Skybox Network Assurance

User Guide

10.0.200

Revision: 11
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intended audience</td>
<td>6</td>
</tr>
<tr>
<td>How this manual is organized</td>
<td>6</td>
</tr>
<tr>
<td>Related documentation</td>
<td>6</td>
</tr>
<tr>
<td>Technical support</td>
<td>7</td>
</tr>
<tr>
<td>Overview of Skybox Network Assurance</td>
<td>8</td>
</tr>
<tr>
<td>Skybox platform</td>
<td>8</td>
</tr>
<tr>
<td>Highlights of Skybox Network Assurance</td>
<td>10</td>
</tr>
<tr>
<td>Basic architecture</td>
<td>15</td>
</tr>
<tr>
<td>Skybox deployment</td>
<td>16</td>
</tr>
<tr>
<td>Planning deployment</td>
<td>16</td>
</tr>
<tr>
<td>Deployment plan</td>
<td>16</td>
</tr>
<tr>
<td>Deployment team</td>
<td>17</td>
</tr>
<tr>
<td>Phases of deployment</td>
<td>17</td>
</tr>
<tr>
<td>Preparing data for Skybox</td>
<td>18</td>
</tr>
<tr>
<td>Building the model</td>
<td>20</td>
</tr>
<tr>
<td>Building the network model</td>
<td>21</td>
</tr>
<tr>
<td>Validating the model</td>
<td>30</td>
</tr>
<tr>
<td>Overview of validating the model</td>
<td>31</td>
</tr>
<tr>
<td>Best practices for model validation</td>
<td>32</td>
</tr>
<tr>
<td>Model validation tasks and analyses</td>
<td>33</td>
</tr>
<tr>
<td>Access Analyzer test queries</td>
<td>40</td>
</tr>
<tr>
<td>Network Map visualization</td>
<td>41</td>
</tr>
<tr>
<td>Task error messages</td>
<td>42</td>
</tr>
<tr>
<td>Item counts</td>
<td>43</td>
</tr>
<tr>
<td>Creating Perimeter Clouds automatically</td>
<td>43</td>
</tr>
<tr>
<td>Network Map</td>
<td>44</td>
</tr>
<tr>
<td>Overview of the Network Map</td>
<td>44</td>
</tr>
<tr>
<td>Creating and saving dedicated maps</td>
<td>45</td>
</tr>
<tr>
<td>Navigating the Network Map</td>
<td>47</td>
</tr>
<tr>
<td>Map Groups</td>
<td>49</td>
</tr>
<tr>
<td>Creating Map Groups</td>
<td>49</td>
</tr>
<tr>
<td>Map Group hierarchies</td>
<td>50</td>
</tr>
<tr>
<td>Working with Map Groups</td>
<td>50</td>
</tr>
<tr>
<td>Configuration Compliance</td>
<td>52</td>
</tr>
<tr>
<td>Overview of Configuration Compliance</td>
<td>52</td>
</tr>
<tr>
<td>Viewing Configuration Compliance</td>
<td>53</td>
</tr>
<tr>
<td>Viewing violations in the configuration file</td>
<td>54</td>
</tr>
<tr>
<td>Network Configuration Compliance reports</td>
<td>56</td>
</tr>
</tbody>
</table>

Skybox version 10.0.200
<table>
<thead>
<tr>
<th>Skybox Network Assurance User Guide</th>
</tr>
</thead>
</table>

| Customizing a Configuration Policy ........................................................................57 |
| Creating and editing Configuration Policies ..............................................................57 |
| Creating Configuration Checks ..................................................................................58 |
| Exporting and importing Configuration Policies ..........................................................64 |

| Access Analyzer .................................................................................................66 |
| Access Analyzer overview ...................................................................................66 |
| Creating new queries .........................................................................................67 |
| Defining the source and the destination ...............................................................67 |
| Defining the scope for network queries ...................................................................70 |
| Defining the services .........................................................................................71 |
| Additional destination options .............................................................................71 |
| Understanding the results .....................................................................................72 |
| Inaccessible entities ..............................................................................................75 |
| Saving an access query as an Access Check .........................................................77 |
| Saving the results ..................................................................................................78 |

| Network Access Compliance ...............................................................................80 |
| Network Access Compliance overview .................................................................80 |
| About Access Policies ..........................................................................................80 |
| Predefined Access Policies ................................................................................81 |
| Use cases for network Access Compliance ..........................................................82 |
| Access Policy management ..................................................................................83 |
| Structure of the predefined Access Policy ...........................................................83 |
| Zone mapping .......................................................................................................89 |
| Exporting and importing Access Policies ...............................................................91 |
| Access Policy analysis .........................................................................................92 |
| Troubleshooting analysis ....................................................................................93 |
| Access Policy compliance and violation management .............................................93 |
| Reviewing compliance metrics ............................................................................93 |
| Reviewing the violating access rules ....................................................................94 |
| Viewing violations ...............................................................................................95 |
| Viewing access results .......................................................................................96 |
| Handling policy violations .................................................................................101 |
| Network Access Compliance reports ..................................................................103 |
| Access Policy customization ...............................................................................104 |
| Customizing policy sections ................................................................................105 |
| Defining exceptions ..............................................................................................105 |
| Creating policy sections ......................................................................................107 |
| Creating zone types ..............................................................................................113 |
| Full Access Checks .............................................................................................113 |
| Access queries ......................................................................................................114 |
| Access Checks reports ........................................................................................114 |
| Firewall ACLs .......................................................................................................115 |
| Comparing access rules between models .............................................................115 |
| Comparing access rules between firewalls ..........................................................117 |
| Comparing routing rules and network interfaces ................................................118 |
Preface

Intended audience

The *Skybox Network Assurance User Guide* explains how work with Skybox Network Assurance. Use this document in conjunction with:

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

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

How this manual is organized

This manual includes the following chapters:

- **Overview of Skybox Network Assurance** (on page 8)
- **Introduction to building the model** (on page 16)
- **Network Map** (on page 44)
- **Configuration Compliance** (on page 52)
- **Access Analyzer** (on page 66)
- **Network Access Compliance** (on page 80)
- **Auditing the network on a continuous basis** (on page 119)
- **Advanced modeling scenarios** (on page 127)

Related documentation

The following documentation is available for Skybox Network Assurance:

- *Skybox Network Assurance Getting Started Guide*

Other Skybox documentation includes:

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

The entire documentation set (in PDF format) is available [here](#).

You can access a comprehensive Help file from any location in 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 you open a case, you need:

› 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 Network Assurance

This chapter is an overview of Skybox Network Assurance.

In this chapter

Skybox platform ................................................................. 8
Highlights of Skybox Network Assurance ......................... 10
Basic architecture .............................................................. 15

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, 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 additional information visit the Skybox 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 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 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>Firewall 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>L2 FW</td>
<td>192.170.22.203</td>
<td>Generic OS</td>
<td>11/5/09 11:15 AM</td>
<td>1/1/2010 1:04 AM</td>
<td></td>
</tr>
<tr>
<td>main_FW</td>
<td>192.170.1.97</td>
<td>Solaris</td>
<td>11/5/09 4:30 AM</td>
<td>1/1/2010 1:04 AM</td>
<td></td>
</tr>
<tr>
<td>noc_FW</td>
<td>192.170.1.49</td>
<td>StreamOS</td>
<td>5/4/18 0:00 AM</td>
<td>1/1/2010 1:04 AM</td>
<td></td>
</tr>
<tr>
<td>PA-2020 sys1</td>
<td>172.20.0.252</td>
<td>PAN-OS</td>
<td>5/4/18 0:00 AM</td>
<td>1/1/2010 1:04 AM</td>
<td></td>
</tr>
<tr>
<td>PA-2020 sys2</td>
<td>172.20.0.252</td>
<td>PAN-OS</td>
<td>5/4/18 0:00 AM</td>
<td>1/1/2010 1:04 AM</td>
<td></td>
</tr>
<tr>
<td>PA-Vm sys1</td>
<td>172.20.0.249</td>
<td>PAN-OS</td>
<td>5/4/18 0:00 AM</td>
<td>1/1/2010 1:04 AM</td>
<td></td>
</tr>
<tr>
<td>prod FW</td>
<td>192.170.33.1</td>
<td>IPSO</td>
<td>10/4/09 4:30 AM</td>
<td>1/1/2010 1:05 AM</td>
<td></td>
</tr>
<tr>
<td>US_ECE01</td>
<td>172.20.0.54</td>
<td>Generic OS</td>
<td>7/2/2014 4:27 PM</td>
<td>1/1/2010 1:05 AM</td>
<td></td>
</tr>
<tr>
<td>US_ECE02</td>
<td>172.20.0.56</td>
<td>Generic OS</td>
<td>7/2/2014 4:27 PM</td>
<td>1/1/2010 1:05 AM</td>
<td></td>
</tr>
<tr>
<td>VCloudPoller_10.0.0.016</td>
<td>10.0.1.0</td>
<td>10.0.1.0</td>
<td>7/6/15 2:46 PM</td>
<td>1/1/2010 1:05 AM</td>
<td></td>
</tr>
<tr>
<td>Vlan-cisco</td>
<td>172.20.0.18</td>
<td>ASA</td>
<td>8/4(2)</td>
<td>5/14/14 4:30 PM</td>
<td>1/1/2010 1:05 AM</td>
</tr>
<tr>
<td>14 Assets</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></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.

- **Configuration Policies**
  - **Standard v9**
    - 1.1 Checkpoint FW Standard Policy
      - 1.1.1 VPN-1/FW-1 control connections - prohibited (2 FWs)
      - 1.1.2 Client access management - restricted
      - 1.1.3 UDP reply packets - filtered (3 FWs)
      - 1.1.4 RIP traffic - filtered
      - 1.1.5 Domain TCP traffic - filtered
      - 1.1.6 Domain UDP traffic - filtered
      - 1.1.7 ICMP traffic - filtered
      - 1.1.8 Logging of implied rules - required (2 FWs)
      - 1.1.9 clear-text topology downloads - prohibited
      - 1.1.10 Established TCP packets logging - required
      - 1.1.11 Certificate Revocation List (CRL) check - required
      - 1.1.12 Gateway filtering in both directions - required
      - 1.1.13 Control on decryption of accepted packets - required (3 FWs)
    - 1.2 Cisco IOS RTR Standard Policy
    - 1.3 Netscreen FW Standard Policy
    - 1.4 Cisco FW Standard Policy
    - 1.5 Palo Alto Networks Standard Policy
    - 1.6 Fortinet FW Standard Policy
    - 1.7 Juniper JUNOS Standard Policy

Access analysis

You can use Access Analyzer to:

- Troubleshoot connectivity issues; 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 device to permit or deny access

Access Analyzer can provide answers to questions including:

- 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 policy as defined by NIST or PCI baselines.
You can view a summary of network Access Compliance.

### Public Access Policies - 89% Compliance

- **18 Violating Rules**
- **2 Compliant**
- **16 Noncompliant**

**Analyzed:** 10/15 4:39 PM

<table>
<thead>
<tr>
<th>Compliant Tests</th>
<th>Info</th>
<th>Low</th>
<th>Medium</th>
<th>High</th>
<th>Critical</th>
<th>Overall</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>706</td>
<td>392</td>
<td>152</td>
<td>1</td>
<td>1,249</td>
</tr>
<tr>
<td>Noncompliant Tests</td>
<td>0</td>
<td>0</td>
<td>145</td>
<td>14</td>
<td>2</td>
<td>161</td>
</tr>
<tr>
<td>Overall</td>
<td>0</td>
<td>0</td>
<td>880</td>
<td>406</td>
<td>154</td>
<td>1,410</td>
</tr>
</tbody>
</table>

### 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

Skybox deployment

This chapter explains how to build and validate a model of your organization in Skybox.

The Skybox model (*the model*) is a schema in the Skybox database that represents all or part of your organization’s network. This is the model that you build—it is used for vulnerability occurrence profiling, attack simulation, risk analysis, and planning mitigation.

In this chapter

- Planning deployment ........................................................... 16
- Building the model .............................................................. 20
- Validating the model ........................................................... 30

Planning deployment

Before you begin deployment on a large network, create a deployment plan and put together a deployment team from all departments involved in the project. Then you must prepare the data.

DEPLOYMENT PLAN

Before you begin deploying Skybox on a large network, create a deployment plan. This plan should include:

- The deployment team
  
  A list of the people who should be involved in the deployment project, their contact information, and the time required from them. For additional information, see Deployment team (on page 17).

- A scope for the deployment
  
  The parts of the network and the Business Units that the deployment is to cover.

- The network data required for deploying Skybox
  
  1. Understand the structure of your network, by using network diagrams and interviewing network administrators.

  2. Prepare the network data for Skybox, including scan results, network diagrams, firewall configuration files, and so on. For additional information, see Preparing data for Skybox (on page 18).
Chapter 2    Skybox deployment

A project timeline
If this is a large deployment, we recommend that you divide it into phases, where each phase has a clear value-adding milestone as its endpoint (see Phases of deployment).

The hardware required for deploying Skybox
This includes a dedicated host for the Skybox Server and, probably, hosts for the Skybox Collector nodes (not necessarily dedicated). For additional information, see the Server system requirements topic in the Skybox Installation and Administration Guide.

For small networks, a complete plan is not crucial, but greatly facilitates the deployment. At a minimum, a plan for a small network should include the deployment team and the scope of deployment, as much network data as possible, and at least 1 dedicated host for Skybox.

Skybox Professional Services personnel, certified resellers, and implementation partners are trained to assist you in building a deployment plan. For information about contacting Skybox, see Technical support (on page 7).

DEPLOYMENT TEAM
Deploying Skybox in a large organization might involve people from several departments, sometimes from different business units. Deploying Skybox Network Assurance alone generally only involves people from the networking department.

Getting the support and cooperation of these people is important for a quick and successful deployment of Skybox; involve them from the early stages of deployment.

Some of these people will use the product directly, some will receive output (reports and notifications), and some will only provide required information. Those who will use the product might benefit from training. To set up training sessions, contact Skybox Support.

PHASES OF DEPLOYMENT
If you are deploying Skybox in a large organization, it is useful to divide the project into phases and to define clear milestones for each phase in both of the following aspects:

Organizational
Complete deployment for a single business unit or division and then continue to the next.

Geographical
Complete deployment for a specific site or location and then continue to the next.

These aspects are not mutually exclusive and can sometimes be used in parallel.
PREPARING DATA FOR SKYBOX

This section explains what data is required for Skybox and how to prepare it.

Information requirements

Getting all required information is a crucial part of Skybox deployment. The required information includes:

- Network information, including basic architecture and which networks host the production servers
- Information about each firewall and other network device, including:
  - The credentials required for access
  - Skybox Collector
  - Data source (online collection / import from files)
  - Location

The more information that you have ready in advance, the faster your deployment project will go. However, you do not need to wait until you have information about all the devices to start the deployment; additional devices can be discovered during the deployment project.

The following sections provide details about preparing the necessary information.

Preparing a list of network devices

After you decide the scope of the network to include in the model, you must get data about each network device in the selected scope.

Prepare a list of the network devices in the scope, including all firewalls, routers, and other L3 devices, and all filtering devices (L2 or L3).

Example list

<table>
<thead>
<tr>
<th>Type</th>
<th>Vendor / Version</th>
<th>Main IP address</th>
<th>Credentials</th>
<th>Skybox Collector</th>
<th>Collection type: Online / Files</th>
<th>Location</th>
<th>Owner</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>FW</td>
<td>FireWall-1 NG</td>
<td>192.168.80.80</td>
<td>SB user/</td>
<td>Paris Collector</td>
<td>Online</td>
<td>Paris - DC1</td>
<td>Jon Smith</td>
<td>Main ISP firewall</td>
</tr>
<tr>
<td>FW</td>
<td>Cisco ASA 8.x</td>
<td>192.168.87.10</td>
<td>SB user/</td>
<td>London Collector</td>
<td>Online</td>
<td>London - DC4</td>
<td>Harry White</td>
<td>Internal network firewall</td>
</tr>
<tr>
<td>Router</td>
<td>Cisco 76xx IOS 12.x</td>
<td>192.168.86.10</td>
<td>SB user/</td>
<td>London Collector</td>
<td>Online</td>
<td>London - DC4</td>
<td>Harry White</td>
<td></td>
</tr>
</tbody>
</table>

Supported data sources

The Skybox platform is compatible with many data sources. Some of the most common are:

- Firewalls
  - Check Point FireWall-1 NG and NGX
  - Check Point Provider-1
  - Cisco PIX/ASA/FWSM

- Routers
  - Cisco IOS

Refer to the Skybox website for a list of supported devices.
Defining the data collection strategy

Define a collection strategy for each network device to be modeled. Refer to the Skybox website for a list of supported devices to discover which network devices are directly supported by Skybox. Mark devices that are not supported directly; each device must be modeled separately (see Modeling unsupported devices (on page 20)).

Skybox supports the following methods of retrieving data from directly supported devices:

- Offline file import: Extract the data from files written by the device. The data files are imported into Skybox using an offline file import task.
- Online collection: Retrieve the data directly from the device or the device management system. You create a task in Skybox, which instructs the Skybox Collector to retrieve the data from the device. This data is then added to the model.

The primary reasons for selecting one strategy over the other are the presence of a data repository, device accessibility, and the rate of changes to the device.

Offline file import is usually used for:

- Devices whose information is stored in a repository.
  If your organization has a repository that contains the necessary data for specific devices, you can import data from the repository into Skybox.
- Devices that cannot be accessed easily by a Skybox Collector.

  Note: If the device is in a segmented network, the alternative is to install an additional Skybox Collector in that network segment.

- Devices for which you do not have the necessary access permissions retrieving the configuration and routing data.
- Devices managed by a team that does not permit you continuous access.
- Infrequently updated devices.
  For infrequently updated devices, you could receive an alert (reminder) and then import the data manually rather than including them in the automated collection.

Online collection is usually used for:

- Devices that are easily accessible and whose configuration and routing information is not stored in a central repository.
- Devices managed by management servers that are supported by Skybox.
- Frequently updated devices.

Installing additional Collectors

For regular deployments, the default Collector installed on the Skybox Server machine as part of the full installation is sufficient.

Additional Collectors are required if:
(Remote data sources) Data sources (devices, file repositories, or another Skybox Server) are installed in remote segments that are isolated by firewalls; the default Collector cannot connect to them.

Solution: For each remote segment, install an additional Collector that can communicate with the Skybox Server over HTTPS on port 8443.

A data source permits only local access: Reading the data source is permitted only on the machine that hosts the data source.

Solution: Install an additional Collector on the data-source machine.

Collector-network connectivity

Each Skybox Collector must have a connection to the networks from which it collects data:

- The Collector needs access to the network. Permissions vary according to device type; information is available in the Skybox Reference Guide.
- For downloading data gathered by a scanner, a connection that has normal permissions is sufficient.

Preparing the data

For each network device that is to be imported, ascertain the files that Skybox requires to model the device and make sure that these files are available. For example, for a Cisco router, Skybox requires the output of the `show running-config` and `show ip route vrf *` commands, stored in separate files. For detailed information, see the Data formats for file import tasks topic in the Skybox Reference Guide.

Devices whose data is actively collected might require advanced preparation. For detailed information, see the section about the relevant device in the Tasks part of the Skybox Reference Guide.

Modeling unsupported devices

You can model devices that are not directly supported by Skybox by:

- Creating a script to translate the device configuration to Skybox Integration XML (iXML) format and import the device data.
  - For information about iXML, see the Integration part of the Skybox Developer Guide.
  - Contact Skybox Support if you need help creating the script.
- Modeling the device manually in Skybox.
  This is the simplest method to use if you have only a few devices that are not directly supported. However, if you make changes to any of these devices, you must update them manually in Skybox.

Building the model

After you have gathered as much information about your network as possible, you can begin building the model. We recommend that you start with a relatively small 1st phase.
BUILDING THE NETWORK MODEL

To build the network model, create and run tasks for online collection and offline file import of data from the network devices that you specified in Preparing a list of network devices (on page 18).

