FORESCOUT

Forescout

eyeSegment Web Portal

How-to Guide

Version 2.0

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

Legal Notice

2019-11-06 17:21

Table of Contents

Welcome

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

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

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. To access the guide from your Forescout Console after the plugin is installed, select **Tools** > **Options** > **Modules**, select **eyeSegment**, and then select **Help**.

About eyeSegment

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.
- 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 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.

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

The eyeSegment product does not support:

- *Certification Compliance mode*
- *Devices that do not have IPv4 addresses*

How It Works

1. The managing Appliances receive and analyze the mirrored traffic data captured by the Forescout Packet Engine and the Forescout Flow Collector.
2. The Forescout Cloud Uploader 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 between dynamic policy groups and zones 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.
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 a simulated 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 based on standard Forescout policy groups that can be populated manually or via a policy. Single IP addresses and Forescout segment objects can be groups. Groups can be arranged in hierarchal levels where each level of the nested structure below Level 0 is a sub-group.

  The eyeSegment module automatically creates virtual zones to includes devices that are not in any of the Forescout policy groups selected as matrix zones. Virtual zone names begin with <).

  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.*
Internal Network	Contains all IP addresses included in Forescout's internal network and not in another user-defined Source or Destination zone in the matrix.
Private Network	Contains all IP addresses that are not in Forescout's internal network but are in the company's private network.
Multicast/Broadcast	Contains multicast and broadcast address ranges.
Internet	Contains all IP addresses that are not in any other zone.

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

- Filters (optional) – Groups or services used to filter the displayed matrix traffic to specific conditions, such as *London Office*, *High-Risk Assets*, and *Remote Devices*, so that the matrix shows only traffic of interest. Filters can be used to create accurate, intersected eyeSegment policy rules.
- Forescout properties - The following device properties are updated upon detection of traffic that violates a simulated eyeSegment policy rule:
  - *Traffic Was Denied from This Client*: Lists all simulated eyeSegment policy rules that denied traffic from the device.
  - *Traffic Was Denied to This Server*: Lists all simulated eyeSegment policy rules that denied traffic to the device.
- eyeSegment Policy Compliance policy template – A template accessible from the Console for creating policies that send notifications when a device's client or server traffic violates an eyeSegment policy rule.

What You Need

Verify that your browser, cloud, and Forescout group requirements are ready.

Supported eyeSegment Browsers

eyeSegment can be accessed 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 the matrix will not be up-to-date.

  For information about the Cloud Uploader and its configuration, contact your Forescout sales representative.

Prepare Groups for the eyeSegment Matrix

Ensure that specific groups defined in your Forescout Console 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.

- Best Practices for Creating eyeSegment Zones
- Best Practices for Creating eyeSegment Filters

Best Practices for Creating eyeSegment Zones

To create groups to be used as eyeSegment zones:

1. To easily identify your potential eyeSegment zones, define a parent group named 'IP Taxonomy Zones'.
2. Create lower level sub-groups under this parent group for all the device types in your environment. The more levels you create, the more you will be able to pinpoint specific traffic patterns in eyeSegment. ***Define the sub-groups so that each device in your network is added to one, and only one, of these sub-groups.***
3. Use policies to assign all the devices in your network to their respective sub-groups in this structure.
4. In the eyeSegment web portal, select your eyeSegment zones from these sub-groups.

Each level of the nested structure includes all of its sub-groups.

The following are sample group levels in an 'IP Taxonomy Zones' structure:

IP Taxonomy Zones

- **A. Servers/Services/Applications**
  - 1. User/Client Enterprise Management (Distributed)
    - a. AD
    - b. Inventory
    - c. Vulnerability Assessment
    - d. Patch Management
    - e. Software Deployment
    - f. MDM
  - 2. Enterprise Services
    - a. Email
    - b. Intranet
    - c. Time Clock
    - d. Instant Messaging
    - e. HR
    - f. Finances
    - g. Legal
    - h. Document Sharing
    - i. Help Desk
    - j. GRC
  - 3. Infrastructure
    - a. Network Devices
    - b. Telecom
    - c. Physical Security Servers
      - (i) Digital Video Records
      - (ii) Badge System Database
    - d. Security Systems
      - (i) Proxy
      - (ii) SIEM
      - (iii) WAF
      - (iv) DLP
      - (v) EPP
      - (vi) EDR
      - (vii) ATD
    - e. Network Packet Brokers
    - f. Virtual
    - g. Out-of-Band Server Management
    - h. SAN/Storage
    - i. Print Servers
    - j. DNS/DHCP
    - k. Load Balancers
    - l. Network and System Monitoring
  - 4. Company Production
    - a. Company & Resource Planning
      - (i) CAD
      - (ii) Enterprise Resource Planning
      - (iii) Manufacturing Execution Systems
    - b. Company Software Development
      - (i) Source Repos, Build Systems, Bug Systems
    - c. Research and Development
      - (i) Corporate & Academic
    - d. Operations
      - (i) Licensing
      - (ii) Warehousing
      - (iii) Customer Success
  - 5. Customer Production
    - a. Customer Payment Card Data
    - b. Customer Health Records
    - c. Customer Education Records
    - d. Customer Financial Records
      - (i) Internal Customer Service
      - (ii) External Customer Website
      - (iii) Money Movement
        - i. Installed Applications *contains* OpenSpan
    - e. Customer Telemetry Records
    - f. Customer Usage and Billing
- **B. Users**
  - 1. By Department/Role from AD
    - a. User Directory
- **C. Clients**
  - 1. Workstation Without a User
  - 2. Enterprise IoT
    - a. Printers
    - b. Telecon
    - c. Videocon
    - d. Smart Meeting room
      - (i) Exterior Room Schedule
      - (ii) Smart White Board
      - (iii) Smart Projector
      - (iv) Room Control
      - (v) Zoom Room, Webex Room
    - e. Digital Signage
    - f. Guest Kiosks
    - g. Mobile Devices
      - (i) Customer demo
      - (ii) Productivity
  - 3. Building IoT(OT)
    - a. Physical Security
      - (i) Cameras
      - (ii) Door Access Control
    - b. Physical Safety
      - (i) Fire Detection, Alarm, Suppression
      - (ii) Severe Weather Alarm
      - (iii) Shooter Detection
      - (iv) Public Safety Integration
    - c. Environmental Controls
      - (i) Lighting
      - (ii) Elevators, Escalators
      - (iii) Climate
    - d. Energy Controls
      - (i) Battery Storage
      - (ii) UPS
      - (iii) Generators
  - 4. Company Production IoT
    - a. Financial Services
      - (i) Cash Machines
      - (ii) ATMs
    - b. Retail
      - (i) Point of Sale
      - (ii) Smart Shopper
    - c. Entertainment
      - (i) Gaming, Gambling
      - (ii) Bowling, Arcade, Golf
    - d. Travel
      - (i) Check-In Systems
      - (ii) Information Systems
      - (iii) Mobile Safety & Customer Service Devices
    - e. Medical Equipment
      - (i) Medical Imaging
      - (ii) Clinical Engineering
    - f. Smart City
      - (i) Parking
      - (ii) Lighting
      - (iii) Mass Transit Ticketing
- **D. OT (ICS Systems)**
  - 1. Energy Generation and Distribution
  - 2. Oil & Gas Production
  - 3. Manufacturing
  - 4. Travel

