Skybox Network Assurance

Getting Started Guide

8.5.600

Revision: 11
Contents

Intended audience .............................................................................................................. 5
How this manual is organized .......................................................................................... 5
Related documentation .................................................................................................. 6
Technical support .......................................................................................................... 6

Overview ......................................................................................................................... 7
Skybox Network Assurance .............................................................................................. 7
How Network Assurance works ...................................................................................... 9
Highlights of Skybox Network Assurance ........................................................................ 9
Basic architecture .......................................................................................................... 14

Before you begin .............................................................................................................. 15
Prerequisites .................................................................................................................... 15
Starting Skybox Network Assurance .............................................................................. 16
Summary page ................................................................................................................ 16
Network Assurance tree ................................................................................................. 18

Network data in Skybox ................................................................................................. 19
Viewing the network ....................................................................................................... 20
Network Map .................................................................................................................. 21
Viewing additional information about an entity ............................................................. 23
Viewing the properties of an entity ................................................................................ 24

Configuration Compliance .............................................................................................. 25
Configuration Compliance overview ............................................................................... 25
Viewing Configuration Compliance .............................................................................. 26
Viewing an overview of Configuration Compliance ..................................................... 28

Access analysis ............................................................................................................... 30
Access Analyzer .............................................................................................................. 30
What is accessible from the internet? ............................................................................ 30
How can I tell if 2 networks are connected? .................................................................. 32

Network Access Compliance ......................................................................................... 34
Network Access Compliance overview ......................................................................... 34
Basic steps for Access Compliance .............................................................................. 34
What is an Access Policy? .............................................................................................. 35
Classifying the network into zones ............................................................................... 37
Analyzing the Access Policy ......................................................................................... 38
Understanding compliance metrics ............................................................ 39
Understanding what caused a violation ...................................................... 41
Creating and editing exceptions ................................................................ 43

Change management .............................................................................. 46
Change management in Skybox ............................................................... 46
Managing changes .................................................................................. 46
Testing changes with the What If model .................................................... 47
Analyzing changes .................................................................................. 48
Viewing changes to access rules between models ....................................... 49

Using Skybox reports ............................................................................. 51
Reports tree ........................................................................................... 51
Report definitions ................................................................................... 51
Report types .......................................................................................... 51
Network Access Compliance reports ....................................................... 52
Preface

Intended audience

The Skybox Network Assurance Getting Started Guide provides background information about what Skybox Network Assurance does and how it works, and explains how to get started using the product. This Getting Started Guide is intended for use with the demo model only. To model your organization’s network and work with that model, see the Skybox Network Assurance User’s Guide.

The intended audience is anyone who wants to learn how to use Skybox Network Assurance.

How this manual is organized

This manual includes the following chapters:

- Overview (on page 7) of Skybox Network Assurance
- Before you begin (on page 15), which includes:
  - Instructions for starting and logging in to Skybox
  - An overview of the GUI
  - Instructions for loading the demo model

If you are familiar with Skybox, you can skip most of this section. However, make sure to load the demo model file.

- Tutorials on:
  - Network data in Skybox (on page 19): How data is imported into Skybox, and various ways of viewing the data
  - Configuration Compliance (on page 25): Viewing compliance between configuration data and best practice Configuration Policies for each type of firewall
  - Access analysis (on page 30): Analyzing access within a network
  - Network Access Compliance (on page 34): Checking the network for compliance to Access Policies
  - Change management (on page 46): Viewing and managing changes in access rules and checking the results of these changes on the network
  - Using Skybox reports (on page 51): Understanding the built-in reports, making changes to the properties of reports, and generating reports

Each tutorial builds on the knowledge gathered in the previous tutorial; they are intended to be used in sequence.
Note: Screen captures in this document were taken using a Skybox installation with a license for Skybox Firewall Assurance and Skybox Network Assurance. If you have a license for only a single Skybox product, some screens look slightly different.

Related documentation

The following documentation is available for Skybox Network Assurance:

▷ Skybox Network Assurance User’s 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

This chapter contains introductory information about Skybox Network Assurance.

In this chapter

Skybox Network Assurance .......................................................... 7
How Network Assurance works .................................................. 9
Highlights of Skybox Network Assurance .................................. 9
Basic architecture ...................................................................... 14

Skybox Network Assurance

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.

Network Assurance provides complete visibility across physical, virtual and cloud networks, giving you the context to see how network devices and security controls work together or leave you exposed. Uncover potential attack vectors, troubleshoot the root causes of network outages and check correct implementation of security zone policies and security groups.

- Visualizes your entire hybrid network and security controls in an interactive model
How Network Assurance works

The following diagram shows the typical process when working with Network Assurance.

1. Collect & Normalize
   - Automatically collect data from all layer three network devices
   - Normalize all network data for fast & consistent analysis

2. Create a Model
   - Create a holistic, visual model of all your network topology
   - Unify hybrid IT & OT environments in one view

3. Analyze in Context
   - Troubleshoot configuration issues, analyze network connectivity end to end & assess compliance with complete context — all within the network model

Highlights of Skybox Network Assurance

You can use Skybox Network Assurance for:

- Network visualization: Viewing your network graphically and viewing inventory tables sorted according to various criteria (for example, all firewalls, all entities in location A, or all assets by operating system or by service)
- Configuration Compliance: Checking the configuration of your devices against best-practice policy
- Access analysis: Planning and troubleshooting connectivity
- Network Access Compliance: Ensuring compliance with your organization’s Access Policy

Network visualization

The Skybox database contains all network devices and their configurations.