To build the network model

1. Click Operational Console.
2. In the Operational Console tree, select the Tasks node.
3. For each set of devices that you want to import, create a task to import their configurations:
   - Click New Task.
     - For information about importing device data offline, see the File import tasks chapter in the Skybox Reference Guide.
     - For information about device-specific online collection tasks, see the Tasks part of the Skybox Reference Guide.
4. After you run each task, check that it succeeded:
   a. In the Operational Console, select Tasks > All Tasks.
   b. In the Table pane, locate the task and check that the task Exit Code is Success.
      If a task fails, check the Messages tab of the Details pane for information about what went wrong.
5. Verify that the import is correct and complete:
   a. In the Model tree select the correct node for the imported devices.
   b. Check that:
      - (For a new device) The imported device is now in the list in the Table pane
      - (For an existing device) The device modification time is the time of this import, not that of a previous import
   c. Check that the network interfaces were imported correctly:
      - Right-click the device in the tree or Table pane and select Firewall Map.
All the network interfaces and the networks to which they are connected are displayed.

Close the map when you are finished.

d. If the device has routing rules:
   i. Right-click the device and select **Routing Rules**. Check that the routing rules were imported.
   ii. Use a sample routing rule to confirm that it was imported correctly—select a routing rule 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, individual rules might not be modeled in the same way that they are modeled in the device.

e. If the device has access rules:
   i. Right-click the device and select **Access Rules**. Confirm that the access rules were imported.
   ii. Select an access rule on the device and try to find its logical match in the access rules in Skybox.

f. On the toolbar, click **Network Map**. Make sure that the imported device is included in the map and that it is correctly connected.

6. (Recommended—especially for large networks) **Create locations** (see page 22). **Locations** group networks and simplify how Skybox displays the model.

**Locations**

A large organization can include hundreds of networks. **Locations** are container entities that create a hierarchic structure for networks in your organization, to make it easier to navigate and view the network structure.
A location can include networks and other locations. For example, a **Europe** location might contain specific networks and **London** and **Paris** locations. These locations, in turn, might each include networks and other locations.

```plaintext
Locations & Networks
  Europe
    London
      gatewaysNorthA [192.170.1.64 / 28]
      gatewaysNorthB [192.170.1.80 / 28]
      financeWindowsWS [192.170.25.0 / 24]
      financeUnixWS [192.170.26.0 / 24]
      financeServers [192.170.27.0 / 24]
  Paris
    gatewaySouthA [192.170.1.0 / 28]
    gatewaySouthB [192.170.1.16 / 28]
    developmentWindowsWS [192.170.17.0 / 24]
    developmentUnixWS [192.170.18.0 / 24]
    developmentServers [192.170.19.0 / 24]
```

Define locations manually in the Model workspace and then add networks or additional locations to them.

---

**Note:** You can create locations using Skybox Integration XML (iXML). For information about iXML, see the Integration part of the Skybox Developer Guide.

If you are working with a large network, define a location for each physical location that you discover and add to it the networks discovered in that network segment. A location can be a very broad grouping (for example, **Europe**) or a much more local grouping (for example, **IT Room** or **2nd Floor**).

For a gateway device to be contained in a location, all its networks must be in that location. If even 1 network belongs to another location (or is not associated with any location), the gateway device appears on the map even when all locations are collapsed. We recommend that you include gateway devices that are internal to a location as part of the location; do not include gateway devices that connect multiple locations in a location.

**To add a location**

1. In the tree, expand the **Locations & Networks** node and locate the desired parent node for the new location.

   If the new location belongs at the top level, select the **Locations & Networks** node as the parent node.
2 Right-click the parent node and select **New > Location**.

3 Type a **Location Name** for the new location. Location names must be unique throughout the model. The characters “/” and “\” cannot be used as part of a location name.

4 (Optional) Click the **Browse** button next to the **Members** field to specify the location’s members. Note: If you define the location before you discover the topology, you cannot select members for the location.

5 (For a specific Skybox user to receive notifications about entities in this location) Click the **Browse** button next to the **Owner** field to specify the location owner from all authorized Skybox users.
To add an existing network or location to a location

1. In the tree, right-click the network or location to add to an existing location and select **Move to Location** or **Attach to Location**.

![Move locations to location](image)

2. As required:
   - Select the parent location for the selected entity and click **OK**.
   - To make this entity part of a new location:
     a. Select the position in the tree for the new (parent) Business Unit.
     b. In the **New** field (which contains a list of parent types), click **Location**.
     c. In the New Location dialog box, type a name and other relevant information.

     The entity that you are attaching becomes a child of the new parent location; you can add other locations and networks using the **Members** field.

     Note: Repeat steps b and c to create a hierarchy of locations. The entity that you attach becomes a child of the most recently selected location in the tree.

     For example, you have a network named Operations Center and it belongs in Miami, but there is no location named Miami. The 1st time that you click **New**, create a location named US. Inside the new US location, create a location named Florida and inside the new Florida location, a location named Miami. The Operations Center network becomes a member of the Miami location.

     d. Click **OK**.

     The new location is created in the selected position in the tree and the selected entity becomes a child node, as do any members selected in step c.
Clouds

Clouds model areas missing in the model so that you can analyze access between the surrounding areas or to and from the missing areas.

Clouds are special network objects that represent networks that are connected to the model but are not modeled completely (for example, the internet, partners, or parts of your organization’s network that are not modeled). Any network over which your organization has no control or for which it cannot retrieve device configurations and scan data should be modeled as a cloud.

There are 2 types of clouds:

- **Perimeter Clouds**: Perimeter Clouds (often referred to as clouds) represent networks or areas in your network that are at the perimeter of the network (for example, partner networks and the internet).
  
  Multiple network interfaces can be connected to the same Perimeter Cloud, but Perimeter Clouds don’t include routing abilities—2 devices connected to the same Perimeter Cloud are connected in the Network Map but access queries (using Access Analyzer) are blocked. Access queries that include a Perimeter Cloud always end in the cloud.

- **Connecting Clouds**: Connecting Clouds represent missing areas in the middle of your organization’s network. These might be parts of your network for which you cannot retrieve data or MPLS networks between parts of your organization’s network.
  
  Unlike Perimeter Clouds, Connecting Clouds have routing abilities. Multiple network interfaces can be connected to the same cloud—they are connected in the Network Map (via the Connecting Cloud), and access queries work between the devices connected to the Connecting Cloud.

**Perimeter Clouds** (on page 26) are usually user-defined but can be created automatically as part of model validation.

**Connecting Clouds** (on page 28) are always user-defined.

For information about cloud properties, see the Clouds section in the Skybox Reference Guide.

**Creating and editing Perimeter Clouds**

You can create Perimeter Clouds manually or automatically.

**Creating Perimeter Clouds manually**

The easiest way to create a Perimeter Cloud is to define an existing network as a Perimeter Cloud. However, this is not sufficient when the Perimeter Cloud represents an area outside the boundaries of your organization’s network.

If you create a Perimeter Cloud that is not based on an existing network, include and exclude IP addresses for the network that you are configuring. For example:

- If you are configuring an internet cloud, exclude the IANA reserved addresses (click **Private** in the Network Properties dialog box).
- If you are configuring a public network, exclude public IP addresses used by your organization. Failure to do so might produce erroneous results in access analysis queries due to spoofed access.
If you know the specific IP addresses for the Perimeter Cloud, configure them in the **Cloud Addresses** tab.

**To define a network as a Perimeter Cloud**

1. In the Model tree, expand the **Locations & Networks** node and locate the network that you wish to define as a cloud.
2. Right-click the network and select **Define Network as Cloud**.
   
   Note: If the cloud is connected to multiple networks, set the **IP Address** and **Mask** fields to **0.0.0.0 / 0.0.0.0**.

**To create a Perimeter Cloud**

1. In the Model tree, expand the **Locations & Networks** node and locate the parent node for the cloud.
   
   If the cloud belongs at the top level, the parent node is the **Locations & Networks** node.
2. Right-click the parent node and select **New > Perimeter Cloud**.
   
   • For information about the properties of Perimeter Clouds, see the Perimeter Clouds topic in the Skybox Reference Guide.
3. In the New Perimeter Cloud dialog box:
   
   a. Type a **Name** for the cloud.
   b. Set the **IP Address** and **Mask** fields to **0.0.0.0 / 0.0.0.0**.
      
      This enables the cloud to be connected to network interfaces of multiple devices. (A cloud’s IP address has no influence on access analysis; use the Cloud Addresses tab to define the scope of the cloud.)
   c. Specify the scope of the cloud using the 2 panes in the **Cloud Addresses** tab:
      
      – Include: A list of IP address ranges to include in the scope of the cloud.
      
      – Exclude: A list of IP addresses to be excluded from the scope of the cloud specified in the Include pane.
   d. In the **Routable from Cloud** tab, define the IP address ranges that are permitted as destination addresses when access is checked from this cloud. Skybox uses these address ranges for all queries starting at the cloud in attack simulation and in Access Analyzer.
      
      – Include: A list of IP address ranges to use as destination addresses from this cloud.
      
      – Exclude: A list of IP address ranges to be excluded from the destination address ranges.
   e. Click **OK**.

**Creating Perimeter Clouds automatically**

We recommend that you create Perimeter Clouds automatically (on page 43) only after the model is as complete as possible, as part of model validation.
Attaching Perimeter Clouds to the network

After you create a Perimeter Cloud manually, you must attach it to the network devices in your organization that border the cloud.

To attach a Perimeter Cloud to a device

1. Open the Network Interfaces dialog box:
   - In the Network Map, right-click the device and select **Network Interfaces**.
   - In the tree:
     a. Navigate to a node that contains the device (for example, **All Network Devices > Firewalls**).
     b. In the Table pane, right-click the device and select **Network Interfaces**.

2. Select the network interface to be attached to the Perimeter Cloud network and click **Modify**.

3. In the `<network interface name>` Properties dialog box, in the **Network** field, select the desired Perimeter Cloud.

4. Click **OK**.

Connecting Clouds

Connecting Clouds represent missing networks (or groups of networks) between 2 entities in the model (for example, sensitive areas in your organization that cannot be fully modeled). When these networks are added to the model, Access Analyzer can analyze access through them.

Where are Connecting Clouds required?

Connecting Clouds are often required when you are creating the model and parts of your organization’s network are not included. Sometimes, you know that specific areas are missing; sometimes, you can use the Network Map to display all gateways that have missing next hops (that is, next routing hops that are mentioned in the routing table but are not connected to the gateway in the model) and decide which of them must be connected.

Viewing gateways with missing next hops

To view gateways with missing next hops

1. Make sure that a **Model Completion and Validation** task has run since the latest imports were done.

   Among other things, this task checks all gateways for missing next hops.
2 Open the Network Map. If necessary, open the map that displays the part of the model on which you want to focus.

3 In the Highlight pane, select **Has Missing Next Hops**.
   All gateways with missing next hops are highlighted. Mouse over a gateway to see a tooltip listing its missing next hops.

### Creating Connecting Clouds

The easiest way to create a Connecting Cloud is to select multiple gateways and networks in the map that should be connected and create a Connecting Cloud from them. Or you can select 2 gateways, networks, or network interfaces in the Table pane and create the Connecting Cloud from there.

**To create a Connecting Cloud**

1. Select the gateways or networks in the map that are missing connections between them.
2. Right-click and select **Connect via Cloud**.
   - For information about the properties of Connecting Clouds, see the Connecting Clouds topic in the Skybox Reference Guide.
3. In the Connect Networks via Cloud wizard, type a **Name** for the new cloud and click **Next**.
4. In the top pane, review the list of gateways and networks:
5. For each gateway (if any) with unspecified networks, select the network interface of the network to use to connect to the cloud.
   The following fields might be helpful in deciding the network interface to use:
   - The **Missing Neighbors** field shows the network interfaces that have missing neighbors.
   - The **Potential Match** field specifies whether the network interface is a good match for the new connection.
   When you select a network interface for the gateway, the network to which that network interface is connected appears next to the gateway in the top pane.
6. Click **Finish** to create the cloud from the specified networks.

**Adding additional connections**

You can add gateways and networks to an existing cloud.

**To add entities to a Connecting Cloud**

1. Select the desired gateways and networks; right-click and select **Connect via Cloud**.
2. In the Connect Networks via Cloud wizard:
   a. Select **Existing Connecting Cloud**, select the desired cloud, and click **Next**.
   b. In the top pane, review the list of gateways and networks.
   c. For each gateway with unspecified networks, select the network interface to use to connect to the cloud.
The following fields might be helpful in deciding the network interface to use:

- **Missing Neighbors** shows the network interfaces that have missing neighbors.
- **Potential Match** specifies whether the network interface is a good match for the new connection.

When you select a network interface for the gateway, the network to which that network interface is connected appears next to the gateway in the top pane.

d. Repeat steps a through c until every item in the list includes a network.
e. Click **Finish** to add the selected entities to the selected cloud.

**Network groups**

You can group networks by role in the model, so that you could have one network group that consists of all the DMZ networks, one that consists of all the internal networks, and one that consists of all the partner networks. Network groups improve performance and they can help Skybox users better understand the model.

*To create a network group*

1. In the Model workspace, right-click the **Network Groups** node and select **New Network Group**.
   - For information about the fields of a network group, see the Network groups topic in the Skybox Reference Guide.
2. In the New Network Group dialog box, fill in the fields and select a zone for the group.
3. Click **OK**.

You are asked whether to remove the zone marking from the group members (so that the network group is marked as a zone and not each member). We recommend that you click **OK**.

Note: Network groups are not part of the model hierarchy.

Note: You can include a network in more than 1 network group.

**Validating the model**

Model Validation is a process to verify that the model is:

- **Complete**: There are no missing elements in the model.
- **Correct**: The model reflects the actual network (for example, the topology was correctly interpreted; external clouds are connected to the correct interfaces).

Inconsistencies can occur because data is collected using different methods. For example, routing rules on a gateway might point to a router that does not exist in the model, indicating that data collection was incomplete; you must add the missing device to the model.
If the model is not accurate, performance, accuracy, and usability suffer. An invalid model causes accuracy issues:

› Access Analyzer
› Access Policy Analysis
› Network Map
› Access Compliance
› Path Analysis (in Change Manager)
› Attack Simulation (in Vulnerability Control)

OVERVIEW OF VALIDATING THE MODEL

Validate the model:

› After every milestone (for example, after adding a segment of your network to the model), to ensure that the model represents the actual access in your organization’s network.
› After collecting data and building the model, before you move on to the analysis stage.

If possible, we recommend that you validate your model with assistance from a Skybox Professional Services engineer. Your organization’s networking team should also be involved.

Common problems that should be solved during the model validation process include:

› Missing devices
› Missing routes
› Inaccessible environments (for example, MPLS networks or the internet)
› Network device misconfiguration
› Modeling inaccuracies
› Disconnected gateways

Model validation is not a 1-time job—it is a continuous process to make sure that every change in the network is reflected and validated. For example, adding a new device in the real network may cause new issues in the model.

Basic validation methods

The following 5 methodologies (listed from most important to least important) can be used in model validation:

1 Model validation task and analyses (on page 33)

The built-in model validation analyses list entities that might need to be fixed. The most important analyses to check at this stage are those that list gateway issues and network interfaces with problems.

• Gateways Validation
• Network Interfaces Validation
2 **Access Analyzer test queries** (on page 40)

Check the access to the organization’s network from different external locations. If there is insufficient access, gateways might be missing in the model. If there is too much access, sets of access rules might be missing.

3 **Network Map visualization** (on page 41)

After you have built the basic topology of the network, use the Network Map to make sure that the whole network is connected. Unconnected nodes or network segments are a sign of missing information.

4 **Task error messages** (on page 42)

Error messages from online collection tasks and offline file import tasks might mean that something went wrong.

5 **Item counts** (on page 43)

Check that the number of assets added to the model is what you expected, and that the element names and types look right.

These methods are explained in more detail in the following sections.

**BEST PRACTICES FOR MODEL VALIDATION**

**Recommended best practices in the model validation process**

1 **Inventory comparison**: Compare the model’s assets and networks with information from other systems, including asset management systems, configuration management systems, and IP Address Management (IPAM) systems.

2 Use **networking resources**: People that know the network well and can identify issues quickly.

3 Concentrate on **completing the model** before checking the model’s accuracy. Tests with Access Analyzer can work, but only after having all the network devices in the model. An incomplete model leads to inaccuracy.

4 **Complete** the model as much as possible before you launch a **Model – Completion and Validation** task that includes actions that change the model (for example, converting perimeter networks to clouds).

5 Look at **missing neighbors** of network interfaces to find missing devices in the model before looking at other issues.

Identify the missing neighbors that are **out of your network**. This can be done by looking at their IP addresses and comparing them to the internal IP addresses or IP address ranges that your organization uses. An IP address that is out of the internal ranges might indicate 3rd-party connections, MPLS networks managed by external providers, or that the missing device is managed by an ISP (for internet connections).

Such missing neighbors can be identified and converted to Perimeter Clouds (internet or 3rd-party) or assigned to Connecting Clouds (MPLS). (You can use a **Model – Completion and Validation** task to create Connecting Clouds for MPLS networks automatically (see the Model completion and validation tasks in the Reference Guide).)
6 Use **naming conventions**: Skybox uses specific naming conventions for clouds. When Skybox identifies a cloud or a network, we recommend that you change its name to match the naming conventions of your organization. This enables you to distinguish clouds in the model that were recently created by Skybox (which require review and validation) from those created previously that are already validated.

7 Use **Mark as viewed** to ignore acknowledged model validation issues.

8 Create **analyses**: Create new model analyses to split the information and get a better understanding of what is happening. For example, you could filter the list of duplicate network interfaces (or any other specific model validation issue) by creating an analysis of duplicate network interfaces that were not marked as viewed.

9 Use the Skybox model to gain **knowledge of the network/device**. Use the routing table or addresses behind interfaces, to identify networks that are behind a specific interface and to understand the context of the device. For example, an interface with ABI that includes many IP addresses but does not include any internal IP addresses is configured to be the default gateway interface. This might mean that the interface is connected to the internet.

10 Most organizations have **defined processes** to decommission network devices or to install new devices in their network. Make sure that, as part of this process, the team responsible for maintaining Skybox is aware of network changes and applies them to the Skybox model (for example, delete decommissioned devices and associated tasks; add a task to collect newly installed devices).

11 After finishing the model validation during deployment, we strongly recommend that you **review and remediate new issues** at least once a week. There are analyses for new assets and interfaces in the model that should be reviewed.

**MODEL VALIDATION TASKS AND ANALYSES**

The built-in model validation analyses list entities that might need to be fixed. The most important analyses to check at this stage are those that list gateway issues and network interfaces with problems.

The Model Validation task creates model validation issues on 2 levels:

- Gateways
- Network interfaces

Model validation issues that are created by the Model Validation task, are listed under **Model Analyses > Model Validation**.

**Validating gateways**

The following sections explain how to validate gateways in the model.

**Disconnected gateways**

**Diagnosis**

Standalone devices that are not connected to any other devices in the model appear as ‘islands’ in the Network Map.
If no network interfaces of a device are connected to any other network device, it is a disconnected gateway.

Unless the gateway has no routing rules (which can be identified using the Gateways with no Routing Rules analysis), at least one network interface of a disconnected gateway has a missing neighbor.

In most cases, disconnected gateways are addressed when fixing other issues (using the Network Interfaces Validation analyses).

**Possible root causes and their solutions**

<table>
<thead>
<tr>
<th>Root Cause</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Missing device in the model (next hop)</td>
<td>Collect or import the missing neighbor.</td>
</tr>
<tr>
<td>Device not mapped to Connecting Cloud</td>
<td>Map the relevant network interface to a Connecting Cloud.</td>
</tr>
<tr>
<td>Decommissioned device</td>
<td>Delete the gateway from the model. Add the gateway to the collection task exclude list.</td>
</tr>
</tbody>
</table>
| Overlapping networks                    | • Fix the device configuration by configuring the network interface subnet mask and re-collecting or re-importing the device to Skybox  
                                        | • Assign the network interface in Skybox to the correct network (affects the Skybox model only) |

**Firewalls with no access rules**

**Diagnosis**

There are Firewall assets in the Skybox model that have no access rules—the list of access rules is empty. A normal firewall in a production network should have at least 1 rule (explicit Deny rule).

