AlgoSec Firewall Analyzer

Software Version: A30.10

User Guide

View our most recent updates in our online ASMS Tech Docs.

Document Release Date: 29 March, 2020 | **Software Release Date**: April 2020

Legal Notices

AlgoSec, FireFlow, AppViz and AppChange are registered trademarks of AlgoSec Systems Ltd. and/or its affiliates in the U.S. and certain other countries.

Check Point, the Check Point logo, ClusterXL, FireWall-1, FireWall-1 GX, FireWall-1 SecureServer, INSPECT, INSPECT XL, OPSEC, Provider-1, Safe@Home, Safe@Office, SecureClient, SecureKnowledge, SecurePlatform, SecuRemote, SecureXL Turbocard, SecureServer, SecureUpdate, SecureXL, SiteManager-1, SmartCenter, SmartCenter Pro, Smarter Security, SmartDashboard, SmartDefense, SmartLSM, SmartMap, SmartUpdate, SmartView, SmartView Monitor, SmartView Reporter, SmartView Status, SmartViewTracker, UserAuthority, VPN-1, VPN-1 Edge, VPN-1 Pro, VPN-1 SecureClient, VPN-1 SecuRemote, VPN-1 SecureServer, VPN-1 VSX, VPN-1 XL, are trademarks or registered trademarks of Check Point Software Technologies Ltd. or its affiliates.

Cisco, the Cisco Logo, Cisco IOS, IOS, PIX, and ACI are trademarks or registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

Juniper Networks, the Juniper Networks logo, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. JUNOS and JUNOSe are trademarks of Juniper Networks, Inc.

All other product names mentioned herein are trademarks or registered trademarks of their respective owners.

Specifications subject to change without notice.

Proprietary & Confidential Information

This document contains proprietary information. Neither this document nor said proprietary information shall be published, reproduced, copied, disclosed, or used for any purpose other than the review and consideration of this material without written approval from AlgoSec, 65 Challenger Rd., Suite 310, Ridgefield Park, NJ 07660 USA.

The software contains proprietary information of AlgoSec; it is provided under a license agreement containing restrictions on use and disclosure and is also protected by copyright law.

Due to continued product development this information may change without notice. The information and intellectual property contained herein is confidential between AlgoSec and the client and remains the exclusive property of AlgoSec If you find any problems in the documentation, please report them to us in writing. AlgoSec does not warrant that this document is error-free.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise without the prior written permission of AlgoSec Systems Ltd.

Contents

Welcome to AlgoSec Firewall Analyzer

AlgoSec Firewall Analyzer (AFA) is a component of the AlgoSecFirewall Analyzer, and is a comprehensive device analysis solution that builds an end-to-end model of your network's security posture and Layer 3 connectivity.

AFA's network model and its graphical map enable you to automatically detect security holes in your device policies, helping you manage your network proactively and efficiently.

Advanced management and troubleshooting

AFA provides operations and security teams with the ability to run interactive traffic simulation queries, to diagnose whether the device is blocking operational traffic.

In situations where a new exploit uses ports that could be blocked by the devices, AFA lets you run a traffic simulation query on all your devices to identify whether you are exposed, and which policies should be tightened up.

AFA reports are very intuitive and user-friendly, allowing you to quickly locate and resolve critical problems with three mouse clicks. Although AFA reports are easy to understand, they comprise a profound analysis of five layers of information, with more than 1500 linked files. The files making up the average AFA report, total about 75 MB* in size.

The following are traffic types analyzed by AFA:

- Every external IP address
- Every internal IP address (private or public, including NAT)
- Every protocol
- All source and destination port numbers and applications
- Both incoming and outgoing traffic

Each report is the result of AFA analysis of more than 1030 possible intrusions.

For more details, see AFA reports.

Risk management

Analyzing complex device policies manually is time consuming and requires an understanding of all the possible options and combinations. As a result, many risks are not detected and impose a threat to the organization's security.

The AFA Risk Management module automatically analyzes every type of packet that a device may encounter and performs a comprehensive analysis - not just a spot check. Therefore, customers have the ability to view all the risks and the specific rules that cause them, across all their devices.

For details, see Customize risk detection.

Change management

Today's constant demand for application and infrastructure changes poses a significant risk of compromising security in the process, and exposes organizations to new risks they might not even know about. That's why an ad-hoc approach to change management is not recommended.

AFA provides a comprehensive solution that helps report all the changes made to your device policies, and analyzes their impact, so that you can review and verify that they are performed correctly. In addition, a complete change history is logged. With AFA, the change process becomes more efficient, safer and easier to control.

For more details, see Manage real-time monitoring and Managing Analyses.

Policy optimization

Devices work more efficiently and are easier to manage when the policies are uncluttered and free of unused rules and objects. AFA enables customers to optimize policies easily and safely, by providing information on the following:

- Unused Rules: rules that are not used according to actual traffic logs
- Covered Rules: rules that are covered by previous rules (and will never be used)
- Disabled rules
- Time-inactive rules

- Rules without logging and without comments
- Unattached, unused and unrouted objects

AFA also includes the Intelligent Policy Tuner, which identifies rules that are too wide and permissive, and rules which contain sparsely used objects, thereby enabling you to fine tune your policy.

For details, see View policy data.

Regulatory compliance and auditing process

AFA helps you comply with standards and regulatory requirements such as:

- Sarbanes-Oxley
- Basel II Capital Accord
- HIPAA
- BS 7799 / ISO 17799
- NIST 800-41
- FISMA
- IAVA
- Payment Card Industry Data Security Standard (PCI DSS)
- Cyber Security Standards (CIP)

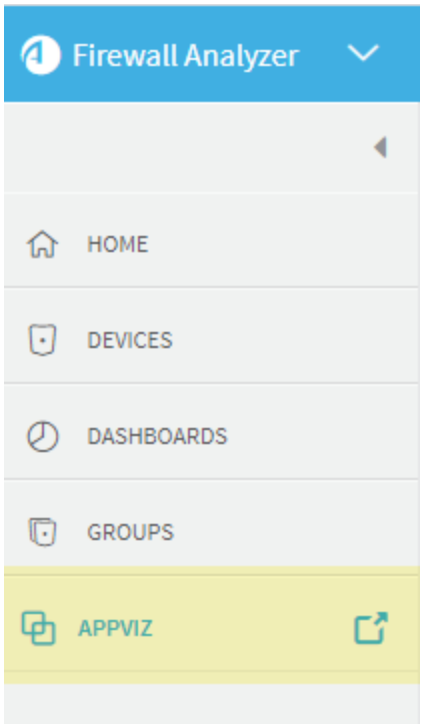
Additionally, AFA enables you to incorporate auditing into your work process. Simply define the schedule for analysis. AFA will automatically perform the analysis according to your defined triggers and e-mail the results to the relevant people upon completion.

For details, see Run traffic simulation queries.

Business application visibility

AFA also enables you to manage your security network policies from the perspective of your business applications, using the additional AppViz plugin.

AppViz is available from the bottom left menu in AFA, and opens in a separate tab.



Logins and other basics

This topic describes the very basics of working with ASMS, such as logging in and out and supported browsers.

Supported browsers

View ASMS in one the following web browsers, at screen resolution of **1920x1080** or above.

- **Mozilla Firefox**
- **Google Chrome**
- **Microsoft Edge**
- **Internet Explorer 11** and higher. Internet Explorer 8.0 is supported for FireFlow requestors only.

Log in to ASMS

Log in to ASMS from any desktop computer using the credentials provided by an AFA administrator.

Do the following:

1. In your browser, navigate to **https://<algosec_server>** where **<algosec_server>** is the ASMS server IP address or DNS name.

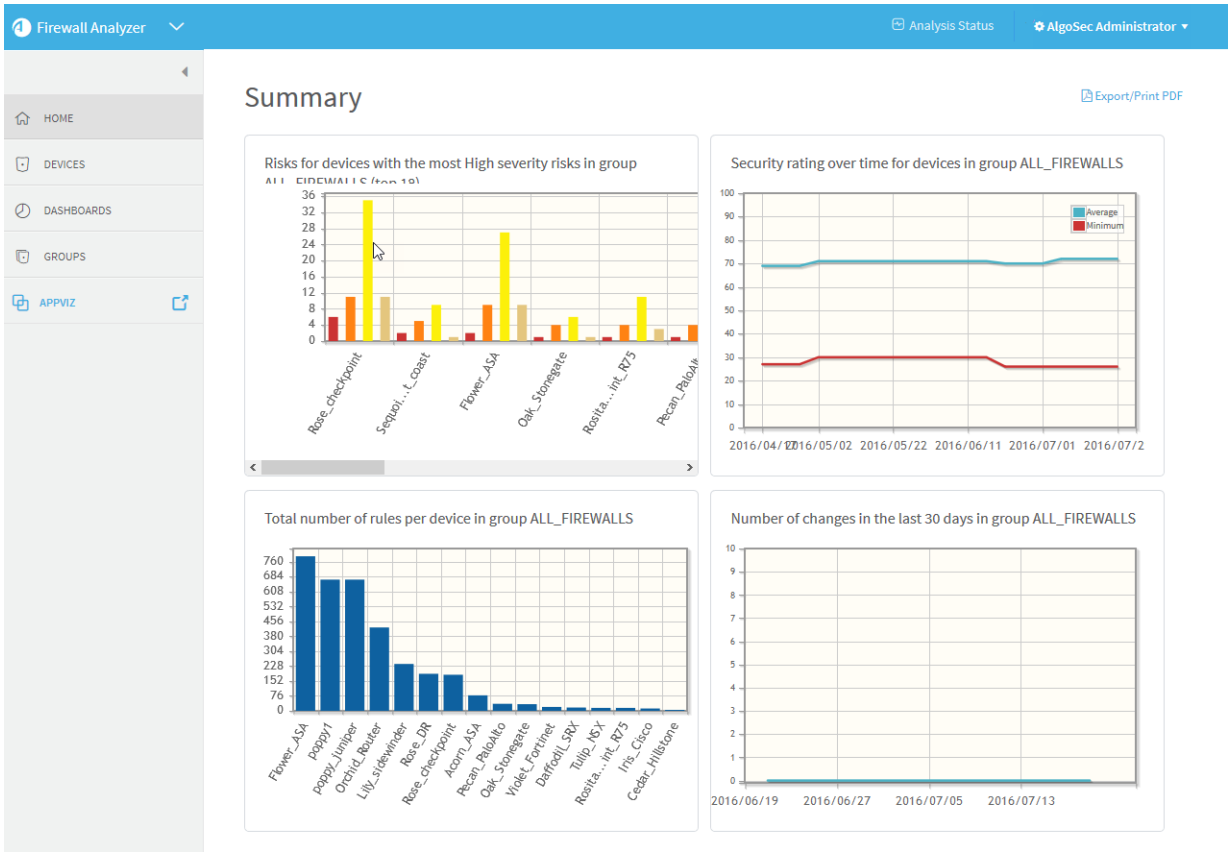
   If a warning message about the web server's certificate appears, click **Accept** or **OK**. For more details, contact your network administrator.

   The **Security Management Suite** login page appears.

2. In the **Username** and **Password** fields, enter your username and password, and click **Login**.

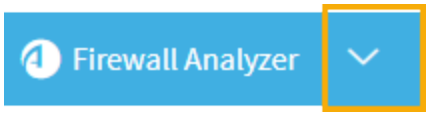
You are logged in, and ASMS displays AFA by default.

For example:

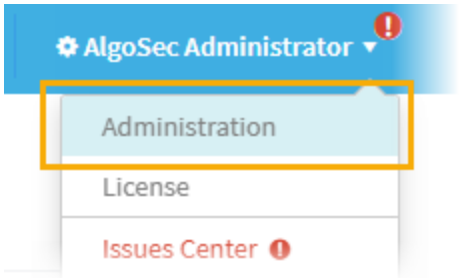


Switch ASMS products

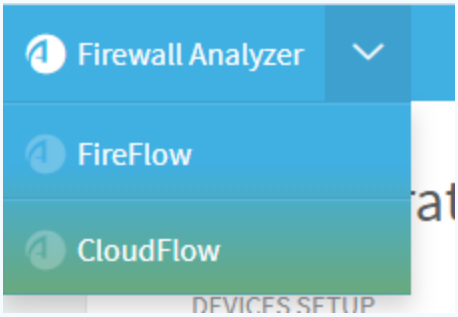
If you are a user in multiple ASMS products, such as AFA, FireFlow, and AppViz, switch between products using the dropdown at the top-left, above the main menu.



If you are an administrator for any of these products, the relevant administration menu is available from your user dropdown at the top-right:



Note: CloudFlow is now accessible from inside ASMS. Click the dropdown at the top-left and select **CloudFlow**.



For more details, see our CloudFlow Help Center.

Adjust your screen space

To adjust the screen space available for your main workspace, hide, display, or change the size of the main menu on the left.

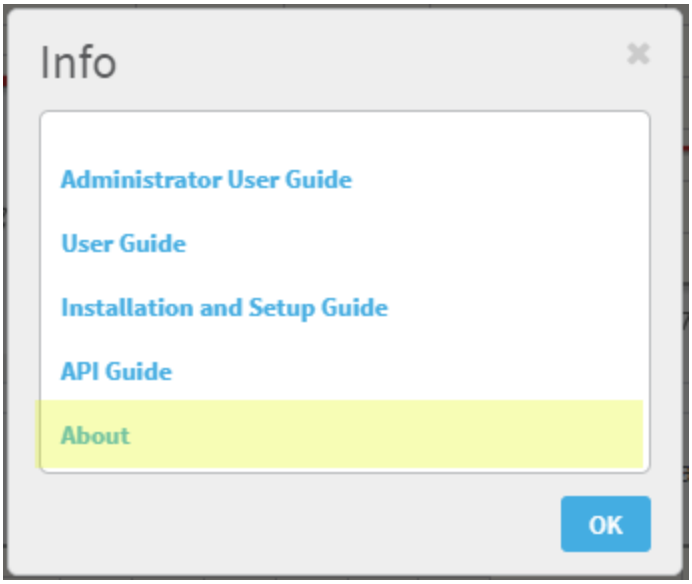
- **To adjust the size of the main menu**, hover between the menu and the workspace and drag the border left or right.
- **To collapse the menu entirely**, click at the top. When collapsed, click to expand it again.

View ASMS product details

This procedure describes how you can identify your AFA, FireFlow, or AppViz installation version and build number.

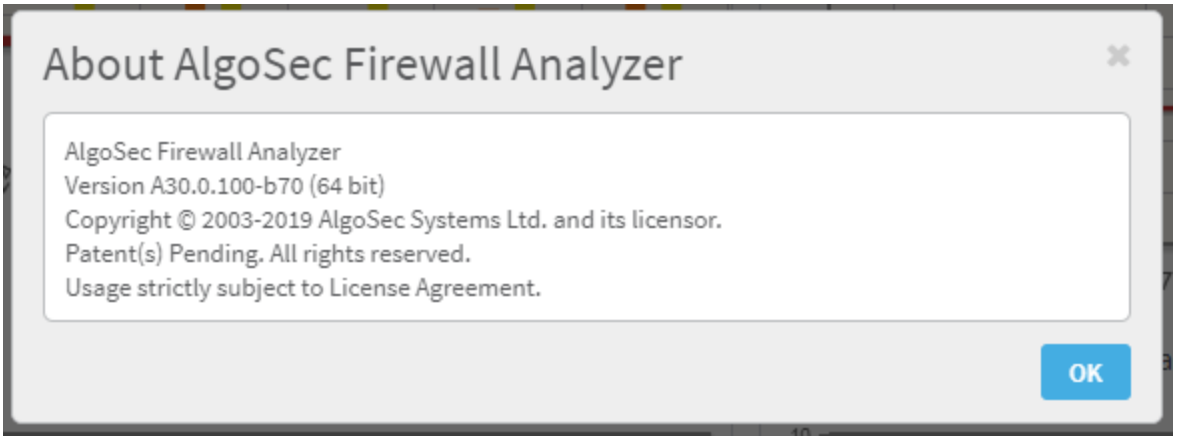
Do the following:

1. In the toolbar, click your username and then select **About** or **Info**.
2. For example, if you're in AFA, in the **Info** dialog, click **About**.



The **About** dialog appears, showing details about the product you have installed.

For example:



Note: If you are running the FIPS 140-2 compliant version of AFA, this information is indicated in the window.

Log out of ASMS

Log out of ASMS by clicking your username at the top right, and selecting **Logout**.

You are logged out of all ASMS products available to you.

Note: If Single Sign On is configured, you must browse to the **Logout** page hosted on your IdP to log out.

For more details, see the *AlgoSec Firewall Analyzer Administrator Guide*.

AFA components

This topic describes the AFA components, including the baseline **Operations and Optimization** component, and additional options for **Risk and Compliance**,and **ActiveChange** for direct change implementations.

AFA Operations and Optimization module

AFA operations and optimization are the baseline of ASMS, supporting device administrators while they perform daily operations and change management activities, as well as providing detailed change history reports for all device configurations.

AFA also enables significant device performance improvements with a rich set of reports and recommendations that help improve device configuration efficiency, such as the **Intelligent Rule Re-Ordering** algorithm.

For more details, see:

- Device analysis and reports for change tracking
- Traffic and routing queries
- Basic compliance
- Rule cleanup and audit
- User notifications

Device analysis and reports for change tracking

Visual display of the device policy, including topology, traffic, rules and objects, including an analysis of the routing table and provides a connectivity diagram changes from previous reports on the same device.

- **Create a report on a group of devices** with either pre-defined or ad-hoc device definitions.
- **Analyze several devices together**, taking into account their relative hierarchy in the network.
- **Schedule an analysis per device or group of devices**, based on pre-defined intervals (daily, weekly, monthly, etc.) and issue a report.
- **Compare any two reports** – either the same device or different devices or different device vendors. Track the changes in a device policy between reports of any two dates. Show the changes in traffic, rules, services, host groups, topology and objects

Traffic and routing queries

Run a traffic simulation query on a specific device or a group of devices to determine which rules control traffic between specific sources and destinations. This enables help desk teams to easily troubleshoot and prevent disruptions. It also provides for seamless server IP migration and security checking.

Routing queries allow you to check the end to end routing between two IP addresses on the map. They are different from the traffic analysis query because they do not take into account any security rules or NAT rules that may block or alter the routing path.

Basic compliance

By exploring the policy and change history an auditor receives the required information to produce a report that complies with corporate and regulatory standards such as the Sarbanes-Oxley Act, Basel II Capital Accord, HIPAA, BS 7799/ISO 17799, FISMA, Payment Card Security Standard (PCI DSS) and Cyber Security Standards (CIP).

Rule cleanup and audit

Identify unused, covered, timed out and disabled rules that are candidates for removal.

- **List rules that may not conform to company security policies**, including rules without comments, rules without logs and rules with comments that do not include a ticket number.
- **Show unused rules**, the most used and the least used rules.
- **Refine your device policy** using AFA's Intelligent Policy Tuner. Identify rules that are too wide and permissive, and rules which contain rarely used and unused objects.
- **Reorder your rules intelligently.**AFA recommends new positions for the rules to increase the device performance. The recommended order retains the policy logic. Typically, by repositioning only a few of the most used rules a significant improvement in performance is seen.
- **List unused, unattached and empty objects** that are candidates for removal.

User notifications

Continuously poll device policy changes and send e-mail alerts when a change is detected

Send e-mails to pre-assigned users following a device analysis with the summary of the analysis and the changes from previous reports.

AFA Risk and Compliance

The optional AFA Risk and Compliance Module adds risk management and compliance verification abilities to AFA Operations and Optimization. Built on AlgoSec's comprehensive knowledge base of industry best practices for device configurations, it allows users to quickly assess the security posture of their device configurations and ensure that all devices meet their specific security controls. It also includes automatically completed compliance reports.

Highlights include:

- **Deep risk analysis:** Identifies every packet the device may encounter. Automatically maps topology and identifies the most serious threats based on industry best practices, prioritizes subsequent risks and offers guidance on what and how to re-mediate.
- **Automatic assessment and compliance reports:** Generates automatically populated per device compliance reports to assure continued adherence to external regulatory standards including SOX, PCI-DSS, ISO 27001, Basel-II, and J-SOX, supplying the end-user or auditor with turnkey reports.
- **Continuous security audit:** Provides a complete audit trail and replaces error prone manual tasks, to ensure configuration is aligned with security policy.
- **Customize risk assessment:** Add risk profiles, based on internal corporate standards and easily customize out-of-the-box risk profiles, with the AlgoSec wizard-driven Risk Profile Editor.
- **E-mail notifications:** Send e-mails to pre-assigned users, following a device risk analysis with the summary of the analysis and the changes to the security posture relative to previous reports.
- **VPN analysis:** Add risks associated with VPN rules and VPN objects to the Change History page and to e-mail notifications.

AFA ActiveChange

The optional ActiveChange license adds the ability to implement AFA recommendations directly from the AFA system for Check Point devices accessed via OPSEC.

> **Note:** When FireFlow is being used, ActiveChange is used from FireFlow and supports many other device brands.

Highlights include:

- **Ability to disable unused, covered, and redundant special case rules**: Rules belonging to any of these three categories can be automatically disabled.
- **Policy backup:** The policy is backed up before changes are made, enabling one to easily revert to the pre-change policy.
- **Full audit trail:** Comments are added to every disabled rule to indicate which user made the change and when. These comments are visible in the Check Point Smart Dashboard.

Navigate around AFA

The main AFA interface includes a main menu on the left, a large workspace in the middle, and a toolbar at the top right.

AFA's main menu

Main menu items include:

	**HOME**. View the default dashboard.
	**DEVICES**. View all devices defined in AFA. Generate, view, compare, and delete device reports, query device policies, customize device topology and trusted traffic, locate objects in devices, and monitor device policies for changes.
	**DASHBOARDS**. View risk summaries, compliance, optimizations, and changes across all devices, and create custom dashbaords.
	**GROUPS**. View device groups defined in AFA. Generate, view, compare, and delete group reports and locate objects in groups.
	**MATRICES**.View matrices defined in AFA. Generate, view, compare, and delete matrix reports and locate objects in matrices.

Tip: Adjust the display by dragging the main menu. For details, see Adjust your screen space.

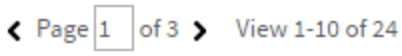
Toolbar

Click your username at the top-right to display system information, view documentation, and log out. Administrators can also access the **Administration** area and view license information.

Click **Analysis Status** to view the status of the most recent AFA analysis run.

AFA grids and tables

Across AFA, grids and tables have various sorting, paging, and filtering options.

Sort tables by columns	Tables columns that can be used to sort have arrows in their headings. For example:  Click a column heading to sort the table. To reverse the sorting order, click the column again. A table already sorted by a specific column displays only one arrow in its heading. For example:  .
Page across tables	When a table contains multiple pages, navigate between them using the controls below the table. For example:  Click an arrow button to move forward or back, or enter a page number in the page box.
Filter table content	Tables that can be filtered have an extra row just below the header. Enter data in the box to filter the table by that column data.  When filtering by multiple columns, the **AND** logic is used between filter texts. **Note:** Filtering tables with many rows may take some time. Administrators can disable filtering for tables over a specific size.

Export AFA screens to PDF

This topic describes how to export various AFA screens, such as dashboards and report pages, to PDF, and also lists recommendations for Print dialog settings per browser type.

Export AFA data to PDF files

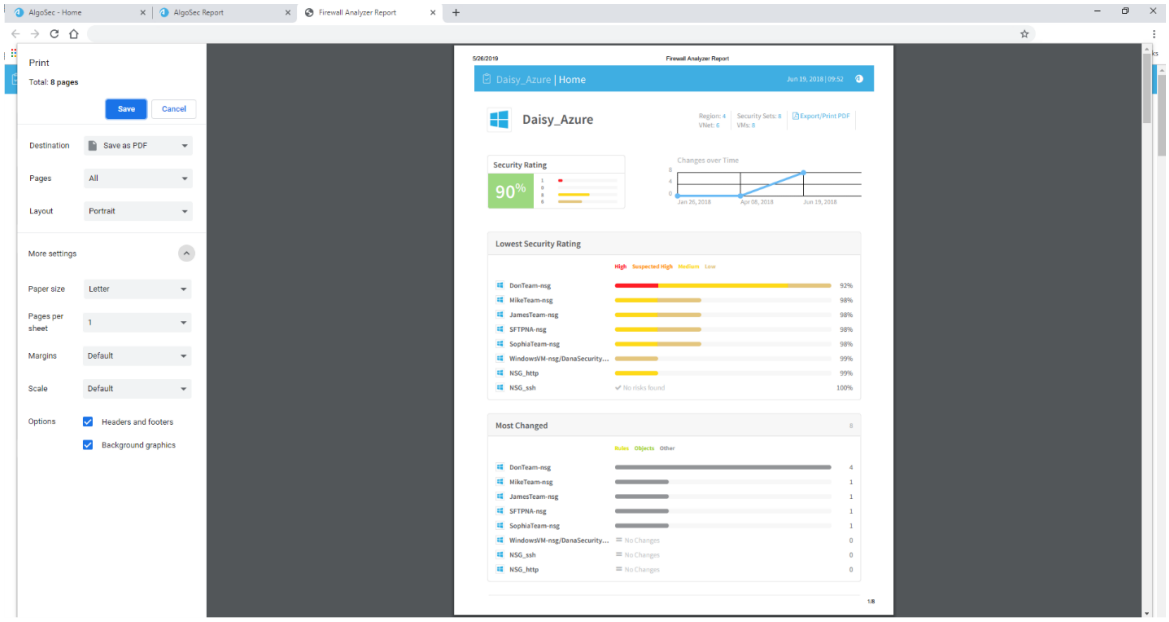
Do the following:

1. Click the **Export/Print PDF** or **Export** link shown in the upper-right corner of the screen.

   One of the following occurs:

Dashboards	On a dashboard page, a PDF of the dashboard is created. Your browser opens a **Print** dialog to print the new PDF.
Reports	On a report page, your browser will either open a **Print** dialog to export the report page currently in view to a PDF, or an **Export item** dialog appears. If the **Export item** dialog appears, select the report pages you want to export to open the browser's **Print** dialog.

   Depending on your browser and its settings, a preview version may open in a separate tab. For example:



2. In the browser **Print** dialog, select to save the file as PDF. Additionally, use the print preview to verify that all other print settings are set to show all colors and graphics, and to ensure that no content is cut off.

   Tip: The process and recommended settings may differ depending on the browser you are using. We recommend using a recent version of Google Chrome for optimal results.

   Use the following recommendations to ensure that your PDF is exported correctly:

   - General Print dialog recommendations
   - Chrome-specific recommendations
   - Firefox-specific recommendations
   - Microsoft Edge-specific recommendations
   - Microsoft Internet Explorer-specific recommendations

3. When you are finished with any adjustments required and are satisfied with your preview, click **Save** to save your PDF.

   In the **Save** dialog, enter a meaningful name for your PDF, and the location you want to save the file.

Note: When the Print Preview dialog is open in one browser tab, ASMS cannot function in a different tab of that browser window.

General Print dialog recommendations

Select the following options, regardless of your browser:

Layout/Orientation	Change the layout to **Landscape**.
Paper Size	Select **A4** or **Letter**.

Scale	Change the **Scale** value as needed so content is shown correctly and nothing is cut off. For example, the traffic simulation query map may not display correctly by default. Adjust your **Scale** settings to fix this.
Background Graphics	Select the **Background Graphics** check box to display the report in full color. Affected elements may be the status detail bars and table cell borders.
Margins	Adjust the margin values as needed so that graphs and tables are shown correctly. For example, if you are exporting traffic simulation query results, adjust the **Margins** until the report displays your map correctly in the print preview.
Header and Footer	Select the **Header and Footer** check box to include optional data in the report.

Chrome-specific recommendations

In the Chrome **Print** dialog, set your **Destination** to **Save as PDF**.

Expand the **More settings** link to adjust additional settings.

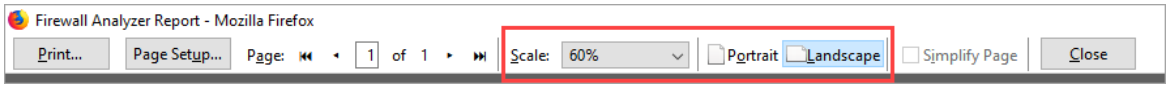
Firefox-specific recommendations

In the Firefox **Print** dialog, set your **Name** to **Microsoft Print to PDF**.

Open the Print Preview by selecting the Firefox menu ☰ button, and then selecting **Print**.

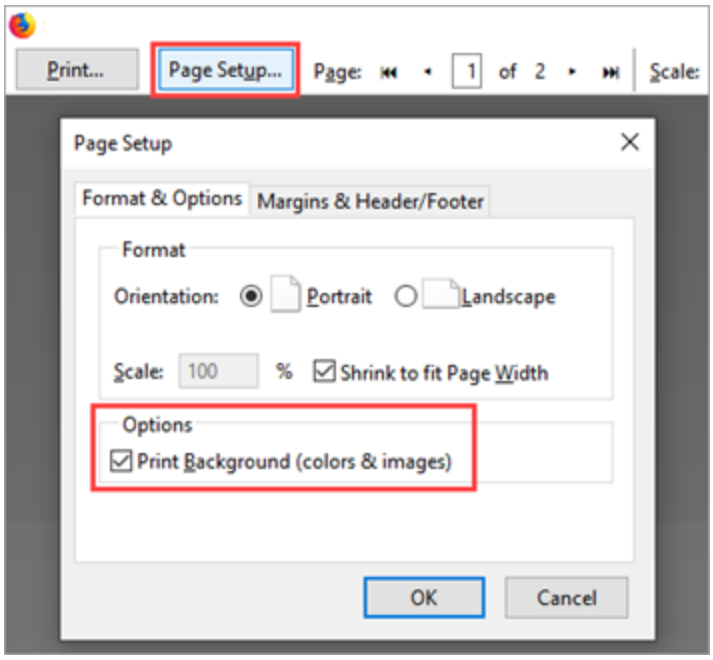
In the Print Preview, update the following as needed:

- Change the **Scale** and select **Landscape**:



- Click **Page Setup** at the top left, and select **Print Background (colors & images)**.

For example:



Firefox troubleshooting

- **Cut off reports:**

  If the print preview shows that the HOME page in the exported report is cut off at the end of the page, especially when printing multiple sections of the report, export one page of the report at a time.

  Do one the following:

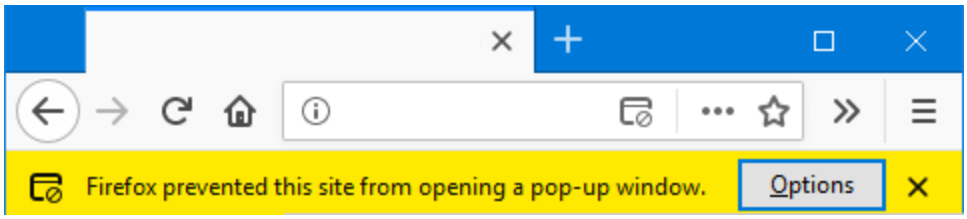
  - In the **Export item** dialog select only one checkbox for each report.
  - Export to PDF directly from a specific page in the report.

  For more details, see the relevant Firefox bug at bugs.launchpad.net.

  On all pages in the report, long frames may be cut off when exporting from FireFox. In such cases, use the scaling options to squeeze more content into the frame, or use a different browser. For more details, see https://bugzilla.mozilla.org/.

- **Print preview window does not open**

If the print preview does not appear, you may need to allow popups from your AFA machine. Click **Options** in the yellow bar at the top of your browser to allow popups for AFA.



Microsoft Edge-specific recommendations

In the Edge **Print** dialog, set your **Printer** to **Microsoft Print to PDF**.

Click **More settings** to adjust additional settings.

Edge troubleshooting

HOME page data cut off	If the print preview shows that the HOME page in the exported report is cut off at the end of the page, especially when printing multiple sections of the report, export one page of the report at a time. Do one the following: • In the **Export item** dialog select only one checkbox for each report. • Export to PDF directly from a specific page in the report.
Certificate requirements	In Edge, AFA does not support exporting the **Policy** tab of the report to PDF on systems that do not have a valid security certificate. Doing this simply shows a Preparing for Export message, without continuing. In such cases, we recommend using a different browser.
Background colors	Microsoft Edge does not support background colors. Therefore, PDFs exported from Edge are in black and white only, and tables may appear without cell borders. For more details, see answers.microsoft.com.

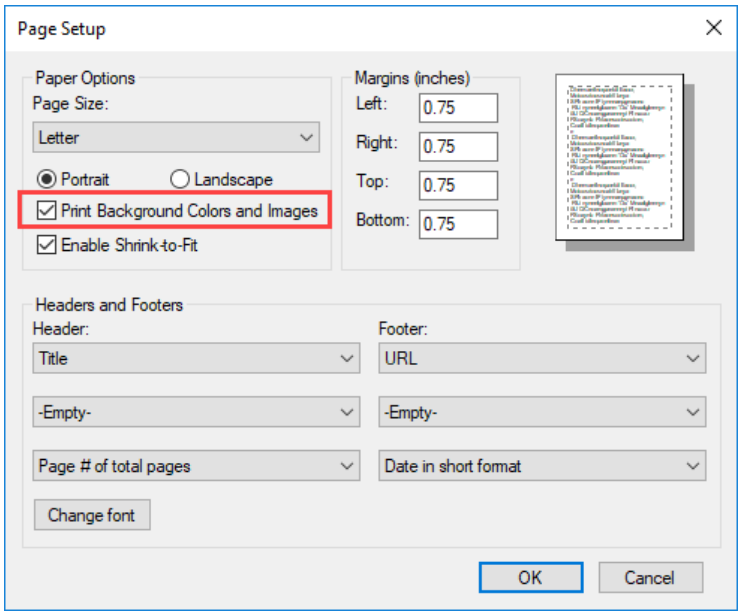
Microsoft Internet Explorer-specific recommendations

In the Internet Explorer **Print** dialog, select **General** > **Select printer**, and set your **Printer** to **Microsoft Print to PDF**.

Click **Preferences** to open a dialog and adjust the following settings:

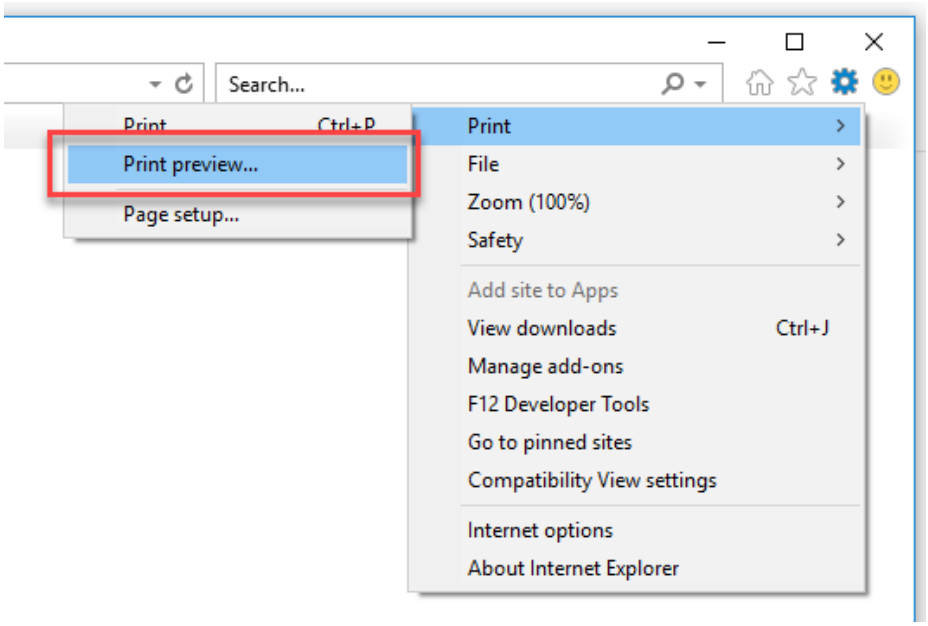
- In the **Layout** tab, select the **Landscape** orientation.
- In the **Paper/Quality** tab, select **Color**.
- Click **Advanced** to open another dialog and adjust additional settings.

To set the **Background graphics** option, select **Settings > Print > Page Setup** window, and select the **Print Background Colors and Images** check box. For example:



If you do not see the Print Preview dialog by default, in the Internet Explorer settings, select **Print** > **Print preview**.

For example:



Quickstart with AFA

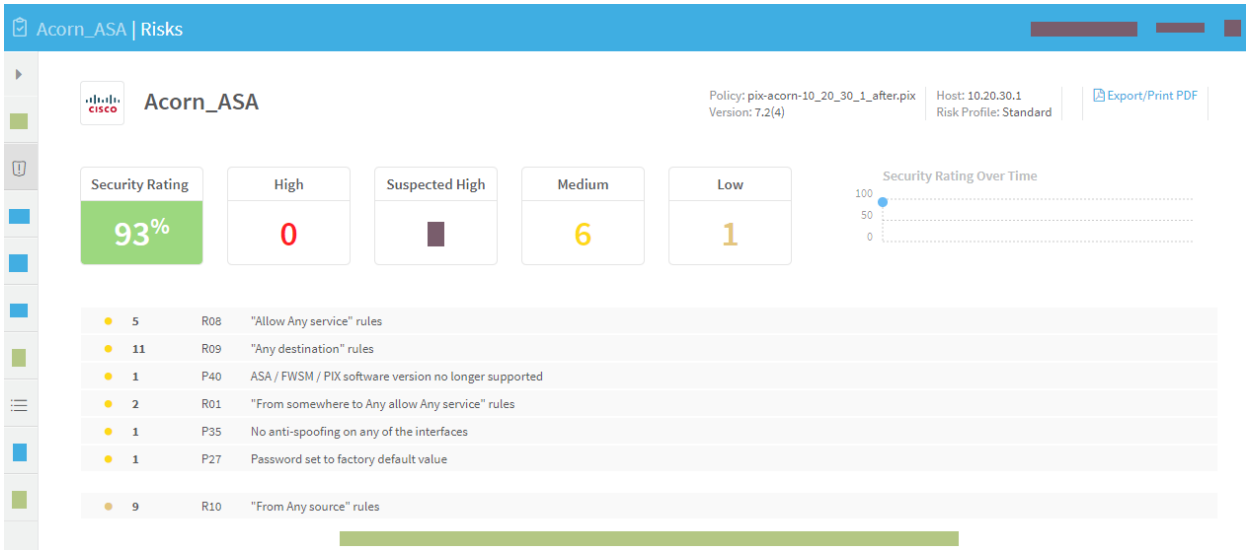
This topic describes how you can quickly get up and running with AFA reports and queries, once an AFA administrator has added devices to your ASMS environment and analysis is running.

View risks and risky rules

The AFA report **RISKS** and **RISKY RULES** pages list security holes in the device. Use the detailed information on these pages to tighten the device policy and improve your organization's security.

For details, see RISKS page and RISKY RULES page.

For example:

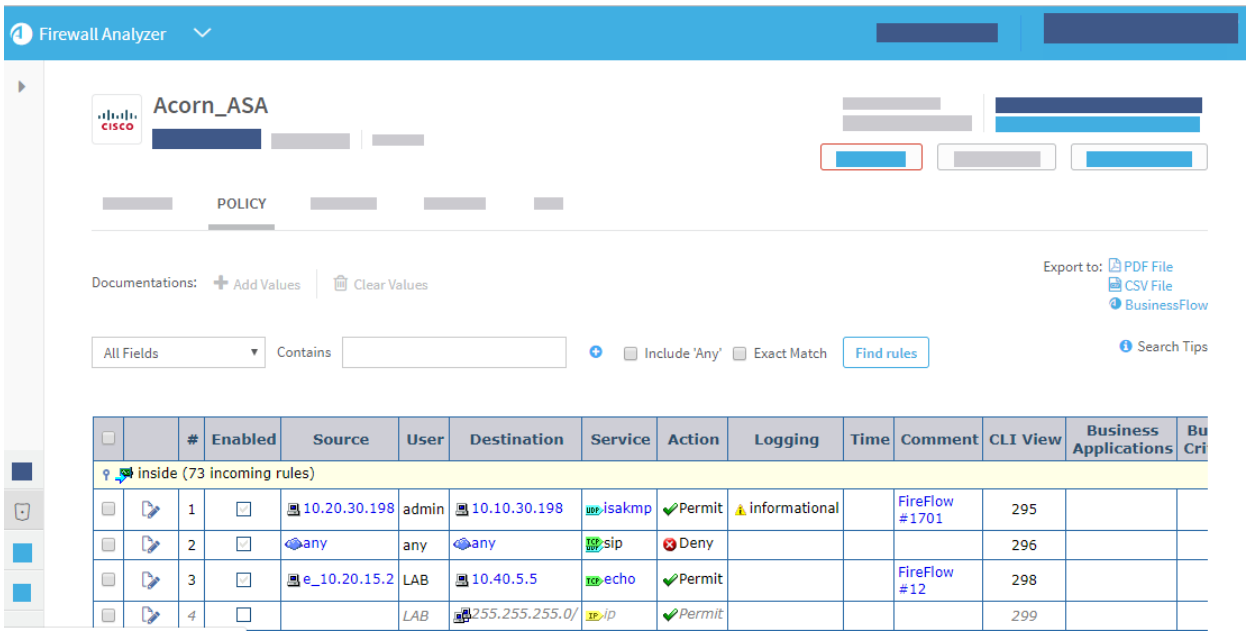


Browse and search through your security policies

Drill down to a specific device, group, or matrix using the main menu options on the left.

Check the **POLICY** tabs for each item to view the rules configured on each device.

Filter rules by rule fields, objects, IP address, and so on. For example:



For more details, see View policy data.

Eliminate risk items that are irrelevant in your environment

AFA provides you with several customization options that let you eliminate "false-positives" - risk items that are irrelevant to your environment:

- Customize the topology to mark your DMZ networks. Be advised about risky DMZ traffic.
- Customize trusted traffic to identify traffic that should not trigger risk items.
- Customize trusted networks to identify machines and subnets that should not trigger risk items.
- Customize Risk Profiles to determine the risk levels and to write your own risk items.

For complete instructions on all these subjects, see Customizing AFA Risk Detection (see Customize risk detection).

View a compliance report

After running a few analyses, familiarize yourself with one of the automatically populated compliance reports (Sarbanes-Oxley, PCI-DSS, ISO/IEC 27001 and others), which may be useful to you even if you are subject to other types of regulations. For details, see the Regulatory Compliance Page (see REGULATORY COMPLIANCE page).

View the real-time monitoring change history

After changing your device policy, browse the device's **Monitoring** tab to view the history of all policy changes made to the device. For complete instructions, see Using Real-Time Monitoring (see Manage real-time monitoring).

Run a Traffic Simulation Query on your network

Once AFA has analyzed your device(s) you can query the policy or policies on specific traffic passing through the device according to a specific source, destination, service or application (HTTP, SMTP, etc.). These queries are then immediately presented in the

AFA user interface. For details, see Running Traffic Simulation Queries (see Run traffic simulation queries).

Optimize your policy

After running an analysis, you can begin optimizing your device policy by pinpointing and then correcting common policy hitches such as having unused policy rules, rules that are covered by other rules or are special cases of following rules, rules that can be merged, rules that can be tightened as they are only partially used, etc. Go to an AFA report and click the **Policy Optimization** tab. For details, see the Policy Optimization Page (see POLICY OPTIMIZATION page).

➔ See also:

- Exploring Your Network (training video)

View policy data

This section explains how to examine polices in AFA.

Note: Searching the policy in the **Policy** tab is the preferred method for locating objects. For details, see Searching policies.

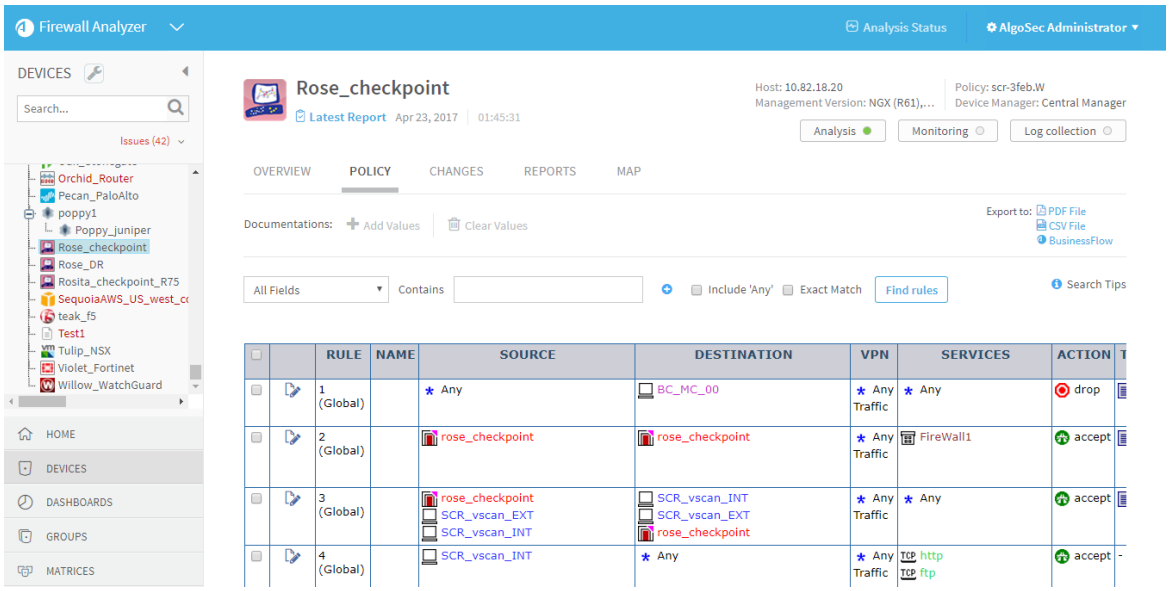
Note: Because the **Policy** tab does not show NAT rules, use the **Locate Object** feature's **Find in Rules** option to locate objects in NAT rules. For details, see Locate rules that use specific objects.

Viewing policies

To view a policy:

1. View the desired device, group, or matrix. For details, see View AFA device data, View AFA group data, and View AFA matrix data.
2. Click the **Policy** tab.

The **Policy** tab appears in the workspace.



The columns which appear in the policy tab are specific to each device brand. If AppViz is licensed, fields from AppViz appear, indicating business information such as which rules are included as flows in which applications.

Note: NAT rules do not appear in the **Policy** tab. To locate NAT rules, see Locate objects.

Note: If AppViz is licensed, you can export traffic flows from the policy to AppViz.

3. To search the policy for rules and objects, see Searching policies.

Searching policies

AFA provides the ability to perform advanced searches on policies.

For example, you can locate all device rules that use a specific object–whether the rules include the object explicitly or include an object containing the object–in any device, group, or matrix, or in any type of report. This is useful when planning to update or

remove an object, since it enables you to detect all the rules that will be affected by the change.

Note: NAT rules do not appear in the **Policy** tab. To locate NAT rules, see Locate rules that use specific objects.

To search a policy:

1. View the policy you want to search. For details, see Viewing policies.
2. In the drop-down list, select the field to search.

   All Fields is the default option.

   If you select the **Source**, **Destination**, **Source or Destination**, **Services** or **All Fields** options in the drop-down list, the search will also return rules with objects that contain the specified IP address(es) or services. All other fields perform a simple textual search.

   Note: Depending on your AFA configuration, this search feature may not function in this way. If your AFA is configured to always perform only a textual search, use the **Locate Object** feature to search for objects that contain specific IP addresses. For details, see Locate objects.

3. In the **Contains** field, type a string, IP address, IP range, service, range of services (eg., "TCP/20-50" or "All TCP"), or object name for which you want to search the policy. To search specifically for empty fields, type **[EMPTY]**.
4. To add another search parameter, click **And**, then complete the fields in the manner previously described.
5. To include results which contain the searched IP address(es) or service(s) only because they contain "any", "all", or "*", select **Include 'ANY'**.
6. To find rules that contain objects which contain only/exactly the IP address(es) or service(s) you searched for, select **Exact Match**.

7. Click **Find rules**.

   The policy is filtered according to the specified parameters.

   Objects that contain what was searched will appear highlighted in the search results.

Note: For Check Point devices, the results show one device to represent each policy. Multiple devices with the same policy will not appear in the search results.

Add/remove AFA rule comments

AFA supports adding comments to rules. The comments will appear in the rules' **Documentation** fields and in all device/group/matrix reports where the rules appear. You can add comments to a single rule, or add the same comments to multiple rules simultaneously.

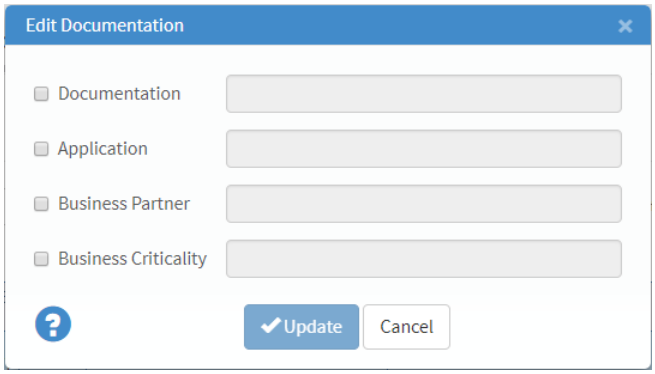
Note: These comments are only visible in AFA, not on the devices themselves.

Note: AFA administrators can disable or enable the **Documentation** field and add more such fields.

To add/remove comments from a single rule:

1. View the device/group/matrix policy, and locate the rule you want to edit. For details, see Searching policies.
2. In the desired rule's row, click  .

   The **Edit Documentation** dialog box appears.



3. Select the check box(es) next to the field(s) you want to edit.
4. Type your comments for the rule in the field(s) or delete the comments you want to remove.
5. Click **Update**.

   The comments are added/removed.

To add or remove the same comments from multiple rules:

1. View the device/group/matrix policy, and locate the rule you want to edit. For details, see Searching policies.
2. Select the check boxes next to the desired rules.
3. Click the **Add Values** link.

   The **Edit Documentation** dialog box appears.
4. Select the check box(es) next to the field(s) you want to edit.
5. Type your comments for the rules in the field(s) or delete any comments you want to remove.
6. Click **Update**.

   The comments are added or removed from all the selected rules.

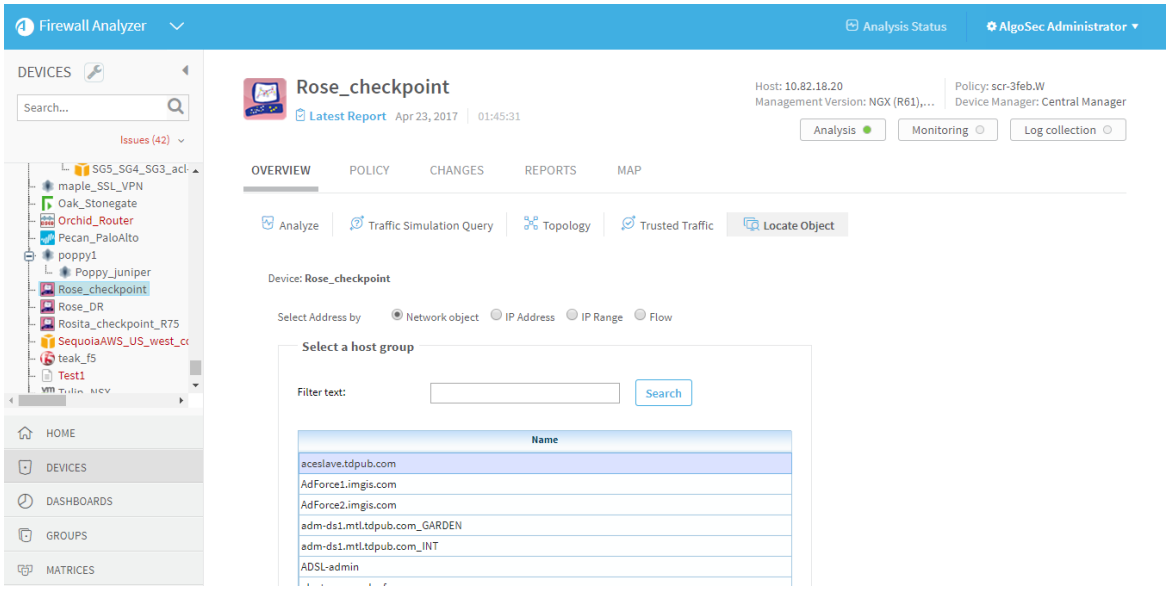
Locate objects

You can locate all objects which contain a specific IP address or range in a device, group, matrix, or in a specific report.

To locate an object:

1. Do any of the following, as described in View AFA device data, View AFA group data, and View AFA matrix data:
   - To search a *device* for an object, view the desired device.
   - To search a *group* for an object, view the desired group.
   - To search a *matrix* for an object, view the desired matrix.
   - To search *a single device report* for an object, view the desired device, click the **Reports** tab, and then select the check box next to the report in which you want to locate the object.
   - To search *all device reports* for an object, view the ALL_FIREWALL group, then click the **Reports** tab, and then select the check box next to the report in which you want to locate the object.
   - To search *a group report* for an object, view the desired group, click the **Reports** tab, and then select the check box next to the report in which you want to locate the object.
   - To search *a matrix report* for an object, view the desired matrix, click the **Reports** tab, and then select the check box next to the report in which you want to locate the object.
2. Click **Locate Object**.

   The **Locate Object** page appears.



3. Specify the object you want to locate.

   You can select an individual IP address, a range of IP addresses, or a host group that is defined on the device(s). If you wish to select a host group, you can search the defined names alphabetically, or by using the search filter.

4. Click **Find in Objects**.

   A new window opens displaying a list of objects with the specified IP address, range, or host group, in the specified devices and/or matrices.

Host Groups that contain Host Group aceslave.tdpub.com

Export/Print PDF
Download as CSV

Firewall: Rose_checkpoint

CONTAINING HOSTGROUP	CONTAINING IP ADDRESSES
NW_SCR_LAN_E_01	10.2.32.0-10.2.47.255
rose_checkpoint_network	10.150.22.0-10.150.22.255 10.2.32.0-10.2.47.255 16.47.59.0-16.47.59.255 10.82.18.16-10.82.18.31 192.168.6.0-192.168.6.255
Print-Test	16.47.70.251 172.17.2.254 200.200.200.251 16.47.71.251 192.168.15.251 10.150.22.0-10.150.22.255 10.0.0.1 10.22.40.17 16.47.76.11 10.82.18.16-10.82.18.31 10.2.32.0-10.2.47.255 172.17.1.254 172.17.3.254 16.47.59.0-16.47.59.255 192.168.6.0-192.168.6.255
FLOWER-star	10.150.22.0-10.150.22.255 10.22.32.0-10.22.47.255 16.47.71.0-16.47.71.255 27.35.176.166 10.2.32.0-10.2.47.255 192.168.6.0-192.168.6.255 10.0.0.0-10.0.0.3 10.82.18.16-10.82.18.31 172.17.3.252-172.17.3.255 200.200.200.0-200.200.200.255 16.47.59.0-16.47.59.255 172.17.1.252-172.17.1.255 192.168.15.0-192.168.15.255 16.47.70.0-16.47.70.255 16.47.76.0-16.47.76.255 172.17.2.252-172.17.2.255
	10.19.4.0-10.19.4.255 10.150.22.0-10.150.22.255 192.168.17.0-192.168.17.255 10.22.32.0-10.22.47.255

5. To export the results to PDF format, click Export/Print PDF. For more details, see Export AFA screens to PDF.

Locate rules that use specific objects

You can locate all device rules that use a specific object–whether the rules include the object explicitly or include an object containing the specific object–in any given device, group, or matrix, or in any type of report. The procedure below should be used when searching for NAT rules.

Otherwise, the recommended method to locate rules is through the **Policy** tab. For more information, see Searching policies. NAT rules do not appear in the **Policy** tab.

To locate rules that use a specific object:

1. Do any of the following, as described in View AFA device data, View AFA group data, and View AFA matrix data:
   - To search a *device* for an object, view the desired device.
   - To search a *group* for an object, view the desired group.

- To search a *matrix* for an object, view the desired matrix.
- To search *a single device report* for an object, view the desired device, click the **Reports** tab, and then select the check box next to the report in which you want to locate the rules.
- To search *all device reports* for an object, view the ALL_FIREWALL group, then click the **Reports** tab, and then select the check box next to the report in which you want to locate the rules.
- To search *a group report* for an object, view the desired group, click the **Reports** tab, and then select the check box next to the report in which you want to locate the rules.
- To search *a matrix report* for an object, view the desired matrix, click the **Reports** tab, and then select the check box next to the report in which you want to locate the rules.