You can:
List the devices according to specific criteria

<table>
<thead>
<tr>
<th>Name</th>
<th>Primary IP Address</th>
<th>OS</th>
<th>OS Version</th>
<th>Creation Time</th>
<th>Modification Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Finance FW</td>
<td>192.170.1.5</td>
<td>IPSEC</td>
<td>6.0.1</td>
<td>10/05/2011 10:45 AM</td>
<td>1/1/2010 10:45 AM</td>
</tr>
<tr>
<td>L2 FW</td>
<td>192.170.22.203</td>
<td>Generic OS</td>
<td>6.0.0</td>
<td>10/05/2011 10:45 AM</td>
<td>1/1/2010 10:45 AM</td>
</tr>
<tr>
<td>main_FW</td>
<td>192.170.1.5</td>
<td>Solaris</td>
<td>5.4.0/18.0</td>
<td>4/11/2011 10:30 AM</td>
<td>1/1/2010 10:45 AM</td>
</tr>
<tr>
<td>noc_FW</td>
<td>192.170.1.5</td>
<td>Solaris</td>
<td>5.4.0/18.0</td>
<td>4/11/2011 10:30 AM</td>
<td>1/1/2010 10:45 AM</td>
</tr>
<tr>
<td>PA-2020 vsys1</td>
<td>172.20.0.252</td>
<td>PAN-OS</td>
<td>6.0.1</td>
<td>7/20/2011 10:21 AM</td>
<td>1/1/2010 10:45 AM</td>
</tr>
<tr>
<td>PA-2020 vsys2</td>
<td>172.20.0.252</td>
<td>PAN-OS</td>
<td>6.0.1</td>
<td>7/20/2011 10:21 AM</td>
<td>1/1/2010 10:45 AM</td>
</tr>
<tr>
<td>PA-Nux�行1</td>
<td>172.20.0.249</td>
<td>PAN-OS</td>
<td>6.0.1</td>
<td>7/20/2011 10:21 AM</td>
<td>1/1/2010 10:45 AM</td>
</tr>
<tr>
<td>Partner FW</td>
<td>300.16.3.1</td>
<td>Windows Server 2003</td>
<td>1/1/2010 10:45 AM</td>
<td>1/1/2010 10:45 AM</td>
<td></td>
</tr>
<tr>
<td>prod FW</td>
<td>192.170.33.1</td>
<td>IPSO</td>
<td>6.0.1</td>
<td>7/20/2011 10:21 AM</td>
<td>1/1/2010 10:45 AM</td>
</tr>
<tr>
<td>US_ECE11</td>
<td>172.20.0.54</td>
<td>Generic OS</td>
<td>6.0.1</td>
<td>7/20/2011 10:21 AM</td>
<td>1/1/2010 10:45 AM</td>
</tr>
<tr>
<td>US_ECE22</td>
<td>172.20.0.56</td>
<td>Generic OS</td>
<td>6.0.1</td>
<td>7/20/2011 10:21 AM</td>
<td>1/1/2010 10:45 AM</td>
</tr>
<tr>
<td>VCloudRouter_10.0.0.0/16</td>
<td>10.0.1.0</td>
<td>Generic OS</td>
<td>6.0.1</td>
<td>7/20/2011 10:21 AM</td>
<td>1/1/2010 10:45 AM</td>
</tr>
<tr>
<td>Vmware-cisco</td>
<td>172.20.0.19</td>
<td>ASA</td>
<td>8.4(2)</td>
<td>9/14/2011 10:21 AM</td>
<td>1/1/2010 10:45 AM</td>
</tr>
</tbody>
</table>

View the topology of the network
Configuration Compliance for network devices

You can check the configuration of all the network devices against a benchmark policy of best-practices. There are predefined policies for the most common platforms, which you can customize, including adding new checks. You can add policies for additional platforms.

Access analysis

You can use the Access Analyzer to:

› Troubleshoot connectivity issues; the Access Analyzer simulates access against the Skybox database

› To plan changes to connectivity by running a query that reveals the path of a specific connection, identifying all network devices along the way and the specific access rules used by each firewall or router to permit or deny access

The Access Analyzer can provide answers to questions such as:

› Are any parts of our network accessible from the internet?
Is access available between network A and network B?
Network Access Compliance

When you define the roles of the networks in your organization, Skybox checks whether your network complies with your organization’s policy as defined by NIST or PCI baselines.

- NIST 800-41 Policy (88%)
  - NIST External Access (94%)
    - NIST-External to Partner (100%)
    - NIST-External to DMZ (71%)
    - NIST-External to Internal (98%)
      - Block ICMP Echoing Messages (100%)
      - Block Login Services (100%)
      - Block Miscellaneous (100%)
      - Block RPC and NFS (100%)
      - Block Small Services (100%)
      - Block Trojan and Worm Ports (100%)
      - Block Windows NetBIOS (100%)
      - Block X-Windows (100%)
      - No Access - non-specified services (83%)
      - Limited number of ports per IP (50 ports) (100%)
  - NIST Partner Access (95%)
  - NIST DMZ Access (99%)
  - NIST Internal Access (81%)
- NIST 800-41 8 Application Policy (89%)
- PCI DSS V3.1 Policy
  - 1.1 Firewall Configuration Standards
  - 1.2 Restrict Untrusted Access to Cardholder Data Environment
    - 1.2.1 Limit Access to Cardholder Data Environment
    - 1.2.2 Secure and Synchronize Configuration Files [NA]
    - 1.2.3 Wireless Networks Protected by Perimeter Firewalls
  - 1.3 Restrict Access from Internet to Cardholder Data Environment
    - 1.4 Install Personal Firewalls for Mobile Devices [NA]
    - 1.5 Firewall Security Policies and Operational Procedures [NA]
- NSX Access Queries
- AWS Access Queries
- Azure Access Queries
You can view a summary of network Access Compliance.

**Public Access Policies - 89% Compliance**

19 Violating Rules  (2 written 16 digital)

**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*.
Chapter 2

Before you begin

This chapter contains introductory information about working with Skybox.

In this chapter

Prerequisites ................................................................. 15
Starting Skybox Network Assurance ......................... 16
Summary page ............................................................. 16
Network Assurance tree ............................................... 18

Prerequisites

▷ Skybox must be installed on your system before you can begin to work with the tutorials in this guide.

▷ The Skybox Server must be running before you can start the Skybox Manager. If it is not running on your local machine, you need its name or IP address to connect to it.
Starting Skybox Network Assurance

To start Skybox Network Assurance

1. In the Windows system tray, right-click the Skybox icon (️) and select Open Skybox.

2. Note that you can log in to any Skybox product at this point by clicking its icon above the User Name field. Make sure that Skybox Network Assurance is selected.

3. Type your user name and password.
   If you were not assigned a user name and password by your Skybox administrator, use the default user name skyboxview with the password skyboxview.

4. If the Server was not specified during installation or you do not want to connect to the default Server, select the desired Server or type its IP address.

5. Click Login.

6. The 1st time that you work with Skybox, click the Load demo model link in the workspace to load the demo model file.
   The display refreshes after the model is loaded.

   Note: The demo model file includes a small model for which data has been collected and various configuration tasks have already been run.

Summary page

After the demo model loads, you can view Network Assurance information.