**Possible root causes and their solutions**

<table>
<thead>
<tr>
<th>Root Cause</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Import or collection issue</td>
<td>Check the import or collection task messages for errors. Make sure that the access rules are in the configuration in Skybox.</td>
</tr>
<tr>
<td>Firewall has no access rules</td>
<td>Check with the firewall administrator if this is correct. Can be ignored if acknowledged by the firewall administrator.</td>
</tr>
</tbody>
</table>

**Gateways with no routing rules**

**Diagnosis**

There are network devices in the Skybox model with no routing rules—the list of routing rules is empty. Normal network devices in production with routing abilities should have at least 1 rule. Gateways with no routing rules cause speculation (possible inaccurate results and poor performance) in access analysis and inaccurate Access Compliance results.
### Possible root causes and their solutions

<table>
<thead>
<tr>
<th>Root Cause</th>
<th>Solution</th>
</tr>
</thead>
</table>
| **Collection issue**  
The device was collected by a Skybox Collector using an online collection task | • Check the collection task messages for errors.  
• Check the configuration in Skybox and make sure that the routing rules file is there.  
• Check the Routing Table Collection command in the task’s **Advanced** tab.  
• Check that you have authorization to run the command with the task’s credentials.  
After fixing, re-collect the device. |
| **Import issue**  
The device was imported into Skybox from raw configuration files | • Check the collection task messages for errors.  
• Check the configuration in Skybox and make sure that the routing rules file is there.  
• Make sure that routing information is in the same file as the configuration data or that both files are in a separate 1st-level subdirectory of the specified directory.  
• Make sure that the routing file includes routing rules.  
After fixing, re-import the device configuration and routing data. |

### Validating network interfaces

The following sections explain how to validate network interfaces on assets in the model.

#### Disconnected interfaces

**Diagnosis**

There are device interfaces that are not connected to any network. This can cause missing connectivity, incorrect visualization, and incorrect access results.

**Possible root causes and their solutions**

<table>
<thead>
<tr>
<th>Root Cause</th>
<th>Solution</th>
</tr>
</thead>
</table>
| Interfaces for sync between clusters | • (Normal behavior) Acknowledge (“Mark as Viewed”)  
• Create a new network  
• Assign interfaces to the correct network |
| Interface with netmask /32 (255.255.255.255) | • (Normal behavior) Acknowledge (“Mark as Viewed”)  
• Create a new network  
• Assign interfaces to the correct network |
| Merging issue when there are 2 networks that are both candidates for the network interface (misconfiguration of netmask in devices) | Investigate the root cause and act accordingly. Try to look at the modeled networks to find the networks that match the interface (assign them to locations if overlapping). |
Next hop and destination networks not in model

**Diagnosis**

“Next hop and destination networks not in model” issues highlight gateways that are missing in the Skybox model.

Examine the routing rules for each device. A typical entry includes:

- Destination network: “Where am I trying to get to?”
- Gateway: “How do I get there?” (that is, Next Hop – IP Address)

The Model Validation task examines each entry to find the gateway (an IP address), and to check whether the gateway exists in the Skybox model. The task also looks for the destination network, to check whether the destination network exists in the Skybox model. If an entry has a gateway that is not in the Skybox model, and the destination network is not in the Skybox model either, the Model Validation task adds an interface issue of “Next hop and destination networks not in model”.

If you know that the destination network is not in the model, it means that no other network device in the model holds that network. If the network should not exist in Skybox (use an IP address management tool to look for those networks and confirm that they are not part of your organization’s networks), the most likely remediation is to convert the network to a Perimeter Cloud.

**Possible root causes and their solutions**

<table>
<thead>
<tr>
<th>Root Cause</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Missing device (the gateway should be in the Skybox model)</td>
<td>Import or collect the missing next hop device</td>
</tr>
<tr>
<td>Out of scope device</td>
<td>- Convert the network to a Perimeter Cloud</td>
</tr>
<tr>
<td></td>
<td>- Assign the network interface to the relevant Connecting Cloud</td>
</tr>
<tr>
<td>Old routing rule (no longer in use)</td>
<td>- Fix the routing issue (device configuration)</td>
</tr>
<tr>
<td></td>
<td>- Acknowledge the issue in Skybox (“Mark as Viewed”)</td>
</tr>
</tbody>
</table>
Next hop exists in a separate network

**Diagnosis**

The routing rules for each device are examined. The networks and gateway exist in the model. However, the gateway is connected to another network.

<table>
<thead>
<tr>
<th>Network</th>
<th>Interface Name</th>
<th>IP Address</th>
<th>Network</th>
<th>Missing Neighbor</th>
</tr>
</thead>
<tbody>
<tr>
<td>124F</td>
<td>CIS</td>
<td>10.200.100.73</td>
<td>10.200.100.72/29</td>
<td>10.200.100.74</td>
</tr>
<tr>
<td>382RR</td>
<td>Data12</td>
<td>10.200.100.73</td>
<td>10.200.100.72/29</td>
<td>10.200.100.74</td>
</tr>
</tbody>
</table>

**Possible root causes and their solutions**

**Root Cause**

Network devices can be misconfigured (different netmask assignments) but work in real life

**Solution**

Fix the network device configuration (assign the same netmask for interfaces).

Determine the network that contains the gateway and then open the interface properties and assign the correct network (this is applicable for Skybox only and has no impact on the network device).

---

**Potential matching network for interface assigned to cloud**

**Diagnosis**

An interface is connected to a cloud but has a missing next hop that appears in another network of the model.

**Possible root causes and their solutions**

<table>
<thead>
<tr>
<th>Root Cause</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Model Validation task created the cloud before importing the missing next hop</td>
<td>Assign the interface to the regular network instead of the cloud.</td>
</tr>
<tr>
<td>The interface is locked to the cloud</td>
<td>Unlock the interface from the cloud. Assign the interface to the regular network.</td>
</tr>
</tbody>
</table>
VPN or tunnel end point is missing

**Diagnosis**

In a VPN or tunnel interface with peer-to-peer configuration, one peer exists in the Skybox model as part of the asset or interface that has the issue, but the other peer doesn’t exist in the Skybox model.

Treat this issue as a “Missing next hop” issue. A missing peer points to a missing interface on a device that is missing in the model.

**Possible root causes and their solutions**

<table>
<thead>
<tr>
<th>Root Cause</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Missing device</td>
<td>Import or collect the missing device</td>
</tr>
<tr>
<td>The missing peer is part of an in-scope network device that does not exist in the Skybox model</td>
<td></td>
</tr>
<tr>
<td>Out of scope device</td>
<td>Convert the device to a Perimeter Cloud</td>
</tr>
<tr>
<td>The missing peer is part of a network device that does not exist in the Skybox model and the device is out of scope</td>
<td></td>
</tr>
</tbody>
</table>
**Root Cause** | **Solution**
---|---
Old VPN or tunnel configuration | Fix the device configuration
The VPN or tunnel is configured on the device, but the other peer doesn’t exist as it was decommissioned | Delete the network assignment from the network interface and lock it
| Acknowledge (“Mark as Viewed”)

**Duplicated network device**

**Diagnosis**
There is an interface that is part of a duplicate network device. The Model Validation task checks duplication of devices based on name and network interfaces. If multiple devices have the same name and the same interface configurations, interfaces that are part of the duplicate devices have this issue.

**Possible root causes and their solutions**

| **Root Cause** | **Solution** |
---|---
Merging issue | Consult with Skybox Support. You must identify differences between the devices. Merge manually (see page 147).
Skybox didn’t merge the devices |

**Duplicate IP address in network**

**Diagnosis**
There are multiple interfaces with the same IP addresses in the same network entity. In normal network behavior, there should be no duplicate IP addresses in the same network (except for virtual addresses and interfaces). An organization can have overlapping IP addresses, but these should be configured in the Skybox model as different networks, each in a different location.

**Possible root causes and their solutions**

| **Root Cause** | **Solution** |
---|---
An old network device | Delete the asset from the model. Exclude the asset from the task, using the collection task exclude list.
An old interface entry in Skybox |
A merging issue in assets with the same interface that creates the same interface multiple times in the same network | Consult with Skybox PS / Support. You must identify differences between the devices. Merge manually (see page 147).
Overlapping networks | Create locations and move the overlapping networks to different locations. Assign each network interface to a different network entity (in a different location). Overlapping networks exist in the real network, but their locations were not specified |
Overlapping networks

**Diagnosis**

There are multiple overlapping networks, meaning that 1 network is covered by another. This causes connectivity issues (2 devices that should be connected are not).

**Possible root causes and their solutions**

<table>
<thead>
<tr>
<th>Root Cause</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network devices can be misconfigured (different netmask assignments)</td>
<td>Determine the network that contains the gateway Fix the network device configuration (assigning the same netmask for interfaces) Open the interface properties and assign the correct network (applicable in Skybox only – has no impact on the network device)</td>
</tr>
</tbody>
</table>

**ACCESS ANALYZER TEST QUERIES**

Check the access to the organization’s network from different external locations. If there is insufficient access, gateways or network segments might be missing in the model. If there is too much access, sets of access rules might be missing.

Check access by creating ‘real world’ queries and results (5 to 10 samples) in Access Analyzer.

Test queries can include:

- A spectrum of test types
- Internet inbound
- User environment to internet
- User environment to user environment
- Customer and network specific
Start with simple queries and progress to more complex.

NETWORK MAP VISUALIZATION

Skybox creates a map of all the interconnections in your network named the Network Map. After you have built the basic topology of the network, use the Network Map to make sure that the whole network is connected. Unconnected nodes or network segments are a sign of missing information. Search for 'islands'—parts of the networks that are disconnected.
Network visualization (maps)

To open the Network Map from Skybox Manager, click on the toolbar. When you open the Network Map, it is redrawn according to the most recent information in your model. You can create and save maps of specific sections of your network.

Note: If this is the 1st time that you are opening the map, either open Organizational Map to load the map of your entire model or select a different map that someone else created.

For additional information, see Network Map (on page 44).

TASK ERROR MESSAGES

Error messages from tasks might mean that something went wrong.

Note: Successful import or collection of a device does not necessarily mean that Skybox retrieved all the required information. For example, if you import a device without its routing file, Skybox models the device, but the dynamic routing rules are missing.
ITEM COUNTS

Check that the number of assets added to the model is what you expected, and that the element names and types look right.

<table>
<thead>
<tr>
<th>Assets Analysis: Routers</th>
<th>Name</th>
<th>Primary IP Address</th>
<th>OS</th>
<th>Status</th>
<th>Has Access Rules</th>
<th>Modification Time</th>
<th>Routing Rules</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.200 43</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

CREATING PERIMETER CLOUDS AUTOMATICALLY

**Model – Completion and Validation** tasks can create Perimeter Clouds automatically; this completes the model with clouds, and fixes missing parts of the model. This feature is disabled in the **Model Validation** task; we recommend that you enable it only after you are sure that all devices are in the model, so as not to create unnecessary Perimeter Clouds.

The task converts perimeter networks to Perimeter Clouds in the following cases:

- A VPN or tunnel network, peer-to-peer, for which a peer is missing.
  
  In this case, Skybox changes the name to `%PEER1-IP%_%PEER2-IP%`.

- A regular network that is a perimeter network. A perimeter network is a network with missing next hops.
  
  In this case, Skybox changes the name to Accessible Via %LIST-OF-MISSING-NEXT-HOPS-FROM-THE-SAME-INTERFACE% or leaves the Perimeter Cloud name as the network name.

Running the **Model Validation** task with automatic creation of Perimeter Clouds fixes the following model validation issues:

- Next hop not in model
- Next hop and its destination network not in model
- VPN or tunnel end-point is missing

The Model Validation task cannot always complete the whole model. In some cases, Skybox cannot complete the model or create Perimeter Clouds automatically. For example:

- Skybox cannot create a Perimeter Cloud for a perimeter network that is configured on a device that is not in the model
- A device without routing information
  
  Missing next hop analysis is based on routing rules; if these don’t exist, Skybox cannot convert networks to clouds.

For additional information about these tasks, see the Model completion and validation tasks topic in the Skybox Reference Guide.
Chapter 3

Network Map

Use the Network Map to view the topology of the model.

In this chapter

Overview of the Network Map ................................................................. 44
Creating and saving dedicated maps ..................................................... 45
Navigating the Network Map ............................................................... 47
Map Groups ......................................................................................... 49

Overview of the Network Map

To display the Network Map of your organization’s model, click on the toolbar. Then, in the Map field, select Organizational Map.

You can create maps for specific locations (see page 45) so that you can focus on those locations. The Network Map is dynamic; when you open a saved map, it is redrawn based on the current model.
The Network Map is integrated with Access Analyzer; you can use it to display the path between a source and destination.

Creating and saving dedicated maps

By default, the organizational map displays the entire model. However, it is generally easier to work if you create dedicated maps for specific scopes. We recommend that you create a separate map for each network scope that you want to view in detail.
Creating a dedicated map

To create a map

1. In the File pane of the control panel, click New...

   ![New Network Map dialog box]

   - For information about the properties of Network Maps, see the Properties of single maps section in the Skybox Reference Guide.

2. Define the scope of the map.
3. Click OK.

Saving maps

To save a map

- To save the map (including any changes that you made): In the File pane of the control panel, click Save.
- To save the map (including changes) with a different name: In the File pane of the control panel, click Save As.

Viewing changes to the map

Changes to the model that occur while the Network Map window is open are not reflected in the map. If you know that changes were made, click at the top of the control panel. You are prompted to save all unsaved maps, the map definitions from the Server are refreshed, and the selected map is reloaded to the Map pane.
Navigating the Network Map

Navigate the Network Map using the control panel.

Map layout

Skybox lays out the nodes of the selected map. You can:

- Select and move nodes of the map to make the map easier for you to work with.
- Click `Relayout` to redraw the map using the same calculation formula. This is useful if you changed the display somewhat (for example, if you created map groups or hid nodes). The results might be easier for you to use.
  
  If you did not change the display, or if relayout does not make the map easier for you to use, tune the layout properties using the Layout pane to change the values used in the calculation formula. For additional information, see the Layout properties topic in the Skybox Reference Guide.

- Click `View`. Skybox redraws the map to fit the size of the window.
- Select anywhere inside the white space of the map and scroll to resize the map, or move the mouse to reposition the map in the window.

Highlighting parts of the map

Skybox can highlight specific nodes or sets of nodes in the map to help you to understand your organization’s network. Highlighting is temporary—when you change maps or save a map, all highlighting is turned off.
Highlighting neighbors: By default, when you select a node in the map, the node is highlighted; its immediate neighbors are highlighted in a lighter color than the selected node. This makes it easier to see the context of the selected node. You can change the number of neighbors highlighted by changing the value of the property.

Note: The value of this property is saved with the map.

Highlighting different types of nodes: Use the Highlight pane to specify the node types to highlight in the map (automatically, not by selection). For example, you can highlight all Perimeter Clouds, a specific location, or nodes that have missing next hops. Each type of node is highlighted in a different color; you can select multiple nodes type to highlight at the same time.

Filtering the map
You can filter the map to display only specific nodes. To display the filter pane, click in the control panel.

Note: Use Ctrl-F to display the filter pane, and Esc (in the Show field or in the white space of the Map pane) to close it.

Show: Select nodes in the map by typing in the (full or partial) name or IP address of the desired nodes. Only these nodes (and their neighbors) are displayed.

You can use the characters ? and * for standard pattern matching in the filter; you can also use the following regular expression syntaxes:

- \^X: Specifies an expression (X) that appears at the beginning of the name or IP address
- X$: Specifies an expression (X) that appears at the end of the name or IP address
- [xyz]: Specifies a single character that is either x, y, or z
- [^abc]: Specifies a single character that is anything except a, b, or c

Show Only Highlighted: Filters the map to display only highlighted nodes.

Regular Mouse Mode: When you select nodes in the map, the selected nodes and their neighbors are highlighted.

Focus: When you select nodes in the map, only those nodes and their neighbors (within a radius of Neighbors Distance) are displayed. All other nodes in the map are hidden.

Extend: When you select nodes in the map, the map expands (if parts of it are hidden) by adding all neighbors of the selected node up to a radius of Neighbors Distance.

Display All Nodes: Restores all hidden nodes to the map but keeps the magnification (so that some nodes might not be visible in the display).

Note: This button clears all highlighting.
Exporting maps

You can export maps as graphic files or Visio files.

- Export image: Saves the visible portion of the map as a graphic file to the directory specified in the Export dialog box.
  Note: You can change the resolution of the saved image in the Export dialog box for easier viewing outside of Skybox.

- Export to Visio: Exports the visible portion of the map as a Microsoft Visio VDX file so that non-Skybox users can view or print the map.

For additional information about the control panel and the filter pane, see the Network Map control panel topic in the Skybox Reference Guide.

Map Groups

A Map Group (#region) represents a region or area in the network. Map Groups can include gateways, networks, and other Map Groups. Normally, map group members are topologically related, so that a collapsed group makes sense.

Defining Map Groups reduces the complexity of the model in the Network Map and provides better orientation in large networks. Each Map Group can be highlighted in a different color, enabling you to easily see the entities that belong to each group. You can collapse a Map Group so that only a representative node is displayed in the map.

Map Groups are stored globally in the model; creating or changing a Map Group in 1 map affects all other maps that contain that Map Group.

Map Group scopes

Each Map Group has a set of defining members (usually the group’s gateways) and additional members. The additional members are the neighbor nodes of the defining member nodes.

The defining member nodes are specified by the user. The additional member nodes are completed by Skybox. This makes the Map Group definition more compact and eliminates the need to explicitly attach newly discovered networks to any Map Group; newly discovered networks are added to the Map Groups of their gateway neighbors.

CREATING MAP GROUPS

Before defining new Map Groups:

- Set the Highlight mode of Map Groups to All (in the Map Group pane, in the Highlight field, select All).
  This highlights each existing Map Group in a separate color and highlights new groups in different colors as they are created.

- Set the Highlight Neighbor distance (at the top of the control panel) to 0.
  This prevents highlighting neighbor nodes when selecting nodes for a Map Group.
To create a new Map Group

1. Select the set of nodes that define the scope of the Map Group.
   Nodes (gateways and networks, but not Perimeter Clouds) whose neighbors all appear in the scope of the Map Group are automatically added to the group as members—it is usually sufficient to select a set of gateway nodes as the defining members. You only need to select network nodes explicitly if they are to be part of the group but some neighbor gateways are not part of the group.

2. Right-click in the selection and select **New Map Group**.

3. In the Map Group dialog box:
   a. Type a **Name** for the group.
   b. (Optional) Change the highlight color of the group.
   c. (Optional) To display the group in collapsed form after it is created, select **Collapse**.
   d. Click **OK** to create the Map Group.

Note: Map Groups have labels; use the View pane of the control panel to toggle whether to display these labels.

MAP GROUP HIERARCHIES

To create a hierarchy of Map Groups, you can work top-down (for example, by creating a Paris Map Group when a Europe Map Group already exists) or bottom-up (for example, by creating a Europe Map Group when Paris and London Map Groups already exist).

To create a Map Group inside an existing Map Group
1. Select the nodes of the existing Map Group to include in the new Map Group.
2. Right-click in the selection and select **New Map Group**.

To create a new Map Group that contains existing Map Groups
1. Select the labels of the existing Map Groups (and any other gateway or network nodes to include in the new Map Group).
2. Right-click in the selection and select **New Map Group**.

To view the hierarchy of Map Groups
1. Right-click a node in the map and select **Attach to Map Group**.
2. In the Attach to Map Group dialog box, view the Map Group hierarchy; then click **Cancel** to close the dialog box (without attaching anything).