Best Practices for Creating eyeSegment Filters

Set up your Forescout environment so that the devices in your network belong also to groups that are not part of the 'IP Taxonomy Zones' structure. Define these additional group structures based on attributes, such as:

- product lifecycle
- connectivity
- network access layer
- location
- vendor
- compliance

- risk

Each device in your network can belong to multiple sub-groups in these structures. Use these additional groups as filters in the eyeSegment web portal.

The intersection of one or more filter groups with the Source and Destination zones enables you to focus on specific types of devices without the need for a complex taxonomy structure.

Use the eyeSegment Web Portal

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

You can do the following in the eyeSegment web portal:

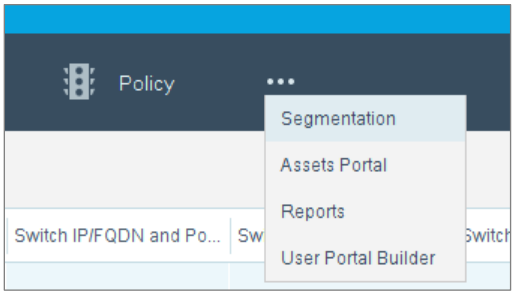
- Open the Web Portal
- Configure the Matrix
- View the Matrix Page
- Filter the Traffic
- View Traffic Details
- View IP-to-IP Traffic Details
- Use an eyeSegment Policy

You can also Delete Traffic Data.

Open the Web Portal

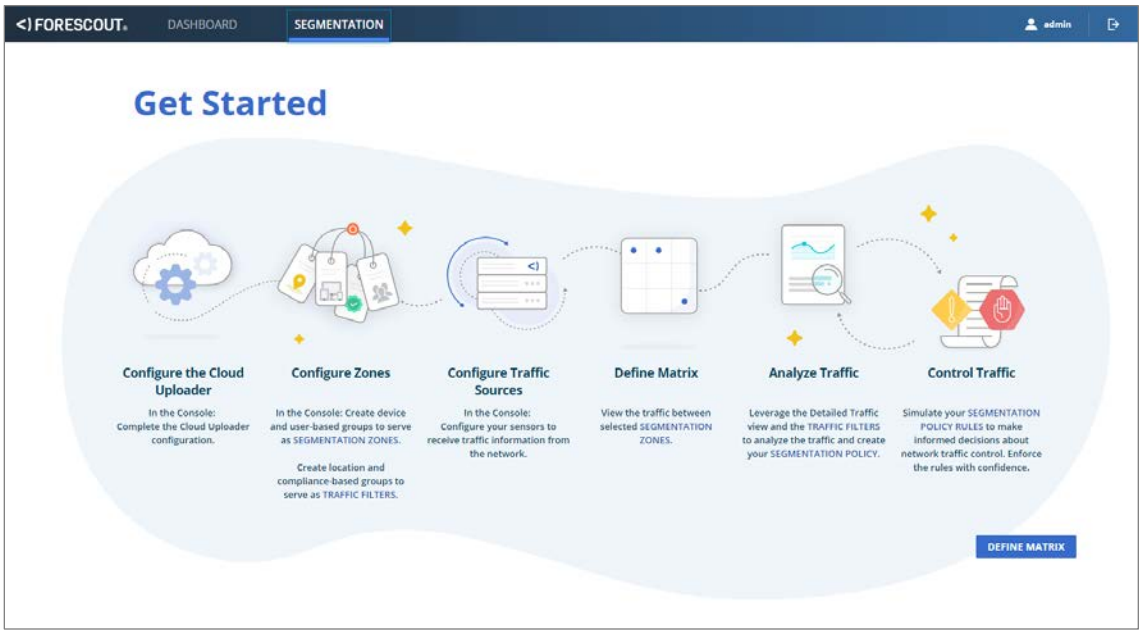
To access the eyeSegment web portal:

1. Do one of the following:
   - Browse to the following URL to log in from a web browser:
     https://<Device_IP>/seg
     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 web portal, the **Get Started** diagram opens.



Select the **Define Matrix** button to configure the matrix.

Configure the Matrix

eyeSegment provides an easily configured matrix made of eyeSegment zones.