To open the Network Assurance workspace

› At the bottom of the Tree pane, click Network Assurance.
The Network Assurance Summary page is displayed. This is the main page for Network Assurance, where you can see summaries about the various types of information that Skybox provides about your network.

The page contains summary information about:

- **Model Summary**: How many network devices and individual networks are included in the Skybox model of your organization’s network
  
  Expand the section to view links to the lists of routers and firewalls in the network.

- **Access Compliance**: The Policy compliance level, and a link to the violating rules and violations to the firewall ACLs

- **Configuration Compliance**: The security level of the firewall configurations, based on platform security checks, and a link to the violations

From the Summary page, you can drill down to the violations or violating rules of whichever type of compliance interests you, or to a list of firewalls or routers. Alternatively, you can drill down using the Tree pane.
Network Assurance tree

The Network Assurance tree is used for navigation when working with Skybox Network Assurance.

- **Access Policies**
  - **Public** and **Private Access Policy** folders
    The public folder is shared by all users, while each user has their own private folder. Only **Admins** can modify the public folder, while all users can modify their own private folder.
  - **Access Policy Violations**: Lists of Access Policy violations. There are separate lists for all violations and critical violations. In each list, you can sort and group the violations.
  - **Zones**: All defined zone types.

- **Configuration Policies**: All the Configuration Policies

- **All Network Devices**: All the network devices in the Skybox model, divided by device type

- **Analyses**: All Assets and Network Interfaces analyses
Chapter 3

Network data in Skybox

In Skybox, data about your organization is stored in the form of a hierarchic model that includes the networks and the devices connecting them.

In these tutorials, you work with a model of an example organizational network. The example represents a relatively small network, where data collection and various configuration tasks were already performed.

The model of your organization’s network is built from the configuration of your network devices. You can import configuration data (using prepared files) or collect the data directly from the devices using either the Add Firewalls Wizard or Skybox tasks that collect the data on a specific schedule. You can model devices that are not directly supported by Skybox using Skybox’s Integration XML (iXML) format. For information about iXML, see the Integration part of the Skybox Developer’s toolkit.

In this chapter

Viewing the network ................................................................. 20
Network Map ........................................................................... 21
Viewing additional information about an entity ..................... 23
Viewing the properties of an entity ....................................... 24
Viewing the network

To view the network

1. In the Tree pane, expand the All Network Devices node and select Firewalls.

   A list of all the firewalls in the model appears in the Table pane. The 1st firewall in the list is selected; you can see information for the selected firewall in the Details pane below the list.

   
   To view the network

   1. In the Tree pane, expand the All Network Devices node and select Firewalls.

   A list of all the firewalls in the model appears in the Table pane. The 1st firewall in the list is selected; you can see information for the selected firewall in the Details pane below the list.

<table>
<thead>
<tr>
<th>Firewalls</th>
<th>Name</th>
<th>Primary IP Address</th>
<th>OS</th>
<th>Status</th>
<th>Creation Time</th>
<th>Modified By</th>
<th>Configured</th>
<th>Configurable</th>
<th>New</th>
</tr>
</thead>
<tbody>
<tr>
<td>PA: FW</td>
<td>Finance FW</td>
<td>192.170.65</td>
<td>IPSO</td>
<td>Up</td>
<td>10/04/14 4:50 AM</td>
<td>41/01/14 1:01 AM</td>
<td>0%</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ELFW</td>
<td>192.170.22.200</td>
<td>Generic OS</td>
<td>Up</td>
<td>11/09/14 1:19</td>
<td>41/01/14 1:04 AM</td>
<td>0%</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td></td>
<td>PA: FW</td>
<td>192.170.37</td>
<td>Solaris</td>
<td>Up</td>
<td>10/04/14 4:50 AM</td>
<td>12/05/14 4:12</td>
<td>0%</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Net: FW</td>
<td>193.170.49</td>
<td>Cisco IOS</td>
<td>Up</td>
<td>4/11/13 10:30</td>
<td>41/01/14 5:06 AM</td>
<td>0%</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td></td>
<td>PA: 2020/1</td>
<td>172.20.352</td>
<td>PAN-OS</td>
<td>Up</td>
<td>5/41/11 11:00 AM</td>
<td>50/14/14 5:01</td>
<td>0%</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td></td>
<td>PA: 2020/2</td>
<td>172.20.352</td>
<td>PAN-OS</td>
<td>Up</td>
<td>7/20/11 12:41</td>
<td>50/14/14 5:07 AM</td>
<td>0%</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td></td>
<td>PA: 2020/3</td>
<td>172.20.249</td>
<td>PAN-OS</td>
<td>Up</td>
<td>9/05/15 5:18 PM</td>
<td>52/01/14 4:37 PM</td>
<td>53%</td>
<td>16</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Partner1</td>
<td>200.16.0.1</td>
<td>Windows Server 2003</td>
<td>Up</td>
<td>11/04/11 1:55</td>
<td>41/01/14 3:35 AM</td>
<td>0%</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Pod: FW</td>
<td>192.170.33.1</td>
<td>IPSO</td>
<td>Up</td>
<td>10/04/14 4:50 AM</td>
<td>41/01/14 1:04</td>
<td>0%</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td></td>
<td>AW: ECE</td>
<td>172.20.54</td>
<td>Generic OS</td>
<td>Up</td>
<td>7/22/14 4:27 PM</td>
<td>52/01/14 3:37</td>
<td>0%</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td></td>
<td>AW: ECE</td>
<td>172.20.56</td>
<td>Generic OS</td>
<td>Up</td>
<td>7/22/14 4:27 PM</td>
<td>52/01/14 3:35</td>
<td>0%</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td></td>
<td>AW: Valsa</td>
<td>172.20.10</td>
<td>ASA</td>
<td>Up</td>
<td>9/14/14 4:09 PM</td>
<td>50/14/14 3:41</td>
<td>40%</td>
<td>50</td>
<td></td>
</tr>
</tbody>
</table>

2. At the bottom of the Tree pane, click Model to switch to the Model workspace.

3. The Locations and Networks node in the tree displays the hierarchical structure of the model.

   Note: The All Network Devices node that you viewed in the previous step is also available in the Model workspace.
4 Expand this node to see all the networks and locations in the demo model.