WORKING WITH MAP GROUPS

The following options in the Map Groups pane of the control panel are useful:

- **Highlight All**: Highlights each Map Group in a different color
- **Collapse All / Expand All**: Collapse or expand all Map Groups. Collapse replaces the members of a map group by a representative node.
The following options on the shortcut menu are useful when you edit a Map Group:

- **Collapse Map Group**: Right-click a member of the Map Group or the group label, and then select **Collapse Map Group**.
- **Expand Map Group**: To display all the members of a collapsed Map Group, right-click the node representing the Map Group and select **Expand Map Group**.

**To attach nodes to a Map Group**

1. Select a set of nodes or labels of Map Groups to be attached to another Map Group.
2. Right-click in the selection and select **Attach to Map Group**.
3. Specify the target Map Group in the dialog box. The selected nodes or Map Groups are detached from any previous Map Groups to which they were attached and are attached to the selected target Map Group.

**To detach nodes from a Map Group**

1. Select a set of nodes or labels of Map Groups to be detached from the Map Groups to which they are attached.
2. Right-click in the selection and select **Detach from Map Group**.

**To delete a Map Group**

1. Select a Map Group (by selecting either the Map Group’s collapsed node or its label).
2. Right-click the selection and select **Delete Map Group**.

Note: This command deletes the map group definition, but does not delete the member nodes of the map group nor any subgroups of the selected group.
Chapter 4

Configuration Compliance

This chapter explains how to use Skybox Network Assurance to check firewall configurations across all or part of your organization’s network.

Note: Configuration Compliance for networks is only available with a Network Assurance license.

In this chapter

Overview of Configuration Compliance ................................... 52
Viewing Configuration Compliance ........................................ 53
Viewing violations in the configuration file .............................. 54
Network Configuration Compliance reports ......................... 56
Customizing a Configuration Policy .................................... 57

Overview of Configuration Compliance

Configuration Compliance enables you to audit the platform security of your firewalls and understand weaknesses in a firewall 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 check the configuration data of your organization’s firewalls against a Configuration Policy (a set of Configuration Checks). After Skybox analyzes the information, you can view any failed Configuration Checks, with detailed information about each failure.

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

Configuration Policies

A Configuration Policy is a set of Configuration Checks; a Configuration Check is a regular expression. When firewall 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.

### Configuration Policies

- **Standard**
  A 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 firewall type.
  
  Note: There is no predefined Configuration Policy for Check Point Gaia.

- **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). The set 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: This set includes Configuration Checks for Cisco firewalls and Cisco IOS routers. You can control the set of Configuration Checks to be applied to your organization’s firewalls, see Customizing a Configuration Policy (on page 57).

Before working with Configuration Compliance:

1. (Recommended) Make sure that all the firewalls to be analyzed are up-to-date.
2. Run the Analyze Network Policy Compliance task.
   - For information about the properties of this task, see the Policy Compliance tasks topic in the Skybox Reference Guide.

### Viewing Configuration Compliance

For each Configuration Check, you can view all the analyzed firewalls, and drill down to view violation details.
To view Configuration Compliance

1. Select the Configuration Policy that matches the firewalls that interest you. The Table pane lists the Configuration Checks in the policy; you can see the checks that are violated.

2. Double-click the desired Configuration Check. The Configuration Check Details page shows information about the check.

3. Click the **Analyzed Devices** tab to view the list of firewalls analyzed for this check.

4. Select a firewall to view its violation details.

5. (Optional) View each violation in its configuration file (as explained in the following section) 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. The Viewer also displays the configuration file in which the violation is found. If possible, the 1st violation instance in the file is highlighted in the file.

2. As required:
   - 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 find 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.
Network Configuration Compliance reports

Skybox includes Network Configuration Compliance reports that provide policy-related information about the compliance of your organization’s network. These reports help you to understand the compliance status of your network to your Configuration Policy and to identify problematic device configuration in your network.

To generate a Network Configuration Compliance report

Note: Folders and Configuration Policies that were not analyzed are not included in these reports, even if they are in the defined scope.

1. Open the Reports workspace.
2. In the Tree pane, click Reports.
4. For the Report Type, select Network Configuration Compliance.
5. Fill in the fields and select the information to include in the report.
   For additional information, see the Network Configuration Compliance reports topic in the Skybox Reference Guide.
6. Click Generate.
   You are asked whether to generate the report in the background or in the foreground. It can take time to generate large reports, so it is often useful to generate in the background and keep working.
7. Select the desired 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 compliance data is generated from the report definition. When generation finishes, the report is displayed in the workspace.

Note: If you generate reports in the background, they are not visible in the workspace until you click $\rightarrow$.

You can:

- Change the format of a report (to HTML or RTF)
- Change the scope of a report to include only specific parts of the Configuration Policy or only specific parts of the network
- Create definitions for additional Network Configuration Compliance reports
- Schedule reports to run at specific times and be sent to specified Skybox users

For additional information, see the Working with reports section in the Skybox Reference Guide.
Customizing a Configuration Policy

Configuration Policies are displayed under the **Configuration Policies** node in the Network Assurance tree.

You can:

- 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**.

**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>General</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>
</tbody>
</table>
### Property Description

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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>Networks and Locations</td>
<td>The assets and container entities from which firewalls are checked by this Configuration Policy.</td>
</tr>
<tr>
<td>Exclude from Scope</td>
<td>Assets and container entities that match the policy scope, whose firewalls 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 scope.

### CREATING CONFIGURATION CHECKS

A Configuration Check is a specific test (often in the form of a regular expression) that is run on a firewall 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 this case, 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.

### Editing Configuration Checks

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

To 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 into Skybox.
### Configuration Check properties

The properties of Configuration Checks in Skybox Network 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 Skybox Professional Services has created external scripts for more sophisticated testing.</td>
</tr>
<tr>
<td>Severity</td>
<td>The severity of the Configuration Check.</td>
</tr>
<tr>
<td>Enable</td>
<td>Specifies whether Skybox uses the Configuration Check in policy analysis.</td>
</tr>
<tr>
<td><strong>Search</strong></td>
<td></td>
</tr>
<tr>
<td>Search Scope</td>
<td>• <strong>Entire Configuration</strong>: The entire configuration file is checked for the search string.</td>
</tr>
<tr>
<td></td>
<td>• <strong>For Each</strong>: Each block of the configuration file is checked for the search string. If you select this option, click <img src="image" alt="block" /> 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 information about defining blocks, see Defining blocks for Configuration Checks (on page 61).</td>
</tr>
<tr>
<td>Search for</td>
<td>The regular expression (see page 62) to use as the search pattern.</td>
</tr>
<tr>
<td>Ignore order</td>
<td>(For multi-line search patterns) Specifies whether the order of the lines matters. In some cases, the search pattern must be matched exactly; in other cases, provided that each line is found, the order is irrelevant.</td>
</tr>
<tr>
<td></td>
<td>• Clear this option to check the search pattern against the configuration in the order in which it was entered.</td>
</tr>
<tr>
<td></td>
<td>• Select this option to check each line of the search pattern against the configuration, regardless of its order in the search pattern.</td>
</tr>
<tr>
<td><strong>Advanced</strong></td>
<td></td>
</tr>
<tr>
<td>In regular expressions, some characters are intended as special constructs. To control the display of the search string in the <strong>Search for</strong> field, click <img src="image" alt="special_chars" />.</td>
<td></td>
</tr>
<tr>
<td>Escape Special Characters</td>
<td>Sets all special characters (&quot;[&quot;, &quot;,&quot;, &quot;^&quot;, &quot;,$&quot;, &quot;:&quot;, &quot;,&quot;, &quot;<em>&quot;, &quot;</em>&quot;, &quot;,&quot;, &quot;,&quot;, &quot;,&quot;, &quot;,&quot;, &quot;<em>&quot;, &quot;</em>&quot;, &quot;,&quot;, &quot;<em>&quot;, /</em>&quot;, /<em>&quot;, &quot;</em>/&quot;, and &quot;,&quot;) in the selected part of the search pattern to literal by adding a &quot;&quot; before each of them.</td>
</tr>
<tr>
<td>Reset Special Characters</td>
<td>Resets all escaped special characters (&quot;[&quot;, &quot;,&quot;, &quot;^&quot;, &quot;,$&quot;, &quot;,&quot;, &quot;<em>&quot;, /</em>&quot;, /<em>&quot;, &quot;,&quot;, /</em>&quot;, /*&quot;, and &quot;,&quot;) in the selected part of the search pattern, by deleting the &quot;&quot; before each of them.</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>View</td>
<td>Specifies the display mode for the <strong>Search</strong> field:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Full mode (editable)</strong>: View the regular expression as is, including the &quot;&quot; preceding special characters that are escaped. Use this view to edit the search pattern.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Readable mode</strong>: (Read-only) View the regular expression as it appears in the configuration file, without the preceding &quot;&quot; in front of special characters that are escaped.</td>
</tr>
<tr>
<td>Violation When</td>
<td>Specifies whether to create a violation of the Configuration Check when the search pattern is found or when it is not found.</td>
</tr>
<tr>
<td>Violate if the block isn’t found</td>
<td>Specifies whether to create a violation of the Configuration Check if the specified block is not found in the configuration.</td>
</tr>
<tr>
<td>Test</td>
<td>Opens an additional section of the dialog box where you can test the regular expression. For additional information, see <strong>Testing a Configuration Check</strong> (on page 63).</td>
</tr>
<tr>
<td>Limit Check to Version</td>
<td>Specifies whether the Configuration Check runs only on specific versions of the device. Write the version numbers as a regular expression. For information about regular expressions, see <strong>Regular expressions</strong> (see page 62).</td>
</tr>
<tr>
<td></td>
<td>Note: The device type is specified in the Configuration Policy.</td>
</tr>
</tbody>
</table>
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 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 ID that follows the common prefix; each set of lines with a different entity ID 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 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.
- 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 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 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 Open the expanded Check: <Configuration Check name> Properties dialog box:
  • Right-click the Configuration Check in the tree and select Configuration Check Test.
  • In the Check: <Configuration Check name> Properties dialog box, click 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.
To test the regular expression against text: Type or paste the desired text in the text box below the **Find** field.

4 Click **Test**.

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. If 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, 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 specific device types. If this pattern exists in the configuration file, it is a violation—HTTP is 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 and 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. 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 Manager

- 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 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 of the output file.

3 (Optional) To save the policies 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**.

Note: The default export format is XMLX (encrypted XML). However, if you must make changes to a specific policy outside of Skybox, you can save the file in XML format. To do this, change the value of `db_xml_backup_mode` to `true` in `<Skybox_Home>/server/conf/sb_server.properties`. Then, for the export, change the format of the output file to XML. (After the export, remember to change the value of `db_xml_backup_mode` to `false`.)

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 to import.

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

3 Click **OK**.
Chapter 5

Access Analyzer

This chapter describes how to use Access Analyzer to provide information about access in the model.

In this chapter

- Access Analyzer overview .................................................... 66
- Creating new queries .......................................................... 67
- Defining the source and the destination ................................. 67
- Understanding the results .................................................... 72
- Inaccessible entities ............................................................ 75
- Saving an access query as an Access Check ........................... 77
- Saving the results .................................................................. 78

Access Analyzer overview

Access Analyzer is a powerful simulation tool that analyzes access in the network, taking into account access rules, routing rules, and network topology. It works by answering specific queries about access in your organization’s network (for example, “Is network X available from network Y over HTTP?”).

You can use Access Analyzer for many purposes, including verifying network connectivity and network security in existing scenarios (Live model) and test scenarios (What If model), and for troubleshooting the network.

**Note:** Access Analyzer also supports checking connectivity through a single firewall (in Firewall mode).

The main use cases for Access Analyzer are:

- Which networks and ports in your organization are accessible from a specific source?
- Is there access between 2 networks?
- Is there access between 2 virtual assets, or a virtual asset and a physical network?
- Why is there no access between 2 entities (networks and virtual assets)?

When you examine why there is no access, you can check the inaccessible entities in Access Analyzer to discover which access rules in which firewalls are blocking the access. This is useful for troubleshooting (to help you to understand why there is no connection), and for planning new connections.

Use Access Analyzer by defining a query and then analyzing the results.
Creating new queries

In the context of Access Analyzer, a query is a question about access in your organization’s network that is phrased so that Skybox can provide an answer. For example, “Which networks and ports in the organization's network are accessible from the internet?”

Use the Access Query pane to create queries. The pane contains input fields (including source, destination, and specific access properties (for example, IP address spoofing)) that tell Access Analyzer the access that you want it to verify and the additional factors to consider in the analysis.

To define a query

1. Click Access on the toolbar.
2. Verify that Network Mode (rather than Firewall Mode) is selected on the Access Analyzer toolbar.
3. Define the source and the destination (on page 67).

   Note: Source and Destination cannot both be Any.

   • For information about these and other query fields, see the Access Analyzer query fields topic in the Skybox Reference Guide.

4. (For advanced users) To configure additional settings, click Advanced.

After providing values for the query fields, click Analyze. Access Analyzer analyzes access between the source and the destination. The results of the analysis are displayed in the results tree.

If you change the values of any query fields after the query is analyzed, reanalyze the query.

Note: You can save queries created in Access Analyzer as part of the Access Policy and reuse them from there (see Saving an access query as an Access Check (on page 77)).

Defining the source and the destination

The source and destination of access queries are defined by their scope and the services on which access is verified. The destination can have other defining information (see page 71).

DEFINING THE SCOPE FOR NETWORK QUERIES

The scope of the source specifies the source points for access analysis; the scope of the destination specifies the destination points for access analysis. Access analysis can be done:

- From physical networks to physical networks
- From virtual domains, security tags, or virtual assets to virtual domains, security tags, or virtual assets
From physical networks to virtual domains, security tags or virtual assets, and vice versa

Note: Physical and virtual entities cannot be mixed in either the source or the destination.

Use the value **Any:**

- As the source: To show the source points that can access the specified destination
- As the destination: To show the destinations that can be reached from the specified source point

Note: The source and destination cannot both be **Any**.

**To use the Source and Destination Scope dialog box**

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

2. Define the source and destination scopes as explained in the following procedures.

3. Click **OK**.
To define the source scope

1. To use specific entities in the source scope: In the Available Entities field, select all entities that are part of the scope and click to move them to the Selected Source field.

   Note: If you query from a network or a location containing networks, access is analyzed using the IP address ranges of the networks rather than each asset within the networks. To analyze access using routing rules or access rules on specific assets, select the assets rather than selecting the networks containing the assets.

2. To use IP address ranges in the source scope:
   a. In the Use IP Ranges field of the Source area, specify IP addresses:
      - Type an IP address range (or single IP address)
      - Click the Browse button next to the Use IP Ranges field to select IP address ranges
   b. If you are using a single IP address or IP address range and you want to include the entity to which the IP address range belongs, click Find Networks. Select a matching network and click Select.

   If you select an entity and specify alternate IP address ranges, the analysis starts from the selected entities, but Skybox uses the alternate IP addresses instead of the entity IP addresses.

To define the destination scope

1. To use specific entities in the destination scope: In the Available Entities field, select all entities that are part of the scope and click to move them to the Selected Destination field.

2. To use IP address ranges in the destination scope:
   a. In the Use IP Ranges field of the Destination area, specify IP addresses:
      - Type an IP address range (or single IP address)
      - Click the Browse button next to the Use IP Ranges field to select IP address ranges
   b. Select a network:
      - If you are using a single IP address or IP address range and you want to include the entity to which the IP address range belongs, click Find Networks. Select a matching network and click Select.
      - If you are searching from IP addresses in the source to IP addresses in the destination, click OK after specifying the IP addresses. Skybox suggests matching sets of networks for the query; select the network to use.
DEFINING THE SERVICES

By default, access between the source and destination is verified on all available services. However, you can specify specific services on which access is verified for the source or the destination. If specific services are specified, access is verified only on those services, rather than on all available services.

To specify specific services through which access is checked

1. (To specify services for the source) Click \( \text{\textless} \) in the Source area.
   
   The Services field appears in the dialog box.

2. Click the Browse button next to the Services field.

3. In the Services dialog box:
   
   - By default, the Available Services list is sorted by ports. To sort it alphabetically, click \( \text{\textless} \).
   - By default, common service families are displayed. To display all service families, click \( \text{\textless} \).
   
   3. In the Services dialog box:
      
      - In the Available Services field, select the desired source or destination ports and click \( \text{\textgreater} \) to move them to the Selected Services field.
      
      - Click the Browse button next to the Additional Services field to specify additional ports to use when checking access.
4 Click **OK**.
5 To use all services except those selected, select **NOT**.

### ADDITIONAL DESTINATION OPTIONS

Usually, you use the destination **Scope** field to define the destination scope—a collection of assets or networks that should be reachable by all packets. You can define a **Sending To** scope, consisting of IP address ranges. Skybox uses all IP addresses in the ranges that you specify in the **IP Ranges** field as destination addresses at the beginning of the access analysis, before network addresses are translated. Services specified in the related **Services** field are handled similarly.

Note: When you define **Sending To** properties, the destination **Scope** and **Services** fields are referred to as the **Arriving At** scope and services.

For example, you select **Internet** as the source **Scope**, you do not select a destination **Scope**, and you set the destination **IP Ranges** field to **1.2.3.40-1.2.3.50**. This query means “What networks, assets, and services are reached if a packet with a destination in the IP address range 1.2.3.40 to 1.2.3.50 is sent from the internet?”

If you select **Arriving At** entities and **Sending To** ranges, access is analyzed using the selected IP address ranges, but only the selected entities are displayed (that is, the selected entities filter the results).

**To use the additional destination options**

1 In the Access Query pane, click to expand the Destination area.

   The original destination scope and services are now shown in the Arriving At area and another area, Sending To, opens in the dialog box.
2 Click the **Browse** button next to the **IP Ranges** field.

3 In the IP Ranges dialog box, for each IP address range to be used, click **Add**, type the IP addresses of the range and click **OK**.

4 (Optional) Specify specific services through which to check access:
   a. Click the **Browse** button next to the **Sending To – Services** field.
   b. In the Services dialog box:
      - In the **Available Services** field, select services and click to move them to the **Selected Services** field.
      - Click the **Browse** button next to the **Additional Services** field to specify additional destination services to use when checking access.
   c. Click **OK**.
   d. To use all services except those selected, select **NOT**.

**Understanding the results**

The results of access analysis appear in the Analysis Results pane. By default, accessible entities are displayed, grouped by locations and networks or by security tags.

<table>
<thead>
<tr>
<th>Accessible Destinations</th>
<th>Group By</th>
<th>Network</th>
<th>Authentication</th>
</tr>
</thead>
<tbody>
<tr>
<td>Europe [768 IPs, 1 TCP port]</td>
<td>Network</td>
<td>Authentication</td>
<td></td>
</tr>
<tr>
<td>US [256 IPs, 5 TCP/UDP ports]</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**To understand the results**

1 Expand the tree.

Under the lowest locations are the accessible networks.

- View the networks without the locations by clicking **</>**.
Under each network is the range of IP addresses in the network that are accessible from **Internet**.

2. Expand the IP address ranges to see the services (') through which the network can be accessed.

3. (Optional) Group the results by services instead of networks by selecting **Service** in the **Group By** field on the toolbar.

4. By default, IP address ranges are shown in the results rather than specific assets.
   - View the accessible assets in the model rather than the IP address ranges by clicking .
   - Switch back to viewing IP address ranges by clicking .
5 Select a lowest-level node (asset or service).

A step-by-step explanation of the access route between the source and destination is displayed in the Access Route pane.

Note: If you do not have permissions for any of the devices in the route, you can see device names but no details about them, including access rules.
A visualization of the access route is displayed in the Map pane. The source is highlighted in green and the destination in turquoise.

If there are multiple routes, you can switch between them using the Routes control.

Inaccessible entities

In some cases, Access Analyzer shows that there is no access from the source to the destination. (This might or might not be the desired outcome of access analysis.)