2. Click **Locate Object**.

   The **Locate Object** page appears.

3. Specify the object you want to locate, by doing one of the following:
   - To select a host group that is defined on the device(s):
     1. In the **Select Address by** area, choose **Host group**.
     2. Select the host group you wish to locate. You can search the defined names alphabetically, or by using the search filter.
   - To select an individual IP address:
     1. In the **Select Address by** area, choose **IP Address**.
     2. Type the IP address you wish to locate.
     3. To locate rules with objects that contain only the specified IP address, select the **Exact match** check box.

- To select a range of IP addresses:
    1. In the **Select Address by** area, choose **IP Range**.
    2. Type the starting and ending IP addresses for the IP range you wish to locate.
    3. To locate rules with objects that contain only the specified IP range, select the **Exact match** check box.
- To select a specific traffic flow:
    1. In the **Select Address by** area, choose **Flow**.
    2. Specify the source and destination by selecting or typing an individual IP address, a range of IP addresses, or a host group. If you wish to select a host group, you can search the defined names alphabetically, or by using the search filter.

       If you type a host group that has an IP address as its name, put it in quotations (for example "10.20.1.1").
    3. To locate rules with objects that contain only the IP addresses specified in source and destination, select the **Exact match** check box.

Note: For Cisco devices, locating rules with the exact match feature will not return results where the IP address was added directly to the rule (not within a network object).

4. Click **Find in Rules**.

   A new window opens displaying a list of rules containing the specified object, in the specified devices and/or matrices.

Firewall: Rose_checkpoint

Export/Print PDF
Download as CSV

Rules that contain host group Any

	RULE	NAME	SOURCE	DESTINATION	SERVICES	ACTION	COMMENT	COUNT	LAST USE	PERCENTAGE	INSTALL	BUSINESS APPLICATIO
1	1 (Global)		* Any	BC_MC_00	* Any	drop	FireFlow #78: Eliminate the clutter...	0	N/A	0.000%	rose_checkpoint	
2	4 (Global)		SCR_vscan_INT	* Any	TCP http TCP ftp	accept	FireFlow #149: eSafe needs to bypass itself	0	N/A	0.000%	rose_checkpoint	
3	7 Disabled		* Any	rose_checkpoint	* Any	drop	FireFlow #1: No one gets to the firewall	0	Disabled	0.000%	rose_checkpoint	
4	8		scr1401.scr.tdpub.com_INT	* Any	TCP ftp	accept	Eagle Flight Pagation Server. Need to bypass eSafe for FTP.	0	N/A	0.000%	rose_checkpoint	
5	9 Disabled		* Any	* Any	Bad_Services	drop	No ping, tracert, etc. FireFlow #251: Removed NBT from this list	0	Disabled	0.000%	rose_checkpoint	
6	32		GP_NW_SLI_All	* Any	* Any	drop	FireFlow #319: Drop all remaining traffic from SLI. Log until complete.	0	N/A	0.000%	rose_checkpoint	
7	37		GP_NW_Garden_ICN	* Any	* Any	accept	-	0	N/A	0.000%	rose_checkpoint	
8	38		GP_NW_BAI_LAN	* Any	General_services smtp->SCR_SMTP_Scan http->SCR_HTTP_Scan ftp->SCR_FTP_Scan	accept	FireFlow #323: Scan for viruses logging enabled DT2007/02/05	0	N/A	0.000%	rose_checkpoint	
9	39 Disabled		GP_NW_BAI_LAN	* Any	General_services smtp->SCR_SMTP_Scan TCP ftp TCP http	accept	FireFlow #324: Scan for viruses disabled Aug 27, 2007 CVP errors not eSafe	0	Disabled	0.000%	rose_checkpoint	
10	48		GP_Dthomson	* Any	TCP tcp-1863-MSM-Messenger NetMeeting	accept	FireFlow #344: MicroSoft Windows Update	0	N/A	0.000%	rose_checkpoint	
11	52 (Global)		* Any	* Any	* Any	drop		0	N/A	0.000%	rose_checkpoint	

The yellow highlighting indicates which IP address, range of IP addresses, or host groups contain the object you want to locate.

5. To see a host group's definition, click on the host group.
6. To export the results to PDF format, in the top-right corner of the report, click Export/Print PDF. For more details, see Export AFA screens to PDF.

   Tables at the end of each device display relevant network and service object definitions. Clicking on the object in a rule will bring you to its definition in these tables.
7. To export the results to CSV format, in the top-right corner of the report, click Download as CSV. Follow your browser prompts to open the file.

AFA reports

This section explains how to understand and use AFA device, group, and matrix reports.

For more details, see Device report pages, Group report pages, and Matrix report pages.

Comparison reports

AFA enables you to compare reports from the same device from different dates, or compare reports from different devices. Comparing reports not only detects differences in objects, but also provides an analysis of the differences' effects.

For example, it reveals which traffic is allowed by one device and not by the other, and vice-versa. This can be used to determine what has changed in a device over a long period of time, or to determine whether a vendor conversion project was performed correctly.

Tip: You may want to compare reports from different vendors if you are considering migrating your devices to a new vendor.

For details, see:

- Compare reports from the same device
- Compare reports from different devices
- View comparison reports

Note: For full traffic comparison, enable **Comprehensive Mode** in the AFA Administration area General options.

This ensures that AFA analyzes all services defined on the device, and not only the ones relevant for risks.

Compare reports from the same device

Comparing reports from the same device from different dates lists the differences in traffic, service definitions, hostgroup definitions, topology, risks, and rules.

Do the following:

1. In AFA, navigate to the device you want to compare reports for. For details, see View a specific device.

   View the desired device as described in , then click the **Reports** tab.

   The relevant page appears with a list of reports.

2. On the device details page, click **Reports** to display a list of available reports.
3. Select the reports you want to compare, and then click Compare.
4. In the **Compare reports** dialog, click **Compare**, and watch while AFA compares the selected reports.

   To stop report comparison, click **Stop Comparison**.

When complete, the comparison report opens in a new window. The comparison report is also attached to the more recent of the device reports you compared.

Compare reports from different devices

Comparing reports from different devices provides differences in provides differences in traffic, service definitions, hostgroup definitions, topology, and risks. When comparing reports for two Check Point devices with different policies, differences in rules are also included by default.

Do the following:

1. Either select both devices from the **ALL_FIREWALLS** group, or select each device one at a time.

   For details, see Viewing the ALL_FIREWALLS Group and View a specific device.

   - If selecting from the **ALL_FIREWALLS** group, click the **All Reports** tab, and select the reports you want to compare.
   - If selecting from a specific device, browse to your device and click the **Reports** tab. Then select a report to compare and click Compare.

At the prompt, select your second device and report, and click Compare again.

Tip: When selecting devices to compare, you may see light & dark-colored device report entries.

- Dark entries mean that you have the appropriate permissions to perform all actions on the device (i.e., customizing the topology, trusted traffic, refreshing, and deleting report).
- A light-colored entry means you have read-only permission.

2. In the **Compare reports** dialog, click **Compare**, and watch while AFA compares the selected reports.

   To stop report comparison, click **Stop Comparison**.

When complete, the comparison report opens in a new window. The comparison report is also attached to the more recent of the device reports you compared.

View comparison reports

This procedure describes how to view a comparison report between two devices.

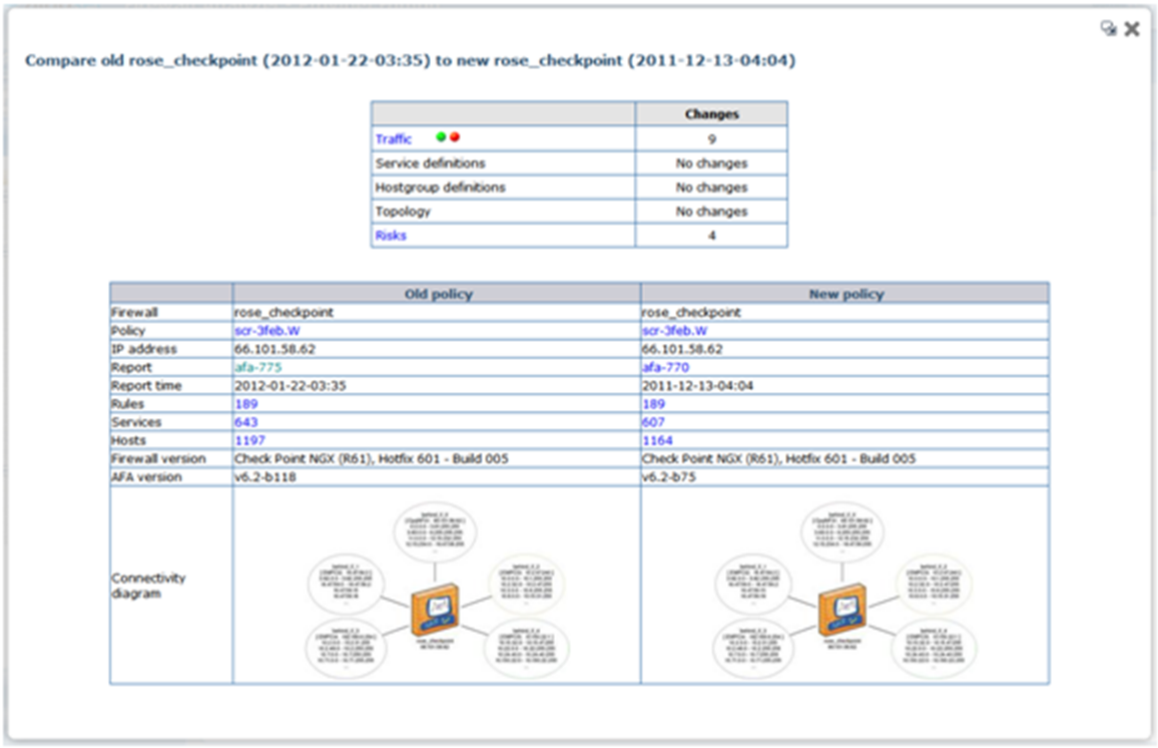
Comparison reports are attached to the more recent of two reports compared. For more details, see Comparison reports.

Do the following:

1. View a device report to which a comparison is attached. For details, see View device reports.
2. Click the **Policy** tab. In the Comparisons area, select the comparison report you want to view.

   The two reports are displayed side by side, with a summary table at the top.

   For example:



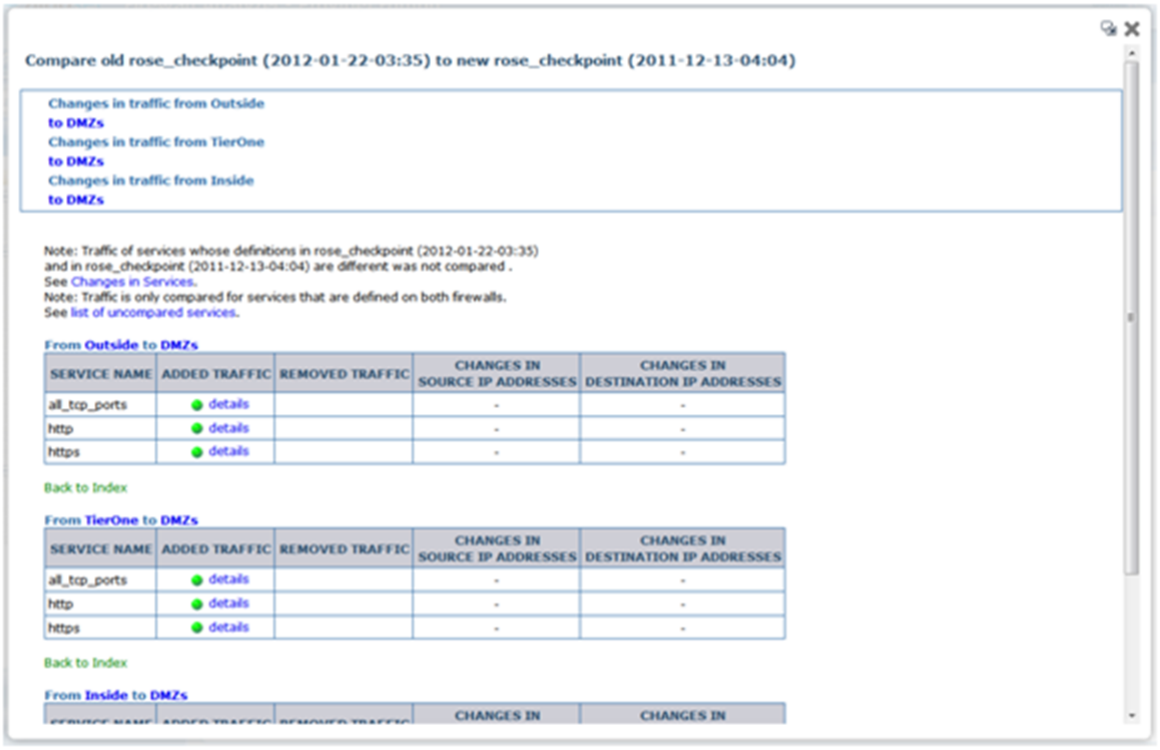
Compare old rose_checkpoint (2012-01-22-03:35) to new rose_checkpoint (2011-12-13-04:04)

	Changes
Traffic	9
Service definitions	No changes
Hostgroup definitions	No changes
Topology	No changes
Risks	4

	Old policy	New policy
Firewall	rose_checkpoint	rose_checkpoint
Policy	scr-3feb.W	scr-3feb.W
IP address	66.101.58.62	66.101.58.62
Report	afa-775	afa-770
Report time	2012-01-22-03:35	2011-12-13-04:04
Rules	189	189
Services	643	607
Hosts	1197	1164
Firewall version	Check Point NGX (R61), Hotfix 601 - Build 005	Check Point NGX (R61), Hotfix 601 - Build 005
AFA version	v6.2-b118	v6.2-b75
Connectivity diagram		

3. To drill down to more details, click the **Traffic** link in the summary table.

   Traffic details are displayed, with green bullets indicating added traffic and red bullets indicating removed traffic.



Each traffic direction is listed separately, with hyperlinks to each section at the top of the page. In each table, rows represent services and contain details about the traffic changes that occurred.

For example, added traffic might include details about what was blocked before and is allowed now. Removed traffic might include what was allowed before and is blocked now.

In each row, click **details** to drill down even further.

Note: The comparison report does not cover traffic of services that are defined in only one report, or are configured differently in each report.

Export reports to PDF

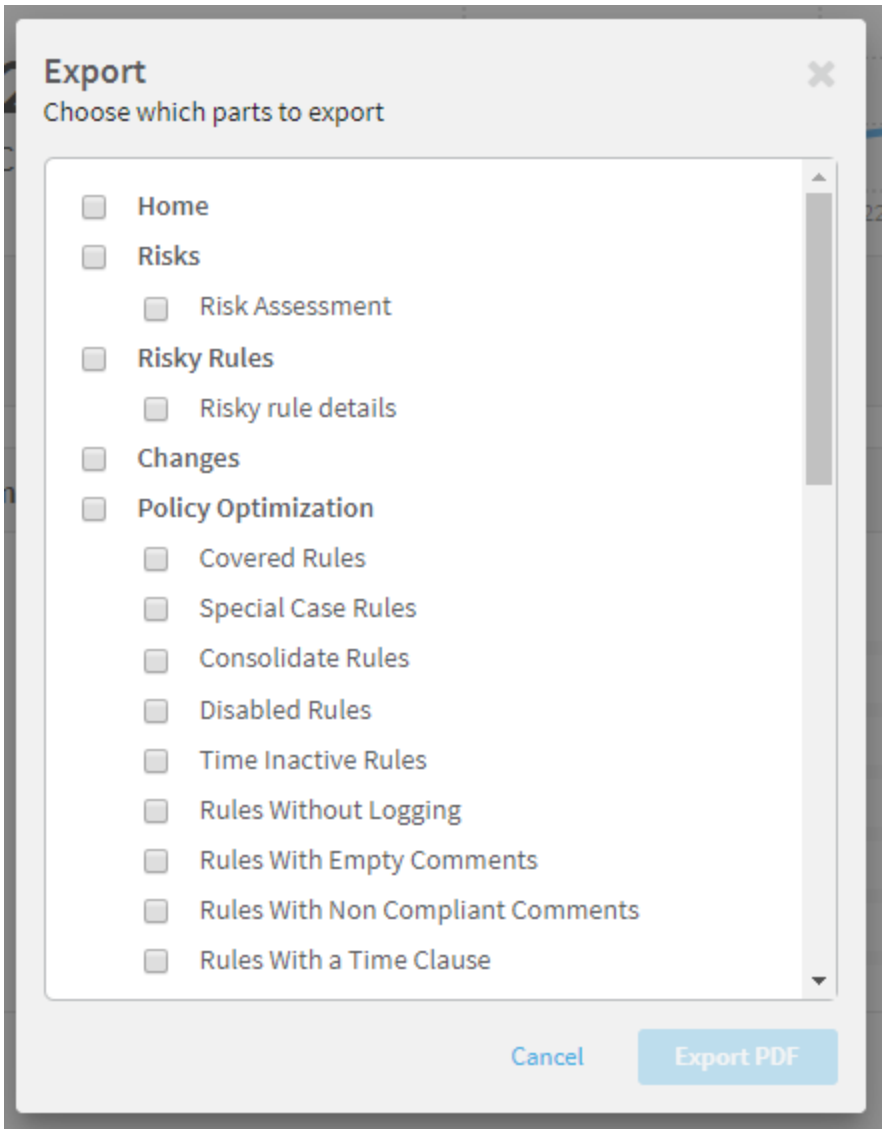
This procedure describes how to export entire AFA reports or individual report pages to PDF.

Do the following:

1. In the top-right corner of the report, click **Export/Print PDF**.

   If you started from the **HOME** tab of the report, a dialog appears where you can select specific pages to export.

   For example:



   Select the pages you want to export, and click **Export PDF**.

If you started from any other page in the report, the print preview opens with an optimized version for saving to PDF.

Note: Depending on your web browser, there may be adjustments in the print preview dialog for optimal output.

For details, see Export AFA screens to PDF.

Delete reports

This procedure describes how to delete reports from AFA.

Do the following:

1. Navigate to the report you want to delete, and then click the **Reports** tab.

   For more details, see:

   - View AFA device data
   - View AFA group data
   - View AFA matrix data

   If you are deleting reports for multiple devices, view the **ALL_FIREWALLS** group, and then click the **All Reports** tab. For details, see Viewing the ALL_FIREWALLS Group.

2. In the list of reports, select the checkboxes for the report or reports you want to delete.
3. Click **Delete**. In the confirmation message, click **OK**.

The reports are deleted, and are no longer accessible from AFA.

Manually generated reports

Run a manual analysis to create an unscheduled report, including the following types:

- **Reports on individual devices, groups, and matrices defined in** AFA. For details, see Run a manual AFA analysis.

- **Reports on potential policy configurations**. For details, see Perform a what-if analysis.
- **Reports on configuration files**, for devices not defined in AFA. For details, see Analyze device configuration files.

Run a manual AFA analysis

This procedure describes how to manually generate an AFA report.

By default, when a group or matrix report is generated manually, AFA generates a new report for each member of the group or matrix, and then also generates a group or matrix report. You can also select to aggregate the group or matrix members existing report into a new group or matrix report.

Do the following:

1. In AFA, navigate to the device, group, or matrix you want to create the report for. For details, see View AFA device data, View AFA group data, and View AFA matrix data.

   Note: When you select a "parent" tier device, all the devices beneath it are automatically analyzed with each analysis.

2. In the **Overview** tab, click **Analyze**.

   Define the **Analyze** dialog fields as needed, and then click **Start Analysis**. For details, see Analyze dialog field reference.

   AFA starts creating the report.

For more details, see Managing Analyses.

Perform a what-if analysis

A what-if analysis generates a report based on a potential policy. What-if analysis reports enable you to examine the implications of a policy change before implementing

the change.

Do the following:

1. Access the policy you want to use as a template.

   Click **Save as** to save it with a new name, and Edit the policy as needed.

2. Run an analysis on the policy. For details, see Run a manual AFA analysis, selecting **What-if analysis** in the **Analyze** dialog.

For Cisco, Juniper Netscreen, Juniper SRX, Fortinet Fortigate, and Palo Alto Networks devices, this procedure differs.

For these devices, do the following instead:

1. In AFA, navigate to the report you want to use to perform the analysis, and click the **Explore Policy** tab.
2. In the **Device Configuration** area, click **Raw Files**.
3. Right click the configuration file and select **save link as** to download the file locally.

   The configuration file will have a suffix that corresponds to the device type, such as .**nsc** or .**fgate**.

4. Edit the downloaded file, changing the relevant areas as needed. For example, you might want to edit the areas in the **show config** section.
5. Save the file, ensuring that you keep the suffix the same.
6. Use the file to run an analysis. For details, see Analyze device configuration files

Analyze device configuration files

This procedure describes how to manually generate a report from data in a device configuration file.

You might want to do this to perform a what-if analysis on specific device types, or when testing configurations in a lab environment.

Do the following:

1. In AFA, navigate to the **ALL_FIREWALLS** group. For details, see Viewing the ALL_FIREWALLS Group.
2. Click the **All Reports** tab, and then click **Analyze File**.
3. In the **Analyze File** dialog, click **Browse** to browse to the file you want to analyze.

   Note: The file size must be 20 MB or less. If you have a larger file, have an AFA administrator add it to AFA as a device.

4. Define the **Analyze** dialog fields as needed, and then click **Start Analysis**. For details, see Analyze dialog field reference.

   AFA starts creating the report.

For more details, see Managing Analyses.

Analyze dialog field reference

In the **Analyze** dialog, enter the following values as needed:

Select risk profile	Select the Risk Profile to use for performing the analysis. Alternatively, you can use the **Standard** profile, which is the default.
What-if analysis	Select to perform a what-if analysis and generate a report based on a potential policy. For more details, see Perform a what-if analysis.
Avoid e-mail notification	Select to configure AFA not to send email notifications when the report is complete.

Analysis based on logs from X to Y	Select to generate the report using only logs from a specific date range. Specify the date you want to start the date range. The end date is always the current day. **Note:** You cannot select a date earlier than the existing AFA logs begin.
Analyze X based on existing reports	Select to aggregate the group/matrix members' *existing* reports into a group/matrix report, instead of generating new reports for each member before aggregating them. Displyed only when generating group reports and matrix reports.

Scheduled analysis and manual analysis requests

AFA administrators can also schedule recurring analysis. Scheduled analysis supports multiple reports running in parallel, with maximums depending on your AFA system configuration and power. For details, see

- If a manual report is already running when AFA is otherwise scheduled to run a scheduled monitoring process, the scheduled monitoring for that device is skipped. AFA attempts the next monitoring cycle as scheduled.
- If a monitoring cycle is already running on a specific device when a manual report is requested, AFA waits for the monitoring process to complete before generating the report.

Devices, groups, and matrices

This section describes how devices added to AFA can be viewed and their reports analyzed, on their own or within the context of a group or matrix.

For details, see:

View AFA device data	Describes how to work with individual devices and their reports.
View AFA group data	Describes how to work with groups of devices, and reports that cover the entire group. AFA groups are sets of devices that are managed together without any connection to the relationships between the member devices. AFA treats groups as a single unit, providing a birds-eye view of your group-wide risk exposure. **Tip:** AFA provides a default group called **ALL_FIREWALLS**. This group includes all devices in the entire system, and enables you to generate reports for all your AFA devices.
View AFA matrix data	Describes how to work with matrices, and reports that cover then entire matrix. AFA matrices are sets of devices that are managed together with consideration as to the relationships between the member devices. When a matrix is created, AFA attempts to calculate the relationships between the devices, and also enables you to edit the topology manually. AFA manages a matrix's policy as a single unit, providing a birds-eye view of your matrix-wide risk exposure.

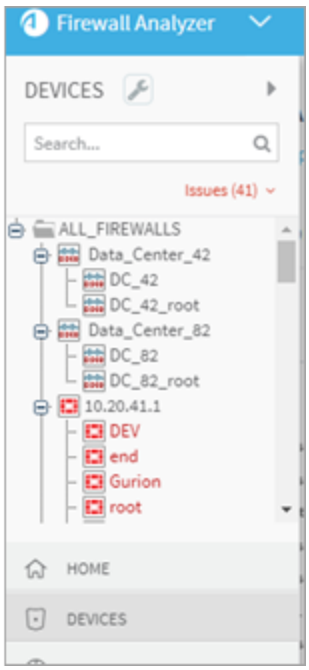
➔ See also:

- AFA reports

View AFA device data

This topic describes how to view and work with the device data displayed in AFA.

AFA's device tree



Many devices supported by AFA are actually a system of devices in a hierarchy that work together. Each device defined in AFA is represented as a node in the tree, and any physical or virtual devices it manages appear as sub-nodes.

AFA enables you to manage and view data for each individual node or parent nodes. Reports at a parent level aggregate all analysis information for each of the sub-devices. Running an analysis on a parent node also updates data for each of the children.

Palo Alto Networks Panorama and Juniper SRX devices

Palo Alto Networks Panorama devices also display the device's group. Click the link to open a list of all device groups.

Additionally, Palo Alto Networks Panorama devices and any Juniper SRX devices that are configured to display virtual routers, VRs appear as the last tier in the device tree.

In this case, AFA provides reports for each VR under each VSYS/LSYS. Although the VSYS/LSYS analysis aggregates the data for each child VR, it does not contain the full VR tier data, as is usually the case for parent reports.

Data for individual VRs include topology and routing information, and the risky rules associated with the traffic they route. These reports should be consulted to troubleshoot routing issues, or to view risky rules. All other data, such as policy optimization recommendations, is in the VSYS/LSYS reports.

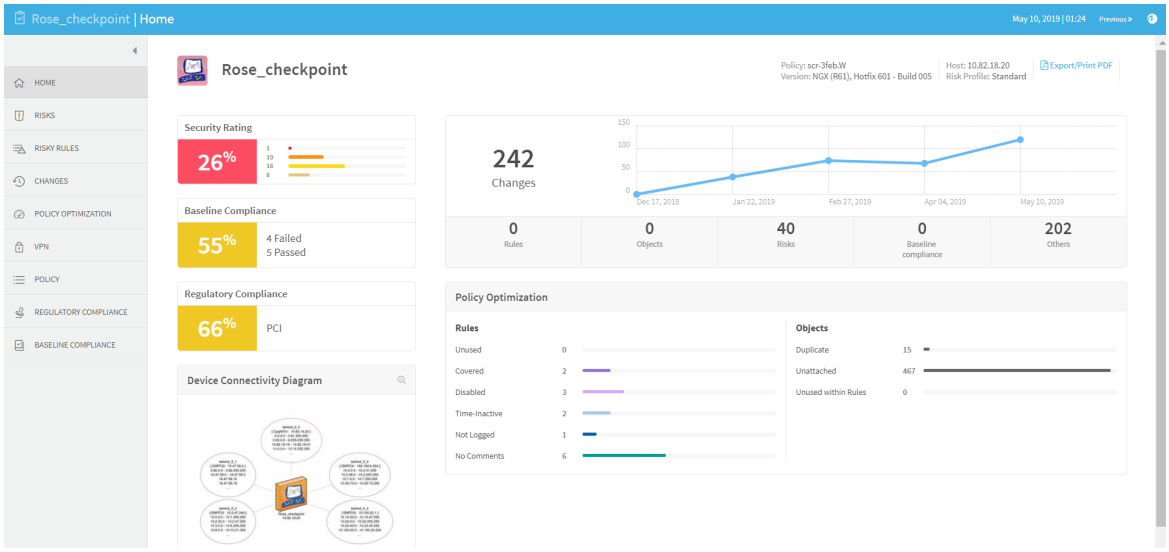
Note: This behavior is not relevant to Juniper Netscreen or NSM devices configured to display virtual routers. Netscreen devices are not sub-devices of a virtual system, and are displayed as parallell.

View a specific device

To view data for a specific device, do the following:

1. In the main menu on the left, click DEVICES.
2. Browse to or search for your device's name.
   - Devices for which the last report generation, real-time monitoring, or log collection failed appear in red.
   - Layer 2 devices that are not placed on the map appear in orange.

   Tip: To filter out devices with issues from being listed in the tree, click the **Issues** link at the top, and clear the selection for any item types you want to hide. Click the **Issues** link again to return to the standard view.
3. Click your device in the tree to view full details in the workspace.



The information displayed at the top of the workspace for each device varies by its relative position in the hierarchy of the device tree.

Data displayed per device type

All tiers	Data displayed for all tiers includes: • **A link to the latest report,** with the date and time the device was last analyzed at that tier. For example:  • **Status indicators** for the latest analysis, monitoring, and log collection processes. Green items indicate success, red indicates failures, and grey indicates a run in process or no data available.
Parent devices	Parent devices are also displayed with the number of devices they manage.
Individual devices	The following additional data is displayed for individual devices: • **Host**. The device's IP address. • **Management/Device Version**. The device's version and build. • **Policy**. The device's policy. • **Device Manager**. The remote agent that performs data collection for the device. Only displayed if geo-distribution is enabled. If the device is managed locally, this field displays **Central Manager**. • **Monitoring and log collection status** for the specific device: . Last cycle succeeded. . Last cycle failed. . Monitoring / log collection disabled.

For more details, see:

- AFA's graphic network map
- Managing Analyses
- Manage real-time monitoring
- Run traffic simulation queries
- Customize risk detection

Device data for cloud devices

AFA represents cloud "devices" with a three-tiered hierarchy:

- **AWS**. User account > Region / VPC > Security set
- **Azure**. Subscription > Region / VPC > Security set

In AFA, **security sets** are groups of instances, ALBs, or VMs with the exact same security group and network ACLs or subnet security groups applied. Each instance, ALB, or VM in a security set has identical security policies.

Details shown for each cloud device varies at each tier, and you can manage each tier individually, such as running analysis on a specific tier only. Reports for "parent" tiers appear as group reports, and when an analysis is run on a "parent" tier, reports are automatically generated for each tier below it. For more details, see View AFA group data.

Cloud data per tier

The following details are presented at **all tiers**:

The following additional data is presented for the **top two tiers** only (**account** / **subscription** and **region** / **VPC** / **VNet**):

- **The number of regions** with the tier.
- **The number of VPCs or VNets** in the tier.
- The number of instances, ALBs, or VMs in the tier.

Click the linked number to open a full list of items. For example:

The following information is presented at the **security set tier** only:

Security group or network security group	The name of the security set's group. Click the link to show a list of the security groups and IDs.
Network ACLs or subnet network security group.	The name of the security set's ACLs or subnet network security group. Click the link to show a list of the security groups and IDs.
Region	The name of the security set's region.
VNet or VPC	The name of the security set's VPC or VNet.
Instances, ALBs, or VMs	The number of instances, ALBs, or VMs. Click the link to open a searchable list of the instances, ALBs, or VMs and IDs.
Subnets	The number of subnets. Click the link to open a list of the subnets and IDs.
Monitoring and log collection	The monitoring and log collection status for the specific device. . Last cycle succeeded. . Last cycle failed. . Monitoring / log collection disabled.

View device reports

Device reports provide details about a single device, either a device that's defined individually or the lowest tier in the device tree for a system of devices.

View the latest report

To view the full and latest report for a specific device, browse to and select a specific device, and then click the Latest Report link at the top of the workspace.

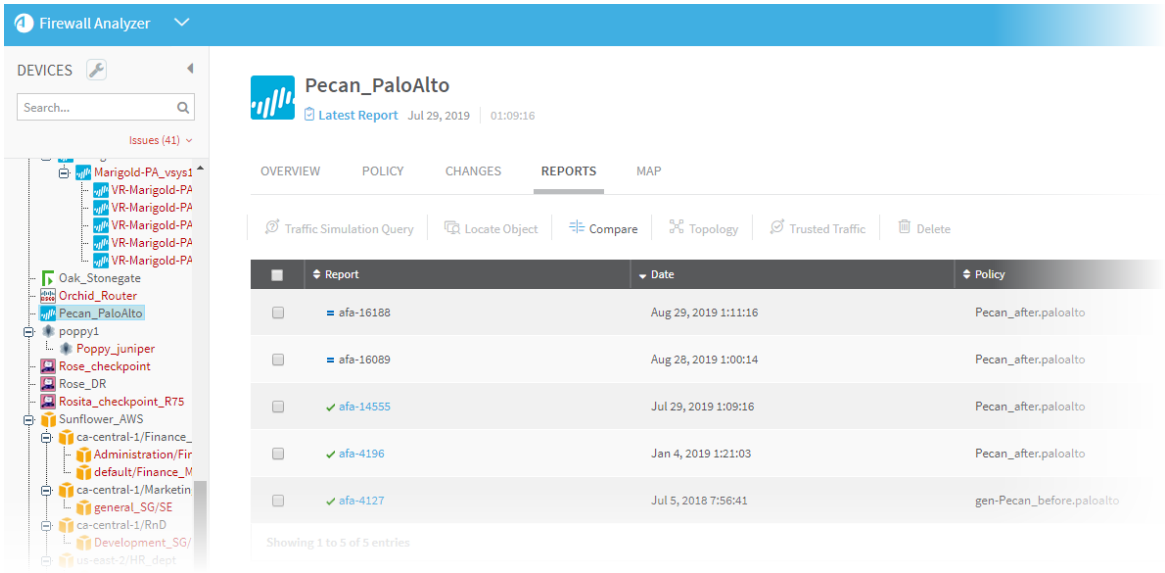
The report opens in a separate tab. For more details, see AFA reports.

View an earlier report for a specific device

Do the following:

1. Browse to and select your device in the device tree.
2. In the workspace, click the **REPORTS** tab, which displays a list of all available reports for the device.

   For example:



   Report status is listed as follows:

   - ✓ Report was generated successfully
   - ⧗ Report is currently being generated
   - ✕ Report failed to generate

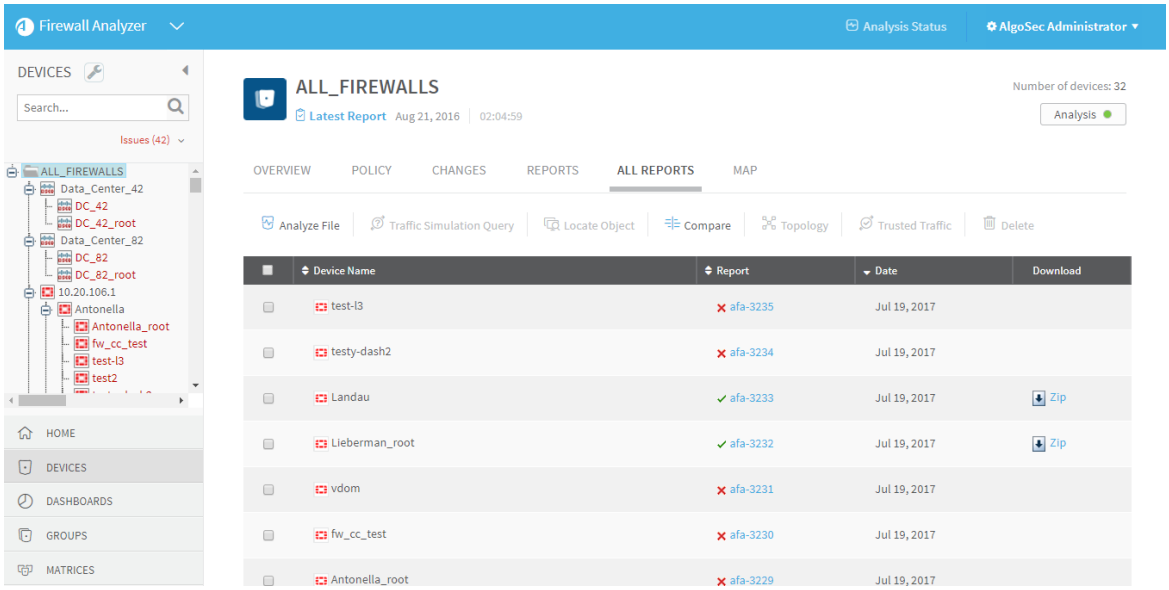
3. Do one of the following:
   - To view a report online, click the report's name.
   - To download a report to your computer, click the **Zip** link in the row for the report you want to download.

   For more details, see AFA reports.

View a report for all devices

Do the following:

1. At the top of the device tree, click the **ALL_FIREWALLS** node.
2. In the workspace, click the **REPORTS** tab, which displays a list of all available reports for all devices in the system.



3. Click the **All Reports** tab.

   The **All Reports** tab appears, displaying a list of all available reports for all devices in the system.

   Report status is listed as follows:

   - ✓ Report was generated successfully
   - ⧗ Report is currently being generated
   - ✗ Report failed to generate

4. Do one of the following:

   - To view a report online, click the report's name.
   - To download a report to your computer, click the **Zip** link in the row for the report you want to download.

   For more details, see AFA reports.

Tip: At the top right of each page in the report, click **Export / Print PDF** to export the report to a shareable PDF file. For more details, see Export AFA screens to PDF.

Device report page reference

The following tables describe the pages included in device reports.

	**Home**. Provides a general overview of the report, including basic device information and statistics, changes to the device, and device connectivity. For details, see HOME page.
	**Risks**. Provides a high-level executive summary of the risk analysis findings. Available only with the AFA Risk and Compliance Module. For details, see RISKS page.
	**Risky Rules**. Provides a list of all the risky rules (vs. the actual risk displayed in the summary page) found in the device policy, along with links to all the risks to which each rule contributed. Available only with the AFA Risk and Compliance Module. For details, see RISKY RULES page.
	**Changes**. Displays the changes in rules, objects, and the resulting changes in allowed traffic and risks, over all the history of AFA reports for this device. For details, see CHANGES page.
	**Policy Optimization**. Find out what you can eliminate from your device policy to optimize it and make it more efficient and maintainable. For details, see POLICY OPTIMIZATION page.
	**VPN**. Allows navigating through the VPN definitions on your device: identify the users, user groups, VPN rules, and VPN communities, and the relationships between these entities. For details, see VPN page.
	**Policy**. Provides access to the wealth of detailed information collected and identified during the analysis. For details, see POLICY Page.

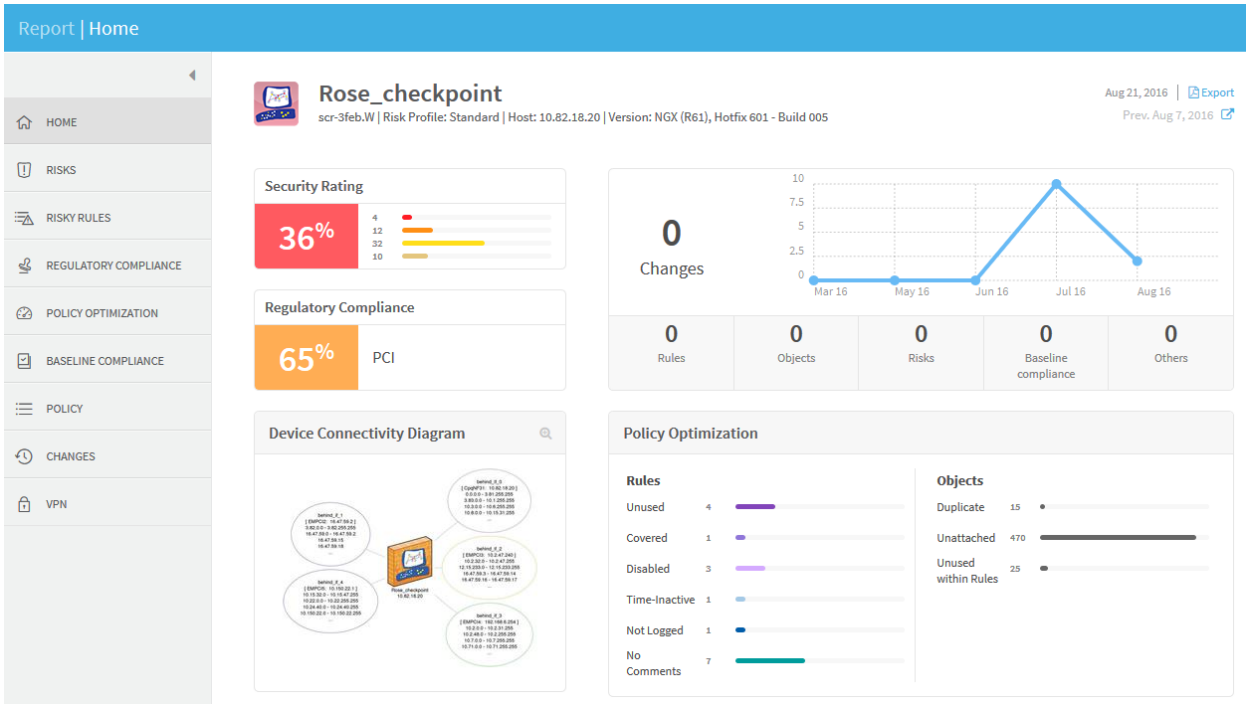
	Regulatory Compliance. Access a variety of automatically-filled compliance reports. Available only with the AFA Risk and Compliance Module. For details, see REGULATORY COMPLIANCE page.
	Baseline Compliance. Indicates whether the device's configuration complies with a certain baseline. For details, see BASELINE COMPLIANCE page.

Device report pages

This topic describes the pages included in device reports. For more details, see View AFA device data.

HOME page

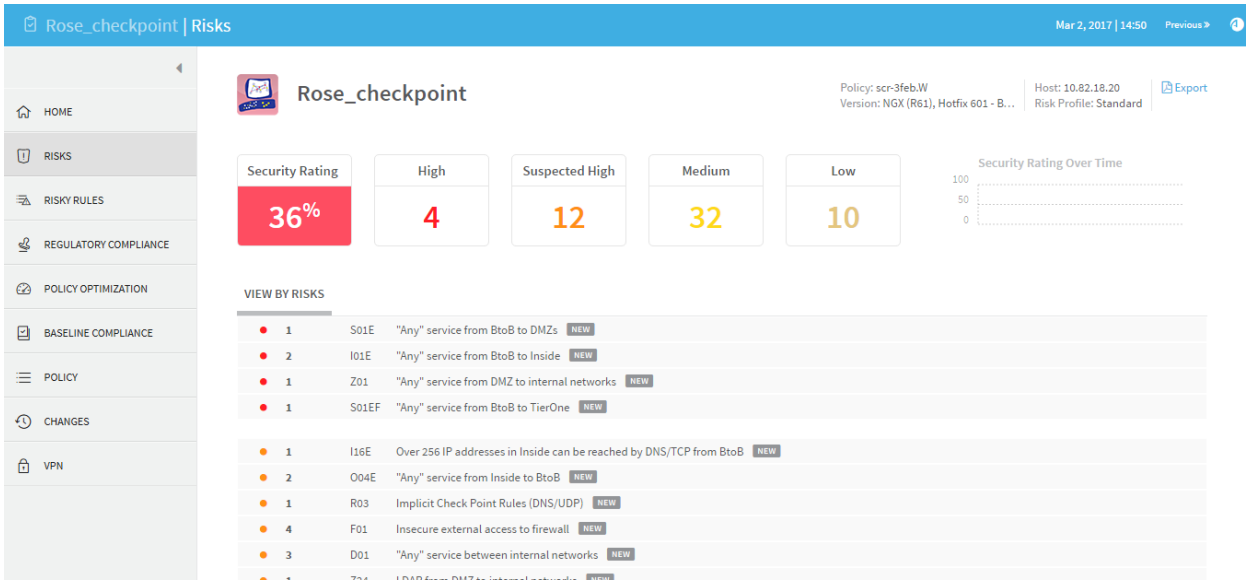
The **HOME** page provides an overview of the device report. The page's content depends on your AFA modules.



- Click the titles of the various widgets on the page to dive down to other pages in the report.
- Click the **Device Connectivity Diagram** to zoom in for details.

RISKS page

The **RISKS** page summarizes all risk analysis findings.



The **Risks** page provides the following details:

- The **security rating** for the device.

  The security rating indicates the device's degree of compliance with security standards. A security rating of 100% indicates full compliance.
- The **total number of risks** in each severity category, not counting duplicates.
- A graph displaying the **security rating trend** over time.
- A list of **all the device's risks**, in decreasing order of severity.

  The list includes a brief summary of each threat: the risk, its trigger count (the number of times it was detected), and a brief description. The **New** label indicates risks that were not present in the previous report.

> **Tip:** Click a risk to drill down to a Risk Assessment page for more details about the risk and any related rules.

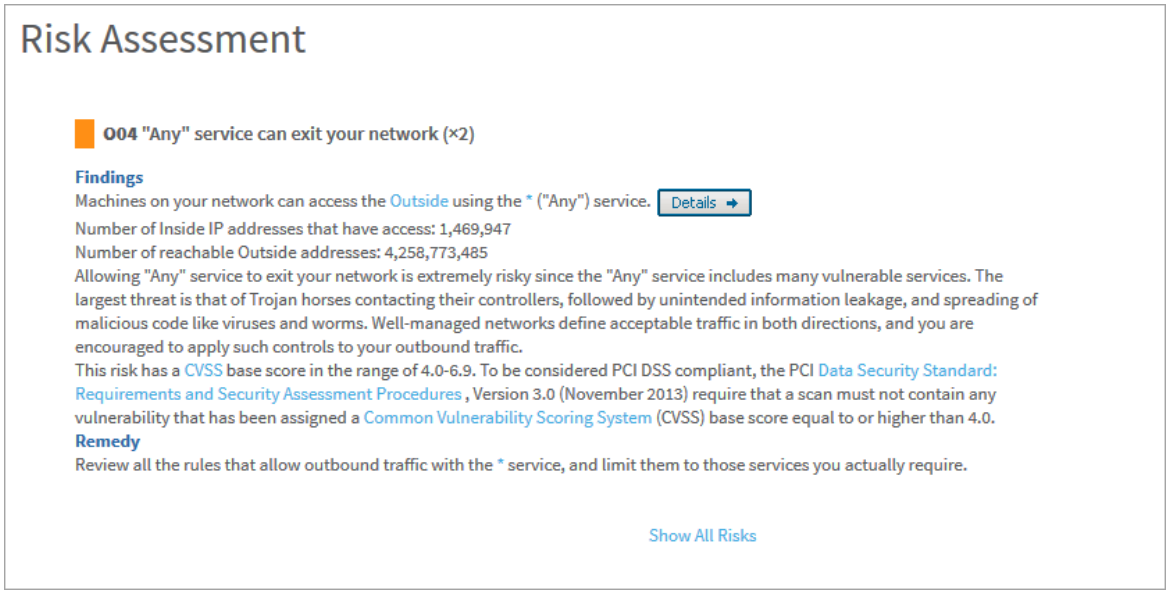
Risks page use case scenario

The following demonstrates a typical workflow to drill down to a problematic rule or group from the risks page.

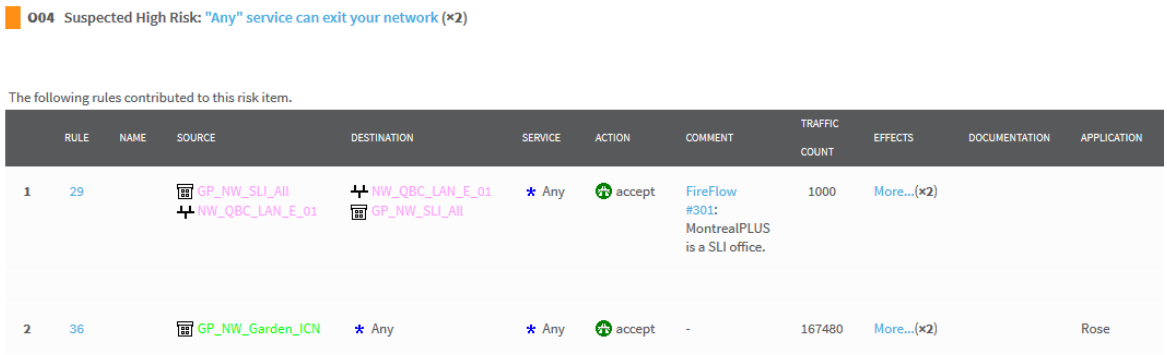
1. On the **RISKS** page in a report, click on a risk.

   The **Risk Assessment** appears, displaying the findings and the recommended remedy. The risk is presented in a descriptive manner with links to every entity that is associated with the risk.

   In the example below, AFA shows you the number of internal and external IP addresses that have access or are reachable by the risky service.



2. Click the **Details** button to view the specific rules that allow access to the risky services.

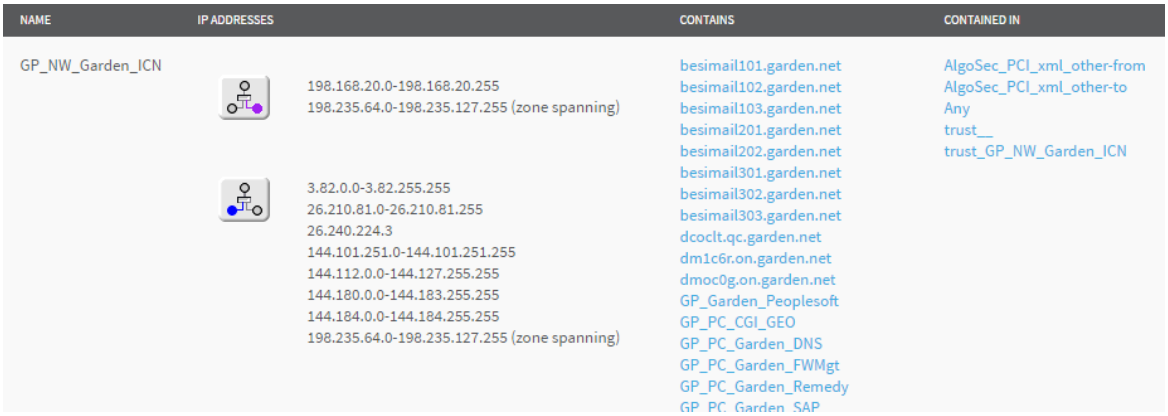


004 Suspected High Risk: "Any" service can exit your network (×2)

The following rules contributed to this risk item.

	RULE	NAME	SOURCE	DESTINATION	SERVICE	ACTION	COMMENT	TRAFFIC COUNT	EFFECTS	DOCUMENTATION	APPLICATION
1	29		GP_NW_SLI_All NW_QBC_LAN_E_01	NW_QBC_LAN_E_01 GP_NW_SLI_All	* Any	accept	FireFlow #301: MontrealPLUS is a SLI office.	1000	More...(×2)		
2	36		GP_NW_Garden_ICN	* Any	* Any	accept	-	167480	More...(×2)		Rose

3. In the example above, we see that rule **36** looks like an **accept** rule that allows outbound access. Allowing any outbound service is not recommended since it may be used by Trojan horses to attack business partners. However, this does not explain why any service is allowed from the outside. Therefore, we navigate further and click on the group GP_NW_Garden_ICN to examine its definition.



NAME	IP ADDRESSES	CONTAINS	CONTAINED IN
GP_NW_Garden_ICN	198.168.20.0-198.168.20.255 198.235.64.0-198.235.127.255 (zone spanning)	besimail101.garden.net besimail102.garden.net besimail103.garden.net besimail201.garden.net besimail202.garden.net besimail301.garden.net besimail302.garden.net besimail303.garden.net dcoclt.qc.garden.net dm1c6r.on.garden.net dmoc0g.on.garden.net GP_Garden_Peoplesoft GP_PC_CGI_GEO GP_PC_Garden_DNS GP_PC_Garden_FWMgt GP_PC_Garden_Remedy GP_PC_Garden_SAP	AlgoSec_PCI_xml_other-from AlgoSec_PCI_xml_other-to Any trust__ trust_GP_NW_Garden_ICN
	3.82.0.0-3.82.255.255 26.210.81.0-26.210.81.255 26.240.224.3 144.101.251.0-144.101.251.255 144.112.0.0-144.127.255.255 144.180.0.0-144.183.255.255 144.184.0.0-144.184.255.255 198.235.64.0-198.235.127.255 (zone spanning)		

4. The above figure shows that host group **GP_NW_Garden_ICN** spans the device:
   - The purple icon tells us that some of its IP addresses are outside of the network.
   - The blue icon shows that other IP addresses are on the inside.

   Since the rule that uses this host group allows access to any destination, the outside addresses (**198.168....**) are allowed to enter the network with any protocol. **This is a serious vulnerability.**

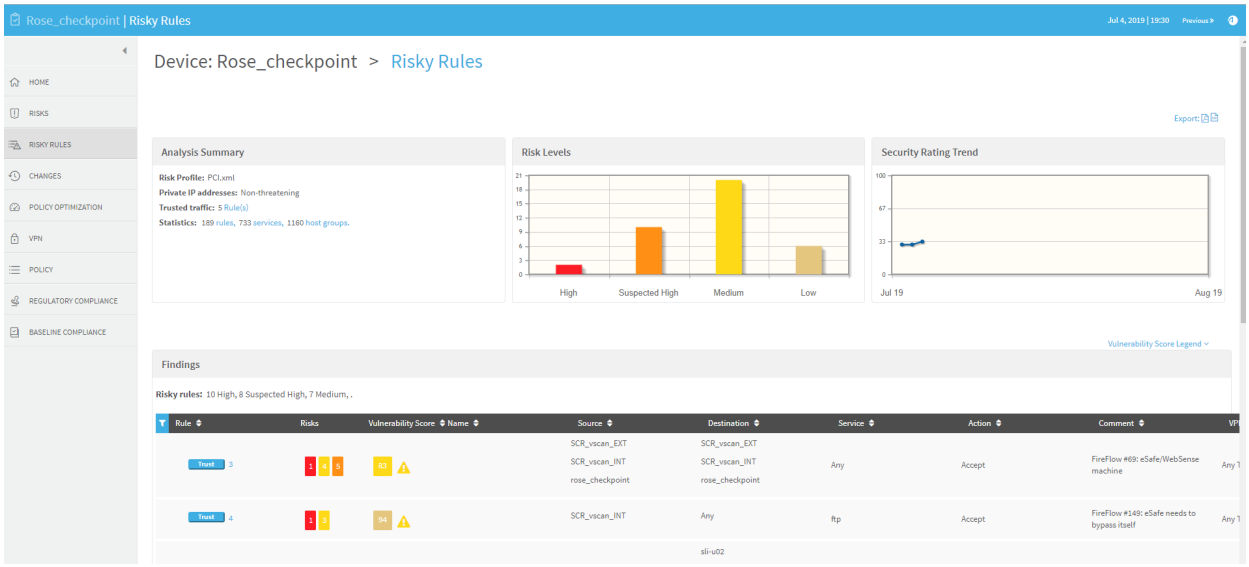
In this case, the likely culprit is a typing error: the administrator probably planned to type "**192**" (which is an inside address) and mistakenly typed "**198**".

Note: Similar vulnerabilities exist in virtually every large organization. A scanner will never find it. A human audit will rarely find it, since all IP addresses look the same. AFA finds and highlights all these vulnerabilities automatically, within minutes.

Tip: Click on the icons in the **IP ADDRESSES** column to see where the IP addresses are located in the Connectivity Diagram.

RISKY RULES page

The **RISKY RULES** page shows the rules that pose risk to the policy. As opposed to the **RISKS** page which shows the risks triggered by risky policy rules, the **RISKY RULES** page details the rules that cause these risks.

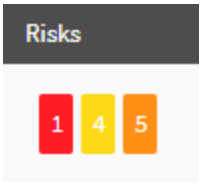


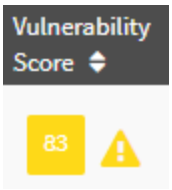
At the top of the page, do any of the following:

- In the **Analysis Summary** area, click links to drill down to rules, services, and host groups.

- In the **Risk Levels** and **Security Rating Trend** graphs, view data about the risks on the device over time.

