Forescout
eyeSegment Application
How-to Guide

Version 3.9
Contact Information
Forescout Technologies, Inc.
190 West Tasman Drive
San Jose, CA 95134 USA
https://www.Forescout.com/support/
Toll-Free (US): 1.866.377.8771
Tel (Intl): 1.408.213.3191
Support: 1.708.237.6591

About the Documentation
- Refer to the Technical Documentation page on the Forescout website for additional documentation: https://www.Forescout.com/company/technical-documentation/
- Have feedback or questions? Write to us at documentation@forescout.com

Legal Notice
© 2020 Forescout Technologies, Inc. All rights reserved. Forescout Technologies, Inc. is a Delaware corporation. A list of our trademarks and patents can be found at https://www.Forescout.com/company/legal/intellectual-property-patents-trademarks. Other brands, products, or service names may be trademarks or service marks of their respective owners.
# Table of Contents

About the eyeSegment Application .................................................................................. 4

What You Need for the eyeSegment Application ............................................................ 7

Use the eyeSegment Application .................................................................................... 9
  Open the eyeSegment Application .............................................................................. 9
  Configure the eyeSegment Matrix Settings ................................................................ 11
  View the eyeSegment Matrix Page ............................................................................ 13
    eyeSegment Matrix ...................................................................................................... 14
    eyeSegment Menu Button .......................................................................................... 18
    eyeSegment Widgets ................................................................................................. 19
  Find & Filter Specific eyeSegment Traffic ................................................................. 22
  Focus on an eyeSegment Matrix Row, Column, or Cell ............................................ 26
  View eyeSegment Traffic by Service ........................................................................... 30
  Export eyeSegment Traffic Details ............................................................................ 33
  View IP-to-IP eyeSegment Traffic Details .................................................................. 34
  Delete eyeSegment Traffic ....................................................................................... 36
  Ignore eyeSegment Traffic of Specific Devices ......................................................... 37
  Run an eyeSegment Health Check ............................................................................ 38

About the eyeSegment Policy ......................................................................................... 39
  About eyeSegment Policy Rules .................................................................................. 40
  Visualize the eyeSegment Policy in the Matrix ......................................................... 41

Create eyeSegment Policy Rules .................................................................................... 42

Edit or Delete eyeSegment Policy Rules ......................................................................... 43

Configure eyeSegment Policy Rules ............................................................................... 44

eyeSegment Application Considerations and Troubleshooting .................................. 46
About the eyeSegment Application

Welcome to eyeSegment, where you can simplify segmentation planning and automate ACL/VLAN assignment to reduce your attack surface.

Your version of the release might differ slightly from the version described in this guide.

If you are the Forescout administrator, refer to the eyeSegment Module Configuration Guide for information about configuring your Forescout platform to enable viewing and leveraging dynamic zone-to-zone relationship mapping data.

eyeSegment allows you to analyze your physical network traffic from a dynamic zone perspective. This helps you decouple the static constraints of a physical network from the dynamic business logic that modern segmentation policies require.

The eyeSegment product provides:

- Segmentation intelligence driven by the fusion of dynamic zone context and dynamic flow context
- A network traffic baseline using traffic data accumulated over time
- A consolidated visibility pane for mapping and analyzing traffic to and from various sources in and out of the network, and for identifying simulated traffic rule violations and conflicts
- A policy management pane for creating an eyeSegment policy using rules that simulate allowing or denying specific traffic

Use the eyeSegment product to:

- Monitor traffic to understand device dependencies, then map, plan, and deploy network segments.
- Assess devices on the fly to automate segmentation assignment.
- Monitor the network for anomalous communication.
- Focus on a matrix row, column, or cell to view a matrix of all the sub-zones of the selected Source or Destination parent zone. This 'focus' feature allows you to see multiple types and levels of information for hierarchical structures.
- Use dynamic Source and Destination zones to easily create and visualize an eyeSegment policy that simulates denying traffic for a specific segment and filter, and enable notification or other actions when a simulated traffic violation is detected.
- Identify simulated traffic violations to improve your enforcement and eyeSegment policy rules.
- Visualize the policy rules as a layer in the matrix, and ensure that devices do not have conflicting rules.
- Export details about selected traffic for further study.

You can define and manage a single matrix that shows traffic for the eyeSegment zones you select.
How eyeSegment Works

1. The managing Appliances receive and analyze the mirrored traffic data captured by the traffic sensors configured in your environment.

2. The Forescout Cloud Uploader Plugin compresses the traffic data, and then uses encrypted protocol to send it to the cloud where the data is processed and analyzed.

3. The communication patterns among Forescout policy groups and eyeSight segments is dynamically mapped in a web-based matrix of network traffic connectivity.

4. Drill down into the matrix to learn:
   - The ports used by the traffic.
   - The traffic volume between any pair of zones.
   - The IP addresses and other details of the devices that used each traffic pattern.
   - Which traffic violated your eyeSegment policy rules.

5. Use the displayed information to:
   - Redefine your matrix to focus on traffic of interest.
   - Plan your eyeSegment policy for controlling the traffic between specific zones.
   - Refine your eyeSegment policy to ensure that it tags suspicious traffic.
   - Visualize a dashboard for SOC monitoring.

6. If a device sends or receives traffic that violates an eyeSegment policy rule:
   - A Forescout policy can send email and Syslog notifications. (Optional)
   - You can apply a network or endpoint action, such as a Switch Block or Virtual Firewall action. (Optional)

eyeSegment Components

eyeSegment uses the following components:

- eyeSegment zones – Dynamically tagged devices based on detected characteristics, such as function, user role and/or location. Zones are selected from:
  - Forescout eyeSight segments
  - Standard Forescout policy groups that can be populated manually or via a Forescout policy

Single IP addresses can be zones. Segments and groups can be arranged in hierarchical levels where each level of the nested structure below Level 0 is a sub-zone.

In addition to the user-selected zones, the eyeSegment module automatically creates virtual zones to include devices that are not in any of the eyeSight segments or Forescout policy groups selected as matrix zones. Virtual zone names include the symbol «».

eyeSegment zones can include the following:
Forescout policy groups
These groups are selected by the user to be included in the matrix.  
*Note: Each level of a nested structure includes all of its sub-groups.*

eyeSight segments
These segments are selected by the user to be included in the matrix.
*Note: Each level of a nested structure includes all of its sub-segments.*

<table>
<thead>
<tr>
<th>Group</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal Network</td>
<td>Contains all IP addresses included in Forescout's internal network and not in another user-defined Source or Destination zone in the matrix.</td>
</tr>
<tr>
<td>Private Network</td>
<td>Contains all IP addresses that are not in Forescout's internal network but are in the company's private network.</td>
</tr>
<tr>
<td>Multicast/Broadcast</td>
<td>Contains multicast and broadcast address ranges.</td>
</tr>
<tr>
<td>Internet</td>
<td>Contains all IP addresses that are not in any other zone.</td>
</tr>
</tbody>
</table>

Each eyeSegment zone can be designated as a Source zone or a Destination zone or both.