There are 2 basic reasons why a network or asset is inaccessible:

- The route is blocked: An access rule denies access between the source and the destination (this is the most common reason).
- The route is broken: No routing exists from the source to the destination.

Use **Show Blocked Sources** or **Show Blocked Destinations** to discover why there is no access.
Blocked routes

If routes between the source and destination are blocked, the Access Route lists all hops from the source to the point where the route is blocked. The final entry in the table shows what is blocking the route—usually an access rule on a firewall. The full destination is displayed after the table, as for all access routes.

In the following figure, the route between the Development network and the Finance Servers was checked for access and no access was found. To see where the access is blocked, use **Show Blocked Destinations**.

The Access Route shows that access is denied (blocked) by the finance FW firewall and that the specific rule used is access rule 6.

Broken routes

If an entity is inaccessible for routing reasons (for example, some routers are missing in the model), the route is not blocked, but rather broken (incomplete). This can happen when:

- The source knows the destination by a different name or IP address (because of NAT rules).
- The model is incomplete and gateways that connect between the source and the destination are missing.
Routing rules are missing in gateways between the source and the destination.

There is a route to a null (black hole) in a gateway between the source and the destination.

If a route is broken, the Access Route provides an explanation of what happened, as in the following figure.

Saving an access query as an Access Check

You can save queries created in Access Analyzer and reuse them.
To save a query for later use

1. Click ☐.

![Save Access Query dialog box]

2. Type a name for the access query and select a location in the Access Policies tree.

To use a saved access query

1. Click ☐.
2. In the Open Access Query dialog box, expand the tree and select the desired access query.

Saving the results

You can save the results of access analysis in 3 different formats:

> As a CSV file

This saves a list of the source-destination-port combinations through which the specified access can be achieved, as in the following example.

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Authenticated</th>
</tr>
</thead>
</table>
## Chapter 5  Access Analyzer

### Source Destination Service Authenticated

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Authenticated</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.170.25.0-</td>
<td>192.170.33.0-</td>
<td>1-65535/20-21/TCP;</td>
<td>FALSE</td>
</tr>
<tr>
<td>192.170.27.255</td>
<td>192.170.33.255</td>
<td>1-65535/20-21/TCP;</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>1-65535/53-53/TCP;</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>1-65535/79-80/TCP;</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>1-65535/179-179/TCP;</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>1-65535/443-443/TCP;</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>1-65535/535-535/TCP</td>
<td></td>
</tr>
</tbody>
</table>

### As an XML file

This saves the results tree as an XML file, as in the following example.

```xml
<ExplainTree>
  <Location name="US">
    <Location name="New York">
      <Network name="dmz [192.170.33.0 / 24]"
        count_description="256 IPs;6 TCP/UDP ports">
        <IpRange name="192.170.33.0-192.170.33.255"
          count_description="256 IPs; 6 TCP/UDP ports">
          <PortRange name="21 (TCP)" count_description="0 IPs" />
          <PortRange name="25 (TCP)" count_description="0 IPs" />
          <PortRange name="53 (TCP)" count_description="0 IPs" />
          <PortRange name="80 (TCP)" count_description="0 IPs" />
          <PortRange name="443 (TCP)" count_description="0 IPs" />
          <PortRange name="53 (UDP)" count_description="0 IPs" />
        </IpRange>
      </Network>
    </Location>
  </Location>
</ExplainTree>
```

### A specific route as an HTML file

This saves the route displayed in the Details pane as an HTML file, as in the following example.

```
Access Route
  From: Internet (cloud)
  To: dmz (192.170.33.0/24)

Source
Internet (cloud)
source IP range(s): 0.0.0.0-9.255.255.255, 10.0.0.0-16.0.0.0, 16.0.0.2-172.15.255.255, ... source service(s): 1-65535/TCP, 1-65535/UDP
Sending To IP Range(s): 192.170.33.0-192.170.33.255
sending to Service(s): 21/TCP, 25/TCP, 53/TCP, 80/TCP, 443/TCP, 53/UDP

<table>
<thead>
<tr>
<th>#</th>
<th>Network Device</th>
<th>Inbound Access Rules</th>
<th>Outbound Access Rules</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>src mem FW (16.0.0.1)</td>
<td>2 (ACCESS) - Allow</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>src prod FW (192.170.198)</td>
<td>2 (ACCESS) - Allow</td>
<td></td>
</tr>
</tbody>
</table>

Destination
dmz (192.170.33.0/24)
destination IP range(s): 192.170.33.0-192.170.33.255
destination service(s): 21/TCP, 25/TCP, 53/TCP, 80/TCP, 443/TCP, 53/UDP
```
Chapter 6

Network Access Compliance

This chapter explains how to use Skybox Network Assurance to check access across all or part of your organization’s network.

In this chapter

Network Access Compliance overview ............................................. 80
Access Policy management .......................................................... 83
Access Policy analysis ..................................................................... 92
Access Policy compliance and violation management .................... 93
Access Policy customization............................................................ 104
Access Checks reports .....................................................................114
Firewall ACLs ................................................................................115

Network Access Compliance overview

Skybox Network Assurance provides a set of predefined Access Policies that you can customize for your organization. By marking areas in the model as belonging to different zones, Skybox checks the policies against your organization’s network.

ABOUT ACCESS POLICIES

An Access Policy defines the constraints on the traffic in a network. It verifies that users can access essential assets and that no security holes are exposed by firewall access rules. The Access Policies node is divided into public and private folders; each folder can contain multiple Access Policies. You can divide each Access Policy into folders to create a meaningful hierarchy. Each Access Policy folder contains Access Policy sections—groups of Access Checks defining the relationship between a specified source and destination. Usually, the source and destination of a policy section are zones, but they can be specific networks or virtual assets.

Each policy section consists of a source, a destination, and Access Checks that define the relationship between the source and the destination. For example, one Access Check defines the amount of HTTP access and another Access Check blocks Trojan and worm ports.
PREDEFINED ACCESS POLICIES

Skybox includes a set of predefined best practices Access Policies that includes implementation for NIST 800-41 guidelines and for PCI DSS guidelines.

The predefined set of Access Policies:

- Is a template of best practices that you can modify to match your organization by mapping the different parts of the network to specific zones. The template contains policy sections that represent the relationship between these zones.
- Enables you to check whether your organization is compliant with known security issues and helps to identify specific services and access rules that must be fixed.
- Includes separate Access Policies for NIST 800-41 and for PCI DSS, and separate predefined zones for each.

The predefined zones represent common network areas that are frequently used in organizations’ networks; the policy sections in the predefined Access Policies reference the predefined zones.

Note: Although **PCI DSS V3.2 Policy** is included in the Network Assurance tree, it is relevant only for firewalls audited in Skybox Firewall Assurance.

You can modify a policy to correspond to your network by, for example, adding additional zones and policy sections to match your organization’s specific security issues, hiding policy sections that do not match your network, and tweaking access limits in other policy sections.

Before using any predefined Access Policy to test your network, assign a zone type to each network that you want to test.
USE CASES FOR NETWORK ACCESS COMPLIANCE

Typical use cases for monitoring network Access Compliance:

› On a continuous basis
   You can schedule a Skybox task that updates Access Compliance to run in on a regular basis. You can check for violations by examining the Access Policies, or you can schedule a report every time that an Access Policy is updated and view the report to look for violations.

› As required, with a report of Access Compliance as the result

› Before planned changes to the firewalls or the policy, to check the effects of the planned change
   Use the What If model to try out changes and compare access between the What If and Live models to understand the effects of the planned changes.

Basic workflow for using Skybox Network Assurance to verify network Access Compliance

1 Mark networks, network groups, virtual domains and security tags/groups as zones (see Zone mapping (on page 89)).
2 (Recommended) Review the predefined Access Policies and modify them to correspond to your organization.
   One area that might need modifying in the predefined policies is the definition of the limits on Limited Access Checks. For example, in the Limited SMTP Access Check, access from the External zone is limited to 5 mail servers. If your organization has more than 5 mail servers that must be accessible, change this limit. For additional information, see Policy management (on page 83).
   Note: You can review and modify the policy after analysis. In this case, access violations found the 1st time might be caused by Access Checks that are not correctly defined for your organization.
3 After you click Analyze, Skybox applies the Access Policies to the zones, checking the traffic across the network according to the definitions in the Access Policies. For additional information, see Policy analysis (on page 92).
4 Review the violations to understand where changes are necessary. Review the results of the analysis to see whether the network is compliant with the Access Policies. If it is not compliant, check which access rules of which firewalls are causing the problems. For additional information, see Access Policy compliance and violation management (on page 93).
5 Make changes to the violations (see Handling policy violations (on page 101)).
6 Generate and send policy Access Compliance reports (see Network Access Compliance reports (on page 103)).
Access Policy management

This section explains the predefined NIST Access Policy for network Access Compliance auditing.

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 policy.

STRUCTURE OF THE PREDEFINED ACCESS POLICY

The predefined NIST 800-41 Access Policy is divided into folders according to the access that is to be tested.

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

**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 the following 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**: (Used if the previous 2 sets of Access Checks do not cover all services) Services (that are not specified by the previous 2 sets) 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.

  > **Limited Services Access Checks**

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

  > If 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.”

  > If 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.”

  If you limit access by IP addresses, the limit can be specified as:

  > 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.

  > A 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 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**

  If you limit 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.”

  > A 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 a single destination IP address are accessible, the tested device is non-compliant.

Access tests
Skybox divides each Access Check in a policy section 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 entities that are connected to and deleted from the zone type dynamically as the network evolves.

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

Policy sections that use zones
If the source or destination is a zone type, each zone (that is, each network) of that zone type is used as a separate source or destination to create the tests. Because 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 model contains the following locations:

- External zones: Internet, Partner

DMZ-US is mapped as a single zone because the user wants to view this location’s overall Access Compliance results and is not interested in the connections between the US sublocations.

DMZ-Europe is mapped as 2 zones (DMZ-Europe-London and DMZ-Europe-Paris) because the user wants to view each location’s Access Compliance results separately and is also interested in the connections between the European sublocations.

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:

- Internet to DMZ-Europe-London
- Internet to DMZ-Europe-Paris
For a policy section with **Source** = DMZ zones and **Destination** = DMZ zones, the connections between DMZ-Europe-London and DMZ-Europe-Paris are tested, whereas the connections between DMZ-US-NY and DMZ-US-LA are not tested.

### Access Checks that use a specific list of sources or destinations

If there is a specific list of sources or destinations, Skybox uses the specified entities to create the tests.

For example, for an Access Check with **Source** = Internet and **Destination** = DMZ-Europe-Paris, DMZ-Europe-London, DMZ-US-NY, DMZ-US-LA, the following access tests are created:

- Internet to DMZ-Europe-London
- Internet to DMZ-Europe-Paris
- Internet to DMZ-US-NY
- Internet to DMZ-US-LA

You can view these tests in the **All Access Tests** tab of the workspace.

### Viewing and managing access tests

Even before the results of an Access Check are analyzed, the **All Access Tests** tab of the Table pane displays a list of all access tests for an Access Check. After analysis, each access test has a compliance indicator (pass or fail) instead of a question mark—you can view a list of non-compliant tests for the Access Check in the **Violations** tab.

Review the list of access tests before you analyze the Access Check. If the list of tests is not what you expect, it could mean that the Access Check is not defined correctly or that you did not define zones at the correct granularity—either the zones defined are not specific enough (you selected parent entities as zones instead of subentities) or the zones defined are too specific (you selected subentities instead of parent entities)—you might need to redefine the zones on the parent or child entities of the entities that you originally used. Check the zones in the **Zones** node of the Network Assurance tree.

### Disabling access tests

When you view the access tests, there might be tests that are not necessary or should not be analyzed. You can disable tests that do not need to be analyzed. If you disable an analyzed test, its analysis results are erased.
To disable or enable a test

- With the Access Check selected in the tree, 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.

Opening access tests in Access Analyzer

To explore the results of an access test, you can open the access test in Access Analyzer. You can use the properties of the test as the basis for additional queries about the model. You can view the results in different formats (based on source or destination, services, interfaces, and entities), without affecting the Access Policy.

To open an access test in Access Analyzer

- In the list of access tests (or violations) in the Table pane, right-click the desired test and select Open in Access Analyzer. The results are displayed in the Analysis Results pane and the access test is displayed in the Access Query pane—you can modify the query.

ZONE MAPPING

To use zones, you assign zone types to network entities in the model. For example, you can designate the internet cloud as External and the DMZ network group as DMZ. After the zones are defined, you can check the network for compliance with the Access Policy. Skybox checks compliance with every policy section for which your organization has networks in the zone type of the source and in the zone type of the destination.

Predefined zone types

Skybox Network Assurance has 4 predefined zone types:

- External: A public network 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.
- Partner: Partner or B2B networks outside your organization. Partner networks usually have limited access to DMZ networks and to the internal assets of your organization.
- DMZ: A network between a trusted internal network and an untrusted external network. The DMZ contains devices accessible to the external network via protocols that can include HTTP (web), FTP, SMTP (email), and DNS.
- Internal: A trusted network inside your organization that contains internal assets.

These zone types cannot be deleted. They are used in the predefined Access Policy and you can use them in Access Checks.

The predefined Access Policy is based on these zone types. To use the Access Policy, map the network groups or networks to be checked to the zone types. To use the Access Policy to test access between 2 zone types, define zones of each of those types.
Note: The same Access Policies and zones are used in Skybox Network Assurance and Skybox Firewall Assurance. The predefined set of Access Policies includes PCI zones and a PCI Access Policy; these are intended for use only when working with Skybox Firewall Assurance for PCI firewall audits.

**Marking zones**

You mark zones in the Model workspace.

You can mark the following entities as zones:

- Networks
- Network groups
- Locations
- Security tags

To improve performance when checking compliance of medium to large organizations, we recommend that you mark network groups or locations rather than individual networks, because then the whole network group or location is checked for compliance together, rather than checking each network separately. For information about creating network groups, see Network groups (on page 30).

**To mark entities as zones**

1. Select relevant entities:
   - In the Locations & Networks tree, navigate to a location; click the Networks tab in the workspace; select the network or networks to mark.
     - If all the networks in the location have the same role, select the location instead of the separate networks.
   - In the Virtual Domains tree, navigate to a security tag.
   - In the list of network groups, select a network group.

2. Right-click the selected entity or entities and select **Mark as Zone**.

3. In the Zone Type field, select the zone type for this entity.

4. Click **OK**.

Note: If you mark a network group as a zone and networks in the group are already marked as zones, select the option that removes the zone marking on the individual networks.

If the entity Properties dialog box is open, you can define the zone using the Zone Type field.
You can add entities to a zone using the list of zones in the Network Assurance workspace.

**To add entities to a zone**

1. In the Network Assurance tree, select **Zones**.
2. In the Table pane, right-click a zone type and select **Mark Entities as Zones**.
3. In the **Select Entities** field, select the desired entities from the tree. You can select multiple locations, networks, security tags, segments, or network groups to mark as instances of the selected zone type; each selection becomes a separate zone.
4. Click ![right arrow] to move the selected entities to the **Selected Entities** field.
5. Click **OK**.

**EXPORTING AND IMPORTING ACCESS POLICIES**

You can export Access Policies and reimport them later. 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 compare the policies and select the one that better meets your 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 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 to import.
   To use a file from a local directory (rather than a file on the Server machine), click Upload.

3 Click OK.

Access Policy analysis

When Skybox analyzes network Access Compliance, it:

- Analyzes the access routes between the specified source and destination, based on network topology, access and routing rules, address translation, and port translation
- Checks whether the existing access complies with the selected policy

You can analyze the Access Policies tree or any part of it.

To analyzes network Access Compliance

1 Select the node in the Access Policies tree to analyze.

2 Click Analyze.
   Access results are displayed in the workspace and compliance indicators appear in the Access Policies tree.

To analyze a specific access test

1 Select an access test in the Table pane.

2 Click Analyze.
   Compliance results are displayed on the test.

Note: Analysis of large Access Policies can take up to several hours. For best results, schedule the analysis to run at nighttime or weekends, using a Policy Compliance task (which is explained in the Skybox Reference Guide).
TROUBLESHOOTING ANALYSIS

After an Access Policy (or any part thereof) is analyzed successfully, compliance results are displayed in the Tree pane, including pass/fail indicators and compliance metrics. If no compliance results are displayed after analysis finishes, the analysis failed.

Issues that can cause Access Policy analysis to fail are listed in the following table.

<table>
<thead>
<tr>
<th>Possible cause of failure</th>
<th>Information about how to fix issue</th>
</tr>
</thead>
<tbody>
<tr>
<td>Problems in the network model</td>
<td>Building the model (on page 20)</td>
</tr>
<tr>
<td>Missing zone definitions</td>
<td>Defining zones (on page 90)</td>
</tr>
<tr>
<td>Improperly defined policy sections or Access Checks</td>
<td>Policy customization (on page 104)</td>
</tr>
</tbody>
</table>

Access Policy compliance and violation management

This section explains how to verify that your organization’s network complies with its Access Policy, and how to view and handle Access Policy violations.

REVIEWING COMPLIANCE METRICS

After analysis, compliance metrics present an overall summary of Access Compliance for the whole Access Policy and for every policy folder. Compliance metrics show the percentage of compliance, and how many tests are compliant and not compliant.

The main Summary page of the Network Assurance node contains summary information about Access Compliance, including a link to the violating rules and a link to the violations.
You can also view compliance metrics by drilling down from the main page for each Access Policy, policy folder, or policy section.

REVIEWING THE VIOLATING ACCESS RULES

Sometimes, many violations are caused by a single access rule in a single firewall. It is easy to see 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 an Access Policy, policy folder, policy section, or Access Check.

- If you sort the list by number of violations, you can see the access rules that cause the most violations. The Details pane lists the attributes of 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 a single network or asset.

When you select an access rule, the Details pane includes:

- Highlights of the access rule compliance and its **business attributes** (see page 94)
- A list of the violations for that access rule
- 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 95).

**Business attributes**

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

Skybox includes the following business attributes for access rules:
Administrators can create additional (custom) business attributes for their organization.

**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 displayed 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 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.

**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.

You can view violations using:

- **Tie Violations** links of the Network Assurance Summary page
- The **Violations** tab of an Access Check, to view a list of violations for that Access Check

You can view violations in the **All Tests** tab, together with compliant tests.

- **Access Policies > Access Policy Violations**, to view different groups of the violations:
  - All violations from all Access Checks
  - Critical violations from all Access Checks

For each violation, you can see:

- **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:

| Too many IP addresses are accessible in the destination dmz [192.170.33.0 / 24]. The limit in the Access Check specifies that no more than 5 destination IP addresses should be accessible for the service [25/TCP] - smtp. The following IP address exceeded the limit by being accessible on too many IP addresses: 25 (TCP) - reached on 256 IP addresses |

Violating Rules: A list of all the access rules that contributed to this violation

Access Results: Violations show the entities that violate the Access Check; compliant tests show (by default) the entities that comply with the Access Check (see Viewing access results (on page 96)).

Exceptions: A list of exceptions defined for this access test.

Note: You can view the same information for compliant tests of an Access Check by using the All Access Tests tab.

VIEWING ACCESS RESULTS

You can view the access results of tests in the Access Results tab of the Details pane.

To view access results for an access test

1 Select a violation or test:
   - Select an Access Check in the tree and then select the violation or test in the Violations or All Access Tests tab of the Table pane.
   - Select a node in the Violations folder of the tree and then select a violation in the Table pane.

2 Click the Access Results tab in the Details pane.

Display filters

The toolbar at the top of the Access Results tab of the Details pane contains display filters that define what information displayed in the results tree and how it is displayed.

Show: 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 inaccessible sources or destinations are displayed in the results tree, all names in the tree are italicized.

- **Group by**: Specifies whether to group the entities displayed in the results tree by networks, services, or security tags (for virtual assets).