In the **Findings** table below the graphs, view details about each risky rule found. Additionally, do any of the following:

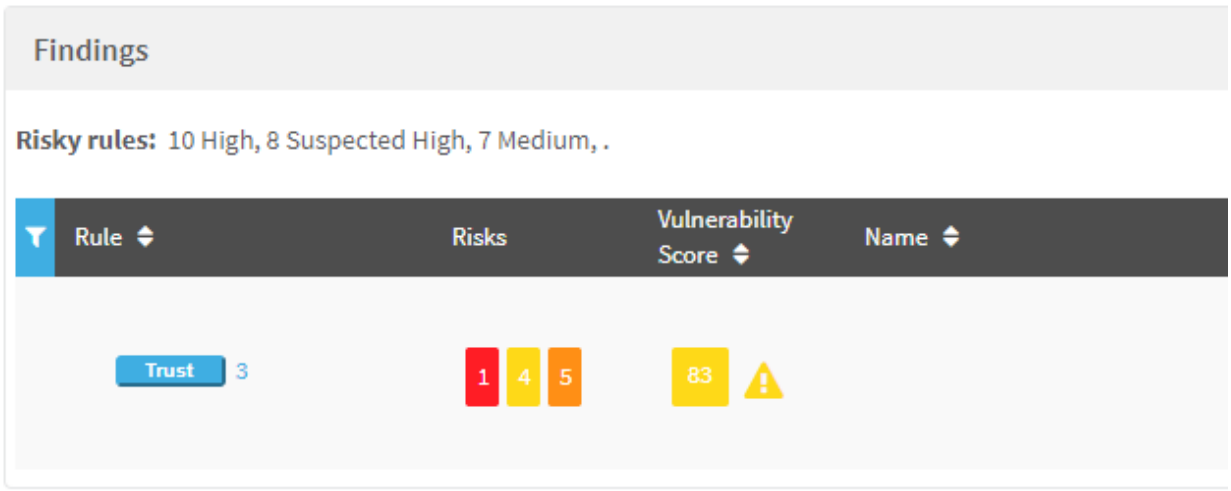
Filter the table rows	Click  to filter the rules displayed.
Sort the table	Click  in each column to sort the table by that column.
Trust specific rules	Click **Trust** to add that rule to trusted traffic. For more details, see Customize trusted traffic.
View rule details	Click the rule number to drill down to more details about that rule.
View risks	Risks are shown as colored boxes in the **Risks** column, indicating the number of risks in each severity for the rule described in that row. For example, the following image shows that there is 1 risk with critical severity, 4 with medium, and 5 with suspected high.  Click a colored box to drill down to the selected risky rule and its risks. For more details, see Risks and vulnerabilities in AlgoSec Firewall Analyzer reports.

View vulnerabilities	Vulnerabilities are shown in the **Vulnerability Score** column, including the overall vulnerability score for the IP addresses covered by the selected rule, the number of vulnerabilities found and the scanning status. For example, the following image indicates a vulnerability score of medium, with 83 vulnerabilities found, and one or more unscanned servers.  Click a colored box to drill down to the selected risky rule and its vulnerabilities. For more details, see Risks and vulnerabilities in AlgoSec Firewall Analyzer reports. **Note:** Vulnerabilities with a CVSS score of **0** are ignored.

Risks and vulnerabilities in AlgoSec Firewall Analyzer reports

When you click a colored box in the **Risks** or **Vulnerability Score** column on the Risky Rules page, the page is refreshed with details about the selected risky rule only, and risks and vulnerabilities for that rule are shown in tabs below.

For example:



Do any of the following:

- Switch back and forth between the tabs as needed, and continue to drill down to view additional information.
- Use the breadcrumbs at the top of the page or the **RISKY RULES** menu item at the left to jump back to the main risky rules table.
- Click the **Vulnerability Score Legend** link above the **Findings** table for details about vulnerability score colors.

  ⚠ Indicates that you have unscanned servers.

Note: Vulnerabilities are displayed only if you have AppViz configured with vulnerability scanners in the AppViz**Administration** area.

Risk levels are configured in the AlgoSec Firewall Analyzer**Administration** area.

Risky rules for Palo Alto Networks Panorama and Juniper SRX devices

The **Risky Rules** page is not included for VSYS/LSYS-level reports on the following device types:

- **Palo Alto Networks Panorama** devices
- **Juniper SRX** devices configured to display virtual routers

For these devices, the **Risky Rules** page is provided for VR reports only, because risky rules only trigger risks on VRs that route traffic.

Note: VSYS/LSYS reports *do* include all the risks for each of its VRs in the **Risks** page. For details, see RISKS page.

Additionally, this behavior is not relevant to Juniper Netscreen or NSM devices configured to display virtual routers. For Netscreen, the VR is not a sub-device of a virtual system, so every report includes the **Risky Rules** page.

REGULATORY COMPLIANCE page

The **REGULATORY COMPLIANCE** page includes several reports that describe how compliant your security policy is to specific regulatory standards.

The **Regulatory Compliance** page provides the following regulatory compliance reports:

- Payment Card Industry Data Security Standard (PCI DSS)
- Sarbanes-Oxley
- ISO/IEC 27001
- NERC Standards for Critical Infrastructure Protection (NERC CIP)
- NIST SP 800-171
- NIST SP 800-53
- NIST SP 800-41
- Gramm-Leach-Bliley Act (GLBA)
- Basel-II
- ASD ISM
- Financial Instruments and Exchange Law (Japan)
- MAS TRM
- HIPAA
- GDPR

To view a training video that follows an Information Security Officer preparing for an annual PCI-DSS audit and involves analyzing different sets of reports, see Performing Compliance and Risk Analysis Using AFA Reports.

Payment Card Industry Data Security Standard (PCI DSS)

This page follows the item numbering and instructions of PCI DSS v3.2 audit procedures, and fills in any data that is already available to AFA. Using this report can save you hours of work when you need to prepare your annual or quarterly PCI DSS compliance report.

If AppViz is being used with a vulnerability scanner, this report can be configured to display the vulnerability of PCI applications. Requirement 6.1 specifies whether AppViz is being used and whether vulnerability scanner integration is enabled. If you configure the PCI zone and a vulnerability threshold in AFA, the requirement additionally specifies the servers in the PCI zone and the vulnerability assessment for all AppViz applications which intersect the PCI zone.

Sarbanes-Oxley

This report explains how your current AFA configuration settings support CobiT 5 control objectives and COSO components. Use this report to learn how well you are doing, and to present to your auditors as needed.

The first part of the report deals with automation and monitoring, and the control objectives that require them. The report tabulates the details of the AFA automation capabilities that you have turned on.

Automation and Monitoring Settings

AlgoSec Feature	Setting	Details	Status
Change History	On	Records available since 2013-03-07	✓
Scheduled Analysis	On	Daily at 01:00	✓
E-Mail Notification	Off	These users get an email when the following occurs: None	✗
Covered Rule Analysis	On		✓
Unused Rule Analysis	Off		✗
Unattached Object Analysis	On		✓
Disabled/Timed-out Rules	On		✓
No-Log Rules	On	Rules with no logs: 1 . Click here to view	✗
No-Comment Rules	On	Rules with empty comments: 6 . Click here to view.	✗

The next part of the report deals with risk management, and the control objectives that relate to risk. In this part you can see the general risk management settings you have in place, followed by the *full* list of all the risks that AFA searched for in the current report. The **Status** column tells you if the risk was found (indicated with a red X) or if your device is compliant with respect to this risk (indicated with a green check mark). All risks that are found appear with their details in the AFA front page.

Risk Assessment Criteria

Criterion	Setting	Details
Risk Profile	AlgoSec Standard	Revision: 1.54
RFC 1918 IP addresses	Trusted	
Trusted Traffic	On	6 Trusted Traffic Rules

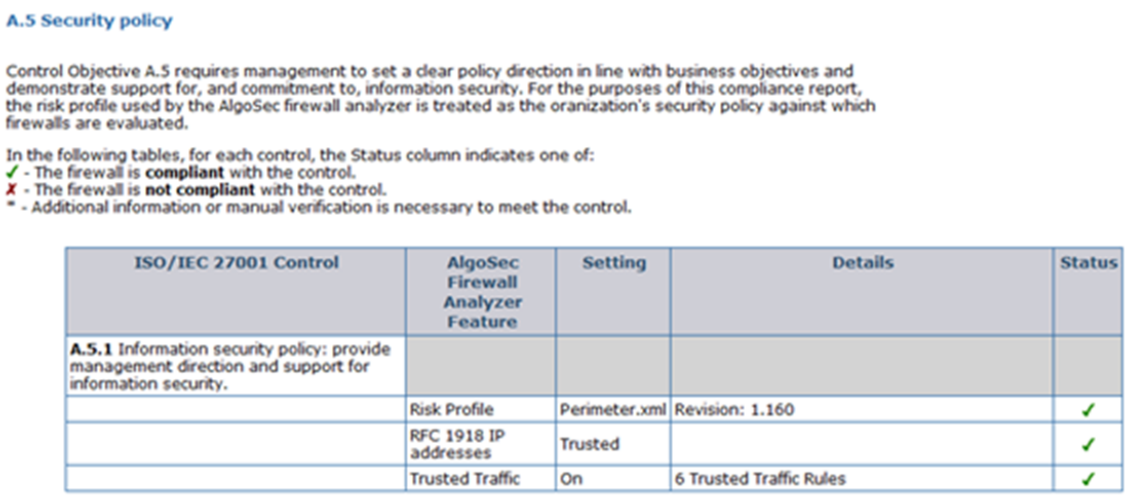
Findings

The following table lists all the risk items that were searched for according to the Risk Assessment Criteria. For each risk item, the Status column indicates one of:
✓ - the risk item **was not** found
✗ - the risk item **was** found
* - the risk item was found, but it is a special case of a more general risk item. Only the more general risk item that applies is marked with an ✗.

		Code	Risk Description	Status
1.		I01	"Any" service can enter your network	✗
2.		I02	TCP on all ports can enter your network	*
3.		I03	UDP on all ports can enter your network	*
4.		I07	Risky Microsoft services can enter your network	*

ISO/IEC 27001

This page follows the item numbering and instructions of ISO/IEC 27001:2013 International Standard "*Information technology - Security techniques - Information security management systems - Requirements"* and of the companion ISO/IEC 27002:2013 *"Code of practice for information security management"* International Standard, and fills in any data that is already available to AFA. Using this report can save you hours of work when you need to prepare your annual or quarterly ISO/IEC 27001 compliance report.



A.5 Security policy

Control Objective A.5 requires management to set a clear policy direction in line with business objectives and demonstrate support for, and commitment to, information security. For the purposes of this compliance report, the risk profile used by the AlgoSec firewall analyzer is treated as the oranization's security policy against which firewalls are evaluated.

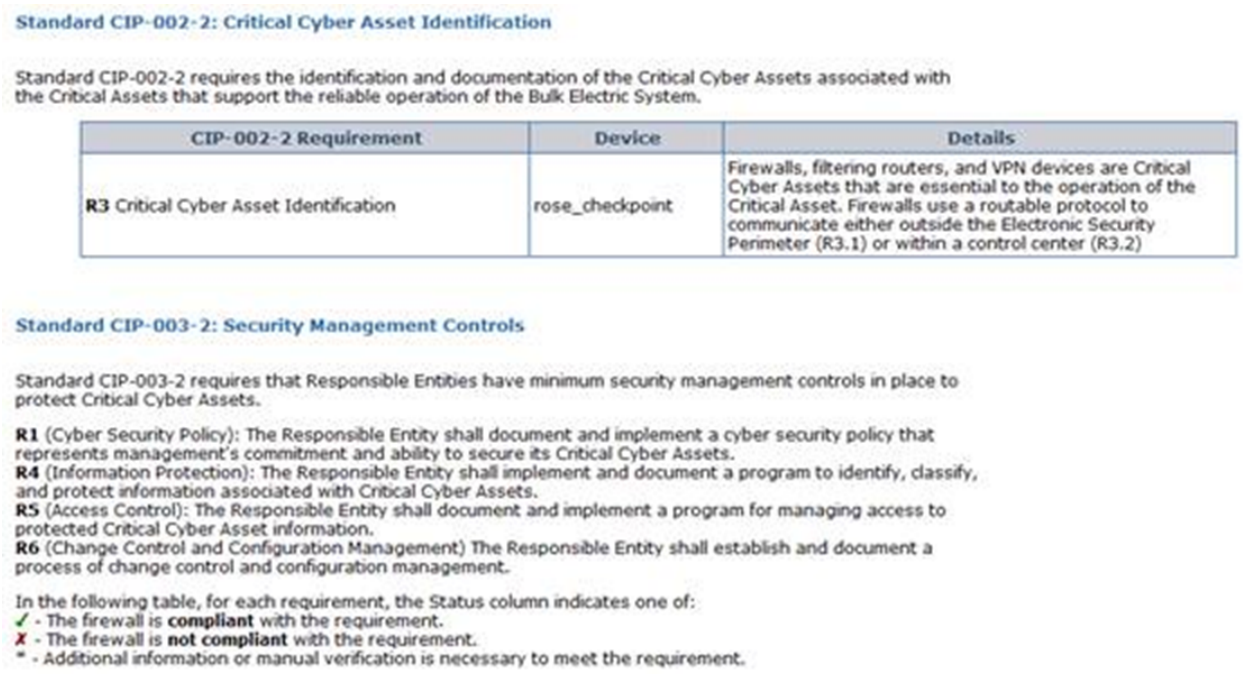
In the following tables, for each control, the Status column indicates one of:
✓ - The firewall is **compliant** with the control.
✗ - The firewall is **not compliant** with the control.
* - Additional information or manual verification is necessary to meet the control.

ISO/IEC 27001 Control	AlgoSec Firewall Analyzer Feature	Setting	Details	Status
A.5.1 Information security policy: provide management direction and support for information security.				
	Risk Profile	Perimeter.xml	Revision: 1.160	✓
	RFC 1918 IP addresses	Trusted		✓
	Trusted Traffic	On	6 Trusted Traffic Rules	✓

NERC Standards for Critical Infrastructure Protection (NERC CIP)

This report addresses the requirements that apply to devices, filtering routers, and VPNs, as specified in NERC Standards CIP-002-2, CIP-003-2, CIP-004-2, CIP-005-2, and CIP-007-2. Compliance with these requirements is required of all NERC-registered entities by June 30, 2010, and this report can save auditors time when compiling CIP documentation.

Note: By default, NERC version 4 is displayed. It is possible to configure AFA to simultaneously display version 3 and 4. Contact AlgoSec support for assistance.



Standard CIP-002-2: Critical Cyber Asset Identification

Standard CIP-002-2 requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System.

CIP-002-2 Requirement	Device	Details
R3 Critical Cyber Asset Identification	rose_checkpoint	Firewalls, filtering routers, and VPN devices are Critical Cyber Assets that are essential to the operation of the Critical Asset. Firewalls use a routable protocol to communicate either outside the Electronic Security Perimeter (R3.1) or within a control center (R3.2)

Standard CIP-003-2: Security Management Controls

Standard CIP-003-2 requires that Responsible Entities have minimum security management controls in place to protect Critical Cyber Assets.

R1 (Cyber Security Policy): The Responsible Entity shall document and implement a cyber security policy that represents management's commitment and ability to secure its Critical Cyber Assets.
R4 (Information Protection): The Responsible Entity shall implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets.
R5 (Access Control): The Responsible Entity shall document and implement a program for managing access to protected Critical Cyber Asset information.
R6 (Change Control and Configuration Management) The Responsible Entity shall establish and document a process of change control and configuration management.

In the following table, for each requirement, the Status column indicates one of:
✓ - The firewall is **compliant** with the requirement.
✗ - The firewall is **not compliant** with the requirement.
* - Additional information or manual verification is necessary to meet the requirement.

The requirement numbers listed in the report are aligned with those specified in the relevant NERC Standards.

NIST SP 800-171

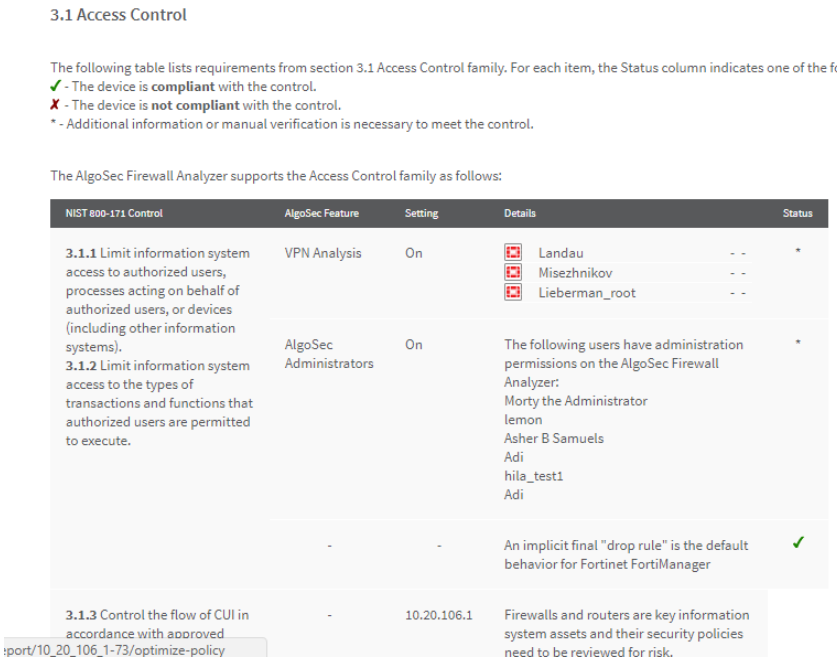
The AlgoSec Firewall Analyzer compliance report for NIST Special Publication 800-171 uses the National Institute of Standards and Technology (NIST) document Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations, Revision 1 (June 2015).

This publication provides federal agencies with recommended requirements for protecting the confidentiality of Controlled Unclassified Information (CUI):

(i) when the CUI is resident in non-federal information systems and organizations;

(ii) when the information systems where the CUI resides are not used or operated by contractors of federal agencies or other organizations on behalf of those agencies;

(iii) where there are no specific safeguarding requirements for protecting the confidentiality of CUI prescribed by the authorizing law, regulation, or government wide policy for the CUI category or subcategory listed in the CUI Registry.



3.1 Access Control

The following table lists requirements from section 3.1 Access Control family. For each item, the Status column indicates one of the following:
✓ - The device is **compliant** with the control.
✗ - The device is **not compliant** with the control.
* - Additional information or manual verification is necessary to meet the control.

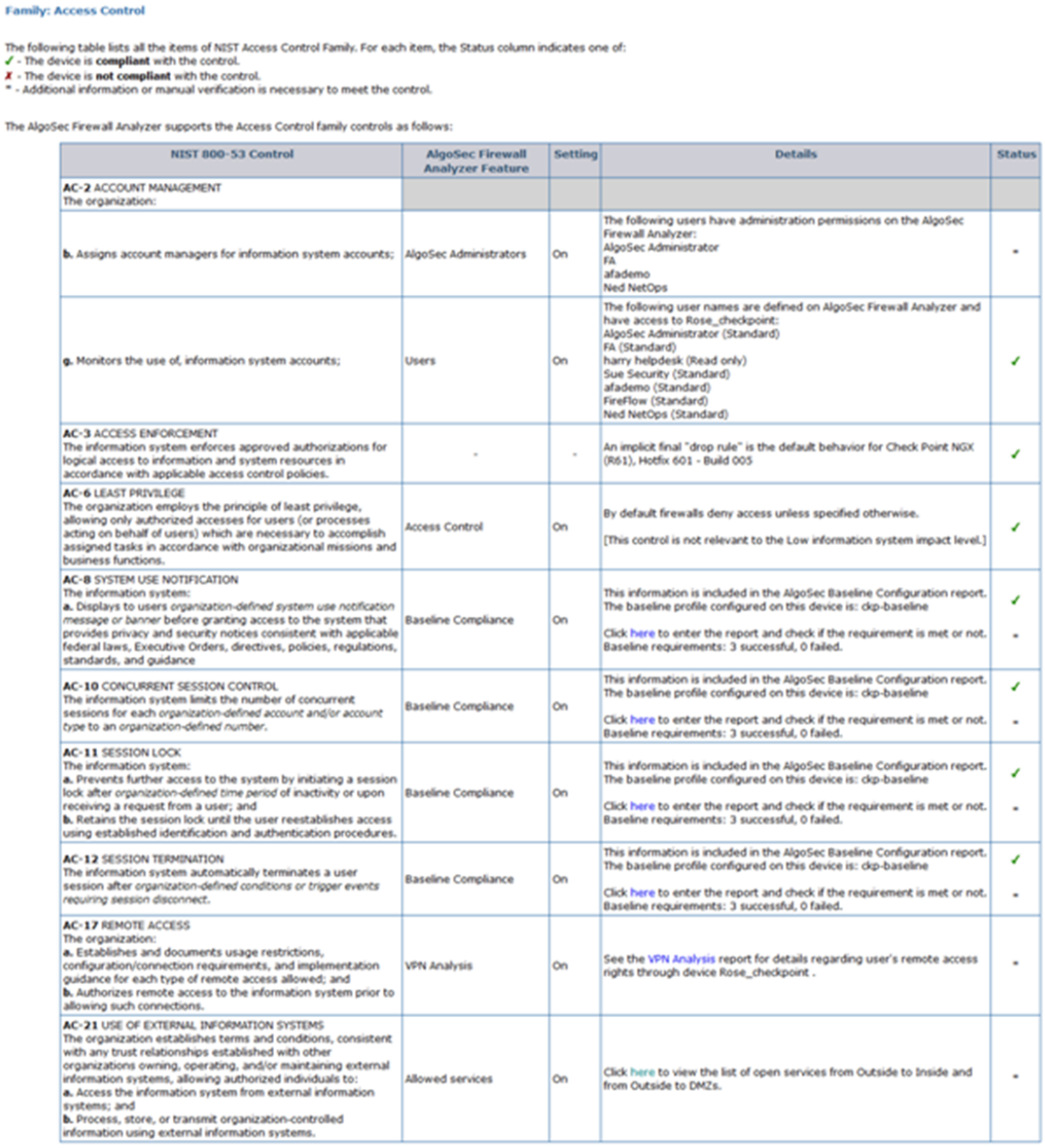
The AlgoSec Firewall Analyzer supports the Access Control family as follows:

NIST 800-171 Control	AlgoSec Feature	Setting	Details	Status
3.1.1 Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems). **3.1.2** Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	VPN Analysis	On	Landau - - Misezhnikov - - Lieberman_root - -	*
	AlgoSec Administrators	On	The following users have administration permissions on the AlgoSec Firewall Analyzer: Morty the Administrator lemon Asher B Samuels Adi hila_test1 Adi	*
	-	-	An implicit final "drop rule" is the default behavior for Fortinet FortiManager	✓
3.1.3 Control the flow of CUI in accordance with approved	-	10.20.106.1	Firewalls and routers are key information system assets and their security policies need to be reviewed for risk.	

eport/10_20_106_1-73/optimize-policy

NIST SP 800-53

The AlgoSec Firewall Analyzer NIST Special Publication 800-53 Compliance report uses the National Institute of Standards and Technology (NIST) Security and Privacy Controls for Federal Information Systems and Organizations , Revision 4 (April 2013). FIPS Publication 200, Minimum Security Requirements for Federal Information and Information Systems , is a mandatory federal standard developed by NIST in response to FISMA. To comply with the federal standard, organizations first determine the security category of their information system in accordance with FIPS Publication 199, Standards for Security Categorization of Federal Information and Information Systems, derive the information system impact level (High, Moderate or Low) from the security category in accordance with FIPS 200, and then apply the appropriately tailored set of baseline security controls in NIST Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations.



Family: Access Control

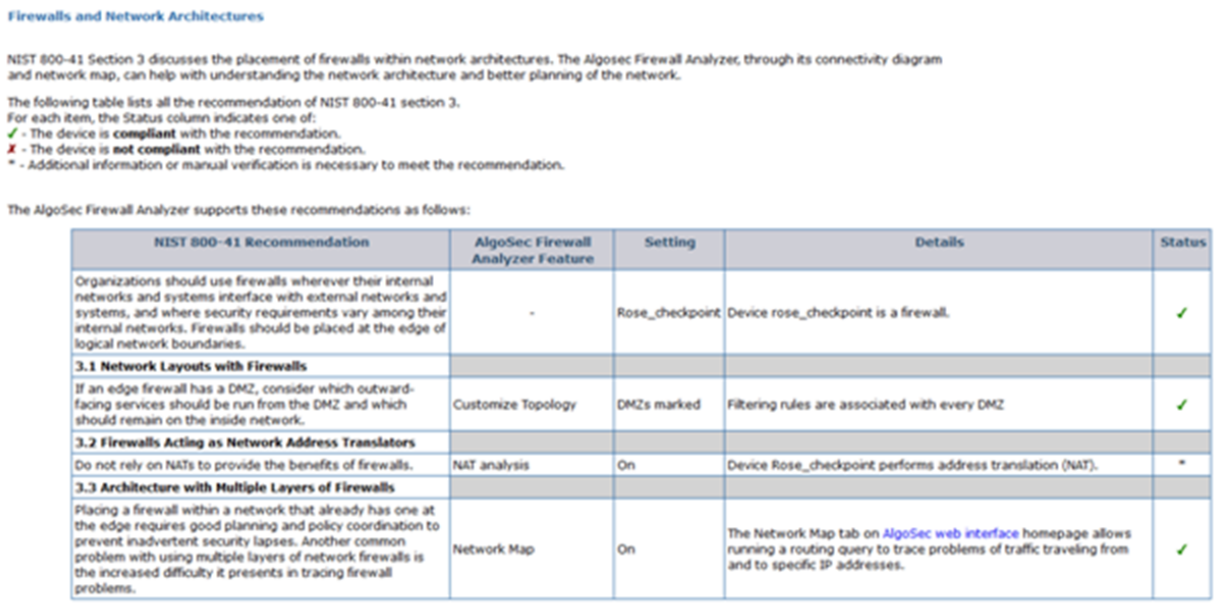
The following table lists all the items of NIST Access Control Family. For each item, the Status column indicates one of:
✓ - The device is **compliant** with the control.
✗ - The device is **not compliant** with the control.
* - Additional information or manual verification is necessary to meet the control.

The AlgoSec Firewall Analyzer supports the Access Control family controls as follows:

NIST 800-53 Control	AlgoSec Firewall Analyzer Feature	Setting	Details	Status
AC-2 ACCOUNT MANAGEMENT The organization:				
b. Assigns account managers for information system accounts;	AlgoSec Administrators	On	The following users have administration permissions on the AlgoSec Firewall Analyzer: AlgoSec Administrator FA afademo Ned NetOps	*
g. Monitors the use of, information system accounts;	Users	On	The following user names are defined on AlgoSec Firewall Analyzer and have access to Rose_checkpoint: AlgoSec Administrator (Standard) FA (Standard) harry helpdesk (Read only) Sue Security (Standard) afademo (Standard) FireFlow (Standard) Ned NetOps (Standard)	✓
AC-3 ACCESS ENFORCEMENT The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.	-	-	An implicit final "drop rule" is the default behavior for Check Point NGX (R61), Hotfix 601 - Build 005	✓
AC-6 LEAST PRIVILEGE The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.	Access Control	On	By default firewalls deny access unless specified otherwise. [This control is not relevant to the Low information system impact level.]	✓
AC-8 SYSTEM USE NOTIFICATION The information system: **a.** Displays to users *organization-defined system use notification message or banner* before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance	Baseline Compliance	On	This information is included in the AlgoSec Baseline Configuration report. The baseline profile configured on this device is: ckp-baseline Click here to enter the report and check if the requirement is met or not. Baseline requirements: 3 successful, 0 failed.	✓ *
AC-10 CONCURRENT SESSION CONTROL The information system limits the number of concurrent sessions for each *organization-defined account and/or account type* to an *organization-defined number*.	Baseline Compliance	On	This information is included in the AlgoSec Baseline Configuration report. The baseline profile configured on this device is: ckp-baseline Click here to enter the report and check if the requirement is met or not. Baseline requirements: 3 successful, 0 failed.	✓ *
AC-11 SESSION LOCK The information system: **a.** Prevents further access to the system by initiating a session lock after *organization-defined time period* of inactivity or upon receiving a request from a user; and **b.** Retains the session lock until the user reestablishes access using established identification and authentication procedures.	Baseline Compliance	On	This information is included in the AlgoSec Baseline Configuration report. The baseline profile configured on this device is: ckp-baseline Click here to enter the report and check if the requirement is met or not. Baseline requirements: 3 successful, 0 failed.	✓ *
AC-12 SESSION TERMINATION The information system automatically terminates a user session after *organization-defined conditions or trigger events requiring session disconnect*.	Baseline Compliance	On	This information is included in the AlgoSec Baseline Configuration report. The baseline profile configured on this device is: ckp-baseline Click here to enter the report and check if the requirement is met or not. Baseline requirements: 3 successful, 0 failed.	✓ *
AC-17 REMOTE ACCESS The organization: **a.** Establishes and documents usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and **b.** Authorizes remote access to the information system prior to allowing such connections.	VPN Analysis	On	See the VPN Analysis report for details regarding user's remote access rights through device Rose_checkpoint .	*
AC-21 USE OF EXTERNAL INFORMATION SYSTEMS The organization establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to: **a.** Access the information system from external information systems; and **b.** Process, store, or transmit organization-controlled information using external information systems.	Allowed services	On	Click here to view the list of open services from Outside to Inside and from Outside to DMZs.	*

NIST SP 800-41

The AlgoSec Firewall Analyzer NIST Special Publication 800-41 Compliance report uses the National Institute of Standards and Technology (NIST) Guidelines on Firewalls and Firewall Policy , Revision 1 (Sep 2009).



Firewalls and Network Architectures

NIST 800-41 Section 3 discusses the placement of firewalls within network architectures. The Algosec Firewall Analyzer, through its connectivity diagram and network map, can help with understanding the network architecture and better planning of the network.

The following table lists all the recommendation of NIST 800-41 section 3.
For each item, the Status column indicates one of:
✓ - The device is **compliant** with the recommendation.
✗ - The device is **not compliant** with the recommendation.
* - Additional information or manual verification is necessary to meet the recommendation.

The AlgoSec Firewall Analyzer supports these recommendations as follows:

NIST 800-41 Recommendation	AlgoSec Firewall Analyzer Feature	Setting	Details	Status
Organizations should use firewalls wherever their internal networks and systems interface with external networks and systems, and where security requirements vary among their internal networks. Firewalls should be placed at the edge of logical network boundaries.	-	Rose_checkpoint	Device rose_checkpoint is a firewall.	✓
3.1 Network Layouts with Firewalls				
If an edge firewall has a DMZ, consider which outward-facing services should be run from the DMZ and which should remain on the inside network.	Customize Topology	DMZs marked	Filtering rules are associated with every DMZ	✓
3.2 Firewalls Acting as Network Address Translators				
Do not rely on NATs to provide the benefits of firewalls.	NAT analysis	On	Device Rose_checkpoint performs address translation (NAT).	*
3.3 Architecture with Multiple Layers of Firewalls				
Placing a firewall within a network that already has one at the edge requires good planning and policy coordination to prevent inadvertent security lapses. Another common problem with using multiple layers of network firewalls is the increased difficulty it presents in tracing firewall problems.	Network Map	On	The Network Map tab on AlgoSec web interface homepage allows running a routing query to trace problems of traffic traveling from and to specific IP addresses.	✓

Gramm-Leach-Bliley Act (GLBA)

This report uses the Information Security IT Booklet issued by the Federal Financial Institutions Examination Council (FFIEC) in order to comply with the GLBA Safeguards Rule (section 501(b)).

Information Security Risk Assessment

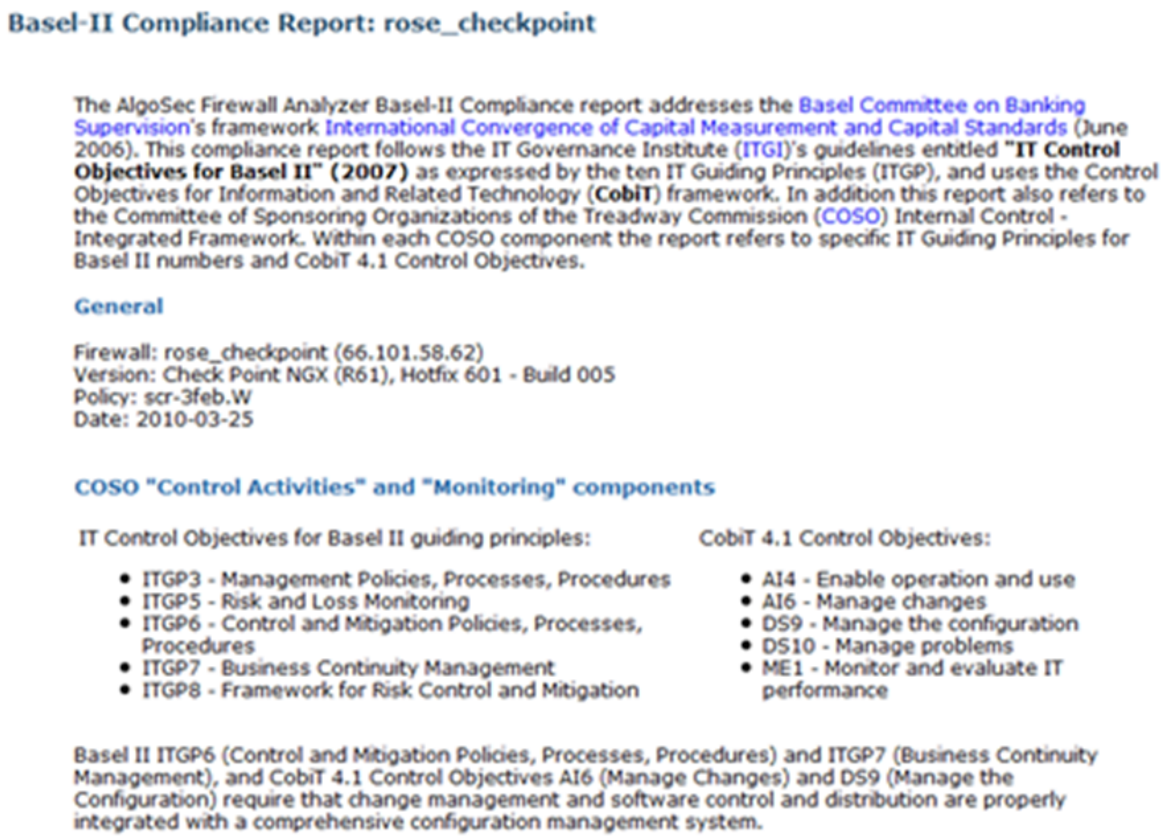
The first area of the FFIEC Information Security IT Booklet, Information Security Risk Assessment, indicates that Financial institutions must maintain an ongoing information security risk assessment program. The AlgoSec Firewall Analyzer, through its Risk Management and Connectivity Diagram, can help with implementing risk assessment and better planning of the network.

The following table lists all the recommendation of the Information Security Risk Assessment section. For each item, the Status column indicates one of:
✓ - The device is **compliant** with the requirement.
✗ - The device is **not compliant** with the requirement.
* - Additional information or manual verification is necessary to meet the requirement.

FFIEC Recommendation	AlgoSec Firewall Analyzer Feature	Setting	Details	Status
1. Gather Necessary Information	Data Collection	On	The AlgoSec Firewall Analyzer collects and stores the device's configuration, policies and rule sets. The collected data is available from the raw files page.	✓
	Network Map	On	The Network Map tab is available on AlgoSec web interface homepage.	✓
2. Identification of Information and Information Systems	Network Map	On	The AlgoSec Firewall Analyzer calculates a graphic network map that includes all of the devices in the system, as well as the networks and routers that are directly connected to them.	✓
	Connectivity Diagram	On		✓
3. Analyze the Information				
3.1 Assess Threats and Vulnerabilities	Risk Analysis	On	Risks found: 3 high risks, 10 suspected high risks, 23 medium risks, 7 low risks See the Offline Security Scan results below for details. For details regarding the controls used in conjunction with the risk profile see the Risk Assessment Criteria	✗
3.2 Evaluate Control Effectiveness	Scheduled Analysis	Off	The Algosec Firewall Analyzer produces reports that include detailed examination of devices configuration, policies, risk assessment and also VPN access. Analysis is run	✗
4. Assign Risk Ratings	Security Rating	On	 Each of the AlgoSec risks has a severity level varying from high to low. The AlgoSec Firewall Analyzer aggregates the individual risk levels into a single Security Rating.	✓
5. Key Risk Assessment Practices	Risk Profile	On	The AlgoSec Standard Risk Profile is a knowledge base of risk items that is included with the AlgoSec Firewall Analyzer. The risk items and their severities are derived from a variety of sources including industry best practices, regulatory guidelines, and AlgoSec internal resources.	✓

Basel-II

This page addresses the Basel Committee on Banking Supervision's framework International Convergence of Capital Measurement and Capital Standards (June 2006). It follows the IT Governance Institute (ITGI)'s guidelines entitled "IT Control Objectives for Basel II" (2007) as expressed by the ten IT Guiding Principles (ITGP), and uses the Control Objectives for Information and Related Technology (CobiT) framework. In addition this report also refers to the Committee of Sponsoring Organizations of the Treadway Commission (COSO) Internal Control - Integrated Framework. Within each COSO component the report refers to specific IT Guiding Principles for Basel II numbers and CobiT 5 Control Objectives.



Basel-II Compliance Report: rose_checkpoint

The AlgoSec Firewall Analyzer Basel-II Compliance report addresses the Basel Committee on Banking Supervision's framework International Convergence of Capital Measurement and Capital Standards (June 2006). This compliance report follows the IT Governance Institute (ITGI)'s guidelines entitled **"IT Control Objectives for Basel II" (2007)** as expressed by the ten IT Guiding Principles (ITGP), and uses the Control Objectives for Information and Related Technology (**CobiT**) framework. In addition this report also refers to the Committee of Sponsoring Organizations of the Treadway Commission (COSO) Internal Control - Integrated Framework. Within each COSO component the report refers to specific IT Guiding Principles for Basel II numbers and CobiT 4.1 Control Objectives.

General

Firewall: rose_checkpoint (66.101.58.62)
Version: Check Point NGX (R61), Hotfix 601 - Build 005
Policy: scr-3feb.W
Date: 2010-03-25

COSO "Control Activities" and "Monitoring" components

IT Control Objectives for Basel II guiding principles:

- ITGP3 - Management Policies, Processes, Procedures
- ITGP5 - Risk and Loss Monitoring
- ITGP6 - Control and Mitigation Policies, Processes, Procedures
- ITGP7 - Business Continuity Management
- ITGP8 - Framework for Risk Control and Mitigation

CobiT 4.1 Control Objectives:

- AI4 - Enable operation and use
- AI6 - Manage changes
- DS9 - Manage the configuration
- DS10 - Manage problems
- ME1 - Monitor and evaluate IT performance

Basel II ITGP6 (Control and Mitigation Policies, Processes, Procedures) and ITGP7 (Business Continuity Management), and CobiT 4.1 Control Objectives AI6 (Manage Changes) and DS9 (Manage the Configuration) require that change management and software control and distribution are properly integrated with a comprehensive configuration management system.

ASD ISM

This page describes how well your current AFA configuration settings comply with the Australian Signals Directorate's strategies to mitigate targeted cyber intrusions.

Mitigation Strategies

The following table lists all the mitigation strategies of ASD.
For each item, the Status column indicates one of:
✓ - The device is **compliant** with the recommendation.
✗ - The device is **not compliant** with the recommendation.
* - Additional information or manual verification is necessary to meet the recommendation.

The AlgoSec Firewall Analyzer supports these mitigation strategies as follows:

Mitigation Strategy	AlgoSec Firewall Analyzer Feature	Setting	Details	Status
1. Application whitelisting of permitted/trusted programs, to prevent execution of malicious or unapproved programs including .DLL files e.g. using Microsoft AppLocker.	Risk Analysis	On	The AlgoSec Firewall Analyzer check for risks that can be mitigated within the network. Risks found: 3 high risks, 10 suspected high risks, 23 medium risks, 7 low risks See the Offline Security Scan results below for details. For details regarding the controls used in conjunction with the risk profile see the Risk Assessment Criteria.	✗
	Risk Profile	On	The Algosec Firewall Analyzer uses the Perimeter.xml Revision: 1.27 risk profile on Rose_checkpoint.	✓
	Security Rating	On	Security Rating: 40% 	✓
3. Patch operating system vulnerabilities. Patch or mitigate "extreme risk" vulnerabilities within two days. Avoid continuing to use Microsoft Windows XP or earlier versions.	Risk Analysis	On	The AlgoSec Firewall Analyzer risk check helps find devices that have software that is unsupported installed on them. Please review the End of Maintenance risks table below.	*
4. Minimise the number of users with domain or local administrative privileges. Such users should use a separate unprivileged account for email and web browsing.	AlgoSec Administrators	On	The following users have administration permissions on the AlgoSec Firewall Analyzer: AlgoSec Administrator fA afademo Ned NetOps	*
6. Multi-factor authentication especially implemented for remote access, or when the user is about to perform a privileged action or access a sensitive information repository.	VPN Analysis	On	See the VPN Analysis report for details regarding remote access rights through firewall Rose_checkpoint	*
7. Network segmentation and segregation into security zones to protect sensitive information and critical services such as user authentication and user directory information.	Customize Topology	DMZs marked	Filtering rules are associated with every DMZ	✓
8. Application based workstation firewall, configured to deny traffic by default, to protect against malicious or otherwise unauthorized incoming network traffic.	-	-	An implicit final "drop rule" is the default behavior for Check Point NGX (R61), Hotfix 601 - Build 005.	✓
9. Application based workstation firewall, configured to deny traffic by default, that whitelists which applications are allowed to generate outgoing network traffic.	-	-	An implicit final "drop rule" is the default behavior for Check Point NGX (R61), Hotfix 601 - Build 005.	✓
10. Non-persistent virtualised trusted operating environment, hosted within the organisation's Internet gateway, for risky activities such as reading email and web browsing.	Customize Topology	DMZs marked	Filtering rules are associated with every DMZ	✓
13. Centralised and time-synchronised logging of allowed and blocked network activity, with automated immediate log analysis, storing logs for at least 18 months.	No-Log rules	On	Rules with no logs: 1 . Click here to view	✗
	Delete Reports	Off	The AlgoSec Firewall Analyzer retains reports for a user defined period. In the current configuration reports are not deleted. Please make sure that the above matches the organization-defined time period. In order to change these settings go to the administration screen, click on options tab and then go to storage.	*
	Baseline Compliance	On	The Baseline configuration report can check for NTP settings configured on the device. The baseline profile configured on this device is: ckp-baseline Click here to enter the report and check if the requirement is met or not. Baseline requirements: 3 successful, 0 failed.	✓ *
14. Whitelisted email content filtering, only allowing business related attachment types. Preferably analyse/convert/sanitise hyperlinks, PDF and Microsoft Office attachments.	Risk Analysis	On	To ensure that the email filter is not bypassed you need to ensure that email can only enter and exit your network through the designated mail gateways. The AlgoSec Firewall Analyzer risk check helps you check if protocols such as POP, IMAP, and SMTP are allowed through the firewall, please review the Email Configuration risks table below for further details.	*
16. Web domain whitelisting for all domains, since this approach is more proactive and thorough than blacklisting a tiny percentage of malicious domains.	Allowed services	On	Click here to view the list of open services from Outside to Inside and from Inside to Outside.	✓
17. Web domain whitelisting for HTTPS/SSL domains, since this approach is more proactive and thorough than blacklisting a tiny percentage of malicious domains.	Allowed services	On	Click here to view the list of open services from Outside to Inside and from Inside to Outside.	✓
22. Computer configuration management based on a hardened Standard Operating Environment with unrequired operating system functionality disabled e.g. IPv6 and autorun.	Baseline Compliance	On	The Baseline configuration report is based on various per vendor hardening guides. The baseline profile configured on this device is: ckp-baseline Click here to enter the report and check if the requirement is met or not. Baseline requirements: 3 successful, 0 failed.	✓ *
24. Deny direct Internet access from workstations by using an IPv6-capable firewall to force traffic through a split DNS server, an email server, or an authenticated web proxy.	IPv6 Rules	-	-	*
27. Enforce a strong passphrase policy covering complexity, length, and avoiding both passphrase reuse and the use of dictionary words.	Baseline Compliance	On	The Baseline configuration report can check length and complexity of configured passwords. The baseline profile configured on this device is: ckp-baseline Click here to enter the report and check if the requirement is met or not. Baseline requirements: 3 successful, 0 failed.	✓ *
28. Restrict access to Server Message Block (SMB) and NetBIOS services running on workstations and on servers where possible.	Risk Analysis	On	The AlgoSec Firewall Analyzer risk check helps find devices that allow access to Microsoft's NetBIOS services. Please review the NetBIOS risks table below.	✓
31. Disable LanMan passphrase support and cached credentials on workstations and servers, to make it harder for adversaries to crack passphrase hashes.	Baseline Compliance	On	The Baseline configuration report can check length and complexity of configured passwords. The baseline profile configured on this device is: ckp-baseline Click here to enter the report and check if the requirement is met or not. Baseline requirements: 3 successful, 0 failed.	✓ *
34. Gateway blacklisting to block access to known malicious domains and IP addresses, including dynamic and other	-	-	An implicit final "drop rule" is the default behavior for Check Point NGX (R61), Hotfix 601 - Build 005.	✓

Financial Instruments and Exchange Law (Japan)

Like the AlgoSec Sarbanes-Oxley report, this page explains how your current AFA configuration settings support CobiT 5 control objectives, in the Japanese language. Use this report to learn how well you are doing, and to present to your auditors as needed.

The first part of the report deals with automation and monitoring, and the control objectives that require them. The report tabulates the details of the AFA automation capabilities that you have turned on. The next part of the report deals with risk management, and the control objectives that relate to risk. In this part you can see the general risk management settings you have in place, followed by the *full* list of all the risks that AFA searched for in the current report. The **Status** column tells you if the risk was found (indicated with a red X) or if your device is compliant with respect to this risk (indicated with a green check mark). All risks that are found appear with their details in the AFA front page.

Note: If you see the titles of the risk items in English it means that you are using the English language pack.

CobiT 4.1 のコントロール目標 AI6 (変更管理) 及び DS9 (構成管理) は、変更管理とソフトウェアコントロールと配布が、網羅的な構成マネジメントシステムと適切に統合されていることを要求している。AlgoSec ファイアウォールアナライザーは、オートメーションスィートを通じて、これらのコントロール目標を多種多様な方法 (複数のファイアウォールは異なる周期において分析可能、変更は自動的に報告可能) でサポートしている。これらの変更は、要求された承認済みのファイアウォール変更要求のみが実行されることを保証する変更要求フォームに適合するものである。電子メール通知は変更イベントが発生し、詳細な変更履歴が自動的に維持された時に送られるものとする。

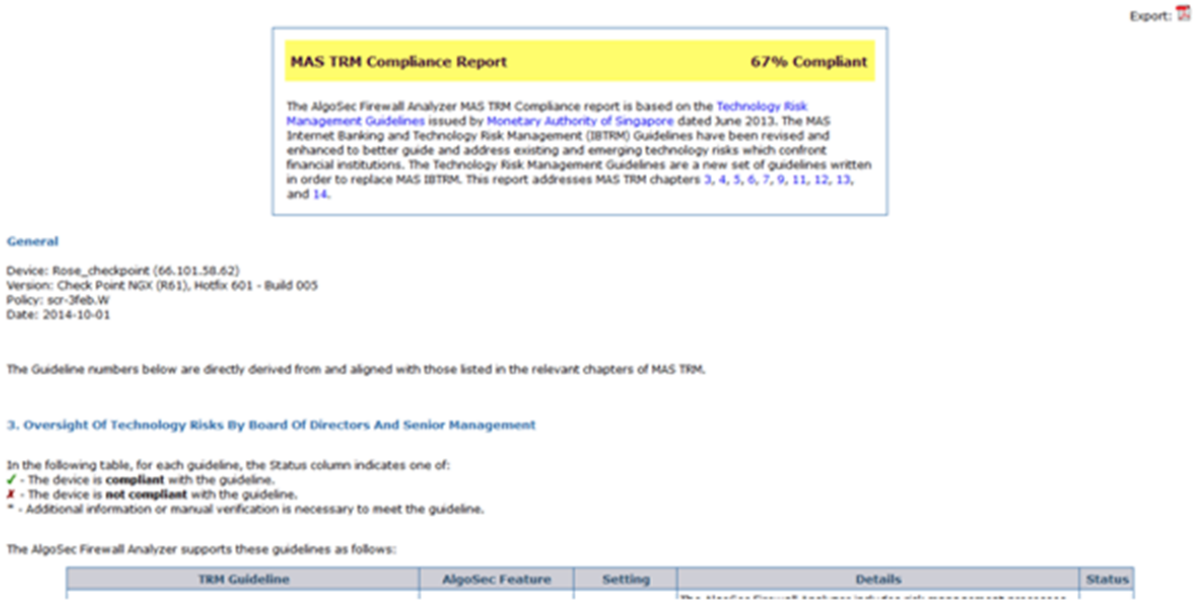
オートメーション及びモニタリング設定

AlgoSec ファイアウォールの特徴	設定	詳細	ステイタス
変更履歴	On	Records available since 2008-08-18	✓
スケジュールされた分析	Off		✗
電子メール通知	On	AlgoSec Administrator: Report is ready, Real time alerting Sue Security: Report is ready, Real time alerting afademo: Report is ready, Real time alerting Ned NetOps: Report is ready, Real time alerting	✓
隠れたルール分析	On	[*]	✓
未使用ルール分析	Off		✗
未接続目標分析	On	[*]	✓
無効 / タイムアウトルール	On	[*]	✓
No-Log/No-Comment Rules	On	[*]	✓

[*] これらの特徴はポリシーオプティマイゼイション分析として常時アクティブになっている。

MAS TRM

This page describes how well your current AFA configuration settings comply with the Technology Risk Management Guidelines issued by Monetary Authority of Singapore dated June 2013.


Export:

MAS TRM Compliance Report **67% Compliant**

The AlgoSec Firewall Analyzer MAS TRM Compliance report is based on the Technology Risk Management Guidelines issued by Monetary Authority of Singapore dated June 2013. The MAS Internet Banking and Technology Risk Management (IBTRM) Guidelines have been revised and enhanced to better guide and address existing and emerging technology risks which confront financial institutions. The Technology Risk Management Guidelines are a new set of guidelines written in order to replace MAS IBTRM. This report addresses MAS TRM chapters 3, 4, 5, 6, 7, 9, 11, 12, 13, and 14.

General

Device: Rose_checkpoint (66.101.58.62)
Version: Check Point NGX (R61), Hotfix 601 - Build 005
Policy: scr-3feb.W
Date: 2014-10-01

The Guideline numbers below are directly derived from and aligned with those listed in the relevant chapters of MAS TRM.

3. Oversight Of Technology Risks By Board Of Directors And Senior Management

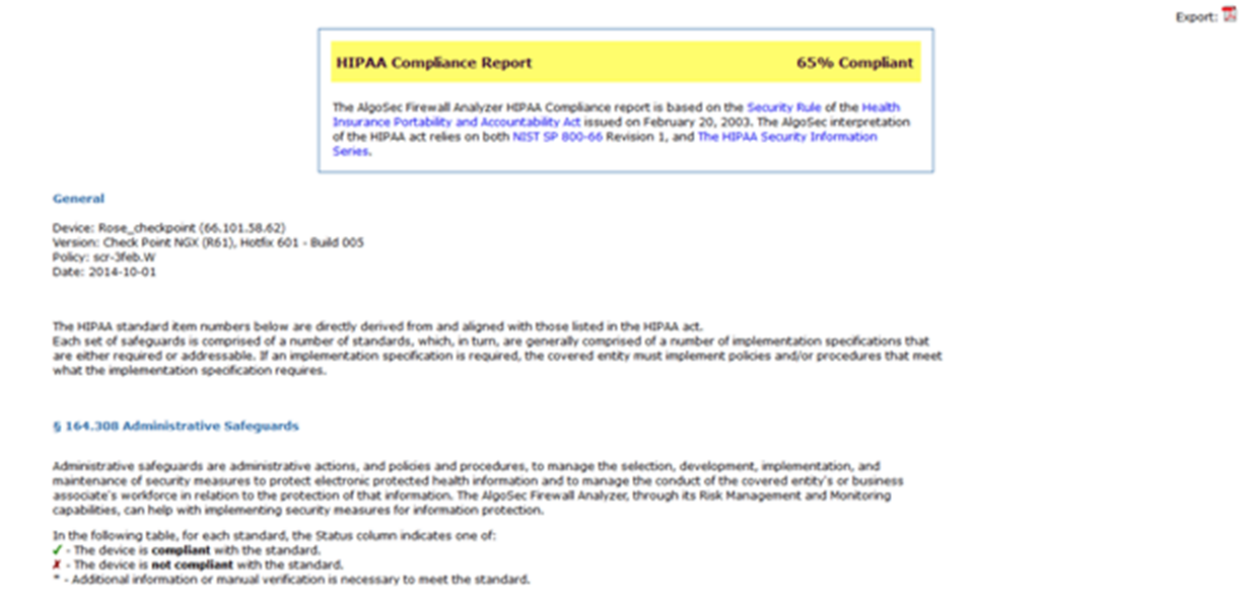
In the following table, for each guideline, the Status column indicates one of:
✓ - The device is **compliant** with the guideline.
✗ - The device is **not compliant** with the guideline.
* - Additional information or manual verification is necessary to meet the guideline.

The AlgoSec Firewall Analyzer supports these guidelines as follows:

TRM Guideline	AlgoSec Feature	Setting	Details	Status

HIPAA

This page describes how well your current AFA configuration settings comply with the Security Rule of the Health Insurance Portability and Accountability Act issued on February 20, 2003. The AlgoSec interpretation of the HIPAA act relies on both NIST SP 800-66 Revision 1, and The HIPAA Security Information Series.


Export:

HIPAA Compliance Report 65% Compliant

The AlgoSec Firewall Analyzer HIPAA Compliance report is based on the Security Rule of the Health Insurance Portability and Accountability Act issued on February 20, 2003. The AlgoSec interpretation of the HIPAA act relies on both NIST SP 800-66 Revision 1, and The HIPAA Security Information Series.

General

Device: Rose_checkpoint (66.101.58.62)
Version: Check Point NGX (R61), Hotfix 601 - Build 005
Policy: scr-3feb.W
Date: 2014-10-01

The HIPAA standard item numbers below are directly derived from and aligned with those listed in the HIPAA act.
Each set of safeguards is comprised of a number of standards, which, in turn, are generally comprised of a number of implementation specifications that are either required or addressable. If an implementation specification is required, the covered entity must implement policies and/or procedures that meet what the implementation specification requires.

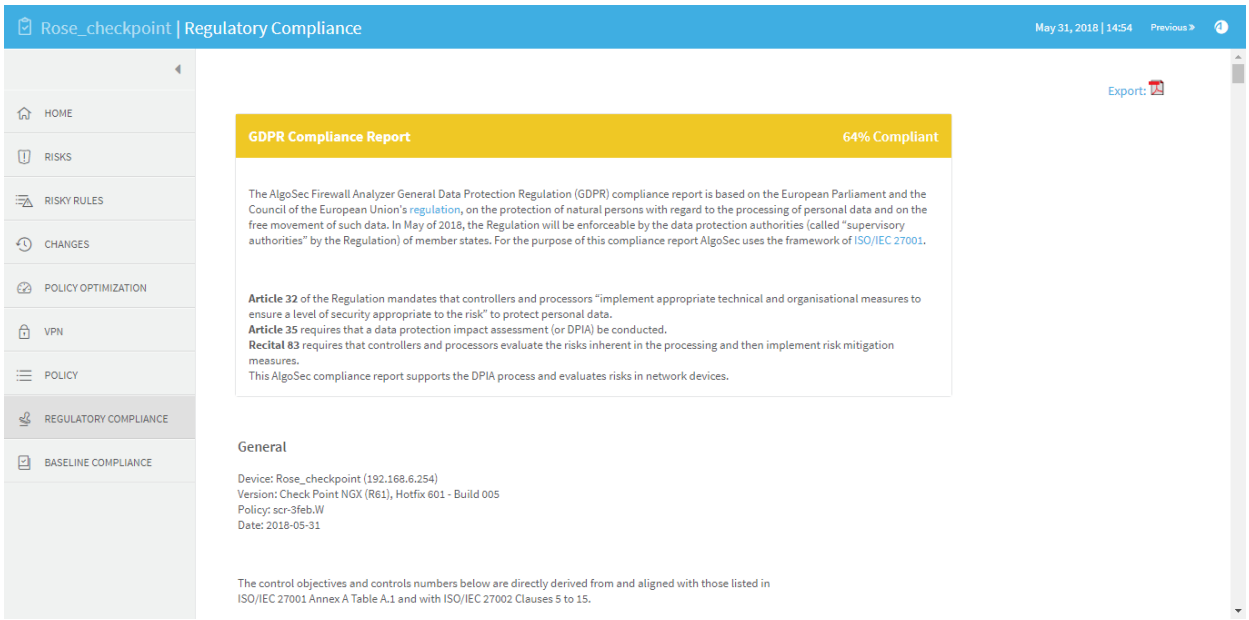
§ 164.308 Administrative Safeguards

Administrative safeguards are administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's or business associate's workforce in relation to the protection of that information. The AlgoSec Firewall Analyzer, through its Risk Management and Monitoring capabilities, can help with implementing security measures for information protection.