<table>
<thead>
<tr>
<th>Model</th>
<th>Locations &amp; Networks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Europe</td>
<td></td>
</tr>
<tr>
<td>Paris</td>
<td></td>
</tr>
<tr>
<td>Russia</td>
<td></td>
</tr>
<tr>
<td>US</td>
<td></td>
</tr>
<tr>
<td>EU-Prod_Net1</td>
<td>subnet: 10.0.0.0/24</td>
</tr>
<tr>
<td>EU-Prod_Net8</td>
<td>subnet: 10.0.1.0/24</td>
</tr>
<tr>
<td>db</td>
<td>subnet: 10.0.2.0/24</td>
</tr>
<tr>
<td>internal</td>
<td>subnet: 10.0.3.0/24</td>
</tr>
<tr>
<td>mgd</td>
<td>subnet: 10.0.4.0/23</td>
</tr>
<tr>
<td>GatewaySubnet</td>
<td>subnet: 10.0.6.0/24</td>
</tr>
<tr>
<td>Net_10.1.0.0/24</td>
<td>subnet: 10.1.0.0/24</td>
</tr>
<tr>
<td>SubNet_10.0.0.0/24</td>
<td>subnet: 10.0.0.0/24</td>
</tr>
<tr>
<td>DB_Subnet_10.2.1.0/24</td>
<td>subnet: 10.2.1.0/24</td>
</tr>
<tr>
<td>Net_10.3.0.0/24</td>
<td>subnet: 10.3.0.0/24</td>
</tr>
<tr>
<td>Dev_WebServers</td>
<td>subnet: 10.4.0.0/24</td>
</tr>
<tr>
<td>Dev_BackEnd_Server</td>
<td>subnet: 10.4.0.0/24</td>
</tr>
<tr>
<td>Dev_Training_CRM_Servers</td>
<td>subnet: 10.4.0.0/24</td>
</tr>
<tr>
<td>Prod_WebServers</td>
<td>subnet: 10.5.0.0/24</td>
</tr>
<tr>
<td>Prod_DB_Servers</td>
<td>subnet: 10.5.0.0/24</td>
</tr>
<tr>
<td>Prod_BackEnd_Servers</td>
<td>subnet: 10.5.0.0/24</td>
</tr>
<tr>
<td>Prod_CRM_APP_Servers</td>
<td>subnet: 10.5.0.0/24</td>
</tr>
<tr>
<td>Prod_CRM_APP_Servers_Net1</td>
<td>subnet: 10.5.0.0/24</td>
</tr>
<tr>
<td>Europe_Customers</td>
<td>subnet: 10.7.0.0/24</td>
</tr>
<tr>
<td>Africa_Customers</td>
<td>subnet: 10.8.0.0/24</td>
</tr>
<tr>
<td>North_America_Customers</td>
<td>subnet: 10.9.0.0/24</td>
</tr>
<tr>
<td>10.10.0.0/24</td>
<td>subnet: 10.10.0.0/24</td>
</tr>
<tr>
<td>10.10.10.0/24</td>
<td>subnet: 10.10.10.0/24</td>
</tr>
<tr>
<td>10.10.10.20/32</td>
<td>subnet: 10.10.10.20/32</td>
</tr>
<tr>
<td>10.10.20.0/24</td>
<td>subnet: 10.10.20.0/24</td>
</tr>
<tr>
<td>10.13.0.0/24</td>
<td>subnet: 10.13.0.0/24</td>
</tr>
<tr>
<td>10.17.0.0/24</td>
<td>subnet: 10.17.0.0/24</td>
</tr>
<tr>
<td>10.20.0.0/24</td>
<td>subnet: 10.20.0.0/24</td>
</tr>
</tbody>
</table>

When you select a node in the tree, the workspace displays information about the selected node:

- When you select a location, you can see all the networks and locations within the selected location.
- When you select a network, you see a list of all the devices in the selected network.

**Network Map**

The Network Map is a graphical representation of your organization’s network.

*To use the Network Map*

1. On the toolbar, click ![Network Map](Network Map). The Network Map window opens.
2 In the Map field, select Organizational Map.

The map displays all networks in the model and the devices that connect between them.

3 Click a node in the map; that node and its immediate neighbors are highlighted. Click a location label (for example, Resellers, US, or London), and all the members are highlighted.

4 The Node Selection Effect area of the control panel defines what happens when you select a node in the map. (The selected node and its neighbors are always highlighted.) The following options are available:

- **Focus**: Display only the selected node and its neighbors within a radius of Distance. All other nodes in the map are hidden.
- **Expand**: Expand the map (when parts of it are hidden) by adding all neighbors of the selected node up to a radius of Distance.
- **Select**: Highlight the selected node but does not change which nodes are displayed.

Note: Use to redisplay the entire map.

5 Use the Network Map to show access routes in the model:

   a. At the bottom of the control panel, click Access Query; the Access Query control panel replaces the Network Map control panel.

   b. Click the Browse button in the Source section.

   c. In the Available Entities pane, select Locations & Networks > Europe > Paris > developmentServers and click Source >.

   d. Now select Internet (Perimeter Cloud) and click Destination >.

   e. Click OK, and then click Analyze.
f. In the top pane, set **Group By** to **Networks**, then expand the results and select a network.

g. In the toolbar below the list of results, switch the **View** to 🗺.

The Network Map is displayed in the bottom pane; you can see the access route between the selected source (**development Servers**) and the selected destination (**Internet**).

At the bottom of the control panel, click **Network Map** to switch back to displaying only the map; the route remains visible.

6 Close the Network Map.

Viewing additional information about an entity

The Details pane displays detailed information for the entity selected in the Table pane. The information in the Details pane is divided into tabs according to the type of entity selected. By default, only tabs containing basic information are displayed, but you can display additional (advanced) tabs.

**To display advanced tabs**

1. With **All Network Devices > Firewalls > main_FW** selected in the Table pane, look at the Details pane.

   ![Firewall Details Pane]

   - **Asset**: main_FW [190.170.1.97]
   - **Type**: Firewall
   - **Status**: Up
   - **OS**: Juniper Solaris
   - **Platform**: Generic firewall 3.0.1774
   - **Forwarding**: Yes
   - **IPS Enabled**: No
   - **Other Names**: main_FW/hostname
   - **Firewall Type**: Check Point Firewall
   - **ACL Enabled**: Yes
   - **Dynamic Routing**: No
   - **Virtual Routing**: No
   - **Layer 2**: No
   - **Do Not Disable**: No

2. Click ⚪ to display additional tabs.

   You can now view information about the firewall’s network interfaces, services, patches applied, and more.
Viewing the properties of an entity

You can view the properties of any entity in the Details pane, and you can view and edit the main properties of each entity in a separate dialog box. In this exercise, you view the properties of **main_FW**.