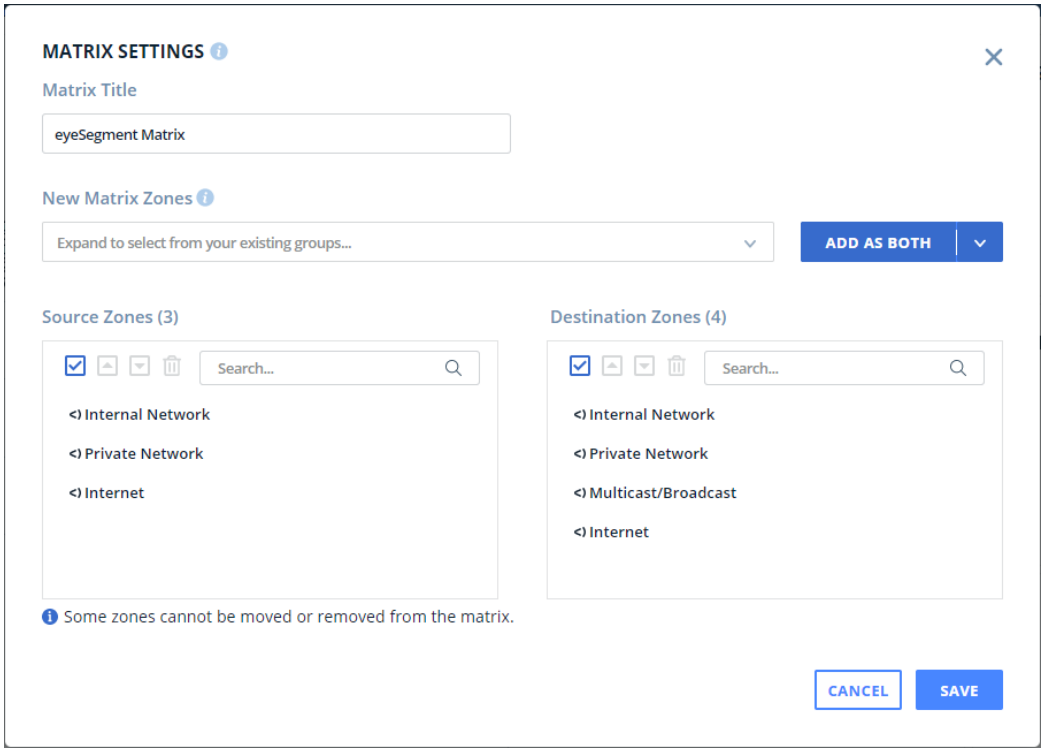
By default, the matrix includes the following virtual zones as both Source and Destination zones (unless otherwise noted):

Internal Network	Contains all IP addresses included in Forescout's internal network and not in another user-defined Source or Destination zone in the matrix.
Private Network	Contains all IP addresses that are not in Forescout's internal network but are in the company's private network.
Multicast / Broadcast	Contains multicast and broadcast address ranges. (Destination zone only)
Internet	Contains all IP addresses that are not in any other zone.

The matrix shows the traffic from each Source zone to each Destination zone. You can add policy groups of interest as Source and Destination zones.

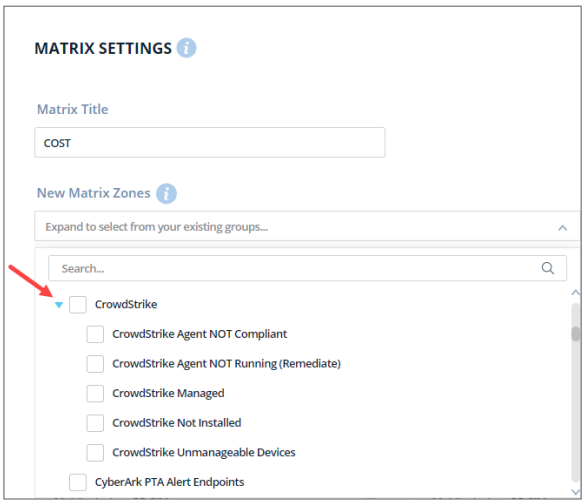
To configure the matrix settings:

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



2. Configure the following matrix settings:

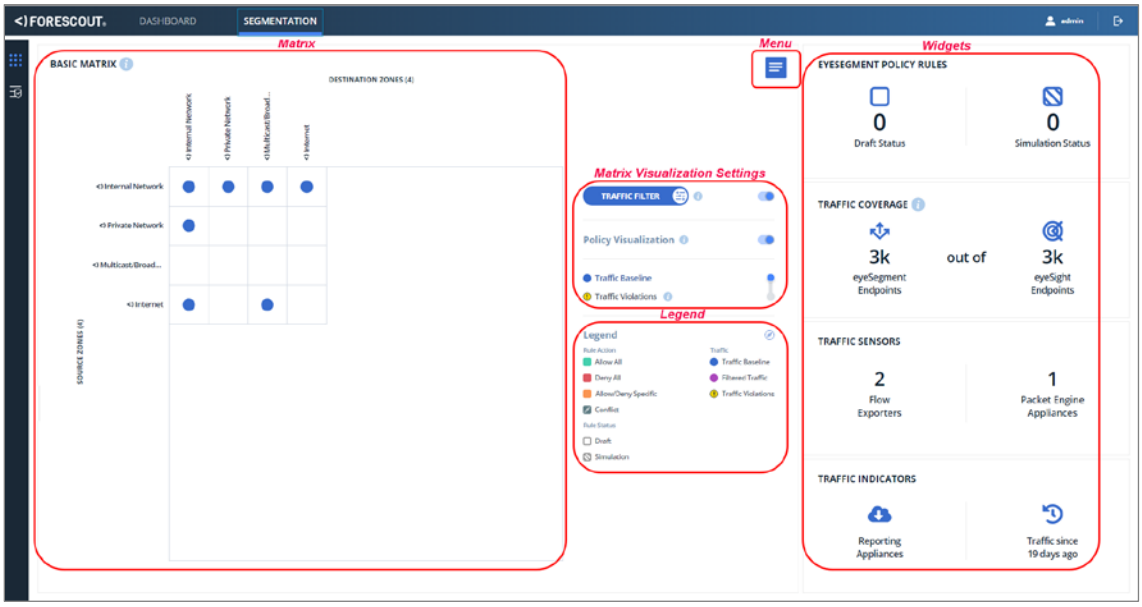
Matrix Title	Enter a meaningful name to be shown in the eyeSegment web portal.