In the following table, for each standard, the Status column indicates one of:
✓ - The device is **compliant** with the standard.
✗ - The device is **not compliant** with the standard.
* - Additional information or manual verification is necessary to meet the standard.

GDPR

The AlgoSec Firewall Analyzer General Data Protection Regulation (GDPR) compliance report is based on the European Parliament and the Council of the European Union's regulation, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

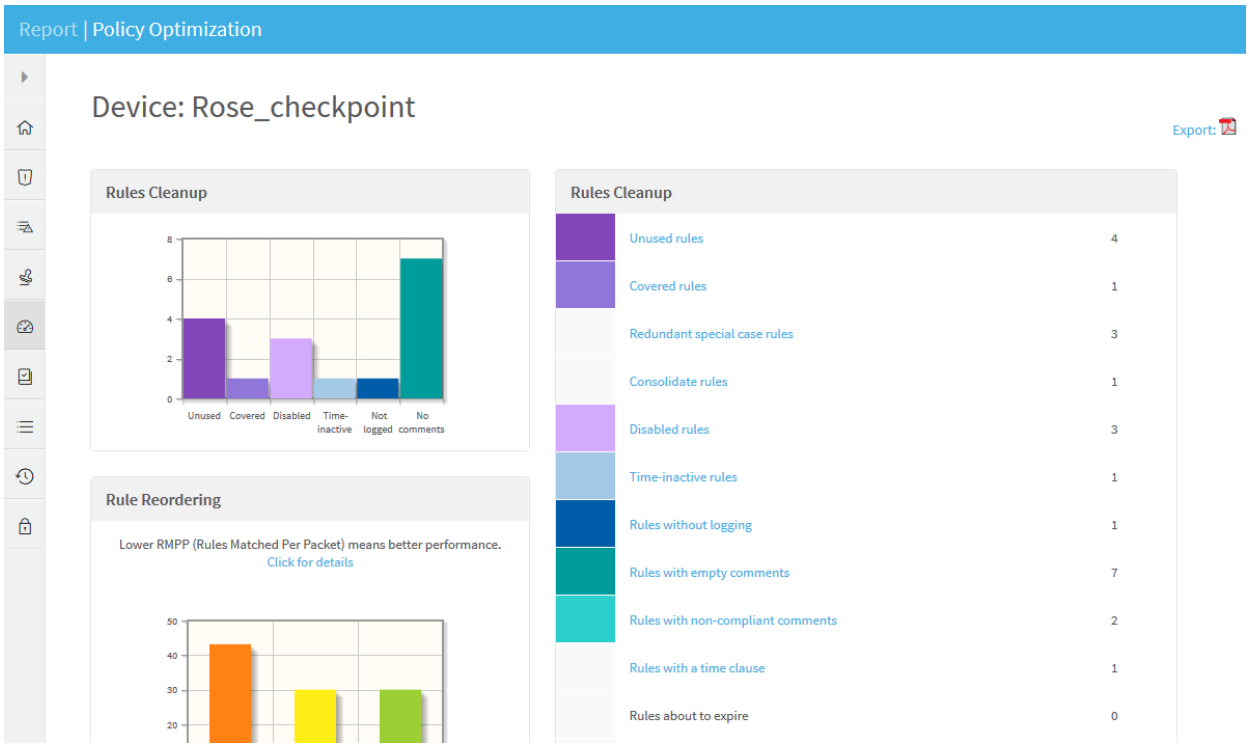


POLICY OPTIMIZATION page

To optimize your policy, you need to find out which rules are redundant, unused or already covered by other, more general rules. These rules are prime candidates for removal from your device policy. In addition, you need to see the statistics on the most and least used rules of a policy: the device's performance may improve if highly used rules are placed near the top of the rule-set, and infrequently used rules are moved further down. In addition, you need to know about unused and empty host group definitions and unused access lists, because these unused definitions clutter up the configuration and reduce your ability to manage your devices effectively.

Note: For Panorama or FortiManager devices, usage on a specific rule in a specific device will reflect the counts of all the devices that share this policy.

To view a training video that follows an Information Security Officer optimizing his organization's firewall policies, see Performing Policy Optimization (https://portal.algosec.com/en/training_academy/policy_optimization_online_training).



In the **Policy Optimization** page, you can view the rules and objects which diminish your policy's effectiveness and efficiency. Additionally, a graphic display of the number of unused, time-inactive, un-logged and rules already covered by other rules is provided.

When you click on a link in the **Rules Cleanup** area all of the relevant rules appear. The columns which appear for each rule are specific to each device brand. If AppViz is licensed, fields from AppViz appear, indicating business information such as which rules are included as flows in which applications.

Below is a description of the different areas of the **Policy Optimization** page, including a summary of the types of rules and objects that can make a policy perform sub-optimally:

Rules Cleanup

Rules Cleanup enables the user to make your policy more streamlined and effective. It may include the following:

Unused rules

Rules that did not match any traffic according to the log data. By default, log data is kept for 60 days back. For Check Point and Juniper, this analysis is based on the collected logs. For Cisco Routers, AFA recognizes unused rules based on the access-list match counters.

> **Note:** The match counters are collected every time the analysis runs, and their values are saved by AFA to allow long-term usage analysis (even when the device resets and counters are cleared).

If FireFlow is installed, you can open a FireFlow change request to disable these rules directly from the report. See Disabling Device Rules (see Disabling Device Rules).

Covered rules

Rules that are covered by other, more general rules. A rule is covered if there is a combination of rules that are located above it in the rule set that together match all the traffic that could have been matched by the covered rule. As long as a rule is covered by

other rules, it will *never* match any traffic. Therefore, covered rules are good candidates for elimination from the policy.

Note: Check Point's SmartDashboard automatically performs a quick check for covered rules; however, this test does not go into any depth. In contrast, AFA will find covered rules even if it is covered by a combination of multiple rules, and even if the host and service group names on the rules are different (but the IP addresses and port numbers are the same). In Cisco Routers a rule may even be covered by a combination of rules that are located in other access lists and attached to other interfaces: AFA will report on these rules as well.

If FireFlow is installed, you can open a FireFlow change request to disable these rules directly from the report. See Disabling Device Rules (see Disabling Device Rules).

Clicking the **Covered rules** link will display each covered rule in a separate table along with the rules that cover it. The covered rule is at the bottom of the table (shaded in light gray).

Redundant special case rules

Rules that are included in a subsequent rule and can therefore be removed.

If FireFlow is installed, you can open a FireFlow change request to disable these rules directly from the report. See Disabling Device Rules (see Disabling Device Rules).

Note: When determining whether a rule is a redundant special case rule, AFA checks that both the rule and the subsequent rule that includes it have the same logging setting (enabled or disabled). If the setting is different, the rule will not be listed as a redundant special case rule. The logging setting is also examined when checking whether a rule is a consolidate rule. However, this setting is ignored for covered rules. If the traffic is caught by the first rule, it does not matter whether logging is enabled for the second rule, since the second rule will never be activated,

and therefore can be safely deleted.

Consolidate rules

Rules that can be consolidated into one rule because they are identical except for one field: source, destination or service. The rules that AFA recommends to consolidate will always be allowing rules.

If FireFlow is installed, you can open a FireFlow change request to consolidate rules on Cisco Firewalls directly from the report. If desired, you can edit the AFA recommendation before opening the change request. See Consolidating Device Rules (see Consolidating Device Rules).

Unrouted rules

Rules that are not routed through the device. A rule is unrouted if the entire source is not in the source zone, or the entire destination is not in the destination zone. Removing these rules will not affect the device's effective security policy.

Clicking the **Unrouted rules** link will display the rules in a table. The objects that are not in their respective zone appear highlighted.

Note: Unrouted rules are only supported for Juniper SRX, Juniper Netscreen, Juniper NSM, Palo Alto Networks, and Fortigate devices. Fortigate devices are not supported when defined in AFA via FortiManager, and SRX devices are not supported when defined in AFA, via Juniper Space.

Unrouted objects within rules

Rules with source objects that are not in the source zone or destination objects that are not in the destination zone. Removing these objects from the rules will not affect the device's effective security policy.

Clicking the **Unrouted objects within rules** link will display the rules in a table. The objects that are not in their respective zone appear highlighted.

Note: Unrouted objects within rules are only supported for Juniper SRX, Juniper Netscreen, Juniper NSM, Palo Alto Networks, and Fortigate devices. Fortigate devices are not supported when defined in AFA via FortiManager, and SRX devices are not supported when defined in AFA, via Juniper Space.

Disabled rules

Disabled rules are rules that were disabled temporarily.

Time-inactive rules

Time Inactive Rules are rules that only apply at certain dates or times - and are inactive at the time of analysis. Such rules are often leftovers from fix-time projects and temporary patches, and may be candidates for elimination.

Rules without logging

Rules without logging are rules that do not produce log records when they match packets. Many organizations require all, or nearly all, rules, to produce logs, thus a list of rules without a log keyword may let you ensure that your policy complies with your organization's requirements. With the exception of Cisco devices, these rules are always excluded from the list of unused rules since an absence of log records does not confirm that no traffic was matched.

Note: For Cisco devices, AFA does not rely on logs to determine if a rule is unused.

Rules with empty comments/Rules with no remarks

These rules are rules that do not have comments. Many organizations require all rules to have a comment indicating who wrote the rule, when, why, and with whose authorization. For Cisco Routers, AFA recognizes rules with empty comments based on

"set access-list remark" statements.

Rules with non-compliant comments

Many corporate policies dictate that rule comments must contain the ID number for the change request for which the rule was created or changed. AFA allows specifying a regular expression that matches these ticket numbers, and then presents the rules with non-compliant comments (no ticket number).

To configure this functionality, complete the **Report rules whose comment field...** field in the **General** sub-tab of the **Options** tab in the Administration area. For Cisco Routers, AFA recognizes rules with non-compliant comments based on "set access-list remark" statements.

Rules with a time clause

Rules with a time clause are rules that only apply at certain dates or times. Such rules may become redundant when their activity time passes (In which case they will be reported also as Time Inactive Rules).

Rules about to expire

These are rules that will expire within a certain number of days. To configure the number of days before expiration that a rule should be flagged as About to Expire, complete the **Days before expiration alerts** field in the **General** sub-tab of the **Options** tab in the Administration area. The default is 14 days.

Unused NAT rules (Check Point)

Unused NAT rules are rules that, according to the device logs, are not used by the device.

All NAT rules usage (Check Point)

Usage information about all NAT rules.

Redundant NAT rules (Check Point)

Redundant NAT rules translate traffic that is not permitted by any of the device policy rules.

Intelligent Policy Tuner

The Intelligent Policy Tuner (IPT) enables you to refine your policy, by identifying rules that are too wide and permissive, and rules which contain sparsely used and unused objects. It also provides recommendations for replacing permissive rules with new, tighter rules. See Refining Rules via the Intelligent Policy Tuner (see Refining Rules via the Intelligent Policy Tuner).

This area includes the following:

Tighten Permissive Rules	Permissive rules that should be refined.
Unused objects within rules	Rules containing objects that have not been used recently.
Policy tuner analysis for all rules	Usage information about all rules.

VPN Cleanup (Check Point)

For Check Point devices, the **Policy Optimization** page also includes several items that refer to the VPN analysis page (see The VPN Page (see VPN page)):

Expired users	Any VPN user whose access expiration date occurred before the report's date is flagged as Expired.
Users about to expire	Any VPN user whose access expiration date is a certain number of days after the report's date is flagged as About to Expire. To configure the number of days before expiration that a VPN user should be flagged as About to Expire, complete the **Days before expiration alerts** field in the **General** sub-tab of the **Options** tab in the Administration area.
Unattached user groups	VPN user groups that do not appear in any rule in any policy that is managed by the Check Point SmartCenter or CMA are flagged as an Unattached User Group.

Unattached users	Any VPN user that does not belong to any user group is flagged as Unattached. Such users do not have any real VPN access since no rule can refer to them.

Application Control Rules Cleanup (Check Point)

For Check Point devices, if there is at least one application control rule, the **Policy Optimization** page also includes information about application control rules:

Unused rules	Application control rules that did not match any traffic according to the log data.
Rules without logging	Application control rules that do not produce log records when they match packets.
Disabled rules	Application control rules that were disabled temporarily.
All rules usage (count, last date)	Usage information about all application control rules.

Rule Reordering

These areas provide recommendations for optimizing the device rules for best performance and lower CPU utilization, an estimate for the device's performance, and suggestions for improving the performance with the most effective rule reordering. For more information, see Reordering Rules (see Reordering Rules).

Rule Usage Statistics

In this area, you have access to the five most- and least-used rules. You can use this information to re-order your policy so the most popular rules are placed near the top of the rule set.

Policy optimization procedures

Removing Device Objects

If FireFlow is installed, you can submit an **Object Change** request to remove unattached, empty, and unused objects in the device's policy, as well as unrouted

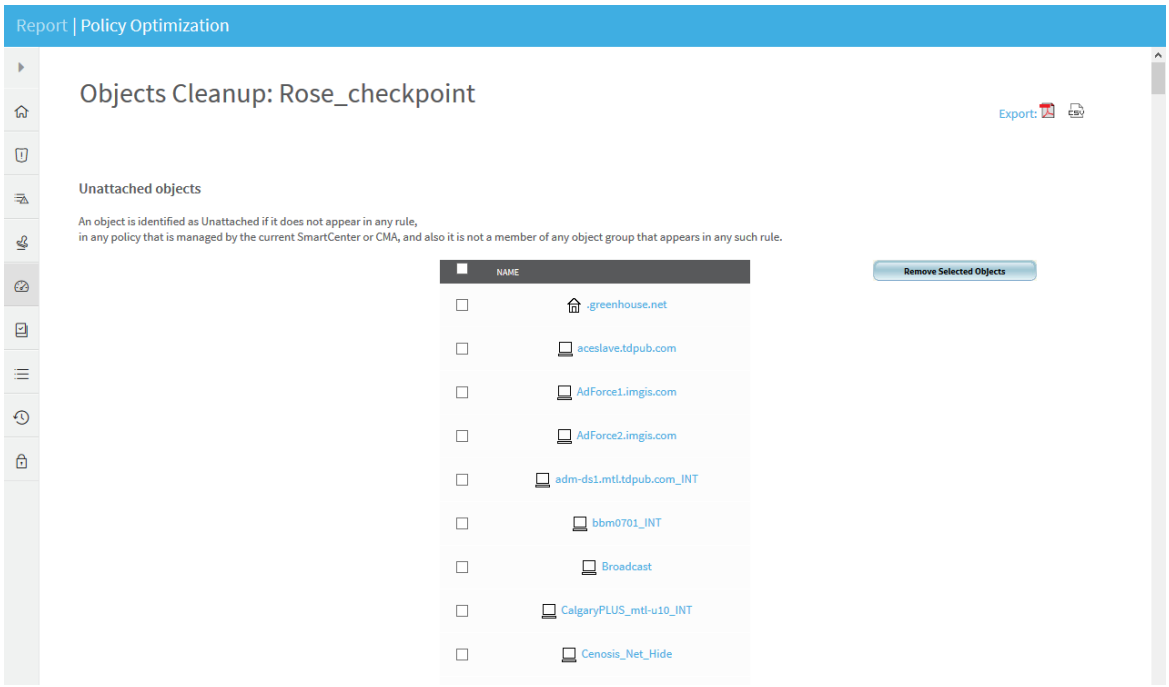
objects within rules, directly from the **Policy Optimization** page.

To open a FireFlow change request to remove objects

1. View the desired device's device report. For details, see View AFA device data.
2. Click the **Policy Optimization** tab.

   The **Policy Optimization** page appears.
3. Click on one of the supported object categories (**Unattached objects**, **Empty objects**, and **Unused objects**).

   The objects in the selected category appear.



4. Do one of the following:
   - In the first column, select the check boxes next to the objects you want to remove.
   - Select the check box in the table heading to select all objects.
5. Click **Remove Selected Objects**.

The change request is created, and a notification appears with a link to the change request.

If desired, the change request's fields may be modified later on.

Note: When you remove more than one object, one change request is opened with multiple object lines.

6. Click **OK**.

Consolidating Device Rules

If FireFlow is installed, you can consolidate rules on Cisco ASAdevices directly from the **Policy Optimization** page, by doing the following:

1. Open a FireFlow change request to add one or more consolidated rules, using the procedure below.

   The procedure describes two options:

   - Open the change request directly from the report.

     This option requires the **190:Verbatim Rule Addition** request template (which is based on the bulk rules addition workflow) to be active in FireFlow.

   - Download a CSV file which you can edit and then use to manually open the

change request in FireFlow.

You can manually open the change request with the the **190:Verbatim Rule Addition** request template or any custom template/workflow for adding rules to devices.

Once the change is implemented on the device, the next AFA report will automatically identify the original rules as redundant. They will appear in the report as **Redundant special case rules**.

2. Remove the redundant rules by opening another change request from the new report. See Disabling Device Rules (see Disabling Device Rules).

> **Note:** The original rules will only be marked as **Redundant special case rules** if there are no rules with a "deny" action below the lowest original rule.

To open a FireFlow change request to add consolidated rules

1. If not already configured, enable the **Access Lists** traffic field to the **190:Verbatim Rule Addition** FireFlow change request template, by doing the following:

> **Note:** When opening the change request directly from the AFA report, this is the only request template that can be used. If you use the AFA provided CSV file to manually open a change request (an option discussed below), you can use the **190:Verbatim Rule Addition** template or any custom template for adding rules to devices. The **Access Lists** traffic field must be enabled in the template you use.

   a. Switch to FireFlow. For details, see Switch ASMS products
   b. In the main menu, click **Request Templates**.

      The **Request Templates** page appears.
   c. Select the **190:Verbatim Rule Addition** template.

The template's settings appear.

d. In the **Traffic** area, click the **+Add or remove traffic fields** link.

The **Add or remove traffic fields** window appears.

e. In the **Traffic** area, select the **Access Lists** check box.

f. Click **Save**.

g. Click **Save template**.

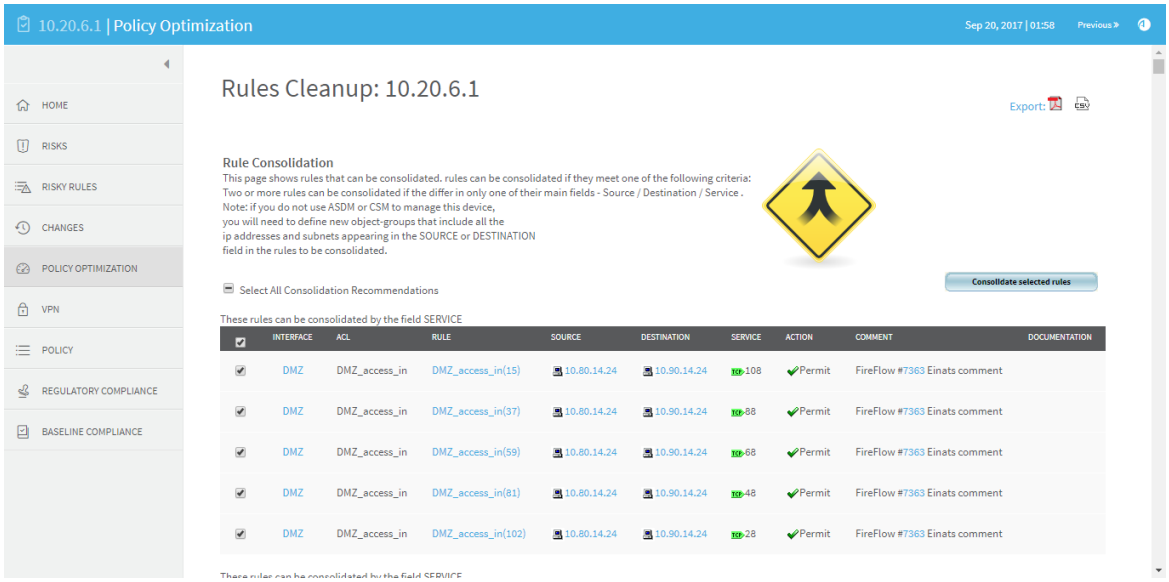
2. In AFA, view the desired device's device report. For more details, see View AFA device data.

3. Click the **PolicyOptimization** tab.

The **Policy Optimization** page appears.

4. Click **Consolidate rules**.

The consolidated rules appear. Each table represents a single consolidated rule and shows the existing rules it could replace.



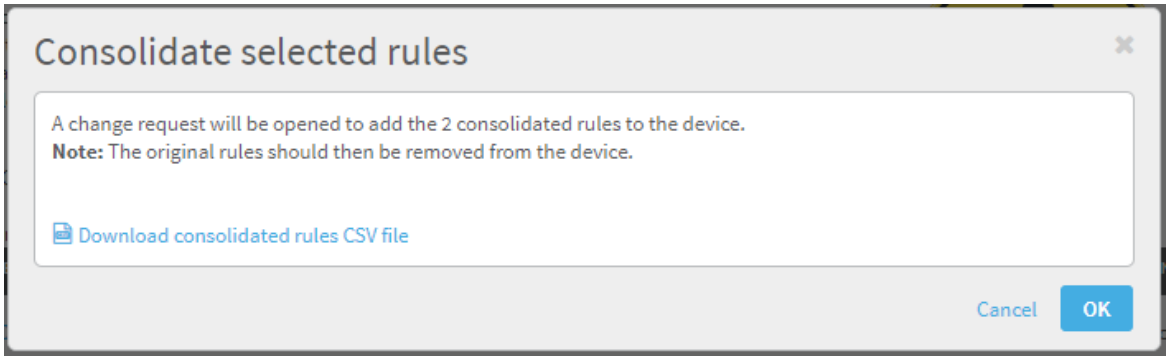
Each table of rules represents a group of rules you can consolidate into a single rule.

5. Select the rules you want to consolidate.

   You can choose all or only some of the rules from a table. Choosing rules from multiple tables will create a single change request for adding multiple consolidated rules, one for each table.

6. Click **Consolidate selected rules**.

   The **Consolidate selected rules** window appears.



7. Do one of the following:

   - To automatically open the change request, click **OK**.

     A confirmation window appears with the change request information.

   - To edit the consolidated rules before opening the change request, do the following:

     1. Download a CSV file with the consolidated rules you specified by clicking the **Download consolidated rules CSV file** link.
     2. Edit the file, as desired.
     3. Manually create a change request in FireFlow using the **190:Verbatim Rule Addition** request template.
     4. Populate the traffic area of the change request by clicking the **Import traffic from CSV** link and selecting the consolidated rules CSV file.
     5. Complete the other fields in the template and submit the change request.

Disabling Device Rules

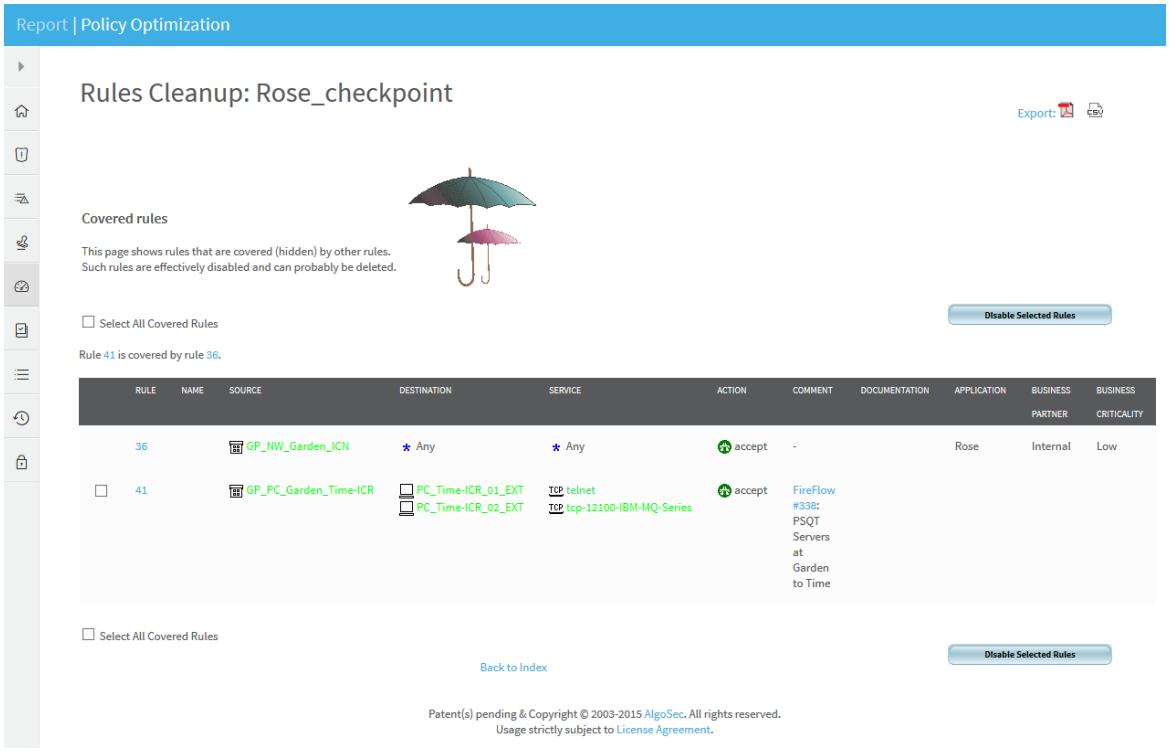
If FireFlow is installed, you can submit a **Rule Removal** request to disable redundant, unused, unrouted, and covered rules in the device's policy, directly from the **Policy Optimization** page.

To open a FireFlow change request to disable device rules

1. In AFA, view the desired device's device report. For more details, see View AFA device data.
2. Click the **PolicyOptimization** tab.

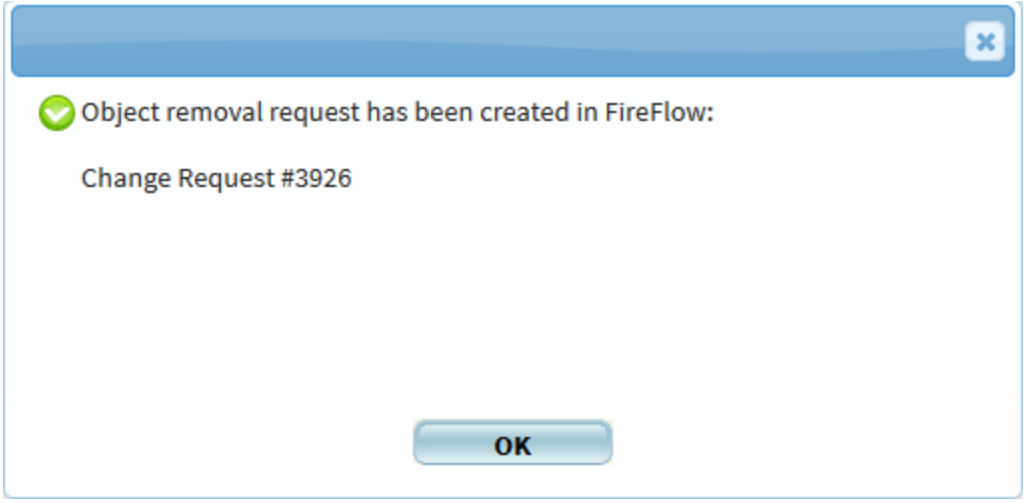
   The **Policy Optimization** page appears.
3. Click on one of the supported rule categories (**Unused rules**, **Covered rules**, **Redundant special case rules**, and **Unrouted rules**).

   The rules in the selected category appear.



4. Do one of the following:
    - In the first column, select the check boxes next to the rules you want to disable.
    - Select the **Select All Covered Rules/Select All Unused Rules/Select All Special Case Rules** check box to select all the rules.
5. Click **Disable Selected Rules**.

    The change request is created and a notification appears with a link to the change request.



    If desired, the change request's fields may be modified later on.

    Note: When you disable more than one rule, a separate change request is created for each rule.

6. Click **OK**.

Refining Rules via the Intelligent Policy Tuner

The **Policy Optimization** page's Intelligent Policy Tuner (IPT) enables you to refine your policy, by identifying rules that are too wide and permissive, and rules which contain sparsely used and unused objects. In addition, it provides recommendations for replacing permissive rules with new rules that are tighter, but which still allow all traffic

allowed by the original rules.

If desired, you can change how IPT generates recommendations for replacing permissive rules.

Note: The Intelligent Policy Tuner is only available for devices on which Extensive logging has been enabled. To enable **Extensive** logging, add or edit the desired device, and in the Log Analysis column, select **Extensive**.

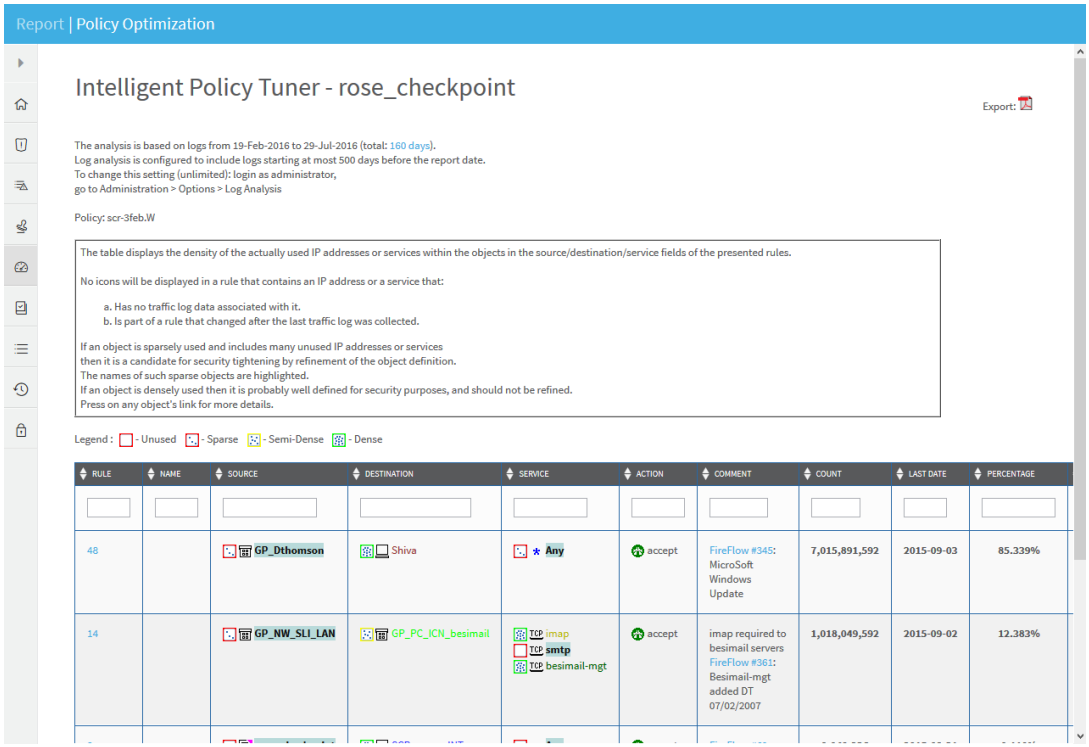
Note: Generating recommendations for replacing permissive rules may take a while, thus extending the report generation time. If desired, you can disable this feature. .

To refine rules

1. In the **Policy Optimization** page's **Intelligent Policy Tuner** area, do one or more of the following:

   - To view overly permissive rules, click **Tighten Permissive Rules**.

     The **Intelligent Policy Tuner** page appears.



A table displays a list of permissive rules that should be refined. For information on the columns, see the table below.

Icons appear next to the objects in each rule, indicating the object's degree of use. You can mouse-over the icons to view the exact percentage of use.

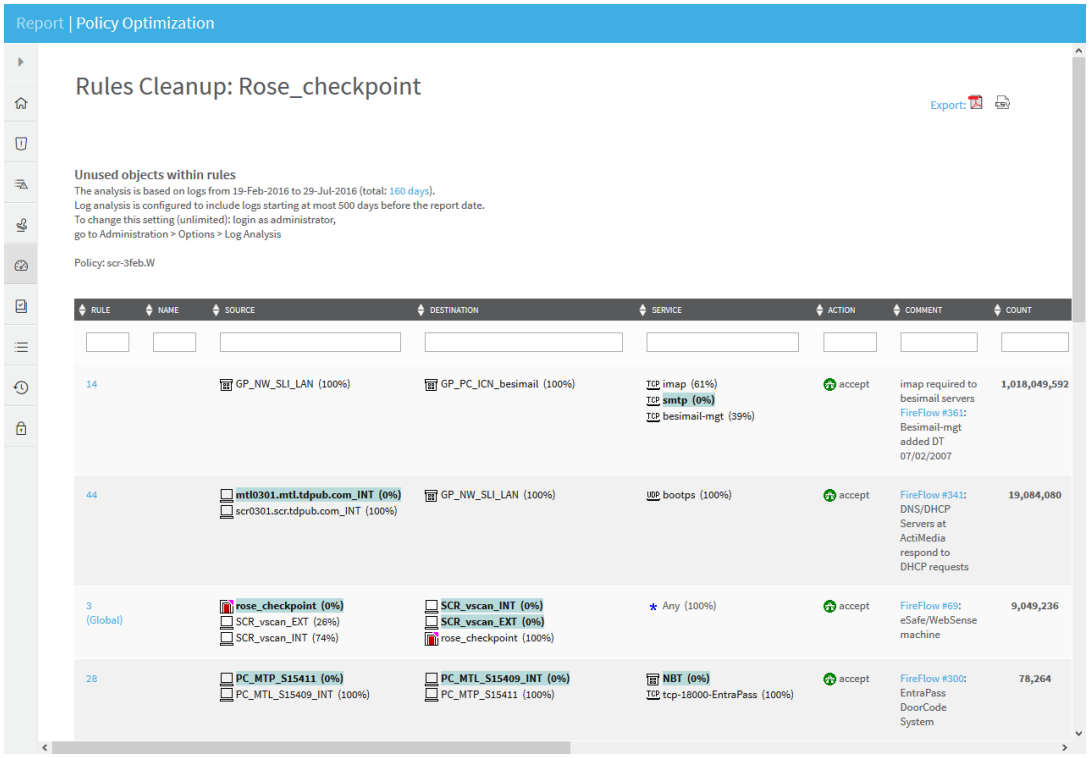
Objects that are sparsely used and include many unused IP addresses or services are highlighted in blue. It is recommended to refine these objects' definitions.

If an object is densely used, then it is not recommended to refine it.

The **Intelligent Policy Tuner Recommendation** area displays recommendations for replacing permissive rules with new, tighter rules, as well as recommendations for new objects to be used in the rules.

- To view unused objects that appear within rules, click **Unused objects within rules**.

  The **Rules Cleanup** page appears.

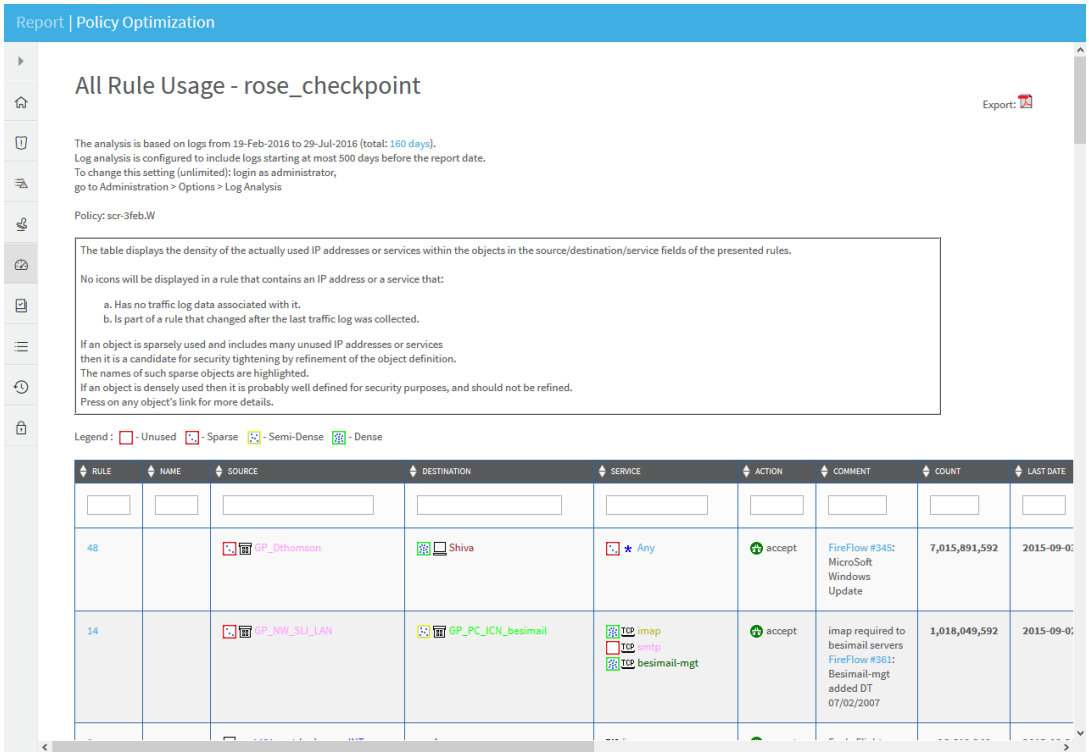


The table displays a list of rules containing objects that have not been used recently. For information on the columns, see the table below.

The unused objects are highlighted in blue and can be removed.

- To view all rule usage, click **Policy tuner analysis for all rules**.

  The **All Rule Usage** page appears.



A table displays a list of all rules. For information on the columns, see the following table.

Icons appear next to the objects in each rule, indicating the object's degree of use. You can mouse-over the icons to view the exact percentage of use.

If an object is sparsely used, it is recommended to refine its definition. If an object is densely used then it is not recommended to refine it.

2. Click on any object to drill-down and view more details.
3. Refine the rules in your policy as desired.

Intelligent Policy Tuner Columns

This column...	Displays this...
RULE	The rule number.
NAME	The rule name.
SOURCE	The device object representing the connection source.

This column…	Displays this…
DESTINATION	The device object representing the connection destination.
SERVICE	The device object representing the service for the connection.
ACTION	The device action performed for the connection.
COMMENT	A comment on the rule.
COUNT	The number of times that an IP address in the specified range appeared in the traffic that traversed the rule.
LAST DATE	The latest date on which the IP address or range appeared in the traffic logs.
PERCENTAGE	The percentage of times that this rule was used, out of all rules.

Reordering Rules

The **Policy Optimization** page's **Rule Reordering** areas provide recommendations for optimizing the device rules for best performance and lower CPU utilization, an estimate for the device's performance, and suggestions for improving the performance with the most effective rule reordering.

The algorithm relies upon the rule usage statistics collected from the device to compute a RMPP (Rules Matched per Packet) score that measures the device's performance. The RMPP is the average number of rules that are compared to filtered packets until the device finds a match, where the average assumes the mix of packets that is observed in the device rule usage statistics. The RMPP is closely correlated with the device’s CPU utilization: a lower RMPP typically means a lower CPU utilization.

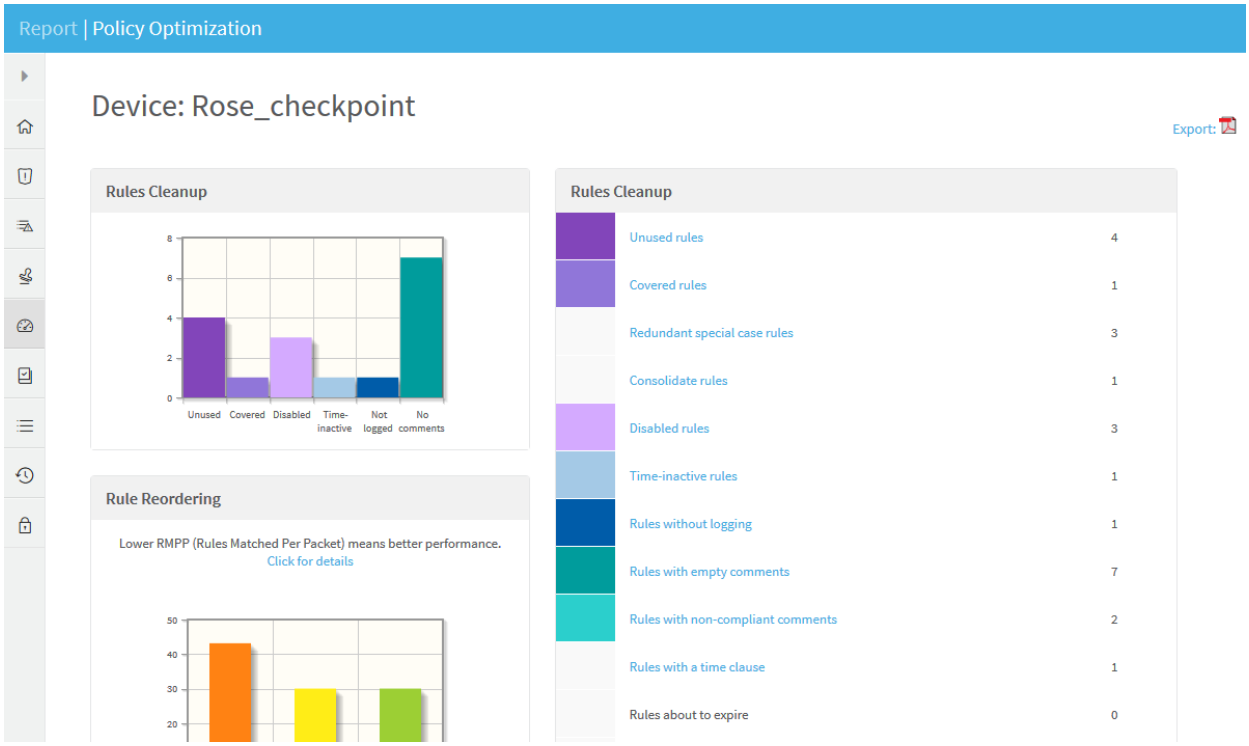
The intuition behind the RMPP calculation is as follows: Suppose that the rule that ultimately matched a connection is rule number "i". Then the device spent a computational effort testing whether the connection matched each of rules 1, 2, …, i-1, until it arrived at rule "i", found that rule "i" matches the connection, and stopped. We see that the computational effort to filter this connection is approximately proportional to the sequence number "i". Therefore, to model the general computational effort the

device is spending, we calculate the mean (expected) number of rules that the device had to check against incoming connections, when the mean is weighted using the rule usage statistics gathered from the log data.

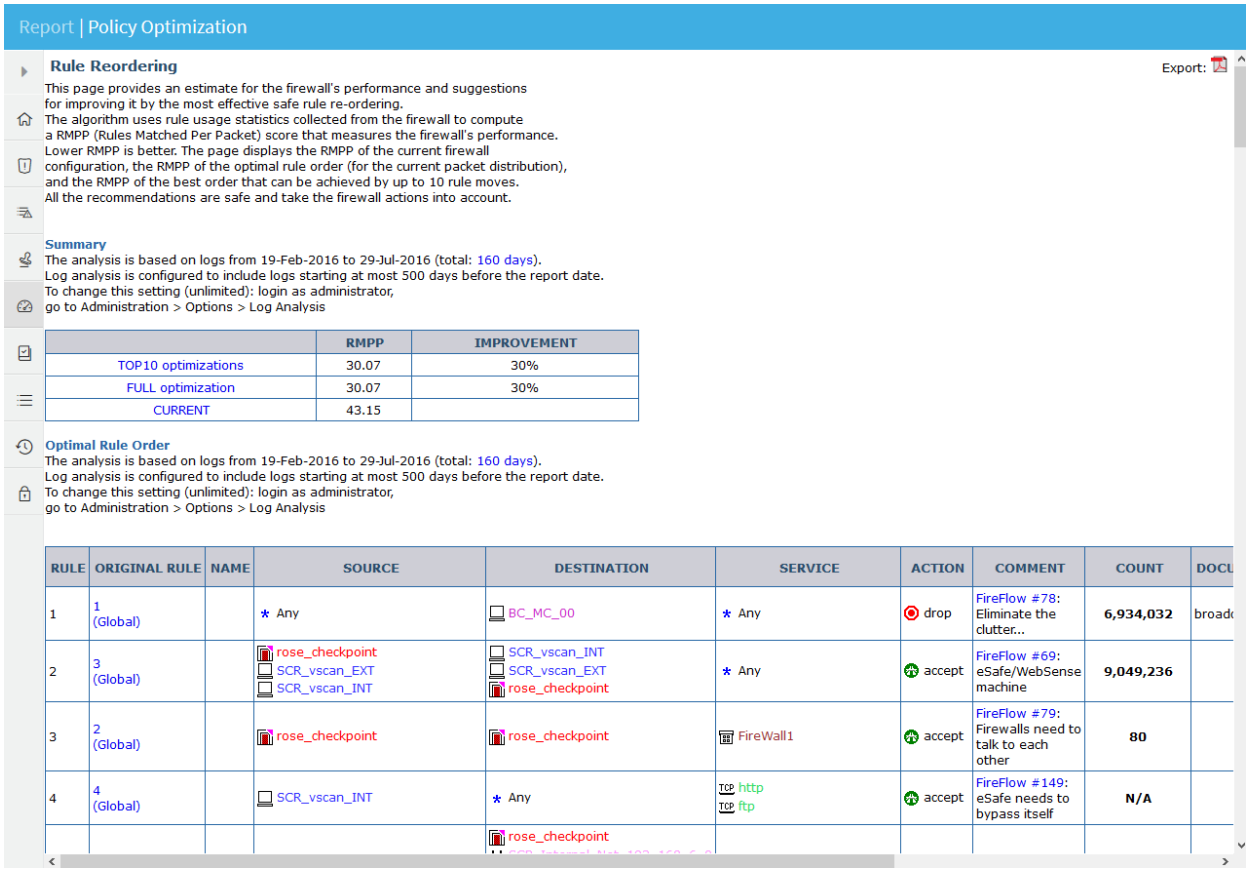
If there are N rules in the rule-base then the RMPP is always a number between 1 and N. Here are some examples. If every connection is always matched by the first rule in the rule-base then RMPP=1. Conversely, if all the connections are matched by the last rule then RMPP=N. If neither of the extreme cases occurs then the RMPP will be a value larger than 1 and smaller than N: E.g., if rule 1 matches 50% of the connections, rule 10 matches 30%, and rule 25 patches 20%, then RMPP = 1*0.5 + 10*0.3 + 25*0.2 = 0.5+3+5 = 8.5. This means that, on average, for the mix of connections observed by this device, the device compares 8.5 rules to each connection it needs to filter in order to reach a decision.

Clearly, we should strive to reduce the RMPP: If we can lower the RMPP toward 1, it means that on average the device will compare fewer rules to each incoming connection, and its CPU utilization will drop accordingly.

The **Rule Reordering** area displays a bar chart showing the RMPP of the current device configuration, the optimal configuration (using the same set of rules), and a midway configuration, which can be achieved from the current configuration by up to 10, most effective rule moves.



Clicking on the bar chart leads to the **Rule Reordering** page, which provides a detailed analysis.



Report | Policy Optimization

Rule Reordering

Export:

This page provides an estimate for the firewall's performance and suggestions for improving it by the most effective safe rule re-ordering.
The algorithm uses rule usage statistics collected from the firewall to compute a RMPP (Rules Matched Per Packet) score that measures the firewall's performance. Lower RMPP is better. The page displays the RMPP of the current firewall configuration, the RMPP of the optimal rule order (for the current packet distribution), and the RMPP of the best order that can be achieved by up to 10 rule moves.
All the recommendations are safe and take the firewall actions into account.

Summary

The analysis is based on logs from 19-Feb-2016 to 29-Jul-2016 (total: 160 days).
Log analysis is configured to include logs starting at most 500 days before the report date.
To change this setting (unlimited): login as administrator,
go to Administration > Options > Log Analysis

	RMPP	IMPROVEMENT
TOP10 optimizations	30.07	30%
FULL optimization	30.07	30%
CURRENT	43.15	

Optimal Rule Order

The analysis is based on logs from 19-Feb-2016 to 29-Jul-2016 (total: 160 days).
Log analysis is configured to include logs starting at most 500 days before the report date.
To change this setting (unlimited): login as administrator,
go to Administration > Options > Log Analysis

RULE	ORIGINAL RULE	NAME	SOURCE	DESTINATION	SERVICE	ACTION	COMMENT	COUNT	DOCU
1	1 (Global)		* Any	BC_MC_00	* Any	drop	FireFlow #78: Eliminate the clutter...	6,934,032	broad
2	3 (Global)		rose_checkpoint SCR_vscan_EXT SCR_vscan_INT	SCR_vscan_INT SCR_vscan_EXT rose_checkpoint	* Any	accept	FireFlow #69: eSafe/WebSense machine	9,049,236	
3	2 (Global)		rose_checkpoint	rose_checkpoint	FireWall1	accept	FireFlow #79: Firewalls need to talk to each other	80	
4	4 (Global)		SCR_vscan_INT	* Any	http ftp	accept	FireFlow #149: eSafe needs to bypass itself	N/A	
				rose_checkpoint					

The **Rule Reordering** page consists of three sections:

- **Summary**. Summarizes the current RMPP (Rules Matched per Packet) situation.

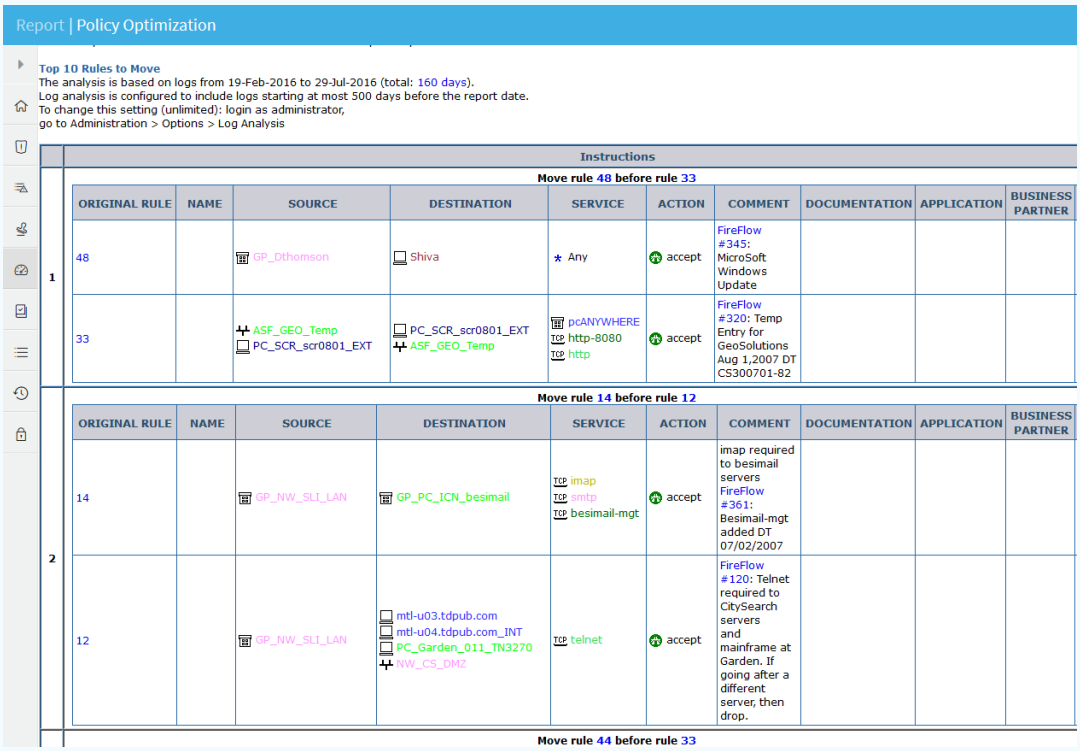
  Note: This summary is also depicted graphically in the **Policy Optimization** page in a second **Rule Reordering** area.

- **Optimal Rule Order**. Provides a complete list of all device rules, arranged in the optimal order for best performance based on RMPP.
- **Top 10 Rules to Move**. A list of up to ten of the most effective steps to generate the greatest improvement in the RMPP score. Each step is a recommendation to move one rule to a different location on the list, and shows the projected RMPP improvement that it will provide.

  Note: The description above refers to the Check Point device screen. The screen

differs per device vendor as follows:

- **Cisco** – Each access list has its own Optimal access-list order (one list per interface).
- **Netscreen** – Each policy list has its own Optimal Policy list.



Report | Policy Optimization

Top 10 Rules to Move
The analysis is based on logs from 19-Feb-2016 to 29-Jul-2016 (total: 160 days).
Log analysis is configured to include logs starting at most 500 days before the report date.
To change this setting (unlimited): login as administrator,
go to Administration > Options > Log Analysis

Instructions

Move rule 48 before rule 33

	ORIGINAL RULE	NAME	SOURCE	DESTINATION	SERVICE	ACTION	COMMENT	DOCUMENTATION	APPLICATION	BUSINESS PARTNER
1	48		GP_Dthomson	Shiva	Any	accept	FireFlow #345: MicroSoft Windows Update			
	33		ASF_GEO_Temp PC_SCR_scr0801_EXT	PC_SCR_scr0801_EXT ASF_GEO_Temp	pcANYWHERE http-8080 http	accept	FireFlow #320: Temp Entry for GeoSolutions Aug 1,2007 DT CS300701-82			

Move rule 14 before rule 12

	ORIGINAL RULE	NAME	SOURCE	DESTINATION	SERVICE	ACTION	COMMENT	DOCUMENTATION	APPLICATION	BUSINESS PARTNER
2	14		GP_NW_SLI_LAN	GP_PC_ICN_besimail	imap smtp besimail-mgt	accept	imap required to besimail servers FireFlow #361: Besimail-mgt added DT 07/02/2007			
	12		GP_NW_SLI_LAN	mtl-u03.tdpub.com mtl-u04.tdpub.com_INT PC_Garden_011_TN3270 NW_CS_DMZ	telnet	accept	FireFlow #120: Telnet required to CitySearch servers and mainframe at Garden. If going after a different server, then drop.			

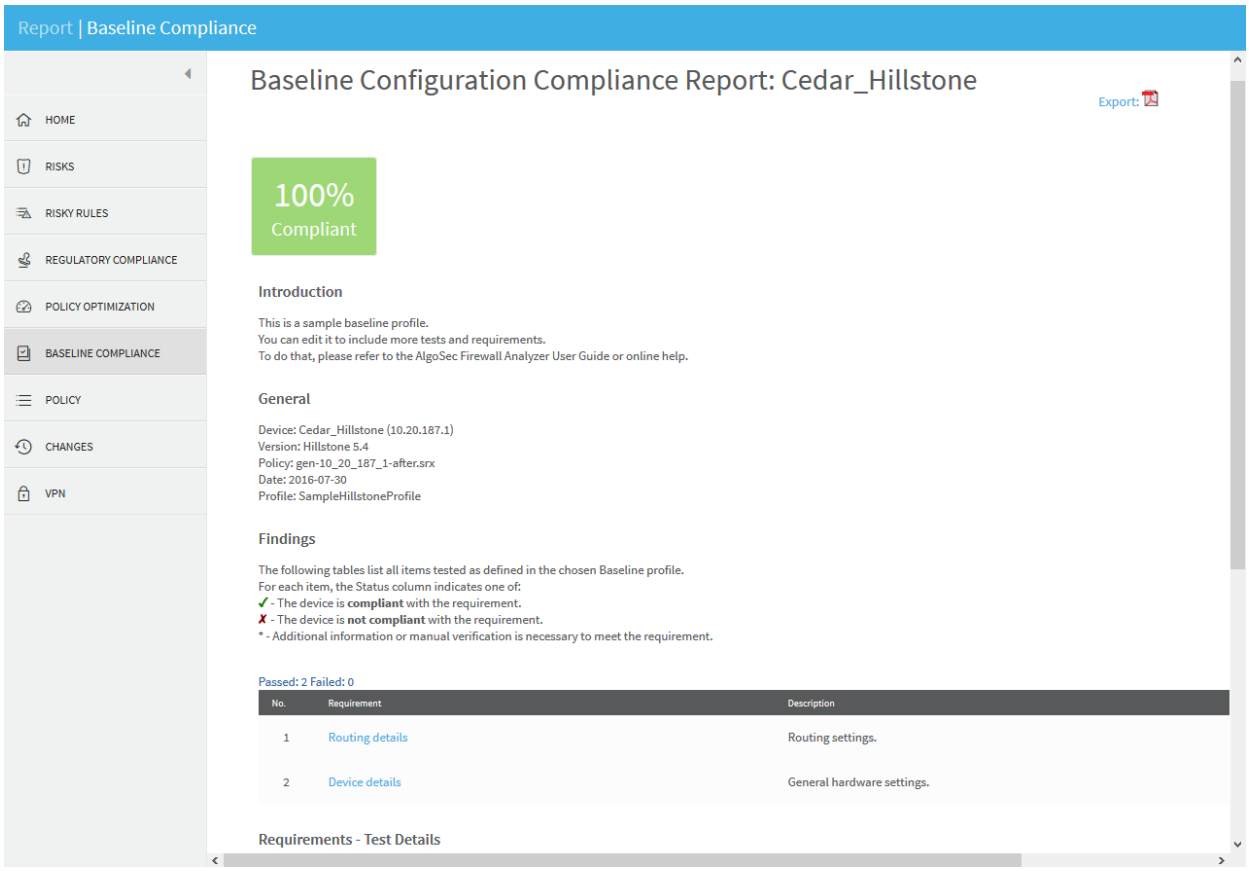
Move rule 44 before rule 33

> **Note:** For Cisco ASA devices version 7.0 or above, access lists are always "compiled". Consequently, the expected performance gain obtained by reordering the rules is small.

