check is usually relevant but there is business justification for granting exceptional permission in specific cases
When working to solve policy violations, consider all these possibilities for each violation. After the Access Policy is debugged and the firewall is up-to-date, most violations that occur indicate problems in the firewall configuration.

To fix an Access Check

In the Table pane, right-click the violation and select **Edit Access Check**.

To grant exceptional permission (that is, to create an exception)

1. In the Table pane, right-click the relevant access rule and select **Mark as Exception**.
2. Fill in the fields of the exception as explained in Properties of exceptions (on page 30).

**PCI DSS SUPPORT IN SKYBOX FIREWALL ASSURANCE**

Skybox Firewall Assurance supports PCI DSS Requirement 1: “Install and maintain a firewall configuration to protect cardholder data, a sensitive area within the trusted network of a company.”

Requirement 1 calls for protection of all system areas from unauthorized access, to prevent unprotected pathways into key systems.

Requirement 1 is preconfigured in Skybox using an Access Policy and specific PCI zone types, so that you can use Skybox Firewall Assurance to check whether your firewalls are compliant. **PCI DSS V3.2 Policy** is organized using a similar structure to the hierarchy of sections in Requirement 1 of the policy.

To run a PCI audit for a firewall, use the workflow for Access Compliance (see page 31), mapping the firewall’s network interfaces to the PCI zones rather than to the regular (NIST-related) zones and then generate a PCI Firewall Compliance report. This report describes how each firewall in the report scope complies with PCI DSS Requirement 1.

For information about PCI Firewall Compliance reports, see **PCI Firewall Compliance reports** (on page 129).

For information about the properties and sections of these reports, see the PCI Firewall Compliance reports topic in the Skybox Reference Guide.
CUSTOMIZING AN ACCESS POLICY

This section explains how to customize an Access Policy to meet your organization’s requirements.

Note: The predefined **NIST 800-41 Policy** is used by Skybox Firewall Assurance and Skybox Network Assurance. If you are using both products, keep this in mind when making changes to this Access Policy.

**Policy customization overview**

You can change a predefined Access Policy by:

- Adding new Access Policy folders
  
  You can add new folders for new groups of policy sections or to improve the hierarchy of the Access Policy. (To add a new Access Policy folder, right-click the parent node in the tree and select **New > Access Policy Folder**.)

- Adding new policy sections

- Adding new Access Checks to existing policy sections

- Editing existing policy sections and Access Checks
  
  Note: If you change a predefined Access Check, update its description (comment) to reflect the changes. Otherwise, other users who try to understand the Access Check by reading its description might be misled.

- Adding exceptions: Excluding specific entities from the definition of the Access Check

- Deleting or disabling Access Checks, policy sections, or policy folders that are not relevant for your organization from the predefined policy

- Changing the severity of Access Checks

- Reorganizing the hierarchy of the policy: For example, adding or deleting policy folders or moving Access Checks between folders

We recommend that you add your organization’s best practice guidelines to the Skybox Access Policies, to ensure continued compliance to industry and organizational standards.

You can generate an **Access Checks report** (see page 117) that lists all the policy sections and Access Checks in a specified Access Policy scope.

**Creating zone types**

The predefined NIST 800-41 Access Policy uses 4 zone types (External, Partner, Internal, and DMZ) and the PCI DSS Access Policy uses 5 zone types (PCI_Internet, PCI_Partners, PCI_Cardholder Data Environment, PCI_Untrusted_Wireless, and PCI_DMZ). You can create additional zone types as necessary and then create policy sections that check access between these zone types.
To create a zone type

1. In the Access Policies tree, right-click the Zones node and select New Zone Type.

2. Type a name and a description of the zone type.
   The description is optional. It is displayed next to the name in the workspace when you select the Zones node.

3. Click OK.

Customizing policy sections

You can change the source and destination of policy sections.

Note: Usually, the name of the section is based on the source and the destination and changes if you change the source or the destination. However, if you modify the name it no longer updates automatically.

You can add Access Checks to a policy section or modify existing Access Checks, including changing their limits, and disabling or enabling them. Skybox prevents the creation of conflicts between Access Checks in the same policy section. For example, if you have an Access Check that defines how to limit access to all non-specified services, it is disabled if you create an Access Check that blocks all access.

Creating policy sections

The predefined Access Policy includes policy sections that check access between all the predefined zone types in both directions. If your organization wants to split any of these zone types (for example, having several types of internal zones with different security levels), create additional zone types and then create policy sections to define the relationships between them. You can create a policy section to define the relationship between 2 specific network interfaces.

For information about creating new zone types, see Creating zone types (on page 47).
To create an Access Policy section

1. Right-click the Access Policy under which you want to create the new Access Policy section and select **New > Access Policy Section**.

   ![Access Policy Section Properties](image)

   By default, the policy section includes an Access Check for all other services and an Access Check for number of ports per destination IP address. Even if you do not define other Access Checks for this policy section, each service is limited to 50 destination IP addresses and each destination IP address is limited to 50 ports.

2. **Define the source and the destination** (see page 50).

3. **Define or copy the Access Checks** (see page 51).

4. If necessary, change the value of the **All Other Services** Access Check and the **Number of ports per destination IP** Access Check.

   Note: Each policy section can have only a single Access Check that deals with all services or all other services. For example, if the policy section blocks access to all services, the **All Other Services** Access Check is disabled.

5. **Click OK**.
Defining the source and destination

Note: The default scope for source and destination is Any. You must define a specific scope for at least 1 of them; Skybox does not verify access from Any to Any.

To define the source and the destination of a policy section

1. Click the Browse button next to the Source field.

2. If necessary, change the scope type. To define a policy section for a specific firewall, use Network Interfaces.

3. To define the source, do any of the following:
   - In the Available Entities field, select all entities that are part of the scope and click to move them to the Selected Source field.
   - In the Selected Source area, click the Browse button next to the Use IP Ranges field to select specific IP address ranges for the scope.

4. To define the destination, do any of the following:
   - In the Available Entities field, select all entities that are part of the scope and click to move them to the Selected Destination field.
In the Selected Destination area, click the **Browse** button next to the **Use IP Ranges** field to select specific IP address ranges for the scope.

5 Click **OK**.

The default name of the policy section is based on the source and the destination.

**Adding Access Checks**

You can add Access Checks to a policy section:

- By copying Access Checks from existing policy sections and making necessary changes
- By creating new Access Checks

**Copying Access Checks from existing policy sections**

You can copy Access Checks from policy sections.

When you add Access Checks to a policy section by copying from existing policy sections, Skybox examines the selected Access Checks and warns you if any of the following are selected:

- 2 Access Checks with the same name
- 2 Access Checks with the same unique type (**Number of Ports** or **All Other Services**)
- An **All Other Services** Access Check with an Access Check that covers all other services

If you receive any warnings, modify your selection before continuing.

To copy Access Checks from existing policy sections

1 In the Policy Section Properties dialog box, click **Copy from...**.
2 In the Select Access Checks dialog box, select the Access Checks to copy:
   - Copy the Access Checks from a specific policy section: Select the policy section in the **Available Access Checks** field and click **””**.
     The Access Checks in the selected policy section are copied to the **Selected Access Checks** field.
   - Select specific Access Checks from policy sections: Select the desired Access Checks in the **Available Access Checks** field and click **””**.
     (Repeat this action as often as necessary to select all the Access Checks that you need.)
     The selected Access Checks are copied to the **Selected Access Checks** field.
3 If conflicts are reported, refine your selection.
4 Click **OK**.
Creating new Access Checks

To create a Limited Access Check

1. Open the New Limited Access Check dialog box:
   - Right-click the policy section and select Properties and then, in the Limited Services area, click Add.
   - Right-click the policy section and select New > Limited Access Check.

2. Fill in the fields according to the table in Access Check properties (see page 53).
   At a minimum, specify values for the following fields: Services, Limitation, and Description.

3. Click OK.

To create a No Access Check

1. Open the New No Access Check dialog box:
   - Right-click the policy section and select Properties and then, in the Risky Services to Block area, click Add.
   - Right-click the policy section and select New > No Access Check, and either Services or Applications, depending on whether you want to block specific services (ports) or specific web applications.

Note: Access Checks for applications are only tested on NGFWs (for example, Palo Alto Networks firewalls and FortiGate firewalls).
2 Fill in the fields according to the table in Access Check properties (see page 53).

At a minimum, specify values for the following fields: Services or Applications, and Description.

3 Click OK.

Access Check properties

The properties of Access Checks in Skybox Firewall Assurance are described in the following table.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A name for the Access Check.</td>
</tr>
<tr>
<td>Source</td>
<td>(Read-only) The source point for access analysis (taken from the policy section).</td>
</tr>
<tr>
<td>Destination</td>
<td>(Read-only) The destination point for access analysis (taken from the policy section).</td>
</tr>
<tr>
<td>Type</td>
<td>(Read-only) The type of Access Check:</td>
</tr>
<tr>
<td></td>
<td>• Limited Access: Confirms that the access between 2 points does not exceed a specified limit.</td>
</tr>
<tr>
<td></td>
<td>• No Access: Verifies that all routes between the source and the destination (via the selected services or applications) are blocked.</td>
</tr>
<tr>
<td>Severity</td>
<td>The severity of this Access Check.</td>
</tr>
<tr>
<td>Authentication</td>
<td>• No: Block or limit regular traffic (without authentication). That is, regular access rules (without authentication) limit or deny access.</td>
</tr>
<tr>
<td></td>
<td>• Yes: (Limited Access Checks only) Limit traffic for authenticated users. That is, access for authenticated users is limited to a specific number of IP addresses or ports.</td>
</tr>
<tr>
<td></td>
<td>• N/A: Block or limit all traffic (whether authenticated or not).</td>
</tr>
<tr>
<td>NAT</td>
<td>(No Access Checks only)</td>
</tr>
<tr>
<td></td>
<td>• None</td>
</tr>
<tr>
<td></td>
<td>• No Source NAT</td>
</tr>
<tr>
<td></td>
<td>• No Destination NAT</td>
</tr>
<tr>
<td>Services</td>
<td>(Service No Access Checks and Limited Access Checks only) The services on the source zones to use to analyze access. Click the Browse button to select services.</td>
</tr>
<tr>
<td></td>
<td>• Not: Analyze access on all services except those selected.</td>
</tr>
<tr>
<td>Applications</td>
<td>(Application No Access Checks only) The applications on the source zones to check for access. Click the Browse button to select applications.</td>
</tr>
<tr>
<td></td>
<td>• Not: Check access for all applications except those selected.</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Limitation on Destination IP addresses       | (Limited Access Checks only) The amount and type of permitted access:  
- **Number of IP addresses per service**: For each accessible destination port, the maximum number of IP addresses that can be accessed from that port.  
- **Not all IP addresses can be reached**: For each accessible destination port, there must be IP addresses that are not accessible.  
- **Limit to a specific scope**: For each accessible destination port, only the selected IP addresses are accessible. |
| Limitation on Source IP addresses            | (Limited Access Checks only) The amount and type of permitted access:  
- **Number of IP addresses per service**: For each accessible destination port, the maximum number of source IP addresses permitted.  
- **Not all IP addresses can be reached**: For each accessible destination port, there must be source IP addresses that are blocked.  
- **Limit to a specific scope**: Source IP addresses must match the selected IP addresses. |
| Description                                  | A free text description of the Access Check.                                                                                                                                                        |
| **Advanced**                                 |                                                                                                                                                                                                     |
| Routing Rules                                |  
- **Use All**: Use all routing rules.  
- **Ignore All Rules**: Ignore routing rules—route each packet through all available interfaces. This option is useful for connectivity testing and model verification.  
- **Ignore Dynamic Rules Only**: Use only static routing rules; packets that do not match the static routing rules are routed through all available interfaces.  
  
**Note**: This option has no effect on assets and gateways without routing rules. For such assets, packets are routed through all available interfaces. |
| Routes per Service                           | The number of routes to analyze for each service. If the displayed route is incomplete, increase this value to provide a more complete result.  
  
**Note**: Increasing the value of this property increases the analysis time for this query.  
  
**Note**: The default value is controlled by the AccessAnalyzer_max_routes_for_service property in <Skybox_Home>/server/conf/sb_server.properties |
| Simulate IP Spoofing During Analysis         | Specifies whether access is analyzed from any IP address (to simulate IP address spoofing).                                                                                                                                                                    |
| Create as Single Test                        | Specifies whether to create a single access test for all sources and destinations together. If cleared, a separate access test is created for each source-destination pair.                                                                 |

**Note**: If you change any of these values after the Access Check is analyzed, you must reanalyze the Access Check for the changes to take effect.
Mapping PCI policy folders

Each folder of the predefined PCI DSS Access Policy correlates directly to the subsection of PCI DSS Requirement 1 with the same name. However, you can change the hierarchy of the PCI policy or create your own PCI policy. In these cases, to display information from the PCI policy correctly in PCI DSS – Firewall Compliance reports, you must map the Access Policy folders to the appropriate PCI requirements.

Note: PCI Access Policies must be located directly under the Public Access Policies folder.

To map PCI Access Policy folders to the appropriate sections of the PCI requirement

1. In the Access Policies tree, locate the PCI Access Policy to map.
2. Right-click the policy and select Map PCI Access Policy Folders.
3. Make sure that the correct PCI DSS policy version is selected.
4. For each subsection of the PCI requirement, click Browse and select the appropriate policy folders.

Note: If a subsection is not mapped, the details for that subsection contain the text “Tests for this requirement are unavailable”.

If multiple folders are mapped to a single requirement, consider the mapped folders together as input for that requirement in the structure of the report.

5. Click OK.
Exporting and importing Access Policies

You can export Access Policies and reimport them later as necessary. This is useful when:

- You are working with multiple Servers and want to copy the policy between them.
- Skybox is upgraded and there are changes to the predefined Access Policy.
  The predefined policy is not upgraded automatically. Rather, the new policy is available as an import so that you can look at both policies and decide which better meets your organization’s requirements.
- You want to make changes to the policy; exporting generates a backup file.

You can export a single Access Policy or all the Access Policies in your Public Policies or Private Policies folder. The result of the export is always a single file.

When you import, each selected Access Policy from the file is saved separately in the selected folder. Multiple policies with the same name are saved separately; they are not merged.

To export a policy folder or Access Policy

1. Right-click the policy folder or specific Access Policy and select Export Access Policy.

2. (Optional) Change the name or type of the output file.
   By default, Access Policies are stored in the <Skybox_Home>/data/access_policy directory.

3. If you also want the policy saved on the Manager machine, select Save copy to a local directory and select the directory.
   This is useful if you want to copy the policy to another Server.

4. Click OK.

To import a policy folder or Access Policy

1. Right-click the policy folder into which you want to import and select Import Access Policy.

2. Select the file to load and the Access Policies that you want to import.
   To use a file from a local directory (rather than a file on the Server machine), click Upload.

3. Click OK.

Configuration Compliance

Configuration Compliance enables you to audit the platform security of your firewalls and understand weaknesses in a firewall’s configuration (for example, whether the firewall can be accessed using the default password, whether logging is enabled, and whether the management protocol is encrypted).
To analyze Configuration Compliance, you import firewalls and then check their configuration data against a Configuration Policy (a set of Configuration Checks) to see if the firewalls’ configurations comply with the policy. After Skybox analyzes the information, you can view any failed Configuration Checks, with details about each failure.

Note: You can run Configuration Compliance in Firewall Assurance mode or Network Assurance mode. In Firewall Assurance mode, only firewalls in the All Firewalls tree are analyzed; in Network Assurance mode, you can analyze all firewalls in the model.

CONFIGURATION COMPLIANCE OVERVIEW

A Configuration Policy is a set of Configuration Checks, each of which is a regular expression. When a firewall’s configuration data is analyzed, it passes only if the regular expression is matched in the configuration file.

Skybox comes with 2 sets of predefined Configuration Policies.

- **Standard**
  A default set of Configuration Policies that check device configuration files against known best practice guidelines for various platforms.

  This set can be applied to most firewalls automatically. Each Configuration Policy applies to a specific group of firewalls according to the firewall type and other selected properties. For example, there is a policy for Check Point firewalls and a policy for Cisco firewalls.

- **STIG**
  A Security Technical Implementation Guide (STIG) is a cybersecurity methodology for standardizing security protocols to enhance overall security.

  This set is intended for firewalls in organizations that must comply with STIG standards used by the Department of Defense (DoD). It includes those STIG standards that can be verified by analyzing device configuration files. Other standards require manual verification or can be verified by analyzing the access rules.

  Note: Currently, this set includes Configuration Checks for Cisco firewalls and Cisco IOS routers. Additional device types will be added in the future.
You can customize the set of Configuration Checks to be applied to the firewalls, see Customizing a Configuration Policy (on page 61).

There are 2 ways to view the analyzed Configuration Compliance data:

- Per firewall
- For all analyzed firewalls

**VIEWING CONFIGURATION COMPLIANCE PER FIREWALL**

In the All Firewalls tree, you can see all the Configuration Checks analyzed for a firewall and information about any violations found in the firewall’s Configuration Compliance node.