- **Find & Filter criteria (optional)** – A combination of policy groups, Forescout eyeSight segments, IP addresses, services, inspected protocols, and time range. These criteria filter the displayed matrix traffic to specific conditions, such as London Office, High-Risk Assets, Remote Devices, and the past week, so that the matrix shows only traffic of interest. The Find & Filter criteria can be used to create accurate, intersected eyeSegment policy rules, and for finding specific traffic.

Each user can create and maintain their own Find & Filter criteria for the shared matrix.

- **Forescout properties** - The following device properties are updated upon detection of traffic that violates an eyeSegment policy rule:
  - **Traffic Was Denied from This Client**: Lists each eyeSegment policy rule that traffic from the device violated.
  - **Traffic Was Denied to This Server**: Lists each eyeSegment policy rule that traffic from the device violated.
  - **Server Groups to Which Traffic Was Denied**: Lists the lowest-level Forescout policy group or virtual zone (for devices that are not members of any of your Forescout policy groups) in each eyeSegment policy rule, including exceptions, that contains members to which the rule denied traffic from this client.
  - **Client Groups from Which Traffic Was Denied**: Lists the lowest-level Forescout policy group or virtual zone (for devices that are not members of any of your Forescout policy groups) in each eyeSegment policy rule, including exceptions, that contains members from which the rule denied traffic to this server.

The following zones are not written to the Server Groups to Which Traffic Was Denied or Client Groups from Which Traffic Was Denied properties:
- Internal Network
What You Need for the eyeSegment Application

To use the eyeSegment application in your environment, the following items must be configured:

- **eyeSegment License**
- **Supported eyeSegment Browsers**
- **Cloud Connectivity**
- **User Permissions**
- **eyeSight segments (optional)**
- **Groups for the eyeSegment Matrix (optional)**

For other requirements, refer to the *eyeSegment Module Release Notes*.

**eyeSegment License**

Ensure that you have a valid *Forescout eyeSegment* license for the eyeSegment Module.

For information about the license, refer to the *Forescout Administration Guide* or the *Flexx License How-to Guide*.

**Supported eyeSegment Browsers**

The eyeSegment application is accessed through the Forescout Web Client using any of the following browsers:

- Microsoft Edge
- Mozilla Firefox 43.0 and above
- Safari 9.0 and above on MAC OS
- Chrome 46 and above

*Internet Explorer is not supported.*

**Cloud Connectivity**

- Your Forescout Enterprise Manager must be able to access the Internet. Ensure that your Enterprise Manager’s firewall allows incoming connections from *.*forescoutcloud.net.*
For the Forescout Cloud Uploader to report traffic data to the cloud, ensure that your managing Appliances’ firewalls allow outgoing connections to *.forescoutcloud.net. If traffic cannot be reported, the data shown in your matrix will not be up-to-date.

For information about the Cloud Uploader and its configuration, refer to the Cloud Uploader Configuration Guide.

User Permissions

To use eyeSegment features, you must have Forescout permissions configured for you.

If you have View level permissions, you can use the eyeSegment application to:

- View the eyeSegment Matrix Page
- Click eyeSegment Widgets on the Matrix page to see more information
- Toggle the matrix Policy Visualization view
- Toggle the matrix Traffic Violations view
- Manage your own fields to Find & Filter Specific eyeSegment Traffic
- Focus on an eyeSegment Matrix Row, Column, or Cell
- Drill down to View eyeSegment Traffic by Service
- Drill down to view device properties
- Export eyeSegment Traffic Details to a CSV file for further evaluation
- Hover over the left side navigator, and select eyeSegment Policy to view the eyeSegment policy and its rules
- Run an eyeSegment Health Check
- Access this eyeSegment Application How-to Guide online

If you also have Update level permissions, you can do the following activities that affect what all users see in their application:

- Configure the eyeSegment Matrix Settings
- Delete eyeSegment Traffic
- Ignore eyeSegment Traffic of Specific Devices
- Refresh the Traffic Coverage widget information
- Create eyeSegment Policy Rules
- Edit or Delete eyeSegment Policy Rules
- Configure eyeSegment Policy Rules

Groups for the eyeSegment Matrix

If you are the Forescout administrator, ensure that specific groups defined in your Forescout configuration contain the devices whose traffic you want to track. To further narrow the device scope of an eyeSegment policy rule, arrange groups in hierarchal levels. Each level of the nested structure below Level 0 is a sub-group.
Ensure that the policies that manage the groups are run on the devices to be included in the matrix.

To prepare groups for the eyeSegment matrix, refer to the best practice recommendations in the *eyeSegment Module Configuration Guide*.

**Use the eyeSegment Application**

If you have a valid *Forescout eyeSegment* license for the eyeSegment Module, you can *Open the eyeSegment Application* from a web browser, or directly from the Console.

If you have the required *User Permissions*, you can do the following in the application:

- Open the eyeSegment Application
- Configure the eyeSegment Matrix Settings
- View the eyeSegment Matrix Page
- Find & Filter Specific eyeSegment Traffic
- Focus on a Row or Column
- Focus on a Cell
- View eyeSegment Traffic by Service
- Export eyeSegment Traffic Details
- View IP-to-IP eyeSegment Traffic Details
- Delete eyeSegment Traffic
- Ignore eyeSegment Traffic of Specific Devices
- Run an eyeSegment Health Check

**Open the eyeSegment Application**

The application is accessed through the Forescout Web Client.

**To access the eyeSegment application:**

1. Do one of the following:
   - Browse to the following URL to log in from a web browser:
     *https://<Device_IP>/forescout-client*
     where `<Device_IP>` is the IP address of the Enterprise Manager or standalone Appliance.
   - Select the Ellipsis icon  from the Console toolbar, and then select *Segmentation* from the dropdown menu.
2. If your configuration requires you to log in, enter your Forescout credentials. Your network configuration might require:
   - Smart Card authentication with or without two-factor authentication
   - acceptance of corporate terms and conditions

3. Select the Segmentation view.

4. The first time you open the eyeSegment application, the Get Started diagram opens.
Select the **Define Matrix** button to configure the matrix.

## Configure the eyeSegment Matrix Settings

eyeSegment provides an easily configured matrix made of eyeSegment zones. The matrix shows the traffic from each Source zone to each Destination zone. You can add Forescout policy groups and eyeSight segments of interest as Source and Destination zones.

- **To configure the matrix settings, you might need to have additional Forescout permissions configured for you.**

By default, the matrix includes **Virtual Zones** as both Source and Destination zones (unless otherwise noted).