- **Authentication**:
  - No: Non-authenticated traffic
  - Yes: Authenticated traffic
  - N/A (Both): Authenticated and non-authenticated traffic

- **Entities**:
  - **Model Entities Only**: Assets and services that are part of the current model. If these existing entities are hidden, only the IP address and port ranges are shown.
  - **Possible IP Ranges**: All IP addresses and port ranges that are exposed by firewall access rules, even if they do not exist in the model.

Note: The default view (model entities or IP address ranges) depends on the expected type of access.

- **Show / Hide locations**: Specifies whether to group networks into locations.

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

- **Mark as Exception**: Specifies whether to mark 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 possible access routes for the selected entity in the results tree.

- **What If**: Specifies whether to include the reply route when an Access Route is displayed.

- **What If**: Runs a comparison between access in the current model (usually Live) and access in the What If model. You can select a different model with which to compare the current model.

**Access Results tab**

The **Access Results** tab contains a results tree. You can expand the services to see the relevant networks or security tags and then expand these networks or security tags to see the assets or IP address ranges.
If results are grouped by networks or security tags, you can expand these to see the assets or IP address ranges and then expand these to see the relevant services.

Depending on the selected view (that is, the selected value of the Show field), the results tree displays:

- **Accessible Destinations**: The destinations accessible from the specified source point
- **Sources Accessing the Destination**: The 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)

The content of each view depends on the display filters (see page 96) that you select.

If destinations are displayed, you can drill down from a destination asset to see accessible or blocked services on that asset. If source points are displayed, you can drill down from a destination network to see the gateways that enable or block access.

**Viewing the Access Route**

The *Access Route* shows every potential route 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 asset or a service.
2. Click Show Access Route.

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

If inaccessible entities are displayed in the results tree, the dialog box shows every blocked route.

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

- The 1st step is the source point.
  - If the source point is a subset of the source specified in the Source field, the source IP address ranges are listed.
  - Intermediary steps list gateways passed on the way, with their access rules and address translation rules (if any).

Rules are shown with their direction, rule number, ruleset name, and rule action. Each intermediary step includes an inbound rule and an outbound rule. Click the link in a rule to open the Access Control List Editor for easier viewing of the rule in the context of the ACL.

If access goes through a VPN tunnel, Encrypted is listed in the step, as well as information about the VPN tunnel.
The final point is the destination. Asset name, IP address, service type and port number are displayed.

For inaccessible (blocked) routes, all hops from the source to the point where the route is blocked are displayed. The final entry shows what is blocking the route—usually an access rule on a firewall. For information about inaccessible routes, see Inaccessible entities (on page 75).

Comparing access between two models

You can view the results of an access test on 2 models at the same time; the differences between the results in the models are displayed side-by-side. You can check whether the access results change after changes are made to the network or access rules.

For example, if you have an access problem in the Live model (representing your actual network configuration), try making changes to firewall policies in the What If model and check whether the access problem is resolved.

To compare access between 2 models

1. In the Access Policies folder, locate the required Access Check.
2. In the All Access Tests tab or the Violations tab, select the desired test.
3. In the Details pane, click the Access Results tab.
4. On the Access Results toolbar, click What If.

Note: By default, when working with the Live model, comparison is to the What If model. However, you can select the Forensics model.

Access is analyzed for both models; the Results pane is split to display the results.

There is a separate compliance indicator (red or green icon) for each model.

- If the current model does not comply with the desired access, but the comparison model does, the changes that you made (between the current model and the comparison model) resolved the access problem.
- If the current model complies but the comparison model does not, the changes that you made to the firewall caused additional, undesired access changes.

5. If both trees display actual results (that is, not a message saying that the test is compliant), you can compare the results for a specific entity:
   - Click ⌁ and select the desired entity in a results tree.
     If the selected entity exists in the other model, it is selected in the other tree.
Synchronization between the 2 trees continues until you click 🔄 again.

6 To show access to an entity in either results tree, select the entity and click Show Access Rule.

7 To view the access rules for the desired model, in the Access Route Details dialog box (opened in the previous step) click the link in an access rule.

HANDLING POLICY VIOLATIONS

Policy violations (noncompliant tests) might mean that:

▷ The Access Check is not defined correctly and must be fixed

For example:

- The predefined policy states that there must be no more than 5 SMTP servers in the DMZ; if your organization’s network has more than 5 SMTP servers in the DMZ, this limit could be changed to 10.
- There might be an Access Check that states “Computer A must not have access to Computer B”. Analysis might discover that Computer A has access to Computer B on port <n>, so that the network is not compliant with the Access Check. In fact, the access on port <n> is not a problem, so if the Access Check is redefined as “Computer A must not have access to Computer B except on port <n>,” the network is compliant the next time that it is analyzed.

▷ Entities in the source or destination of the access test should be marked as exceptions

Sometimes, specific entities in a location or zone that is being tested have different access permissions than the other entities in that location or zone and should be excluded from the access test. If these entities are marked as exceptions (see page 102), the test is compliant.

▷ There is a problem in the network

For example, a firewall was changed so that a client cannot access a server; the access rule (or the network) must be fixed to permit the desired access.

- You can view the firewalls and access rules that caused the violation
- You can open a ticket on the violating access rules. Include the details of the violations and request that the violating access rules be recertified or fixed (see Creating tickets (on page 102)).

▷ The Access Policy and the network are correct, but the network is not modeled correctly in Skybox.

This could be caused by old configuration files from network devices or by missing information. You can fix the model by reimporting the device configuration files (see Building the network model) (on page 21) or by creating clouds to fill the gaps (see page 26). In this case, the Access Check is compliant the next time that it is analyzed.

When you are working to solve policy violations, consider all these possibilities for each violation. After the Access Policy is debugged and the model is up-to-date, most violations are caused by problems in the network.
To fix an Access Check

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

Marking entities as exceptions

You can mark entities as exceptions to specific access tests using the Access Results tab. When you mark exceptions in this way, they are added to the list of exceptions for the access test and you can manage them as policy exceptions.

Note: You can also define exceptions for Access Checks, policy sections, and policy folders (see Defining exceptions (on page 105)).

To mark entities as an exception

1 In the Table pane, select the access test; in the Details pane, click the Access Results tab.
2 In the results tree, locate and select the entities to mark as exceptions.
   - For information about exception properties, see Exception properties (on page 106).
3 Right-click the entity or entities and select Mark as Exception.
4 (Recommended) Add a description of the exception.
5 (Optional) Add an expiration date for the exception.
   When the exception expires, the violation reappears.
6 Click OK.
   The results tree is refreshed and the marked entities are omitted. You can view a list of exceptions for the selected access test in the Exceptions tab.

Note: If you mark exceptions on the source, the results tree cannot be refreshed until the test is reanalyzed.

Creating tickets

Violating access rules should be reported so that they can be examined and, possibly, changed. This is usually done via policies that your organization sets up. These policies check the access rules for risk and, if necessary, create tickets listing the rules that should be reviewed. Firewall administrators review these tickets in Skybox Change Manager and determine whether the rules continue to be valid (create an exception) or need fixing (create tickets requesting changes to the access rules).

Although these tickets are usually created automatically, at times you might want to create tickets manually for violating rules.

To create a ticket for violating access rules

1 Display the violating rules in the Table pane (for example, by clicking the Violating Rules link when Network Assurance is selected in the tree.
2 Select the access rules that should be reviewed by a firewall administrator.
3 Right-click and select Recertify Rule.
4 In the New Rule Recertification Ticket dialog box, select a workflow (if there is a choice), the priority of the ticket, and an owner.

5 Click OK.

The tickets are created and links to the new tickets in Skybox Change Manager are displayed. If any of the access rules have tickets, links to those tickets in Skybox Change Manager are displayed. Only a single recertification ticket can be open for an access rule at any time.

Note: You can view the tickets that you created in the Tickets workspace.

For additional information about the review and recertification process, see the Rule review and recertification chapter in the Skybox Firewall Assurance User Guide.

NETWORK ACCESS COMPLIANCE REPORTS

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

There are 2 predefined Network Access Compliance reports:

› **Network Compliance – Overview**: Presents an overview of your organization’s network’s Access Compliance. The report contains information about the success rate of the Access Policy and the number of Access Policy violations and their types, grouped by policy section.

› **Network Compliance – Details**: Presents detailed information about your organization’s network’s Access Compliance. The report contains information about the success rate of the Access Policy, the number of Access Policy violations and their types, and details of the non-compliant Access Checks.

To generate a Network Access Compliance report

Note: Folders and Access Checks that were not analyzed are not included in these reports, even if they are in the defined scope.

1 Open the Reports workspace.

2 In the Tree pane, click Reports.

3 Select Public Report Definitions > Network Compliance and then select the desired report definition.

   The workspace displays the properties of the report.

4 Click Generate.

   You are asked whether to generate the report in the background or in the foreground. It can take time to generate large reports, so it is often useful to generate in the background and keep working.
5 Select the desired generation method (background or foreground) and click OK.

If the report is generated in the background, you can double-click in the status bar to open the Operational Console and follow the task’s progress (using the displayed messages).

A report based on the compliance data is generated from the report definition. When generation finishes, the report is displayed in the workspace.

Note: If you generate reports in the background, they are not visible in the workspace until you click $\clubsuit$.

You can:

- Change the format of a report (to HTML or RTF)
- Change the scope of a report to include only specific parts of the Access Policy
- Create definitions for additional Network Access Compliance reports
- Schedule reports to run at specific times and be sent to specified Skybox users

For additional information, see the Working with reports section in the Skybox Reference Guide.

For additional information about defining Network Access Compliance reports and the sections that can be included in the reports, see the Network Access Compliance reports topic in the Skybox Reference Guide.

Access Policy customization

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

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.

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.

DEFINING EXCEPTIONS

Sometimes, the Access Policy checks access from a source to a destination, but there are specific entities (in the source or the destination) or specific services to exclude from access tests.

In theory, you can create a policy section by listing the specific assets or services to include (rather than specifying the entire source or destination) and leaving out the assets and services to exclude. However, it is usually easier to create the policy section using the desired scopes and then specify the exceptions to the rule on specific tests.

There are 2 ways to define policy-related exceptions:

➢ From the definition of a policy folder (if the exceptions are relevant for all the policy sections), policy section, or a specific Access Check, when you know of specific entities to exclude from the rule

If you know there are specific assets in the source or destination—or specific services on source or destination assets—to exclude from the analysis, define them as exceptions before compliance is analyzed.

➢ After compliance is analyzed, if you realize that you want to exclude some results for an access test

If, when reviewing the results of an access test, you find specific assets or services to exclude, mark them as exceptions in the results tree (see page 102).

Both methods add exceptions to the properties of the policy folder, policy section, or Access Check, so that the exceptions are considered when compliance is analyzed. You can modify the list of exceptions.

Note: After you define policy exceptions, reanalyze the affected tests.
To define policy exceptions

1. Right-click the policy folder, policy section, or Access Check (depending on the scope of the exception) and select Exceptions.
2. In the Exceptions dialog box, define the exceptions:
   a. Click Add.
   b. In the New Access Policy Exception dialog box, define the exception as explained in Exception properties (on page 106).
   c. Click OK.
   d. Repeat steps a through c for additional policy exceptions.

Exception properties

The properties of Access Policy exceptions are described in the following table.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exception ID</td>
<td>(Read-only) An ID for the exception. The ID is filled in when the exception is saved.</td>
</tr>
<tr>
<td>Scope</td>
<td>The policy folder, policy section, or specific Access Check to associate with the exception. If you create an exception by clicking on a test result, the default scope includes only the relevant Access Check. However, you can extend the scope.</td>
</tr>
<tr>
<td>Test</td>
<td>The access test with which this exception is associated.</td>
</tr>
<tr>
<td>Test ID</td>
<td>(Read-only) The test ID of the selected access test. If you select an Access Check, Access Policy, or policy section or folder, this field is empty.</td>
</tr>
<tr>
<td>Source</td>
<td>The source to use for the exception.</td>
</tr>
<tr>
<td>Destination</td>
<td>The destination to use for the exception.</td>
</tr>
<tr>
<td>Services</td>
<td>The services to use for the exception.</td>
</tr>
<tr>
<td>Rule Applications</td>
<td>The applications to use for the exception.</td>
</tr>
<tr>
<td>Expiration Date</td>
<td>Specifies the date after which the exception expires.</td>
</tr>
<tr>
<td>Note: After the exception expires, the violation reappears.</td>
<td></td>
</tr>
<tr>
<td>Tag</td>
<td>Enables you to categorize the exception according to your requirements; use this field to search for the exception.</td>
</tr>
<tr>
<td>Ticket ID</td>
<td>The ticket ID of the Change Manager ticket associated with this exception (when available).</td>
</tr>
<tr>
<td>User Comments</td>
<td>Enables you to add comments.</td>
</tr>
<tr>
<td>User Comments (History)</td>
<td>(Read-only) A list of all the previous user comments for this exception.</td>
</tr>
</tbody>
</table>
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 a zone type (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 113).

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.

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 108).

3 Define or copy the Access Checks (see page 109).
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 one of them; they cannot both be **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 specific networks or virtual assets, use **Network Entities**.

Note: Skybox only uses policy sections created for Zone Types when checking compliance via Change Manager.

3 To define the source:
   - In the **Available Entities** field, select all entities that are part of the scope and click **Source** 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.
If you select an entity and then specify IP address ranges, the analysis starts from the selected entities, but Skybox uses the specified IP addresses instead of the entity IP addresses. If you specify IP address ranges without selecting any source entity, you must select entities in Destination Scope. In this case, Skybox uses the specified IP addresses as source addresses for analyzing access to the Selected Destination entity.

4 To define the destination:
   - In the Available Entities field, select all entities that are part of the scope and click Destination 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.
If you add Access Checks to a policy section by copying from existing policy sections, Skybox examines the selected Access Checks and warns you if there are:
   - Two Access Checks with the same name
   - Two 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 until you have selected 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, 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** (on page 111).

At a minimum, specify values for the 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, select New > No Access Check, and then select:
     - Services: To block specific services (ports)
     - Applications: To block specific web applications

Note: Access Checks for applications are only tested on NGFWs.

2. Fill in the fields according to the table in Access Check properties (on page 111).
   At a minimum, specify values for the fields Services or Applications, and Description.

3. Click OK.

Access Check properties

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

Note: If you change any value after analyzing the Access Check, reanalyze the Access Check for the changes to take effect.

**CREATING 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, which is optional, is displayed next to the name in the workspace when you select the **Zones** node.

3. Click **OK**.

**FULL ACCESS CHECKS**

Full Access Checks confirm that there is full access between 2 points. For example, use a Full Access Check to verify that users of an asset have full access to the servers of that asset.
In the Access Policies tree, a Full Access Checks is displayed with \[ \text{ɪ} \] next to its name.

Note: You can create Full Access Checks as part of a (private) Access Policy or policy folder, but not as part of a policy section; policy sections contain only Limited-Access and No-Access Access Checks.

**To create a Full Access Check**

- In the Private Access Policies tree, right-click the parent node and click **New > Full Access Check**.

**ACCESS QUERIES**

To analyze access without checking for compliance, create an access query. For example, some tests might be used regularly by the development team but are not part of any Access Policy.

Access queries are displayed with \[ \text{🔧} \] next to their name.

**To create an access query**

- In the Private Access Policies tree, right-click the parent node and select **New > Access Query**.

Although access queries are not part of an Access Policy, they are included in the tree and are analyzed as part of **Analyze Access Compliance**. However, they do not appear in Access Policy reports and do not affect the compliance results of the Access Policy.

**Access Checks reports**

Skybox enables you to generate 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 a 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. It can take time to generate large reports, so 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 in the status bar to open the Operational Console and follow the task’s progress (using the displayed messages).

A report based on the 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 defining these reports, see the Working with reports section in the Skybox Reference Guide.

### Firewall ACLs

When you work with Skybox Network Assurance, you can:

- View firewall ACLs
- Edit an ACL in the What If model and view the differences between the edited ACL and the current ACL (in the Live model)

You can compare the network Access Compliance results of the changed model to the results in the Live model to understand whether the changes improved network Access Compliance.

- View a historical ACL by loading a saved model to the Forensics model and compare it to the current model

You can use the following Skybox tools to work with firewall ACLs:

- Access Control List Editor
- Compare dialog box (see page 117)

### COMPARING ACCESS RULES BETWEEN MODELS

*To compare access rules*

1 In the current model, right-click the relevant firewall and select **Advanced > Compare > Access Rules to** and the model to use for the comparison.

In the Compare dialog box, the most common view is selected in the left-most pane; you can switch views.
If an access rule has changed significantly between models (for example, **Source** and **Destination**—2 important fields—have changed), it is considered a new rule and displayed as such in the Compare dialog box.

The rules in the current model are displayed in the left-hand rule-data pane; the rules in the model selected for the comparison in the right-hand rule-data pane. Differences are color-coded by type; icons indicating the type of change are displayed to the left of the table.

By default, the comparison uses the names of firewall objects and not the resolved IP addresses of each object name.

1. To view a comparison of the resolved IP addresses for firewall objects, click **Show Resolved Addresses**.
2. To see the comparison for a rule chain other than the default rule chain or the comparison for an object, click the rule chain in the left-most pane.
4. To see information about a change, click the icon or double-click anywhere in the row of the change.

5. In the left-hand pane, select the changes to view in the rule. For changed rules, the 2 versions of the rule are displayed side-by-side. For added or deleted rules, the rule is displayed in the model in which it exists. The model names are displayed on top of the rule data.

COMPARING ACCESS RULES BETWEEN FIREWALLS

Some networks use asset clusters to provide redundancy capability. In some cases (for example, Check Point FireWall-1 clusters), the cluster members usually have the same access rules. In other cases (for example, Cisco HSRP clusters), the policies of the cluster members might become unsynchronized. Use Skybox’s access rule comparison to compare access rules between any 2 network devices in the model, including clustered devices.

You can compare access rules between devices in the same model by:

- Selecting 2 devices and comparing their access rules
- Selecting 1 device and searching for the 2nd device

To compare access rules between 2 selected devices
1. Select the 2 devices on which to compare access rules.
2. Right-click a selected device and select Compare Access Rules.

   In the Compare dialog box, access rule differences are color-coded by type, with icons indicating the type of change displayed to the left of the table.

   You can toggle the display between object names and resolved IP addresses (click Resolved Addresses).
3 View the details of a change:
   • Click the change icon.
   • Double-click anywhere in the row of the change.

To compare devices
1 Select the device whose access rules you wish to compare.
2 Right-click the selected device and select Advanced > Compare > Access Rules to > Other Device.
3 In the Other Device dialog box, select the comparison device and click OK.
   Note: If the device is part of a cluster, Skybox suggests another cluster member as the comparison device.
4 View the details of a change:
   • Click the change icon.
   • Double-click anywhere in the row of the change.

COMPARING ROUTING RULES AND NETWORK INTERFACES
Use Skybox to:
   › Compare routing rules and network interfaces between models
   › Compare routing rules between gateways in the same model (for example, in a cluster)

To compare routing rules
1 In the current model, right-click the relevant gateway and select Advanced > Compare > Routing Rules to and the model (or gateway) to use for the comparison.
   • If there are no differences between the 2 sets of routing rules, you get a message to that effect. Click OK.
   • If a routing rule has changed significantly (for example, the Destination Address has changed), it is treated as a new rule and displayed as such in the Compare dialog box.
2 To see the details of a change, click the icon or double-click anywhere in the row of the change.

To compare network interfaces
1 In the current model, right-click the gateway or asset and select Advanced > Compare > Network Interfaces to and the model to use for the comparison.
   • If there are no differences between the network interfaces in the 2 models, you get a message to that effect. Click OK.
   • If a network interface has changed significantly between models (for example, the IP address has changed), it is treated as a new interface and displayed as such in the Compare dialog box.
2 To see the details of a change, click the icon or double-click anywhere in the row of the change.
Chapter 7

Auditing the network on a continuous basis

This chapter explains how to set up and use automated workflows in Skybox Network Assurance so that you can audit the network on a continuous basis.