*To view Configuration Compliance for a firewall*

1. Add the firewall to Skybox Firewall Assurance using the Add Firewalls Wizard (if it is not already there) or reimport its data.
2. If an analysis task wasn’t done, select the firewall in the tree and click Analyze on the toolbar.
3. Display Configuration Checks:
   - Click the Configuration Compliance link in the firewall’s Summary page.
   - Select the firewall’s Configuration Compliance node in the Tree pane.
   You can see the list of Configuration Checks applied to the firewall, with their compliance status (✔️ or ✗️).
4. For each Configuration Check, use the Result Details tab to view the expected and actual results of the Configuration Check.

```
<table>
<thead>
<tr>
<th>Checked Configuration: UDP reply packets - filtered</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="General Result Details" /></td>
</tr>
</tbody>
</table>

**Expected Result**

The following pattern should exist in the configuration file:

```
udpReply["\(\[FALSE\]\false)"
```

**Actual Result**

- The pattern was not found in the configuration file

5. (Optional) Select a violation in the Table pane and view it in the configuration file (see page 59).

**VIEWING THE ANALYZED FIREWALLS FOR A CONFIGURATION CHECK**

From the Configuration Policies tree, you can view all the analyzed firewalls for a specific Configuration Check, and drill down to view violation details.
To view the analyzed firewalls for a Configuration Check

1. Select the Configuration Policy that matches the firewalls in which you are interested.

2. If analysis was not done recently, click Analyze on the toolbar.
   The Table pane lists the Configuration Checks in the policy; you can see which checks are violated.

3. Select a Configuration Check.
   The Configuration Check Details page shows information about the check.

4. Click the Analyzed Firewalls tab to view the list of firewalls analyzed for this check.

5. Select a violating firewall to view the violation details in the Details tab.

6. (Optional) View the violation in the configuration file (see page 59) to understand where the violation occurred.

VIEWING VIOLATIONS IN THE CONFIGURATION FILE

You can view configuration violations as they appear in the configuration file.
To view a violation in context

1. Select the violation and click [View Configuration].

The Configuration Files Viewer shows the expected results and the actual results of the tested Configuration Check. It also displays the configuration file in which the violation is found. When possible, the 1st violation instance in the file is highlighted in the file.

2. Do any of the following:
   - Use the **Find** field to search in the file for the violating string (or any other string).

   Note: The Find field searches for simple strings, not for strings expressed as regular expressions.

   - Use the **Go to line** field to navigate to a specific line in the file.
   - If there are multiple violations of this Configuration Check in the file, use **Browse Violations** to move between them.
CUSTOMIZING A CONFIGURATION POLICY

Configuration Policies are displayed under the Configuration Policies node in the Firewall Assurance tree. The predefined folder of Configuration Policies is named Standard.

You can make the following changes:

› Create a Configuration Policy or import a Configuration Policy from a file
› Export Configuration Policies
› Customize a predefined Configuration Policy (or a Configuration Policy that you created or imported) by:
  • Changing its scope (to which firewalls it applies)
  • Modifying its Configuration Checks
  • Adding new Configuration Checks and deleting existing checks
  • Enabling and disabling its Configuration Checks

Configuration Policies

› To make changes to an existing Configuration Policy or to export it, right-click the Configuration Policy and select the appropriate menu item.
› To create or import a Configuration Policy, right-click the Configuration Policies node and select the appropriate menu item.

Configuration Checks

› To make changes to an existing Configuration Check, right-click the Configuration Check and select the appropriate menu item.
› To add a Configuration Check, right-click its policy and select New Configuration Check.
› To test the validity of the regular expression used by a Configuration Check, right-click the Configuration Check and select Configuration Check Test.

Some Configuration Checks might not be relevant for all firewalls that match their policy’s filter; to disable (or enable) any Configuration Check for a specific firewall, right-click the Configuration Check in the Configuration Compliance tab of the firewall and select Disable Configuration Check in this Firewall (or Enable Configuration Check in this Firewall).

Creating and editing Configuration Policies

A Configuration Policy consists of a Configuration Checks to be run on a set of firewalls. The scope of the policy defines the set of firewalls.

Creating a Configuration Policy

To create a Configuration Policy

1 Right-click a policy folder and select New Configuration Policy.

Note: To create a new policy folder, right-click the main Configuration Policies node and select New Policy Folder.
2 Define the policy according to the properties described in the following table.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General</strong></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>A name for the Configuration Policy.</td>
</tr>
<tr>
<td>Description</td>
<td>A description of the Configuration Policy.</td>
</tr>
<tr>
<td><strong>Scope</strong></td>
<td></td>
</tr>
<tr>
<td>Firewall Type</td>
<td>The type of device that this Configuration Policy checks.</td>
</tr>
<tr>
<td>Platform</td>
<td>The device platforms that this Configuration Policy checks.</td>
</tr>
<tr>
<td>Operating System</td>
<td>The device operating systems that this Configuration Policy checks.</td>
</tr>
<tr>
<td>Firewall Scope</td>
<td>The firewalls and firewall folders that are checked by this Configuration Policy.</td>
</tr>
<tr>
<td>Exclude from Scope</td>
<td>Firewalls and firewall folders that match the policy’s scope but are not to be checked against this Configuration Policy.</td>
</tr>
</tbody>
</table>

**Editing a Configuration Policy**

You can redefine the scope of a Configuration Policy at any point. For example, you can exclude specific firewalls that otherwise match the policy’s scope.

**Creating and editing Configuration Checks**

A Configuration Check is a specific test (often in the form of a regular expression) that is run on a firewall’s configuration.

**Scope of Configuration Checks**

You can define the scope of each Configuration Check. The scope can be:

- The entire configuration file
- Specific blocks within the file, in which case you must define the block:
  - Contiguous blocks defined by a start pattern and an end pattern (for example, `^interface` and `^(\!/|[a-z]+)`)
  - Blocks defined by a command prefix (for example, `set interface`)

These blocks might not be contiguous, but all lines starting with the command prefix are considered part of the block.
Creating Configuration Checks

To create a Configuration Check

1. Right-click the desired Configuration Policy node and select New Configuration Check.

2. Type a name for the check and fill in the fields according to Configuration Check properties (on page 63).

Editing Configuration Checks

To edit a Configuration Check, right-click the Configuration Check and select Properties.

If you must make global changes or edit multiple Configuration Checks together, it might be easier to save the Configuration Policy in XML format (rather than XMLX), edit the file, and then reimport it to Skybox.

Configuration Check properties

The properties of Configuration Checks in Skybox Firewall Assurance are described in the following table.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General</strong></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>A name for the Configuration Check.</td>
</tr>
<tr>
<td>Policy</td>
<td>(Read-only) The Configuration Policy to which this Configuration Check belongs.</td>
</tr>
<tr>
<td>ID</td>
<td>(Read-only) The ID of the Configuration Check.</td>
</tr>
<tr>
<td>Type</td>
<td>Set <strong>Type</strong> to <strong>Regular Expression</strong> unless agreed that Skybox Professional Services will create external scripts for more sophisticated testing. For additional information, contact Skybox Professional Services.</td>
</tr>
<tr>
<td>Severity</td>
<td>The severity of the Configuration Check.</td>
</tr>
<tr>
<td>Enable</td>
<td>Specifies whether the Configuration Check is used in policy analysis.</td>
</tr>
<tr>
<td><strong>Search</strong></td>
<td></td>
</tr>
<tr>
<td>Search Scope</td>
<td></td>
</tr>
<tr>
<td>• <strong>Entire Configuration</strong>: Specifies that the entire configuration file is checked for the search string.</td>
<td></td>
</tr>
<tr>
<td>• <strong>For Each</strong>: Specifies that each block of the configuration file is checked for the search string.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>When you select this option, click 🖊 to specify (or edit) the blocks to be used.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: A block is a repeating section in the configuration that has a specific starting pattern and ending pattern.</td>
</tr>
<tr>
<td></td>
<td>For additional information about defining blocks, see Defining blocks for Configuration Checks (on page 65).</td>
</tr>
<tr>
<td>Search for</td>
<td>The regular expression (see page 66) to use as the search pattern.</td>
</tr>
</tbody>
</table>
| Ignore order   | (For multi-line search patterns) Specifies whether the order of the lines matters. In some
### Property | Description
--- | ---
| | cases, the search pattern must be followed exactly; in other cases, provided that each line is found, the order is irrelevant.
| | - Clear this option to check the search pattern against the configuration in the order in which it was entered.
| | - Select this option to check each line of the search pattern against the configuration, regardless of its order in the search pattern.
| **Advanced** | In regular expressions, some characters are intended as special constructs. To control the display of the search string in the **Search for** field, click [✓].
| **Escape Special Characters** | Sets all special characters ("[", ",", "^", ",", ",", ",", ",", ",", ",", ",", ",", ",", "(?", ",", ",", ",", ",", ",", ",", ",", ",")", and ",") in the selected part of the search pattern to literal by adding a "\" before each of them.
| **Reset Special Characters** | Resets all escaped special characters ("[", ",", "^", ",", ",", ",", ",", ",", ",", ",", "(?", ",", ",", ",")", and ",") in the selected part of the search pattern, by deleting the "\" before each of them.
| **View** | Specifies the display mode for the **Search** field:
| | - **Full mode (editable)**: View the regular expression as is, including the "\" preceding special characters that are escaped. Use this view to edit the search pattern.
| | - **Readable mode**: (Read-only) View the regular expression as it appears in the configuration file, without the preceding "\" in front of special characters that are escaped.
| **Violation When** | Specifies whether the Configuration Check is violated when the search pattern is found or when it is not found.
| **Test** | Opens an additional section of the dialog box where you can test the regular expression. For additional information, see **Testing a Configuration Check** (on page 67).
| **Limit Check to Version** | Specifies whether the Configuration Check is run only on specific versions of the device. You must write the version numbers as a regular expression. For more information about regular expressions, see **Regular expressions** (see page 66).
| Note: The device type is specified in the Configuration Policy.
Defining blocks for Configuration Checks

You define blocks in the Blocks Repository Editor, available from the Configuration Check dialog box by clicking in the Search Scope area.

To define a block
1. Click **Create New Block**.
2. Type a name for this type of block.
   You can reuse block definitions in other Configuration Checks.
3. For contiguous blocks:
   a. Select **Separate Blocks**.
   b. Type the **Start Pattern** and **End Pattern** that define each block of this type, using regular expressions as necessary.
4. For blocks defined by a common prefix:
   a. Select **Set of commands with common prefix**.
   b. Type the **Command Prefix** that defines each line of blocks of this type, using regular expressions as necessary.

To edit a block definition
1. Click **Edit Existing Blocks**.
2. Select the desired block definition and click **Edit**.
3. Make the necessary changes to the block definition.
How common prefix blocks are checked
When Skybox checks a configuration file for common prefix blocks, it looks for the common prefix. Lines containing the common prefix are divided according to the entity identifier following the common prefix; each set of lines with a different entity identifier is considered a separate block.

Regular expressions in Configuration Checks
The regular expression language used for Configuration Checks is the Java standard, as explained in http://java.sun.com/javase/6/docs/api/java/util/regex/Pattern.html
The regular expression language permits:

› Simple 1-line expressions
› Multi-line expressions where new lines in the expression defined by the user are interpreted as such
› Multi-line expressions with gaps
   For example, the string ".*" specifies a gap in the expression of several characters or lines

Optimizing regular expressions
Parsing regular expressions might take a long time—we recommend that you optimize the regular expressions used in Configuration Checks. In some cases, this can drastically cut down the processing time. We recommend the following guidelines as a starting point:

› Do not use unnecessary ".*" or "|" constructions. For example, instead of (123|124), write 12(3|4)
› Consider changing ".*" to ".*+

Advanced optimization suggestions
Note: These suggestions are intended for users who are experienced in the use of regular expressions.

› If you know the length of the input string, write \d{<length>}. This expression is internally optimized so that if the input string is not <length> characters long, the engine reports a failure without evaluating the entire regular expression.
› If you want to retrieve everything between one a and the next a in an input string, it is much more efficient to use a([^a]*)a than a(.*)a.
›[^a]*+a is much more efficient than[^a]*a. The former fails faster because after it has tried to match all the characters that are not a, it does not backtrack; it fails immediately.
› Consider using the following lookahead constructions:
   • Positive lookahead: (?=X)
   • Negative lookahead: (?=!X)
   • Positive lookbehind: (?<=X)
   • Negative lookbehind: (?<!X)
Look-around constructions only check forward or backward; they do not change the current position in the input string. Use a positive lookaround if you want the expression to match; use a negative lookaround if you do not want the expression to match.

Testing a Configuration Check

Skybox can test Configuration Checks:

- To verify that the regular expression is valid
- To check whether the regular expression has the expected result

To test a Configuration Check

1. Do either of the following:
   - In the Configuration Check Properties dialog box, click **Test**.
   - Right-click the Configuration Check in the tree and select **Configuration Check Test**.

2. To test the regular expression against a file:
   a. Click the **Browse** button next to the **Configuration File** field.
   b. Select the firewall whose configuration file you want to use for testing and then select the file to test.

   The configuration file data is shown in the text box.

3. To test the regular expression against text: type or paste the desired text in the text box below the **Find** field.
4 Click 

The validity of the regular expression is tested. If it is not valid, an error message is displayed in the Test Results field. If it is valid, the regular expression is tested against the selected text, and the results are shown in the Test Results field. When the regular expression is found in the tested file, it is highlighted in the file data.

5 If necessary, change the search scope and the search string as necessary and keep testing until the expected results are achieved.

You can use the Find field to look for specific patterns in the configuration file. This can be useful to make sure that the absence of the expected pattern is not the reason that the regular expression does not work or to see if you are searching for the correct pattern in the regular expression.

For example, you create a Configuration Check to test for the existence of the pattern “set interface mgmt manage web” in the configuration files of specified types of devices. If this pattern exists in the configuration file, it is a violation—HTTP is being used for web management. You test the pattern against a configuration file that does contain the pattern, but the test result shows that the pattern is not found. You then examine the regular expression to make sure that you copied the pattern correctly. Upon careful examination of the regular expression, you find that you misspelled “interface” or typed “mgt” instead of “mgmt”. You can then fix the mistake in the dialog box, test again, and if it works, fix the Configuration Check.

### Exporting and importing Configuration Policies

You can export Configuration Policies and reimport them later as necessary. This is useful when:

- You want to make changes to the policy:
  - Exporting generates a backup file
  - Global changes might be easier to make in the XML file rather than in the GUI

- Skybox is about to be upgraded and there are changes to the predefined Configuration Policy

  Note: The predefined policy is not upgraded automatically. Rather, the new policy is available as an import so that you can look at both policies and select the policy that better meets your organization’s requirements.

- You are working with multiple Servers and want to copy the policy between them

You can export a single policy folder (that is, a single set of Configuration Policies) or all policy folders in your model. The result of the export is always a single file.

When you import, each selected Configuration Policy is saved separately in the selected folder. Multiple policies with the same name are saved separately; they are not merged.
To export Configuration Policies

1. Right-click the Configuration Policies node or a specific Configuration Policy folder and select Export Configuration Policy.

2. (Optional) Change the name or format of the output file.

   Note: The default format is XMLX (encrypted XML), but if you must make changes to a specific policy outside of Skybox, save the file in XML format.

3. If you want the policies saved on the Manager machine as well, select Save copy to a local directory and select the directory.

   This is useful if you want to copy the policies to another Server.

4. Click OK.

To import Configuration Policies

1. Right-click the Configuration Policies node and select Import Configuration Policy.

2. Select the file to load and the Configuration Policies that you want to import.

   To use a file from a local directory (rather than a file on the Server machine), click Upload.

3. Click OK.

DETECTING VULNERABILITY OCCURRENCES ON NETWORK DEVICES

Skybox can detect vulnerability occurrences on firewalls and other network devices based on their configuration data. This is useful because scanners have limited or no access to firewalls, or it is considered risky to scan them, but it is important to know if there are vulnerability occurrences on these devices that might expose them to attacks.

The following devices are currently supported:

- Arista
- Check Point
- Cisco ASA and FWSM
- Palo Alto
- Juniper NetScreen
- Juniper Junos

1. Import the device’s configuration information via whatever task you usually use for this.

   Note: For Check Point firewalls, the hotfix collection task must be run after the configuration import. See the Check Point Firewall-1 hotfix collection tasks topic in the Skybox Reference Guide.

2. Run an Analysis – Vulnerability Detector for Network Devices task.

   - For information about these tasks, see the Vulnerability detection tasks: device configuration topic in the Skybox Reference Guide.
To view the information, select the `<firewall name> > Configuration Compliance` node in the tree and look at the `Vulnerability Occurrences` tab.
Chapter 4

Optimization and cleanup

Skybox’s Optimization and Cleanup feature can help you to clean up and optimize access rules on a firewall.

- **Shadowing and redundancy** is based on a logical analysis of the firewall’s ACL to find rules that can never be reached and other rules that you can delete without changing the behavior of the firewall.

- **Rule usage analysis** is based on firewall activity logs. It groups rules in the firewall according to the frequency of their usage.

  Rule usage analysis can help you to find rules that are not used but are not included in the shadowing and redundancy analysis. For example, you might find rules whose source or destination no longer exists.

We recommend that you use both analyses to get a complete picture of the optimization status of the firewall’s ACL. However, if activity logs are not available for a firewall for a reasonable period of time, you can use only the shadowing and redundancy analysis.

**Important**: These analyses provide suggestions of rules that you can delete from the firewalls or reorder within the rule chains without affecting the functioning of the firewalls. However, you should make the final decision according to the business requirements of your organization.

In this chapter

- **Shadowing and redundancy analysis** ........................................ 71
- **Rule usage analysis** .................................................................. 75

Shadowing and redundancy analysis

Skybox can analyze the access rules of a firewall to find unused rules or rules that might be unnecessary. This analysis is useful in the following circumstances:

- When auditing a firewall: You can identify inconsistencies in the policy (for example, Allow rules that exist in a rule chain but are shadowed by a Deny rule higher in the chain)

- When trying to optimize or clean up a firewall: You can identify shadowed and redundant access rules and decide whether to delete them

**Shadowed rules** are rules that are never reached because their scope is completely covered by rules above them in the rule chain.

For example, if you have the following 2 access rules in a rule chain, it is clear that the 1st rule grants more access than the 2nd rule, so the 2nd rule is never reached by any packets:
Rule 56: Network A to Network B on any port (any service)
Rule 121: Network A to some locations in Network B on port 21

For shadowed rules, it does not matter whether the action of the 2 rules is the same or different. In the preceding example, the 1st rule’s action could be **Deny** and the 2nd rule’s action could be **Allow**; the 2nd rule is never reached.

**Redundant rules** are rules whose scope is completely covered by rules with the same action below them in the rule chain. Deletion of redundant rule does not change the access behavior of the firewall as any packet that matches the redundant rule matches a rule below it with the same action.

For example, if you have the following access rules in a rule chain:

- Rule 1: Development Network to All Production Application Servers on FTP port, action = Allow
- Rule 2: DMZ to Lab Network port on all ports, action = Deny
- Rule 3: Development Network to Organization Network on all ports, action = Allow

Rule 1 is redundant since its scope is completely covered by rule 3 and both rules have the same action (Allow).

Note that rule 2 does not interfere with the coverage of rule 1 by rule 3 since it relates to a different scope. In general, the redundancy check verifies that the scope coverage is not disrupted by intermediate rules.

**Exceptions**

Implied firewall rule (rules not added explicitly by a user) are not reported as shadowed or redundant.

Any-Any Deny rules at the end of a rule chain are not used in the analysis of redundant rules, as redundancy caused by such rules is usually not an issue.

**SETTING UP SHADOWING AND REDUNDANCY**

**Preparing the analysis information**

To view shadowed and redundant rules, run an **Analysis – Rule Optimization Status** task. You can run the task for specific firewalls and firewall folders, or for all the firewalls in the firewall list. Each time a firewall is updated, the analysis information for that firewall is cleared and you must rerun the task to view the updated information. Schedule the rule optimization status analysis task immediately after the offline file import or online collection tasks that add firewall data to the model.

For information about **Analysis – Rule Optimization Status** tasks, see the Rule optimization status tasks topic in the Skybox Reference Guide.

**WORKING WITH SHADOWED AND REDUNDANT RULES**

After Skybox has analyzed shadowing and redundancy, you can view the resulting data in the **All Firewalls** node of the Firewall Assurance tree or export the data to a CSV file (see page 131).
A good way to start is to look at the **Shadowed Rules** column in the **Firewalls** tab to identify which firewalls have shadowed rules (you can sort the table on that column). There is also a **Redundant Rules** column.

**To view shadowed rules**

1. In the Firewall Assurance tree, under **All Firewalls**, select the required firewall.

2. In the Summary page, in the Optimization and Cleanup pane, click the **Shadowed Rules** link.

The Table pane contains a list of the rules in this firewall that are shadowed (that is, not reached). When you select a shadowed rule, the bottom table lists the rules that shadow (that is, contain) the rule followed by the shadowed rule.

3. Click **Explain** to open a dialog box that displays the shadowed rule next to the shadowing rules in separate panes, to help you to understand how the scope of the shadowed rule is covered by the shadowing rules.

When you click a node in 1 pane, what covers (or shadows) that node is highlighted in the other pane. The icons in the Causes Shadowing pane indicate the type of coverage (identical, containing, or partial coverage) for that node.
4 Close the explanation view.
5 To view the shadowed rule and the rules that shadow it in the context of the rule chain, click **Open in ACL Editor**.

**To view redundant rules**
1 In the Firewall Assurance tree, under **All Firewalls**, select the required firewall.
2 In the Optimization and Cleanup pane, click the **Redundant Rules** link.

The Table pane contains a list of the rules in the firewall that are redundant (that is, covered by other rules below them in the rule chain). When you select a rule, the bottom table lists the selected redundant rule followed by the rules that cause the rule to be redundant.
3 Click **Explain** to open a dialog box that displays the redundant rule next and the rules that cause the redundancy in separate panes, to help you to understand how the scope of the redundant rule is covered by the rules that cause it to be redundant.