New Matrix Zones	The matrix shows traffic from selected Source zones to selected Destination zones. Groups already included in the matrix as zones are shown in the Source and Destination Zone Lists below. **To add groups to the matrix:** **1.** Expand the dropdown menu to view the list of groups in your Forescout configuration. A blue triangle indicates a *nested structure* of groups. Select it to expand the structure if you want to select sub-groups.  **2.** Select one or more groups to be added as Source zones or Destination zones or both. If you followed the recommendations in Best Practices for Creating eyeSegment Zones, only select sub-groups in the 'IP Taxonomy Zones' structure. *Note: The number of Source zones need not match the number of Destination zones.*
Add As	▪ Select **Add as Source** if you want the matrix to show traffic originating from any IP address in the groups you just selected. ▪ Select **Add as Destination** if you want the matrix to show traffic that ended at any IP address in the groups you just selected. ▪ Select **Add as Both** if you want the matrix to show traffic that originated or ended at any IP address in the groups you just selected.
Source and Destination Zone Lists	The groups 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. *Note: You cannot remove the Internal Network and Private Network zones from the Source or Destination zone lists.*
Save / Cancel	Save or cancel your changes.

View the Matrix Page

After the initial matrix definition, the matrix is shown whenever you open the eyeSegment web portal.

It might take a minute or two the first time the data is loaded.



The eyeSegment Matrix page includes the following areas:

- Matrix
- Matrix Visualization Settings
- Legend
- Menu
- Widgets

Matrix

The matrix area contains:

- The matrix title.
- The Source and Destination zone names for each 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.
  - A blue ● icon indicates that the traffic is not filtered and all detected traffic is indicated in the matrix.
  - A violet ● icon indicates that a traffic filter is applied and that additional traffic might have been detected but is not shown due to the filter.

– A yellow icon indicates traffic that violated one of your simulated policy rules.

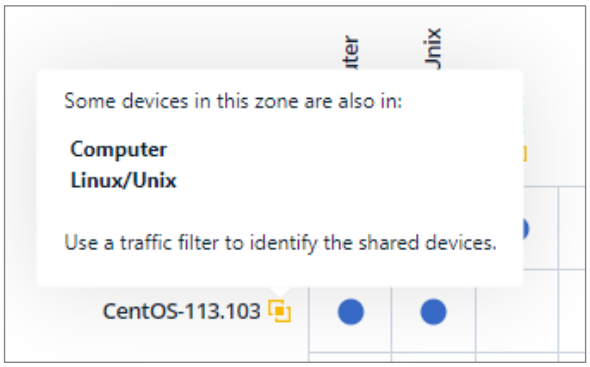
You can select a traffic icon to view details of the detected traffic. See View Traffic Details.

- If a filter is applied, a filter indicator FILTERED is displayed above the top left corner of the matrix.

Overlapping Zone Indicators

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.

The Overlapping Zones icon is displayed next to the zones that have shared members. Hover over an icon to view the names of the other zones with which it shares one or more devices.



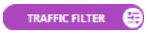
To identify the shared devices:

1. For each Source or Destination zone with an Overlapping Zones icon :
   a. Filter the Traffic for both of the following:
      › the Source or Destination zone of the matrix cell
      › one of the zones in its tooltip
   b. Select each Filtered Traffic icon, and drill down into the matrix to view the matching IP addresses.
2. Repeat step 1 for each zone in each Overlapping Zone.

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

Matrix Visualization Settings

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

	Select to view or change Source, Destination and Service (port/protocol) traffic filters to the traffic shown in the matrix. See Filter the Traffic. Blue  indicates that the traffic shown is not filtered. Violet  indicates that a traffic filter is applied. The matrix shows only traffic that matches all of the zones and one of the services defined in the traffic filter. Use the toggle to apply or remove the filter 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 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, select **Traffic Violations** to hide all traffic except traffic that violated any of your simulated policy rules. Select ! to view details of the traffic. See View Traffic Details.

Legend

The Rule Action and Rule Status indicators are only displayed in the matrix when **Policy Visualization** is applied. The color indicates the rule action 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 are unpredictable.

Filtered Traffic icons are only displayed in the matrix when the **Traffic Filter** is applied.

Traffic Violation icons are only displayed in the matrix when the **Traffic Violations** is selected.

Menu

Select the menu to view the following options:

- **Matrix Settings** to view or modify the matrix name and its zones. See Configure the Matrix.
- **Traffic Filter** to add Source, Destination and Service (port/protocol) traffic filters to the traffic shown in the matrix. See Filter the 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 Traffic Data.
- **Get Started** to view the Get Started diagram in a different browser tab.
- **Help** to view this How-to Guide on the web.