In this chapter

Auditing the network .......................................................... 119
Automated policy analysis ................................................... 119
Using tasks for automation ................................................. 120
Triggers .............................................................................. 126

Auditing the network

To audit the network, on a regular basis:
1. Run data collection and other tasks that update the model
2. Analyze the data; tickets and alerts can be created as part of the analysis

Note: You can integrate Skybox with other ticketing systems (see the Tickets API chapter in the Skybox Developer Guide or contact Skybox technical support (see page 7)).

Auditing the network on a continuous basis requires automation.

Automated policy analysis

Analysis – Policy Compliance tasks analyze compliance with your organization policies. In Skybox Network Assurance, you can use these tasks for Access Compliance and for Configuration Compliance. As with all tasks, you can set them to run on a specific schedule or triggered by the outcome of another task.

You can create multiple Analysis – Policy Compliance tasks to analyze different types of compliance, different policy folders, and so on.

To create an Analysis – Policy Compliance task

1. Click Operational Console.
3 In the **Task Type** field, select **Analysis – Policy Compliance**.
   - For information about the task properties, see the Policy compliance tasks topic in the Skybox Reference Guide.

4 Select the policy types that you want the task to analyze and, for each type, select the scope of the analysis.
   
   Note: Rule Policy compliance is not relevant for Network Assurance; the fields are ignored when the task is run.

5 In the **Advanced** tab, in the **Test Type** field, select **Network**.

6 (Optional) Define a schedule for the task in the **Schedule** tab.

7 (Optional) Add the task to a task sequence.

8 Click **OK**.

   For additional information about setting up and working with tasks, see Using tasks for automation (on page 120).

### Using tasks for automation

Scheduled tasks and task sequences can be used in Skybox to automate processes, including data updates, model maintenance, and reports.

This section explains how to work with task sequences and how to schedule tasks and task sequences. For information about using tasks and about each specific task, see the Tasks part of the Skybox Reference Guide.

   Note: Only **Admins** and **Users** can work with tasks. **Admins** can work with all tasks; **Users** can work with a limited range of tasks, including tasks that generate reports and CSV files, tasks that create tickets, and tasks that analyze data.

### TASK SEQUENCES

In a task sequence, each task in the sequence runs as soon as the 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, 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 specific tasks, see the Tasks part of the Skybox Reference Guide.

### Best practice for setting up task sequences

#### General best practice advice

The following is general best practice advice for setting up task sequences:

- Set up and schedule task sequences; *do not* schedule tasks individually (unless there is a very specific need to do so).
- If you have a set of tasks that need to be run only after another set of tasks finishes running, use sequence dependencies (one sequence running another
sequence). For example, run a set of analysis tasks only after the set of collection tasks has finished.

- In general, try to avoid separate schedules even on sequences. Some tasks, such as collection-type tasks, may take more or less time, and it is hard to predict when to schedule another sequence based on that.

**Best practice for order of operations**

The recommended order of operations is shown in the following table. You can create a task sequence for each type of operation and then create a master task sequence that includes them all.

<table>
<thead>
<tr>
<th>Order</th>
<th>Operation</th>
<th>Examples</th>
<th>Why</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Initialization</td>
<td>Model Backup</td>
<td>Backup everything before making any changes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Data Copy/Prep</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Update Dictionary</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Device Collection</td>
<td>Directory Import</td>
<td>Build/Update the network model</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Router/Firewall Online Collection</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Vulnerability and Asset Collection</td>
<td>Qualys</td>
<td>Assets are sitting in networks that are part of the network model</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Rapid7</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Nessus</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>SCCM</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Vulnerability Detector</td>
<td>Vulnerability Detector</td>
<td>After importing the new asset information, we want to deduce vulnerabilities and update the status of existing vulnerabilities</td>
</tr>
<tr>
<td>5</td>
<td>Audit Logs Collection</td>
<td>Change Tracking Events Collection</td>
<td>Needs to be done before Change Tracking Analysis</td>
</tr>
<tr>
<td>6</td>
<td>Model Validation &amp; Integrity</td>
<td>Model Validation</td>
<td>After the new information has been imported, and before running the analysis, since it may affect the results</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Model Integrity</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Calculation and Analysis</td>
<td>Change Tracking Analysis</td>
<td>All the information is in the model and up to date – need to analyze the results</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Security Metrics Analysis</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Policy Compliance</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Reporting</td>
<td>CSV Data Export</td>
<td>Analysis tasks produce new results that need to be reported</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PDF Report Generation</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>Housekeeping</td>
<td>Scripts for moving, cleaning up data</td>
<td>Clean up</td>
</tr>
<tr>
<td>10</td>
<td>Log Collection</td>
<td>LEA, Syslog</td>
<td>Can take a long time to run, especially during working hours</td>
</tr>
<tr>
<td>11</td>
<td>Rule Usage Reporting</td>
<td>CSV Data Export, PDF Report</td>
<td>There are results from log collection that need to be reported</td>
</tr>
</tbody>
</table>

**About log collection in the order of operations.**

Log collection may involve a large number of files. It is best to run log collection after all collection and analysis and reporting is complete.

Depending on the size and scope of log collection requirements, it may be necessary to set up a separate sequence for log collection on a schedule that does not conflict with normal collection. In this case, rule usage reporting should be part of the sequence for log collection and not part of

**Creating task sequences - NA**

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 and all subsequent tasks are not launched. For example, you can make the Analyze Firewall Policy Compliance task dependent on a task that imports data from multiple 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.

Note: Before you create a task sequence, define the tasks that are to run in the sequence.
For information about creating task sequences for triggered collection and analysis of firewalls, see the Creating triggered collection and analysis task sequences topic in the Skybox Firewall Assurance User Guide.

To create a task sequence

1. On the Operational Console toolbar, click
   ![New Task Sequence](NewTaskSequence.png).
2. Type a **Name** for the sequence; leave **Basic** selected as the type of the task sequence.
3. Click **Next**.
4. In the Tasks pane, click **Add**.
5. Select a task to add to the sequence and click **OK**.
   The task is added as the 1st task in the task sequence.
6. Add additional tasks to the task sequence:
   a. Click **Add**.
   b. Select a task to add to the sequence.
      A dependency is created so that this task runs after the previous task finishes with any of the specified exit codes.
      Note: A single task can only be used once per task sequence. However, you can use several different tasks of the same type.
   c. To change the triggering task, select a different task in the **Depends on Task** field.
   d. To change the exit codes (on page 123) of the triggering task, click the **Browse** button next to the **Depends on Exit Codes** field.
      If the triggering task ends with a different exit code, the dependent task is not triggered.

7. Click **Next**.

The Firewall Filters page 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 any tasks, 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).

8. If your task sequence includes any firewall collection or analysis tasks, you can modify the values.
9. Click **Next**.
10. **Schedule the task sequence** (see page 123) to run as often as necessary.
11. 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**.
Task exit codes

The following are the task exit codes for all Skybox tasks.

<table>
<thead>
<tr>
<th>Exit code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>The task completed successfully.</td>
</tr>
<tr>
<td>Success (No Update)</td>
<td>The task completed but no data was updated. (Used only for <strong>Dictionary Update</strong> tasks when no update was available.)</td>
</tr>
<tr>
<td>Warning</td>
<td>The task was partially successful. For example, a task to collect 5 firewalls was only able to collect 3 of them. You can get more information from the warning messages.</td>
</tr>
<tr>
<td>Error</td>
<td>The task failed. You can get more information from the error messages.</td>
</tr>
<tr>
<td>Fatal</td>
<td>The task failed with a fatal error. For example, the configuration files being collected are corrupt.</td>
</tr>
<tr>
<td>Time Out</td>
<td>The task did not finish because no data or response was received by the time the task reached its timeout.</td>
</tr>
<tr>
<td>Terminated</td>
<td>The user aborted or terminated the task.</td>
</tr>
</tbody>
</table>

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 most recent 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

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

SCHEDULING TASK SEQUENCES

You can define a task sequence (or a task) so that it runs at scheduled times. Although sequences are usually scheduled to run on the Live model, you can schedule them to run on any model.

Note: As mentioned in **Best practice for setting up task sequences** (on page 120), we recommend that you group tasks into sequences rather than run or schedule individual tasks.
To schedule a task sequence (or task)

1. Locate the task sequence in the Operational Console tree.
2. Right-click the task sequence and select Properties.
3. In the <Task name> Properties dialog box, click the Schedule tab.
4. For each schedule:
   a. Click Add.
   b. Select a time slice and fill in the corresponding fields.
   c. If the task sequence is to run a limited number of times, select End after and type the number of times that you want it to run.
   d. If necessary, in the Model field, change the model on which the task sequence runs.
   e. Click OK.
      The new schedule is added to the list of schedules for this task sequence.
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.

TASK GROUPS

You can group a set of tasks together so that you can run them as part of a task sequence (see page 120).

When you create a task group, Skybox creates a separate folder for the group, where you can view and edit the list of tasks in the group.
Chapter 7  Auditing the network on a continuous basis

Note: You can only run a whole task group as part of a task sequence. Otherwise, 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.

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 updated task for the failed firewall.

You can view 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 specific users for failed tasks. You can configure global settings and you can 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  Go to Tools > Options > Server Options > Task Settings > Task Alert Settings.
2  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:
   - **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 Network Assurance supports sending email notifications or running scripts when there are specific changes to a network. A *trigger* is a rule that defines the exact changes that cause these notifications and scripts.

If email notifications are sent, they include information about the changes.

**Network Access Compliance violation notifications**

A Network Access Compliance violation is triggered by a new Access Policy violation on a network. For example, if an access test for a firewall that was previously compliant with the Access Policy now becomes non-compliant, the owner of that network receives a notification. New violations might mean that a recent change to an access rule on the firewall is problematic.

Network Access Compliance violations trigger notifications or scripts when **Analysis – Policy Compliance** tasks are run and new violations (that meet the trigger criteria) are found.

**To create a trigger**

1 Select **Tools > Administrative Tools > Triggers**.
2 In the Skybox Admin window, right-click **Triggers** and select **New Trigger**.
3 In the New Trigger dialog box, select the **Network Access Compliance Violation Trigger Type** and fill in the fields as specified in the Skybox Reference Guide.
4 Click **OK**.
Chapter 8

Advanced modeling scenarios

This chapter explains how to model entities that need additional configuration.

In this chapter

Modeling VPNs ................................................................. 127
Modeling L2 networks ......................................................... 131
Mapping overlapping networks ............................................ 136
Virtual routers ................................................................... 139
Virtual firewalls .................................................................. 140
Virtualization and clouds ..................................................... 140
Clusters ............................................................................ 143
Merging data ..................................................................... 143

Modeling VPNs

A VPN is a private network that uses a public network to connect remote sites or users:

▶ Site to Site VPN: Connects multiple sites over a public network
▶ Remote Access VPN: Connects a single user to a LAN from a remote location

Skybox supports Site to Site VPNs and models them as a direct link between the participating gateways. This link is represented as a special tunnel network. VPN configuration details are represented by VPN units on each gateway. A VPN unit includes ‘protected’ networks and services, and an interface that connects the gateway to the secure VPN.

Creating VPNs

You can create VPNs in Skybox using online collection or offline file import tasks or manually, as described in this section.

AUTOMATED MODELING

When a VPN is created by online collection or offline file import, the configuration of the gateways provides all the information necessary to create the tunnel network and the VPN units, including the interfaces that connect the VPN units to the tunnel network.

Skybox supports online collection and offline file import of VPN information for:

▶ Check Point VPN-1 firewalls
You can model VPN information for other devices manually using Skybox Manager or using Skybox Integration XML (iXML) format. For information about iXML, see the Integration part of the Skybox Developer Guide.

Usually, VPNs are imported as a tunnel of type **VpnTunnel** with a **Vpn** network interface. For VPNs from specific vendors, the tunnel can be of type **Tunnel** with a **Tunnel** network interface.

Note: This issue is vendor-dependent; both configurations model the VPN equally well.

**MANUAL MODELING**

If you create a VPN manually, use the **VpnTunnel** tunnel type and the **Vpn** interface type.

There are 3 steps to creating a VPN:

1. Create the (VPN) tunnel network: Each endpoint of the tunnel is the IP address of a connected gateway (see **Creating VPN tunnels** (on page 128))

2. Create a VPN unit for each of the 2 gateways that are connected by the VPN tunnel: Connect the VPN interface of each VPN unit to the (VPN) tunnel network created in the previous step (see **Creating VPN units** (on page 129))

3. Create access rules on each gateway, which specify that data travels over the VPN tunnel: In the VPN pane of each access rule, specify the VPN unit to use (see **Creating access rules for the VPN** (on page 130))

When any part of the VPN is updated using a task, the manually created entities and connections are preserved.

**CREATING VPN TUNNELS**

If you model a VPN manually, start by creating the VPN tunnel. Afterwards, connect the gateways to the tunnel via their network interfaces. For information about VPN tunnels, see **Creating VPN units** (on page 129).

**To create a VPN tunnel**

1. In the **Locations & Networks** node of the Model tree, right-click the parent node for the tunnel. The parent node can be a specific location in the hierarchy or the **Locations & Networks** node.

2. Select **New > Network**.
   - For information about network properties, see the Networks topic in the Skybox Reference Guide.

3. In the New Network dialog box, fill in the fields of the tunnel network:
   - Ignore the values in the **IP Address** and **Mask** fields; these fields are not used for tunnel networks.
   - In the **Type** field, select **Secure VPN** or **Tunnel**. If you are not sure which to select, use **Secure VPN**.
Note: The tunnel type and the network interface type must match (either **Tunnel/Tunnel** or **Secure VPN/Secure VPN**).

- In the **Endpoint 1** and **Endpoint 2** fields, type the IP addresses of the connected gateways.

4 Click **OK**.

**CREATING VPN UNITS**

You create a VPN unit by:

- Defining the networks and services (in your organization’s network) that are protected by the VPN
- Selecting or creating the interface that connects the gateway of the VPN to the tunnel network

**To create a VPN unit**

1 Right-click a gateway of the tunnel and select **Manage VPNs**.
2 In the Manage Host VPNs dialog box, click **Add**.
3 In the New VPN dialog box, fill in the fields according to the following table. If there is no appropriate network interface for the VPN unit, create a new interface:
   a. Click **New**.
   b. In the New Network Interface dialog box, fill in the fields.
      Type of network interface:
      - For tunnels modeled using the **Secure VPN** type, select **Secure VPN** as the network interface **Type**.
      - For tunnels modeled using the **Tunnel** type, select **Tunnel** as the network interface **Type**.
      Note: This issue is vendor-specific. Both configurations model VPN tunnels equally well.

   Network:
   - In the **Network** field select the tunnel network to which the VPN unit is connected.
   - If the tunnel network was not created, leave the value of the **Network** field as **None** until you create the tunnel network and then set the value of this field to be the newly created tunnel network. For instructions, see **Connecting VPN gateways to the tunnel network** (on page 130).

   For information about network interface properties, see the Network interfaces topic in the Skybox Reference Guide.
   c. Click **OK**.

VPN unit properties are described in the following table.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the VPN unit</td>
</tr>
</tbody>
</table>
### Property Description

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Original Text</td>
<td>The name of the original object from which this unit was created.</td>
</tr>
<tr>
<td>My Domain</td>
<td>The networks protected by this gateway.</td>
</tr>
<tr>
<td>Peer Domain</td>
<td>The networks protected by the endpoint gateway. Only packets with networks that match these domains can pass thought the VPN tunnel. <strong>Note:</strong> This field is referred to as the encryption domain in Check Point terminology and the proxy in Cisco terminology.</td>
</tr>
<tr>
<td>Services</td>
<td>The protected services.</td>
</tr>
<tr>
<td>Network Interface</td>
<td>The network interface that connects the VPN unit to the tunnel network.</td>
</tr>
</tbody>
</table>

### CONNECTING VPN GATEWAYS TO THE TUNNEL NETWORK

If the VPN units were created before the tunnel network, connect each VPN gateway to the tunnel network.

*To connect a VPN gateway to the tunnel network*

1. In the Table pane, select the gateway.
2. In the Details pane, click the **Network Interfaces** tab.

   **Note:** If necessary, click ![button](image) to display the **Network Interfaces** tab.

3. Right-click the VPN interface and select **Properties**.
4. In the **Network** field of the <Network interface> Properties dialog box, select the tunnel network.
5. Click **OK**.

### CREATING ACCESS RULES FOR THE VPN

After you create the VPN, create an access rule on each gateway that permits data to pass through the VPN.

*To create an access rule*

1. Right-click the gateway and select **Access Rules**.
2. In the Access Control List Editor, click **New** to create an access rule.
3. Fill in the fields in the New Access Rule dialog box according to how the data behaves in the actual device (for a description of each field, see the Access rule properties topic in the Skybox Reference Guide).
   a. In the **VPN Usage** field, select:
      - **Specific** (to send the data via a specific VPN unit)
      - **Any** (to send the data over any VPN unit of this gateway)
   b. If you selected **Specific** in the **VPN Usage** field, click the **Browse** button next to the **Specific** field and select a VPN unit.
4 Click **OK**.

5 If necessary, move the new access rule to its correct location in relationship to the other rules using **Move Up**, **Move Down**, and **Move To**. If you created the rule in the wrong rule chain, click **Move To Other Chain** to move it to the correct chain.

6 Click **OK**.

---

### Modeling L2 networks

L3 routers, firewalls, load balancers, and proxies control traffic between different parts of your organization’s network and between your organization’s network and the outside world.

L2 gateways (bridges, switches, and transparent firewalls) add additional segmentation or protection to a network. In Skybox, L2 gateways are only modeled when they affect network accessibility by splitting networks into segments.

L2 gateways are modeled in Skybox in almost the same way as L3 gateways, except that an L2 gateway is marked as **Layer 2** and must have an L2 network interface. Access rules for L2 gateways are the same as those for regular (L3) gateways.

L2 network interfaces are similar to regular (L3) network interfaces, except:

- No IP address is required (the value 0.0.0.0 represents the IP address).
- Because an L2 interface has no IP address, it must be connected to a segment, rather than to a network.

After the L2 gateway device is created, you divide the network into segments and attach the network interface of the L2 device to the segments.
The following figures illustrate the difference between a regular (L3) network and an L2 network.

CREATING L2 DEVICES

You can create L2 devices using online collection tasks, offline file import tasks, or manually.

You create an L2 device manually in the same way that you create a regular (L3) device, except that you must:
Select **Layer 2**.

Create L2 network interfaces for the device. Each L2 network interface connects the device to a network segment. The L2 device might have L3 network interfaces.

If device configuration data is collected from a device or imported from a file, L2 network interfaces are created but they are not attached to the network because they do not have IP addresses; attach the interfaces to the network (and segment the network) manually.

**SEGMENTING NETWORKS**

In Skybox, a network segment is a portion of an IP network that is physically separated from other parts of the network by an L2 gateway device. You must create network segments manually: 1 segment for each part of the network that is behind a different network interface of the device. Afterwards, assign each asset in the network and each network interface of the L2 device to the appropriate segment.

Note: You can segment the network and assign the L2 network interfaces using Skybox Integration XML (iXML). For information about iXML, see the Integration part of the Skybox Developer Guide.

**CREATING NETWORK SEGMENTS**

Usually, an L2 device splits a network into 2 segments. However, it can split a network into multiple segments or split multiple networks. You must create each segment manually in the model. As you create the segments, you assign the appropriate assets in the network to the segment via their network interfaces.

*To create a network segment*

1. In the Model tree, right-click the network to be segmented and select **Manage segments**.
2. Click **Add**.

3. Type a **Name** for the segment.

4. You can define the IP address ranges for the segment and select a zone type.

5. The **Available** field lists the network interfaces of all assets in this network. For each asset that is in the segment, select the relevant network interface in the **Available** field and click ➤ to move it to the **Selected** field.

6. Click **OK**.

   In the Tree pane, the network contains the segments that you created and an **Unsegmented Assets** node.