When you click a node in 1 pane, it lists what covers (or is covered by) that node in the other pane. The icons in the Causes Redundancy pane indicate the type of coverage (identical, containing, or partial coverage) for that node.

4 Close the explanation view.

5 To view the redundant rule and the rules that cause it to be redundant in the context of the rule chain, click **Open in ACL Editor**.

### Rule usage analysis

Use Skybox rule usage analysis to streamline the process of optimizing access rules and to find the rules and objects in a firewall’s rulebase that are not used.

Rule usage analysis enables you to:

- Optimize access rules
- Make access rules more effective
- Reduce time and labor involved in firewall maintenance
- Generate out-of-the-box audit reports
- Improve the performance of your organization’s firewalls
RULE USAGE ANALYSIS IN SKYBOX

To analyze rule usage information for a firewall, you must set up Skybox to collect the firewall’s activity logs (see Setting up rule usage analysis (on page 76)).

After rules and firewall objects are imported into the model, their usage patterns for specific time frames are analyzed (see Working with rule usage data (on page 77)).

Rule usage analysis for clusters

Although data collection for each firewall of a cluster is currently done separately, firewall clusters are modeled as a single firewall in rule usage analysis.

› Traffic from all cluster members is processed together to provide the hit counts and usage data.
› All cluster members show the same hit counts and usage data.
› Each data collection for a firewall adds the new data to all cluster members.

SETTING UP RULE USAGE ANALYSIS

In Skybox, rule usage data (that is, firewall activity logs) can only be collected for firewalls that are in the model and whose configuration in the model matches the current configuration of the firewall.

The following firewall types are supported for rule usage analysis:

› Check Point FireWall-1 (R75 or higher)
› Cisco PIX/ASA/FWSM
› Cisco IOS
› Juniper Networks Junos
› Juniper Networks NetScreen
› Fortinet FortiGate
› Palo Alto Networks
› Stonesoft (McAfee) StoneGate
› McAfee Enterprise (Sidewinder)

To set up Skybox for rule usage analysis

1 Update the firewall.
   • For firewalls that are not in the model: Add the firewall to the model using the Add Firewalls Wizard or the relevant task (see the Firewall configuration tasks chapter in the Skybox Reference Guide).
   • For firewalls that are in the model: Update the firewall using Import Configuration or the relevant task.

2 Configure and run a task for collection of activity logs.
   • For all supported firewall types, you collect the log data from the relevant syslog server. For information about how to collect this log data, see the Syslog traffic event collection tasks topic in the Skybox Reference Guide.
• For Check Point FireWall-1 firewalls, you can collect the log data from the 
  FireWall-1 Management Server instead of from the syslog server. For 
  information about how to collect this log data, see the Check Point 
  FireWall-1 LEA collection tasks topic in the Skybox Reference Guide. This 
  method requires configuring access to the Management Server.

Note: For Cisco firewalls, rule usage data can be collected directly from 
the firewall collection task by selecting Collect hit counts (and hit counts 
are collected automatically if you use an Import – Directory task and 
include the output of the show access-list command). However, the 
information collected does not include actual usage data.

Best practice for collecting rule usage data

Rule usage data is collected from log files that store data about traffic through a 
firewall (or other device). As the data is read from the log files it is processed; 
only information relevant for rule usage analysis is stored as part of the model. 
These log files are often very large and processing them can take some time. We 
recommend that you set up a scheduled task to collect the logs every night 
(when there is less demand on the Server); set the Collection Period field of 
the task to Last Day.

Note: You can collect logs from up to 3 months (100 days) ago.

Clearing rule usage data

If you are no longer interested in seeing the current rule usage data, you can 
remove it from the display.

To clear rule usage data

1 Right-click the firewall or folder for which you do not want to see the current 
  rule usage data.

2 Select the data to clear:

• Select Optimization and Cleanup > Clear Rule Usage Data >
  Clear Rule Usage and Trace Data to clear the regular rule usage data (hit 
  counts) and the actual rule usage data (addresses and ports that were 
  used).

• Select Optimization and Cleanup > Clear Rule Usage Data >
  Clear Only Trace Data to clear only the actual rule usage data.

Note: New rule usage data is shown for the firewalls the next time the online 
collection task runs and new data is collected.

WORKING WITH RULE USAGE DATA

After Skybox has collected the rule usage data, you can view the data from the 
All Firewalls node of the Firewall Assurance tree or generate a Rule Usage 
Analysis report.

When the rule usage patterns are analyzed (during data collection), each access 
rule and each firewall object in the model is assigned a usage type based on its 
usage patterns (hit count) over the period for which data was collected, by 
comparing the access rules in the model with the data in the log.
Usage types

The following usage types are assigned to access rules (for hits during the analysis period):

- Unused: The rule had no hits.
- Used: The rule had hits and all objects referenced in the rule had hits.
- Contains Unused Objects: The rule had hits, but some objects referenced in the rule had no hits.
- Not Logged: No hit count is available for the rule. The rule could be logged, but logging is disabled in the firewall configuration.
- Unloggable: Access rules that cannot be logged. These are implicit rules and rules entered manually in Skybox.

The following usage types are assigned to objects (for hits during the analysis period):

- Unused: The object had no hits.
- Unused in Some Rules: The object is used in at least 1 rule and unused in at least 1 rule.
- Used: The object is used in all rules that reference it.
- Not Logged: No hit count is available for the object.

Note: This usually refers to objects that are referenced by implicit rules only or by rules for which logging is disabled.

You can change the minimum usage thresholds for rules and objects so that **Unused** means that the number of hits is less than a specified threshold (rather than meaning no hits). These thresholds are specified in the **Rule-base analysis properties** section of `<Skybox_Home>\server\conf\sb_server.properties`, as described in the following table.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>rule_unused_threshold</td>
<td>The threshold of number of hits; less than this number of hits, access rules are considered unused. You can specify the threshold as a percentage of the total rule hit count (for example, <code>rule_unused_threshold=10%</code>). The default value is 0.</td>
</tr>
<tr>
<td>object_unused_threshold</td>
<td>The threshold of number of hits, less than this number of hits, firewall objects are considered unused. You can specify the threshold as a percentage of the total object hit count (for example, <code>object_unused_threshold=10%</code>). The default value is 0.</td>
</tr>
</tbody>
</table>

Viewing rule usage data

There are 2 levels of rule usage data: regular (hit count) data and actual usage data, which includes information about which addresses and ports included in an access rule were used. For information about viewing actual usage data, see the following topic (on page 80).
To view rule usage data for a firewall

1. In the Firewall Assurance tree, under All Firewalls, select the desired firewall.

2. In the Summary page, at the right-hand side of the Optimization and Cleanup pane, click.

The pane expands to display a pie chart displaying the usage patterns for the firewall’s access rules and tables with links to groups of rules and objects (for example, unused rules, rules with unused objects, and objects unused in some rules).

3. Click a link in a table to view the selected data in the Rule Usage tab (for rule links) or the Object Usage tab (for object links). You can also switch to these tabs directly.

   - The Rule Usage tab shows the firewall’s access (and NAT) rules grouped by their usage type.
     
     This tab includes a Shadowed column that specifies whether an access rule is unused is because it is shadowed (completely covered) by a rule that is above it in the rule chain.

     Note: Shadowing information is not displayed until an Analysis – Rule Optimization Status task is run (see Shadowing and redundancy analysis (on page 71)).

   - The Object Usage tab shows the firewall’s firewall objects grouped by object type and then by usage type.
4 When you select a rule in the **Rule Usage** tab, you can see the objects used by that rule in the Object tree in the right-hand pane.

5 To toggle the grouping in the **Rule Usage** and **Object Usage** tabs, right-click a column heading and select **Group by Column** or **Don’t Group by Column**.

*To view the rules that reference a firewall object*

- In the **Object Usage** tab, right-click the firewall object and select **Show Referencing Rules**.

The list of access rules for the firewall appears. Rules that reference the selected object (whether the object is used or not) are displayed in boldface. Select an access rule to see its objects in the Object tree.

*To view the referencing rules when the firewall object is not used*

- In the **Object Usage** tab, right-click the firewall object and select **Show Unused Rules**.

The list of access rules for the firewall appears. The rules that reference the selected object but in which the object had no hits are displayed in boldface.

**Viewing actual usage data**

If you collected actual usage data from the firewall logs, you can see detailed information for each access rule—which of the addresses and ports listed in the rule (source, destination, or services) were used.

**Note:** By default, actual usage data is collected for rules that have **Any** in their Source, Destination, or Service.
The information is displayed in the **Actual Rule Usage** column and is available for used rules and rules containing unused objects.

The **Actual Rule Usage** column shows what percentage of the addresses and ports included in the access rule were used (that is, the percentage of addresses and ports out of all those used in the rule that had hits). The icons indicate how critical the rule is in terms of actual usage. Best practice for access rules is that they expose the minimum number of addresses and ports possible. Rules that have very little usage are good candidates for tightening (changing the rule to permit access only via addresses and ports used). Rules that have wider usage might need some tightening, but not as much.

**Viewing object usage within a rule**

When viewing a rule with actual usage data, the Object tree shows the hit counts of objects for the selected rule.

Usage data is available for source, destination, and port objects. For firewalls that support users and applications (for example, Palo Alto Networks firewalls), usage data is also available for user and application objects.

You can click an object in the Object tree to view additional information about that object in the Details pane.

**Viewing actual rule usage details**

When you select a rule in the **Rule Usage** tab, the Details pane shows the actual usage, according to addresses in the access rule’s source and destination, and ports in the services, as found in the firewall activity log. The objects are listed in hierarchical order. For firewalls that support applications and users, these are also displayed in the Details pane.

You can show all actual usage or filter the display to show only poor usage (that is, rules that probably need more urgent tightening).
Unsynchronized hit counts

Sometimes, the hit counts in the Rule Usage and Object Usage columns and those in the Actual Rule Usage column (and the Details pane) are not the same. There are 2 reasons for this:

- The collection periods differ, since rule usage data is collected on a regular basis, while collection of actual usage data is often less frequent
- The methods used for counting the hits are different

Changing the analysis time frame

When you analyze rule usage on a firewall, all the collected rule usage data for the firewall is displayed; you can focus on a specific analysis time frame.

To change the analysis time frame

1. In the tree, right-click the Optimization and Cleanup node of the firewall and select Rule Usage Period.
2. Specify the analysis time frame:
   - Select a predefined time frame.
   - Select Custom and define the time frame.
3. Click Okay.

Viewing data collection coverage

When you are analyzing hit patterns for a firewall’s access rules, it is useful to know how many times data was collected, so that you can understand whether the hit counts are a real reflection of traffic in the network. For example, if you are looking at hit counts for the past month, but data was only collected twice within that month, the rule usage data is not a very reliable indicator.

For the selected analysis period, you can view all the dates on which no data was collected and all the dates on which data was collected.

To view collection coverage

- With the Rule Usage or Object Usage tab selected, click the Missing Collection Dates link at the top-right side of the workspace.

The Coverage of RUA Collection dialog box appears.

![Coverage of RUA Collection during All Available Dates](image)

<table>
<thead>
<tr>
<th>Coverage</th>
<th>Dates</th>
<th>Total Days</th>
</tr>
</thead>
<tbody>
<tr>
<td>No RUA data was collected</td>
<td>4/1/13 - 6/9/13, 6/10/13 - 12/25/13</td>
<td>259</td>
</tr>
<tr>
<td>RUA data was collected</td>
<td>4/10/13</td>
<td>1</td>
</tr>
</tbody>
</table>

Usage Data Available: 4/10/13 - 6/10/13
**Best practice for analyzing rule usage data**

The following are some tips to remember when analyzing rule usage data.

**Frequency of data review**

Although you should collect log data every day, you can review the data less frequently. We recommend that you review the data at a frequency between every week and every 3 months. If you wait longer between reviews, it is hard to accurately analyze the usage data, as rules used a year ago might no longer be used.

**Unloggable rules**

Unloggable rules are not enabled for logging on the firewall. You should enable logging for most of the rules, so that Skybox can analyze their usage patterns. If logging many rules on a regular basis is too resource intensive, enable them at least 2 weeks before each audit or optimization session, so that you have enough data for an accurate analysis.

**Deleting unused rules**

Before you delete an unused rule from the firewall, try to understand why the rule is unused. Rules might be unused because they are no longer necessary or because they were specifically created to deal with emergency situations that did not occur during the time frame under analysis. Do not delete unused emergency rules.

**Deleting unused objects**

The **Summary** tab includes a list of unused objects and a list of objects that are used in some rules but not used in others. Often, you can optimize the rulebase by deleting the objects that are not used in any rule.

If an object is used in only a few rules (and is unused in many rules), perhaps you can rewrite the rules that use the object so that the object is no longer necessary and you can delete it from the Skybox database. You can ascertain which rules use an object by looking at the difference between **Show Referencing Rules** and **Show Unused Rules**.

**Rule Usage Analysis reports**

Rule Usage Analysis reports present rule usage information for firewalls to help you to understand the usage patterns of the access rules. These reports present all firewalls in the selected scope that have unused access rules or access rules with unused objects.

You can generate a report for a single firewall.

**Note:** These reports do not include actual rule usage data. This information can currently be exported only in CSV format.
To generate a report for a single firewall

1. In the Firewall Assurance tree, navigate to the desired firewall.
2. Right-click the **Optimization and Cleanup** node and select **Rule Usage Analysis Report**.
   - For information about the properties of Rule Usage Analysis reports, see the Rule Usage Analysis reports topic in the Skybox Reference Guide.

In the Report Properties dialog box, the **Network Scope** is set to the selected firewall and the **Analysis Period** is set to the current analysis period.

3. You can change the analysis period for the report and the format of the report.
4. Click **Generate Now**.
   The report is generated and displayed in a separate window.

   **Device: main FW [192.169.1.1]**

   **Activity time:** 1/21/07 - 1/23/07

   **Note:** The requested analysis period exceeds the time period for which usage data is available.

   **Total number of rules:** 17

   **Device Description:** External Firewall connected to the Internet and Partners

   ![Pie chart showing rule usage](chart.png)

   - Not Logged  - Contains Unused Objects  - Unused

   **Rules Summary**

<table>
<thead>
<tr>
<th>Rules</th>
<th>Unused</th>
<th>Contains Unused Objects</th>
<th>Not Logged</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1</td>
<td></td>
<td>3</td>
<td>7</td>
</tr>
</tbody>
</table>

   **Objects Summary**

<table>
<thead>
<tr>
<th>Objects</th>
<th>Unused</th>
<th>Unused in Some Rules</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1</td>
<td></td>
<td>14</td>
</tr>
</tbody>
</table>

You can generate Rule Usage Analysis reports manually in the Reports workspace or on a specific schedule using a **Report – Auto Generation** task.

You can export rule usage analysis data to a CSV file:

- Manually (**File > Export Table to CSV**; see Exporting model data (on page 131))
- By using a CSV – Optimization and Cleanup Export task
Chapter 5

Change tracking

Change tracking in Skybox helps you to keep track of changes implemented on firewalls. When you use change tracking, Skybox saves the changes so that you can review the history of access rules whenever necessary.

Users can sign up for alerts on new changes and can receive reports on changes that occurred during a selected tracking period.

In this chapter

- Change tracking overview .................................................... 85
- Setting up change tracking .................................................. 86
- Viewing changes ..................................................................... 88
- Viewing the history of an access rule ..................................... 90
- Change Tracking reports ...................................................... 90
- Recovering lost changes ........................................................ 91
- Reviewing and reconciling changes ....................................... 92

Change tracking overview

Each time a firewall’s configuration is collected, you should run a change tracking task to check for differences between the previous configuration file and the current file. These differences are stored in Skybox as changes.

The following changes are recorded by Skybox:

- New access rule or object
- Deleted access rule or object
- Changed field in access rule or object
- Timestamps and users who made the changes (via syslog change events)

By default, only changes from the last 7 days are displayed; you can change this value.

You can view the changes for all firewalls, a folder of firewalls, or a specific firewall. When you view access rules in the Access Control List Editor, the history of each access rule is available.
Setting up change tracking

Each time a firewall’s configuration data is collected, the raw data is stored as a configuration file. The change tracking feature works by comparing the configuration file of the current data collection with the configuration file of the previous data collection.

**Analysis – Change Tracking** tasks compare between the 2 files and create change records inside Skybox. You can select the firewalls to include in the comparison and the frequency of the task. We recommend that you collect data and analyze change tracking on a regular basis, as frequently as required. You can create task sequences (see page 110) to run all the necessary tasks.

For additional information about **Analysis – Change Tracking** tasks, see the Change tracking tasks topic in the Skybox Reference Guide.

**Change tracking using syslog events**

You can use a **Change Tracking Events – Syslog Import** task to import changes to access rules and objects from syslog events for the following firewalls and firewall management systems:

- Juniper Networks Junos
- Juniper Networks NetScreen
- Fortinet FortiGate
- Cisco PIX/ASA/FWSM
- Palo Alto Networks
- Palo Alto Panorama

These tasks create a partial change record for every change event reported by syslog. These partial change records provide near real-time change tracking but contain only the minimal information available in syslog about each change (including the timestamp for the change and who made the change).

After additional data collection, the next time an **Analysis – Change Tracking** task is run, the partial change records are completed with access rule information from the configuration files—each change record now includes the change time and changed by information from syslog and the other information available from the configuration file.

**Note:** If the global unique identifier (GUID) of an access rule is changed, it cannot be matched to the full change record. In some devices (for example, Palo Alto Networks and Junos), the rule name is used as the GUID.

For additional information about **Change Tracking Events – Syslog Import** tasks, see the Syslog change events collection tasks topic in the Skybox Reference Guide.

**Change tracking for Cisco devices using hit counts**

You can retrieve the hit counts for the access rules of Cisco firewalls when you collect or import the firewall configuration data:
Select **Collect hit counts** in the task properties of a *Firewalls – Cisco PIX/ASA/FWSM Collection* task or a *Routers – Cisco IOS Collection* task.

If you import the configuration data using an *Import – Directory* task and include the output of the `show access-list` command, hit counts are collected automatically as part of the import.

If hit counts are collected, rule usage analysis is available immediately; you do not need to run a *Change Tracking Events – Syslog Import* task.

### Change tracking for Check Point devices using audit log events

You can use a *Change Tracking Events – Check Point Audit Log Collection* task to import changes to access rules and objects on Check Point devices. These tasks create a partial change record for every change event reported by the audit log. These change records provide near real-time change tracking, but contain only the minimal information available in the audit log about each change (including the timestamp for the change and who made the change).

After additional data collection, the next time an *Analysis – Change Tracking* task is run, the partial change records are filled in with full access-rule before and after views from the configuration files. At this point, each change record includes the accurate change time and changed by information and all the other information available from the configuration file.

For additional information about *Change Tracking Events – Check Point Audit Log Collection* tasks, see the Check Point FireWall-1 change events collection tasks topic in the Skybox Reference Guide.

### Limitation on number of changes

In general, if the change tracking task detects more than 100 changes on a firewall, it does not create each change separately in the model, but rather creates 1 change record stating “major access list change”. Usually, such a large number of changes indicates a major change to the firewall or a reorganization of the firewall policy, and users would not want to view every change separately. However, there are 2 cases where it might be necessary:

- If you need to see every change to make sure that it is correct
- If there are other reasons (in your system) why many changes could happen in a short time (for example, a change to an object that is used in more than 100 access rules)

In these cases, you can modify the number of changes that must occur for each change to be listed separately.

**To change the limitation on the number of changes to be added separately**

1. In `<Skybox_Home>\server\conf\sb_server.properties`, find the property `change_tracking_access_list_change_limit`.
2. Increase the value of this property according to the size of your firewall and the complexity of the firewall objects.
3. Rerun the task for the firewall in question and see if you get the desired results (that is, separate change records).
Viewing changes

After firewall changes are analyzed, you can view the changes.

To view changes to the firewalls

1. In the tree, select All Firewalls and look at the Change Tracking section of the Summary page.
   
   You can see whether changes to any of the firewalls were found.

   Note: If you are using the Change Reconciliation feature, the Change Tracking section also includes a breakdown of authorized, unauthorized, and pending changes. For information about change reconciliation, see Reviewing and reconciling changes (on page 92).

2. The change tracking period is the period for which changes are displayed. Depending on what you want to see and the frequency of data collection and change tracking, you can change the tracking period (see page 89).

3. View a graph of the changes by expanding the Change Tracking area (click ). You can change the graph’s frequency using the drop-down list.

4. Click the link in the Total Changes field to see a list of all the changes.

When you select a change, you can see additional information in the Details pane. If the change involves an object, the **Affected Access Rules** tab lists all access rules affected by the changes in this object.
5 Click the **Changes by Firewall** tab to view a summary of changes per firewall.

The Details pane contains a list of changes for the selected firewall.

**To view changes for a single firewall**

▷ In the tree, select the firewall’s **Change Tracking** node.

You can see all the changes for the selected firewall that occurred during the selected change tracking period.

The Details pane contains information about the selected change. For new or deleted access rules or objects, their properties are displayed. For changed entities, there is a before-and-after view of the change.

- If the changed entity is an object, you can see its affected access rules (in the **Affected Access Rules** tab).
- If the change was originally detected via syslog, you can see the original syslog messages (in the **Log Messages** tab).

To view all the changes between the current and previous configurations in the context of the raw configuration files, right-click the firewall’s **Change Tracking** node and select **Compare Current Configuration to Previous**.

**CHANGING THE TRACKING PERIOD**

You can change the tracking period for which changes are displayed.

**To change the tracking period**

▷ Click the link in the change tracking summary section, in its expanded view.