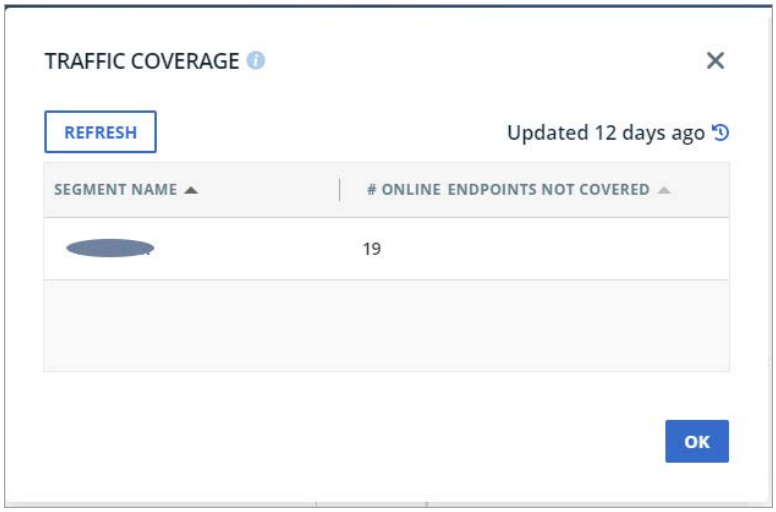
Widgets

Widgets display helpful information about your eyeSegment configuration.

- The **eyeSegment Policy Rules** widget indicates how many of your policy rules are in Draft status and how many are in Simulation status. Click anywhere in the widget to open the eyeSegment Policy page that lists all the rules.
- The **Traffic Coverage** widget indicates how many endpoints eyeSegment received traffic data for, and how many endpoints are online in your internal network (eyeSight). Click anywhere in the widget to discover which segments in your internal network include endpoints that haven't reported traffic data to eyeSegment.

  It might take a few minutes to load the data.

  Endpoints that are not included in any defined segment are listed in the virtual segment named 'N/A'.



- The **Traffic Sensors** widget shows information about the devices that report traffic data to eyeSegment:
  - **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.

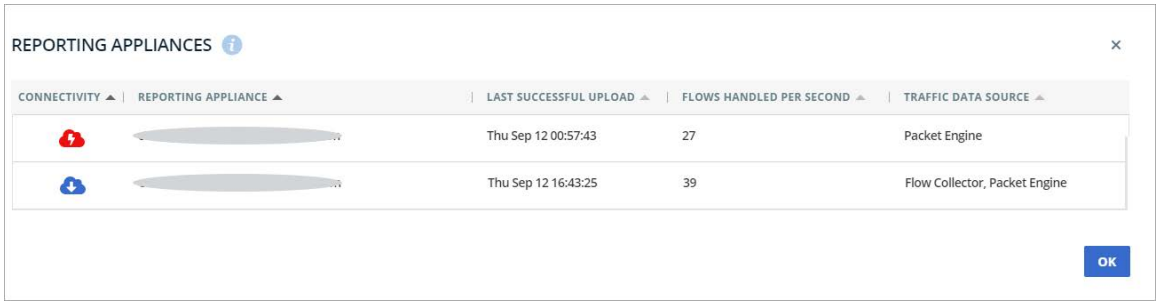
    Note: These are not Appliances.

  - **Packet Engine Appliances**: Appliances on which the Packet Engine is configured to 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.*

- Use the **Traffic Indicators** widget to determine if all the traffic data in your network has been uploaded to eyeSegment.
  - **Reporting Appliances**: 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 minute
    - Traffic data source: Packet Engine and/or Flow Collector



> *If* Packet Engine *is not listed as a data source, verify that the channels were configured correctly on the Appliance.*

– How long the real-time traffic data shown in the matrix has been collected.

> *Traffic collection does not begin until the Cloud Uploader Plugin is configured.*

Filter the Traffic

When a filter is applied, traffic from the Source zone to the Destination zone is only shown if it meets all the filter conditions. You can include any Forescout policy group as a Source or Destination filter.

For example, filter the matrix to only display traffic sent from the devices in the Source zone that are also in *all* of the following groups:

- London Office
- High-Risk Assets
- Remote Devices

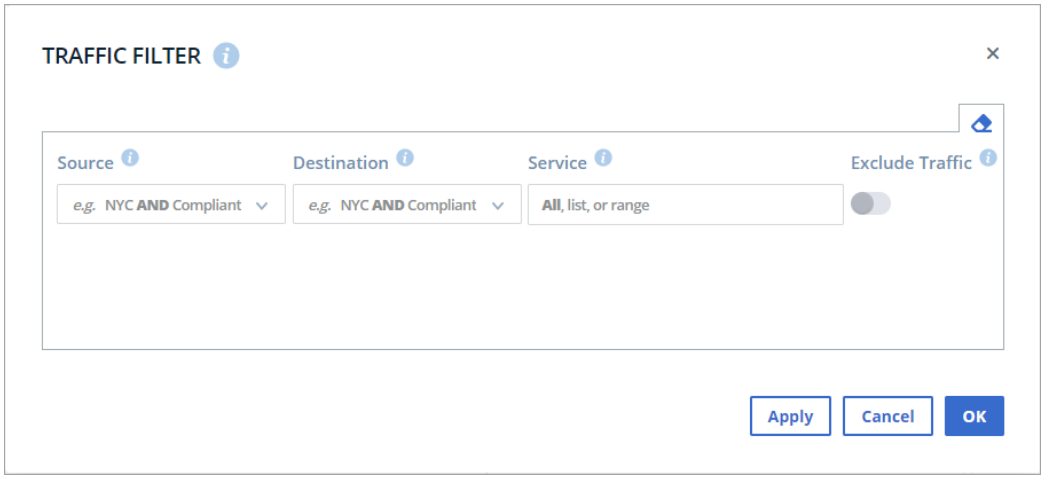
Each filter field — Source, Destination, Service — is applied if at least one value is defined for it.

> *Ensure that the policies that manage the filter groups are run on the devices to be shown in the matrix.*

To add or modify a traffic filter:

1. Select the Traffic Filter button 

to open a draggable Traffic Filter window, and select one or more filter fields.