### Virtual Zones

<table>
<thead>
<tr>
<th>Zone</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal Network</td>
<td>Contains all IP addresses included in Forescout's internal network and not in another user-defined Source or Destination zone in the matrix.</td>
</tr>
<tr>
<td>Private Network</td>
<td>Contains all IP addresses that are not in Forescout's internal network but are in the company's private network.</td>
</tr>
<tr>
<td>Multicast/Broadcast</td>
<td>Contains multicast and broadcast address ranges. (Destination zone only)</td>
</tr>
<tr>
<td>Internet</td>
<td>Contains all IP addresses that are not in any other zone.</td>
</tr>
</tbody>
</table>
To configure the matrix settings:

1. If this is not the first time you are opening the eyeSegment application, select **Matrix Settings** from the menu icon on the eyeSegment Matrix page.

2. Configure the following matrix settings:

<table>
<thead>
<tr>
<th>Matrix Title</th>
<th>Enter a meaningful name to be shown in the eyeSegment application.</th>
</tr>
</thead>
<tbody>
<tr>
<td>New Matrix Zones</td>
<td>The matrix shows traffic from selected Source zones to selected Destination zones. Groups and segments already included in the matrix as zones are shown in the <strong>Source and Destination Zone Lists</strong> below.</td>
</tr>
</tbody>
</table>

**To add groups and segments to the matrix:**

1. Expand the dropdown menu to view the list of groups and eyeSight segments in your Forescout configuration. An arrow indicates a nested structure of groups or segments. Select it to expand the structure if you want to select sub-groups or sub-segments.
2. Select one or more groups, sub-groups, segments, and sub-segments to be added as Source zones or Destination zones or both. If your Forescout administrator followed the best practice recommendations in the eyeSegment Module Configuration Guide, only select sub-groups in the 'IP Taxonomy Zones' structure.

*Note: The number of Source zones need not match the number of Destination zones. The matrix can have up to 50 Source zones and 50 Destination zones.*

<table>
<thead>
<tr>
<th>Add As</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add as Source</td>
<td>Select <em>Add as Source</em> if you want the matrix to show traffic originating from any IP address in the groups and segments you just selected.</td>
</tr>
<tr>
<td>Add as Destination</td>
<td>Select <em>Add as Destination</em> if you want the matrix to show traffic that ended at any IP address in the groups and segments you just selected.</td>
</tr>
<tr>
<td>Add as Both</td>
<td>Select <em>Add as Both</em> if you want the matrix to show traffic that originated or ended at any IP address in the groups and segments you just selected.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Source and Destination Zone Lists</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The groups and segments selected as Source and Destination zones are listed in the order in which they appear in the matrix. You can select one or more to remove from the matrix, or select one and use the arrow buttons to change its position in the matrix. Notes:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Deleted Zone</strong> - indicates an eyeSight segment that was deleted from the Forescout platform. It is recommended to remove all deleted zones from your matrix and your policy rules.</td>
</tr>
<tr>
<td></td>
<td>- You cannot remove the <code>&lt; Internal Network</code> or <code>&lt; Private Network</code> zone from the Source or Destination zone lists.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Save/Cancel</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Save/Cancel</td>
<td>Save or cancel your changes.</td>
</tr>
</tbody>
</table>

**View the eyeSegment Matrix Page**

After the initial matrix definition, the matrix is shown whenever you open the eyeSegment application.
The matrix might take a minute or two to appear the first time the data is loaded. After the matrix appears, it is refreshed periodically. To see the latest traffic in the matrix, refresh the browser.

The eyeSegment Matrix page includes the following areas:

- **eyeSegment Matrix**
- **eyeSegment Matrix Visualization Settings**
- **eyeSegment Matrix Legend**
- **eyeSegment Menu Button**
- **eyeSegment Widgets**

To see the widget area, you might need to do one of the following:

- Hover your mouse over the right side of the Matrix page.
- Click the chevron at the right side of the Matrix page.

**eyeSegment Matrix**

The matrix area contains:

- The matrix title.
- The Source and Destination zone names for each cell.

You can select a row, column, or cell to see its lower level sub-groups or sub-segments. See [Focus on an eyeSegment Matrix Row, Column](#) and [Focus on a Cell](#).

- Traffic icons inside cells to indicate that traffic was detected from the Source zone to the Destination zone during the time range shown at the bottom right of the page.
Traffic is only shown if it occurred within the past 90 days.

- A blue icon indicates that the traffic is not filtered, and all detected traffic is indicated in the matrix.
- A violet icon indicates that Find & Filter criteria are applied, and that additional traffic might have been detected but is not shown due to the filter.
- A yellow icon indicates traffic that violated a policy rule whose status is Simulation or Response.

You can select a traffic icon to view details of the detected traffic. See View eyeSegment Traffic by Service.

- If Find & Filter criteria are applied, a filter indicator followed by the filter criteria are displayed as a tag at the bottom of the matrix. If the criteria list is very long, hover over the tag to see all the filter criteria.

**eyeSegment Matrix Visualization Settings**

Use the matrix visualization settings to display additional levels of information in the matrix.

Select to view or change the Date Range, Source, Destination and Service (port/inspected protocol) filter criteria for the traffic shown in the matrix. See Find & Filter Specific eyeSegment Traffic.

Blue indicates that all the traffic is shown, and Find & Filter criteria are not applied.

Violet indicates that the criteria set in the Find & Filter window are applied. See Find & Filter Specific eyeSegment Traffic.

Use the toggle to apply or remove the Find & Filter criteria from the matrix.
If you've created eyeSegment policy rules, use the **Policy Visualization** toggle to apply or remove a color-coded visualization of your policy rules on each cell in the matrix. Hover over a color-coded indicator and select **Policy Rules** to view the name of the eyeSegment policy rule that applies to that traffic.

For more information, see [Visualize the eyeSegment Policy in the Matrix](#).

If you've created eyeSegment policy rules in Simulation or Response status, select **Traffic Violations** to hide all traffic except traffic that violated any of these policy rules. Select ⬤ in the matrix to view details of the traffic. See [View eyeSegment Traffic by Service](#).

**eyeSegment Matrix Legend**

**Traffic**

Traffic Baseline icons show that there was traffic between the Source and Destination zones.

Filtered Traffic icons are only displayed when *Find & Filter* criteria are applied.
Traffic Violation icons are only displayed when the Traffic Violations is selected.

Zones

Overlapping Zones

The Overlapping Zones icon is displayed next to zones that have shared members for which traffic was detected. If a device is a member of more than one zone in the matrix, there is a risk that different eyeSegment policy rules will apply conflicting actions to it. If the device’s traffic violates a policy rule, the traffic violation information displayed in the matrix might be incorrect.

Hover over an icon to view the names of the other zones with which it shares one or more devices.

![Image]

This icon is not displayed in a focused matrix.