Right-click a folder or firewall and select *Change Tracking > Change Tracking Period*.  
Right-click the *Change Tracking* node of a firewall and select *Change Tracking Period*.

Viewing the history of an access rule

You can view the history of changes for a specific access rule, including changes in objects related to the access rule.

*To view the history of changes to an access rule*

1. Select the *Rule Review* node of the firewall for which you want to see changes.
2. Double-click the desired access rule to open its Properties dialog box and click the *Change Tracking* tab.

Note: For firewalls where the access rules do not have a unique ID (for example, Cisco firewalls), no history is available. No history is available for implied rules (displayed with a green background in the Access Control List Editor) either, for the same reason.

Change Tracking reports

Change Tracking reports present change tracking information about firewalls to help you to understand the changes in the firewall objects and access rules. These reports present all firewalls in the selected firewall scope that have changes.

You can generate a Change Tracking report for a single firewall directly from the Firewall Assurance tree.
To generate a report for a single firewall

1. In the Firewall Assurance tree, navigate to the required firewall.
2. Right-click the Change Tracking node and select Change Tracking Report.
   
   In the Report Properties dialog box, the Firewall Scope is set to the selected firewall and the Tracking Period is set according to the Tracking Period specified in the GUI.

3. Click Generate Now.

   The report is generated and displayed in a separate window.

<table>
<thead>
<tr>
<th>#</th>
<th>Change Time</th>
<th>Rule ID</th>
<th>Source</th>
<th>Destination</th>
<th>Services</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>141</td>
<td>2/1/12 11:21 AM</td>
<td>28</td>
<td>guy_machines</td>
<td>192.168.100.3</td>
<td>tcp_all</td>
<td>✔️</td>
</tr>
<tr>
<td>142</td>
<td>2/1/12 11:21 AM</td>
<td>33</td>
<td>Partner_Nets</td>
<td>net_g1</td>
<td>GRE/Any, UNKNOWN/Any</td>
<td>✔️</td>
</tr>
<tr>
<td>130</td>
<td>2/1/12 11:19 AM</td>
<td>28</td>
<td>guy_machines</td>
<td>192.168.100.3</td>
<td>tcp_1 tcp_all</td>
<td>✔️</td>
</tr>
<tr>
<td>131</td>
<td>2/1/12 11:19 AM</td>
<td>33</td>
<td>Partner_Nets</td>
<td>net_g1</td>
<td>OSPF/IGP/Any, UNKNOWN/Any</td>
<td>✔️</td>
</tr>
</tbody>
</table>

You can generate Change Tracking reports manually from the Reports workspace or on a specific schedule using a Report – Auto Generation task.

For information about creating report definitions and working with reports, see the Working with reports section in the Skybox Reference Guide.

For information about the properties of Change Tracking reports, see the Change Tracking reports topic in the Skybox Reference Guide.

Export to CSV

You can export changes to a CSV file:

- Manually (right-click the Change Tracking node and select Export to CSV – Change Tracking Data)
- By scheduling a CSV – Change Tracking Export task

Recovering lost changes

Skybox provides a utility that compares 2 firewall configurations from the past. This is useful for cases when change tracking analysis was not done between imports, so some configuration data was lost.

Example

- change_tracking -host_name "Main-FW" -format fw1_conf -current \temp\current 090820140000 Standard -baseline \temp\baseline 08082014000 Standard
This command creates changes for a firewall named **Main-FW** by comparing the FW1 configuration in \temp\current to the configuration in \temp\baseline. The current configuration is from 9 Aug 2014 and the baseline is from 8 Aug 2014. Both configurations use the **Standard** rulebase.

For additional information, see [Change tracking utility](on page 135).

### Reviewing and reconciling changes

You can review the change records to determine whether changes make sense. For example, that they connect a user to a service; are not too permissive; or were requested by someone in your organization. There are 3 levels in this process:

- **View the list of changes** (on page 88).
  - Make sure that you do not see anything that looks ‘wrong’.

- **Review each change record** (on page 93).
  - Look at the details
  - View the ticket ID extracted from the access rule or firewall object
    In some organizations, the ticket ID of the relevant change request is added to the access rule as a comment by the firewall administrator who makes the change; this is helpful in the review process.
  - Change the status (to authorized, unauthorized, pending, or ignored), and write a comment explaining why you did or did not authorize the change

- **Reconcile the changes with Skybox tickets** (on page 95), providing documentation for each change.
  - This step requires Skybox Access Change tickets. You can create these tickets using Skybox Change Manager or by importing external tickets to Skybox (see [Prerequisite for change reconciliation](on page 94)).
  - Reconciling changes enables you to associate tickets with changes, so that you can see which ticket ‘caused’ each change.

The goal of reviewing the firewall changes in Skybox is to check that each change was authorized (and provide supporting documentation, if required), and to report any unauthorized changes.

### SETTING UP CHANGE REVIEW AND RECONCILIATION

All change review and reconciliation options are disabled by default.

To set up the feature you must:

1. Enable the feature.
2. Analyze change tracking.
To enable the change reconciliation feature

1. From the Tools menu, select **Options > Server Options > Change Tracking Settings**.

2. To enable extraction of ticket IDs from the comments of access rules and firewall objects during offline file import or online collection of firewall data:
   a. Select **Extract Ticket ID**.
   b. By default, Skybox searches for a 5-digit number in the **Comment** field of each access rule and firewall object found in the configuration file and (if found) extracts this number as the ticket ID. If there is a different way of representing ticket IDs in your organization, change the regular expression in the **Ticket ID Regex** field.

3. To enable automatic matching between firewall changes and change requests in Skybox tickets:
   a. Select **Enable Change Reconciliation**.
   b. Specify how the matching is done and whether changes are only authorized if they have matching Skybox tickets (see the Change Tracking Settings topic in the Skybox Installation and Administration Guide).

To analyze change tracking

- Run the **Analyze Firewall Changes** task.
- Select **All Firewalls** and click **Analyze**.

REVIEWING THE CHANGES

When the Change Reconciliation feature is enabled, each change imported to Skybox is assigned a status:

- **Pending**: This is the default status for new changes before any matching is performed
- **Authorized**: Changes that are authorized by the **Analyze Firewall Changes** task or by a user
  Changes that have 100% coverage from Skybox tickets are authorized by the task.
- **Unauthorized**: Changes that are defined as unauthorized by a user or by the **Analyze Firewall Changes** task.
  The task assigns this status to changes that are older than 14 days and in **Pending** status.
Ignored: Changes that are not supported

To review the changes for a firewall

1 In the tree, select the firewall’s Change Tracking node.

You can see all the changes for the selected firewall that occurred during the selected change tracking period, including the extracted ticket ID for each change (if there is a ticket for the change).

2 For each pending change, see if you can tell whether it should be authorized or unauthorized.

3 If the change includes a specific ID in the Extracted Ticket ID field, you can look up the change request in your organization’s ticketing system and see whether the change made is the same as the change requested.

4 Update the status of a reviewed change:
   - Right-click the change and select Set Status; change the status and add a comment; click OK.

PREREQUISITE FOR CHANGE RECONCILIATION

Change reconciliation in Skybox is done by matching Skybox tickets with changes to access rules and firewall objects based on IP addresses and ports. To use change reconciliation, you must have tickets in Skybox that include the IP addresses and ports that are changed in the access rule.

Note: Change reconciliation uses Access Change tickets only.

Skybox tickets documenting change requests can be created in:
Skybox using Skybox Change Manager (see the Submitting change requests section in the Skybox Change Manager User’s Guide).

An external system and added to the model using the API (see the Tickets API chapter in the Skybox Developer’s Guide).

COVERAGE OF CHANGES

Skybox provides information about:

- How much of the change (recorded in the change record) is fulfilling a change request in the system

  This is important information for auditors, because changes to access rules should only be made if they are requested. Changes that are much wider than the request might leave your organization’s network at unnecessary risk.

  For example, if the change permits access from a partner’s network to a specific network in your organization but the change request is limited to 10 machines in the partner’s network, then only a small percentage of the change is fulfilling the change request.

- How much of the requested change (in the ticket) is covered (that is, fulfilled) by the actual change (as recorded in the change record)

  For example, if the requested change is access to specific internal servers from a partner network over a specific port and the actual change only provided this access to 2 of the partner’s machines rather than all of them, only a certain percentage of the request is fulfilled by the change.

The Ticket Coverage icon indicates how the change and the change requests relate to each other. The dark area in the icon represents the change request; the white area represents the change.

- If the dark area fully covers the white area, then the whole change was requested.
- If the dark area partially covers the white area, then the change is wider than the request.
- If the dark area has sections that do not overlay the white area, the change implements only part of the request.

Note: It is possible that several changes were made that, taken together, implement the change request.

RECONCILING CHANGES

Automatic reconciliation

When the automatic matching options for change tracking are enabled (see Setting up change review and reconciliation (on page 92)), matching between change records with Pending status and Closed or Resolved tickets (that is, tickets whose requested changes were already made) is done automatically:

- Using the Change Tracking task
- When you click [Analyze] to analyze the firewall ad hoc
If the matching tickets provide 100% coverage for a change, the change is authorized automatically. All other changes are left with Pending status and must be reconciled manually.

Note: If Authorized changes must have tickets is enabled, changes are not authorized unless there is a ticket that provides 100% coverage for the change.

Manual reconciliation

To reconcile changes manually

1. Look at each change listed in the Table pane and use the Change Reconciliation tab in the Details pane to see which tickets Skybox matched with it, including the percentage of coverage.

2. If the percentage of coverage provided by the matching tickets is satisfactory, you can authorize the change (with the change selected, click Set Status).

3. If there are no matching tickets or if the coverage found by the automatic process is not complete:
   a. Click Reconcile.
      
      Information about the change record is displayed at the top of the Reconcile dialog box; all Closed or Resolved tickets whose last change is within the time frame specified in Date Filter are listed at the bottom. The best matches are at the top of the list, and tickets that are already matched with this change are marked.

      Note: You must change the date filter if the tickets are older.

   b. Mark additional tickets and clear marked tickets as relevant.
   c. To mark the change as Authorized or Unauthorized in addition to saving the changes to the list of matched tickets, click Save & Set Status.
Note: If you see a change that you can authorize but it has no matching ticket to back it up, you can create a ticket for it later and then match the new ticket with the existing change. This could occur if an urgent change is approved quickly without opening a ticket.
Chapter 6

Rule review and recertification

Rule review and recertification is a process by which firewall administrators verify periodically that the firewalls access rules are still relevant and compliant with the organization’s policies. The recertification process is started by opening a recertification ticket on an access rule; after the ticket is opened, the process is managed in Skybox Change Manager.

In some organizations, this process is ad hoc; in some, it involves a more formal workflow. Skybox can support both ad hoc and formal workflows, and any combination thereof.

In this chapter

Overview of rule review and recertification ............................. 98
Reviewing a rule ................................................................. 99
Business attributes ............................................................ 100
Recertification ................................................................... 101
Starting the recertification process manually ......................... 102
Automatic update of next review dates ................................. 102
Automatic ticket creation for rules needing review ................. 103

Overview of rule review and recertification

Rule review is a process that checks firewall access rules and decides whether they meet the organization’s standards or need modification.

There are several ways to do rule review:

▷ Manual (ad hoc) rule review
  Associative review of rules; check rule compliance, changes, and usage without taking formal actions

▷ Automatic recertification workflow
  1. Create policies specifying how often rules should be reviewed. For example, unused rules with critical violations should be reviewed every 6 months. These rules are then flagged for review in Skybox 6 months after they are added to Skybox or since their last certification.
  2. Create policies for automatic ticket creation for rules needing review and recertification. The tickets are then managed in Change Manager.
  3. Run the policies automatically on a regular basis.
Any mixture of manual and automatic
For example, review all the rules from 1 firewall and manually create a recertification ticket or manually update their next review date.

Reviewing a rule

The Rule Review table includes:

- **Next Review Date**: The next time that the rule needs to be reviewed. If you sort by this field, you can find items that have passed their review date.

Updating the next review date can be automated—you can create rules to automatically provide new review dates (see page 102).

- **Last Certified Date**: When each rule was last certified. Rules with no last certified date were never certified in Skybox.

- **Recertification Status** for each access rule, where you can track the ticket’s progress, even if it is managed in Skybox Change Manager. Statuses include:
  - **None**: This rule has never been through the recertification process
  - **In Progress**: This rule has an open ticket and is waiting for recertification
  - **Rejected**: This rule was a candidate for recertification, but was rejected
  - **Certified**: This rule was recertified

Note: There can only be one recertification process (that is, ticket) open on an access rule at one time. However, you can request another round of recertification on a rule that was already rejected or certified.

When you select an access rule in the Rule Review table, you see the highlights of the rule’s compliance in the **Highlights** tab of the Details pane.

Click a link in the Compliance section of the highlights to display the details in the Access Rule Properties dialog box. This dialog box provides the information that you might need when reviewing the rule. For information about the fields of an access rule, see the Access rule properties: rule review section in the Skybox Reference Guide.
In the Business Attributes section, you can see the rule’s business attributes (see page 100) (if the information was added), including the owner, business function, and next review date.

Business attributes

Business attributes are business information about access rules that can be stored with the access rule in the model. Business attribute information must be added manually, but you can add it for multiple rules at a time. This information is useful when reviewing the access rules for certification.

Note: Business attributes are accessible anywhere access rules are displayed in Firewall Assurance.

Skybox includes the following business attributes for access rules:

- Owner
- Email
- Business Function
- Next Review Date
- Comment
- Ticket ID

Administrators can create additional (custom) business attributes for their organization (on page 101).

To view the business attributes of an access rule

- In a list of access rules, right-click the desired rule and select Set Business Attributes.

Note: You can view attributes for multiple rules, but if the rules have different values for any of the attributes, those values are not visible when you view them together.
To set or edit the business attributes of selected access rules

1. In a list of access rules, right-click the rules and select **Set Business Attributes**.
2. Make the necessary changes.

   Note: If any rules have different values for any attribute, you cannot see the current values for that attribute. If any rules have a different **Next Review Date**, you cannot change the review date value until you click **X** in this field.

### ADDING CUSTOM BUSINESS ATTRIBUTES

If there is additional information that should be stored for each rule, administrators can define custom business attributes. The attributes are added to each access rule; users can work with these attributes in the same way that they work with predefined attributes.

**To add custom attributes**

1. From the **Tools** menu, select **Options > Server Options > Business Attributes > Access Rules**.
2. For each attribute that you want to add:
   a. In the Custom Fields section, click **Add**.
   b. In the **Field Title** field, add a name for the attribute.
   c. In the **Field Type** field, select the type of the attribute.

### Recertification

Skybox Firewall Assurance supports a scalable process for rule recertification. When doing rule recertification:

- Each rule has full supporting information for recertification, including compliance, usage data, and change history, as explained in **Reviewing a rule** (on page 99).
- Each rule can have additional attributes containing administrative metadata (for example, owner and business function), as explained in **Business attributes** (on page 100).
- You can review the access rules on an ad hoc basis or you can create policies that set the next review date for each rule, based on compliance and usage data, as explained in **Automatic update of next review dates** (on page 102).
- You can create tickets **manually** (see page 102), or rule recertification ticket policies can create tickets automatically based on the next review date, as explained in **Automatic ticket creation** (on page 103).
- After tickets are created, Change Manager is used for reviewing the rules and either recertifying or modifying the rules. For additional information, see the Rule recertification topic in the Skybox Change Manager User’s Guide.
Starting the recertification process manually

To request recertification (open a ticket)

1. In the Rule Review table, right-click the access rule or rules that you want to recertify and select Recertify Rule.

2. In the New Rule Recertification Ticket dialog box:
   a. Select an owner for the ticket.
   b. Select the recertification workflow. Usually, the workflow names describe their purpose.
   c. If necessary, change the priority.
   d. If you selected a single access rule, you can change the suggested title of the ticket and the description.

3. Click OK.

A ticket is created. If the access rules have multiple owners, a separate ticket is created for each owner that includes only that owner’s rules. If any of the selected rules are already in the recertification process, no ticket is created for them. The pop-up message contains links to all the new tickets, as well as links to existing tickets for rules that are already in the recertification process.

Note: If you want to see the IDs of the tickets that determined the certification or rejection status of the access rules, you can display the Ticket ID column in the table (right-click any column header, select Customize Current View, and then select Ticket ID. For tickets that are in progress, this is the current ticket.

Automatic update of next review dates

Access rules should be reviewed on a regular basis, but not all rules need the same review schedule. You might decide to review critical rules 3 months after certification, but medium rules only after a year. Administrators can create policies specifying how often to review different types of access rules, and then run these policies to update the next review date of the relevant access rules.

Automatic update of next review dates involves 3 steps:

1. Create the necessary rule review policies (see page 103).

2. Initialize the last certification date (see page 103) of all rules that are to be automatically reviewed.

3. Set up a task of type Policy Rule Review to run the rule review policies on a regular basis.

   For additional information, see the Policy rule review tasks topic in the Skybox Reference Guide.
CREATING RULE REVIEW POLICIES

To create a rule review policy

1. Open the Skybox admin tool by clicking on the toolbar.
3. Fill in the fields according to the Rule review policies topic in the Skybox Reference Guide.

INITIALIZING THE LAST CERTIFICATION DATE

Rule review policies work by checking the last certification date of access rules. However, access rules that were not yet certified within Skybox do not have a last certification date. For the rule review policies to work, you must initialize the last certification dates for all firewalls to which you want to apply rule review policies.

Note: You only need to do this once per firewall.

You can initialize all firewalls with the same date, or use different dates for specific firewalls and folders. You can initialize to the current date or to any date in the past.

To initialize the last certification date for firewalls

1. In the Firewall Assurance tree, right-click All Firewalls or the folder or firewall that you want to initialize, and select Rule Review > Initialize Certification Date.
2. In the Set Last Certification Date field, select a date.
3. Specify which access rules to initialize: either all rules, or only those that were created before a specified date.

Only access rules whose recertification status is None are initialized.
4. Click OK.

Automatic ticket creation for rules needing review

Rule recertification ticket policies enable Skybox to automatically create rule recertification tickets for any access rules that are about to reach their next review date and meet the other criteria in the policy.

Automatic ticket creation involves 3 steps:
1. Create and run rule review policies or update next review dates manually.
2. Create the necessary rule recertification ticket policies.
3. Set up a task of type Ticket – Auto Generation to run the policies on a regular basis.

For additional information, see the Ticket creation tasks topic in the Skybox Reference Guide.
CREATING NEW RULE RECERTIFICATION TICKET POLICIES

To create a Rule Recertification Ticket Policy

1. Open the Skybox admin tool by clicking on the toolbar.
3. Fill in the fields according to the Rule recertification ticket policies topic in the Skybox Reference Guide.
Intrusion prevention systems

Skybox Firewall Assurance offers the following information regarding IPS coverage of your organization:

- Overall signature coverage from Palo Alto Networks devices per new threats reported over a period of time and threat level
- Information about signatures in prevention mode vs. detection mode so that you can understand the actual coverage provided by the IPS device in the context of the network architecture
- Signatures (in prevention mode or detection mode) correlated against critical vulnerability occurrences that exist in your organization using Skybox Vulnerability Control

You can then make informed decisions about which signatures to change from detection mode to prevention mode, and which signatures to deactivate.

Information is provided per IPS-enabled device.

Viewing IPS information

Skybox Firewall Assurance provides IPS information for Palo Alto Networks firewalls. This information is displayed as at the bottom of the summary page of these firewalls, in the IPS pane.

2 types of information are available:

- Signature coverage of vulnerability occurrences in your organization: The coverage of vulnerability occurrences found in your organization by signatures activated on the device
  
  Note: If you are working with a Firewall Assurance-only license and are not using vulnerability occurrences, the signature coverage section shows general information about the IPS signatures on the device rather than coverage of the vulnerability occurrences found in your organization.

- New threat coverage by signature: The coverage of new threats (Vulnerability Definitions) by signatures activated on the device.

At the top of the pane, there is a link to the list of IPS signatures that are active on the device.

![IPS](image)
The list of signatures is divided into groups according to their enabled status (protect or detect).

When the model includes vulnerability occurrences, these groups list protected and detected signatures that are relevant to your organization, and there is a 3rd group that shows enabled (protect or detect) signatures that are not relevant to your organization.

Note: For Firewall Assurance-only licenses, administrators can enable display of vulnerability occurrences (if vulnerability occurrence data was collected) on the Tools > Options > Server Options > Change Manager Settings > Risk Assessment page.

VIEWING IPS INFORMATION WITH VULNERABILITY OCCURRENCES

Signature coverage of vulnerability occurrences

When your organizational model includes vulnerability occurrences, the following information is displayed on the left-hand side of the pane:

- IPS signature coverage of active signatures in correlation to the vulnerability occurrences in the model, including a link.
- A chart and table that link to the lists of relevant, active Prevent and Detect signatures, and relevant disabled signatures.

The links open the list of IPS signatures with the selected section displayed.
Recent Threat Coverage

The right-hand side of the pane shows coverage of new threats (Vulnerability Definitions) by active signatures in the device. You can modify the time frame to view and the CVSS threshold of the Vulnerability Definitions.

Clicking a link opens the relevant list of Vulnerability Definitions. For each Vulnerability Definition, you can see information about the Vulnerability Definition itself, the IPS status (Active Prevent, Active Detect, or Disabled) of the signatures covering the Vulnerability Definition, and the signature or list of signatures that cover it.