BASELINE COMPLIANCE page

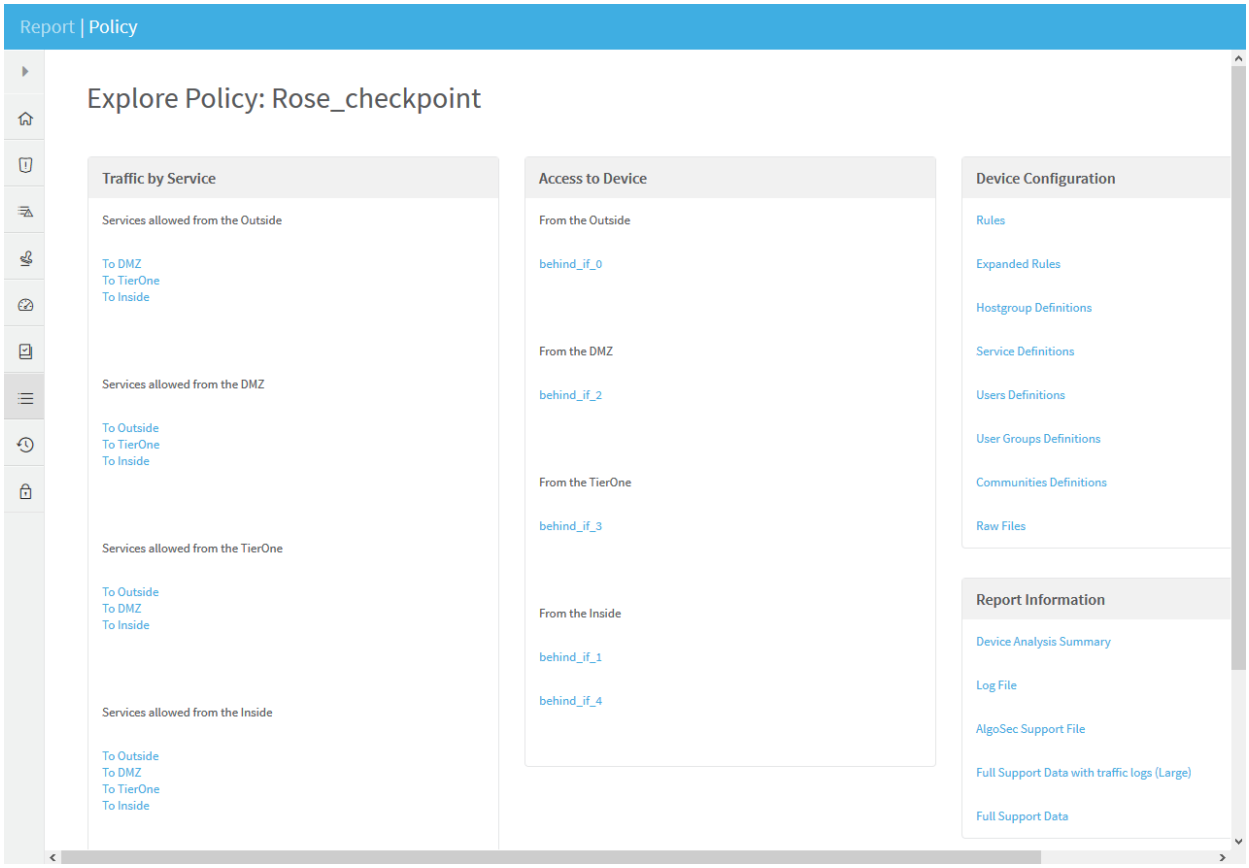
If a baseline compliance profile is specified for the device, the report will include the **Baseline Compliance** page. This report indicates whether running the commands specified in the baseline compliance profile on the device results in the output specified in the baseline compliance profile. If so, then the device is considered to be in compliance.

Baseline compliance profiles are specified per device when defining the device in AFA.

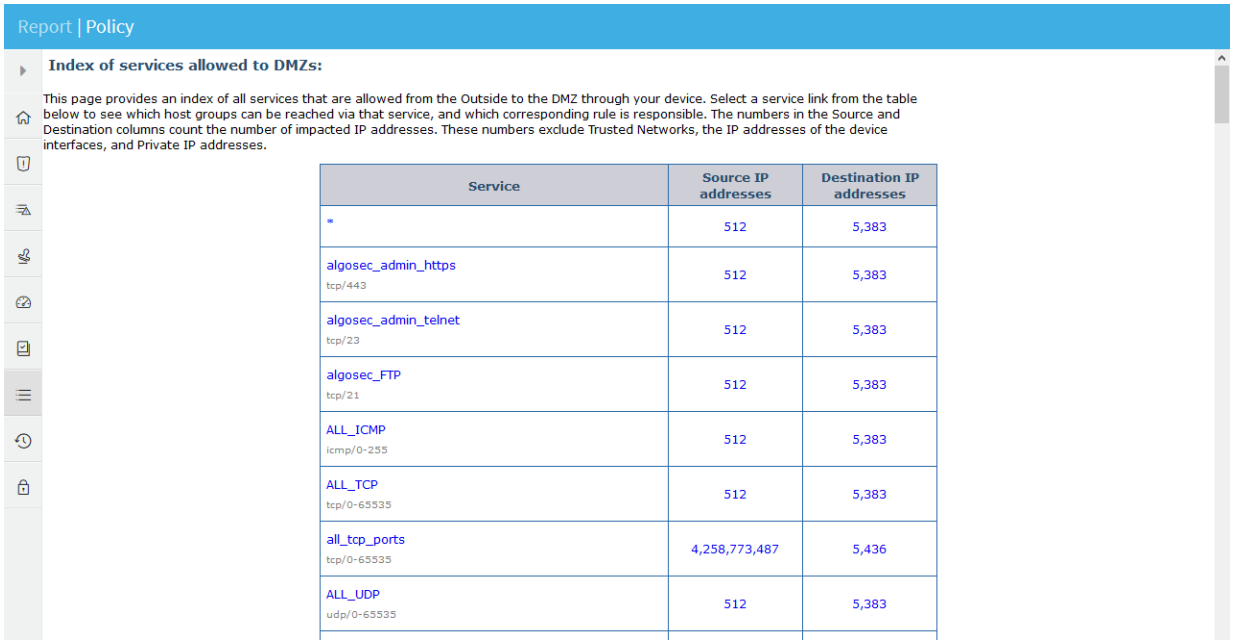


POLICY Page

AFA provides various advanced capabilities that enable you to explore complex details of your device policy. Click on the **Policy** tab in the report to drill down into various aspects of your policy:

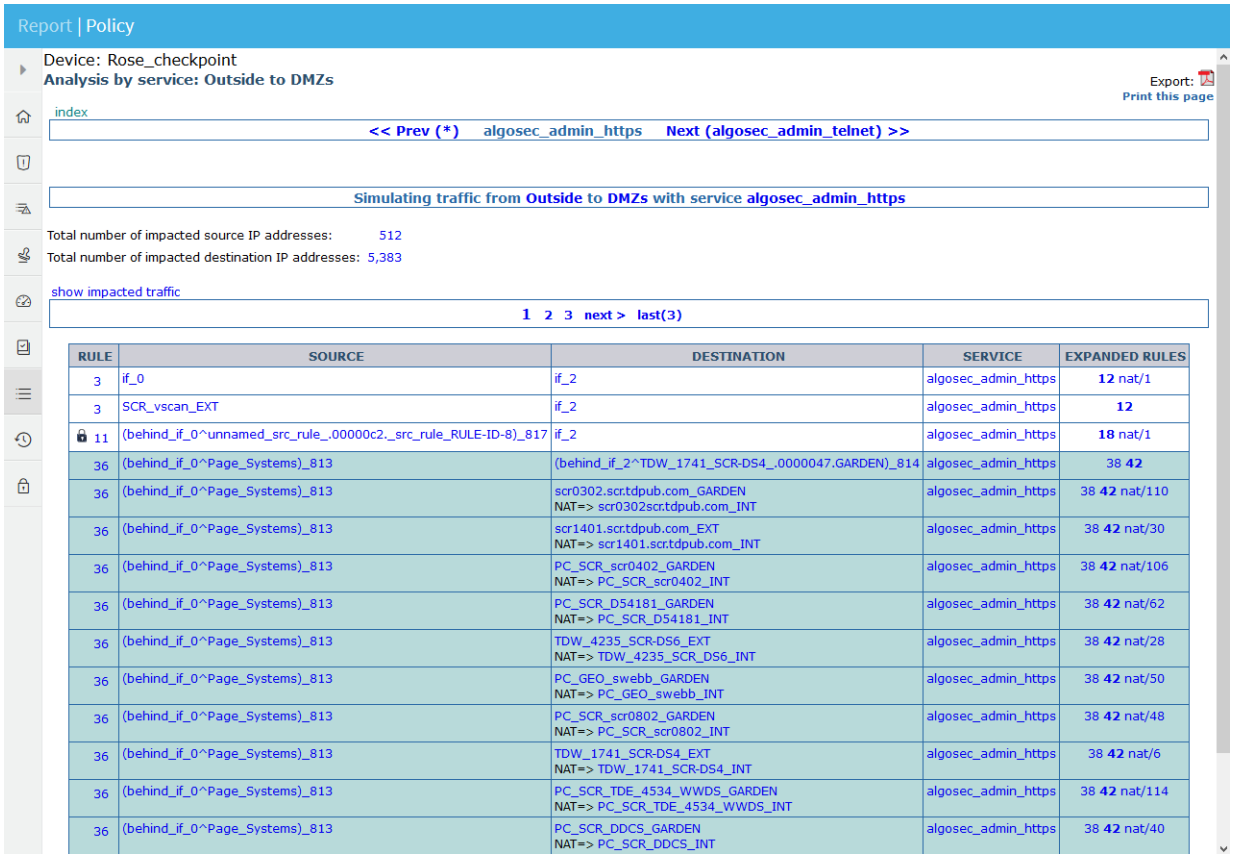


You can focus in on a sensitive host group to see which services can reach it and which corresponding rule is responsible, by clicking the links in the one **Traffic by Service** area.



The values in the **Source IP addresses** and **Destination IP addresses** columns are the number of IP addresses impacted by the service, excluding Trusted Networks, the IP addresses of the device interfaces, and Private IP addresses.

You can further explore where a specific service can reach by clicking its link in the **Service** column.



Report | Policy

Device: Rose_checkpoint
Analysis by service: Outside to DMZs

Export:
Print this page

index

<< Prev (*) algosec_admin_https Next (algosec_admin_telnet) >>

Simulating traffic from **Outside** to **DMZs** with service **algosec_admin_https**

Total number of impacted source IP addresses: 512
Total number of impacted destination IP addresses: 5,383

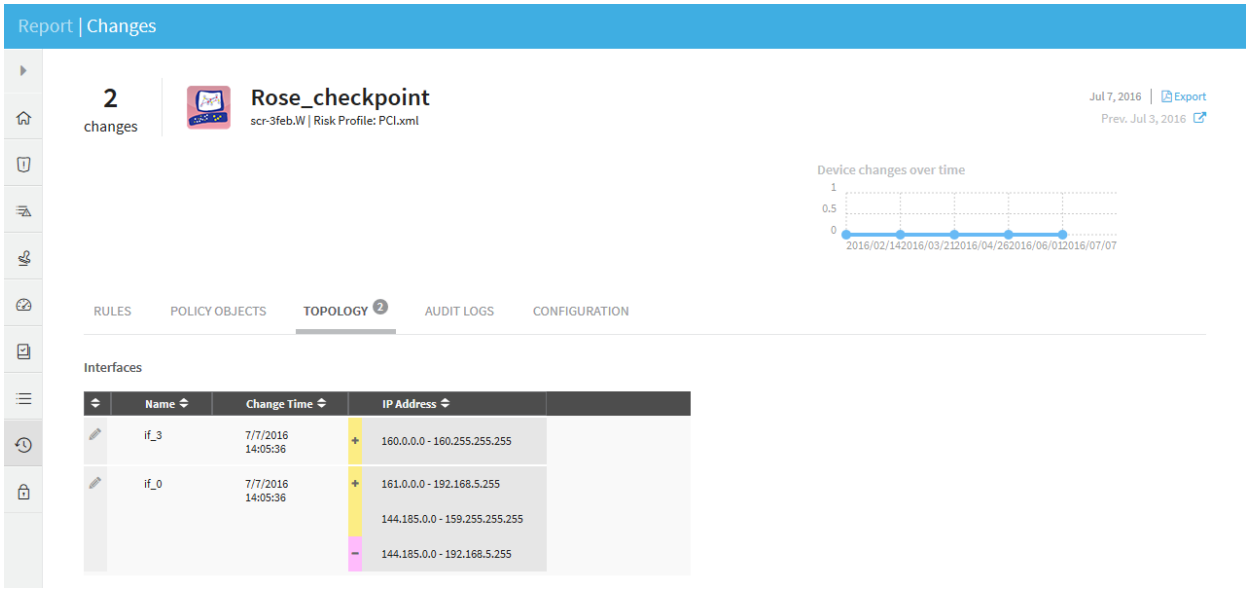
show impacted traffic

1 2 3 next > last(3)

RULE	SOURCE	DESTINATION	SERVICE	EXPANDED RULES
3	if_0	if_2	algosec_admin_https	**12** nat/1
3	SCR_vscan_EXT	if_2	algosec_admin_https	**12**
11	(behind_if_0^unnamed_src_rule_.00000c2._src_rule_RULE-ID-8)_817	if_2	algosec_admin_https	**18** nat/1
36	(behind_if_0^Page_Systems)_813	(behind_if_2^TDW_1741_SCR-DS4_.0000047.GARDEN)_814	algosec_admin_https	38 **42**
36	(behind_if_0^Page_Systems)_813	scr0302.scr.tdpub.com_GARDEN NAT=> scr0302scr.tdpub.com_INT	algosec_admin_https	38 **42** nat/110
36	(behind_if_0^Page_Systems)_813	scr1401.scr.tdpub.com_EXT NAT=> scr1401.scr.tdpub.com_INT	algosec_admin_https	38 **42** nat/30
36	(behind_if_0^Page_Systems)_813	PC_SCR_scr0402_GARDEN NAT=> PC_SCR_scr0402_INT	algosec_admin_https	38 **42** nat/106
36	(behind_if_0^Page_Systems)_813	PC_SCR_D54181_GARDEN NAT=> PC_SCR_D54181_INT	algosec_admin_https	38 **42** nat/62
36	(behind_if_0^Page_Systems)_813	TDW_4235_SCR-DS6_EXT NAT=> TDW_4235_SCR_DS6_INT	algosec_admin_https	38 **42** nat/28
36	(behind_if_0^Page_Systems)_813	PC_GEO_swebb_GARDEN NAT=> PC_GEO_swebb_INT	algosec_admin_https	38 **42** nat/50
36	(behind_if_0^Page_Systems)_813	PC_SCR_scr0802_GARDEN NAT=> PC_SCR_scr0802_INT	algosec_admin_https	38 **42** nat/48
36	(behind_if_0^Page_Systems)_813	TDW_1741_SCR-DS4_EXT NAT=> TDW_1741_SCR-DS4_INT	algosec_admin_https	38 **42** nat/6
36	(behind_if_0^Page_Systems)_813	PC_SCR_TDE_4534_WWDS_GARDEN NAT=> PC_SCR_TDE_4534_WWDS_INT	algosec_admin_https	38 **42** nat/114
36	(behind_if_0^Page_Systems)_813	PC_SCR_DDCS_GARDEN NAT=> PC_SCR_DDCS_INT	algosec_admin_https	38 **42** nat/40

CHANGES page

The **CHANGES** page provides detailed information about changes to the device, over the whole history of AFA reports for the device. Reports include all change monitoring supported for real-time change monitoring as well as changes to risks and baseline compliance.



For more details, see Manage real-time monitoring.

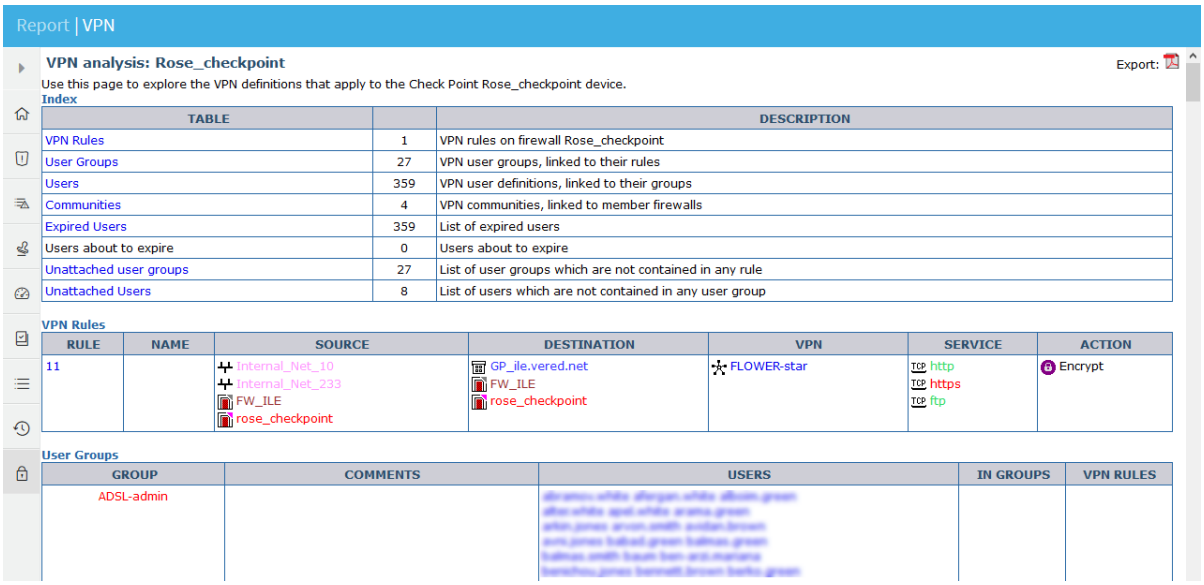
VPN page

The **VPN** page in the AFA report provides you with a clear view of all your VPN settings, and gives you a single place from which to navigate and review the details of your definitions. The report covers VPN definitions related to remote login users that are terminated on the device, and also to point-to-point VPNs. The contents of this page depend on the device vendor.

For Check Point devices, the VPN report consists of the following sections:

- **VPN Rules**: lists all the VPN rules found on the device, with links to the user groups that are in use.
- **User Groups**: lists all the user groups, with links to the rules each group participates in, and the users that belong to the group.
- **Users**: lists all the users defined on the device, each with its authentication and encryption parameters and expiration date, with links to all the groups each user belongs to.

- **Communities**: lists all the VPN communities, each with all the member devices.



For Juniper, the VPN report includes the **VPN Rules**, **VPN Tunnels**, **IKE Information**, **User Groups** and **Users definitions**.

For Cisco ASA devices, the VPN report includes the **Crypto maps**, **Transform sets**, and **IKE Policy**.

The VPN report page is not available for Forcepoint (McAfee) Security Management Center, Forcepoint (McAfee) SideWinder, F5 Big-IP, Juniper Space, Fortinet, and Hillstone devices.

Note: The **Policy Optimization** page also contains information which is relevant to VPN management. Specifically, it contains a list of expired users, unattached user groups, and unattached users. See the Policy Optimization Page (see POLICY OPTIMIZATION page).

Note:

Support for the Forcepoint brands (Sidewinder, StoneGate) and Hillstone was deprecated in ASMS version A30.00.

If you had defined these devices in an earlier version of ASMS, these devices are still available to you, with all the existing capabilities, but you cannot add new ones after upgrading.

We recommend backing up device data before or after upgrading and then removing these devices from AFA. Make sure to download any report zip files for the device before deleting.

For more details, see the relevant AlgoPedia KB article.

View AFA group data

A *group* is a set of devices, in which *no* information about the relationships between the member devices is provided, or when the devices are not connected in a tiered network. AFA manages a group's policy as a single unit, providing a bird's-eye view of your group-wide risk exposure.

In addition to user-defined groups, AFA includes a built-in group called ALL_FIREWALLS. This group consists of all devices in the system, and you can generate reports for it like any other group.

Note: For additional information on Cisco User Awareness - How to Define a User/User Group in a Rule, see this AlgoPedia Knowledge Base article.

Viewing User-Defined Groups

To view a user-defined group:

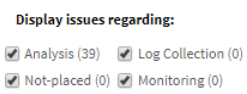
1. Click **Groups** in the main menu.

   The **Groups** menu appears in the main menu, displaying all of the groups defined in AFA. Groups for which the last report generation failed appear in red. Groups for which real-time monitoring or log collection have failed appear in orange.

2. (Optional) Search for the desired group, by doing the following:
   a. Type part or all of the desired group's name in the **Search** field.
   b. Press enter or click .

      The device tree appears with the search results. Device results appear with the group to which they belong. Group results appear with their device members collapsed.
3. (Optional) To filter out the groups with issues, do one of the following:
   - To filter by only the issues you specify:
     1. Next to the **Issues** link, click .

        The **Display issues regarding** window appears.

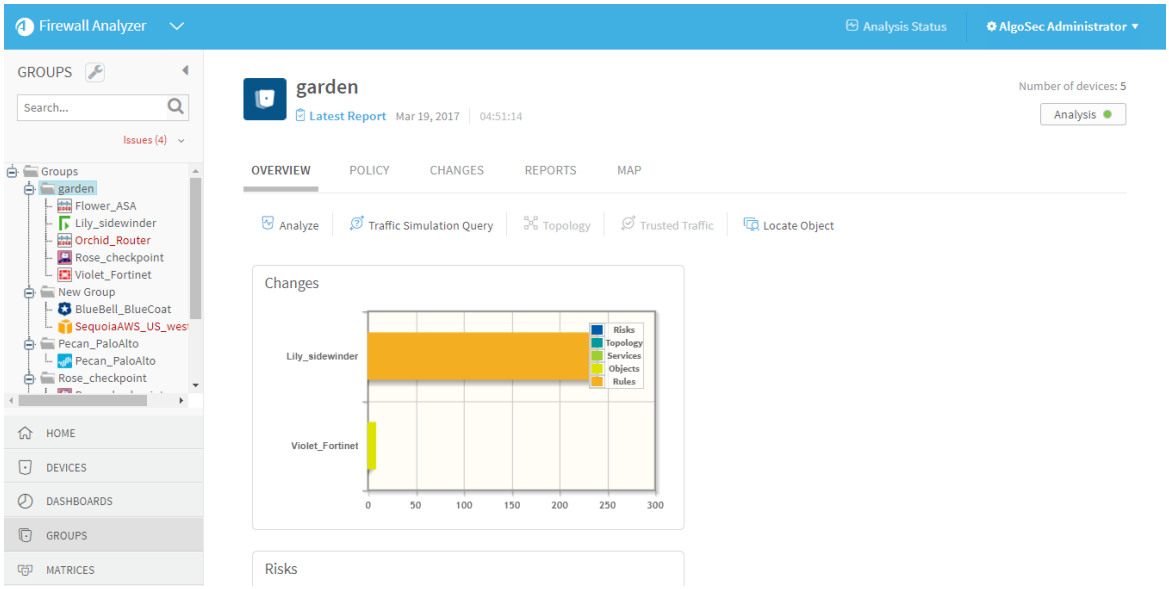
        

     2. Clear the check boxes of the issues you do not want to appear in the filtered results.
     3. Click outside the window.
   - To filter all issues (default), click **Issues**.

     The device tree appears with only devices with issues and their group. If you specified which issues should appear, only those issues appear.

     To revert to the standard view, click the **Issues** link.
4. Select the desired group.

   The group appears in the workspace.



For details of the information displayed at the top of the workspace, see Group Information Fields (see Group Information Fields).

You can view the individual devices in the group by selecting them in the in the menu.

Group Information Fields

This field...	Displays this...
Latest Report	A button that brings you to the last successful report generated for this group.
Date and Time	The date and time when the group was last analyzed.
Number Of devices	The number of devices in the group.

Viewing the ALL_FIREWALLS Group

To view the ALL_FIREWALLS *group*:

1. Click **Devices** in the main menu.

   The **Devices** menu appears in the main menu, displaying all of the devices defined in AFA. Devices for which the last report generation failed appear in red. Devices for which real-time monitoring or log collection have failed appear in orange.

2. In the devices list, click **ALL_FIREWALLS**.

   The ALL_FIREWALLS group appears in the workspace.

   For information on the fields displayed at the top of the workspace, see Group Information Fields (see Group Information Fields).

Viewing Group Reports

Group reports provide information for a group of devices. Group reports are provided for the ALL_FIREWALLS group and for groups manually defined in AFA.

AFA provides the following options for viewing group reports:

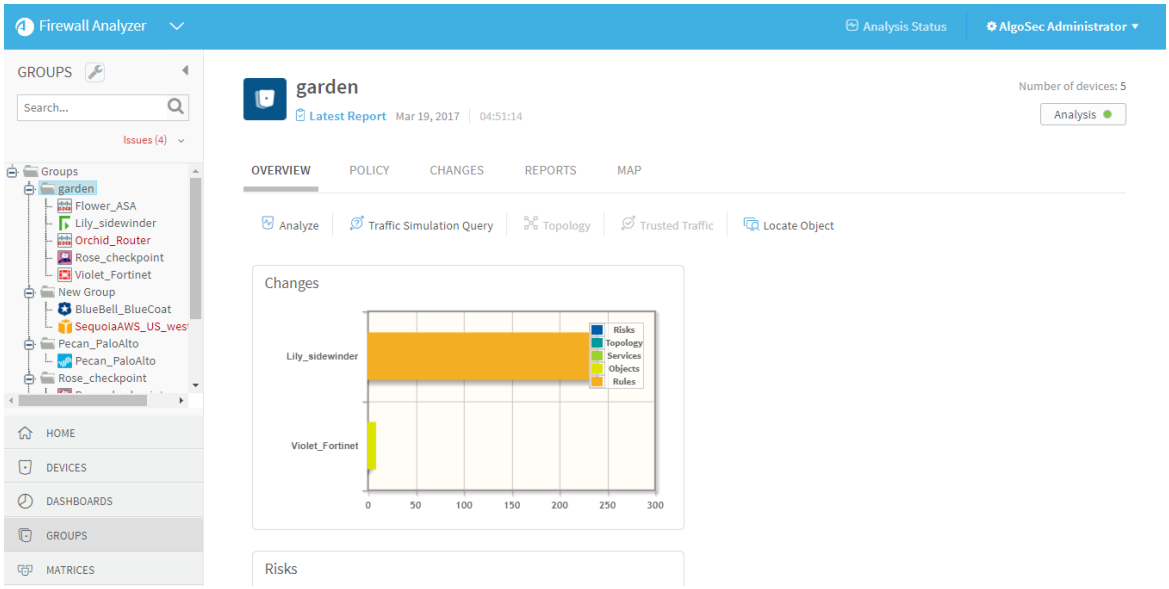
- Viewing the Latest Report for a Group
- Viewing Any Report for a Group
- View AFA group data

Viewing the Latest Report for a Group

To view the latest report for a group:

1. View the desired group. For details, see Viewing User-Defined Groups.

   The **Overview** tab displays a preview of the latest report for the group.



The color of the Analysis , Monitoring , and Log collection icons at the top of the page signify the status of their last process:

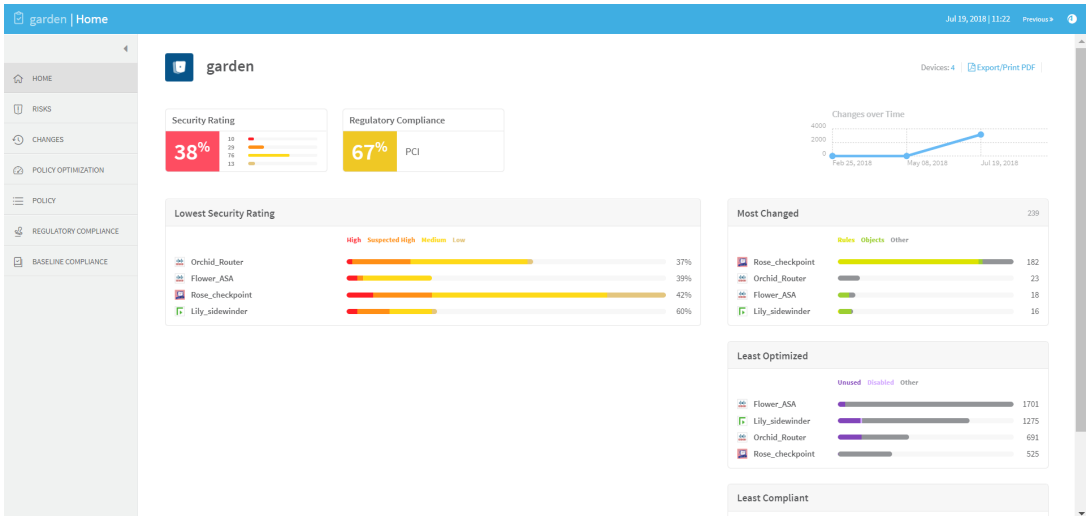
- **Red**. The last process failed.
- **Green**. The last process succeeded.
- **Gray**. The process has never run.

If the last analysis failed, see or an analysis is in progress, see Managing Analyses for more information.

2. When the last analysis succeeded, view the report by do one of the following:
   - At the top of the workspace, click Latest Report .

     The latest report opens, displaying the report's **Home** page in the workspace.
   - Within the **Overview** tab, click on the report section you want to view.

     The latest report opens, displaying the specified section in the workspace.



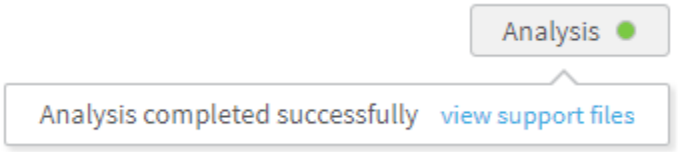
The report menu appears in the left pane, and the selected page appears in the workspace. You can navigate between the different pages of the report by selecting the page in the report menu. For information on each of the various report pages, see Group report pages.

All report pages are structured to allow drilling down from a high-level overview to low-level, detailed information. Any item that appears underlined when you hover over it can be clicked for further details.

3. When the last analysis succeeded, you can view support files for it by doing the following:

   a. Click the **Analysis** button.

      The support files link appears.



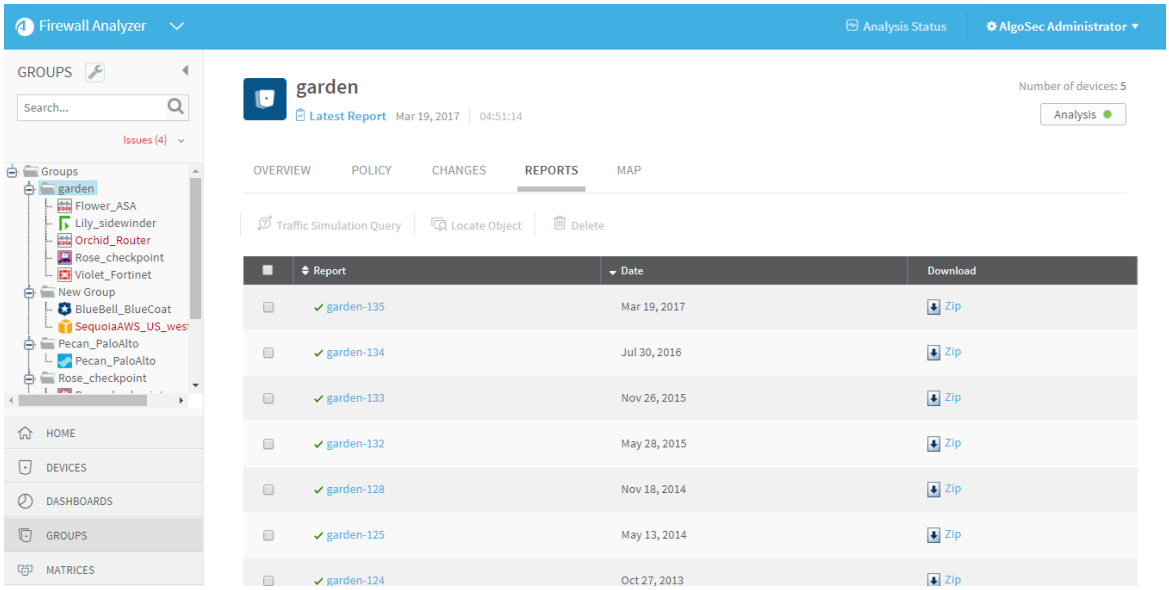
   b. Click the link.

Viewing Any Report for a Group

To view or download any available report for a group:

1. View the desired group. For details, see Viewing User-Defined Groups.
2. Click the **Reports** tab.

   The **Reports** tab appears, displaying all of the available reports for the group.



   Reports that were successfully generated are marked with a ✓. Reports that are currently being generated are marked with a ⧗. Reports for which generation failed are marked with a ✕.

3. Do one of the following:
   - To view a report without downloading it, in the **Report** column, click on the desired report's name.
   - To download a report to your computer, in the desired report's row, click **Zip**.

   The compressed report downloads to your computer. Unzip the report to view it.

   The report opens, displaying the **Home** page.

   The report menu appears in the left pane, and the selected page appears in the workspace. You can navigate between the different pages of the report by

selecting the page in the report menu. For information on each of the various report pages, see Group Report Pages (see Group report pages).

All report pages are structured to allow drilling down from a high-level overview to low-level, detailed information. Any item that appears underlined when you hover over it can be clicked for further details.

Group report page references

The following pages are available in group reports:

Page	Description
HOME page	Provides a general overview of the report, including a list of devices in the group, changes to the devices, risks, and policy optimization.
RISKS page	Provides a high-level executive summary of the risk analysis findings. **Note:** Available only with the AFA Risk and Compliance Module
REGULATORY COMPLIANCE page	Access a variety of automatically-filled compliance reports for this group. **Note:** Available only with the AFA Risk and Compliance Module
POLICY OPTIMIZATION page	Find out what you can eliminate from each device's policy to optimize it and make it more efficient and maintainable.
BASELINE COMPLIANCE page	Indicates whether group members' configurations comply with certain baselines.
POLICY page	Provides access to the wealth of detailed information collected and identified during the analysis.

Page	Description
CHANGES page	Displays the changes in rules, objects, and the resulting changes in allowed traffic and risks, over all the history of AFA reports for devices in this group.

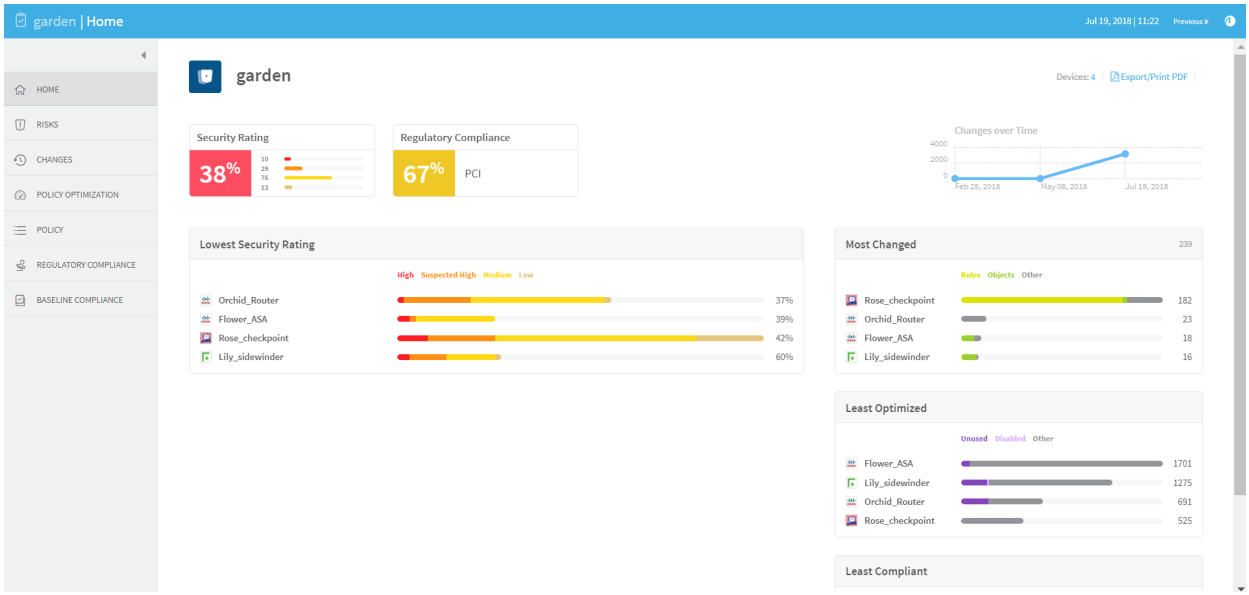
Group report pages

This topic describes the pages available in group reports, most of which are very similar to device reports.

For more details, see View AFA group data, View AFA device data, and Device report pages.

HOME page

The **Home** page provides an overview of the group report. The page's content depends on your AFA modules.



RISKS page

The **Risks** page summarizes all risk analysis findings by providing the following:

- The security rating for the group.

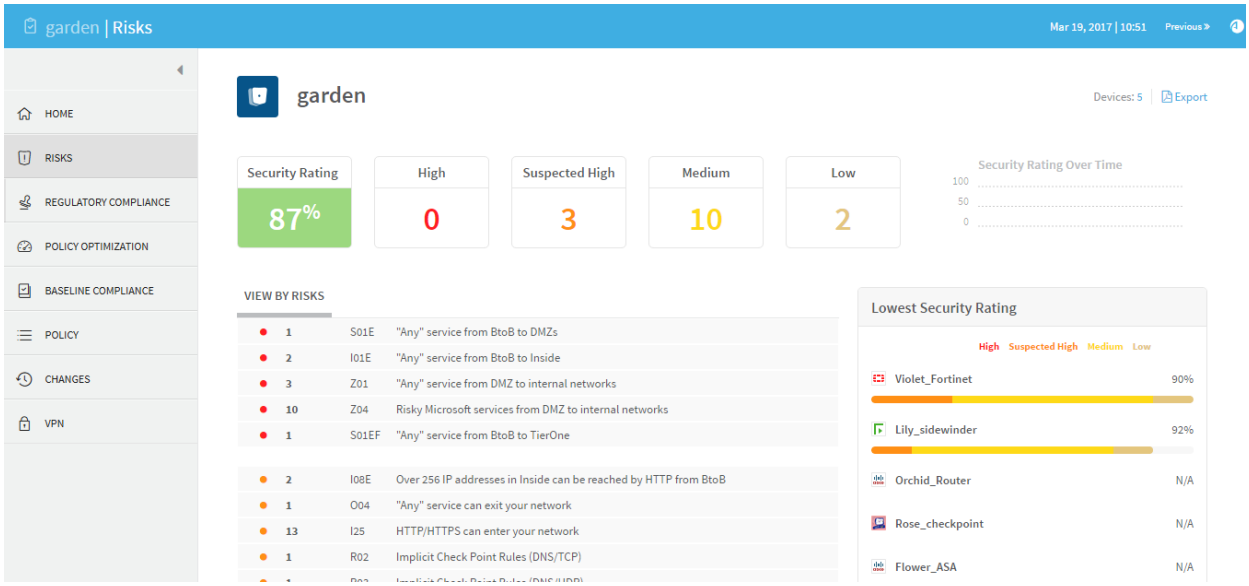
The security rating indicates the group's degree of compliance with security standards. A security rating of 100% indicates full compliance.

- The total number of risks in each severity category, not counting duplicates.
- A graph displaying the security rating trend.
- A list of all the group's risks, in decreasing order of severity.

The list includes a brief summary of each threat: the risk, its trigger count (the number of times it was detected), and a brief description. The **New** label indicates risks that were not present in the previous report.

- The ability to easily drill down to specific rules and groups.
- A visual representation of the risks per device, with each device's security rating.

To access an individual device's report, in the **Lowest Security Rating** area, click on the device's name.



For further information about the **Risks** page, see RISKS page.

REGULATORY COMPLIANCE page

The **Regulatory Compliance** page includes aggregated compliance reports for the entire group.

To view a report, click the desired report's name.

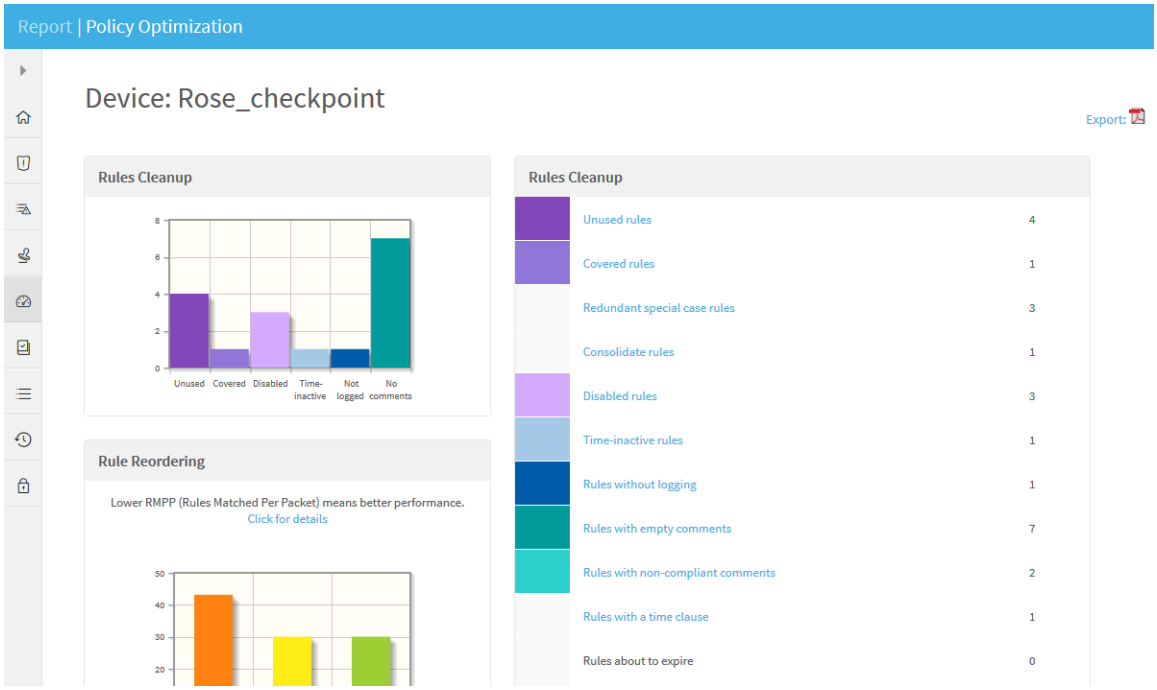
For information on each report, see:

- Payment Card Industry Data Security Standard (see Payment Card Industry Data Security Standard (PCI DSS))
- Sarbanes-Oxley Compliance Report (see Sarbanes-Oxley)
- ISO/IEC 27001 Compliance Report (see ISO/IEC 27001)
- NERC Standards for Critical Infrastructure Protection (see NERC Standards for Critical Infrastructure Protection (NERC CIP))
- NIST SP 800-53 Compliance Report (see NIST SP 800-53)
- NIST SP 800-41 Compliance Report (see NIST SP 800-41)
- Gramm-Leach-Bliley Act (GLBA) Compliance Report (see Gramm-Leach-Bliley Act (GLBA))
- Basel-II Compliance Report (see Basel-II)

- ASD ISM Compliance Report (see ASD ISM)
- Financial Instruments and Exchange Law (Japan) Compliance Report (see Financial Instruments and Exchange Law (Japan))
- MAS TRM Compliance Report (see MAS TRM)
- HIPAA Compliance Report (see HIPAA)

POLICY OPTIMIZATION page

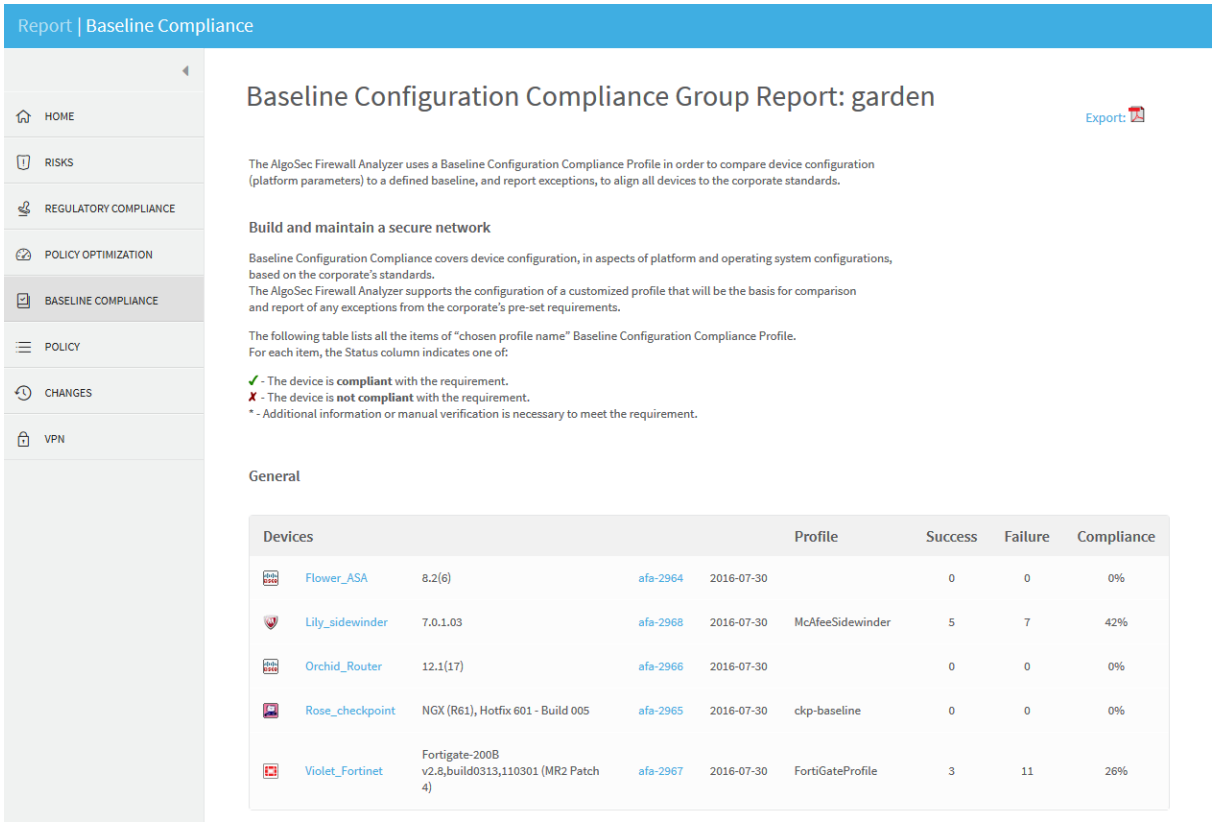
The **Policy Optimization** page enables you to optimize your policy, by identifying inefficient rules and objects. A separate list is provided for each device in the group.



For more information on using this page, see Policy Optimization Page (see POLICY OPTIMIZATION page).

BASELINE COMPLIANCE page

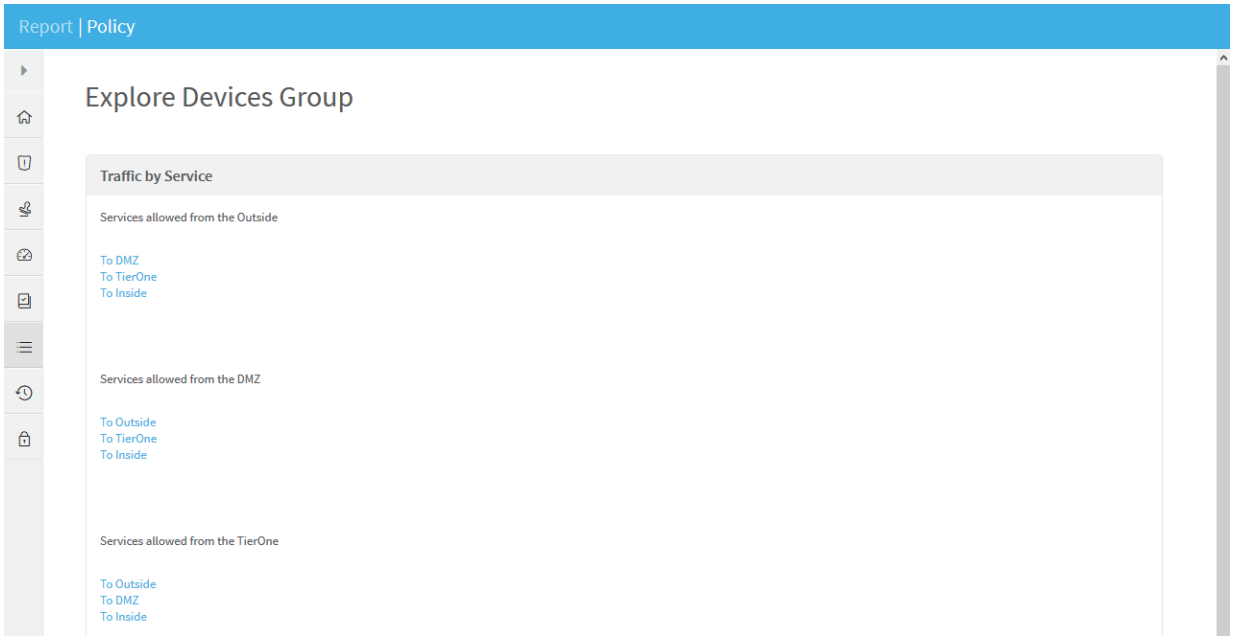
The **Baseline Compliance** page includes aggregated baseline compliance reports for the entire group.



For further information, see Baseline Compliance Page (see BASELINE COMPLIANCE page).

POLICY page

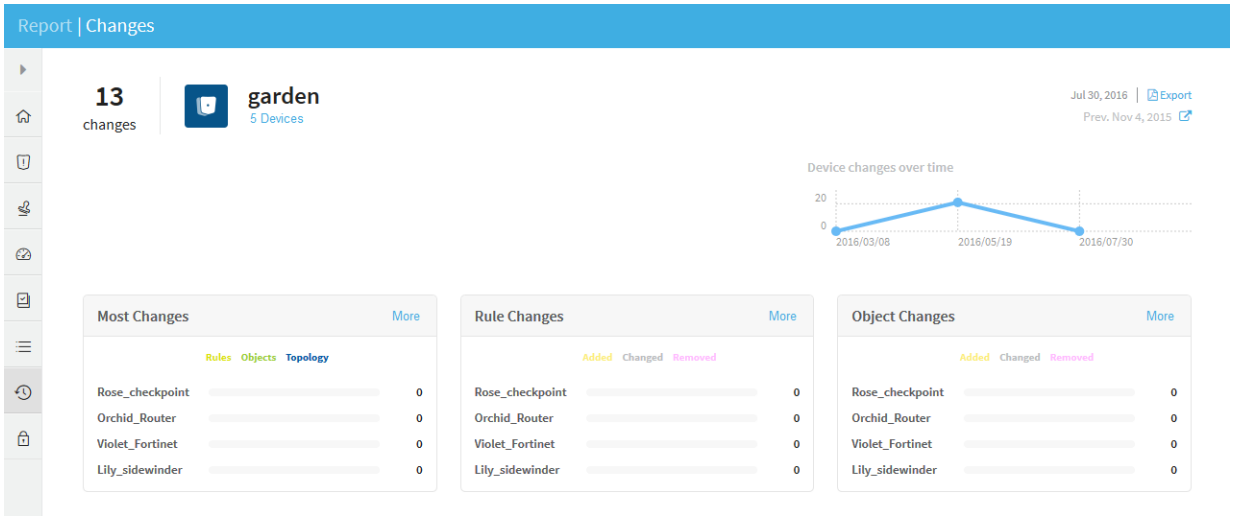
The **Policy** page enables you to drill down into various aspects of your policy.



For further information, see Policy Page (see POLICY Page).

CHANGES page

The **Changes** page provides detailed information about changes to the devices in the group, over the whole history of AFA reports for the group.



For further information, see Changes Page (see CHANGES page).

View AFA matrix data

A *matrix* is a set of devices, in which information about each device member's position in the network hierarchy is provided. AFA manages a matrix's policy as a single unit, taking into account the relationships between each member device.

Viewing Matrices

To view information about a matrix:

1. Click **Matrices** in the main menu.

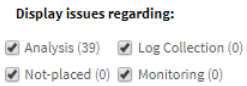
   The **Matrices** menu appears in the main menu, displaying all of the matrices defined in AFA. Matrices for which the last report generation failed appear in red. Matrices for which real-time monitoring or log collection have failed appear in orange.

2. (Optional) Search for the desired matrix, by doing the following:
   a. Type part or all of the desired matrix's name in the **Search** field.
   b. Press enter or click  .

      The device tree appears with the search results. Device results appear with the matrix to which they belong. Matrix results appear with their device members collapsed.

3. (Optional) To filter out the matrices with issues, do one of the following:
   - To filter by only the issues you specify:
     1. Next to the **Issues** link, click .

        The **Display issues regarding** window appears.



2. Clear the check boxes of the issues you do not want to appear in the filtered results.
3. Click outside the window.

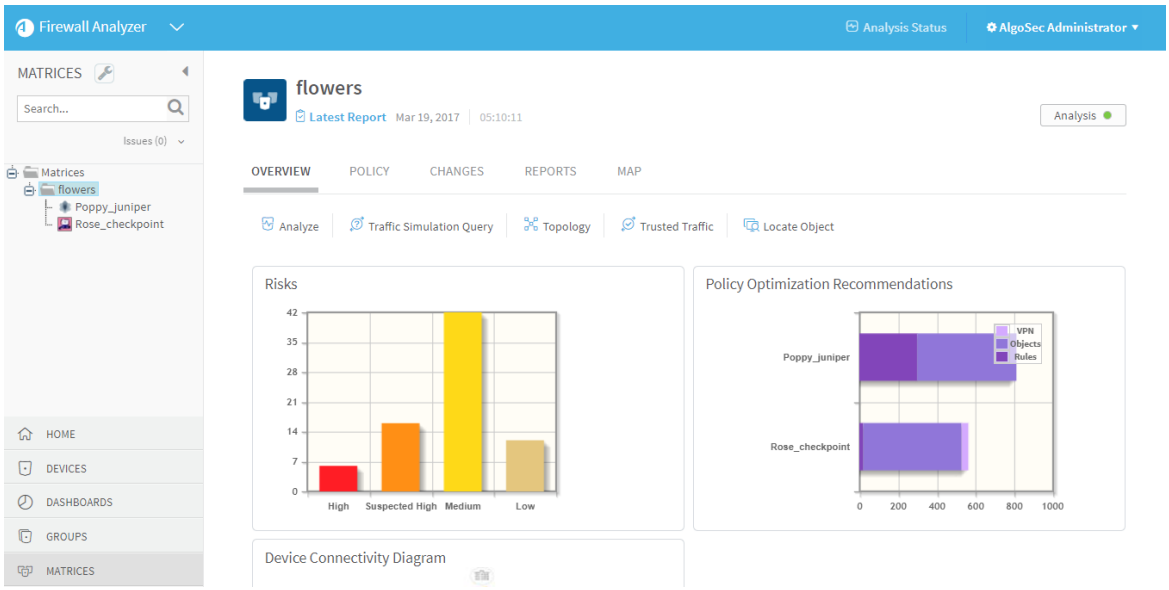
- To filter all issues (default), click **Issues**.