- If **Exclude Traffic** is not selected, traffic is only shown if it meets all of the following conditions:
  - The traffic originated at a device that is a member of *all* the groups selected in the **Source** filter field. The matrix will show no other traffic.
  - The traffic ended at a device that is a member of *all* the groups selected in the **Destination** filter field. The matrix will show no other traffic.
  - The traffic used *one* of the **Service** filter fields. The matrix will show no other traffic.
- If **Exclude Traffic** is selected, traffic is only shown if it meets all of the following conditions:
  - The traffic originated at a device that is not a member of *any* of the groups selected in the **Source** filter field.
  - The traffic ended at a device that is not a member of *any* of the groups selected in the **Destination** filter field.
  - The traffic did not use *any* of the **Service** filter fields.

  The Source and Destination dropdown lists are shown in alphabetical order. Sub-groups are listed under their Level 0 in the group hierarchy.

  You can use the Clear Filter icon  *to clear all the filter fields.*

2. Select **Apply** to see how your filter selections affect the displayed traffic.

   Drag the Traffic Filter window if it is blocking part of the display.

3. When a filter is applied, the traffic icons and the Traffic Filter button are violet to indicate that the matrix shows only traffic that matches the filter.

View Traffic Details

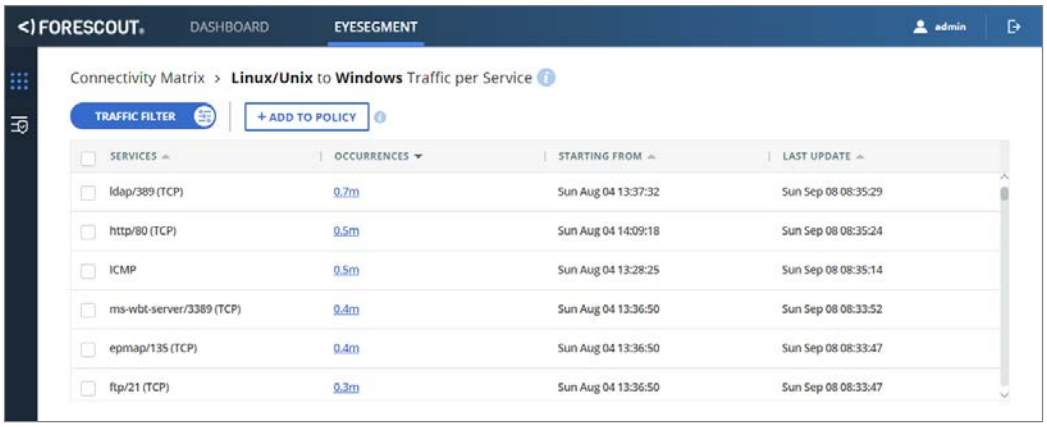
For each traffic icon, you can view the sub-groups, services, Source and Destination IP addresses, and the number of occurrences of the traffic within the defined time range. Use this information to help decide which groups to add to the matrix or to a filter.

You can select the filter indicator to add a filter or to view the existing filter.

To view details of a specific traffic pattern:

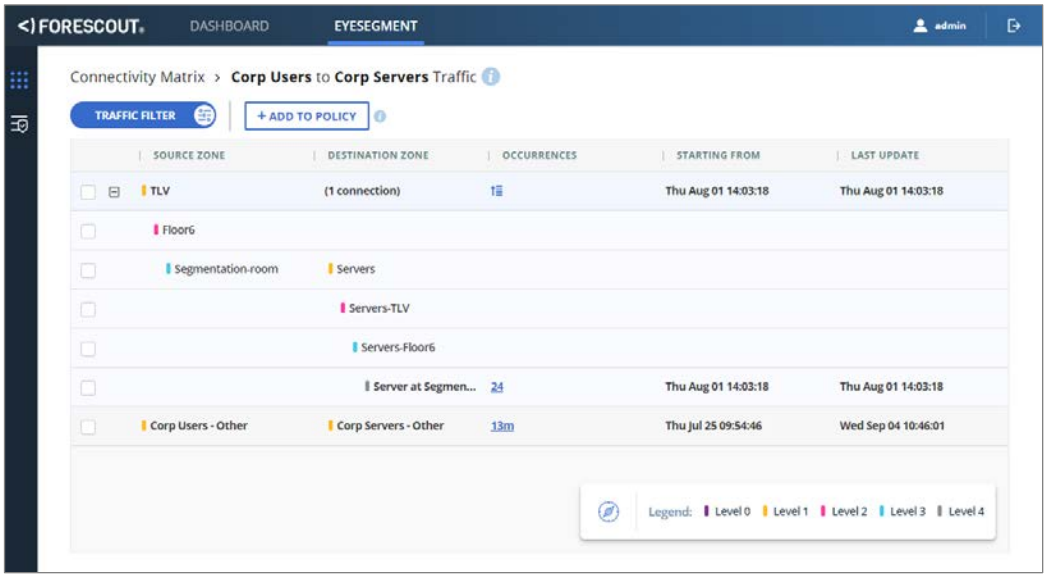
1. In the matrix, select the traffic icon (, , or) of the specific Source and Destination zone. Details are shown for each service used by the traffic.
2. If neither of the selected zones is a nested structure, the detected traffic is listed per service.

   In the example below, details are shown for all traffic originating from devices in the *Linux/Unix* zone and ending at devices in the *Windows* zone.



3. If one of the selected zones is a nested structure, a color indicates the level of each sub-group for which traffic was detected. If lower-level sub-groups 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 it is in, followed by '- Other'.

In the example below, details are shown for the detected traffic originating from devices in the *Corp Users* zone sub-groups and ending at devices in the *Corp Servers* zone sub-groups.