VIEWING IPS INFORMATION WITHOUT VULNERABILITY OCCURRENCES

Recent Threat Coverage

When the organizational model does not include vulnerability occurrences, the left-hand side of the pane shows coverage of new threats (Vulnerability Definitions) by active signatures in the device. You can modify the time frame to view and the CVSS threshold of the Vulnerability Definitions.

Clicking a link opens the relevant list of Vulnerability Definitions. For each Vulnerability Definition, you can see information about the Vulnerability Definition itself, the IPS status (Active Prevent, Active Detect, or Disabled) of the signatures covering the Vulnerability Definition, and the signature or list of signatures that cover it.

Signature Coverage

The following information is displayed on the right-hand side of the pane:

- Total vendor signatures available on the device
- Activated signatures on the device
- A chart and table that link to the lists of active Prevent signatures, active Detect signatures, and disabled signatures of both types.
Chapter 8

Auditing firewalls on a continuous basis

You can automate the audit process when the firewall configuration is imported directly from the firewall (or management system) by running the online collection tasks and the analysis on a regularly scheduled basis to keep the information up-to-date. This is best done using task sequences (see page 110).

You can also set up collection and analysis of recently changed firewalls (see page 109). Use this for:

› Change tracking
  • See the full firewall change tracking events on a regular basis
  • Authorize changes quickly using change reconciliation

› Policy compliance
  • Have an up-to-date picture of your firewall compliance level

Note: You can set notifications to alert on a new firewall violation.

In this chapter

Triggered collection and analysis ............................................... 109
Task sequences ................................................................. 110
Scheduling tasks and task sequences ..................................... 113
Monitoring task results ......................................................... 114
Triggers ............................................................................... 115

Triggered collection and analysis

Triggered collection and analysis uses task sequences. The sequences differ in which collection and analysis tasks they include, but the idea is that some of or all the tasks are set to run only on firewalls that are new or firewalls that have recent changes.

For example:

› When working with firewalls for which logs are collected, Skybox starts by collecting the logs from the specified firewalls. In the next step, Skybox can check each firewall to see if there are changes in its log, and only collect configuration data from firewalls with configuration changes (found in the logs). Afterwards, the firewall analysis tasks (change tracking, policy
compliance, and shadowed and redundant rules) can be set to analyze only the firewalls with recent changes. This type of task sequence is much faster than running the tasks on all the firewalls, and can be run as often as needed.

For nightly collection and analysis tasks, firewall management collection tasks can be set to collect and analyze only new firewalls.

Task sequences

You can define task sequences, where each task in the sequence runs as soon as a previous task ends. This is useful when you often want to run a set of tasks in a specific order.

You can use separate task sequences for different purposes (for example, data collection and maintenance), different parts of the system, and different frequencies.

A task sequence can include task groups. The tasks in a task group are run in parallel.

For information about tasks, see the Tasks part of the Skybox Reference Guide.

CREATING TASK SEQUENCES

A task sequence is an ordered set of tasks where each task (or task group) in the sequence depends on the outcome of another task. If the outcome of the previous task is not what you specified, the next task is not launched. For example, you can make the Analyze Firewall Policy Compliance task dependent on a task that imports data from several firewalls and completes with a status of Success: if the import completes with any errors that prevent it from having the Success status, the Analyze Firewall Policy Compliance task is not launched.

Subsequent tasks that depend on a task that was not launched are also not launched. If, in the previous example, the Generate Firewall Compliance Report task is the next task in the sequence and it is scheduled to run after the Analyze Firewall Policy Compliance task completes, it does not run.

Note: Before you create a task sequence, you must define the tasks to run in the sequence.

For information about creating task sequences for triggered collection and analysis of firewalls, see the following topic (on page 111).

To create a task sequence

1 On the Operational Console toolbar, click New Task Sequence.
2 In the New Task Sequence wizard:
   a. Type a Name for the sequence.
   b. Select Basic.
   c. Click Next.
3 Add the 1st task or task group:
   a. Click Add.
b. In the Add Task dialog box, select a task to add to the sequence and click **OK**.

4 For each subsequent task you are adding to the task sequence, do the following:
   a. Click **Add**.
   b. In the Add Task dialog box, select a task to add to the sequence and click **OK**.
      
      A dependency is created so that this task is run after the previous task (in the list) finishes.
   c. To change either the triggering task or the exit codes of the triggering task, click the task in the list and click **Edit**.

   Note: A single task can only be used once per task sequence. However, you can use different tasks of the same type in a task sequence.

5 Click **Next**.

The Firewall Filters screen enables you to change the firewall filter values of the firewall collection or analysis tasks in your task sequence. If there are no tasks of these types, all the parameters are disabled. If there are tasks of any of these types, you can keep the original firewall filters for the tasks or change the set of firewalls on which the tasks are to run (to recently changed firewalls or new firewalls).

6 If your task sequence includes any firewall collection or analysis tasks, you can modify the values.

7 Click **Next**.

8 **Schedule the task sequence** (see page 113) to run as often as necessary.

9 Click **Finish**.

**Creating similar task sequences**

After a task sequence for a set of tasks is created, you can use it as a template for similar task sequences: Right-click the task sequence and select **Create Task Sequence Like**.

**CREATING TRIGGERED COLLECTION AND ANALYSIS TASK SEQUENCES**

The following types of firewalls and firewall management systems are supported in these sequences:

- Juniper Networks Junos
- Juniper Networks NetScreen
- Fortinet FortiGate
- Cisco PIX/ASA/FWSM
- Palo Alto Networks
- Palo Alto Panorama
- Check Point
To create a task sequence for triggered collection and analysis

1 On the Operational Console toolbar, click New Task Sequence.
2 In the New Task Sequence wizard, type a Name for the sequence.
3 In the Type field, select Firewalls – Triggered Collection and Analysis.
4 Click Next.

The Log Collection screen is used to select the log collection tasks to run as part of this task sequence.
5 Type a name for the group of log collection tasks.
6 Click Add and select the desired tasks.
7 Click Next.

The Firewall Collection screen is used to select the firewall collection and management collection tasks to run as part of this sequence.
8 Type a name for the group of firewall collection tasks.
9 Click Add, and select the desired tasks.
10 Define the exit codes for the log collection task group that cause the firewall collection task group to run.
11 Define the firewall filter for the collection tasks. This enables you to override the filter in each collection task as to which firewalls are to be collected. The default for triggered collection, Recently changed firewalls, means that the collection tasks only run on firewalls on which changes are found in their logs.

Note: The original filters in the tasks are not changed. When the tasks are run individually, the original filters are used.

12 Click Next.

The Firewall Analysis screen is used to select the analysis tasks to run as part of this sequence.
13 Type a name for the group of firewall analysis tasks.
14 Click Add, and select the desired tasks.
15 Define the exit codes for the firewall collection task group that cause the firewall analysis task group to run.
16 Define the firewall filter for the analysis tasks.
17 Set the schedule for the task sequence.
18 Click Finish.

VIEWING AND EDITING TASK SEQUENCES

To view task sequences

1 In the Operational Console tree, select Tasks > Task Sequences.
2 Select a task sequence.

Tasks in the sequence are listed in the Table pane and general information or messages from the last run of the selected task in the Details pane.
Editing task sequences
You can add tasks to and remove tasks from a sequence and change the order of
the tasks in the sequence and the exit conditions for the triggering task.

To edit a task sequence

› Right-click the task sequence in the tree and select Properties.

TASK GROUPS
You can group a set of tasks together so that you can run them as part of a task
sequence (see page 110).
When you create a task group, Skybox creates a separate folder for it, where you
can view and edit the list of tasks in the group.

Note: You can only run a whole task group as part of a task sequence.
Otherwise, you must launch or schedule each task separately. When run as part
of a task sequence, the tasks in a task group run in parallel.

To create a task group
1 On the Operational Console tree, right-click Task Groups.
2 In the New Task Group dialog box:
   a. Type a name for the group.
   b. In the User Comments field, type a description of the group.
   c. To select tasks to include in this group, click the Browse button next to
      the Tasks field.
   d. Click OK.
      A folder for this group is added under the Task Groups node.

Scheduling tasks and task sequences
You can define a task or a task sequence so that it runs at scheduled times (for
example, on Sundays at 5 p.m. and Wednesdays at 4 a.m., on the 15th and 28th
of every month, or every 15 minutes). Although tasks and sequences are usually
scheduled to run on the Live model, you can schedule them to run on any model.

To schedule a task or task sequence
1 Navigate to the task or sequence in the Operational Console tree.
2 Right-click the task or sequence and select Properties.
3 In the <Task name> Properties dialog box, click the Schedule tab.
4 For each schedule (for example, the 1st of every month or every Sunday):
   a. Click **Add**.

   ![New Task Schedule](image)

   - b. Select a time slice and fill in the corresponding fields.
   - c. If the task is to run a limited number of times, select **End after** and type the number of times that you want the task to run.
   - d. If necessary, in the **Model** field, change the model on which the task runs.
   - e. Click **OK**.

   The new schedule is added to the list of schedules for this task.

5 Click **OK**.

   Note: If auto-launch is not enabled for a task, it does not run on its specified schedules. However, it does run as part of a task sequence.

---

**To view scheduled tasks and sequences**

- In the Operational Console tree, select **Tasks > Schedules**.

   Defined schedules are listed in the Table pane and the scheduled entities are listed in separate tabs (**Tasks** and **Sequences**) in the Details pane.

---

**Monitoring task results**

**Task messages**

After running a task, you can check the task results to make sure that the outcome is what you expected. For example, after updating firewall configurations (using tasks), check the task results to confirm that all data was properly imported into Skybox. Check for failed tasks; if a task failed, find out why it failed, make the necessary changes, and rerun the update task for the failed firewall.

You can see a list of tasks that failed in the Operational Console window, at **Tasks > Failed Tasks**. For each task, you can see the messages from the task’s most recent run.
Task alerts
You can set up Skybox to send email alerts to various users for failed tasks. You can configure global settings and also configure specific settings in the task properties of a specific task. By default, tasks alerts are sent for each task that runs. However, if you do not want task alerts sent for a specific task, you can disable them in the task properties.

To configure global task alerts
1 Select Tools > Options > Server Options > Task Settings > Task Alert Settings.
2 Do any of the following in the Email to field:
   • Type the email addresses to which alerts are to be sent.
     Multiple addresses must be comma-separated, with no space between the comma and the following address.
   • Click the Browse button; select Skybox users who are to receive alerts and add the external email addresses of other desired recipients.
     All alerts are sent to each specified recipient.
3 Modify the following as necessary:
   • Email on: The exit codes on which to send task alerts.
   • Messages Count: The maximum number of messages from the failed task to include in the task alert.
4 Click OK.

Triggers
Skybox Firewall Assurance supports sending email notifications when there are specific changes to a firewall. A trigger is a rule that defines the changes for which these alerts are created and sent.

The email message includes information about the changes. For example, when you run the Analyze Firewall Changes task, Skybox checks whether there are any change tracking triggers and whether any of the new changes match these rules.

Firewall compliance violation notifications
Firewall compliance violation notifications indicate new policy violations for a firewall. For example, if an access test for a firewall that was previously compliant with the Access Policy now becomes a violation, the owner of that firewall receives a notification. New firewall violations might mean that a recent change to an access rule on the firewall is problematic.

Firewall compliance violation notifications are created when Analysis – Policy Compliance tasks are run and new violations (that meet the trigger criteria) are found.
Change tracking notifications

Change tracking notifications indicate changes to the access rules and objects of a firewall. These notifications are created when Analysis – Change Tracking tasks are run and new changes (that meet the trigger criteria) are found.

Skybox Change Manager ticket notifications: Requests for firewall changes

Skybox also supports sending notifications on tickets created and managed in Skybox Change Manager. These tickets include requests for changes to firewall access rules and objects. In addition to sending notifications, it is also possible to trigger a script to run as a Skybox task.

For additional information, see the Creating notifications topic in the Change Manager User’s Guide.

CREATING TRIGGERS

To create a trigger

2. In the Skybox Admin window, right-click Triggers and select New Trigger.
3. In the New Trigger dialog box, select the Trigger Type and fill in the fields according to the relevant table in the Skybox Reference Guide:
   - Firewall compliance violation trigger properties
   - Change tracking trigger properties
4. Click OK.

   Email notifications are triggered and sent according to the selected properties.
Chapter 9

Advanced topics

This chapter describes various advanced topics in Skybox Firewall Assurance.

In this chapter

Reports ............................................................................ 117
Searching for access rules................................................... 132
Other ways to import data offline ......................................... 135
Change tracking utility ....................................................... 135
Cisco configuration diffs ...................................................... 137
Addresses behind network interfaces ................................. 138
Multi-zone interfaces .......................................................... 142

Reports

Reports in Skybox are detailed accounts of specific data in the model (for example, compliance violations or firewall changes). You can schedule reports to run at specific times and be sent to specified Skybox users.

You can generate reports for single firewalls from the Firewall Assurance workspace, but you work with reports for multiple firewalls in the Reports workspace.

ACCESS CHECKS REPORTS

Skybox includes Access Checks reports that display information about the Access Checks in your Access Policy. These reports list all Access Checks in your Access Policy or those in a specified scope. The Access Checks are grouped by policy section.

Overview reports list the Access Checks in table format, with basic information about each Access Check. Detailed reports list the Access Checks in table format and, separately, detailed information about each Access Check.

There is 1 predefined overview report of the Access Checks, named Policy Document.
To generate an Access Checks report

1. Open the Reports workspace.
2. In the Tree pane, click Reports.
   
   The properties of the report are displayed in the workspace.
   
   - For information about the properties of Access Checks reports, see the Access Checks reports topic in the Skybox Reference Guide.
4. Click Generate.
   
   You are asked whether to generate the report in the background or in the foreground. As it can take some time to generate the report, it is often useful to generate in the background and keep working.
5. Select a generation method (background or foreground) and click OK.
   
   If the report is generated in the background, you can double-click Currently 1 task is running in the status bar to open the Operational Console and follow the task’s progress (using the displayed messages).
   
   A report based on the current Access Policy is generated from the report definition. When generation finishes, the report is displayed in the workspace.

You can change the format of a report (to HTML or RTF) and change the scope of the report to include only specific policy folders or policy sections. You can create definitions for additional reports. For additional information about reports, see the Working with reports section in the Skybox Reference Guide.

ACCESS COMPLIANCE REPORTS

Skybox includes Access Compliance reports that provide policy-related information about specified firewalls. These reports help you to understand the compliance status of your policy as applied to each of the specified firewalls and to identify problematic access configuration in the firewalls. You can use them to decide whether to make changes in the Access Policy or in the firewalls themselves.
What’s in an Access Compliance report

The 1st section of the report displays a summary of Access Compliance for firewalls in the scope of the report, followed by links to information about each analyzed firewall.

1. Summary

Average Compliance for Firewalls in Scope: 44%

Number of Firewalls in Scope: 7 Firewalls
Number of Compliant Firewalls: 6 Firewalls
Number of Non-Compliant Firewalls: 2 Firewalls
Number of Uncalculated Firewalls: 5 Firewalls

Breakdown of Access Tests and Violations

- 45% Successful Access tests
- 20% High Violations
- 30% Medium Violations
- 4% Critical Violations

Firewall Compliance

<table>
<thead>
<tr>
<th>Firewall</th>
<th>Compliance Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>prod FW [192.170.33.31]</td>
<td>29%</td>
</tr>
<tr>
<td>main FW [192.168.1.1]</td>
<td>59%</td>
</tr>
<tr>
<td>dev FW [192.170.1.1]</td>
<td>No Data</td>
</tr>
<tr>
<td>ops FW [192.170.1.33]</td>
<td>No Data</td>
</tr>
</tbody>
</table>
The rest of the report is per firewall. For each firewall, the report includes a linked list of policy sections with their compliance, followed by a linked list of violating access rules for each policy section, information about each Access Check, and a list of Access Checks violated by that access rule.

3. Firewall: main FW

IP Address: 192.159.1.1
Compliance Percentage: 59%
Number of Violating ACLs: 10
Number of Violations: 40
Number of Exceptions: 1
Number of ACL Rules: 20

Policy Sections

<table>
<thead>
<tr>
<th>Section Name</th>
<th>Source</th>
<th>Destination</th>
<th># Violating ACLs</th>
<th>Compliance Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>NIST-Internal Servers to DMZ</td>
<td>Internal Servers</td>
<td>DMZ Zones</td>
<td>3</td>
<td>0%</td>
</tr>
<tr>
<td>NIST-Partner to DMZ</td>
<td>Partner Zones</td>
<td>DMZ Zones</td>
<td></td>
<td>0%</td>
</tr>
<tr>
<td>NIST-Internal Servers to External</td>
<td>Internal Servers</td>
<td>External Zones</td>
<td></td>
<td>0%</td>
</tr>
<tr>
<td>NIST-Partner to Partner</td>
<td>DMZ</td>
<td>Partner</td>
<td></td>
<td>0%</td>
</tr>
<tr>
<td>NIST-External to DMZ</td>
<td>External Zones</td>
<td>DMZ Zones</td>
<td></td>
<td>0%</td>
</tr>
<tr>
<td>NIST-External to Internal Servers</td>
<td>External Zones</td>
<td>Internal Servers Zones</td>
<td></td>
<td>0%</td>
</tr>
<tr>
<td>NIST-DMZ to Internal Servers</td>
<td>DMZ Zones</td>
<td>Internal Servers Zones</td>
<td></td>
<td>0%</td>
</tr>
<tr>
<td>NIST-Partner to Internal Servers</td>
<td>Partner Zones</td>
<td>Internal Servers Zones</td>
<td></td>
<td>0%</td>
</tr>
</tbody>
</table>

3.1. Violating ACLs for firewall main FW

All violating ACLs found for main FW firewall, grouped by policy sections.

Section: NIST-Internal Servers to DMZ

<table>
<thead>
<tr>
<th>#</th>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Violation Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Development_Net</td>
<td>Any</td>
<td>Any</td>
<td>7</td>
</tr>
<tr>
<td>2</td>
<td>Finance_Net</td>
<td>Any</td>
<td>Any</td>
<td>7</td>
</tr>
<tr>
<td>11</td>
<td>Internal</td>
<td>app1</td>
<td>ftp</td>
<td>2</td>
</tr>
</tbody>
</table>

ACL #1

Original ID: 1
Source: Development_Net
Destination: Any
You can include a list of the violations or access tests, a list of the access rules defined on the firewall, and a list of exceptions relevant for the firewall.

### Section: NIST-Internal Servers to DMZ

<table>
<thead>
<tr>
<th>APR Name</th>
<th>Test ID</th>
<th>Source</th>
<th>Destination</th>
<th>Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Block ICMP Replaying Messages</td>
<td>5000</td>
<td>int15 (192.168.1.1, Internal Servers)</td>
<td>int2009 (192.170.1.97, DMZ)</td>
<td>ICMP, 0/ICMP, 4/ICMP, 11/ICMP, 12/ICMP</td>
</tr>
<tr>
<td>Block Small Services</td>
<td>5119</td>
<td>int15 (192.168.1.1, Internal Servers)</td>
<td>int2009 (192.170.1.97, DMZ)</td>
<td>37/TCP, 37/UDP, - time, 1-20/TCP, 1-20/UDP</td>
</tr>
<tr>
<td>Block X-Windows</td>
<td>5553</td>
<td>int15 (192.168.1.1, Internal Servers)</td>
<td>int2009 (192.170.1.97, DMZ)</td>
<td>0/0/0-0/255/TCP</td>
</tr>
<tr>
<td>Block Login Services</td>
<td>5973</td>
<td>int15 (192.168.1.1, Internal Servers)</td>
<td>int2009 (192.170.1.97, DMZ)</td>
<td>22/TCP, - winet, 22/TCP, - ssh, 125/TCP, 129/UDP, - pwgen, [512/TCP], - exec, [515/TCP], ...</td>
</tr>
<tr>
<td>Block Trojan and Worm Ports</td>
<td>5817</td>
<td>int15 (192.168.1.1, Internal Servers)</td>
<td>int2009 (192.170.1.97, DMZ)</td>
<td>4553 [21227/TCP, 21317/TCP], accessschema, [240/12/TCP], agent, 4041, [500/TCP:4041/TCP], ...</td>
</tr>
<tr>
<td>Block Miscellaneous</td>
<td>5767</td>
<td>int15 (192.168.1.1, Internal Servers)</td>
<td>int2009 (192.170.1.97, DMZ)</td>
<td>[2060/TCP, 1089/UDP], - socks, [119/TCP], - ntp, [122/UDP], - rtp, [101/TCP, 101/UDP], - smtp, [182/UDP], ...</td>
</tr>
<tr>
<td>Block Computer Network Services</td>
<td>8486</td>
<td>int15 (192.168.1.1, Internal Servers)</td>
<td>int2009 (192.170.1.97, DMZ)</td>
<td>[111/TCP, 111/UDP], - suripc, [2046/TCP, 2043/UDP, 100000/RPC], - nfs, nlockmgr, ...</td>
</tr>
<tr>
<td>Limited Access Services (10 ports)</td>
<td>8552</td>
<td>int15 (192.168.1.1, Internal Servers)</td>
<td>int2009 (192.170.1.97, DMZ)</td>
<td>Any</td>
</tr>
</tbody>
</table>

### Generating Access Compliance reports

To generate an Access Compliance report

1. Open the Reports workspace.
2. In the Tree pane, click Reports.
3. Select Public Report Definitions > Firewall Compliance and then select a report definition.
4. Click Generate.

   The time to generate a report varies according to the number of firewalls and their complexity.

You can change the scope of predefined reports or create additional report definitions; for example, you can have a separate report definition for each firewall that you are auditing or separate reports for access rules and exceptions. You can schedule reports to run at specific times and be sent to designated recipients. For additional information, see the Working with reports section in the Skybox Reference Guide.

For additional information about Access Compliance reports, see the Access Compliance reports topic in the Skybox Reference Guide.

You can export Access Compliance data to a CSV file:

- Manually (File > Export Table to CSV; see Exporting model data (on page 131))
- By using a CSV – Compliance Results Export task
FIREWALL ASSURANCE REPORTS

Skybox includes Firewall Assurance reports that provide a complete overview of the state of firewalls in the network. These reports can include any combination of the following topics: compliance for Access and Rule Policy, Configuration Compliance, Optimization & Cleanup, and Change Tracking.

Note: Detailed Firewall Assurance reports can provide very large amounts of data. We recommend that you include a limited set of firewalls in each report (for example, a firewall folder, or all firewalls of a specific type or at a specific location).

What’s in a Firewall Assurance report

If the report is generated for a specific folder (including All Firewalls), the 1st section includes summary information similar to that displayed in the Summary page of a firewall folder.

1 Folder Summary for All Firewalls

1.1 Policy Compliance

Access Compliance

<table>
<thead>
<tr>
<th>Compliant</th>
<th>Non-Compliant</th>
<th>Unanalyzed</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>3</td>
<td>1</td>
</tr>
</tbody>
</table>

Rule Compliance

<table>
<thead>
<tr>
<th>Critical</th>
<th>High</th>
<th>Medium</th>
<th>Low</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

1.2 Configuration Compliance

Compliance

Rule Compliance

<table>
<thead>
<tr>
<th>#</th>
<th>Firewalls with Critical Violations</th>
<th>Firewalls with High Violations</th>
<th>Firewalls with Medium Violations</th>
<th>Firewalls with Low Violations</th>
<th>Firewalls with Info Violations</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

1.3 Optimization and Cleanup

Analysis Period: All Available

<table>
<thead>
<tr>
<th>Rule Usage</th>
<th>#</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full Usage</td>
<td>0</td>
</tr>
<tr>
<td>Partial Usage</td>
<td>1</td>
</tr>
<tr>
<td>Unanalyzed</td>
<td>9</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Shadowed and Redundant Rules</th>
<th>#</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewalls with Shadowed Rules</td>
<td>2</td>
</tr>
<tr>
<td>Firewalls with Redundant Rules</td>
<td>2</td>
</tr>
</tbody>
</table>

1.4 Change Tracking

<table>
<thead>
<tr>
<th>Change Tracking</th>