   ![Segmentation Interface](image)

   - US
     - Los Angeles
       - gatewayWestA [192.170.1.32 / 28]
       - gatewayWestB [192.170.1.48 / 28]
       - nccWindowsVS [192.170.21.0 / 24]
       - nccUnixWS [192.170.22.0 / 24]
       - Trusted
       - Untrusted
       - Unsegmented Hosts
       - nccServers [192.170.23.0 / 24]
Assets that are not assigned to a segment in the segmented network are displayed when you select the Unsegmented Assets node.

Repeat this process for each segment that you need. Each asset now belongs to a network segment. If the L2 device has a management (L3) network interface, the L3 interface should not belong to either of the segments. The L2 device is listed in every segment, and it is also listed in the Unsegmented Assets node because of the L3 network interface.

Note: When you delete a network segment, all assets (according to their network interfaces) that are part of that segment become unsegmented assets in the network.

CONFIGURING THE L2 NETWORK INTERFACES

After the network is segmented, assign the L2 network interfaces of the L2 device to the appropriate segments.

To assign an L2 network interface to a network segment

1 Select the L2 device in the Table pane.
2 In the Network Interfaces tab of the Details pane, select the interface to be connected and open its Properties dialog box.
3 In the **Network** field, select the network segment to which the interface is attached.

4 Click **OK**.
   
   If this L2 device is updated using a task, the connection between the L2 interfaces and their network segments is preserved.

**Mapping overlapping networks**

Overlapping networks are networks that have identical or overlapping IP addresses and subnets. These networks are usually in different parts of your organization, separated by network devices.

These networks are discovered or collected as part of the topology. For Skybox to distinguish between 2 overlapping networks, define locations so that you can assign each such network to a unique location. As new data from these networks is imported into Skybox, the locations ensure that the networks are kept separate.
IMPORTING OVERLAPPING NETWORKS

Before importing network information:

› If there are no overlapping networks, you do not need to make any special preparations before importing new information.

› If you know that overlapping networks exist:
  1. Make sure that each overlapping network is in a unique location; you can add locations to the model before importing the data.
     – For information about defining unique locations in Skybox, see Defining unique locations for overlapping networks (on page 138).
  2. Create a definition file for an Import – Advanced task. This file must contain location hints for each overlapping network (see Adding location hints to the definition file (on page 138)).

› If overlapping networks are identified after the model is built, these networks are merged in the model and might include assets from both overlapping networks. Delete these networks manually from the model, create an input file with location hints, and import the data again.

MERGING OVERLAPPING NETWORKS

If a network is imported with a location hint, Skybox attempts to find an identical network under the same location as the specified location hint. Possible outcomes are listed in the following table.

<table>
<thead>
<tr>
<th>If...</th>
<th>Then...</th>
</tr>
</thead>
<tbody>
<tr>
<td>An identical network was found under the same location</td>
<td>The newly imported network is merged with the existing network in the base model</td>
</tr>
<tr>
<td>No identical network was found</td>
<td>A new network is created in the specified location</td>
</tr>
<tr>
<td>Identical networks were found Note: This can happen when the location hint is not clear enough. For example, if there are identical networks in the US/New York location and the US/Boston location, and the location hint is “[US]”.</td>
<td>A warning message is issued and the network is not created</td>
</tr>
</tbody>
</table>

If a network is imported without a location hint, the following outcomes are possible:

If a network is imported without a location hint, outcomes listed in the following table are possible.

<table>
<thead>
<tr>
<th>If...</th>
<th>Then...</th>
</tr>
</thead>
<tbody>
<tr>
<td>If there are no identical networks</td>
<td>The new network is created as usual</td>
</tr>
<tr>
<td>If there is 1 identical network in the model</td>
<td>The new network is merged into the base</td>
</tr>
</tbody>
</table>
If there are multiple identical networks under different locations

Then...
The merger cannot solve the conflict; a warning message is issued and the network is not created

If a network cannot be merged for any of the preceding reasons, no new network is created (and no existing network is changed).

Assets that are part of overlapping networks are handled in a similar manner. If there are identical assets under different locations, the merger cannot solve the conflict and the asset is not imported.

DEFINING UNIQUE LOCATIONS FOR OVERLAPPING NETWORKS

To work with overlapping networks in Skybox, you must define a unique location for each network within the model.

Note: Location names must be unique throughout the model even when there are no overlapping networks.

Overlapping networks cannot exist in 2 locations when 1 location is a direct descendant of the other in the Locations & Networks tree.

For example, in the hierarchy in the following figure:

- **Floor1** and **Floor2** might hold overlapping networks but **Floor1** and **Commonwealth** cannot, because **Floor1** is a direct descendant of **Commonwealth**.
- Overlapping networks can exist under **US** and **Europe** but not under **US** and **Boston**.

```
Locations & Networks
├── Europe
│   ├── Resellers
│   └── US
│       ├── Boston
│           ├── Commonwealth
│           │   ├── Building A
│           │   ├── Floor1
│           │   └── Floor2
│           └── Floor3
│       └── Building B
│           ├── Jim Smith Office
│           └── Joe Brown Office
└── Main Street
```

ADDING LOCATION HINTS TO THE DEFINITION FILE

To add overlapping networks to the model

1. Create a definition file for an Import – Advanced task.

   For information about creating this file, see the Definition file for advanced file import tasks topic in the Skybox Reference Guide.
2 Add location hints to the definition file.

Each line that imports an overlapping network must have the format: `<import format type> <source file | directory> [location hint]`

Note: The square brackets ([ and ]) are part of the format of the line; they do not mean that an element is optional.

For possible values for `<import format type>`, see the Data formats for file import tasks topic in the Skybox Reference Guide.

For example:

```
NMAP_XML c:\sample\result.xml [London\Bakers]
PIX_CONF c:\sample\file.cfg [Paris]
```

You can use "\" and "/" as delimiters in the location hint.

To preserve whitespace in location names, place the location inside double quotation marks. For example:

- PIX_CONF c:\sample\file.cfg [North America/New York]: The location is read as NorthAmerica >> NewYork
- PIX_CONF c:\sample\file.cfg ["North America/New York"]: The location is read as North America >> New York

3 Using an **Import – Advanced** task, import the overlapping networks into the model.

If the location does not exist in the model, it is created during the file import.

Note: For overlapping networks, the files to be imported using the **Import – Advanced** task must be on the Server computer. Location hints are not identified when you run the task on the Collector computer.

### Virtual routers

Virtual routing is a technology that enables multiple instances of a routing table on the same asset at the same time. Each network interface is associated with a single virtual router.

When data packets arrive through a specific interface, the asset uses the routing table associated with that interface to route the packets. Packets arriving from different interfaces can take different paths to the same destination. Because each router is independent, the same or overlapping IP addresses can be used without conflicting with each other.

In Skybox, each virtual router is modeled as a section in the asset’s routing table. Virtual routers are supported for a variety of devices including Juniper Networks Junos routers and firewalls, and Palo Alto Networks firewalls.
Virtual firewalls

Most vendors offer virtual firewalls, which can run multiple firewalls on a single physical device. Each virtual firewall is associated with (inherits) network interfaces from the physical device but has a separate ACL and routing table defined for it.

In Skybox, virtual firewalls are modeled as separate firewalls with separate configurations.

All virtual firewalls derived from the same physical device share a common prefix in their names so that you can easily identify them in the model (for example, if the system is named Alex, the virtual firewalls are named Alex:vsys1, Alex:vsys2, and so on). Skybox also creates an asset group with the name of the system and the virtual firewalls are part of this asset group.

Virtualization and clouds

Skybox supports virtual domains for modeling software-defined networking (SDN). Virtual domains can be modeled in Skybox and access analysis can be performed. The model tree (Virtual Domains folder) shows virtual domains and their security tags, as well as security groups. The relevant Access Policy rules of each security tag can be viewed on the security tag itself and each virtual asset shows its entire Access Policy as derived from its security tags.

The supported connectors are Amazon Web Services, VMware NSX, Microsoft Azure, and Cisco ACI.

- Data from Amazon Web Services data centers can be collected using Cloud & Virtualization – Amazon Web Services Collection tasks.
- Data from VMware NSX Manager servers can be collected using Cloud & Virtualization – NSX and vSphere Collection tasks.
- Data from Microsoft Azure servers can be collected using Cloud & Virtualization – Azure Collection tasks.
- Data from Cisco ACI servers can be collected using Cloud & Virtualization – Cisco ACI Collection tasks.

Additional information about these tasks is provided in the Cloud and virtualization tasks chapter in the Skybox Reference Guide.

The mappings between Skybox terminology and Azure, AWS, and Cisco ACI terminologies are listed in the following table.

<table>
<thead>
<tr>
<th>Skybox</th>
<th>Azure</th>
<th>AWS</th>
<th>Cisco ACI</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset</td>
<td>VM</td>
<td>EC2</td>
<td>VM</td>
</tr>
<tr>
<td>Virtual</td>
<td>VNET</td>
<td>VPC</td>
<td>Tenant</td>
</tr>
</tbody>
</table>
In NSX, Virtual Domains are named Tenants.

Security Tags are Access Policy templates used for assets. Security Tags are modeled as Tag asset groups that also have access rules.

Security Groups are collections of assets. Security Groups are modeled as Security Group asset groups.

Note: Virtual Domains, Security Tags, and Security Groups cannot be created or edited manually, but you can add comments to them and change their owners.

If you select a virtual domain in the tree, you can see its security tags and security groups, or its assets in the Table pane. If you select a security tag or security group, you can see its assets in the Table pane.
You can see the access rules of a security tag by right-clicking it and selecting **Access Rules**.

You can also see the access rules of each virtual asset. The access rules of a virtual asset are the access rules from each of its security tags.

The properties of a virtual asset include the properties of a regular (non-virtual) asset and the asset’s virtualization environment—the virtual domain, security tags, and security groups to which it belongs.

Note: Virtual assets cannot be created manually, but they can be edited and deleted. Their virtualization information, however, cannot be changed.
Clustering

Cisco HSRP clusters

Multiple Cisco routers can form a cluster and communicate using HSRP protocol. The redundancy works by declaring a virtual IP address that is always connected to a router in the cluster. Another router in the cluster takes over the virtual IP address if the 1st router fails. Skybox models these virtual IP addresses as virtual network interfaces with the naming convention of `standby_n` (starting at `standby_0`).

In Skybox, 2 routers belong to the same cluster if they have a virtual interface connected to the same network, with the same name and same IP address. These routers are supposed to have the same access rules for each shared virtual interface.

Check Point clusters

Skybox adds members of a Check Point cluster to a Cluster asset group, with the cluster name as the name of the asset group. The shared IP addresses in the cluster are modeled as virtual interfaces in each cluster member.

Other clusters

Skybox adds members of a NetScreen, Junos, Cisco ASA, Cisco FWSM, Palo Alto, or FortiGate cluster to a Cluster asset group, with the cluster name as the name of the asset group.

Merging data

All data that is imported, collected, discovered, or scanned into the model goes through a process named `merging`, which refines the data and merges the information into the current model. Only data that is added to the model manually does not go through this process.

When new data is retrieved for Skybox, it is collected into an update model. This data is normalized into the format in which it is stored in Skybox (see Normalizing the network information) and merged into the base model (usually the Live model) on a per-entity basis:

1. Identify the entity in the base model (see Identifying entities in the base model). If the entity is new (does not exist in the base model), add the entity to the base model and skip the next step.

2. Merge the entity data from the update model to the base model (see Merging entities).

You should understand when data will be merged and the criteria that Skybox uses for merging each type of entity, so that you know the new data that will be accepted into the model and the data that will be discarded. Usually, merging is a transparent process; sometimes, you must prepare the model to enable merging to proceed correctly.
NORMALIZING THE NETWORK INFORMATION

Skybox does the following to normalize the update model:

- Network status: If the network status is UNKNOWN, it is set to UP. If the interface type is unknown and it is a Loopback interface, its type is set to LOOPBACK; otherwise, the interface type is set to ETHERNET.
- Discovery method for assets, and for access and routing rules: If the discovery method is null, it is set to UNKNOWN.
- Scan time for assets and services: If the scan time of an asset or a service is null, it is set to the current time.
- Network interfaces for devices and assets:
  - Every interface is attached to the correct network
  - Access rules that are attached only to empty interfaces are deleted
  - Empty (0.0.0.0) interfaces are deleted
  - Assets that do not have any interface that can be primary are deleted
    Note: If an entity is deleted from the update model, Skybox does not use it in the merger, because it does not match the qualifying criteria.
  - If a network interface has no name, Skybox generates a name of the form “nif<n>”
- Routing rule gateways:
  - If a routing rule has a zero gateway (0.0.0.0) and other non-zero gateways, the zero gateway is deleted
  - If a routing rule does not have any gateways, a zero gateway is added
- Assets:
  - If an asset has no name, Skybox generates a name of the form “host<n>”
  - If an asset has duplicate services, the duplicates are deleted

After the data in the update model is normalized, Skybox performs the following resolutions:

- Patch identification: Each patch is assigned to a service product (using product banner matching)
- Asset type deduction: The type of each asset is deduced from the services running on the asset
- OS fingerprints translation: The operating system banner is matched to the appropriate service definition
- Product banner translation: Service banners are analyzed to find a match in the Skybox Vulnerability Dictionary
- Product catalog ID resolution: Product catalog IDs are resolved using the Skybox Vulnerability Dictionary
- Vulnerability occurrence matching:
  - Some vulnerability occurrences are discovered indirectly by scanners and then assigned incorrectly. For example, a scanner grabs information about
an asset’s services via SNMP and assigns the vulnerability occurrences found to SNMP; these vulnerability occurrences must be matched to the correct service.

- Some scanners do not report which services are vulnerable, rather they provide 2 separate lists—all vulnerability occurrences found on the asset and all services found on the asset. In this case, the link between services and vulnerability occurrences must be created.

IDENTIFYING ENTITIES IN THE BASE MODEL

Each type of entity has different criteria for identification. For example:

- Most types of networks are identified by IP address and netmask.
- Assets are identified by their network interfaces.

  When you import a new asset, the merger ascertains whether the asset exists in the model by looking for an asset with a network interface with the same IP address that is not of type Virtual, Loopback, Tunnel, or LoadBalancer.

- Services on the same asset are identified by their ports.

  If it is established that an entity in the update model is new (does not exist in the base model), it is added directly to the base model, without going through the final step (entity merge).

MERGING ENTITIES

If an entity in the update model exists in the base model, there are 2 ways to merge the data:

- The information in the 2 models is combined
- The information in the base model is replaced by the information in the update model

Although the methods for merging each entity type are different, the main criteria for the merge are:

- Reliability of source

  For example, imported gateway configurations are considered the most reliable source. Data retrieved from SNMP is considered more reliable than data retrieved by a network scan because it usually contains more detailed information about service and network configuration of the asset.

  If the source of the base model data is more reliable (more accurate and more complete) than the source of the update data, either no data is merged or only new information from the update model is merged.

Note: The properties in the discovery properties (Server & Collector) section of <Skybox_Home>\<component>\conf\sb_common.properties (where <component> is server or collector) define the order of source reliability for different entities.
Newer data is preferred to older data. Time is measured according to the **Scan Time** timestamp.

- **Completeness**
  
  Some data is better than none.

If the data in the update model for a specific entity is older, less reliable, or less complete than the data in the base model, the data from the update model is discarded and the entity in the base model is not changed.

**MERGING ASSETS**

Skybox uses the following network interface types to identify assets:

- NAT
- Ethernet
- WLAN
- TokenRing
- PPP
- Slip
- Other
- Serial
- Tunnel

Skybox does not use **Virtual**, **Loopback**, and **LoadBalancer** network interfaces for identification.

---

Note: When you import asset information, an asset that has different (dynamic) IP addresses in the 2 models is not merged. To ensure that all asset data is merged, use the **Merge assets by WINS name** field in the offline file import and online collection tasks. If you select this option, the merger looks for identical WINS names for merged assets and, if not found, falls back to comparing IP addresses.

When Skybox decides that an asset in the base model and an asset in the update model are the same asset, all elements of the asset are merged, including:

- Network interfaces
- Routing rules
- Access rules
- Services
- Vulnerability occurrences

Each element is merged separately, based on reliability, time, and completeness (see **Merging entities** (on page 145)).
**Network interfaces**

In general, interfaces are merged according to reliability and time. If the discovery method in the update model uses CONFIG or SNMP, which are considered the most reliable sources, the interfaces in the update model overwrite those in the base model. Otherwise, the new interfaces are merged with those in the base model.

Note: If you are working with routers, the default behavior of the merge is to disconnect manually connected network interfaces. To prevent this, ensure that the **Network** field of the network interface is **Locked** (🔒) before the routers are updated.

**Routing rules**

When routing rules are merged, the whole routing table is considered; individual routing rules are not merged separately. Routing tables are merged according to reliability and time.

- If the routing table in the update model is more reliable or newer, it overwrites the routing table in the base model.
- If the base asset does not have a routing table, the routing table of the asset in the update model is merged.

**Access rules**

When access rules are merged, only ACLs are considered; individual access rules are not merged separately. ACLs are merged according to reliability and time.

If the ACL in the update model asset is more reliable or newer, its access rules overwrite those in the base model.

**Services**

When the services of 2 assets are merged, the merger adds new services that do not appear in the base asset and merges the data of services that do exist in the base model. The vulnerability occurrences attached to the services are also merged.

**Vulnerability occurrences**

New vulnerability occurrences on the updated asset’s services are added to the base model. If a vulnerability occurrence already exists in the base model, the vulnerability occurrence data is merged.

**Merging assets manually**

In rare cases, Skybox cannot identify that a scanned asset is the same as an existing asset; Skybox creates a new asset in the model. This usually occurs if:

- An existing asset is renamed: If Skybox cannot verify that the new asset matches the existing asset with the previous name, it creates a new asset with the new name.
- An asset is scanned at different times by different interfaces: On the original scan, this asset was created in the model with 1 IP address. On a subsequent scan it was identified with a different IP address, and a separate asset is created. In fact, it is 1 asset with 2 IP addresses.
If an existing asset was merged incorrectly, you can merge it manually.

**To merge 2 assets manually**

1. Display both assets in the workspace. For example, if both assets are firewalls, use the **All Network Devices > Firewalls** node.
2. Select both assets, right-click, and select **Merge to Single Asset**.
   The asset with the older modification date is selected as primary, and the secondary asset is merged with it in the standard way (see page 146).

**Note:** When assets are merged manually, existing Rule Usage Analysis information is not merged; the Rule Usage information from the asset that was imported into Skybox first is retained.

**MERGING NETWORKS**

Regular and link networks are identified by IP address and netmask.

Some types of networks have slightly different rules for identification because a single IP address and netmask cannot identify them:

- **Tunnel** networks and **Secure VPNs** are identified by the IP addresses of their endpoints.
  - For information about tunnel properties, see the Networks topic in the Skybox Reference Guide.

- **Connecting Clouds** are identified by name.

- **Perimeter Clouds** are identified by IP address and netmask. If necessary, the cloud name is also used.

The following rules are applied when merging networks:

- New networks are added directly to the base model.
- If the network in the base model contains the updated network, the network is not added.
- Network segments are merged in the context of their networks. Network segments are identified by their network and their name.

**Note:** When merging networks, the scan time and the discovery method are ignored.

Skybox uses a different method to handle networks that have identical or overlapping addresses or netmasks, so that the networks are not accidentally merged. For information about how overlapping networks are merged, see **Merging overlapping networks** (on page 137).

**Merging link networks when each part is in a separate location**

A link network is a network whose only assets are gateways (network devices) that connect networks. If a link network consists of gateways that are in 2 different locations and were imported with different location hints, the merger assigns each part of the link network to its own location as a separate (but incomplete) network and does not know how to connect them. In effect, overlapping networks are created instead of a single network.

Manual action is required when merging link networks.
To merge a link network

1. Manually delete all duplicate overlapping link networks.
2. Move the remaining network to the parent location.
   If the network has no parent location, move it to the root location.
3. Run the import again.