**To view properties**

1. If **main_FW** is not listed in the Table pane, select **All Network Devices > Firewalls**.
   
   There are often several paths in the tree to reach the same entity. For example, you can also reach **main_FW** from **Locations & Networks > US > New York > gatewayEastA**.

2. In the Table pane, right-click **main_FW** and select **Properties**.

   ![Property dialog box](image)

   **Note:** In Skybox, firewalls (and other gateway devices) are classified as entities of type **Asset**.

3. Mouse over a field that contains data.
   
   A tooltip listing the values selected for that field appears. This is especially useful for fields that hold multiple values.

4. Click **Cancel**.

   To view additional information about an entity in a table, right-click the entity. For example, when you right-click a firewall, besides its properties, you can view its access rules, routing rules, or network interfaces.
Chapter 4

Configuration Compliance

This chapter explains working with Configuration Compliance in Skybox.

In this chapter

Configuration Compliance overview ....................................... 25
Viewing Configuration Compliance ........................................ 26
Viewing an overview of Configuration Compliance ................. 28

Configuration Compliance overview

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).

Configuration Compliance is analyzed by comparing a firewall’s configuration data with a Configuration Policy—the predefined policy included with Skybox or a customized policy created by your organization. Skybox shows where the configuration data does not comply with the policy.

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

The default set of Configuration Policies (Standard) checks your device files against known best practice guidelines for various platforms. You can customize the default set to suit your organization’s requirements and you can create additional policies as necessary. Each time a Configuration Policy is analyzed, all firewalls that match the policy’s scope are tested against all the Configuration Checks in that policy.

There is also an additional set of Configuration Policies for those whose companies must comply with STIG standards.
Viewing Configuration Compliance

To view Configuration Compliance

1. Expand the Configuration Policies node.

You can see that there is a policy folder named Standard v9. This is the folder that contains the predefined Configuration Policies. When you expand it, you can see these Configuration Policies.

Each Configuration Policy applies to a specific group of firewalls. For example, there is a policy for Check Point firewalls and a policy for NetScreen firewalls. The firewall type is specified in the properties of each policy.
2 Right-click **Cisco FW Standard Policy** and select **Properties**.

You can see that this policy applies to Cisco firewalls at all locations.

3 Close the Properties dialog box.

In the workspace, you can see a list of all the Configuration Checks in this policy, and whether there are violations.

Note: If you do not see any violations at all, click **[Analyze]** to analyze the firewalls for violations.
4 Select a Configuration Check in the Table pane to see its details in the workspace.

5 Click the **Analyzed Devices** tab.

You can see a list of the firewalls analyzed for this Configuration Check and which of these firewalls violated the Configuration Check. In the demo model, only the **vlab-cisco** firewall was analyzed; you can see the expected and actual results in the Details pane.

### Exporting Configuration Compliance information

**To export Configuration Compliance information for a firewall**

- In the tree, select **All Network Devices > Firewalls**. In the Table pane, right-click **vlab-cisco**, and select **Advanced > Export to CSV – Configuration Compliance**.

### Viewing an overview of Configuration Compliance

Skybox includes an overview (dashboard) of Configuration Compliance for all (analyzed) devices and all Configuration Policies.

**To view the overview**

- In the tree, select **Configuration Policies**.
The workspace displays a dashboard of compliance, where you can see overall configuration results grouped by Configuration Policy/Configuration Check and by device.

Use the links to drill down to detailed information.
Access analysis

Access analysis provides a holistic view of what is connected and what is not, based on topology and traffic rules (access, NAT, and routing rules).

In this chapter

Access Analyzer ................................................................. 30
What is accessible from the internet? ................................. 30
How can I tell if 2 networks are connected? ....................... 32

Access Analyzer

The Access Analyzer runs on the current model and finds all routes between the selected source and destination. For each destination asset, you can see:

- The ports that are exposed
- The access route between the source and the destination

The Access Analyzer is generally used:

- To troubleshoot connectivity between 2 points
- To plan changes

You can test the planned changes in Skybox to see if they work as expected (for example, to check whether the change in an access rule causes only the expected results or also additional results, for example, wider access than requested).

What is accessible from the internet?

In this exercise, you see what parts of the sample model are accessible from the internet.
To analyze access from the internet to your organization’s network

1. On the toolbar, click  

2. Verify that **Network Mode** (rather than **Firewall Mode**) is selected on the toolbar of the Access Analyzer.

3. Click the **Browse** button next to a **Scope** field.

4. Select **Internet [Perimeter Cloud]** and click **Source** to move it to the **Selected Source** field.

5. The **Scope** and **Services** fields of the destination are set to **Any**. Do not change them.

6. Click **OK**.

7. Click **Analyze**.

The results of the analysis appear in the Analysis Results pane.
8 On the toolbar (of the results pane), make sure that the **Group By** field is set to **Network**.

| Analysis Results |
|------------------|------------------|
| Show Accessible Destinations | Group By [Network], Authentication |

- Europe [16 IPv4, 1 TCP port]
- US [256 IPv4, 6 TCP/UDP ports]

9 Expand the results.
- Under the lowest locations are the accessible networks (MapView).
- Under each network is the range of IP addresses in the network that are accessible from **Internet**.

10 Expand 1 or 2 of the IP address ranges to see the services (MapView) through which the network can be accessed.

You can scroll inside the tree or resize the window to see the results better.

11 Select **US > NY > dmz > 192.170.33.0-192.170.33.255 > 80 (TCP)**.

The access route from **Internet** (the source) to this service is displayed in the map. The route is displayed to the left of the map.

Note: If you only see the map, click [View Route] to view both the map and the route.

How can I tell if 2 networks are connected?

This exercise explains how to use Skybox to check whether 2 networks are connected. Using Skybox, you can view the accessible routes and the blocked (inaccessible) routes between the 2 networks, in step-by-step format (as an access route) and graphically (on the Network Map).
To check access from the DMZ network to the Windows development network

1. Open the Access Analyzer (or, if it is already open, click to clear it).
2. Click the Browse button next to a Scope field.
3. Select US > New York > dmz and click to move it to the Selected Source field.
4. Select Europe > Paris > developmentWindowsWS and click to move it to the Selected Destination field.
5. Click OK.
6. Click Analyze.