To identify the devices shared among different zones:

1. For each Source Zone in the Overlapping Zones popup window:
   a. Find & Filter Specific eyeSegment Traffic for both of the following Source filters:
      › the Source Zone in the matrix row
      › the zone in the Overlapping Zones popup window
   b. For each Filtered Traffic icon, drill down into the matrix to view the IP addresses common to both zones.

2. For each Destination Zone in the Overlapping Zones popup window:
   a. Find & Filter Specific eyeSegment Traffic for both of the following Destination filters:
      › the Destination Zone in the matrix column
      › the zone in the Overlapping Zones popup window
   b. For each Filtered Traffic icon, drill down into the matrix to view the IP addresses common to both zones.

You can use this information to adjust your Forescout group and segment definitions and/or your matrix zone selections.

Forescout Zones

To ensure that the matrix includes traffic to and from all devices, devices that are not in other zones on your matrix are included in Virtual Zones. These zones are not standard Forescout policy groups or segments.
Rule Action and Rule Status

The Rule Action and Rule Status indicators are only displayed in the matrix when Policy Visualization is applied.

The color indicates the rule action (not including exceptions) for all traffic from the matrix cell's Source zone to its Destination zone:

- ☑️ Allow all traffic.
- ☐ Deny all traffic.
- ☉ Allow or Deny traffic, but with exceptions.
- ☐ At least one rule denies this traffic and at least one rule allows this traffic. The results of this conflict are unpredictable.

The type of fill in each Rule Action indicator indicates the rule status:

- ☑️ Draft status: Traffic violations are not displayed in the matrix.
- ☐ Simulate status: Traffic violations are displayed in the matrix.
- ☐ Response status: Traffic violations are displayed in the matrix, and device properties are written whenever the rule is violated. See Trigger Response Actions.

eyeSegment Menu Button

Select the menu icon to select the following options:

- **Matrix Settings** to view or modify the matrix name, its zones, and their order in the matrix. See Configure the eyeSegment Matrix Settings.
- **Find & Filter Traffic** to add Date Range, Source, Destination and Service (port/inspected protocol) filter criteria to the traffic shown in the matrix. See Find & Filter Specific eyeSegment Traffic.
- **Delete Traffic** to permanently delete some or all the traffic data saved to date. The deleted data is cleared from the matrix. See Delete eyeSegment Traffic.
• **Ignore Traffic** to stop saving traffic data for specific IP addresses. See [Ignore eyeSegment Traffic of Specific Devices](#).
• **Health Check** to ensure that eyeSegment can connect to the eyeSegment server. See [Run an eyeSegment Health Check](#).
• **Get Started** to view the Get Started diagram in a different browser tab.
• **Help** to view this How-to Guide in your browser.

### eyeSegment Widgets

Widgets display helpful information about your eyeSegment configuration.

- To see the widgets if the widget area is hidden:
  Depending on the width of your window, either click the chevron at the top right of the Matrix page, or hover your mouse over the right side of the page.
- To hide the widget area:
  Depending on the width of your window, either click the chevron on the left side of the widget area, or move your mouse to the left.

### eyeSegment Policy Rules Widget

The **eyeSegment Policy Rules** widget indicates how many of your policy rules are in Draft status, how many are in Simulation status, and how many are in Response status.

Click anywhere in the widget to open the eyeSegment Policy page that lists all your rules.

### Traffic Coverage Widget

The **Traffic Coverage** widget indicates how many endpoints eyeSegment received traffic data for, and how many endpoints are online in your internal eyeSight network.
Click anywhere in the widget to discover which Forescout eyeSight segments in your internal network contain endpoints that haven't reported traffic data to eyeSegment. Endpoints that are not included in any defined segment are listed in the virtual segment named 'N/A'.

![Traffic Coverage Widget](image)

You can select **Refresh** to retrieve the latest data.

- *It might take a few minutes to load the data.*
- *To refresh the Traffic Coverage data, you might need to have additional Forescout permissions configured for you.*

**Traffic Sensors Widget**

The **Traffic Sensors** widget shows information about the devices that report traffic data to eyeSegment. A sensor is shown if it has uploaded traffic data to eyeSegment within the last 12 hours.

![Traffic Sensors](image)

Depending on the configuration of your environment, your traffic sensors can include:

- **Flow Exporters**: switches, routers, and other network devices that report flow session data. Click the text to view the IP addresses of these network devices.

  - *Note: These are not Appliances.*
- **Packet Engine Appliances**: Forescout Appliances on which the Packet Engine is configured to parse, analyze, and report mirrored traffic data. Click the text to view the IP addresses of these Appliances.

  If the Packet Engine count is lower than expected, verify that the channels were configured correctly on the Appliances missing from the list.

- **SilentDefense Connections**: Forescout Appliances that use the Forescout Operational Technology Module to audit network traffic. Click the text to view the IP addresses of these Appliances.

- **Medigate Servers**: Medigate Collection Servers (MCS) that capture and collect network traffic. Click the text to view the IP addresses of these Medigate servers.

- **AWS Virtual Private Clouds**: Amazon VPCs from which the Forescout AWS Plugin periodically pulls flow logs containing flow session data. Click the text to view information about these VPCs.

---

### Reporting Appliances Widget

Use the **Reporting Appliances** widget to determine the connectivity of your Appliances that are expected to upload data to eyeSegment. An Appliance is included if it has reported traffic data to eyeSegment within the last 36 hours.

A red icon indicates that some of your reporting Appliances are not reporting any traffic data.

Click the text to view the following information for each Forescout Appliance that reports traffic data:

- Current connectivity status to the cloud
- Forescout Appliance name or IP address
- Time stamp of the last successful traffic data upload to the cloud
- Average number of traffic flows that eyeSegment processed per second during the past ten minutes
- Traffic data sources: Packet Engine, Flow Collector, or other traffic sensors

If Packet Engine is not listed as a data source, and you believe it should be, verify that the channels were configured correctly on the Appliance.

**Traffic Collection Duration Widget**

The Traffic Collection Duration widget shows how long the real-time traffic data shown in the matrix has been collected. Traffic that occurred more than 90 days ago is not shown in the matrix.

Traffic collection does not begin until the Forescout Cloud Uploader Plugin is configured correctly and running.

**Find & Filter Specific eyeSegment Traffic**

A filter enables you to intersect one or more filter groups or segment with the Source and Destination zones and their traffic, letting you focus on traffic between specific types of devices without the need for a complex taxonomy structure. When Find & Filter criteria are applied, traffic from each Source zone to each Destination zone is only shown if it meets all the criteria.