<th>Results for:</th>
<th>All Available</th>
</tr>
</thead>
<tbody>
<tr>
<td>Changed Firewalls</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>Total Changes:</td>
<td>94 (31 Rules, 63 Objects)</td>
<td></td>
</tr>
<tr>
<td>Available Change Dates:</td>
<td>10/28/11 - 7/15/12</td>
<td></td>
</tr>
</tbody>
</table>

The 2nd section is a feature summary that includes a table for each feature in the report. Each row in a feature table displays information about a single firewall.

The rest of the report is divided by firewalls. For each firewall, the report includes some of or all the following information, depending on the sections selected in the report definition:
Basic information about the firewall and overview information about the selected features:

- Policy compliance overview: Access Compliance and Rule Compliance
- Configuration Compliance overview
- Optimization and Cleanup overview
- Change Tracking overview

Detailed information about the selected features

If you select the Details report level in the report properties, there is a separate section in the report for each firewall, which includes all the selected details. When working with Details reports, you can filter according to the details of each feature that you want to see. If there are more than a specified number of firewalls (Advanced > Split if scope greater than), the details section for each firewall is generated as a separate file, with a link from the main report. This prevents details reports from becoming unreasonably large.
Generating Firewall Assurance reports

To generate a Firewall Assurance report

1. Open the Reports workspace.
2. In the Tree pane, click Reports.
3. Select Public Report Definitions > Firewall Compliance and then select a report definition.
4. Click Generate.

The time to generate a report varies according to the number of firewalls and their complexity.

You can change the scope of predefined reports or create additional report definitions; for example, you can have a separate report definition for each firewall that you are auditing or separate reports for access rules and exceptions, or for each desired feature. You can schedule reports to run at specific times and be sent to designated recipients. For additional information, see the Working with reports section in the Skybox Reference Guide.

For additional information about Firewall Assurance reports, see the Firewall Assurance reports topic in the Skybox Reference Guide.

FIREWALL CHANGES REPORTS

Skybox includes Firewall Changes reports that provide information about changes to firewalls in the network. The firewalls’ access rules and objects are compared between 2 different models (usually Live compared with What If or Live compared with Forensics) and any changes are listed in the report.
What’s in a Firewall Changes report

The 1st section of the report displays a linked list of the changed firewalls in the scope of the report with a summary of their changes, and a list of the unchanged firewalls.

Active model: Live

Compared to: What if

Number of Changed Firewalls: 3 out of 12 firewalls in scope

<table>
<thead>
<tr>
<th>Changed Firewalls</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall Name</td>
</tr>
<tr>
<td>main_FW [192.170.1.97]</td>
</tr>
<tr>
<td>prod_FW [182.170.33.1]</td>
</tr>
<tr>
<td>vseb-pix [10.41.1.2]</td>
</tr>
<tr>
<td><strong>Total</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Unchanged Firewalls</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall Name</td>
</tr>
<tr>
<td>dev_FW [192.170.1.1]</td>
</tr>
<tr>
<td>finance_FW [192.170.1.66]</td>
</tr>
<tr>
<td>Internal Router [192.170.8.2]</td>
</tr>
<tr>
<td>L2_FW [192.170.22.200]</td>
</tr>
<tr>
<td>noc_FW [192.170.1.33]</td>
</tr>
<tr>
<td>PA-2020:vse1 [172.20.0.251]</td>
</tr>
<tr>
<td>PA-2020:vse2 [172.170.0.251]</td>
</tr>
<tr>
<td>Partner1_FW [200.160.1.3]</td>
</tr>
<tr>
<td>Skynest_Router [10.40.0.2]</td>
</tr>
</tbody>
</table>
The rest of the report is divided by firewalls. For each firewall, the report includes a summary of the changes to access rules and objects, and then lists of the changed access rules and changed objects with their main properties.

### New ACLs

<table>
<thead>
<tr>
<th>#</th>
<th>Orig ID</th>
<th>Source</th>
<th>Destination</th>
<th>Services</th>
<th>Action</th>
<th>Direction</th>
<th>Rule Chain</th>
</tr>
</thead>
<tbody>
<tr>
<td>28</td>
<td>guy_machines</td>
<td>192.108.100.3</td>
<td>top_1 top_all</td>
<td></td>
<td></td>
<td>inbound</td>
<td>ACCESS</td>
</tr>
</tbody>
</table>

### Changed Access Rules

<table>
<thead>
<tr>
<th>#</th>
<th>Orig ID</th>
<th>Source</th>
<th>Destination</th>
<th>Services</th>
<th>Action</th>
<th>Direction</th>
<th>Rule Chain</th>
</tr>
</thead>
<tbody>
<tr>
<td>30</td>
<td>Any</td>
<td>Any</td>
<td>icmp_p1</td>
<td></td>
<td></td>
<td>inbound</td>
<td>ACCESS</td>
</tr>
<tr>
<td>32</td>
<td>Outside_Nets</td>
<td>Any</td>
<td></td>
<td>1-05535</td>
<td></td>
<td>inbound</td>
<td>ACCESS</td>
</tr>
<tr>
<td>33</td>
<td>Partner_Nets</td>
<td>net_p1</td>
<td>OSPF/GP/Any, UNKNOWN/Any</td>
<td></td>
<td></td>
<td>inbound</td>
<td>ACCESS</td>
</tr>
<tr>
<td>34</td>
<td>10.0.0.0/16</td>
<td>inside Nets</td>
<td>TCP/Any, UDP/Any</td>
<td></td>
<td></td>
<td>inbound</td>
<td>ACCESS</td>
</tr>
</tbody>
</table>

### Deleted ACLs

<table>
<thead>
<tr>
<th>#</th>
<th>Orig ID</th>
<th>Source</th>
<th>Destination</th>
<th>Services</th>
<th>Action</th>
<th>Direction</th>
<th>Rule Chain</th>
</tr>
</thead>
<tbody>
<tr>
<td>28</td>
<td>lab_machines</td>
<td>192.108.100.3</td>
<td>top_all</td>
<td></td>
<td></td>
<td>inbound</td>
<td>ACCESS</td>
</tr>
<tr>
<td>31</td>
<td>lab_machines</td>
<td>192.108.100.3</td>
<td>udp_all</td>
<td></td>
<td></td>
<td>inbound</td>
<td>ACCESS</td>
</tr>
</tbody>
</table>

### Generating Firewall Changes reports

**To generate a Firewall Changes report**

1. Open the Reports workspace.
2. In the Tree pane, click **Reports**.
3. Select **Public Report Definitions > Firewall Compliance** and then select a report definition.
4. Click **Generate**.

The time to generate a report varies according to the number of firewalls and their complexity.

You can change the scope of predefined reports or create additional report definitions; for example, you can have a separate report definition for each firewall or folder that you are auditing. For additional information, see the Working with reports section in the Skybox Reference Guide.

For additional information about Firewall Changes reports, see the Firewall Changes reports topic in the Skybox Reference Guide.

### CHANGE TRACKING REPORTS

Skybox includes Change Tracking reports that provide information about changes to access rules and firewall objects in specified firewalls. These reports help you to understand what changes were made in your firewalls during a specified tracking period.
What's in a Change Tracking report

The 1st section of the report displays a list of all the changed firewalls and how many access rules and firewall objects are changed in each firewall, followed by a list of all the changes.

<table>
<thead>
<tr>
<th>Changed Firewalls</th>
<th>Changed Access</th>
<th>Changed Objects</th>
<th>Total Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall Name</td>
<td>Rules</td>
<td></td>
<td></td>
</tr>
<tr>
<td>vlab-pix[10.41.1.2]</td>
<td>18</td>
<td>10</td>
<td>28</td>
</tr>
<tr>
<td>Total</td>
<td>18</td>
<td>10</td>
<td>28</td>
</tr>
</tbody>
</table>

All Changes

<table>
<thead>
<tr>
<th>Change ID</th>
<th>Change Time</th>
<th>Changed by</th>
<th>FW Name</th>
<th>Changed Entity</th>
<th>Change Type</th>
<th>Change Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>110</td>
<td>5/9/10 4:18 AM</td>
<td></td>
<td>vlab-pix [10.41.1.2]</td>
<td>ACL #30 (ACCESS)</td>
<td>Changed</td>
<td>value changed for Destination, Destination changed from Any</td>
</tr>
<tr>
<td>111</td>
<td>5/9/10 4:18 AM</td>
<td></td>
<td>vlab-pix [10.41.1.2]</td>
<td>ACL #31 (ACCESS)</td>
<td>New</td>
<td>ACL #31 added to access list</td>
</tr>
<tr>
<td>112</td>
<td>5/9/10 4:18 AM</td>
<td></td>
<td>vlab-pix [10.41.1.2]</td>
<td>ACL #33 (ACCESS)</td>
<td>Changed</td>
<td>970 destination ports added to Service</td>
</tr>
<tr>
<td>109</td>
<td>5/9/10 4:18 AM</td>
<td></td>
<td>vlab-pix [10.41.1.2]</td>
<td>Object udp all [10.41.1.2]</td>
<td>New</td>
<td>Object udp all added to access list</td>
</tr>
<tr>
<td>107</td>
<td>5/9/10 4:18 AM</td>
<td></td>
<td>vlab-pix [10.41.1.2]</td>
<td>ACL #28 (ACCESS)</td>
<td>Changed</td>
<td>1 object added to Source, 1 destination port added to Service</td>
</tr>
<tr>
<td>108</td>
<td>5/9/10 4:18 AM</td>
<td></td>
<td>vlab-pix [10.41.1.2]</td>
<td>ACL #32 (ACCESS)</td>
<td>Changed</td>
<td>64511 destination ports removed from Service</td>
</tr>
<tr>
<td>105</td>
<td>5/9/10 4:18 AM</td>
<td></td>
<td>vlab-pix [10.41.1.2]</td>
<td>Object lab_machines [10.41.1.2]</td>
<td>New</td>
<td>Object lab_machines added to access list</td>
</tr>
</tbody>
</table>

The rest of the report is divided by firewalls. For each firewall, you can see all the changed access rules and all the changed objects; you can include detailed information for each changed entity.

Generating Change Tracking reports

To generate a Change Tracking report

1. Open the Reports workspace.
2. In the Tree pane, click Reports.
3. Select Public Report Definitions > Firewall Compliance and then select a report definition.
4. Click Generate.

The time to generate a report varies according to the number of firewalls and their complexity.

You can change the scope of predefined reports or create additional report definitions; for example, you can have a separate report definition for each firewall that you are auditing or reports for different tracking periods. You can schedule reports to run at specific times and be sent to designated recipients. For additional information, see the Working with reports section in the Skybox Reference Guide.

For additional information about Change Tracking reports, see the Change Tracking reports topic in the Skybox Reference Guide.

You can export change tracking data to a CSV file:
NERC COMPLIANCE REPORTS

Skybox includes NERC Compliance reports that provide information about compliance with NERC Critical Infrastructure Protection (CIP) standards of cyber security for the identification and protection of cyber assets. Skybox NERC Compliance reports cover the following requirements:

- CIP-002-3 – Critical Cyber Asset Identification
- CIP-003-3 – Security Management Controls
- CIP-005-3 – Electronic Security Perimeters
- CIP-007-3 – Systems Security Management

Terminology

<table>
<thead>
<tr>
<th>Skybox term</th>
<th>NERC CIP term</th>
</tr>
</thead>
<tbody>
<tr>
<td>Zone</td>
<td>Security perimeter</td>
</tr>
<tr>
<td>Device, firewall, or router</td>
<td>Cyber asset</td>
</tr>
</tbody>
</table>

What’s in a NERC Compliance report

The 1st section of the report displays information about the compliance of your organization’s security perimeters and cyber assets with the documented NERC CIP regulations. The Cyber Assets and Security perimeters table includes links to information about each individual cyber asset. This section provides compliance for CIP-002-3 and CIP-005-3.

The rest of the report is divided by cyber assets. For each cyber asset, you can see summary information about the compliance of that cyber asset with specific NERC CIP requirements. These sections provide compliance for CIP-003-3 and CIP-007-3.

Additionally, you can opt to include detailed information about each cyber asset’s compliance.

Generating NERC Compliance reports

To generate a NERC Compliance report

1. Open the Reports workspace.
2. In the Tree pane, click Reports.
3. Select Public Report Definitions > Firewall Compliance and then select a report definition.
4. Click Generate.

The time to generate a report varies according to the number of firewalls and their complexity.
You can change the scope of the reports or create additional report definitions; for example, you can have a separate report definition for each firewall or folder that you are auditing, or separate reports for summary and detailed information.

You can schedule reports to run at specific times and be sent to designated recipients. For additional information, see the Working with reports section in the Skybox Reference Guide.

For additional information about NERC Compliance reports, see the NERC Compliance reports topic in the Skybox Reference Guide.

**PCI FIREWALL COMPLIANCE REPORTS**

Skybox includes PCI Firewall Compliance reports that provide information about compliance with PCI DSS Requirement 1 for specified firewalls. These reports help you to understand the compliance status of each firewall with this requirement and to identify problematic access configuration in the firewalls.

**What’s in a PCI Firewall Compliance report?**

The 1st section of the report explains the requirement and how it is modeled in Skybox.

The next section includes a summary of compliance for firewalls in the scope of the report, followed by links to information about each included firewall.
The following sections show the compliance of each firewall in the scope to each subsection of the requirement. Detailed reports included a full description of each subsection of the requirement and the violating access rules for each noncompliant subsection.

2 Firewall: prod FW

IP Address: 192.170.33.1
Node Type: Cluster
Number of Compliant Requirements: 19
Number of Non-Compliant Requirements: 9
Number of Exceptions: 0
Number of Unsatisfied Tests: 0

2.1 PCI Requirements Compliance - Summary

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Compliance</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1.1 - Formal Testing Process</td>
<td>Pass</td>
<td>This report provides a summary of the formal testing procedure required for this firewall.</td>
</tr>
<tr>
<td>1.1.2 - Up-to-Date Network Connections Diagram</td>
<td>Fail</td>
<td>Network connections diagram is not up-to-date.</td>
</tr>
<tr>
<td>1.1.3 - Firewall Installed for Each Zone</td>
<td>Pass</td>
<td>All 4 tests passed.</td>
</tr>
<tr>
<td>1.1.4 - Logical Management of Network Components</td>
<td>N/A</td>
<td>(Not Supported)</td>
</tr>
<tr>
<td>1.1.5 - Business Justification for Allowed Services</td>
<td>Fail</td>
<td>Failed tests: 14 out of 24.</td>
</tr>
<tr>
<td>1.1.8 - Review Rule Chains Annually</td>
<td>N/A</td>
<td>(Not Supported)</td>
</tr>
</tbody>
</table>

2.1.2 - Restrict Untrusted Access to Cardholder Data Environment

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Compliance</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.2.1 - Limit Access to Cardholder Data Environment</td>
<td>Fail</td>
<td>Failed tests: 12 out of 18.</td>
</tr>
<tr>
<td>1.2.2 - Secure and Synchronize Configuration Files</td>
<td>N/A</td>
<td>(Not Supported)</td>
</tr>
<tr>
<td>1.2.3 - Wireless Networks Protected by Perimeter Firewalls</td>
<td>N/A</td>
<td>Tests for this requirement are unavailable.</td>
</tr>
</tbody>
</table>

The last section lists compliance per firewall.

How the report works

The PCI Firewall Compliance report automates testing of PCI DSS Requirement 1 by automating testing of most of the subsections of this requirement. Most of the subsections of this requirement define a policy for connectivity to different network areas. Skybox uses access tests to automate these subsections, so that you can see that the firewall is compliant with this subsection if all tests passed. If some access tests failed, the PCI Requirements Compliance – Details section lists the ID numbers of the access tests that failed, so that you can look up each access test, understand why it failed, and later resolve these issues.

Other subsections are automated differently. For example, to check compliance with subsection 1.1.2 (Up-to-Date Network Connections Diagram), Skybox checks that the firewall configuration is not more than 30 days old.

Note: You can customize the age of the firewall configuration to use for this subsection by changing the value of the PCI_report_last_scan_time_within_days property in <Skybox_Home>\server\conf\sb_server.properties.
Some subsection tests cannot be automated; verify these with the help of the appropriate members of your organization. For example, the testing procedure for subsection 1.1.4 is “Verify that firewall and router configuration standards include a description of groups, roles, and responsibilities for logical management of network components.” Such tests cannot be modeled in Skybox.

**Generating PCI Firewall Compliance reports**

Note: If you made changes to the hierarchy of an existing PCI policy or created a new PCI policy, map the folders (see page 55) of the new policy to the subsections of PCI DSS Requirement 1 before generating this report.

*To generate a PCI Firewall Compliance report*

1. Open the Reports workspace.
2. In the Tree pane, click **Reports**.
3. Select **Public Report Definitions > Firewall Compliance** and then select the report definition.
4. Select the desired policy.
5. Click **Generate**.

The time to generate a report varies according to the number of firewalls and their complexity.

You can change the scope of predefined reports or create additional report definitions; for example, you can have a separate report definition for each firewall that you are auditing, list the exceptions per firewall, or add the full text of PCI DSS Requirement 1 as an appendix to the report. You can schedule reports to run at specific times and be sent to designated recipients. For additional information, see the Working with reports section in the Skybox Reference Guide.

For additional information about PCI Firewall Compliance reports, see the PCI Firewall Compliance reports topic in the Skybox Reference Guide.

**EXPORTING MODEL DATA**

You can export tables displayed in the Table pane or the Details pane to CSV files and open these files later using another application. For example, if you select the **Firewalls** node in the Model tree, you can save a table of all firewalls in the current model.

You can save tables containing the following types of entities to CSV files:

- Assets (of any type)
- Firewall objects
- Policy sections
- Rule usage analysis data
- Redundant rules
- Access rules
- Firewall changes
- Violations
- Shadowed rules
To save a table as a CSV file

1. Display the desired table in the Table pane or in a tab of the Details pane.
2. Make sure that the columns to be saved are displayed in the table.
   
   Columns that are not displayed are not saved.
   
   - To display or hide columns, right-click in the header row of the table, select **Customize Current View**, and then select or clear columns.
3. Select a row in the table.
   
   This focuses the Save operation on the selected table.
4. Select **File > Export Table to CSV**.
5. In the Save dialog box, navigate to the desired location and click **Save** (you can change the file name).

Some model data can be exported to CSV using tasks. The following CSV tasks are available for Skybox Firewall Assurance:

- CSV – Access Rules Review Export
- CSV – Analysis Export
- CSV – Change Tracking Export
- CSV – Compliance Results Export
- CSV – Configuration Compliance Results Export
- CSV – Firewall Assurance Export
- CSV – Optimization and Cleanup Export
- CSV – Security Metrics Export

Information about these tasks is available in the Skybox Reference Guide.

Searching for access rules

Skybox includes search capabilities for various entities, including the ability to search the model for assets, locations, networks, and access rules (also named ACL rules). Activate the search bar by pressing **Ctrl-F**.

Search for access rules:

- Using a quick search from the search bar

  You can search for access rules by service, by whole or partial IP addresses and object names, and by whole or partial user and application names. For example, you can search for all access rules that have a specific IP address range or that have an object starting with **NY**. Click the **Browse** button next to **Search in** to limit the search to specific fields.

  - For information about the format of the search string, see **Search formats** (on page 134).

- Using an extended search area with many options

  Open the extended search (see page 133) by clicking **on the search bar.
EXTENDED SEARCH

The following information explains how to use the extended search for access rules.

Search by

You can search by access rule properties using an extended version of the quick search or a more advanced search.

› Use the **Quick Search** option to do simpler searches. For example, search for all access rules that contain a specific object name, IP address, or service name. By default, the fields searched are **Source**, **Destination**, **Service**, **Description**, **Original Text**, and **Original Rule ID**. You can change this to search in only some of these fields.

For example, search for all access rules that have an object named **Finance**. This is useful when you want to make changes to this object and need to know what it affects.

Note: Search time can sometimes be improved by clearing fields that are not relevant for your search.

› Use the **Advanced Search** to search for specific information in specific fields.

For example, search for all access rules whose source includes IP addresses 200.160.1.0-200.160.2.255 (partner network) and whose destination includes IP addresses 192.170.33.0-192.170.33.255 (DMZ). This is useful when you want to check which rules support access from a partner network to your DMZ.

**Important**: Since there are many ways of interpreting search strings (for example, an integer could be interpreted as part of an IP address, a port number, and so on), there are very specific search formats that you must use when searching for IP address ranges, services, and object names. For additional information, see **Search formats** (on page 134).

Search settings

You can change the scope of the search and the definition of how the values in the searched access rules match the searched entities.

› **Scope**: You can change the scope of the search. Usually, the default scope is the whole model. When working in All Firewalls, the default scope is the selected entity.

Note: The following 2 properties are not relevant for object names.

› **Match criteria**:

  • Entire field match: An access rule only matches the search entity if the search entity and the value of the searched field match exactly. For example, if the search value is **2.2.2.2-2.2.2.255**, it would only match if the field value is the same: **2.2.2.2-2.2.2.255**.

  • Specific field match: An access rule only matches the search entity if the search entity exactly matches the value of an entity in the searched field. For example, if the search value is **2.2.2.2-2.2.2.255**, it would match
the following field value: 1.1.1.1, 2.2.2.2-2.2.2.255, 3.3.3.3 (among others). It would not match a field with the value 2.2.2.0-2.2.2.255.

- Contained within: An access rule matches the search entity if the search entity is contained within the value of the searched field. For example, if the search value is 2.2.2.2-2.2.2.255, it would match a field with the value 2.2.2.0-2.2.2.255.

- Intersection: An access rule matches the search entity if the searched field includes any of the searched addresses or ports. For example, if the search value is 1.0.0.6-1.0.0.11, it would match a field with the value 1.0.0.5-1.0.0.10.

- Ignore Rules with Any: Specifies whether Skybox does not search in rules that have Any as the value of the searched fields.

**SEARCH FORMATS**

You can use the following formats when searching.

**Note:** You can enter multiple, comma-separated IP address ranges, service ranges, and port ranges.

### IP address structure

- **aaa.*, aaa.bbb.*, aaa.bbb.ccc*:** Matches access rules that contain addresses that start with the specified prefix
- **aaa.bbb.ccc.ddd-iii.jjj.kkk.lll:** Matches access rules that contain IP addresses in the specified range
- **aaa.bbb.ccc.ddd/n:** Matches access rules that contain the IP address with the specified mask

**Note:** In IP addresses, wildcards are supported only at the end of the address

### Service structure

- **Protocol name**
- **Destination port or range of destination ports:** The search is run on <port>/TCP
- **Destination port or port range/protocol name**

### Object name

- **Structure**
  - Any text that does not match the IP structure or service structure
  - IP structure or service structure surrounded by single or double quotation marks

- **Wildcards:** Use the characters ? and * for standard pattern matching
Skybox adds an asterisk before and after the search string (for example, if the string the user typed is FW, Skybox searches for *FW*) unless wildcards are included in the search string.

Searching in the Destination, Source, and Service fields of the access rule also finds names of sub-objects.

**Users and applications**

- Textual search
- Wildcards: Use the characters ? and * for standard pattern matching

**Other ways to import data offline**

In addition to device-specific tasks, basic file import tasks, and directory import tasks, you can use the following task to import data offline:

- **Import – Advanced** tasks import scan data or configuration files of any number of devices into the model, where the files are located on the local machine.
  - For information about importing collected data, see the Advanced file import tasks topic in the Skybox Reference Guide.

- **Import – Collector** tasks import scan data or configuration files of a single device into the model, where the files are located on a Skybox Collector machine.
  - For information about collecting and importing data from a single device, see the Collector file import tasks topic in the Skybox Reference Guide.

- **Import – Collector Advanced** tasks import scan data or configuration files of any number of devices into the model, where the files are located on a Skybox Collector machine.
  - For information about collecting and importing data from multiple devices, see the Advanced collector file import tasks topic in the Skybox Reference Guide.


**Change tracking utility**

The change tracking utility compares 2 firewall configurations from the past. This is useful for cases when change tracking analysis was not done between configuration file imports, so that some configuration data was lost.

Note: This tool requires familiarity with **Import – Advanced** tasks, because the tool uses the same configuration format and directory structure. For information about **Import – Advanced** tasks, see the Advanced file import tasks topic in the Skybox Reference Guide.
**Input directories**

Before running the utility, copy the relevant configurations into 2 directories, with the naming convention and directory structure used by **Import – Advanced** tasks. The 1st directory contains the newer configuration (referred to as the current configuration) and the other contains the baseline configuration.

For example, if you have a PIX firewall, each directory (current and baseline) must contain `run.txt` and, optionally, `route.txt`.

Changes are created in Skybox by comparing the current configuration to the baseline.

**Identifying the relevant firewall in Skybox**

Changes can only be created for firewalls that already exist in Skybox. Make sure that you know the name (as used in Skybox) or ID of the firewall before starting the utility.

**USING THE CHANGE TRACKING UTILITY**

The Skybox change tracking utility is located in the `<Skybox_Home>\server\bin` directory.

**Usage**