A message in the Analysis Results pane states that there is no access between the source and the destination. When there is no access, you can use Skybox to view the blocked routes. This can be useful if the access is required and you want to know what must be changed to create access.

7. In the Show field on the toolbar of the Analysis Results pane, select Blocked Destinations.
8. Expand the list and select the blocked destination network.

In the Access Route pane, you can see where access was first denied (on prod FW). In the Network Map, you can see that there is a gap in the route.

To see what the route would be if access was not denied anywhere, in the Detail Level field select Display All Blocking Rules. The Access Route now lists the entire route, and the Network map displays the route.
Chapter 6

Network Access Compliance

This tutorial walks you through a typical Access Compliance scenario, using the data in Skybox’s demo model.

In this chapter

Network Access Compliance overview .................................... 34
Basic steps for Access Compliance ........................................ 34
What is an Access Policy? .................................................... 35
Classifying the network into zones ........................................ 37
Analyzing the Access Policy .................................................. 38
Understanding compliance metrics ........................................ 39
Understanding what caused a violation .................................. 41
Creating and editing exceptions ............................................ 43

Network Access Compliance overview

Network Access Compliance involves comparing the actual behavior of traffic in your organization’s network with industry-wide best practice standards (for example, NIST 800-41) and organization-specific standards. Results include compliance metrics for the network and for specific rules, and actual access routes between specific sources and destinations that enable you to understand what is connected or exposed between any 2 points in the network.

For example, a best practice guideline states that there must be no NetBIOS access from any external source to the organization’s DMZ. In Skybox, a rule was created stating that NetBIOS access must be blocked from external sources to the DMZ. When you check for Access Compliance, any route breaking this rule is displayed as a violation, together with the specific access rules that enabled the access.

Basic steps for Access Compliance

The following are the basic steps for managing network Access Compliance:
1 Build the model.
2 Select an Access Policy and map the areas of your network into specific zones (see page 37) according to their function.
   Skybox Network Assurance’s predefined Access Policies are defined in terms of these zones. When you map the networks (using Mark as Zone), the selected Access Policy is applied automatically and can be tested.
3 Analyze the Access Policy (see page 38) to obtain access violations and compliance metrics.
4 Review the violations to decide how to resolve them. See Understanding compliance metrics (on page 39) and Understanding what caused a violation.
5 Make the necessary changes.

What is an Access Policy?

An Access Policy is a set of rules (Access Checks) defining the constraints on the traffic in a network. These rules verify that users can access essential assets while there are no security holes exposed by firewall access rules. There are predefined Access Policies for NIST 800-41 guidelines and for PCI DSS guidelines.

You can apply a predefined policy (or any other policy) to any environment by mapping your organization’s networks to the zone types used by the policy. A zone type is a way of grouping networks that have the same trust level. For example, an organization’s DMZ network is mapped to the DMZ zone type, while the internet and other external networks are mapped to the External zone type. To verify compliance, the zone types used in the predefined policy are translated into the mapped networks as each policy rule is tested. For example, an Access Check that checks that NetBIOS access is blocked from External zones to DMZ zones is tested separately for the internet to the DMZ network and for each of the other external networks to the DMZ network.

To view the Access Policy
1 In the tree, expand the Access Policies > Public Access Policies node.
   The Public Access Policies node contains 2 policies (NIST and PCI), in addition to several sets of access queries.
   1. Expand the NIST 800-41 & Application > NIST External Access folder.
   The folder is divided into policy sections: NIST-External to Partner, NIST-External to DMZ, and NIST-External to Internal. Each policy section specifies the desired access relationship between 2 specific zones.
3 When you expand these policy sections, you can see the Access Checks in each section.

Some Access Checks in different policy sections have similar names because they test the same type of access (for example, that all Trojan and worm ports are blocked), but between different areas or zones in the network. For example, in the External to DMZ policy section, the Block Trojan and Worm Ports Access Check tests that there is no access to Trojan and worm ports in the DMZ zone from the external zone; in the External to Internal policy section, the Access Check with the same name tests that there is no access to Trojan and worm ports in the internal zone from the external zone.

Customizing the Access Policies

The predefined Access Policies tree includes a policy that includes NIST 800-41 and other industry-wide best practice guidelines, and another policy for PCI DSS. However, most organizations have additional best practice guidelines of their own; you can add these guidelines to the appropriate policy in the form of custom Access Checks and custom zones, or you can add them as a separate Access Policy. You can modify or disable Access Checks.
Classifying the network into zones

To check your organization’s network for compliance to best practice guidelines, you must classify areas in the model into zones. For example, if you classify a specific network as your DMZ and 2 partner clouds as Partner zones, the Access Checks that test connections between DMZ and partner zones can check compliance in your network.

Note: There are separate zones for predefined policies. Use PCI zones only when you are doing a PCI audit.

To classify a network as a zone
1. Open the **Model** workspace.
2. In the tree, expand **Locations & Networks > US > New York**.
3. Right-click the **dmz** network and select **Mark as Zone**.

The **dmz** network is marked as a zone of type **DMZ**.
4. Open the **Zone Type** drop-down list to see the other types of zones.
5. Click **Cancel**.

To view the network zones
1. Open the Network Assurance workspace.
2. In the tree, expand the **Access Policies** node and then click the **Zones** node.
3. In the Table pane, click **DMZ**.

The **dmz** network is the only regular network that is marked as a DMZ zone.
4. Click (on the toolbar) to return to the list of zones.
5. Click **Internal**.
Some networks are classified as Internal zones. When an Access Check tests access between Internal zones and the DMZ zone (or any other type of zone), access between each of these networks and the DMZ network is tested separately.

To test access between other types of networks, you can create additional zone types to represent these types of networks and then create Access Checks to test the access between them.

Analyzing the Access Policy

After the networks are classified into zones, you analyze compliance with the Access Policy.

During this analysis, 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 following examples describes part of a sample organizational network and the tests that are created using the default Access Policy zones.

Example 1

- Network A is a DMZ (and is marked as a DMZ zone)
- Network C is Internal (and is marked as an Internal zone)

For an Access Check in the policy named **Block Login Services**, a single access test (Network A to Network C) is created.