You can create and maintain your own Find & Filter criteria for the shared matrix. Among the criteria, you can include any Forescout policy group, segment, or IP as a Source or Destination filter. For example, you can filter the matrix to only display traffic sent from the devices that are in the Source zones defined in the matrix and that are also in all of the following groups and segments:

- London Office
- High-Risk Assets
• Remote Devices

重要的：确保管理您的过滤组的策略在要显示在矩阵中的设备上运行。

**To add or modify your Find & Filter criteria:**

1. Select the **Find & Filter** button (或其他) to open the **Find & Filter** window.

2. Enter one or more filter field parameters. Each **Find & Filter** field — Date Range, Source, Destination, Service — is only applied if at least one value is defined for it.

   - In the **Date Range** field, you can select two dates within the past 90 days to define a range. Select the same date twice for a one-day range.

     *Traffic that occurred more than 90 days ago is never shown in the matrix.*

     The filter matches when the traffic data was received by the Forescout cloud during the date range selected.

     *If the upload was delayed, such as by an internet problem, the date the cloud received the data might be later than when the traffic actually occurred.*

   - In the **Source** and **Destination** fields, you can enter any combination of:
     
     › multiple groups
     
     › one segment
     
     › one IP address

     *After typing an IP address in the search field, be sure to select it below the search field.*

     In the Source and Destination dropdowns, **Groups** and **Segments** are listed in their respective alphabetical order. Sub-groups and sub-segments are listed under their Level 0 in the hierarchy.

     The **Source** filter matches when the traffic was from a device that belongs to all the selected groups and to the selected Forescout eyeSight segment, and that has the provided IP address.
The **Destination** filter matches when the traffic was to a device that belongs to *all* the selected groups *and* to the selected Forescout eyeSight segment, *and* that has the provided IP address.

- In the **Service** field, you can enter any combination of:
  - multiple services
  - multiple inspected protocols

> The available services are based on standard Linux port-to-protocol mapping. When Medigate or SilentDefense reports traffic data, their Deep-Packet Inspection (DPI) techniques provide inspected protocol values that are more accurate than the standard mapping.

The filter matches when the traffic used *any* of the selected services or inspected protocols.

- **If Exclude Traffic** is *not* selected, traffic is only shown if it meets all of the following conditions:
  - The traffic data was uploaded to the cloud during the range in the **Date Range** field. The matrix shows no other traffic.
  - The traffic originated at a device that matches the **Source** filter field. The matrix shows no other traffic.
  - The traffic ended at a device that matches the **Destination** filter field. The matrix shows no other traffic.
  - The traffic used one of the **Service** filter fields. The matrix shows no other traffic.

- **If Exclude Traffic** is *selected*, traffic is only shown if it meets all of the following conditions:
  - The traffic data was uploaded to the cloud during the range in the **Date Range** field. The matrix shows no other traffic.

> Unlike the other filter fields, the **Date Range** field is never excluded.

  - The traffic originated at a device that does not match the **Source** filter field.
  - The traffic ended at a device that does not match the **Destination** filter field.
  - The traffic did not use any of the **Service** filter fields.

> You can use the Clear Filter icon to clear all the filter fields except the date range.

3. Select **Apply** to see how your filter selections affect the displayed traffic without closing the Find & Filter window.

4. Select **OK** to close the Find & Filter window and save the filter.

When **Find & Filter** criteria are applied:

- The traffic icons are violet to indicate that the matrix shows only traffic that matches the filter.
- The **Find & Filter** button is violet.

- A filter indicator followed by the filter criteria are displayed as a violet-colored tag at the bottom of the matrix. If the criteria list is very long, hover over the tag to see all the filter criteria.

- On traffic detail pages, the filter criteria are displayed in a violet-colored box above the table. If the criteria list is very long, hover over the tag to see all the filter criteria.
Focus on an eyeSegment Matrix Row, Column, or Cell

With one click you can focus the matrix on a single row, column, or cell. If the selected Source and/or Destination zone is a nested structure, its next-level sub-groups or sub-segments are expanded in the focused matrix.

- To **Focus on a Row or Column**, select the zone name of a matrix row or column.
- To **Focus on a Cell**, hover over the cell of a Source and Destination zone pair, and select **Focused Matrix**.

You can continue to select a zone name or cell in the focused matrix to further focus on lower-level sub-groups and sub-segments.

A focused matrix does not display **Overlapping Zones** indicators.

Devices in the selected Source or Destination zone that are not members of any of the zone’s lower-level sub-zones are included under the name of the lowest-level group or segment they are in, followed by ‘- Other’. If a selected zone has no lower-level sub-zones, all of its devices are included under the name of the zone.

The breadcrumb next to the matrix name indicates that only a selection of the original matrix is displayed. You can select any part of the breadcrumb to return to an earlier display.

Focus on a Row or Column

In the following illustration, a user focuses on rows and columns in a matrix named *The Best Company’s Matrix.*
1. The user selects the Operations Source zone. This expands the entire Source zone, showing its next-level sub-zones as individual Source zones. All other Source zones are removed from the matrix. The Destination zones are unchanged.
2. Next, the user selects the **OT Risk** Source zone’s sub-zone. That sub-zone is expanded, showing its next-level sub-zones as individual Source zones. All other sub-zones of the Source zone are removed from the matrix. The Destination zones are unchanged.

3. Now the user wants to focus on traffic between those sub-zones and the **Function** Destination zone. The Destination zone is expanded, showing its next-level sub-zones as individual Destination zones. All other Destination zones are removed from the matrix. The Source zones are unchanged.
Focus on a Cell

To generate a focused matrix from a single cell:

1. In the matrix, hover over the cell of the specific Source and Destination zones, and select **Focused Matrix**.

The cell’s Source and Destination zones are expanded, showing their next-level sub-zones as individual Source and Destination zones. No other Source and Destination zones are displayed in this focused matrix.
View eyeSegment Traffic by Service

For each traffic icon, you can view its Source and Destination sub-zones, services used, Source and Destination IP addresses, and the number of occurrences of the traffic within the defined time range. Use this information to help decide which groups and segments to add to the matrix or to a filter.

Select the Find & Filter button to add or change filter criteria.

- You can view up to 1,000 entries. If your traffic of interest is not displayed, add filter criteria to display less traffic that is not of interest and focus on only specific traffic.

To view details of a specific traffic pattern:

1. In the matrix, hover over the matrix cell of the specific Source and Destination zone, and select Traffic Details.
2. If one or both of the selected zones contains sub-zones, the detected traffic is shown as a nested structure. A color indicates the level of each sub-zone for which traffic was detected. If lower-level sub-zones exist but the Source or Destination device is not a member of any of them, the device is listed under the name of the lowest level group or segment it is in, followed by '- Other'.
To see traffic by service for nested structures, select the Occurrences value of the Source and Destination zone traffic.

3. Additional options are available when traffic originates or ends at an IP address included in the Internal Network zone. These internal network IP addresses are not in another user-defined zone in the matrix.