```
change_tracking (-host_id <id> | -host_name <name>) -format <format>
    -current <dir date [rulebase]> -baseline <dir date [rulebase]>
```

The Skybox change tracking utility arguments are described in the following table.

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>host_id</td>
<td>The ID (in Skybox of the firewall on which to create changes</td>
<td>You must specify either <strong>host_id</strong> or <strong>host_name</strong>.</td>
</tr>
<tr>
<td>host_name</td>
<td>The name of the firewall on which to create changes</td>
<td>You must specify either <strong>host_name</strong> or <strong>host_id</strong>.</td>
</tr>
<tr>
<td>format</td>
<td>The format of the configuration files (see the Data formats for file import tasks topic in the Skybox Reference Guide)</td>
<td>Yes</td>
</tr>
<tr>
<td>current</td>
<td>The details of the current configuration, including the following arguments:</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>• dir: The directory path</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• date: The configuration timestamp in the format yyMMddHHmmss</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• rulebase (optional): For FW1_CONF format, the name of the rulebase</td>
<td></td>
</tr>
</tbody>
</table>
### Example

The following string creates changes for the firewall **Main-FW** by comparing the FW1 configuration in `\temp\current` to that in `\temp\baseline`. The current configuration is from 9 Aug 2013 and the baseline is from 8 Aug 2013. Both configurations use the **Standard** rulebase.