Example 2

The networks in the organization are assigned to the following zones:

- Network A: DMZ
- Network B: DMZ
- Network C: Internal
- Network D: Internal

For the **Block Login Services** Access Check, the following access tests are created:

- Network A to Network C
- Network A to Network D
- Network B to Network C
- Network B to Network D

Thus, the result of marking zones is that all the necessary tests are created to verify the Access Policy.
Analyzing compliance

To analyze compliance (for all Access Policies)

1. In the Tree pane, select Access Policies.
2. On the toolbar, click Analyze.

Note: You can use the same method to analyze compliance for any node in the Access Policies tree.

Understanding compliance metrics

After the Access Policies node is analyzed, compliance of your organization’s network with the predefined Access Policies is displayed. You can view metrics for the node and for each Access Policy, policy section, and specific Access Check.

To view policy metrics

2. Expand the NIST-External Access folder so that you can see the policy sections.

In the tree, you can see the compliance percentages for the folder and for each policy section. In the workspace, you can see:

- A link to the violating rules for this folder
- The compliance metrics for the folder
- Compliance percentages for each of the policy sections, with links.
The pie chart and table show the compliant and noncompliant tests.

Note: Policy sections and Access Checks for which there are no zones marked in the model do not create tests (and do not display compliance metrics after analysis).

3. In the tree, select **NIST External to DMZ**.

4. Click the **Violating Rules** link to view the access rules that caused the violations to this policy section.

You can see that 1 of the violating access rules is on **main_FW**.

5. Right-click that rule and select **Open in ACL Editor**.

You can see the violating access rule in the context of all the other access rules for this firewall. Close the Access Control List Editor when you are finished.

6. In the Details pane, you can see all the violations caused by this violating access rule. When you click the **Rule Details** tab, you can see additional information about the access rule.
Understanding what caused a violation

This section explains how to view access information for violations. When you understand what caused the violation (that is, why the access test failed), you can try to work out an appropriate solution.

*To view access information for a violation*

1. On the toolbar, click to view the list of policy sections.
2. Select **NIST-External to DMZ**.
3. Click the **Violations** tab.

The Table pane lists the violations for this policy section.

You can see that for this policy section, there are a number of violating Access Checks.

The Details pane contains information about the first violation, with the **Details** tab displayed.

You can see that the name of the rule is **Limited DNS Access** and that this is a Medium violation.

4. Switch to the Violation Explanation tab. You can see that the access test failed because there is too much access between the internet cloud and the dmz network; the Access Check specifies that only 5 destination IP addresses should be available to each service.

5. Click the **Access Results** tab to view the access between the source and the destination.

6. Expand the tree and select a lowest-level node.
7 Click **Show Access Route**.

*Access routes* show the devices and specific access rules through which access passes in the network.

The Access Route Details dialog box shows the accessible route. In this case, there is access to the IP address range **192.170.33.0.-192.170.33.255** via the service (port) **53/TCP**. Access is permitted through inbound access rule **2** of **main_FW** and then passed through **prod FW** also.
8 Click the link to access rule 2 (of main_FW).

You can see information about the access rule in the list of access rules and in the rule objects in the tree on the right-hand side of the dialog box. The Matched Objects information at the top shows how the access rule was matched.

Close the Rule Match Details dialog box and the Access Route Details dialog box.

Creating and editing exceptions

Exceptions are a way to fine-tune the policy according to actual practices or requirements of your organization. Sometimes, specific entities in a location or zone that you are testing have different access permissions from the rest of the entities in that location or zone. Mark these entities as exceptions to the Access Check so that they are not tested.

In our example, it was realized that access over 21(TCP) between the internet and internal networks does not violate your organization’s Access Policy—mark it as an exception.
**To mark exceptions**

1. In the Access Results tree, select the **21 (TCP)** node and click ![Mark as Exception].

2. In the **User Comments** field, type **Access Permitted on 21 (TCP)** and click **OK**.

As this is the only port that violated the Access Check, the test no longer violates the policy and a green compliance indicator (✓) is displayed next to the ID of the test.

You can view and edit exceptions.
To edit an exception

1. In the tree, right-click the Access Check that you are working with (NIST External Access > NIST-External to Internal > No Access – non-specified services) and select Exceptions.

2. In the Exceptions dialog box, select the exception created in the previous exercise and click Modify.

3. As it is not necessary to change the exception’s properties, click Cancel.
Chapter 7

Change management

This tutorial explains various ways to view and manage firewall changes.

In this chapter

Change management in Skybox ............................................ 46
Managing changes .............................................................. 46
Testing changes with the What If model ......................... 47
Analyzing changes .............................................................. 48
Viewing changes to access rules between models .............. 49

Change management in Skybox

You can use Skybox to help manage firewall changes by:

▷ Monitoring the changes
▷ Managing a workflow for firewall change requests in Skybox Change Manager directly or by using the API
▷ Using Skybox features:
  • To check network connectivity
  • To create and test a what-if scenario and see if it has the required results

Managing changes

You can use the following components of Skybox to aid the change management process:

▷ Change tracking
  • In Skybox Firewall Assurance, there is a fully automated feature that enables you to view changes for all firewalls or for a single firewall.

▷ Skybox Change Manager and API
  • Skybox includes Skybox Change Manager, a web interface for change management. For additional information, see the Skybox Change Manager User’s Guide.
  • The API for change management fully supports ticket management, access analysis and compliance checking.

For additional information, see the APIs part of the Skybox Developer’s Guide.
Some organizations use Skybox Change Manager, others prefer to leverage Skybox infrastructure using the API.

You can use the following Skybox features to aid the change management process for ad hoc tasks:

▶ Access Analyzer

You can use the Access Analyzer to find the firewalls that block connectivity between a source and a destination; you can see the exact access rules that are causing the blockage or whether the path is broken. You can then use this information to plan changes.

- For additional information about the Access Analyzer, see Access analysis (on page 30).

▶ What-if

Skybox provides a virtual sandbox, the What If model. Using this model, you can modify the ACLs of firewalls and even change the network topology. You can then use the Access Analyzer to check the impact of the changes. You can compare the differences in the GUI or generate a report that summarizes the changes in the ACLs. (The following sections explain how to use the What If model for change assurance management.)

▶ Historical incident analysis

In Skybox Network Assurance, you can load a backup model to the Forensics model. (You can automate this to run on a regular basis using Model – Copy tasks.). You can then use the Forensics model as a reference model and check the previous state of the network (map and asset list) and firewall configurations.

Testing changes with the What If model

Skybox supports a What If model, where you can simulate the effect of solutions before applying them to your organization’s network. Use this model to test planned changes to architecture or to firewall and router configurations. You can analyze potential risks from the changes without causing any harm to your organization’s network and without changing the Live model.