   - Select **Other Zones** to view these IP addresses in their Forescout groups that you have not included as matrix zones. IP addresses that are in your internal network but not in any defined group are listed as **Not in any group**.

   - **eyeSight segments are not displayed.**

4. If neither of the selected zones is a nested structure, the detected traffic is listed by service.

   - The services are grouped into port ranges of 1,000.
   - Select the port range named **All** to see a list of all the services.
   - Up to 1,000 entries are shown for each port range selected.

In the example below, service details are shown for traffic originating from devices in the EWS zone and ending at devices in the PLCs zone. The **Traffic Violations** box indicates that the Traffic Violations option was selected in the matrix, and the traffic shown violated a policy rule whose status is either **Simulation** or **Response**.
The port-to-protocol service mapping is based on standard static Linux mapping. When Medigate or SilentDefense reports traffic data, their Deep-Packet Inspection (DPI) techniques provide inspected protocol values that are more accurate than the standard mapping.

**Export eyeSegment Traffic Details**

You can download a CSV file containing details about the traffic pattern represented in any **Traffic by Service** window. You can export up to 100,000 records at a time.

The downloaded filename includes the Source and Destination zone names of the exported traffic details, and the UTC file creation date and time.

For each traffic pattern, the exported file includes:

- Source Zone, including each sub-zone
- Source IP address
- Destination Zone, including each sub-zone
- Destination IP address
- Port
- Protocol
- Service
- Earliest date and time of this traffic
- Last date and time of this traffic
- Number of connections

The file also includes the following header rows:

- Source Zone of the **Traffic by Service** page that was exported
- An indication if the Source Zone is a group or a segment
- Destination Zone of the **Traffic by Service** page that was exported
- An indication if the Destination Zone is a group or a segment
- An indication if the contents are **Traffic Violations Only** or **Baseline Traffic**
- Details of the Find & Filter criteria, if applied

  - Some Find & Filter criteria are exported in non-standard formats:
    - Dates are exported as UTC times.
    - Protocols are exported as protocolId decimal values. For more information, refer to https://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml.

- File creation date and time, in UTC
- The names of all eyeSegment policy rules associated with the exported traffic
- Name of the user who created the exported file

**To export details of a specific traffic pattern:**

1. View eyeSegment Traffic by Service.
2. On the Traffic by Service page, select Export to CSV. Traffic that does not meet your applied Find & Filter criteria is not exported.
   
   If the Traffic by Service page shows only policy rule violations, only the violating traffic is exported.

   - The traffic details for all ports are exported, regardless of which port range is selected in the table.

### View IP-to-IP eyeSegment Traffic Details

You can view details about the Source and Destination IP addresses in the selected groups and segments that sent or received traffic.

- If more than 1,000 IP addresses in the selected Source or Destination group or segment had traffic, you can view 1,000 addresses:
  - that had the most amount of traffic
  - that had the least amount of traffic

**To view details of IP addresses that sent or received traffic:**

1. View eyeSegment Traffic by Service.
2. On the Traffic by Service page, select the Occurrences value of a service used by the Source and Destination zone traffic.
   - The traffic details are shown for each IP address within the Source and Destination zones that used the selected service.
   - The selected service is shown on a blue background at the top of the table.

   ![SERVICE: 33495 (UDP)](image)

   - If the applied filter includes the service, the service is shown on the filter’s violet background only.

3. You can view the IP-to-IP traffic details by Source zone IP address, or by Destination zone IP address. To toggle between these views, select the **Group By** button.

4. Select a row to view details about the Source and Destination devices.
The details include:

- All the matrix zones the device is currently a member of
- All the matrix zones the device is not currently a member of, but was a member of within the last 90 days, and so its traffic might be included in these zones
- All the eyeSight segments and Forescout policy groups not shown in the matrix that the device is currently a member of
- All the eyeSight segments and Forescout policy groups not shown in the matrix that the device is not currently a member of, but was a member of within the last 90 days
- Function property value
- Vendor and Model property value
- Operating Systems property value
- Other property values if relevant, such as MAC address, open ports, DNS name, user

**Delete eyeSegment Traffic**

You can permanently delete some or all the traffic data used for the matrix. You might want to do this when:

- some of the traffic shown is not accurate because devices were misclassified and assigned to the wrong zone
- a group used in the matrix becomes divided into multiple groups
- a segment used in the matrix becomes divided into multiple segments

*The delete process might take several minutes. A new delete request cannot be initiated until the previous delete process is finished.*

- To use this feature, you might need to have additional Forescout permissions configured for you.
- Traffic collected previously is deleted, but traffic collected after running the command is displayed as regular traffic. It is recommended to complete all group and segment adjustments before you delete the traffic so that all subsequent traffic is aligned with its correct zones.
- Although deleted data is no longer displayed in the eyeSegment application, it is retained in the Forescout cloud for a certain period. For more information, refer to the Data Security Schedule for Customer Network Data in the Forescout Cloud Service at [https://www.forescout.com/company/legal/data-security-schedule/](https://www.forescout.com/company/legal/data-security-schedule/).

**To permanently delete traffic data:**

1. On the eyeSegment Matrix page, select the menu icon , and select **Delete Traffic**.
2. To permanently delete all the accumulated traffic data and clear the matrix, select **Delete all**.
3. To permanently delete only specific traffic data, select **Delete a specific traffic pattern**, and select the traffic pattern to be deleted.

![Delete traffic pattern screen](image)

4. Confirm that you want to delete the traffic data.

The delete process might take several minutes. If an error message indicates that not all of the traffic was deleted, the remaining traffic continues to be shown in the matrix. Try later to delete the remaining traffic that you intended to delete so that the matrix accurately reflects the traffic in the stated time period.

**Ignore eyeSegment Traffic of Specific Devices**

You can stop the collection of traffic data for specific devices. You might want to do this when the traffic between those devices and all other devices is already well managed.

Traffic saved earlier for these devices is not deleted or cleared from the matrix. Consider creating groups or segments of only these devices so that you can use the **Delete eyeSegment Traffic** option to permanently delete from the matrix all traffic data previously collected for the group or segment.

To use this feature, you might need to have additional Forescout permissions configured for you.

**To stop collecting traffic data of specific devices:**

1. On the eyeSegment Matrix page, select the menu icon , and select **Ignore Traffic**.

![Ignore traffic screen](image)

2. Enter an IPv4 address or a range for which both incoming and outgoing traffic must be ignored.
– Enter an IP address in the format **10.20.30.40**.
– Enter a range in the format **10.20.30.40-10.20.30.45**.
– Do not enter a subnet mask.
– Do not include a slash.

3. Press **Enter**. To enter additional IPv4 addresses or ranges, return to step 2.

4. Select **OK**. A warning message informs you that future traffic for those devices will be ignored, but traffic that was already saved will continue to be included in the matrix.