```plaintext
> change_tracking -host_name "Main-FW" -format fw1_conf -current \temp\current 090820130000 Standard -baseline \temp\baseline 08082013000 Standard
```

### TROUBLESHOOTING

Some problems that might occur when using the change tracking utility are listed in the following table, together with suggested solutions.

<table>
<thead>
<tr>
<th>Problem</th>
<th>Possible cause</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parsing Error</td>
<td>The directories do not contain the expected files or the file themselves cannot be parsed.</td>
<td>Try to import each directory using an <strong>Import – Advanced</strong> task. The task’s error messages explain what went wrong.</td>
</tr>
<tr>
<td>The asset cannot be determined</td>
<td>The configuration files were parsed successfully but they contain more than 1 asset. However, they do not contain an asset with a name that is in Skybox or there is more than 1 asset in Skybox that matches the name.</td>
<td>Check the spelling of the asset name in Skybox and the name in the configuration file. Rename the asset or use the asset ID instead of the asset name.</td>
</tr>
</tbody>
</table>

Note: Running the utility might add duplicate values to the change tables.

### Cisco configuration diffs

Skybox enables you to check for differences between the **startup-config** and **running-config** files of Cisco firewalls and routers. This is done by collecting both files and comparing between them. The check can be made every time the device configuration is collected using the following task types:

- **Firewalls – Cisco PIX/ASA/FWSM Collection**
- **Routers – Cisco IOS Collection**
- **Routers – Cisco Nexus Collection**
To activate collection and comparison of the startup configuration

- In the relevant collection task, select **Collect Startup Configuration** (in the **Advanced** tab).

  Every time this task runs, both the running configuration and the startup configuration are imported.

To view the differences

You can view differences in the following locations in the GUI:

- In the firewall’s summary page, by clicking the **Cisco Configuration Diffs** link at the top of the page.

  ![Cisco Configuration Diffs](image)

- On the **Firewalls** tab of the **All Firewalls** node, by displaying the **Cisco Configuration Diffs** column. Devices that have diffs have a link in this column.

- By right-clicking the device in the tree and selecting **Compare > Compare Running Configuration to Startup**.

  Clicking any of these links opens a comparison of the 2 files in WinMerge, with the differences highlighted.

Addresses behind network interfaces

This section explains how to view and change the IP addresses behind the network interfaces of a firewall in Skybox.

Each interface on a gateway device communicates with a specific set of networks. The IP addresses of these networks often are referred to as **addresses behind the interface**.
In general, these IP addresses are assumed to be distinct on each interface—an IP address that is behind one network interface of a firewall is not also behind another network interface on the same firewall.

When firewalls are imported into the model, Skybox ascertains the IP addresses behind each network interface in the firewall based on the routing table and other information received as part of the firewall import. These addresses are used when analyzing access between network interfaces of the firewall.

When you import a new firewall, check the network interfaces to confirm that IP addresses are assigned to the network interfaces (that is, the routing table was imported).

**Devices whose routing information is imported automatically**

Skybox imports routing information as part of the configuration for many network devices, including Cisco routers, Cisco PIX/ASA/FWSM firewalls, and Juniper Networks NetScreen firewalls. For these devices, IP addresses behind the interfaces are analyzed based on the routing information.

When Skybox Firewall Assurance receives routing information, it can calculate explicit IP address ranges for each network interface. These IP addresses are displayed in the **Specific Addresses** field.

**Devices whose routing information is not imported automatically**

In some devices, the underlying operating system handles routing so that routing information might not be imported together with the firewall configuration and access rules. In these cases, import routing information separately. If you do not import the routing information, IP addresses behind the interface are set to **unknown** for all network interfaces and you must update them manually.

When Skybox Firewall Assurance does not receive enough information to establish the IP addresses behind the network interfaces, each network interface is marked as **Default Gateway/Unknown Addresses** and Skybox assumes that all address ranges are accessible from each network interface on the firewall. In this case, access analysis might produce many routes that seem to be accessible but are not accessible in reality.
Viewing the addresses behind a network interface

To view the addresses behind a network interface

1. In the tree, right-click the firewall and select Network Interfaces.
2. In the Network Interfaces dialog box, select the network interface for which you want to view the IP addresses and click Modify.

Fixing addresses behind network interfaces

If you know that the device has a routing table that was not imported by the Add Firewalls Wizard, you can import the routing table using Skybox tasks. For information about tasks, see the relevant section in the Tasks part of the Skybox Reference Guide.

If the routing table is not available, fill in the expected IP addresses behind each network interface.

You can add IP address ranges for each network interface separately and then test the results. Start with the interfaces connected to internal networks, whose IP addresses are known. Leave the Addresses Behind Interface field for 1 network interface (the default interface or the interface leading to the internet) as Default Gateway rather than providing specific IP addresses. In this way, data that is not routed through any other network interfaces is routed through this network interface.
To change the addresses behind a network interface

1. In the Addresses Behind Interfaces pane, if the network interface is marked as Default Gateway/Unknown Addresses, click Preview to view the IP addresses assigned to it. Otherwise, the system-calculated IP address ranges (if any) are displayed in the Addresses and Excluded fields and you can edit them.
   - The **Addresses** field lists the IP address ranges that are behind this network interface.
   - The **Exclude** field lists IP addresses to exclude from the address ranges in the **Addresses** field.

2. To define the IP address ranges for this network interface:
   a. Click the **Browse** button next to the **Addresses** field.
   b. In the IP Ranges Selection dialog box do any of the following:
      - Add new ranges: Click **Add**.
      - Delete or modify ranges.
      - Include all private IP addresses (listed in RFC 1918): Click and select **Add Private Addresses**.
      - Include all IP addresses of networks directly connected to other interfaces of this firewall: Click and select **Add Directly Connected Addresses**.

3. To exclude IP addresses from the IP address ranges listed in the **Addresses** field for this network interface:
   a. Click the **Browse** button next to the **Exclude** field.
   b. In the IP Ranges Selection dialog box do any of the following:
      - Specify ranges to exclude: Click **Add**.
      - Delete or modify ranges.
      - Exclude all private IP addresses (listed in RFC 1918): Click and select **Add Private Addresses**.
      - Exclude all IP addresses of networks directly connected to other interfaces of this firewall: Click and select **Add Directly Connected Addresses**.

Updating addresses behind network interfaces

By default, the **Addresses Behind Interface** fields are updated every time that Skybox imports the device’s routing table. If you changed the value of the **Addresses Behind Interface** fields manually for a network interface, these fields are **Locked** and their values are not updated by the file import.

Changing the action that assigns addresses behind network interfaces

**Admins** can change the action that assigns addresses behind interfaces:
Disabled: The **Addresses Behind Interface** fields are empty on all interfaces (that is, **Default Gateway/Unknown Addresses** is used).

No Speculation: Addresses behind interfaces are assigned based on the routing table of the firewall but no routing speculation is performed. If there are destination IP addresses that are not found in the routing table, they do not appear as behind any interface.

Full: Addresses behind interfaces are assigned based on the routing table of the firewall. Routing speculation is performed for destination IP addresses that are not found in the routing table; these addresses are added to all interfaces.

To change the action that assigns addresses behind interfaces

1. Select **Tools > Options > Server Options > Access Compliance > Firewall Compliance**.
2. Select an action and click **OK**.

Multi-zone interfaces

In most firewalls, each network interface maps to a specific zone. For example, 1 interface connects to the DMZ network, 1 to an internal network, and 1 to a partner network. Skybox can then check access between 2 different zones by checking the access between their corresponding network interfaces. However, in some firewalls a single network interface has multiple zones behind it. For example, one interface connects directly to a specific zone, but another interface connects to a core network that has other networks behind it. Access must be checked between a zone (on one network interface) and several other zones that are all behind a different network interface.

In Skybox, network interfaces with several zones behind them are **multi-zone interfaces**, and they must be explicitly configured for compliance and access analysis to work correctly.

Multi-zone interfaces are disabled by default. To enable these interfaces, set the `enable_policy_section_zone_to_addresses` property in `<Skybox_Home>\server\conf\sb_server.properties` to **true**.

**OVERVIEW OF MULTI-ZONE INTERFACES**

When you work with multi-zone interfaces, you must customize the Access Policy for firewalls with multi-zone interfaces. You usually do this by creating an Access Policy for each group of firewalls with a common core network.

In an organization with no multi-zone interfaces, there is often 1 Access Policy for the organization’s network. Each network interface of each firewall is mapped to the relevant zone and the policy sections are global—for example, Internet to DMZ, DMZ to Internal, and Internal to Internet.
In organizations with firewalls that have multi-zone interfaces, there is usually a core network surrounded by a group of firewalls. When checking access, the core is a means to get to the zones on its other side. In the following diagram, the right-most firewall is directly connected to Internet, DMZ, and Core. However, it is also necessary to check access via the firewall from these networks to Internal and to the Partner networks.

You check this access by creating a zone named **Core** and then defining the Access Policy to check from 1 network interface to the desired IP addresses behind the core (rather than to all the addresses behind the core).

In this case, the Access Policy might include the following sections:

- Internet to Core (using only IP addresses derived from Partner 1)
- DMZ to Core (using only IP addresses derived from Internal)
- Core (only IP addresses derived from Internal) to Internet

This type of policy is applicable only to this specific group of firewalls with a common core network. If you have 2 such groups of firewalls, you might need 2 sets of zones and a different Access Policy for each set.

**USING MULTI-ZONE INTERFACES**

To use multi-zone interfaces, you must:

1. Define any additional zones. Usually, a zone to represent the core network is sufficient.
2. Make a copy of the Access Policy that you want to use.
3. For each policy section, customize any source or destination that is behind the new zone:
   - In the Available Entities pane, select the new zone and click **Source** or **Destination** to move it to the necessary Selected pane.
   - Below the Selected pane, do either of the following:
     - Select **IP Ranges** and type the IP address range for the actual source or destination network that sits behind the new interface.
Select **Derive Addresses from Zone** and then select the zone from which to derive the addresses.

This enables Skybox to use the exact source or destination when analyzing compliance, and not the entire zone.

For example, if you created a test from **Internet** to **Core** but limited the destination to internal IP addresses according to the customized policy sections, then compliance analysis is done between the **Internet** zone and the **Internal IP addresses behind the Core** zone.

4 Assign network interfaces to the new zones: Right-click the firewall’s **Policy Compliance** node and select **Manage Access Policy**.

After you finish this setup, access is analyzed over regular network interfaces and multi-zone interfaces.