  The device tree appears with only devices with issues and their matrix. If you specified which issues should appear, only those issues appear.

  To revert to the standard view, click the **Issues** link.

4. Select the desired matrix.

   The matrix appears in the workspace.



For details of the information displayed at the top of the workspace, see Group Information Fields.

You can view the individual devices in the group by selecting them in the in the menu.

Viewing Matrix Reports

Matrix reports provide information on a device matrix. AFA provides the following options for viewing matrix reports:

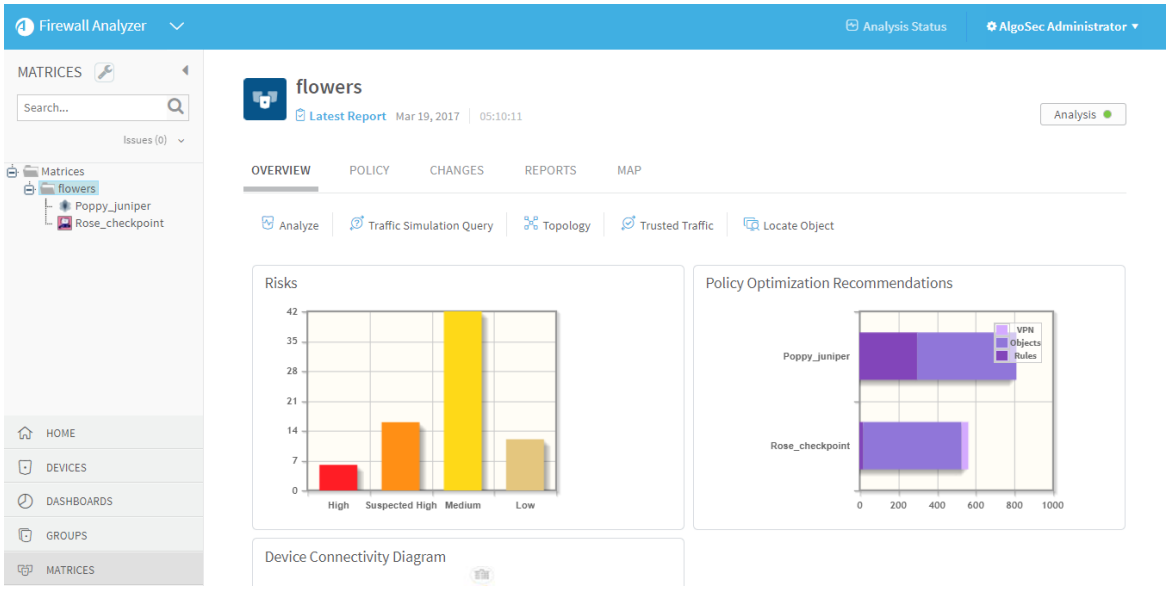
- Viewing the Latest Report for a Matrix
- Viewing Any Report for a Matrix

Viewing the Latest Report for a Matrix

To view the latest report for a matrix:

1. View the desired matrix. For details, see Viewing Matrices.

   The **Overview** tab displays a preview of the latest report for the matrix.



   The color of the Analysis , Monitoring , and Log collection icons at the top of the page signify the status of their last process:

   - **Red**. The last process failed.
   - **Green**. The last process succeeded.
   - **Gray**. The process has never run.

   If the last analysis failed, see or an analysis is in progress, see Managing Analyses (see Managing Analyses) for more information.

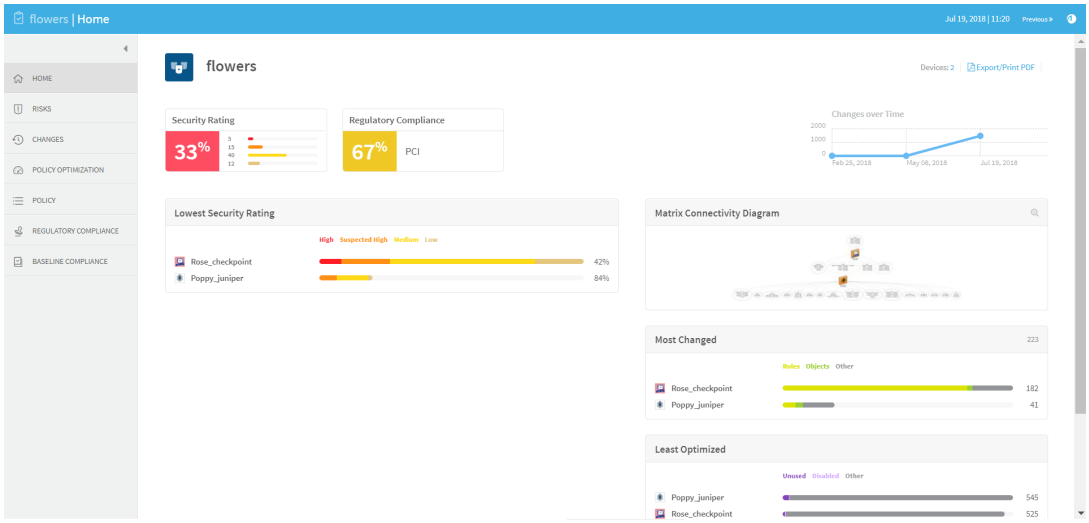
2. When the last analysis succeeded, view the report by do one of the following:

   - At the top of the workspace, click Latest Report .

     The latest report opens, displaying the report's **Home** page in the workspace.

   - Within the **Overview** tab, click on the report section you want to view.

     The latest report opens, displaying the specified section in the workspace.



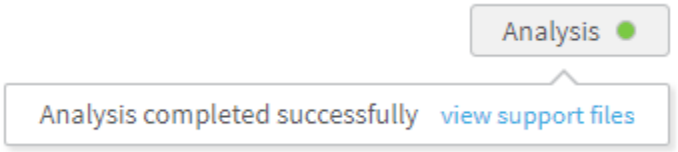
     The report menu appears in the left pane, and the selected page appears in the workspace. You can navigate between the different pages of the report by selecting the page in the report menu. For information on each of the various report pages, see Matrix Report Pages (see Matrix report pages).

     All report pages are structured to allow drilling down from a high-level overview to low-level, detailed information. Any item that appears underlined when you hover over it can be clicked for further details.

3. When the last analysis succeeded, you can view support files for it by doing the following:

   a. Click the **Analysis** button.

      The support files link appears.



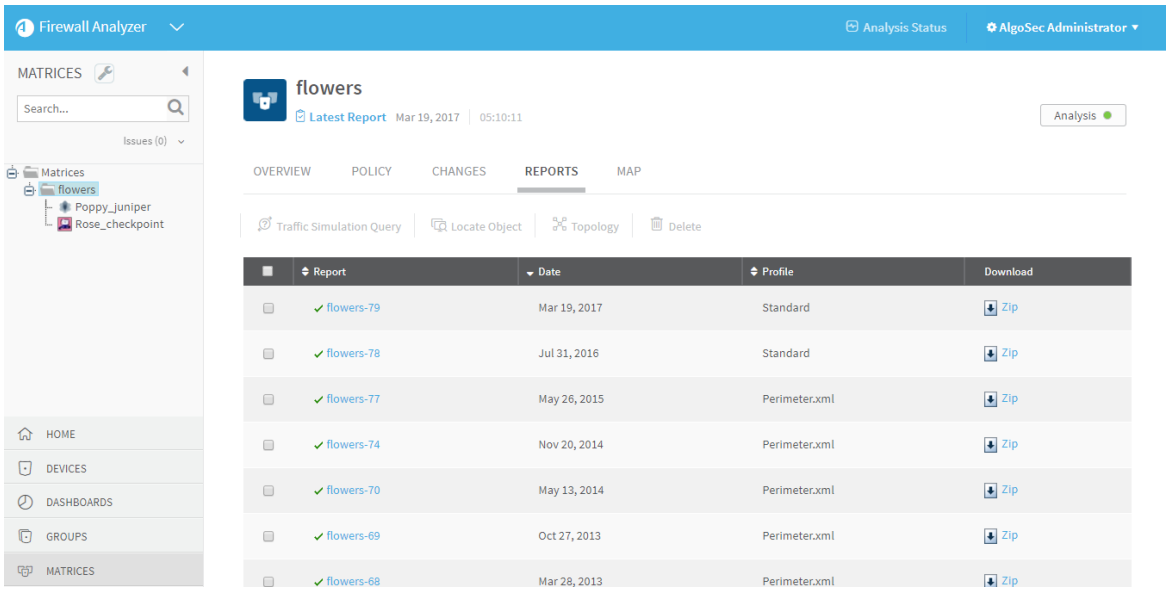
b. Click the link.

Viewing Any Report for a Matrix

To view or download any available report for a matrix:

1. View the desired matrix. For details, see Viewing Matrices.
2. Click the **Reports** tab.

   The **Reports** tab appears, displaying all of the available reports for the matrix.



   Reports that were successfully generated are marked with a ✓. Reports that are currently being generated are marked with a ⧗. Reports for which generation failed are marked with a ✕.

3. Do one of the following:
   - To view a report without downloading it, in the **Report** column, click on the desired report's name.

- To download a report to your computer, in the desired report's row, click **Zip**.

The compressed report downloads to your computer. Unzip the report to view it.

The report opens, displaying the **Home** page.

The report menu appears in the left pane, and the selected page appears in the workspace. You can navigate between the different pages of the report by selecting the page in the report menu. For information on each of the various report pages, see Matrix Report Pages (see Matrix report pages).

All report pages are structured to allow drilling down from a high-level overview to low-level, detailed information. Any item that appears underlined when you hover over it can be clicked for further details.

Matrix report pages

Matrix reports include the following pages.

Some report pages include information about the devices. For more details, see View AFA device data and Device report pages

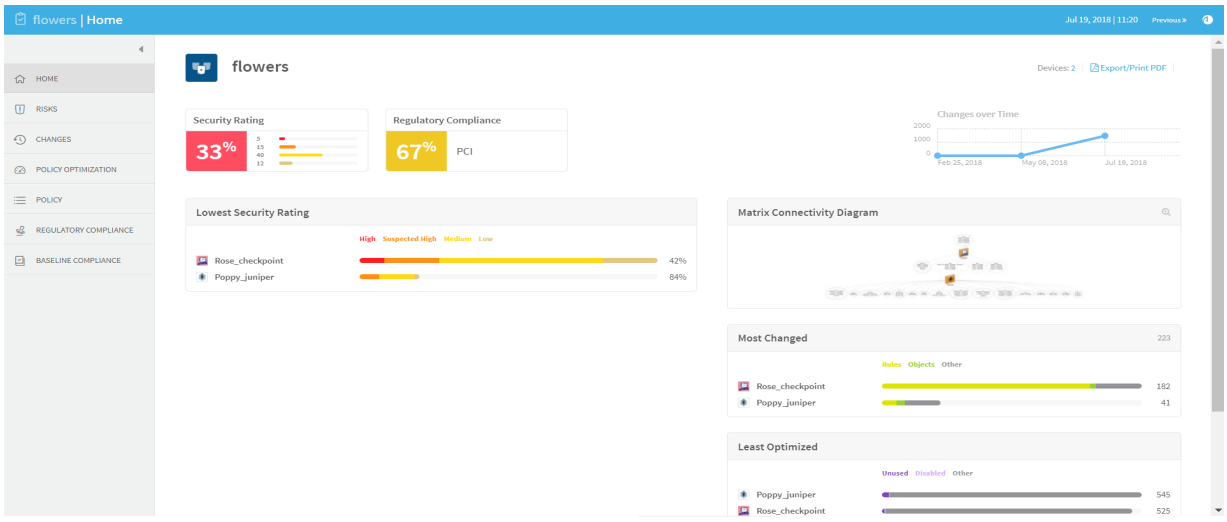
Matrix Report Pages

Page	Description
HOME page	Provides a general overview of the report, including a list of devices in the matrix, changes to the devices, risks, and policy optimization.
RISKS page	Provides a high-level executive summary of the risk analysis findings. Available only with the AFA Risk and Compliance Module
REGULATORY COMPLIANCE Page	Access a variety of automatically-filled compliance reports for this matrix. Available only with the AFA Risk and Compliance Module.

Page	Description
POLICY OPTIMIZATION page	Find out what you can eliminate from each device's policy to optimize it and make it more efficient and maintainable.
BASELINE COMPLIANCE page	Indicates whether matrix members' configurations comply with certain baselines.
POLICY page	Provides access to the wealth of detailed information collected and identified during the analysis.
CHANGES page	Displays the changes in rules, objects, and the resulting changes in allowed traffic and risks, over all the history of AFA reports for this matrix.

HOME page

The **Home** page provides an overview of the matrix report. The page's content depends on your AFA modules.



RISKS page

The **Risks** page summarizes all risk analysis findings by providing the following:

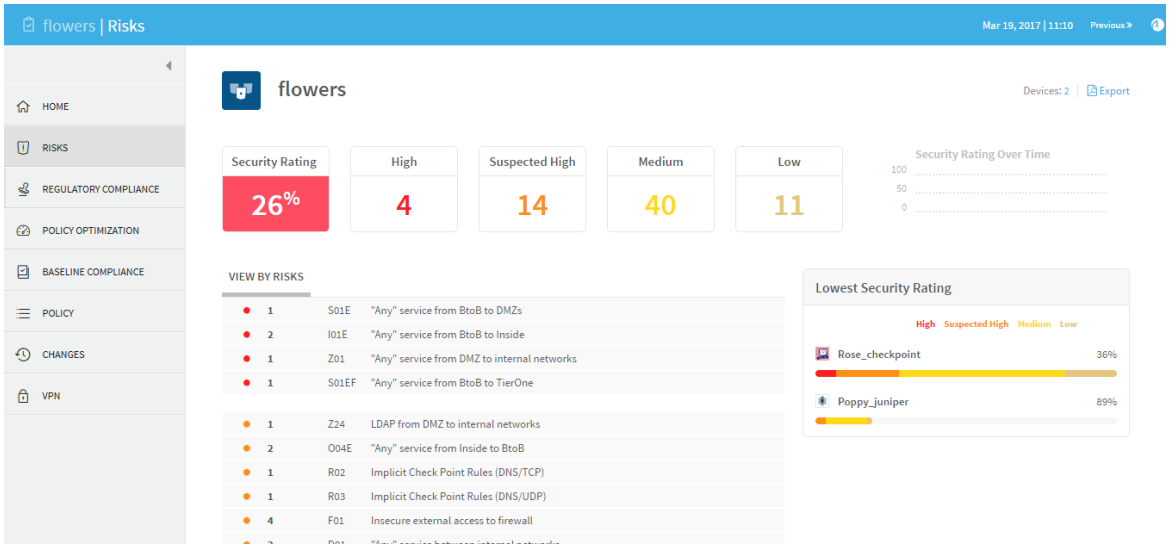
Note: The risks which appear are associated with traffic that is allowed across *all*

devices in the matrix. If one of the devices in the path blocks the traffic, the risk does not appear.

- The security rating for the matrix. The security rating indicates the matrix's degree of compliance with security standards. A security rating of 100% indicates full compliance.
- The total number of risks in each severity category, not counting duplicates.
- A graph displaying the security rating trend.
- A list of all the matrix's risks, in decreasing order of severity.

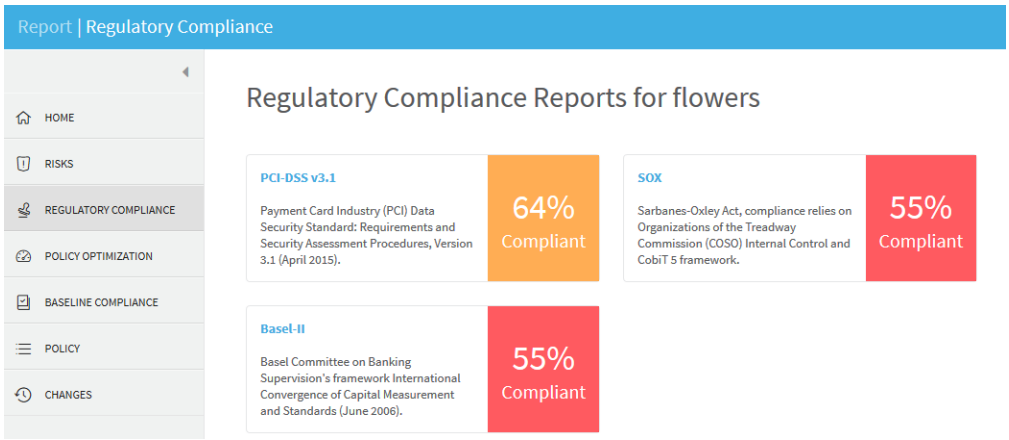
  The list includes a brief summary of each threat: the risk, its trigger count (the number of times it was detected), and a brief description. The **New** label indicates risks that were not present in the previous report.
- The ability to easily drill down to specific rules and groups.
- A visual representation of the risks per device, with each device's security rating.

  To access an individual device's report, in the **Lowest Security Rating** area, click on the device's name.



REGULATORY COMPLIANCE Page

The **Regulatory Compliance** page includes aggregated compliance reports for the entire matrix.



To view a report, click the desired report's name.

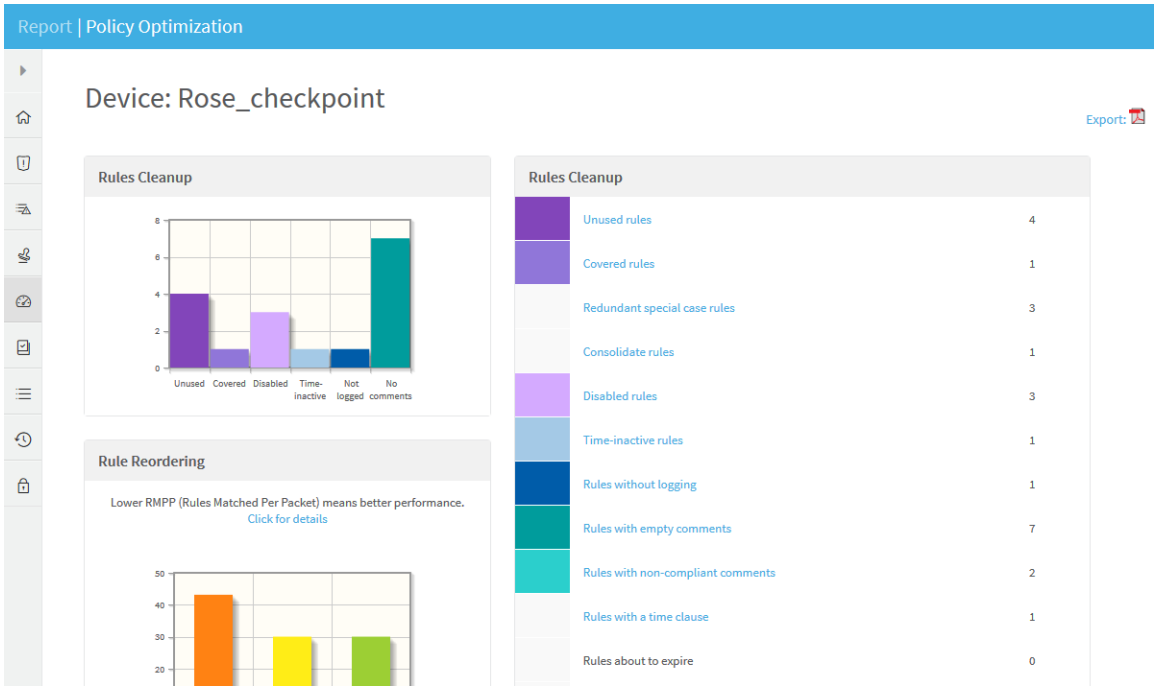
For information on each report, see:

- Payment Card Industry Data Security Standard (see Payment Card Industry Data Security Standard (PCI DSS))
- Sarbanes-Oxley Compliance Report (see Sarbanes-Oxley)
- ISO/IEC 27001 Compliance Report (see ISO/IEC 27001)
- NERC Standards for Critical Infrastructure Protection (see NERC Standards for Critical Infrastructure Protection (NERC CIP))
- NIST SP 800-53 Compliance Report (see NIST SP 800-53)
- NIST SP 800-41 Compliance Report (see NIST SP 800-41)
- Gramm-Leach-Bliley Act (GLBA) Compliance Report (see Gramm-Leach-Bliley Act (GLBA))
- Basel-II Compliance Report (see Basel-II)
- ASD ISM Compliance Report (see ASD ISM)
- Financial Instruments and Exchange Law (Japan) Compliance Report (see Financial Instruments and Exchange Law (Japan))

- MAS TRM Compliance Report (see MAS TRM)
- HIPAA Compliance Report (see HIPAA)

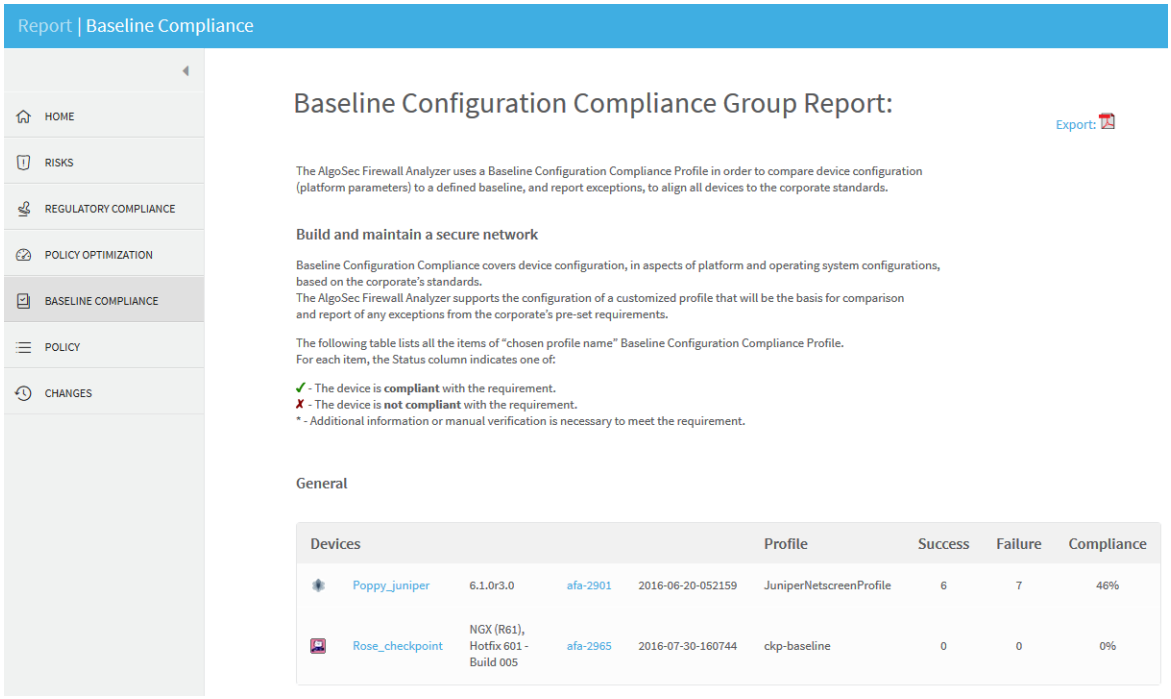
POLICY OPTIMIZATION page

The **Policy Optimization** page enables you to optimize your policy, by identifying inefficient rules and objects. A separate list is provided for each device in the matrix.



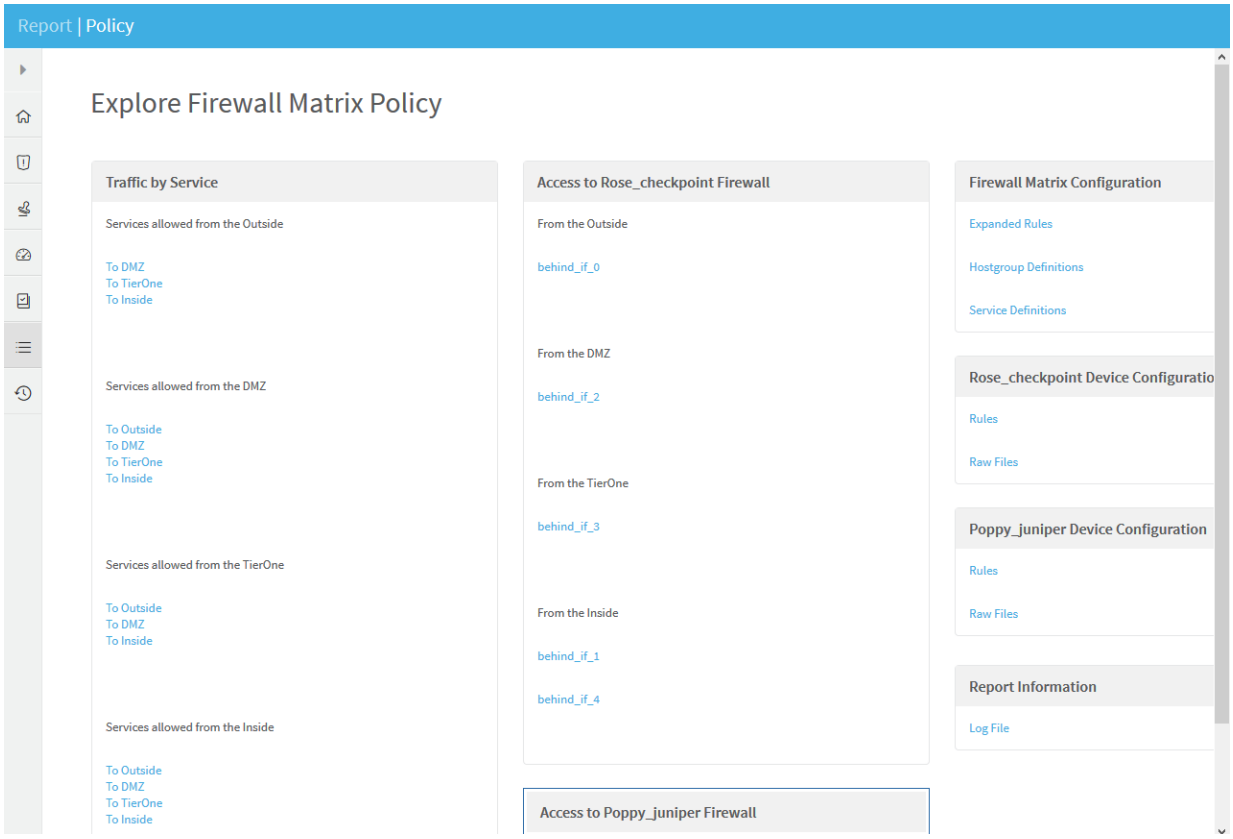
BASELINE COMPLIANCE page

The **Baseline Compliance** page includes aggregated baseline compliance reports for the entire matrix.



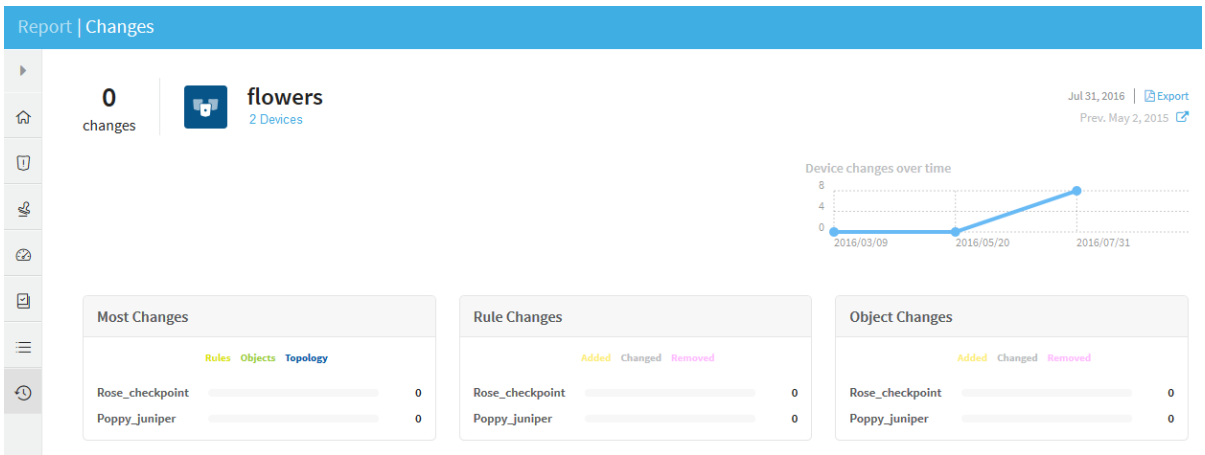
POLICY page

The **Policy** page enables you to drill down into various aspects of your policy.



CHANGES page

The **Changes** page provides detailed information about changes to the devices in the matrix, over the whole history of AFA reports for the matrix. The information is divided into policy changes and risk profile changes.



AFA's graphic network map

AFA calculates a graphic network map that includes the devices in the system, as well as the networks and routers that are directly connected to them. This map is automatically updated each time a device is added or deleted, or when AFA collects a routing table that has been modified.

AFA uses the graphic network map when running traffic simulation queries on groups; therefore, it is important to ensure that the map is correct and that it includes all relevant network elements (especially routers). If necessary, you can modify the graphic network map to better reflect the network architecture.

For more details, see Modify the graphic network map.

Note: From the network map, you can run a routing query to see the devices in the path without policy simulation. For details, see Run a routing query

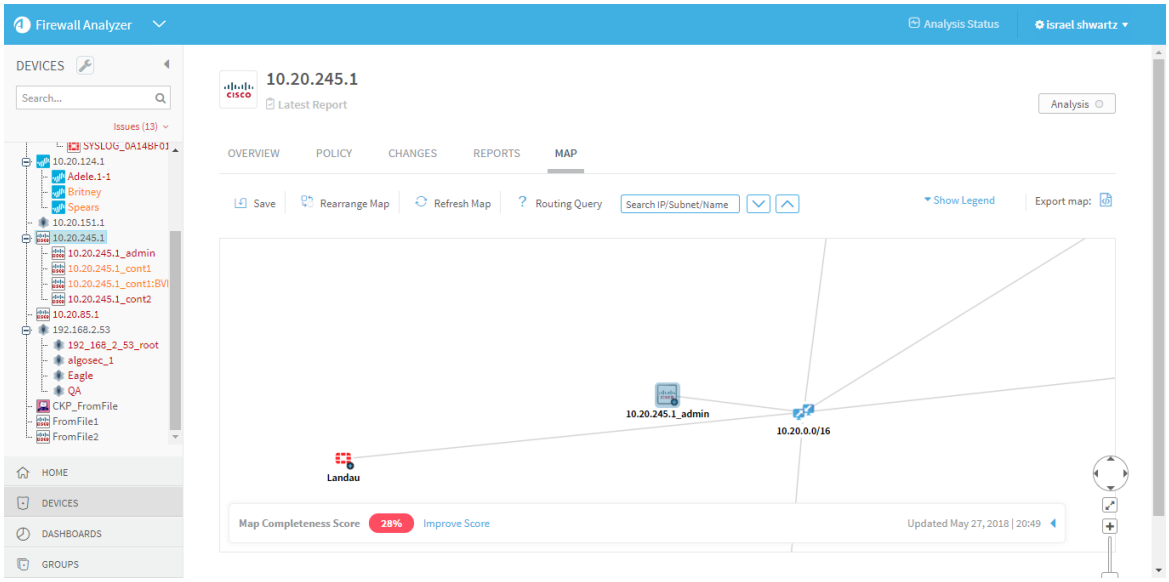
View the network map

AFA's graphic network map displays all of the devices in your ASMS environment. Zoom in and out, move elements around as needed, and hover over elements for more details.

Do the following:

1. View the device, group, or matrix you want to zoom in on. For details, see View AFA device data, View AFA group data, and View AFA matrix data.
2. Click the **Map** tab.

   The **Map** tab appears in the workspace.



All of your devices are shown in the map, but the map centers on the device, group, or matrix you selected.

Note: Management devices are not displayed in the map. Instead, the map shows each individual device, even if it's managed by a management device.

3. Do any of the following:
   - Zoom and pan on the map
   - Search for a specific object
   - Dive down to details
   - View a connectivity diagram
   - View a latest report
   - View a device's route to a specific IP address
   - Show or hide a device's neighborhood
   - Show or a hide the Legend

Note: A score for the completeness of the network map appears at the bottom of the

map. For more details, see Modify the graphic network map.

Zoom and pan on the map

Do any of the following to zoom in or out or pan across the map:

Zoom in or out 	• Click + or − on the zoom bar. • Enter **+** or **-** until you've hit the zoom you want to reach. • Scroll up or down. • Drag the line on the zoom bar up or down.
Resize to fit	To resize the graphic network map to fit the screen, click  .
Pan across the screen 	On the direction control button, click the arrow pointing in the direction you want to take. If the cursor is not in Pan mode, switch by clicking  . Then, click the map and drag it in the desired direction.

Search for a specific object

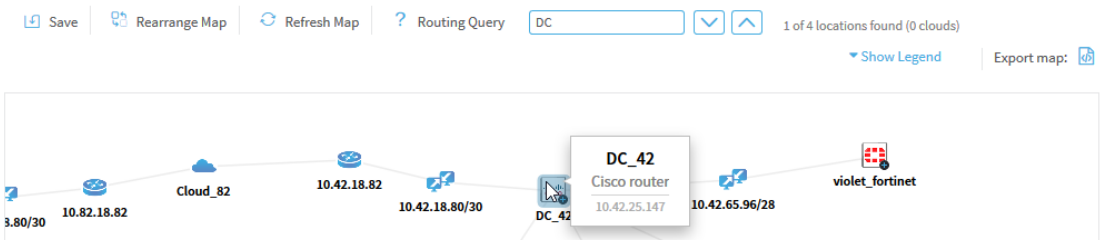
To search for an IP address, range, CIDR, or node name, including devices, subnets, routers, or clouds, in the graphic network map, see Searching the Map.

Dive down to details

To view information about a specific map element (if available), do the following:

1. Hover over the element. If there's any details available, a tooltip appears displaying the information.

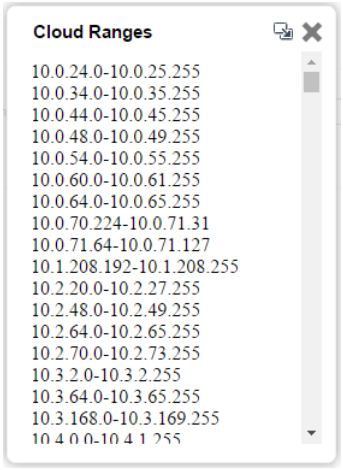
   For example:



For more details, see Network map elements.

2. If the element is a cloud, and the tooltip states that additional information is available, either double-click the cloud, or right-click the cloud and select **View Ranges**.

   The **Cloud Ranges** window appears displaying the cloud's IP address ranges.



View a connectivity diagram

To view a device's connectivity diagram, right-click on the device, then click **Connectivity Diagram**.

The connectivity diagram opens in the new window.

View a latest report

To view a device's latest report, right-click on the device, then click **Latest Report**.

The latest report opens in the new window. For more details, see View AFA device data.

View a device's route to a specific IP address

To view a device's route to a specific IP address, do the following:

1. Right-click on the device, then click **Route Lookup**.
2. In the **Route Lookup** dialog, enter the IP address you want to view the route to.

   One of the following occurs:

   - The route to the IP address appears on the map in blue.
   - If the destination is unreachable, the problematic device is boxed in red, and a pop-up describes the problem.

Show or hide a device's neighborhood

A device's neighborhood includes network map elements that do not connect two devices, but whose existence is inferred from the device definition.

- To show a device's neighborhood, double-click the device, or right-click and select **Expand More**.
- To hide the neighborhood, double-click the device again, or right-click and select **Collapse**.
- To return to the default view, double-click the device or right-click and click **Expand**.

For more details, see Network map elements.

Note: Selecting a device automatically selects its entire neighborhood.

Hidden elements will be exposed in the map they are relevant to a search or Route Lookup.

Show or a hide the Legend

To view the map element legend, click **Show Legend**. **Click Hide Legend** to hide it again.

For more details, see Network map elements.

Host-based devices in the map

Public cloud devices, including AWS and Azure devices, appear in the map as all of their internal elements:

- The elements that make up the AWS or Azure account will appear in the map as individual icons, and traffic simulation queries benefit from the routing information within the system. For Azure, you must first configure this manually.
- The network elements represented in the map include VPC / VNet routers, VPC / VNet peerings, internet gateways, and VPN gateways.
- The subnets coming off the the VPC / VNet router include the containers.

Note: Private cloud devices (VMware NSX and Cisco ACI) do not appear in the graphic network map.

Network map elements

Element	Description
A device icon	**A device defined in AFA.** The device's name appears under the icon. Mouse over to view the device name, brand, and IP address.
	**A transit network.** A network which passes traffic between other networks. The network's name or CIDR is displayed under the icon.
	**A computer network**. A network connected to a single host. The network's name or CIDR is displayed under the icon.

Element	Description
	**A router.** A device with an interface that was discovered as a next-hop in a routing table. The router's IP address is displayed under the icon. Mouse over to view the names of the devices that route to the router.
	**A cloud**. All addresses routed through a discovered router. Mouse over to view the cloud IP address or address ranges.
	**An IPsec tunnel.** A virtual communication channel between two networks. • If only one endpoint of the tunnel is defined in AFA, the IP address of the inferred router is displayed in brackets under the tunnel icon. • If both endpoints of the tunnel are defined in AFA, the IP addresses of each endpoint appear in brackets under the tunnel icon. Mouse over to view the tunnel's CIDR.
	**A routing element.** A generic device defined in AFA with only SNMP credentials. Performs SNMP connections for retrieving routing tables without collecting configurations.
	**An MPLS tunnel.** • If only one endpoint of the tunnel is defined in AFA, the IP address of the inferred router is displayed in brackets under the tunnel icon. • If both endpoints of the tunnel are defined in AFA, the IP addresses of each endpoint appear in brackets under the tunnel icon. Mouse over to view the tunnel's CIDR and route target.
	A layer 2 subnet. A subnet (transit network or computer network) with more than one layer 2 devices placed in it. For more details, see Managing Layer 2 Devices in the Map. Mouse over to view the list of L2 devices in the subnet.
	A layer 2 device. A layer two device placed in a subnet (transit network or computer network). For more details, see Managing Layer 2 Devices in the Map.

Element	Description
	A router that was created by merging more than one router in the graphic network map.
	An edge. This can be either of the following: • An interface between a device and a subnet. Mouse over to view the interface IP and name and virtual IP addresses. • The connection between a router and a cloud.

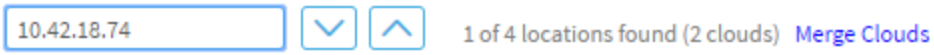
Searching the Map

To search the Graphic Network Map:

1. In the text box above the map, type the IP address, subnet or device name you want to search for, then press Enter.

   The first occurrence of the search input is selected in the network map. The total number of occurrences and the number of occurrences that are clouds are specified.

   If multiple occurrences are clouds, the **Merge Clouds** link appears, enabling you to easily merge any or all of the clouds. For more information on merging clouds, see Merging Clouds.

2. To view the next occurrence of the search input, click  .
3. To view the previous occurrence of the search input, click  .

Exporting the Graphic Network Map to Visio

You can export the graphic network map to the *.svg format, which can be read by Microsoft Visio.

To export the graphic network map to Visio:

1. View the graphic network map. For details, see View the network map.
2. Click  .

   The graphic network map is exported to an *.svg file and can be opened and/or saved to your computer.

Modify the graphic network map

Modifying the graphic network map so that it best represents your network's topology will allow more accurate traffic simulation results, as well as a more accurate visual representation of the network in the map.

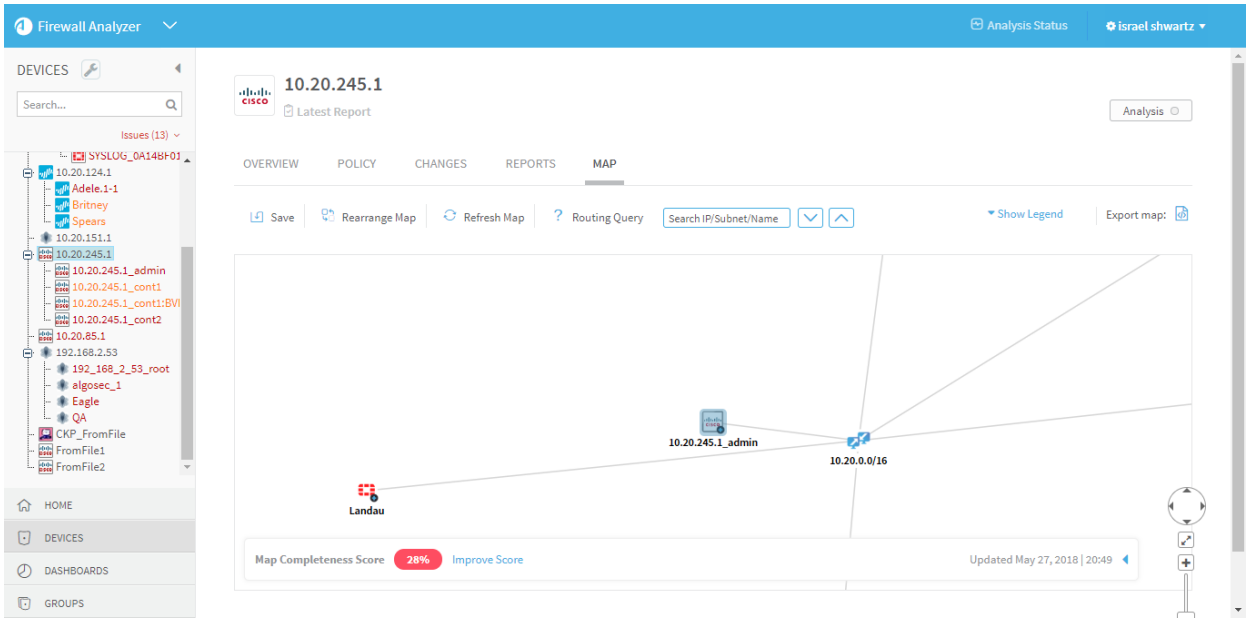
Note: The accuracy of AFA traffic simulation queries affects FireFlow whenever FireFlow uses query results, for example, in Initial Planning.

For instructions for how to perform basic map actions, see Modify the graphic network map.

Match a Risk Profile to Your Topology: Watch to learn about applying risk profiles to your device topology.

Select map elements

Click on an element in the map to select it.



If the neighborhood of a device (network map elements which do not connect two devices) is visible, clicking on a device automatically highlights all neighborhood elements.

Additionally, do any of the following:

Select multiple elements	Use the **SHIFT** or **CTRL** keys to select multiple elements simultaneously. To select all elements within a specific area on the map, press the **SPACEBAR** and drag a selection area around the elements you want to select.
Clear the selection on a single element	If you have multiple elements selected, press **SHIFT** or **CTRL** and click on a specifically selected element to clear the selection on that element.
Clear the selection on multiple selected elements	Either click any open space in the network map, or select a new element. The selection is cleared on all previously selected elements.

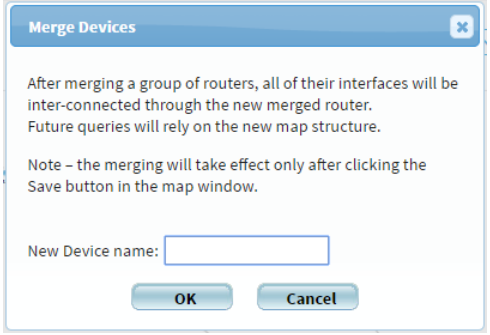
Merge routers

If the same router appears twice in the graphic network map, you may want to merge the two instances.

To merge routers:

1. View the graphic network map. For details, see AFA's graphic network map.
2. Select the two routers you want to merge. For details, see Modify the graphic network map.
3. Right-click on one of the selected routers, and then click **Merge Routers**.

   The **Merge Devices** dialog box opens.



4. In the **New Device name** field, type a name for the merged router.
5. Click **OK**.

   The routers are merged. The routers appear as a single merged router in the map.
6. Click **Save**.

   Note: To ensure that subsequent activity is based on the updated map, save immediately.

   A confirmation message appears.
7. Click **OK**.

Defining a Router as a Routing Element

AFA provides the ability to define a router in AFA as a routing element. A routing element is a generic device which performs SNMP connections for retrieving routing tables, without collecting configurations.

Note: Only administrators can perform this procedure.

Note: You can also add a routing element to AFA as you would add any other device.

To define a router as a monitoring device:

1. View the graphic network map. For details, see AFA's graphic network map.
2. Right click on the router you want to define as a monitoring device, and then click **Define as Routing Element**.

   The **Devices setup** page appears with the IP address field pre-filled.
3. Continue defining the routing element.

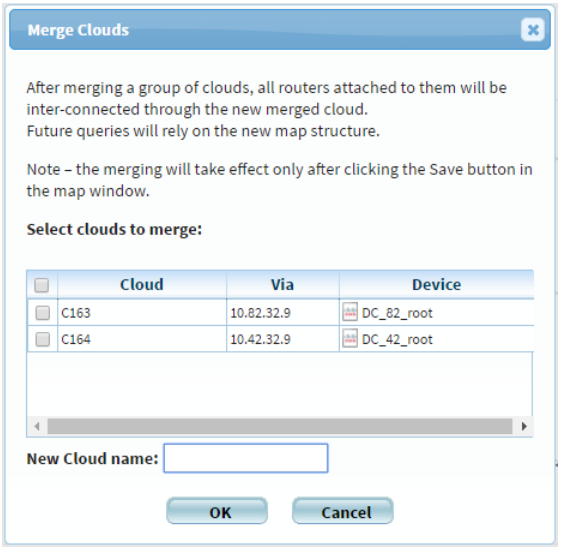
Merging Clouds

If the same cloud appears twice in the graphic network map, you may want to merge the two instances.

To merge two clouds:

1. View the graphic network map. For details, see AFA's graphic network map.
2. Select the clouds by doing one of the following:
   - Search for the clouds:
     1. Search for the clouds.
     2. Click the **Merge Clouds** link.
   - Manually select the clouds:
     1. Select two clouds you want to merge.
     2. Right-click on one of the selected clouds, and then click **Merge Clouds**.

The **Merge Clouds** dialog box opens.



3. If you used the **Merge Clouds** link, select the clouds to merge.
4. In the **New Cloud name** field, type a name for the merged cloud.
5. Click **OK**.

   The merged cloud appears in the map.
6. Click **Save**.

   Note: To ensure that subsequent activity is based on the updated map, save immediately.

   A confirmation message appears.
7. Click **OK**.

Un-merging Merged Clouds

You can unmerge clouds that were merged.

To unmerge merged clouds:

1. View the graphic network map. For details, see AFA's graphic network map.
2. Right-click on the merged cloud, and then click **Un-merge Clouds**.

   The two previously merged clouds appear separately on the map.
3. Click **Save**.

   A confirmation message appears.
4. Click **OK**

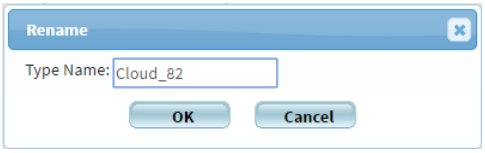
Renaming Graphic Network Map Elements

You can rename any element other than an edge.

To rename elements:

1. View the graphic network map. For details, see AFA's graphic network map.
2. Right-click on the element you want to rename, and then click **Rename**.

   The **Rename** dialog box opens.



3. In the **Type Name** field, type a new name for the element.
4. Click **OK**.

   The element is renamed.
5. Click **Save**.

   A confirmation message appears.
6. Click **OK**.

Moving Graphic Network Map Elements

You can change the location of elements in the graphic network map.

Note: Moving edges directly is not supported. Edges move automatically when the element to which they are connected is moved.

Note: An element will remain in its position for the remainder of the session, even if the map is not saved, and even if you navigate away from the map.

To move an element:

- Click on the desired element and drag it to the desired location on the map.

To move multiple elements:

1. Select multiple elements.
2. Drag the elements to the desired location on the map.

   Note: If the neighborhood of a device (network map elements which do not connect two devices) is hidden, moving the device automatically moves its neighborhood.

Removing Device Interfaces

You can specify that certain device interfaces be ignored in the graphic network map. Removed interfaces will be ignored when performing a traffic simulation query.

To remove device interfaces:

1. View the graphic network map. For details, see AFA's graphic network map.
2. Right-click on the edge that represents the interface you want to remove.
3. Click **Remove Interface**.

   The interface is removed.

Managing Layer 2 Devices in the Map

Many organizations use layer 2 (L2) devices in their network infrastructure as an additional security mechanism for their layer 3 devices. You can place layer 2 devices into subnets in the network map to allow more accurate traffic simulation results and change management, as well as a more accurate visual representation of the network in the map.

An L2 device can be in one of two states in AFA:

- **Unplaced**. Not associated with a subnet.
- **Placed**. Associated with a specific subnet.

To place an L2 device in a subnet (transit network or computer network) from the perspective of the device, see Placing an L2 Device into a Subnet from the Main Menu.

To place or remove L2 devices from the perspective of the subnet (transit network or computer network), see Placing Any L2 Devices into a Subnet or Removing L2 Devices from a Subnet.

Placing an L2 Device into a Subnet from the Main Menu

You can place an L2 device into a subnet directly from the main menu. In the main menu, unplaced L2 devices appear orange.

Note: This procedure is only for L2 devices that appear in the main menu. If the L2 device does not appear in the main menu, see Placing Any L2 Devices into a Subnet.

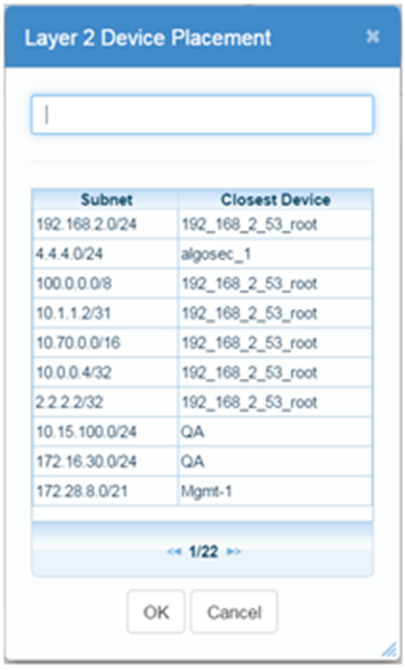
To place an L2 device into a subnet from the main menu:

1. In the main menu, select the L2 Device.

   A notification appears, indicating the device is not placed in a subnet.

2. Click the **Place now** link.

The **Layer 2 Device Placement** dialog box appears.



3. Select a **Subnet/Closest Device**, or perform a search by typing into the field.
4. Click **OK**.

   The device is placed in the subnet.

Placing Any L2 Devices into a Subnet

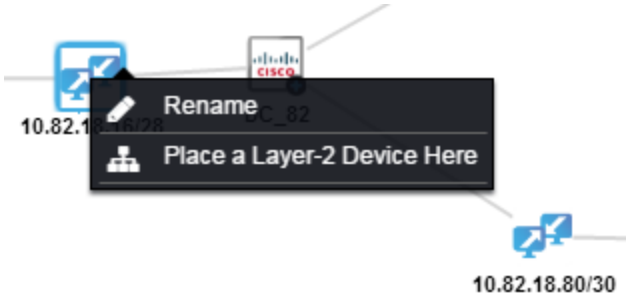
You can optionally place L2 devices from the perspective of the subnet. You can perform the following actions:

- Place an unplaced L2 device into a subnet
- Move placed L2 devices into a different subnet
- Place several L2 devices into a subnet at once
- Place any L2 devices into a subnet that do not appear with a **Place now** link in the main menu

To place any L2 devices into a subnet:

1. In the map, right click the subnet (either a computer network or transit network).

   A menu appears.



2. Select **Place a Layer-2 Device Here**.

   The **Layer 2 Device Placement** dialog box appears.

3. Select one or more devices from the **Device** list, or perform a search by typing into the field.

4. Click **OK**.

   The devices are placed in the subnet.

5. Save the map. For details, see Saving the Graphic Network Map.

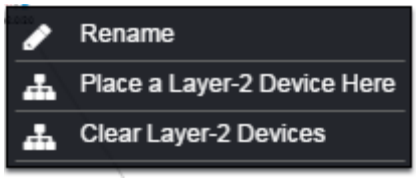
Removing L2 Devices from a Subnet

This procedure is performed from the graphic network map.

To remove all the L2 devices from a subnet:

1. In the map, right click the subnet whose devices you want to remove.

   A menu appears.



2. Select **Clear Layer-2 Devices**.

   All of the subnet's L2 devices are removed.

3. Save the map. For details, see Saving the Graphic Network Map.

Saving the Graphic Network Map

Any changes you make to the graphic network map will not remain in the map unless you save the map.

Note: Unsaved changes are reflected in the map but will **not** be reflected in queries or route lookups.

To save changes made to the graphic network map:

1. View the graphic network map. For details, see AFA's graphic network map.
2. Click **Save**.

   A warning message appears.

3. Click **OK**.

   Your changes are saved.

Automatically Rearranging the Graphic Network Map

You can automatically rearrange the Graphic Network Map to see the elements in a different position.

To rearrange the graphic network map:

1. View the graphic network map. For details, see AFA's graphic network map.
2. Click **Rearrange Map**.

   A warning message appears.
3. Click **OK**.

Refreshing the Graphic Network Map

Refreshing the Graphic Network Map causes the following:

- All device neighborhoods will be hidden
- Any newly added devices will be added
- Any unsaved changes will be discarded

To refresh the graphic network map:

1. View the graphic network map. For details, see AFA's graphic network map.
2. Click **Refresh Map**.

   The map is refreshed.

Run traffic simulation queries

This section explains how to perform traffic simulation queries and routing queries.

Overview

Once AFA has analyzed a device, group, or matrix, you can issue your own traffic simulation query to be tested against the policy. When running a traffic simulation query on a group or matrix, AFA finds the devices in the path of the traffic, using the graphic network map, and queries all these devices. If traffic is blocked by the device, you can determine which rules block it. This provides you with a powerful help desk support functionality. Furthermore, using the traffic simulation query feature allows users to determine whether the devices are protecting the organization's networks against traffic from a new exploit, or which device is letting a particular type of traffic through.

NAT is fully supported for traffic simulation queries on groups of devices. When finding the devices in the path of the traffic for a group, AFA supports both NAT and Proxy ARP. AFA predicts the devices in the path and then validates the prediction with the query information. When the query information matches the path, the source and destination values for all relevant devices in the path are updated. When only part of the traffic is translated, the downstream devices are queried for both the pre- and post-NAT values. This produces an accurate query, where no relevant traffic is ignored. If you want to run a traffic simulation query, but you only know post-NAT values, you can look up the pre-NAT values with which to run the query. For details, see Find NAT values.

AFA additionally provides the option to run a routing query to determine the devices in the path, without policy simulation. Note that routing queries ignore NAT. For details, see Run a routing query.

Run traffic simulation queries on individual devices

AFA enables you to run a traffic simulation query on an individual device's current or past policy.

Do the following:

1. Verify your permissions. To run a successful query, you must have access to all the firewalls that are relevant for your query results path. Queries will fail if the query goes through a non-permitted device.