5. Do one of the following:
   – To continue displaying the traffic saved earlier, select **Keep It**.
   – To open the **Delete eyeSegment Traffic** window where you can delete saved traffic, select **Delete It**.

**Run an eyeSegment Health Check**

Run a health check to confirm that traffic data can be uploaded to the eyeSegment server.

**To run a health check:**

1. On the eyeSegment Matrix page, select the menu icon δ, and select **Health Check**.
2. Select the **Run Health Check** button.

   *The health check might run for several seconds.*
3. If the test fails, use the log to determine the problem.

- If your cloud authentication credentials are invalid, provide valid credentials in the Cloud Uploader configuration. Refer to the Cloud Uploader Configuration Guide for more information.

About the eyeSegment Policy

An eyeSegment policy is a set of rules. Each rule applies to traffic from a specific Source zone to a specific Destination zone. The rule and its exceptions determine which traffic is **allowed** and which is **denied**. Use this feature to define different actions for individual sub-zones and services.

By default, all traffic is allowed.

- In this version, rules that deny traffic do not actually block traffic. They can be used to display suspicious traffic in the matrix, and to optionally trigger an action, such as sending a notification, when suspicious traffic is detected.

Policy rules can include any of the following as Source and Destination zones:

- Forescout policy groups and sub-groups.
- The virtual zone named Private Network that includes all the devices not within Forescout's internal network but that are in the company's private network.
The virtual zone named `Multicast/Broadcast` that includes multicast and broadcast address ranges.

The virtual zone named `Internet` that includes all the devices not within the company's private network.

The virtual zone named `- Any -` that includes all devices.

If an existing rule manages the traffic between a Source zone and a Destination zone, another rule cannot be created for the same two zones.

Policy rules cannot include the following as a Source or Destination zone:

- The virtual zone named `Internal Network`
- A hierarchical group name followed by `'- Other'` which includes all members of that zone that are not members of any of its lower-level sub-zones

What You Need to Know about This Version

In this version:

- The status of a rule can be set to **Draft**, **Simulation**, or **Response**.
  - **Draft status**: Traffic violations are not displayed in the matrix.
  - **Simulation status**: Traffic violations are displayed in the matrix.
  - **Response status**: Traffic violations are displayed in the matrix, and device properties are written whenever the rule is violated. See Trigger Response Actions.
- The eyeSegment policy does not actually deny traffic.

About eyeSegment Policy Rules

When the rule action is **Deny**, a simulated traffic violation is triggered when both of the following occur:

- A device in the rule's Source zone sends traffic to a device in the rule's Destination zone.
  
  **and**
  
  - The traffic pattern is not included in a rule exception.

When a rule exception's action is **Deny**, a simulated traffic violation is triggered when both of the following occur:

- A device in the rule's Source zone sends traffic to a device in the rule's Destination zone.
  
  **and**
  
  - The traffic pattern is included in the rule exception.

To set device properties whenever the rule is violated, set the rule status to **Response**. See Trigger Response Actions.

To visualize the violations on the eyeSegment Matrix page, select **Traffic Violations** in the eyeSegment Matrix Visualization Settings.
**Trigger Response Actions**

Device properties can be set whenever a device is the source or destination of an eyeSegment policy rule’s denied traffic.

If the eyeSegment policy rule status is **Response**, and a traffic violation occurs:

- On the device that sent the denied traffic:
  - In the *Traffic Was Denied from This Client* property, the policy adds the name of the rule that denied the traffic.
  - In the *Server Groups to Which Traffic Was Denied* property, the policy adds the name of lowest-level Forescout policy group or virtual zone in the rule, including exceptions, to which the destination IP address belongs.

- On the device that received the denied traffic:
  - In the *Traffic Was Denied to This Server* property, the policy adds the name of the rule that denied the traffic.
  - In the *Client Groups from Which Traffic Was Denied* property, the policy adds the name of lowest-level Forescout policy group or virtual zone in the rule, including exceptions, to which the source IP address belongs.

The following zones are not written to the *Server Groups to Which Traffic Was Denied* or *Client Groups from Which Traffic Was Denied* properties:
- Internal Network
- - Any -
- zones that are eyeSight segments

You can use these properties to write Forescout policies for handling devices that send or receive denied traffic. For more information about using these properties in a policy, refer to the **eyeSegment Module Configuration Guide**.

**Visualize the eyeSegment Policy in the Matrix**

You can visualize your eyeSegment policy rules in the matrix. This helps you ensure that each network connection of interest is managed by a rule.

- To help you visualize the implications of your eyeSegment policy, Forescout recommends that your matrix include all the zones used in your policy rules.

- The matrix does not display violations of policy rules in Draft status.

All traffic is evaluated by your eyeSegment policy.

- Traffic denied by an eyeSegment policy rule in Simulation or Response status is shown in the matrix as a *Traffic Violation*.

- A conflict occurs when a zone is included in two different rules. This can happen when - **Any** - is selected as a zone in one of the rules. Hover over the *Conflict* icon to identify which rules are in conflict.
Create eyeSegment Policy Rules

There are two ways to create eyeSegment policy rules:

- Manually Create Policy Rules
- Automatically Create Policy Rules

⚠️ To manage the eyeSegment policy, you might need to have additional Forescout permissions configured for you.

Manually Create Policy Rules

To manually create an eyeSegment policy rule:

1. Hover over the side navigator, and select eyeSegment Policy.

2. Select Add Rule.

3. To configure the rule and its exceptions, see Configure eyeSegment Policy Rules.

4. To return to the matrix, hover over the side navigator, and select eyeSegment Matrix.

Automatically Create Policy Rules

You can automatically create an eyeSegment policy rule in Draft status from a Traffic or Traffic by Service page. The rule allows or denies all traffic from the Source zone to the Destination zone except for the traffic patterns you select. If a rule already exists for that traffic, the rule is updated with the selected exceptions.

- On a Traffic by Service page, the rule adds as exceptions all the traffic that uses any of the selected services.
• On a Traffic page, the rule adds as exceptions all selected traffic patterns using any service.
• If Find & Filter criteria are applied, they are automatically included in the rule exceptions.

  The date range filter is not included in rule exceptions.

No changes are made to your eyeSegment policy until you select Save.

To create an eyeSegment policy rule with just a few clicks:
1. View eyeSegment Traffic by Service of the traffic pattern to be included in the rule.
2. Select the checkbox of each service or traffic pattern for which traffic is to be an exception to your rule.

  You can select up to 50 services or traffic patterns as exceptions each time.

3. From the Add to Policy dropdown menu, select one of the following:
   – Deny All Except Selected: The rule denies all traffic from the Source zone to the Destination zone except for the traffic patterns you select.
   – Allow All Except Selected: The rule allows all traffic from the Source zone to the Destination zone except for the traffic patterns you select.