Loading the What If demo model

To test changes, you must load the What If demo model file to the What If model so that Skybox can compare it to the Live model. The information in this file is similar to that in the demo model file, but with some changes to access rules and other entities that simulate changes that might be made to devices in the organization’s network.
To load the What If demo model

1. Select **File > Models > Load.**
2. In the **Model** field, select **What If.**
3. In the **File** field, select the **What If** demo model file (DemoModel-WhatIf.xml).
4. In the Load Scope pane, select **Model** only.
5. Click **OK** and then click **Yes.**

The What If model does not include a Vulnerability Dictionary. If you are asked whether to use the Dictionary from the Live model, click **OK.**

6. Switch to the What If model: on the toolbar, select **What If** from the drop-down list.

When you are working with an actual model, the usual way to way to create a What If model is to copy it from the Live model (**Files > Model > Create Model** where **Source Model** = Live and **Target Model** = What If).

Once you have a What If model, you can make changes (in the What If model) to a firewall’s access rules, network interfaces, or routing rules, and view the effects of these changes.

After you make changes, you can use the Access Analyzer to test access and see whether it works as expected. You can also examine the differences between access in the Live model and access in the What If model, as explained in the following section.

Analyzing changes

You can use Skybox Network Assurance to simulate and view access changes.

To analyze changes

2. Select the **Limited SMTP Access– (5Dest.IPs)** Access Check.
3. At the top of the Table pane, click the **All Access Tests** tab.
4. In the Table pane, select the test.
5. In the Details pane, click the **Access Results** tab.
6 Click Live.

The selected access tests in the What If and Live models are analyzed. The results are displayed side-by-side.

The compliance indicators show that the access limit is exceeded in the Live model but changes made to the access rules of the What If model brings the number of accessible routes under control.

In the Live results tree, the [x] on the service icon of 25(TCP) means that the limit is exceeded—access is available on 256 IP addresses, not the requested 5 or less.

7 Expand the Live results tree to see the range of available IP addresses.

Viewing changes to access rules between models

You can view differences in access rules, routing rules, and network interfaces between models. You can compare the Live model to previous models using the Forensics model or to the What If model so that you can see the effect of planned changes.

When comparing these entities, you can see new, deleted, and changed entities. When comparing access rules, you can also see changes in firewall objects. You can present differences in access rules in Skybox reports.
To view changes to access rules between models

1. In the tree, select the **All Network Devices** > **Firewalls** > **main_FW** node.
2. In the table, right-click **main_FW** and select **Advanced** > **Compare** > **Access Rules to** > **Live**.
3. In the Compare dialog box, click **Show Resolved Addresses**.

You can see various changes between the models.

Note: Make sure you switch back to the **Live** model when you are finished.
Chapter 8

Using Skybox reports

Reports in Skybox are detailed accounts of specific data in the model (for example, Access Policy violations or overdue tickets).

In this chapter

Reports tree ................................................................. 51
Report definitions .......................................................... 51
Report types .................................................................. 51
Network Access Compliance reports .......................... 52

Reports tree

Use the Reports tree to manage report definitions and to generate and view reports. Reports can be emailed to selected users. You can schedule report generation.

The Reports tree is divided into a public folder and a private folder; predefined reports are in the public folder and report definitions that you create are stored in your private folder. You can add subfolders for additional grouping. For example, if you have several Access Policies, you can have separate folders for reports about each of them.

Report definitions

Individual reports are generated from report definitions. A report definition is a template for reports that specifies:

› What information to display
› How to display it
› What output format to use for the report
› (Optional) A list of users who receive the report by email

Skybox Network Assurance includes several predefined definitions for each type of report. The scope of each predefined report definition is the model.

Report types

Skybox Network Assurance has several types of reports:

› Network Access Compliance reports (on page 52): Show the status of the Access Policy and provide policy-related statistics for your organization’s
network. You can use detailed Access Policy reports to understand Access Policy violations.

- Network Configuration Compliance reports: Show the status of the Configuration Policy and provide policy-related statistics for your organization's network. Detailed reports provide information about Configuration Policy violations.

- Tickets reports: Show information about workflow tasks (tickets). You can use ticket reports to track the workflow of policy violations. They are used for remediation.

- Policy Document reports: List the Access Checks in all or part of the Access Policy.

**Network Access Compliance reports**

Network Access Compliance reports enable you to document Access Policy violations that are detected by Skybox and distribute this information to others.

If Access Compliance was not analyzed before you generate a Network Access Compliance report, the report will be empty. If you have worked through the tutorials in order, you already analyzed compliance for the Access Checks in **Public Access Policies > NIST 800-41 & Application > NIST External Access** and this information is used as the basis of the report. Otherwise, analyze at least 1 policy folder before using the following instructions to generate a report.

*To generate a Network Access Compliance – Details report*

1. In the Reports workspace, select **Public Report Definitions > Network Compliance > Network Compliance – Details**.

   The workspace displays the properties of the report.
2 Click **Generate** and then click **OK**.

3 Navigate to the **Access Policy Violations** section of the report.

This section contains a list of the Access Policy violations for each policy section at the network level, sorted by severity.

<table>
<thead>
<tr>
<th>Policy Section</th>
<th>NIST-External to DMZ (71% compliance)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source:</td>
<td>External Zones</td>
</tr>
<tr>
<td>Destination:</td>
<td>DMZ Zones</td>
</tr>
<tr>
<td>Path:</td>
<td>Public Policy / NIST 800-41 Policy / NIST External Access / NIST-External to DMZ</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Access Check Name</th>
<th>Test ID</th>
<th>Source</th>
<th>Destination</th>
<th>Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Limited DNS Access- (5 Dest. IPs)</td>
<td>5924</td>
<td>Internet [Perimeter Cloud]</td>
<td>dmz [192.170.33.0 / 24]</td>
<td>domain_t [53/TCP], domain_u [53/UDP]</td>
</tr>
<tr>
<td>No Access - non-specified services</td>
<td>254100</td>
<td>Internet [Perimeter Cloud]</td>
<td>dmz [192.170.33.0 / 24]</td>
<td>Any</td>
</tr>
</tbody>
</table>

For each violation, you can see the Access Check name, severity, test ID, source, destination, and services.

When you click the link of a violation in the test ID, you see detailed information about the violation in the **Policy Violations – Details** section of the report, including the destination IP addresses and ports that are accessible from the source.