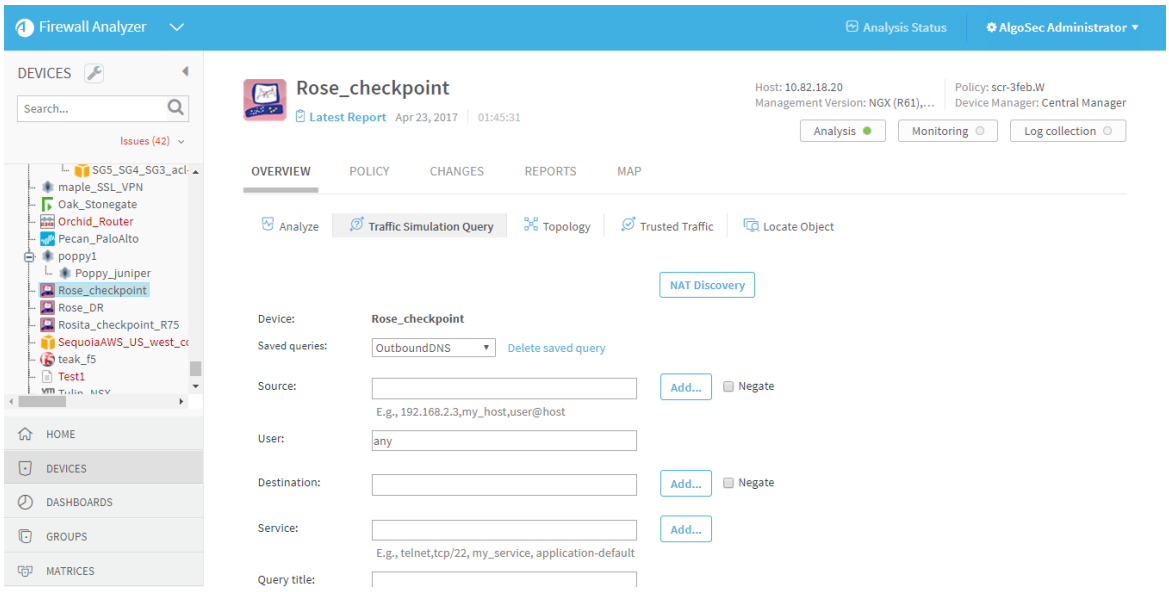
   Users with permissions to view an entire group can run queries on the group. If you do not have permission to view a group of devices, or the **ALL_FIREWALLS** group, we recommend that you perform single-device queries on the devices you have permissions to view. For more details, see Run traffic simulation queries on groups.

2. View a device report, as follows:

Run a query on a device's latest policy	View the device, and then continue with step 2.
Run a query on an earlier version of the device policy	View the device and click the **Reports** tab. There, select the report for the time you want to query, and continue with step 2.

3. Click **Traffic Simulation Query**.

   The **Traffic Simulation Query** page appears.



4. To load a saved query, select the desired query in the **Saved queries** drop-down list.

   The fields are populated with the saved query's data.

   For information on saving queries, see Save traffic simulation queries.

5. Specify the source and destination, by doing one or more of the following:

   Specify a source/destination that is not defined in AFA

   Enter an IP address, IP address range, CIDR, or host group name in the relevant field (**Source** or **Destination**).

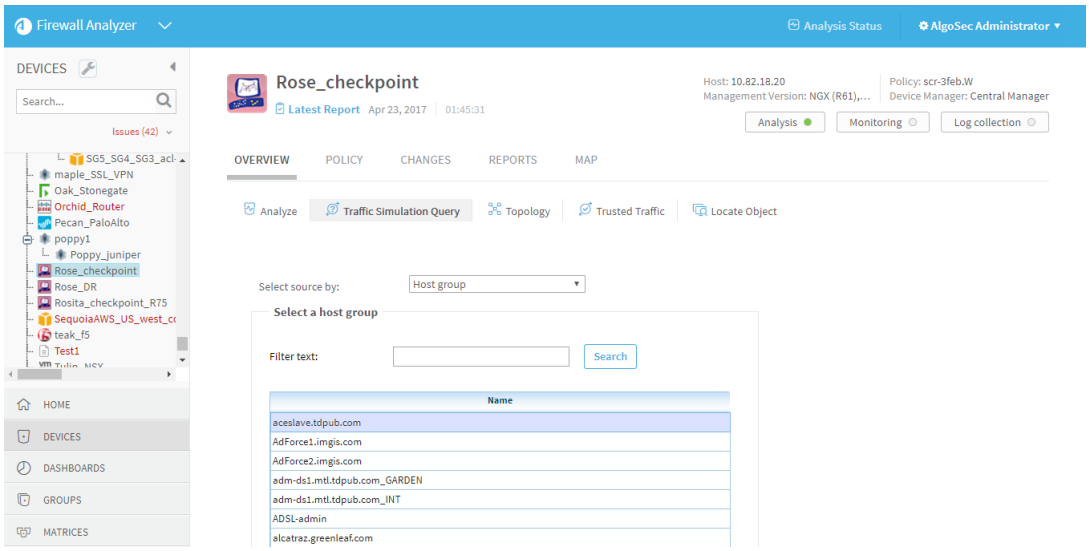
   You can specify multiple sources/destinations by separating them with commas.

   Specify a source/destination already defined in AFA

   Do the following:

   a. Click **Add** to the right of the desired field (**Source** or **Destination**).

      The **Add source** or **Add destination** dialog box appears.



   b. Specify the desired source or destination.

You can select either an individual IP address, a range of IP addresses, CIDR, or a host group that is defined on the device. If you wish to select a host group, you can search the defined names alphabetically, or by using the search filter.

c. Click **OK**.

You can specify multiple sources/destinations, by repeating this step.

Note: You can run a query for the source/destination that you specify, or the negation of the source/destination that you specify (all IPs other than the source/destination that you specify).

6. To negate the source and/or destination that you specified, select the **Negate** check box to the right of the desired field.

   If you specified multiple IP addresses, IP address ranges, and/or hostgroups, the union of these values is negated.

7. Specify the service by doing one or more of the following:

   Specify a service that is not defined in AFA

   In the **Service** field, type the desired service's definition.

   You can query multiple services by separating them with commas. For example: "tcp/123, udp/9911".

   Specify a service that is already defined in AFA

   Do the following:

   a. To the right of the **Service** field, click **Add**.

      The **Select Service** dialog box appears.

b. You can filter the information displayed in the list, by doing one or more of the following:

   - To filter the information displayed in the list by service name, type the desired service name in the **Filter by Name** field, and then click **Filter**.
   - To filter the information displayed in the list by service definition, type the desired service definition in the **Definitions** field, and then click **Filter**.

   To clear the filter, click **Reset**.

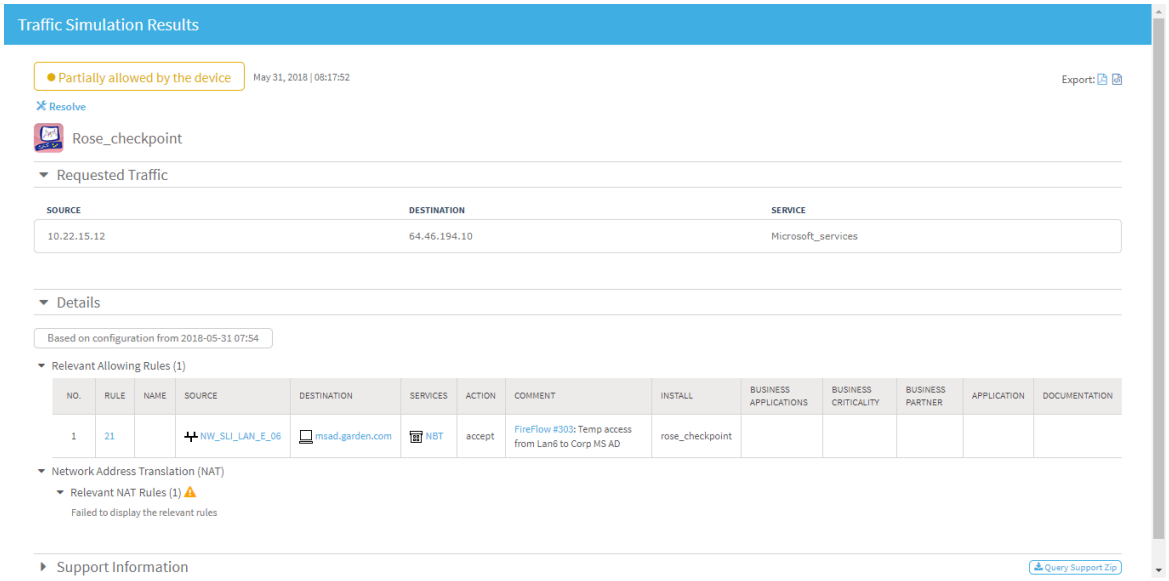
c. Select the desired service.

d. Click **Add**.

   You can specify multiple services, by repeating this step.

8. (Optional) In the **Query title** field, type a name for the query.
9. Click **Run Query**.

   A new window opens displaying the query results.



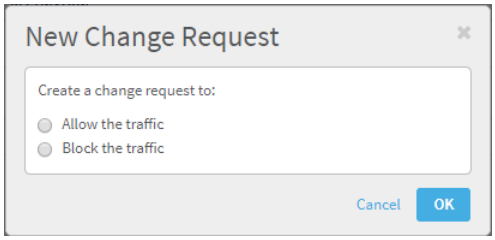
The **Details** area displays the query results. The fields that appear for each rule depends on the device brand. If AppViz is licensed, fields from AppViz appear, indicating business information such as which rules are included as flows in which applications.

If NAT is performed by the device, the NAT rules appear in tooltips in the map. For Check Point and Cisco ASA devices which perform NAT, a table of applied NAT rules appears below the map.

10. To open a FireFlow change request to allow the blocked traffic or block the allowed traffic, do the following:

    a. Click Resolve .

    The **New Change Request** window appears.



If the result of the query is **Blocked**, the change request will open the traffic. If the result of the query is **Allowed**, the change request will block the traffic. If the result of the query is **Partially Allowed**, you are prompted to chose whether to allow or block traffic.

b. If the result of the query is **Partially Allowed**, select whether to block or allow the traffic.

c. Click **OK**.

The change request is opened. Once the change request is successfully created, a link to the change request appears.

By default, the change request will use the default traffic change request template (which is the Standard template, by default).

11. To export the query results to PDF, click in the top-right corner of the report. For more details, see Export AFA screens to PDF.

To export to CSV format, click in the top-right corner of the report. Follow your browser prompts to open or save the CSV file.

Run traffic simulation queries on groups

When running traffic simulation queries on device groups, AFA finds the devices in the path of the query by simulating routing and NAT across the entire network. AFA then simulates the policy on each relevant device to determine if it blocks or allows the traffic that reaches it.

AFA uses the graphic network map when querying groups; therefore, it is important to ensure that the map is correct. For details, see AFA's graphic network map.

To run a traffic simulation query on a group:

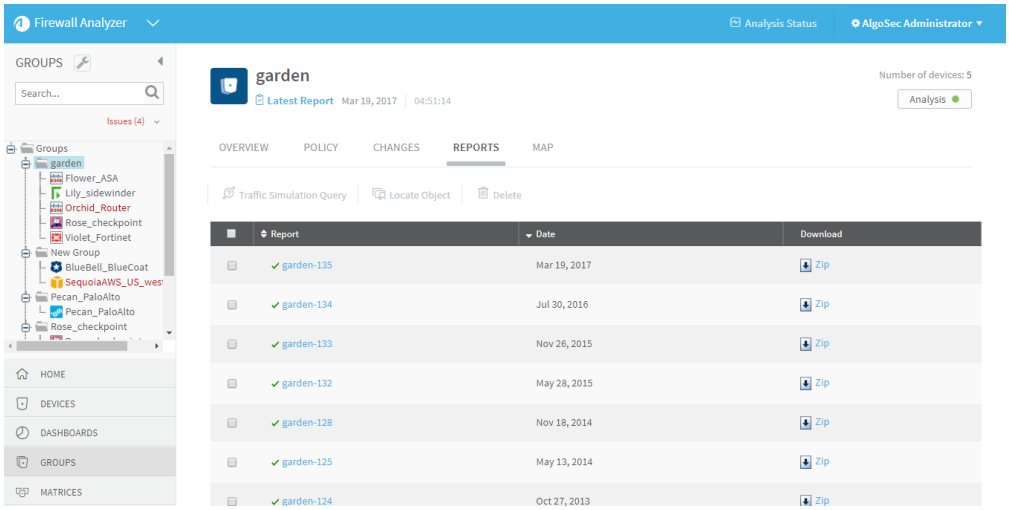
1. Verify your permissions. To run a successful query, you must have access to all the firewalls that are relevant for your query results path. Queries will fail if the

query goes through a non-permitted device.

Users with permissions to view an entire group can run queries on the group. If you do not have permission to view a group of devices, or the **ALL_FIREWALLS** group, we recommend that you perform single-device queries on the devices you have permissions to view. For more details, see Run traffic simulation queries on individual devices.

2. Do one of the following. For details, see View AFA group data.
   - To run a query on a group's latest policies, view the desired group.
   - To run a query on a group's older policies:
     a. View the desired group.
     b. Click the **Reports** tab.

        The **Reports** page appears.



     c. Select the check box next to the desired report.

3. Click **Traffic Simulation Query**.

   The **Traffic Simulation Query** page appears.

4. To load a saved query, select the desired query in the **Saved queries** drop-down list.

The fields are populated with the saved query's data.

For information on saving queries, see Save traffic simulation queries.

5. Specify the source and destination, by doing one or more of the following:

   Specify a source/destination that is not defined in AFA

   Enter an IP address, IP address range, CIDR, or host group name in the relevant field (**Source** or **Destination**).

   You can specify multiple sources/destinations, by separating them with commas.

   Specify a source/desintation that is already defined in AFA

   Do the following:

   a. Click **Add** to the right of the desired field (**Source** or **Destination**).

      The **Add source** or **Add destination** dialog box appears.

   b. Specify the desired source or destination.

      You can select either an individual IP address, a range of IP addresses, CIDR, or a host group that is defined on the device. If you wish to select a host group, you can search the defined names alphabetically, or by using the search filter.

   c. Click **OK**.

      You can specify multiple sources/destinations, by repeating this step.

   Note: You can run a query for the source/destination that you specify, or the negation of the source/destination that you specify (all IPs other than the source/destination that you specify).

6. To negate the source/destination that you specified, select the **Negate** check box to the right of the desired field.

If you specified multiple IP addresses, IP address ranges, and/or hostgroups, the union of these values is negated.

7. Specify the service by doing one or more of the following:

   Specify a service that is not defined in AFA

   In the **Service** field, type the desired service's definition.

   You can query multiple services by separating them with a comma. For example: "tcp/123, udp/9911".

   Specify a service already defined in AFA

   Do the following:

   a. To the right of the **Service** field, click **Add**.

      The **Select Service** window appears.

   b. You can filter the information displayed in the list, by doing one of the following:

      - To filter the information displayed in the list by service name, type the desired service name in the **Filter by Name** field, then click **Filter**.
      - To filter the information displayed in the list by service definition, type the desired service definition in the **Definitions** field, then click **Filter**.

      To clear the filter, click **Reset**.

   c. Select the desired service.

   d. Click **Add**.

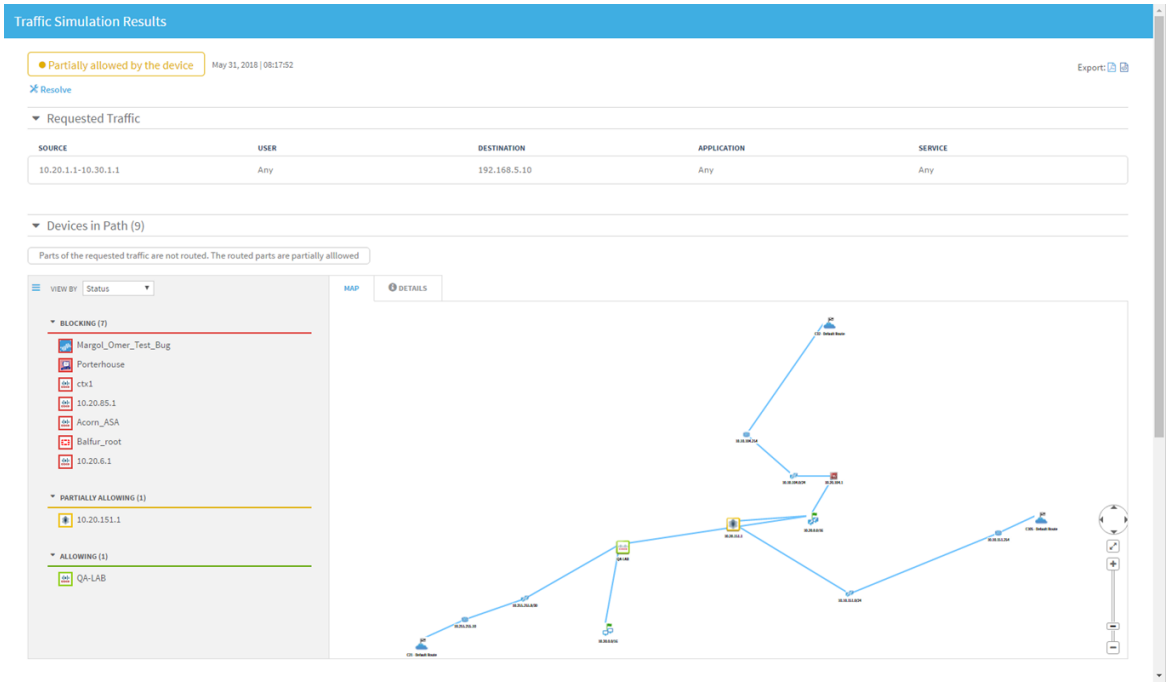
      You can specify multiple services, by repeating this step.

8. (Optional) In the **Query title** field, type a name for the query.
9. (Optional) To specify that query results should be grouped by policy, and only one device should be displayed per policy, select the **Group by Policy** check box.

This option is only available if grouping query results by policy is enabled in the system.

10. Click **Run Query**.

    A new window opens displaying the query results.



The list of devices and the graphic network map appear. In both the map and the list, a colored box around each device indicates whether traffic is allowed (green), blocked (red), or partially allowed through the device (yellow). Clicking on a device in the list will shift the map's focus to that device.

The list of devices appears sorted by **Status**: **Blocking**, **Partially Allowing** or **Allowing**. Details for each device and any support information appears at the bottom of the page.

Note: When the path of the query intersects an IP addresses in a host-based device, the device is represented in the results map. For VMware NSX or Cisco

ACI, the device and relevant IP address is always represented by a single icon. For AWS and Azure, the individual internal elements (such as VPC / VNet routers) may additionally appear in the map.

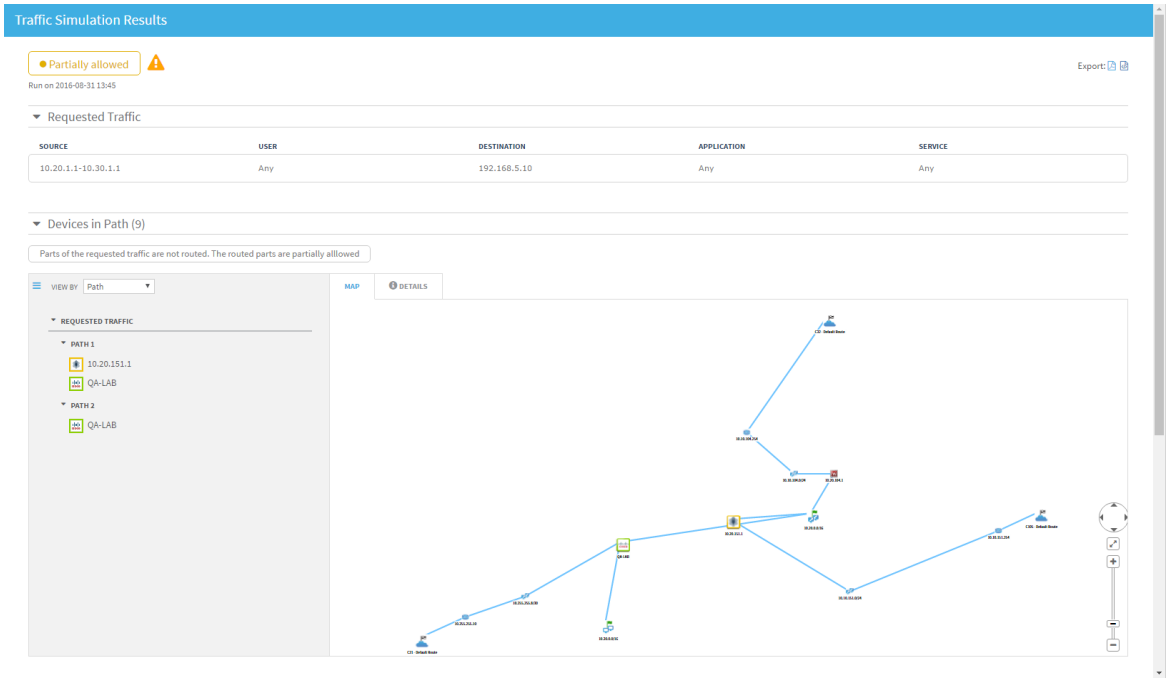
In the map, the sources are marked with a green flag  , and destinations are marked with a checkered flag  . The path between each source and destination is marked in blue. You can zoom in, zoom out, resize the graphic network map to fit the screen, and pan the view. For details, see AFA's graphic network map.

The map indicates if they perform NAT with a NAT icon. Hovering over NAT devices displays the translation information for source and destination. Additionally, a table of applied NAT rules is displayed. If NAT is performed before traffic reaches a device, the results specify that the source and/or destination was modified before reaching the device.

Note: If you ran the query from the **Groups** tab, the query result is also stored and attached to the report. To view it later, go to the **Policy** page in the report. If you specified a query title, then this title will be shown in the **Policy** page. Otherwise a default title is selected.

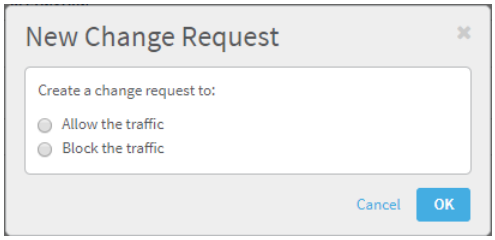
11. To view the list of devices by **Path**, in the **View By** drop-down list, select **Path**.

    The devices appear according to relevant traffic paths. Each device in the path appears sequentially, from source to destination.



12. Right click on the map frame to see (depending upon the device type) the following selections:
    - Routing Information
    - Connectivity Diagram
    - Latest Report
13. To open a FireFlow change request to allow the blocked traffic or block the allowed traffic, do the following:
    a. Click Resolve .

    The **New Change Request** window appears.



If the result of the query is **Blocked**, the change request will open the traffic. If the result of the query is **Allowed**, the change request will block the traffic. If the result of the query is **Partially Allowed**, you are prompted to chose whether to allow or block traffic.

b. If the result of the query is **Partially Allowed**, select whether to block or allow the traffic.

c. Click **OK**.

The change request is opened. Once the change request is successfully created, a link to the change request appears.

By default, the change request will use the default traffic change request template (which is the Standard template, by default).

14. To export the query results to PDF, click in the top-right corner of the report. For more details, see Export AFA screens to PDF.

To export to CSV format, click in the top-right corner of the report. Follow your browser prompts to open or save the CSV file.

Run traffic simulation queries on matrices

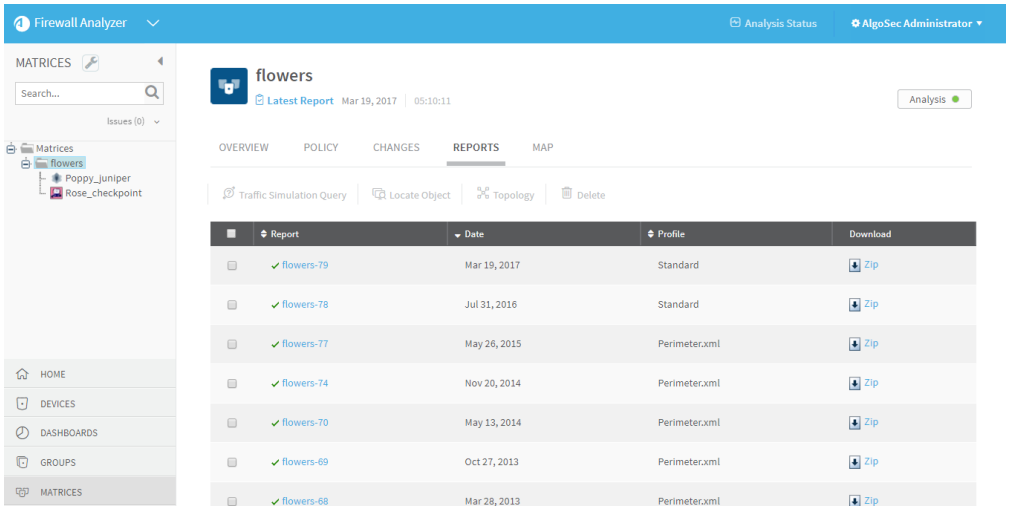
Running a traffic simulation query on a generated matrix analysis report enables you to do the following:

- Determine whether a specific type of traffic is allowed or blocked through the network.
- View the traffic type's returning path across the devices.
- View a list of rules in each device that allow or block the traffic type.

To run a traffic simulation query on a matrix:

1. Do one of the following. For details, see View AFA matrix data.
   - To run a query on a matrix's latest policies, view the desired matrix.
   - To run a query on a matrix's older policies, do the following:
     1. View the desired matrix.
     2. Click the **Reports** tab.

        The **Reports** page appears.

     3. Select the check box next to the desired report.
2. Click **Traffic Simulation Query**.

   The **Traffic Simulation Query** page appears.
3. To load a saved query, select the desired query in the **Saved queries** drop-down list.

   The fields are populated with the saved query's data.

   For information on saving queries, see Save traffic simulation queries.
4. Specify the source and destination, by doing one or more of the following:

Note: You can run a query for the source/destination that you specify, or the negation of the source/destination that you specify (all IPs other than the source/destination that you specify).

- To specify a source/destination that is already defined in AFA:
  1. Click **Add** to the right of the desired field (**Source** or **Destination**).

     The **Add source** or **Add destination** dialog box appears.
  2. Specify the desired source or destination.

     You can select either an individual IP address, a range of IP addresses, CIDR, or a host group that is defined on the device. If you wish to select a host group, you can search the defined names alphabetically, or by using the search filter.
  3. Click **OK**.

     You can specify multiple sources/destinations, by repeating this step.
- To specify a source/destination that is not defined in AFA, type an IP address, IP address range, CIDR, or host group name in the relevant field (**Source** or **Destination**).

  You can specify multiple sources/destinations, by separating them with commas.

5. To negate the source/destination that you specified, select the **Negate** check box to the right of the desired field.

   If you specified multiple IP addresses, IP address ranges, and/or hostgroups, the union of these values is negated.

6. Specify the service, by doing one or more of the following:
    - To specify a service that is already defined in AFA:
        1. To the right of the **Service** field, click **Add**.

           The **Select Service** window appears.
        2. You can filter the information displayed in the list, by doing one of the following:
            - To filter the information displayed in the list by service name, type the desired service name in the **Filter by Name** field, then click **Filter**.
            - To filter the information displayed in the list by service definition, type the desired service definition in the **Definitions** field, then click **Filter**.

           To clear the filter, click **Reset**.
        3. Select the desired service.
        4. Click **Add**.

           You can specify multiple services, by repeating this step.
    - To specify a service that is not defined in AFA, in the **Service**field, type the desired service's definition.

      You can query multiple services by separating them with a comma. For example: "tcp/123, udp/9911".
7. (Optional) In the **Query title** field, type a name for the query.
8. Click **Run Query**.

   A new window opens displaying the query results.

   The **Details** area displays the query results. The fields that appear for each rule depends on the device brand. If AppViz is licensed, fields from AppViz appear,

indicating business information such as which rules are included as flows in which applications.

If NAT is performed by the device, the NAT rules appear in tooltips in the map. For Check Point and Cisco ASA devices which perform NAT, a table of applied NAT rules appears below the map.

Note: If you ran the query from the **Matrices** tab, the query result also is stored and attached to the report. To view it later, go to the **Policy** page in the report. If you specified a query title, then this title will be shown in the **Policy** page. Otherwise a default title is selected.

9. To export the query results to PDF, click in the top-right corner of the report. For more details, see Export AFA screens to PDF.

   To export to CSV format, click in the top-right corner of the report. Follow your browser prompts to open or save the CSV file.

Save traffic simulation queries

Some traffic simulation queries are repeated often. AFA allows saving the source, destination, service and title values of such queries, and then reloading them when they are needed again. The saved queries are kept for each user individually, for maximum customization. Saved queries can be used for both single device queries and group queries.

To save a traffic simulation query:

1. Fill in the query form.
2. Click **Save Query**.

   The **Save Query As** window appears.

3. In the field, type a name for the query.
4. Click **OK**.

   The query is saved.

Delete saved traffic simulation queries

To delete a saved traffic simulation query:

1. Access the query form.
2. In the **Saved queries** list, select the desired query.
3. Click **Delete saved query**.

   The query is deleted.

Find NAT values

AFA provides the ability to look up all the potential translations to and or from an IP address. This is particularly useful if you want to run a traffic simulation query, but you only know a post-NAT value. You can look up the pre-NAT value(s) with which to run the query.

Note: The results of this search include all possible translations across all NAT rules and configurations.

1. View the desired device. For details, see View AFA device data.
2. Click **Traffic Simulation Query**.

   The **Traffic Simulation Query** page appears.
3. Click NAT Discovery.

The **Discover NAT Assistant** dialog box appears.

4. In the **Type a single IP** field, type a single IP address.
5. Using the **IP address can be** check boxes, indicate whether the IP address can be a **Pre-NAT** value, **Post-NAT** value, or both.
6. Using the **Discover NAT address in** check boxes, indicate whether the IP address can be a **Source**, **Destination**, or both.
7. Click **Discover**.

   The results appear.

   The results indicate the device name, the potential pre- and post-NAT values, and whether the NAT is static or dynamic.

Run a routing query

Run a routing query to see the devices in the path of a route without policy simulation.

Note: When running a routing query, NAT is ignored.

Note: Traffic simulation queries include policy simulation and take NAT into account. Consequently, they produce a more accurate path when NAT is involved (especially for a group of devices). For details, see Run traffic simulation queries.

To run a routing query:

1. View the graphic network map. For details, see AFA's graphic network map.
2. Click **Routing Query**.

   The **Routing Query** dialog box appears.
3. In the **Source** field, type the relevant IP address or CIDR.

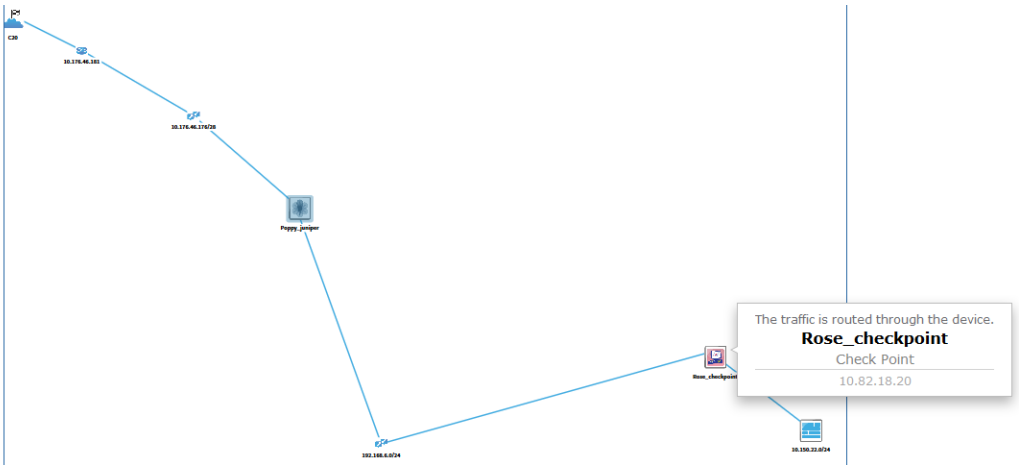
   Note: IP ranges are not a supported format for this field.

4. In the **Destination** field, type the relevant IP address or CIDR.

   Note: IP ranges are not a supported format for this field.

5. Click **Run Query**.

   The results appear in a new window. The path of the traffic is highlighted in blue on the graphic network map. When hovering over the route, all devices in the path display a tooltip that states "Traffic is routed through this device".



AFA dashboards

This section explains how to view dashboards in AFA and how to use the AlgoSec Reporting Tool.

AFA dashboards provide the ability to quickly and easily view a summary of risks, compliance, optimizations, and/or changes for all devices.

Note: For more details, see AlgoSec Reporting Tool.

Built-in AFA dashboards

AFA provides the following built-in AFA dashboards, which display data for all devices defined in the **ALL_FIREWALLS** group.

Summary	Displayed by default when logging in to AFA. Modify this default in the **AFA Administration** area. Includes the following charts: • **Risks per 16 devices with the most High severity risks in group ALL_FIREWALLS.** A bar chart showing the number of high, suspected high, medium, and low risks per device, for the top 16 devices. There are four bars per device. • **Security rating over time for devices in group ALL_ FIREWALLS.** A trend chart showing the average security rating over all devices, over time. • **Total Number of Rules per Device in group ALL_ FIREWALLS.** A bar chart showing the total number of rules per device, for the top 25 devices. • **Number of changes in the last 30 days in group ALL_ FIREWALLS**. A trend chart showing the total number of changes to all devices, over the last 30 days. **Note:** This chart will have no data for devices which have monitoring turned off.

Baseline Compliance	Includes the following charts: • **Devices with lowest baseline compliance score in group ALL_FIREWALLS.** A bar chart showing the 20 lowest baseline compliance scores per firewall. • **Number of devices that have passing baseline score (over 5) in group ALL_FIREWALLS**. A trend chart showing the number of firewalls meeting over 50% of the baseline requirements. • **Baseline compliance score over time for devices in group ALL_FIREWALLS.** A trend chart showing the average and minimum baseline compliance scores of the ALL_FIREWALLS group.
Changes	Includes the following charts: • **20 devices with the most changes in the last 30 days in group ALL_FIREWALLS**. A bar chart showing the total number of changes on each device for the top 20 devices, over the last 30 days. **Note:** This chart will have no data for devices which have monitoring turned off. • **Number of changes in the last 30 days in group ALL_FIREWALLS**. A trend chart showing the total number of changes to all devices, over the last 30 days. **Note:** This chart will have no data for devices which have monitoring turned off.

Optimizations	Includes the following charts: • **Number of Covered Rules per Device on group ALL_ FIREWALLS.** A bar chart showing the number of covered rules per device, for the top 25 devices. • **Number of Special Case Rules per Device on group ALL_ FIREWALLS**. A bar chart showing the number of redundant special case rules per device, for the top 25 devices. • **Number of Unused Rules per Device on group ALL_ FIREWALLS.** A bar chart showing the number of unused rules per device, for the top 25 devices. • **Total Number of Rules per Device on group ALL_ FIREWALLS.** A bar chart showing the total number of rules per device, for the top 25 devices.
Compliance	AFA has a compliance dashboard for each enabled regulatory compliance report. Each one includes the following charts: • **Devices with lowest compliance score in group ALL_ FIREWALLS.** A bar chart showing the 20 lowest compliance scores per firewall. • **Number of devices by compliance score color in group ALL_ FIREWALLS.** A trend chart showing the number of firewalls that have green, yellow or red compliance colors. • **Compliance score over time for devices in group ALL_ FIREWALLS.** A trend chart showing the average and minimum compliance scores of the ALL_FIREWALLS group.

Risks	Includes the following charts: • **Number of devices by leading risk severity in group ALL_ FIREWALLS**. A bar chart showing the number of devices whose highest risk is high, suspected high, medium, and low. • **Risks per 16 devices with the most High severity risks in group ALL_FIREWALLS.** A bar chart showing the number of high, suspected high, medium, and low risks per device, for the top 16 devices. There are four bars per device. • **Number of devices by leading risk severity in group ALL_ FIREWALLS.** A trend chart showing the number of devices whose highest risk is high, suspected high, medium, and low, over time.

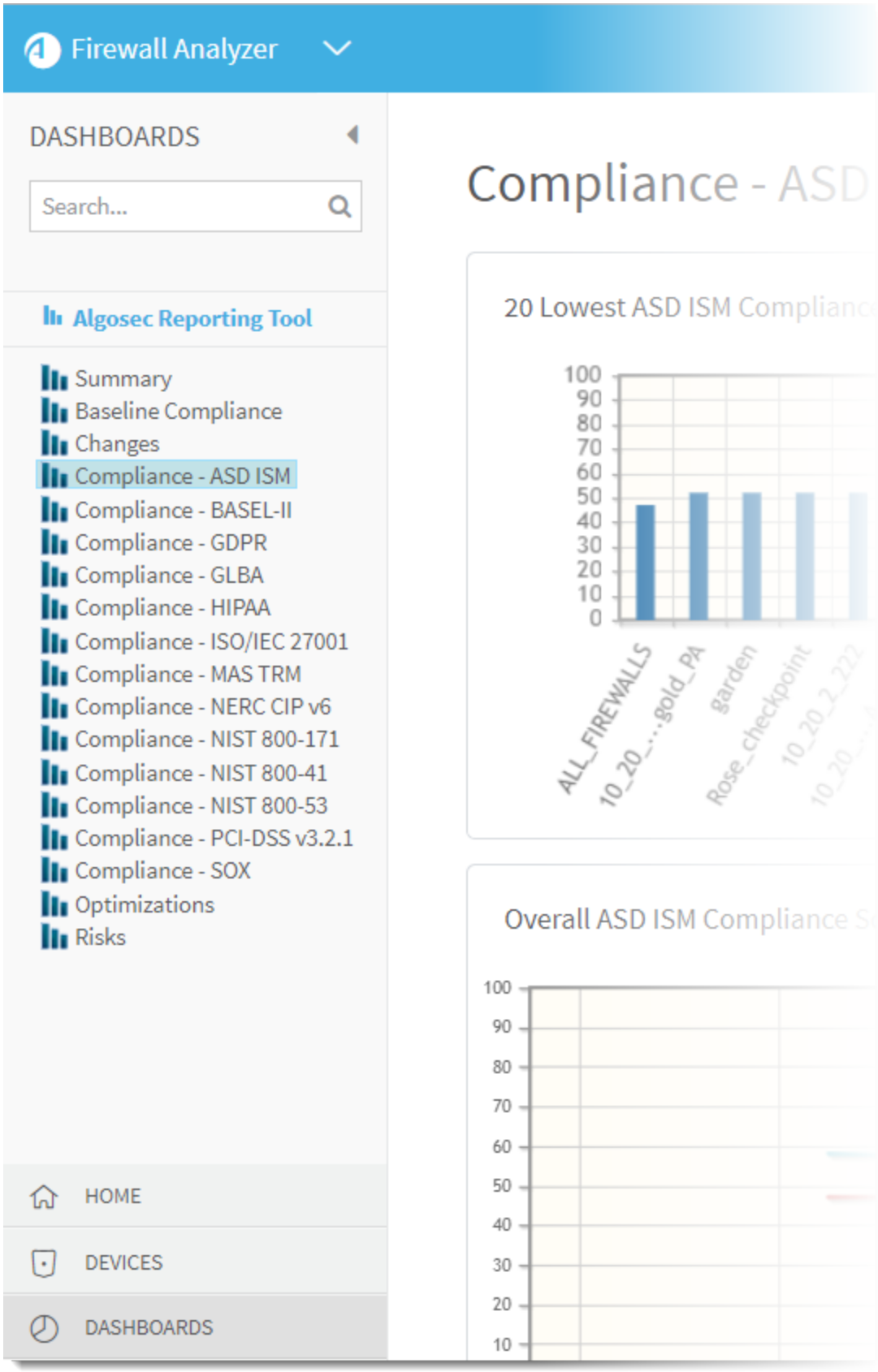
View AFA dashboards

This procedure describes how to view all built-in and custom dashboards defined in AFA.

Do the following:

1. In the main menu on the left, click **Dashboards**.

   The **Dashboards** menu expands, displaying all dashboards defined. For example:


Firewall Analyzer
DASHBOARDS
Search...
Algosec Reporting Tool
Summary
Baseline Compliance
Changes
Compliance - ASD ISM
Compliance - BASEL-II
Compliance - GDPR
Compliance - GLBA
Compliance - HIPAA
Compliance - ISO/IEC 27001
Compliance - MAS TRM
Compliance - NERC CIP v6
Compliance - NIST 800-171
Compliance - NIST 800-41
Compliance - NIST 800-53
Compliance - PCI-DSS v3.2.1
Compliance - SOX
Optimizations
Risks
HOME
DEVICES
DASHBOARDS
Compliance - ASD
20 Lowest ASD ISM Compliance
100
90
80
70
60
50
40
30
20
10
0
ALL_FIREWALLS
10_20_...gold_PA
garden
Rose_checkpoint
10_20_2_222
Overall ASD ISM Compliance S
100
90
80
70
60
50
40
30
20
10

Dashboards appear in red or orange to indicate failures, as follows:

- **Red** dashboards indicate that the last report generation had failed.
- **Orange** dashboards indicate that real-time monitoring or log collection have failed.

2. Click the node for the dashboard you want to view.

The selected dashboard and it's charts appear in the workspace.

AlgoSec Reporting Tool

This topic describes how to use the AlgoSec Reporting Tool (ART), which is an additional AFA reporting tool powered by Kibana.

ART enables you to visualize ASMS data about devices, change requests, and AppViz applications, in a variety of charts, tables, and dashboards.

Note: ART is powered by Kibana version 5.6.16. For more details, see the Kibana resources and documentation.

AlgoSec Reporting Tool prerequisites and permissions

Using ART to create and view advanced dashboards has the following requirements:

Enable ART operations	To enable ART for your ASMS system, you must have the **ART_Operation_Status** parameter set to **on** in the AFA **Administration** area. ART starts collecting data only from the date at which this parameter value is defined.
User access to ART data	ART is available only to users who are configured for access. Non-admin users who have access to ART will only see data relevant to their allowed firewalls.

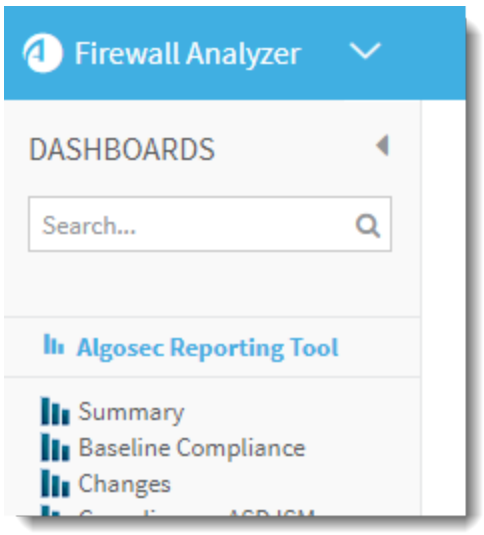
Access the AlgoSec Reporting Tool

The AlgoSec Reporting Tool is available from the main menu on the left in AFA or FireFlow, or from several areas in AppViz.

Access ART from AFA

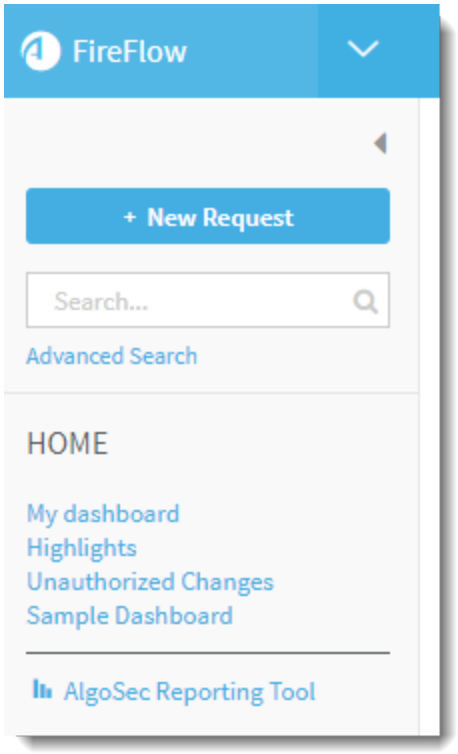
In AFA, click **DASHBOARDS** in the main menu on the left.

Then, above the list of default AFA dashboards, click the **AlgoSec Reporting Tool** link.



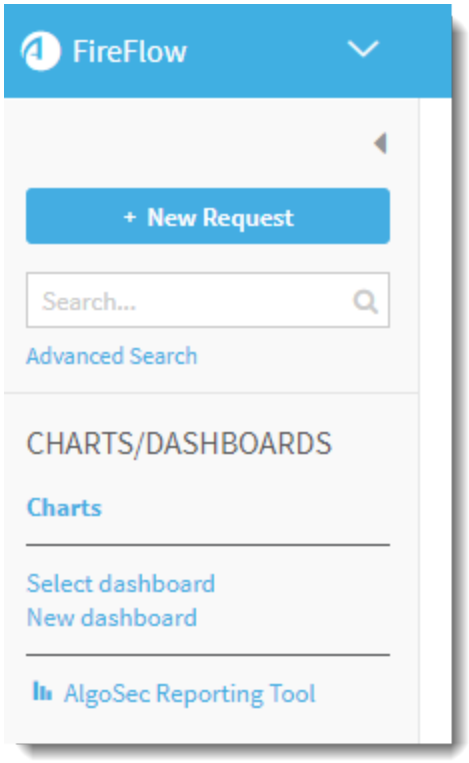
Access ART from the FireFlow HOME page

In FireFlow, click **HOME** in the main menu on the left. Then, below the options to select a dashboard or create a new one, click the **AlgoSec Reporting Tool** link.



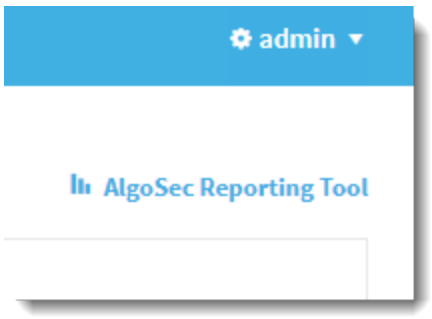
Access ART from the FireFlow CHARTS / DASHBOARDS page

In FireFlow, click **CHARTS/DASHBOARDS** in the main menu on the left. Then, below the options to select a dashboard or create a new one, click the **AlgoSec Reporting Tool** link.



Access ART from AppViz

In AppViz, use the main menu on the left to navigate to the **HOME**, **APPLICATIONS**, **NETWORK OBJECTS**, or **SERVICE OBJECTS** areas. Click the **AlgoSec Reporting Tool** link located just below the username menu.



Once in ART, do the following to view data and create charts and dashboards.

- Discover data
- Visualize data

- Create or edit dashboards

Tip: At the bottom-left, click **Collapse** to collapse the ART main menu. This provides you with more space to create and manage your data displays. Click the **Expand** button to show the menu again.

Discover data

In ART, click **Discover** to browse ASMS data and create search queries to use in graphs and charts. ART provides a few saved search queries out of the box, and also enables to you create custom searches and filters.

Save your search queries, export them, or share links with others.

Tip: Alternately, start by creating graphs and then add your data. For details, see Visualize a specific field and Visualize data.

Do the following:

1. From the main menu on the left, click **Discover**.
2. At the top-left, click the dropdown to select the type of data you want to view.

applications	View data by AppViz application.
change_requests	View data by FireFlow change requests.
devices	View data by devices managed by AFA.

Tip: Alternately, start with a saved search. Either click **Open** at the top of the page, or click **Management > Saved Objects > Searches**.

If you need to, search for the name of your saved search. Click a name to load the saved search.

3. Determine the field data displayed by adding field names to the list of **Selected**

Fields at the top-left.

- In the **Available Fields** area, hover over the field heading and click **Add** to add it to the selected fields.
- To remove a field from this list, hover over the field heading in the **Selected Fields** area and click **Remove**.

4. Filter the values of the fields displayed to further filter the data shown.

   Do the following:

   a. Above the data type dropdown, click **Add a Filter** ✚. For example:

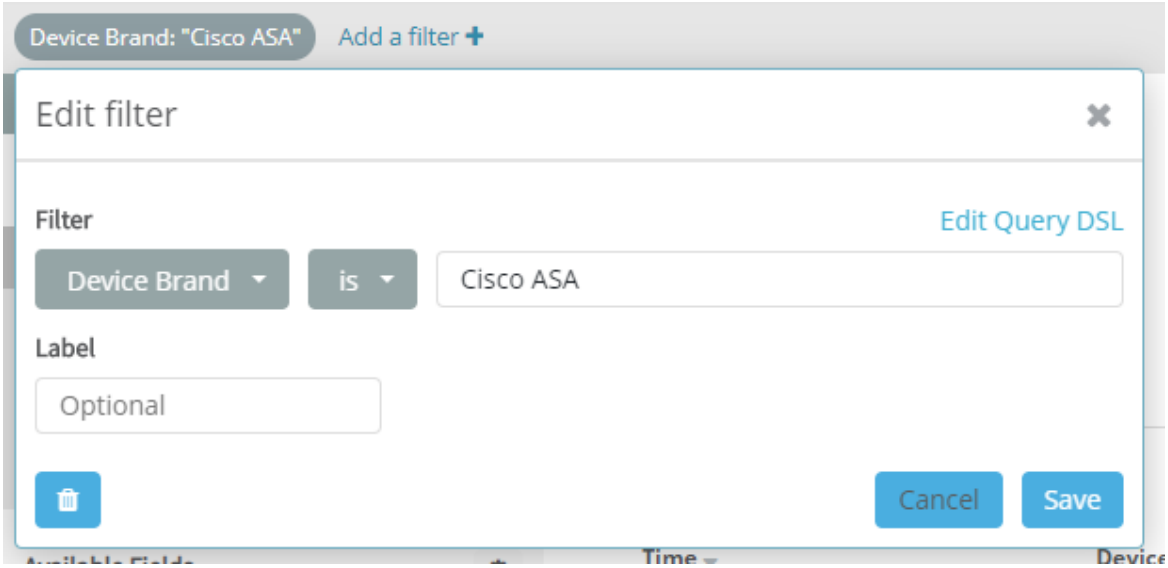
   b. In the **Add filter** dialog, enter a field name, operator, and value.

   > **Note:** When selecting the **is** or **is not** operator, values must match actual values exactly, and are case-sensitive.
   >
   > To display a list of actual field values, click a field value header. A bar graph expands to display the sum of each value for the field.

   c. Click **Save** to add the selected values to the filter.

   The field and value is added to the filter list above the data type dropdown and field lists.

   For example:



Filter field options

Once a field is added to the filter, hover over the field in the filter to display further options.

Do any of the following:

/	**Enable** or **disable** the filter field. Use this option to keep the filter values defined, but temporarily disable it for the current data displayed.
/	**Pin** or **unpin** the filter to the top. Use this option when you have several filters displayed, and you want to select specific filters to view at the top of the list.

/	**Invert** a field definition to show all results that do not match the values selected. Inverting a field turns the field definition red to indicate that the results shown are negative results. Click **Toggle** to return to the original field definition.
	Remove the field from the filter entirely. This removes your field values, and you'll need to define them from scratch if you need them again.
	Edit the field values selected. In the **Edit filter** dialog, update the selected filter name, operator, and value, and then click **Save**.

Tip: At the far right, click **Actions** ▼ to display these same actions for all filters defined.

Advanced query editing

ART provides the following advanced filter editing features for experienced Kibana or Elastisearch users.

- In the search bar at the top of the screen, enter a query syntax manually to define the field names and values for your filter.

  Click **Show Latest** to automatically add the **Current:true** field and filter out all historical data from the data displayed.

  For more details about query syntax, click the **Uses lucene query syntax** link at the right of the search box.

- In the **Edit filter** dialog, click **Edit Query DSL** to manually update or copy in an Elastisearch Query DSL to use for this field value definition.

5. At the top of the page, click any of the following to manage the filtered data:

New	Discard all of your changes and start a new filter from scratch.
Save	Save your filter so that you or other users can return to it later on. Click **Open** to view a list of saved searches.
Share	Display links to either share a saved search or a snapshot. **Tip:** Full link URLs may be long. Click **Copy** to copy the full URL to the clipboard, or **Short URL** to display a shorter URL that's easier to share.
Date selector	Define the date range for the data displayed. For details, see Change date ranges.

Continue with creating graphs and dashboards. For details, see Visualize a specific field, Visualize data, and Create or edit dashboards.

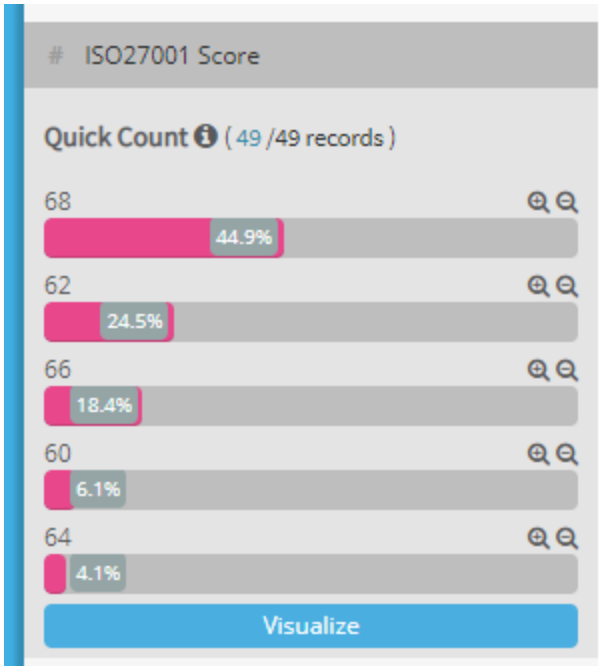
Visualize a specific field

Jump directly from the **Discover** section of ART to **Visualize** in order to create graphs based on a specific filter field.

Do the following:

1. Hover over any filter name in the **Selected** or **Available Fields** list to display a bar chart of the values for that field.

   For example:



2. Click **Visualize** to display the selected field in the **Visualize** area.

For more details, see Visualize data.

Visualize data

In ART, click **Visualize** to start by creating or loading graphs and charts and then adding or modifying the data used.

Export, share, or embed your visualizations in other locations, or add them to ART dashboards. For more details, see Create or edit dashboards.

Tip: Alternately, start by browsing data and then use that data to create graphs. For details, see Discover data.

Do the following:

1. Click **Visualize** from the main menu on the left.

   A list of saved visualizations is displayed.

Tip: Alternately, click **Visualize** from a specific field dropdown in the **Discover** area. For more details, see Visualize a specific field.

- Click the name of a saved search to display a chart based on that data.
- Click

2. Click the name of a saved visualization to view, or click **Create new visualization** to create a new one.

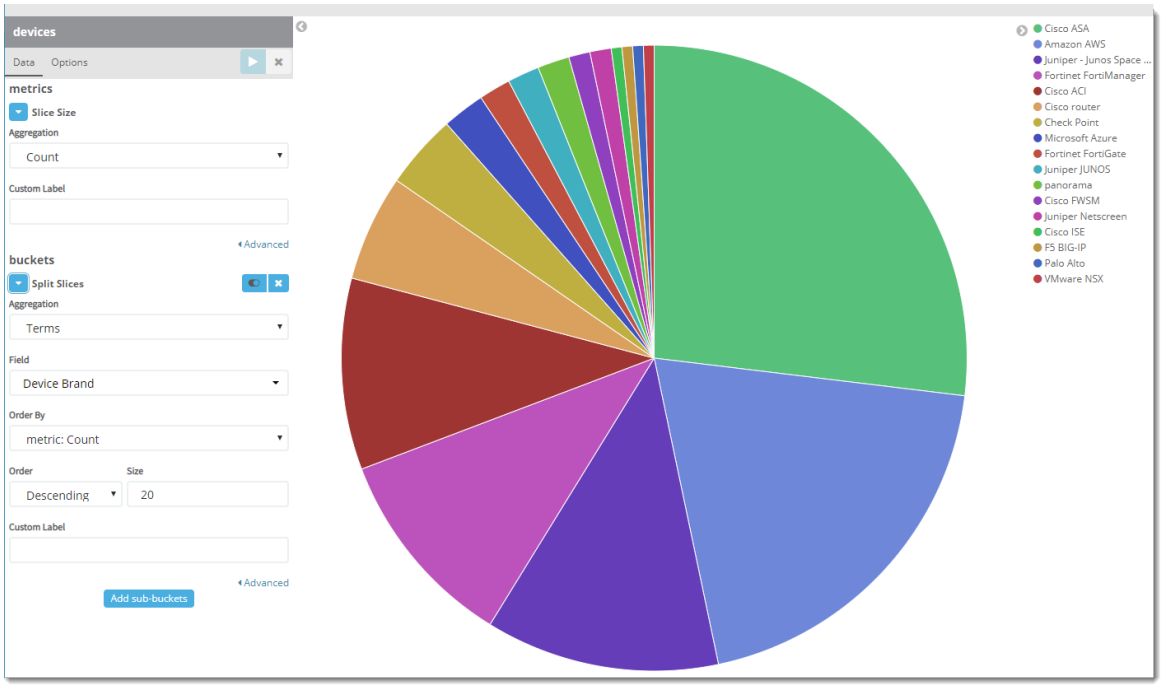
   If you selected to create a new visualization, do the following:

   a. Select a chart type to use.

   b. Select a saved search to use as the data set, or select an index to create a new search. For more details, see Discover data.