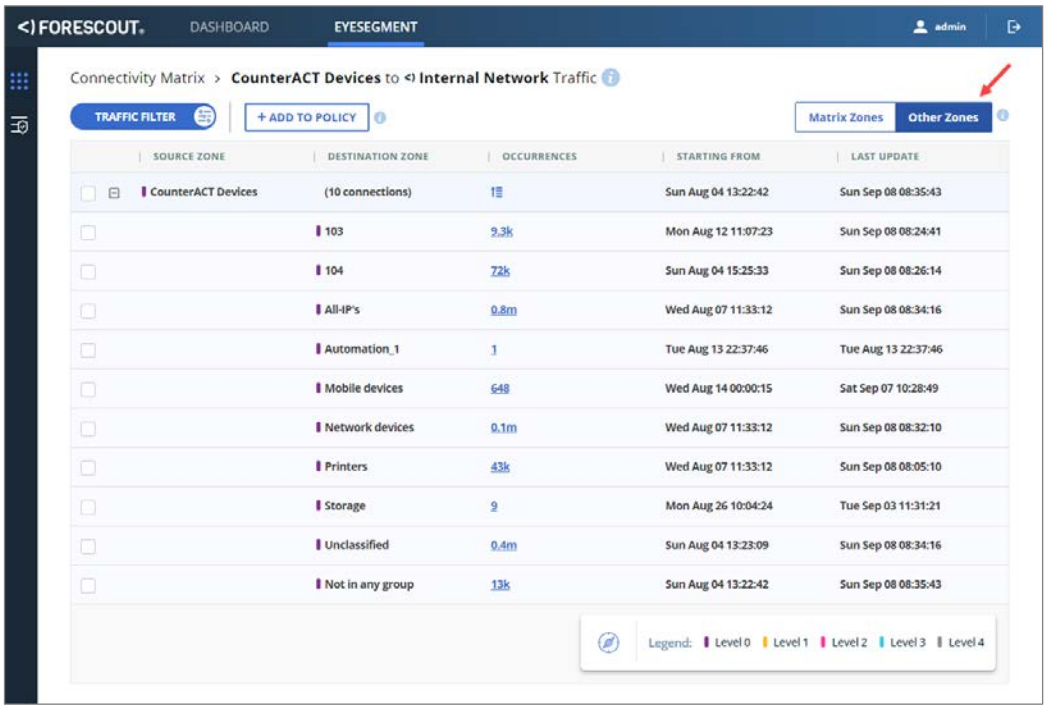


To see traffic per service, select the Occurrences value of the Source and Destination zone traffic.

4. 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 **Matrix Zones** to view these IP addresses as one virtual matrix zone named <) *Internal Network.*

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



View IP-to-IP Traffic Details

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

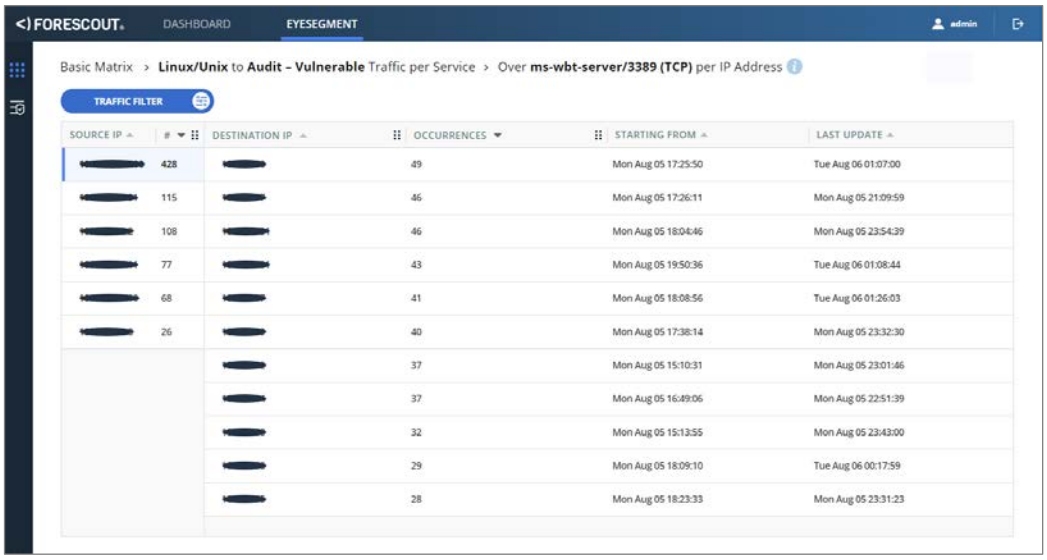
If more than 1,000 IP addresses in the selected Source or Destination group had traffic, you can view 1,000 addresses:

- *that had the most amount of traffic*
- *that had the least amount of traffic*

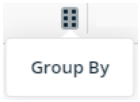
To view details of IP addresses that sent or received traffic:

1. In the Traffic per Service page, select the Occurrences value of the Source and Destination zone traffic. The traffic details are shown for each Source and Destination IP address.