  If a rule for these zones already exists, the selected patterns are added to its list of exceptions.

4. Select Show Me the Rule.
   – If this traffic did not have a rule, a new rule having a default name is displayed. The rule is in Draft status unless you select a different status.
   – If a rule already exists for this traffic, the existing rule is displayed.

The service or traffic patterns you selected are displayed as exceptions to the rule.

5. To edit the rule and its exceptions, see Configure eyeSegment Policy Rules.

Edit or Delete eyeSegment Policy Rules

You can edit one eyeSegment policy rule at a time. You can delete multiple rules at a time.

If you edit or delete a rule in Simulation or Response status, all its previously detected simulated traffic violations are cleared from the matrix.

If you cannot delete a rule, see eyeSegment Policy Rules Cannot Be Deleted in the eyeSegment Application Considerations and Troubleshooting section.
To edit or delete an eyeSegment policy rule:

1. Hover over the side navigator, and select **eyeSegment Policy**.

2. To delete one or more rules, select the rules’ checkboxes, and select **Delete**.

3. To edit a rule and its exceptions, select the rule’s checkbox, and select **Edit Rule**. See **Configure eyeSegment Policy Rules**.

4. To return to the Matrix page, hover over the side navigator, and select **eyeSegment Matrix**.

### Configure eyeSegment Policy Rules

You can change eyeSegment policy rule fields at any time.

*If you save changes to a rule in Simulation or Response status, all its previously detected simulated traffic violations are cleared from the matrix.*
To configure an eyeSegment policy rule:

1. Name the rule.
   - Rule names are displayed on the eyeSegment Policy page.
   - When a rule in Response status denies traffic, the rule name is written to a device property on both the client and the server.

2. In the Status field, do one of the following:
   - If you are not yet interested in seeing simulated traffic violations of this rule, select Draft.
   - To see the rule's violations simulated in the matrix, select Simulation.
   - To see the rule's violations simulated in the matrix and to also set device properties whenever the device is the source or destination of traffic denied by this rule, select Response. See Trigger Response Actions.

3. Select a Source Zone and a Destination Zone. The rule will manage all traffic that originates at an IP address in the selected Source zone and ends at an IP address in the selected Destination zone.

   Notes:
   - A selected zone includes also all IP addresses in its sub-zones.
   - The zone named - Any - includes all IP addresses.
   - If either of the rule zones is not included in your matrix, a pop-up message asks if you’d like to add it to the matrix. Adding the zone enables you to visualize the rule and its violations in the matrix.

4. Do one of the following:
   - To deny all traffic between these zones, with possible exceptions of specific traffic patterns, select Deny all services in the Action field.
   - To allow all traffic between these zones, with possible exceptions of specific traffic patterns, select Allow all services in the Action field.

   To add exceptions for specific traffic patterns, see Add Rule Exceptions.
When Policy Visualization is selected in the eyeSegment Matrix Visualization Settings, you can see an indication that the traffic between these zones is defined as Deny or Allow.

5. To delete an exception, select it, and select Delete.

**Add Rule Exceptions**

You can add exceptions to eyeSegment policy rules. Exceptions that meet all the following conditions override the rule:

- The traffic originates at an IP address that is in the exception's Source Zone and also in all of the exception's Source Filter zones.
- The traffic ends at an IP address that is in the exception's Destination Zone and also in all of the exception's Destination Filter zones.
- The traffic uses one of the exception's Services.

**To add an exception:**

1. On the Add Rule or Edit Rule page, select + Add Exception.

2. In the exception's Source Zone and Destination Zone fields, select the same zones as, or sub-zones of, the zones in the rule.

   - A selected zone includes also all IP addresses in its sub-zones.

3. Optionally select any combination of other groups and a segment as Source or Destination filters.

4. In the exception's Service field, select All for the exception to apply to traffic on all services, or enter a list of specific services on which the exception applies.

5. Select OK for the exception to be added to the Exceptions table.

**eyeSegment Application Considerations and Troubleshooting**

Consider the following when using eyeSegment:

- Forescout Web Client User Security
- Very Little Traffic Data in the Matrix
- Very Little Traffic Data for a Zone
- eyeSegment Policy Rules Cannot Be Deleted
- Groups Cannot Be Deleted from the Forescout Platform
- Segments Are Deleted from the Forescout Platform

Other issues are described in the eyeSegment Module Release Notes.
**Forescout Web Client User Security**

You can hover the mouse over your user name to see the following session information for your account:

- Your user name
- The time and IP address of your previous successful login
- The number of your recent, consecutive login attempts that failed

If you suspect this information is incorrect, report it to your security officer.

**Very Little Traffic Data in the Matrix**

When the eyeSegment Module is started, Appliances begin to report their detected traffic for each Forescout policy group and eyeSight segment defined in the Forescout platform.

Data is not available for any traffic detected:

- before the module was started
- before all traffic data was deleted

As time passes, more traffic data will be reported and shown.

If you suspect that traffic is not being reported, Run an eyeSegment Health Check.

**Very Little Traffic Data for a Zone**

The traffic data of network devices that are not part of any Forescout policy group or eyeSight segment is saved in the **Internal Network** zone.

- The eyeSegment module begins to save reported traffic data for a specific group or segment after the group or segment is created. Earlier traffic is not associated with that group or segment.
- The eyeSegment module begins to save reported traffic data for a specific device to its group or segment after the device has been added to the group or segment. Earlier traffic for that device is not associated with that group or segment.

**eyeSegment Policy Rules Cannot Be Deleted**

When a Forescout policy is created from the eyeSegment Policy Compliance policy template in the Forescout platform, the names of your eyeSegment policy rules might be selected in the **Traffic Was Denied from This Client** and **Traffic Was Denied to This Server** conditions. You cannot delete a rule from your eyeSegment policy if its rule name is selected in a policy condition.
Groups Cannot Be Deleted from the Forescout Platform

The Forescout platform’s Groups Manager does not allow a group to be deleted if it is used in the eyeSegment matrix or in an eyeSegment policy rule. You must first remove the group from the matrix in the eyeSegment Matrix Settings window and from all rules.

Segments Are Deleted from the Forescout Platform

Unlike groups, eyeSight segments can be deleted from the Forescout platform even if they are used in the eyeSegment matrix or in an eyeSegment policy rule. After a segment is deleted from the Forescout platform:

- The name of the segment includes the prefix **Deleted Zone**.
- Segment name changes made after the segment was added to eyeSegment are ignored.
- The matrix continues to show the traffic reported for the segment before it was deleted.
- Subsequent traffic is no longer associated with that segment.
- The segment is removed from all filter fields.
- The zone name prefix **Deleted Zone** is displayed in policy rules that used that segment, but the zone is ignored.

It is recommended to edit the matrix and your policy rules to remove these deleted segments.