3. Once your chart is displayed, define the data metrics and other options for your chart. Click to apply your changes.

   Available options depend on the type of chart you're working with. For example:



4. Above the chart display, define a filter to further filter the data shown.

   Do the following:

   a. Above the chart options, click **Add a Filter** ✚.

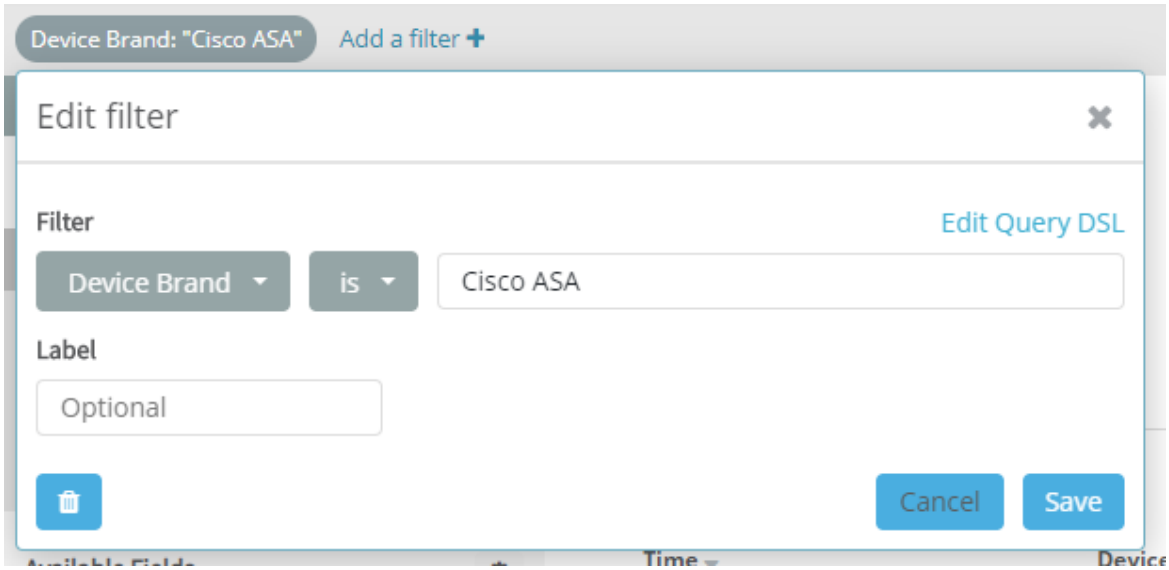
   b. In the **Add filter** dialog, enter a field name, operator, and value.

      > **Note:** When selecting the **is** or **is not** operator, values must match actual values exactly, and are case-sensitive.

   c. Click **Save** to add the selected values to the filter.

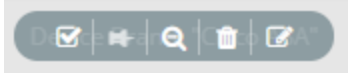
   The field and value is added to the filter list above the data type dropdown and field lists.

   For example:



Filter field options

Once a field is added to the filter, hover over the field in the filter to display further options.



Do any of the following:

/	**Enable** or **disable** the filter field. Use this option to keep the filter values defined, but temporarily disable it for the current data displayed.
/	**Pin** or **unpin** the filter to the top. Use this option when you have several filters displayed, and you want to select specific filters to view at the top of the list.
/	**Invert** a field definition to show all results that do not match the values selected. Inverting a field turns the field definition red to indicate that the results shown are negative results. Click **Toggle** to return to the original field definition.
	Remove the field from the filter entirely. This removes your field values, and you'll need to define them from scratch if you need them again.
	Edit the field values selected. In the **Edit filter** dialog, update the selected filter name, operator, and value, and then click **Save**.

Tip: At the far right, click **Actions** ▼ to display these same actions for all filters defined.

Advanced query editing

ART provides the following advanced filter editing features for experienced Kibana or Elastisearch users.

- In the search bar at the top of the screen, enter a query syntax manually to define the field names and values for your filter.

Click **Show Latest** to automatically add the **Current:true** field and filter out all historical data from the data displayed.

For more details about query syntax, click the **Uses lucene query syntax** link at the right of the search box.

- In the **Edit filter** dialog, click **Edit Query DSL** to manually update or copy in an Elastisearch Query DSL to use for this field value definition.

5. At the top of the page, click any of the following to manage the chart you created:

Save	Save your chart so that you or other users can return to it later on.
Share	Display links to either share a saved chart or a snapshot. Use the **Embedded iframe** URL to embed this chart in another location. **Tip:** Full link URLs may be long. Click **Copy** to copy the full URL to the clipboard, or **Short URL** to display a shorter URL that's easier to share.
Refresh	Refresh the chart currently displayed with updated data from AFA, FireFlow, or AppViz.
Date selector	Define the date range for the data displayed. For details, see Change date ranges.

Continue by creating dashboards that include your charts. For details, see Visualize a specific field, Visualize data, and Create or edit dashboards.

Filter fields by data type

Each data type provides a different set of fields for discovering and visualizing data in ART.

For details, see:

Application filter fields

The following filter fields are available for AppViz application data in the **Discover** and

Visualize areas. For more details, see Discover data and Visualize data

Field	Description
Application ID	The AppViz application ID.
Change requests.Id	A change request ID number.
Change requests.Opened date	The date that a change request was created.
Change requests.Requestor	The requestors of a change request, separated by commas.
Change requests.Status	The status of a change request.
Connectivity status	The connectivity status for an application's flows.
Created	The date an application was created.
Critical process	The name of a critical process.
Current	Determines whether historical data is filtered out. • **True**. Only Current data is shown. • **False**. Current and historical data are shown.
High risks	Defines whether risks are defined as **High**.
Labels	The labels assigned to an application.
Lifecycle phase	Defines the application's lifecycle phase: • **Testing**. The application is undergoing tests before use. • **Staging**. The application is undergoing limited use before it is put into production. • **Production**. The application is currently being used. • **Decommission**. The application is no longer being used.
Name	The name of an application.

Field	Description
Number of blocked flows	The total number of blocked traffic flows.
Number of flows	The total number of traffic flows.
Number of unscanned servers	The number of unscanned servers.
Part of critical process	Defines whether an application is part of a critical process.
Pci application	Defines whether an application assigned to the PCI system label.
Projects.Name	The name of a project that an application is managed by.
Projects.Status	The status of a project.
Relevant devices	The devices associated with an application.
Revision ID	The revision ID of an application.
Revision status	The revision status of an application.
Risk score	The application's risk score.
Vulnerabilities.CVSS	A server severity CVSS score.
Vulnerabilities.Title	A risk item title.
Vulnerability score	A vulnerability score.
_id	An application ID.
_index	An application index.
_score	An application score.
_type	A filter category.

Change Request filter fields

The following filter fields are available for FireFlow change request data in the **Discover** and **Visualize** areas. For more details, see Discover data and Visualize data.

Field	Description
Created	The date a change request was created.
Current	Determines whether historical data is filtered out. • **True**. Only Current data is shown. • **False**. Current and historical data are shown.
DaysOpen	The number of days a change request has been open.
Devices.AFA_ Group	The name of an AlgoSec Firewall Analyzer device group.
Devices.Brand	Device brands.
Devices.Id	Device IDs.
Devices.Name	Device names.
Expiration	A change request expiration date.
Id	A change request ID.
InStatusSince	The date from which a change request has been in its current status.
Owner.Name	The name of a change request's owner.
Owner.Roles	The role of a change request's owner.
PreviousStatus	A change request's prior status.
RequestType	A change request type.
Requestor.Email	The email address of a requestor.
Requestor.Name	The name of a requestor.
ResponsibleRoles	The responsible roles of a requestor.
Status	A current change request status.
Subject	A change request subject.
TemplateName	The name of a change request's template.

Field	Description
WorkFlow	The name of the workflow that controls a change request's lifecycle.
_id	A change request ID.
_index	A change request index.
_score	A change request score.
_type	A filter category.

Device filter fields

The following filter fields are available for AFA device data in the **Discover** and **Visualize** areas. For more details, see Discover data and Visualize data

Field	Description
ASD_ISM Level	An ASD_ISM score level.
ASD_ISM Score	The lowest ASD_ISM compliance score.
BASEL Level	A BASEL score level.
BASEL Score	The lowest BASEL compliance score
Baseline Compliance Level	A Baseline Compliance level.
Baseline Compliance score	The lowest Baseline Compliance score.
Current	Determines whether historical data is filtered out. • **True**. Only Current data is shown. • **False**. Current and historical data are shown.
Device Brand	A brand name.
Device Groups	A device group.
Device IP	A device IP.

Field	Description
Device Id	A device ID.
Device Name	A device name.
GDPR Level	A GDPR score level.
GDPR Score	The lowest GDPR compliance score.
GLBA Level	A GLBA score level.
GLBA Score	The lowest GLBA compliance score.
HIPAA Level	A HIPAA score level.
HIPAA Score	The lowest HIPAA compliance score.
Highest Risk Level	The highest risk score level.
ISO27001 Level	The IS027001 score level.
ISO27001 Score	The lowest IS027001 compliance score.
NERC Level	A NERC score level.
NERC Score	The lowest NERC compliance score.
NIST_800-171 Level	A NIST 800-171 score level.
NIST_800-171 Score	The lowest NIST 800-171 compliance score.
NIST_800-41 Level	A NIST 800-41 score level.
NIST_800-41 Score	The lowest NIST 800-41 compliance score.
NIST_800-53 Level	A NIST 800-53 score level.
NIST_800-53 Score	The lowest NIST 800-53 compliance score.
Number of Baseline Compliance changes	The number of Baseline Compliance changes.
Number of Covered Rules	The number of Covered Rules.
Number of Disabled Rules	The number of Disabled Rules.

Field	Description
Number of Duplicate Objects	The number of Duplicate Objects.
Number of High Risks	The number of High Risks.
Number of Low Risks	The number of Low Risks.
Number of Medium Risks	The number of Medium Risks.
Number of Special Case Rules	The number of Special Case Rules.
Number of Suspected High Risks	The number of Suspected High Risks.
Number of Unused Rules	The number of Unused Rules.
PCI Level	A PCI score level.
PCI Score	The lowest PCI compliance score.
Report Date	A Report Date.
Report Name	A Report Name.
Rule Count	A Rule Count.
SOX Level	A SOX score level.
SOX Score	The lowest SOX compliance score.
Security Rating Score	A Security Rating Score.
TRM Level	A TRM score level.
TRM Score	The lowest TRM compliance score.
_id	A device ID.
_index	A device's index.
_score	A device score.
_type	A filter category.

Create or edit dashboards

ART dashboards consist of graphs, or visualizations created in the **Visualize** area. In addition to the default dashboards that AFA provides out of the box, create or customize your own dashboards to suit your needs.

Do the following:

1. Click **Dashboard** from the main menu on the left. ART displays a list of saved dashboards.

   Search for the dashboard you want to view, or click **Create new dashboard** to create a new one.

2. Do one of the following:

Add new dashboard	If you are creating a new dashboard from scratch, click **Add** to add saved graphs and charts to your dashboard. Click a visualization name to add it to the dashboard draft below. Scroll down to view your dashboard graphs and charts.
Edit saved dashboard	If you are editing a saved dashboard, click **Edit** at the top of the page to modify the graphs and charts on the selected dashboard.

3. Each dashboard widget has the following options shown at the top right:
   - . **Expand** the selected widget to full-screen size.
   - . **Open** the selected chart or graph in the **Visualize** area for editing. For details, see Visualize data.
   - . **Move** the selected widget to a different location in the dashboard.
   - . **Remove** the selected widget from the dashboard.

   To resize a widget, hover over the widget and use the corner icon shown at the bottom right to drag the widget edges to the new size.

   Display advanced dashboard widget details

   Click the arrow at the bottom left of a widget to display the following:

Table	Display the widget data in table form, or export the data. • Below the table, click **Raw** or **Formatted** to export your data. • From the **Page Size** drop down, select an option to determine the number of table rows to display.
Request	Display the Elasticsearch request body.
Response	Display the Elasticsearch response body.
Statistics	Display additional statistics about the Elastisearch request performed for this widget.

4. When you're done customizing your dashboard, click **Save** and enter a name and description for your dashboard.

   Tip: Optionally, select **Store time with dashboard** to update the global date range to the date range currently selected, when you edited the dashboard.

   Click **Cancel** at the top of the page to exit the editing mode and discard your changes.

Note: New custom dashboards created are added to the end of the list of saved dashboards. To find yours, either scroll down the list completely, or enter the dashboard name in the search field.

Dashboard options

Use the following additional options at the top of the page to manage your dashboard:

Share	Display links to either share a saved dahsboard or a snapshot. Use the **Embedded iframe** URL to embed this chart in another location. **Tip:** Full link URLs may be long. Click **Copy** to copy the full URL to the clipboard, or **Short URL** to display a shorter URL that's easier to share.
Clone	Make a copy of the dashboard currently displayed for editing.

Export to PDF	Click to save a PDF with the dashboard data currently displayed.
Mail Schedule	Click to jump in to the AFA Administration area and schedule email updates for the displayed dashboard.
Date selector	Define the date range for the data displayed. For details, see Change date ranges.

Change date ranges

All ART pages provide a date range selector, which enables you modify the date range of the data currently shown.

Do any of the following:

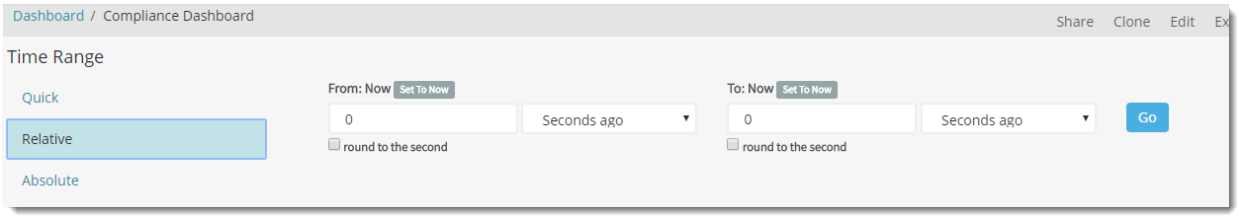
- Use the **< >** arrows to move back and forth between incremental date ranges.
- Click the selected date range, shown in the center of the **< >** arrows, to select a more complex date range.

  The **Time Range** area expands, providing you with a series of options of the following types:

Quick	Provides quick options, like **Today**, **Previous month**, **Last 24 hours**, or **Last 2 years**.
Relative	Enables you to define date ranges from a specified time **ago** or **from now**, to another specified time **ago** or **from now.**
Absolute	Enables you to select specific start and end dates.

Click **Go** to update the data displayed based on your date range selections.

For example:



Manage ART objects

The ART **Management** area enables you to manage saved queries, visualizations, and dashboards.

Warning: The **Management** area also enables you to configure the Kibana **Index** and **Advanced Settings** that control ART functionality.

We recommend keeping the default **Index** and **Advanced Settings** to ensure that ART continues to work as expected. For more details, see the Kibana documentation.

Do the following:

1. From the main menu, click **Management**, and then click **Saved objects**.
2. Click one of the following tabs:
   - **Dashboards**. Manage saved dashboards. For more details, see Create or edit dashboards.
   - **Searches**. Manage saved searches. For more details, see Discover data.
   - **Visualizations**. Manage saved graphs and charts. For more details, see Visualize data.
3. Do any of the following:

Find your object	Browse the list or enter a name in the search field to locate your object.

Edit object settings	Click an object name in the list to make changes, such as to the object title. This option also enables you manage advanced settings, such as supporting JSON code. We recommend making advanced changes like these only if you are an advanced Kibana user.
Open object in ART	Hover over the object name, and click the eye icon to open it **Discover**, **Visualize**, or **Dashboard** areas.
Delete objects	Select one or more objects in the list, and click **Delete** to delete the selected items. In the warning dialog that appears, click **Delete ...** to confirm the deletion.
Export JSON details	Select one or more objects in the list and click **Export** to save the relevant JSON data locally. To export JSON data for all objects, click **Export Everything** at the top of the page.
Import objects	Create ART objects by importing a JSON file. At the top of the page, click **Import** and select a JSON file to import.

Troubleshoot ART

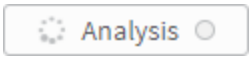
If you run into issues when using the AlgoSec Reporting tool, you may want to check the relevant log files.

ART-related logs are created for the **Elastic**, **Kibana**, and **Logstash** services in the **/var/log** directory on the AFA machine.

Managing Analyses

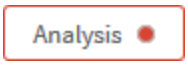
This section describes how to manage analyses (the process of report generation). The information applies equally to manually initiated analyses and scheduled analyses.

Overview

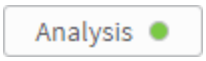
If an analysis is currently in progress, 

appears at the top of the workspace when viewing the device/group/matrix. AFA provides the ability to manage active analyses by doing the following:

- View the progress of a currently running analysis. For details, see Viewing the Progress of an Active Analysis.
- Abort a currently running analysis. For details see Aborting Analyses.

If the last analysis failed, 

appears at the top of the workspace. When an analysis fails, AFA provides failure logs. For details, see Viewing Analysis Failure Logs.

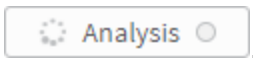
If the last analysis succeeded, 

appears at the top of the workspace. When an analysis succeeds, AFA provides support logs. For details, see Viewing Support Files and AFA reports.

Additionally, you can view a list of all recent analyses. For details, see Viewing the Status of All Recent Analyses.

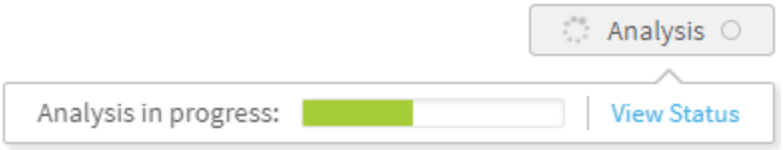
Viewing the Progress of an Active Analysis

To view the progress of an analysis that is progressing successfully:

1. View the desired device. For details, see View AFA device data
2. Click 

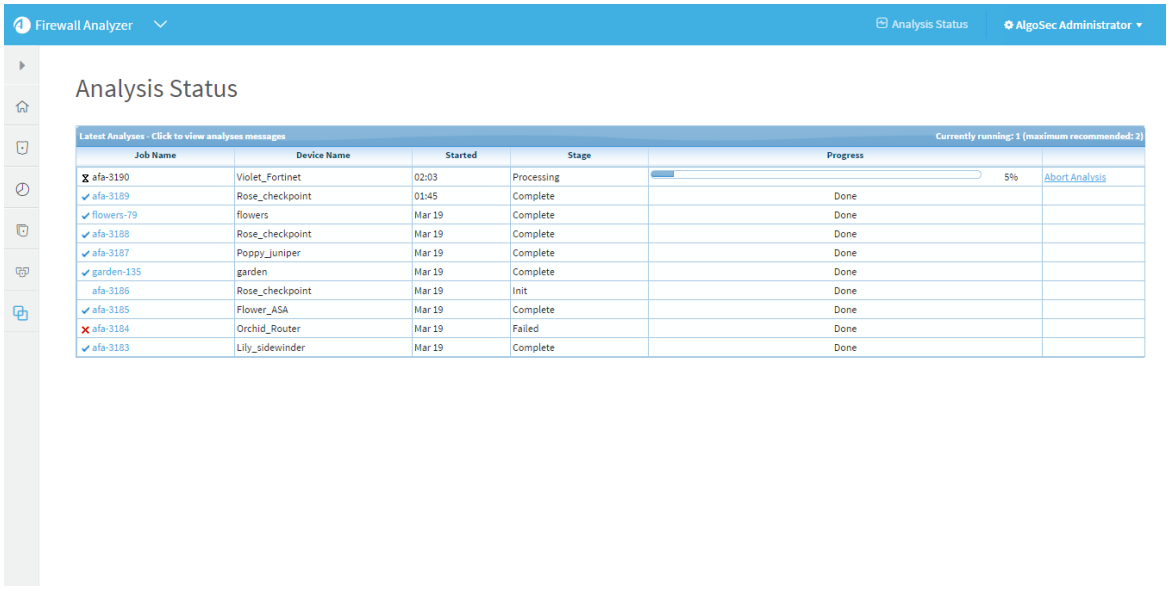
.

   The analysis progress bar appears.



3. To view details of the analysis's status, click the **View Status** link.

   The **Analysis Status** page appears, displaying a list of the most recent analysis jobs.



   For details about the fields in the table, see Analysis Status Fields (see Analysis Status Fields).

   Once the analysis is complete, you can use the generated report. For details, see AFA reports.

Analysis Status Fields

This column...	Displays...
Job Name	The name of the report generated. To view the report, click on the report name.

This column...	Displays...
Device Name	The name of the device on which the analysis ran.
Started	The time or date at which the analysis started. This field is only displayed for analyses that are not currently running.
Slave	The name of the slave appliance running the analysis. This column only appears if a distributed system is configured.
Stage	The status of the analysis. This can be any of the following: • **Collecting data**. Data is being collected from the device(s). • **Processing**. The analysis is currently running. • **Queued (no. X)**. The analysis is queued to run on a slave machine. • **Complete**. The analysis completed successfully. • **Aborted**. The analysis was aborted. • **Failed**. The analysis failed.
Progress	For a currently running analysis, this column displays a progress bar and the percentage of the analysis job that has been completed. For a completed analysis, this column displays **Done** and the name of the report generated. You can click on the report name to view the report.

Aborting Analyses

If desired, you can stop an analysis that is currently running. This task can only be performed by administrators.

To stop a currently running analysis:

1. Open the **Analysis Status** page. For details, see Viewing the Status of All Recent Analyses.

   The **Analysis Status** page appears with a table of recent analyses, including all active analyses.

2. Next to the desired active analysis, click **Abort Analysis**.

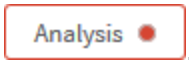
A confirmation message appears.

3. Click **OK**.

   The analysis stops.

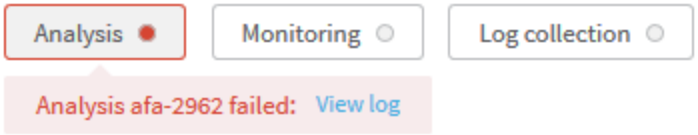
Viewing Analysis Failure Logs

To view logs for an analysis that failed:

1. View the desired device. For details, see View AFA device data.
2. Click 

.

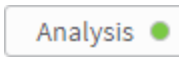
   The analysis progress area appears with a link to report logs.

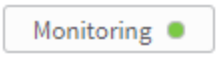


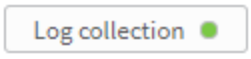
3. Click the **View log** link.

Viewing Support Files

When AFA successfully completes an analysis, monitoring, or log collection, you can view the support files.

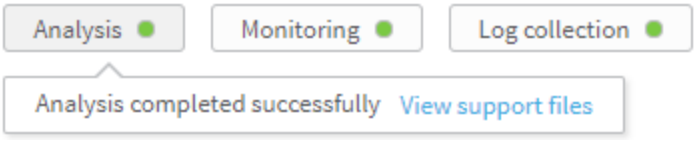
1. View the desired device. For details, see View AFA device data.
2. Click 

, 

, or 

.

   A link to the support files appears.



3. Click the link.

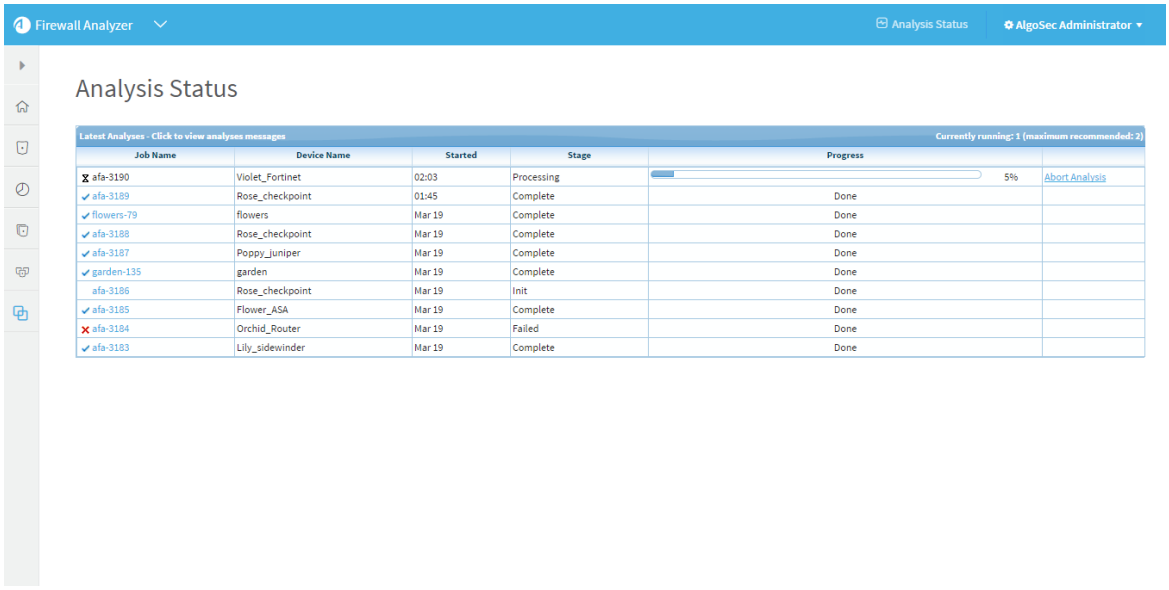
Viewing the Status of All Recent Analyses

You can view details for the 10 most recent analyses, including all currently running analyses.

To view the status of recent analyses:

1. In the toolbar, click Analysis Status.

   The **Analysis Status** page appears.



   For information on the fields, see Analysis Status Fields (see Analysis Status Fields).

Manage real-time monitoring

When real-time monitoring is activated, AFA periodically checks devices for changes. For more details, see Monitored Content.

To view the most recent changes or changes for a specific period of time, see Viewing Real-Time Monitoring Results.

To configure users to receive e-mail notifications when changes are detected, see the *AlgoSec Firewall Analyzer Administration Guide*, **Configuring Event-Triggered Notifications**.

To activate real time monitoring, see the *AlgoSec Firewall Analyzer Administration Guide*, **Configuring Real-Time Monitoring**.

This section explains real-time monitoring results, and how to view the results.

Viewing Real-Time Monitoring Results

You can view the changes detected for individual devices, groups, or matrices. Changes can be viewed in either of the following formats:

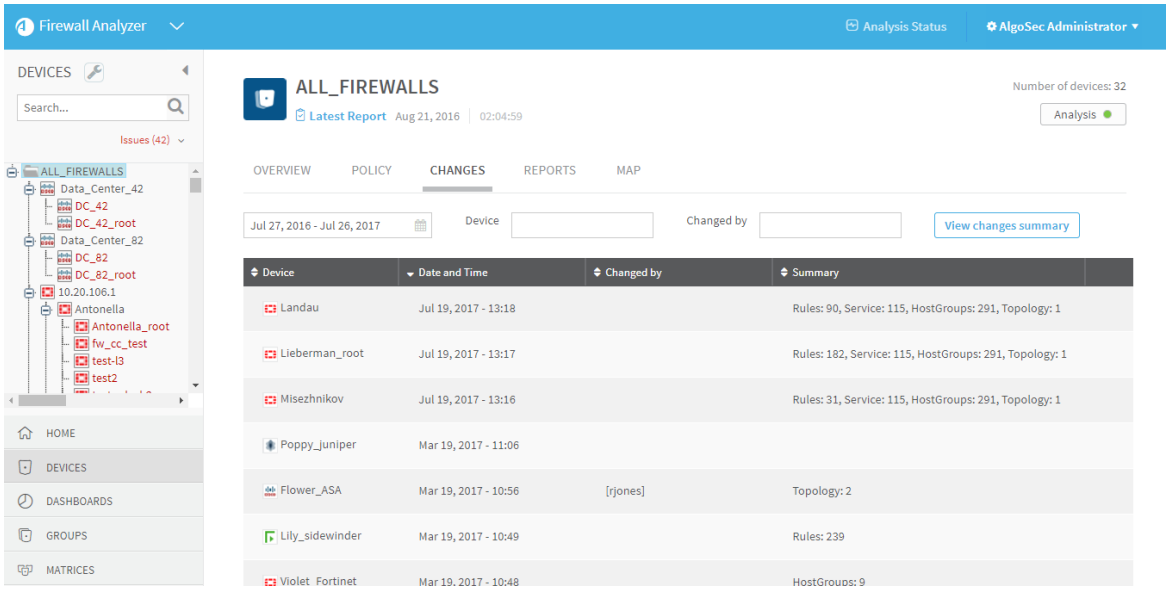
- List of recent changes (from the last 30 days, by default). For details, see Viewing List of Recent Changes.
- Summary of changes over a specific period of time. For details, see Viewing Summaries of Changes for a Specified Period of Time.

Viewing List of Recent Changes

To view a list of recent changes for a device, group or matrix:

1. View the desired device, group, or matrix. For details, see View AFA device data, View AFA group data, and View AFA matrix data.
2. If the **Changes** tab is not selected, click the **Changes** tab.

   The **Changes** tab appears, displaying a list of recent changes for the selected device, group, or matrix.



For information on the list's fields, see the table below.

3. To filter the information displayed in the list, do the following:
    a. To filter by date, click the field displaying the date range, and select a time period in the calendar which appears. You can select a beginning and end date, or you can select one of the relative options, such as **This month**.
    b. To filter by device, in the **Device** field, type the name of the desired device. This field is not relevant for individual devices.
    c. To filter by administrator who performed the change, in the **Changed by** field, type the administrator's user name.
    d. Press Enter.

        The changes are filtered according to the specified parameters.
4. To view a summary of all changes that occurred at a specific instance, do the following:
    a. Hover over a change that occurred at the desired time.

         appears in the row.

b. Click the icon.

The **Changes Summary Report** for the desired instance opens in a new tab.

Changes List Fields

This field…	Displays…
Device	The device on which the change occurred. This field is not relevant for individual devices.
Date and Time	The date and time at which the change occurred.
Changed by	The administrator who performed the change.
Summary	A summary of device items affected by the change.

Viewing Summaries of Changes for a Specified Period of Time

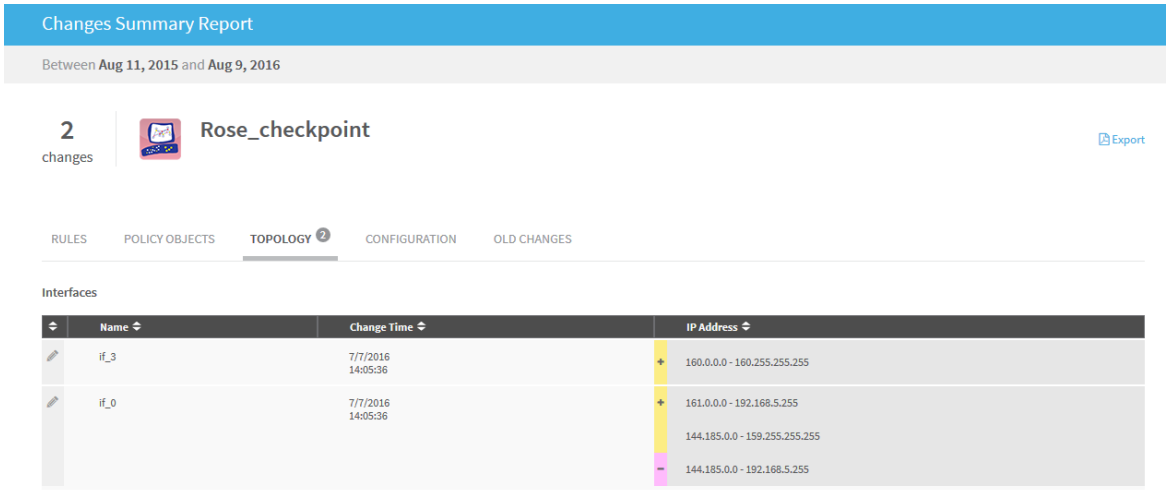
To view a summary of changes for a specified period of time:

1. View the desired device, group, or matrix. For details, see View AFA device data, View AFA group data, and View AFA matrix data.
2. If the **Changes** tab is not selected, click the **Changes** tab.

   The **Changes** tab appears, displaying a list of recent changes for the selected device, group, or matrix.
3. Click the field displaying the date range.

   A calendar appears.
4. Do one of the following:
   - Select a start date, select and an end date, and then click **Apply**.
   - Select one of the relative time frame options, such as **Last 7 Days** or **This month.**
5. Click **View changes summary**.

   The **Changes Summary Report** opens in a new tab.



6. To export the summary to PDF format, click Export. For more details, see Export AFA screens to PDF.

Monitored Content

The change monitoring support for each device brand varies:

- All monitoring devices are monitored for any changes to the full configuration of the device.
- All devices which support full analyses / report generation are monitored for changes to the following:
  - Policy rules
  - Network object definitions
  - Service object definitions
  - Device topology
  - Audit logs
  - Full configuration (not for Check Point)
- For Check Point devices, the following items are additionally monitored:
  - User groups
  - Users

    - VPN communities
    - Global properties
    - NAT rules
    - Application Control Rules
    - Configuration of policy installation
- For cloud devices (such as Amazon Web Services and Microsoft Azure), the following specific items are monitored:
    - For the user account/subscription tier:
        - Aggregated changes in rules/risks/configuration
    - For the Region and VNet/VPC tier:
        - Addition/removal/modification of security sets
        - Aggregated changes in rules/risks/configuration/topology
    - For the security set tier:
        - Additional/removal of instances/ALBs/VMs
        - Changes in rules in security groups/network security groups and network ACLs/subnet network security groups
        - Addition/removal of security groups/network security groups and network ACLs/subnet network security groups

For more information about the different tiers in the device tree for cloud devices, see Device data for cloud devices.

Customize risk detection

You can customize the way that AFA detects risks in the following ways:

- Customize and annotate the network topology.
- Define Trusted Traffic ("white rules") to treat any type of traffic as non-threatening.

Match a Risk Profile to Your Topology: Watch to learn about applying risk profiles to your device topology.

Customizing the Topology

The **Customize Topology** page lets you customize the network topology of a device or matrix that is analyzed by AFA. Customizing the topology allows you to:

- **Mark the DMZs.** You can identify and monitor incoming and outgoing traffic related to the designated DMZs.
- **Choose which interface is external and which interface is internal to your network.** By default, AFA identifies the external interface according to the default route in the routing table. In some cases, for example where the network is connected to a business partner, the default decision is wrong and will cause erroneous reports. Mark multiple external zones and DMZs. Some networks are configured with more than one external zone (i.e., there are two ISPs).
- **Define external zones.** In some cases there is no default route. Using the Customize Topology feature enables you to identify the external zone of the network.

For more details, see:

- Customizing the Device Topology
- Customize matrix topology

Customizing trusted traffic

Defining **Trusted Traffic** allows you to customize AFA to treat any type of traffic as non-threatening. This lets you eliminate any false-alarms triggered by traffic that is necessary for your business.

You can customize trusted traffic from the AFA Web interface or from a device report. For details, see Customize trusted traffic.

Customizing the Device Topology

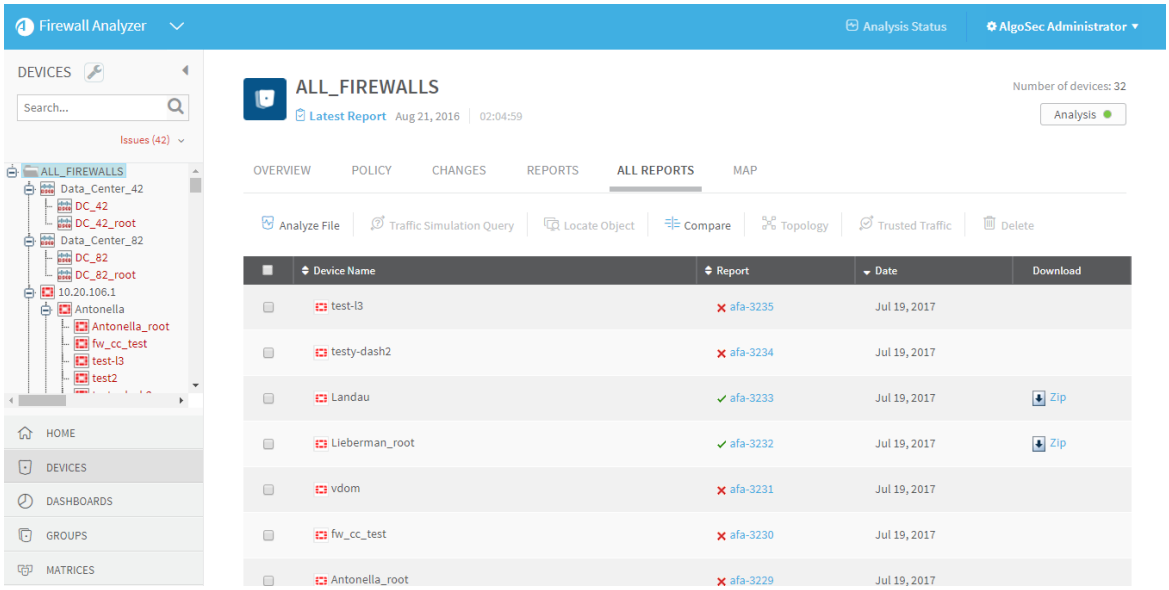
To customize the device topology:

1. Do one of the following:

Customize the device's topology via the device page	View the desired device, either from the **Overview** or **Report** tabs. For details, see View a specific device.
Customize device's topology via the ALL_FIREWALLS page	View the ALL_FIREWALLS group. For details, see View a report for all devices.

2. Click the **All Reports** tab.

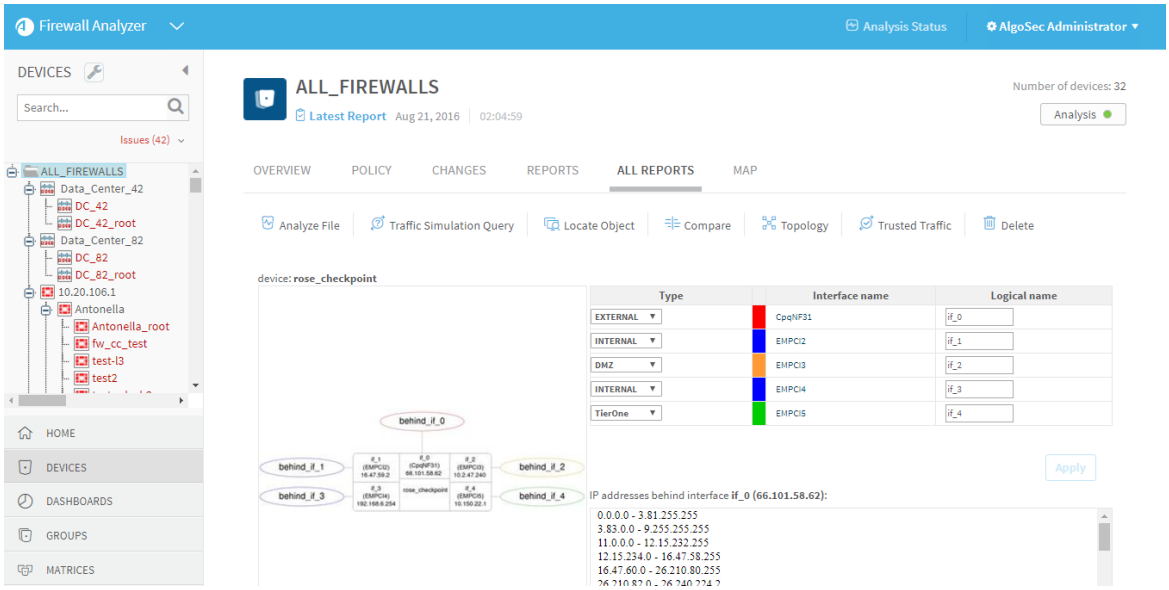
   The **All Reports** page appears.



3. Select the check box next to the desired device.
4. Click **Topology**.

   Note: If you do not have the necessary permissions for customizing topology, this button is disabled.

   The **Topology** page appears.



This page includes a connectivity diagram that shows the network configuration, with color coding designating external (red), internal (blue) or DMZ (orange) zones.

The table on the right lists all of the zones in the device.

5. To change a zone's type, do the following:
    a. Locate the desired zone in the table's **Interface name** column.
    b. In the zone's row, in the **Type** column, select the zone's type.

        This can be any of the built-in types (EXTERNAL, INTERNAL, or DMZ) or a custom zone type.
    c. Click **Apply**.

    The connectivity diagram changes according to your changes.
6. To change a zone's logical name, do the following:
    a. Locate the desired zone in the table's **Interface name** column.
    b. In the zone's row, in the **Logical name** column, type a logical name for the zone.

        In any future reports you generate for this device, the zone will be represented by the logical name entered.
    c. Click **Apply**.

        The connectivity diagram changes according to your changes..
7. To view a list of IP addresses in a specific zone, in the table's **Interface name** column, click on the zone's name.

    The **IP addresses behind interface X** area displays a list of IP addresses in the selected zone.
8. Once you are satisfied with the topology you set, click **OK**.

The new topology will be the default setting of the device and all future reports will be analyzed according to this topology.

A message appears recommending that you run a new analysis for changes to take effect.

9. Click **OK**.

   To run an analysis, see Manually generated reports.

Customize matrix topology

To customize the matrix topology:

1. View the desired matrix. For more details, see View AFA matrix data.

   Note: You can perform this procedure in either the **Overview** or **Reports** tab.

2. Click **Topology**.

   Note: If you do not have the necessary permissions for customizing the topology, this button is disabled.

   The **Topology** page appears.

This page includes a connectivity diagram that shows the matrix's multi-tiered topology, with color coding designating external (red), internal (blue) or DMZ (orange) zones.

The table on the right lists all of the zones in the matrix, their types, and the devices to which they are connected.

3. To change a zone's type, do the following:
    a. Locate the desired zone in the table's **Zone** column.
    b. In the zone's row, in the **Type** column, select the zone's type.

        This can be any of the built-in types (EXTERNAL, INTERNAL, or DMZ) or a custom zone type.

    c. Click **Apply**.

        The connectivity diagram changes according to your changes.
4. To change a zone's name, do the following:
    a. Locate the desired zone in the table's **Zone** column.
    b. In this column, type a new name for the zone.

In any future reports you generate for this matrix, the zone will be represented by the name entered.

c. Click **Apply**.

The connectivity diagram changes according to your changes.

5. To view a list of IP addresses in a specific zone, in the table's **Zone** column, click on the zone's name.

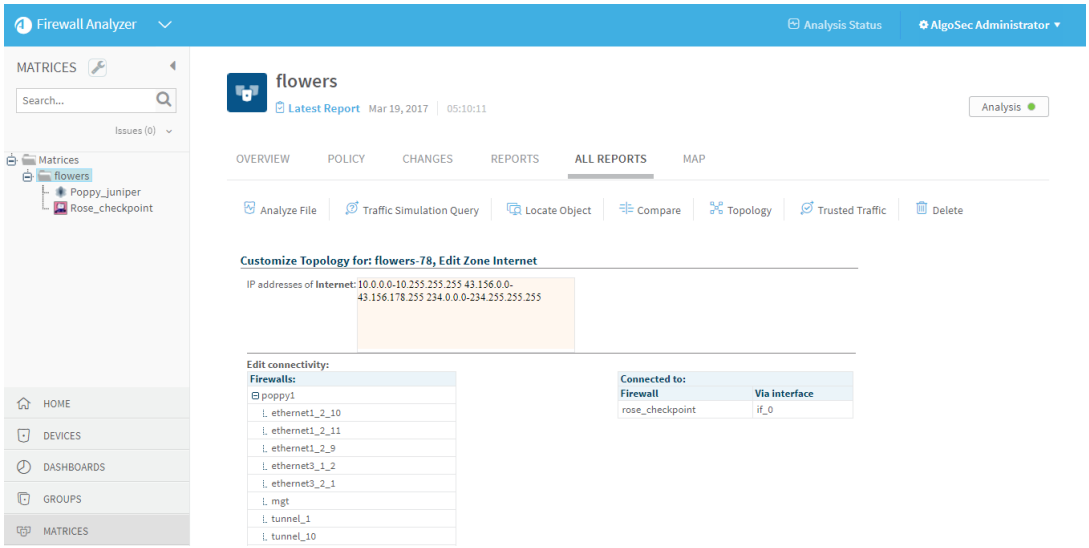
The **IP addresses of X** area displays a list of IP addresses in the selected zone.

6. To edit the list of IP addresses included in a zone, do the following:

a. Locate the desired zone in the table's **Zone** column.

b. In the zone's row, click **Edit**.

The **Edit** dialog box appears.



c. To add an individual IP address, a range of IP addresses, or a host group that is defined on the device, in the **Edit IP Addresses** area, click **Add**.

d. To remove an IP address from the list, select the IP address and click **Remove**.

e. Click **OK**.

f. Click **OK**.

7. To edit a zone's connectivity, do the following:

   a. Locate the desired zone in the table's **Zone** column.

   b. In the zone's row, click .

      The **Edit** dialog box appears.

   c. Specify which devices this zone is connected to, by selecting the devices in the **Firewalls** pane in the **Edit connectivity** area, and clicking **Add**.

   d. To remove a device from the list of devices that the zone is connected to, select the device in the **Connected to** box, and click **Remove**.

   e. Click **OK**.

   f. Click **OK**.

      The connectivity diagram changes according to your changes.

8. Once you are satisfied with the topology you set, click **OK**.

   The new topology will be the default setting of the matrix and all future reports will be analyzed according to this topology.

   A message appears recommending that you run a new analysis for changes to take effect.

9. Click **OK**.

   To run an analysis, see Run a manual AFA analysis.

Customize trusted traffic

Customize trusted traffic from AFA

To customize trusted traffic:

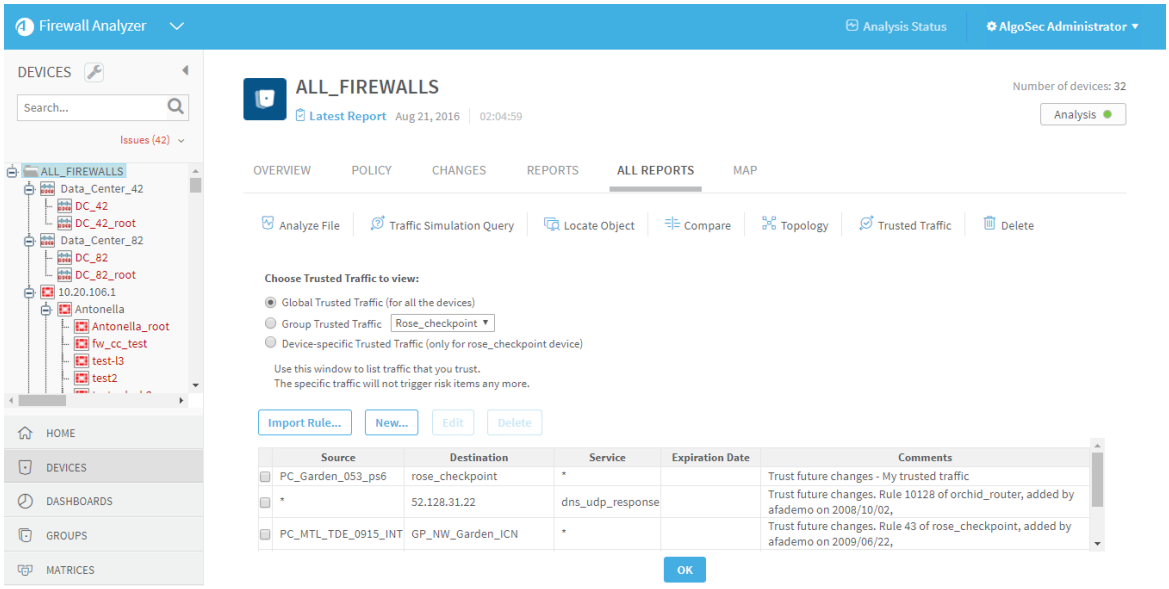
1. Do one of the following:
    - To customize the device's trusted traffic via the device page, view the desired device. For details, see View a specific device.

      Note: You can perform this procedure in either the **Overview** or **Reports** tab.

    - To customize the device's trusted traffic via the ALL_FIREWALLS group page:
        1. View the ALL_FIREWALLS group. For details, see Viewing the ALL_FIREWALLS Group.
        2. Click the **All Reports** tab.

           The **All Reports** tab appears.
        3. Select the check box next to the desired device.
2. Click **Trusted Traffic**.

   The **Trusted Traffic** page appears.



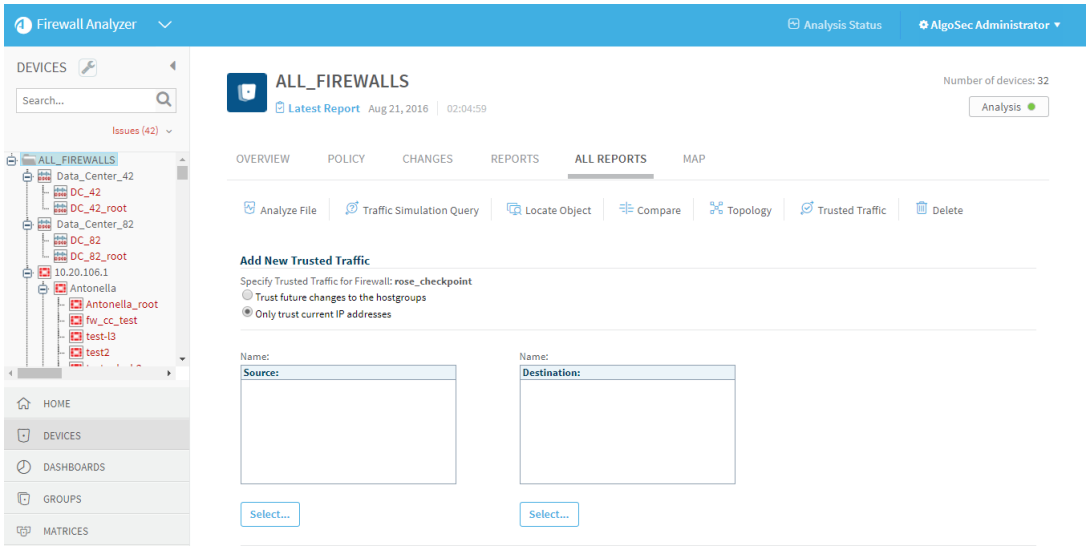
3. Select the type of trusted traffic to view and modify:
   - To work with traffic that is trusted for all devices, click **Global Trusted Traffic**.
   - To work with traffic that is trusted for a specific group, click **Group Trusted Traffic**, then select the desired group from the drop-down list.
   - To work with traffic that is trusted for the current device only, click **Device-specific Trusted Traffic**.

   The desired type of trusted traffic appears in a table at the bottom of the page.

   Note: All changes to trusted traffic will affect the selected type of trusted traffic only.

4. To add or edit trusted traffic:
   a. Do one of the following:
      - To add new traffic, click **New**.
      - To edit existing traffic, select the trusted traffic in the table and click **Edit**.

      The **Add New Trusted Traffic** page appears.



b. In the **Specify Trusted Traffic for Firewall** area, do one of the following:

   - To specify that the host group you selected should remain trusted even if the device administrator changes the IP addresses defined by it, click **Trust future changes to the hostgroups**.
   - To specify that AFA should make a copy of the current definition, and only the IP addresses listed in it should be trusted, click **Only trust the current IP addresses**.

c. Select the source, destination, and service of the traffic that should be trusted.

d. To specify an expiration date for the trusted traffic, select the **Expiration Date** check box and specify the desired date.

e. In the **Comment** field, type any comments.

f. Click **OK**.

   The **Global Trusted Traffic** page re-appears with the new traffic listed.

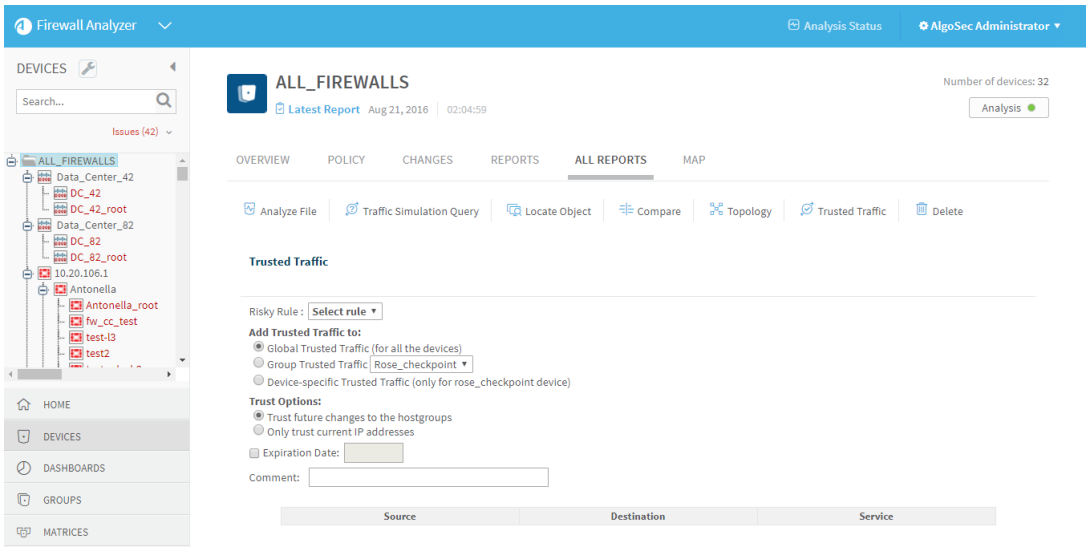
5. To delete trusted traffic, select the desired traffic in the table and click **Delete**.

   The trust for the selected traffic is removed.

6. To import traffic that is specified by a risky rule, do the following:

   a. Click **Import Rule**.

      The **Trusted Traffic** page appears.



   b. In the **Risky Rule** drop-down list, select the desired risky rule.

      The relevant traffic appears in a table at the bottom of the page.

   c. In the **Trust Options** area, do one of the following:

      - To specify that the host group you selected should remain trusted, even if the device administrator changes the IP addresses defined by it, click **Trust future changes to the hostgroup**.
      - To specify that AFA should make a copy of the current definition, and only the IP addresses listed in it should be trusted, click **Only trust the current IP addresses**.

   d. To specify an expiration date for the trusted traffic, select the **Expiration Date** check box and specify the desired date.

   e. In the **Comment** field, type any comments.

f. Click **OK**.

The **Global Trusted Traffic** page reappears with the new traffic listed.

7. Click **OK.**

A message appears recommending that you run a new analysis for changes to take effect.

8. Click **OK**.

To run an analysis, see Manually generated reports.

Customize trusted traffic from a device report

You can customize trusted traffic from a device report's **Risky Rules** page.

Note: Customizing a risky rule from a device report is only available when viewing the report in the AFA Web interface, and **not** when viewing the downloaded report on your computer.

To customize trusted traffic:

1. View a report for the desired device. For details, see View device reports.
2. In the report menu, click the **Risky Rules** tab.
3. In the **Findings** table, click **Trust Rule** next to the desired risky rule.

A new window opens, displaying the **Trusted Traffic** page.

The desired rule is selected in the **Risky Rule** drop-down list, and the relevant traffic appears in a table at the bottom of the page.

4. Do one of the following:

- To specify that the rule traffic should be trusted for all devices, click **Global Trusted Traffic**.
- To specify that the rule traffic should be trusted for a specific group, click **Group Trusted Traffic**, then select the desired group from the drop-down list.

- To specify that the rule traffic should be trusted for the current device only, click **Device-specific Trusted Traffic**.

5. In the **Trust Options** area, do one of the following:
   - To specify that the host group you selected should remain trusted even if the device administrator changes the IP addresses defined by it, click **Trust future changes**.
   - To specify that AFA should make a copy of the current definition, and only the IP addresses listed in it should be trusted, click **Only trust the current IP addresses**.
6. To specify an expiration date for the trusted traffic, select the **Expiration Date** check box. Specify the desired date.
7. In the **Comment** field, type any comments.
8. Click **OK**.

   The **Global Trusted Traffic** page appears.
9. Click **OK**.

   A message appears recommending that you run a new analysis for changes to take effect.
10. Click **OK**.

    To run an analysis, see Manually generated reports.

Send us feedback

Let us know how we can improve your experience with the User Guide.

Email us at: techdocs@algosec.com

Note: For more details not included in this guide, see the online ASMS Tech Docs.