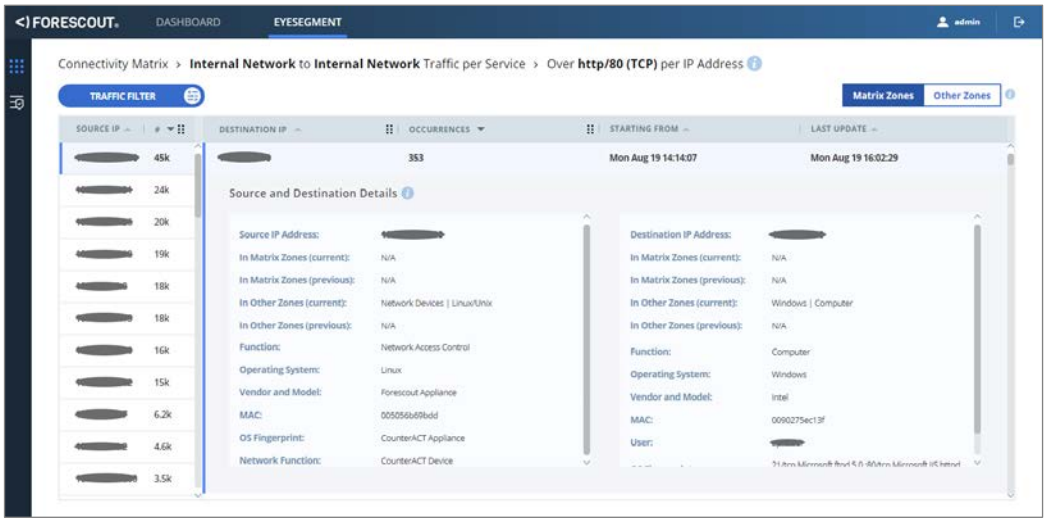
   In the example below, IP addresses are shown for all traffic originating from devices in the *Linux/Unix* zone and ending at devices in the *Audit - Vulnerable* zone and that used *ms-wbt-server* as the service.



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



3. Select a row to view details about the Source and Destination devices.



Delete Traffic Data

You can permanently delete some or all the traffic data used for the matrix. You may 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 is divided into multiple groups

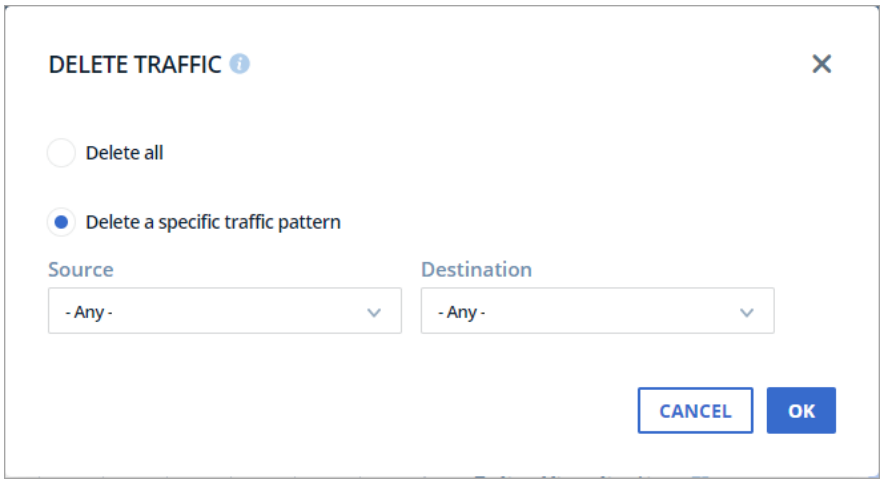
Complete all group adjustments before you delete the traffic so that all subsequent traffic is aligned with its correct groups.

Many resources are required for traffic data deletion, and the process might take a few minutes. To maintain efficiency, eyeSegment limits how often you can delete the data. You can delete the traffic data not more often than:

- once per hour
- 30 times per week

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.



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

   The delete process may take several seconds.

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 all the traffic so that the matrix accurately reflects the traffic in the stated time period.

Use an 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-groups and services.

By default, all traffic is allowed.

> *In this version, rules that deny traffic cannot actually block traffic. They can be used to display suspicious traffic in the matrix and also to send a notification when this traffic is detected.*

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.*

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

- Specific groups and sub-groups defined in your Forescout configuration.
- 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 group that are not members of any of its lower-level sub-groups.

There are two ways to create eyeSegment policy rules.

- Manually Create Policy Rules
- Automatically Create Policy Rules

What You Need to Know about This Version

In this version:

- The status of a rule can be set to either **Draft** or **Simulation**.
- The eyeSegment policy is for simulation purposes only.
- The policy cannot actually deny traffic.

Simulated Rules

When the rule status is *Simulation* and 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.
- The traffic pattern is not included in a rule exception.

When the rule status is *Simulation* and an 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.
- The traffic pattern is included in the rule exception.

If **Notification** is selected in the rule and a simulated traffic violation occurs:

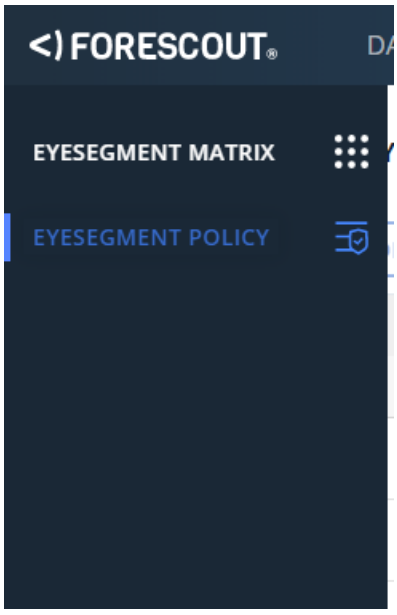
- On the device that sent the traffic violation, the policy adds the name of the rule that denied the traffic to the *Traffic Was Denied from This Client* property.
- On the device that received the traffic violation, the policy adds the name of the rule that denied the traffic to the *Traffic Was Denied to This Server* property.

To visualize the violations on the eyeSegment Matrix page, select **Traffic Violations** in the matrix visualization settings.

Manually Create Policy Rules

To manually create an eyeSegment policy rule:

1. In side navigator, select the **eyeSegment Policy** page.



2. Select **Add Rule**.
3. See Configure Policy Rules.

Automatically Create Policy Rules

You can automatically create an eyeSegment policy rule in Draft status from a *Traffic* or *Traffic per 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 per 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 a filter is applied, it is automatically included in the rule exceptions.

To automatically create a rule and exceptions for specific traffic patterns, select the sub-groups and services to be the 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 Traffic Details 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.

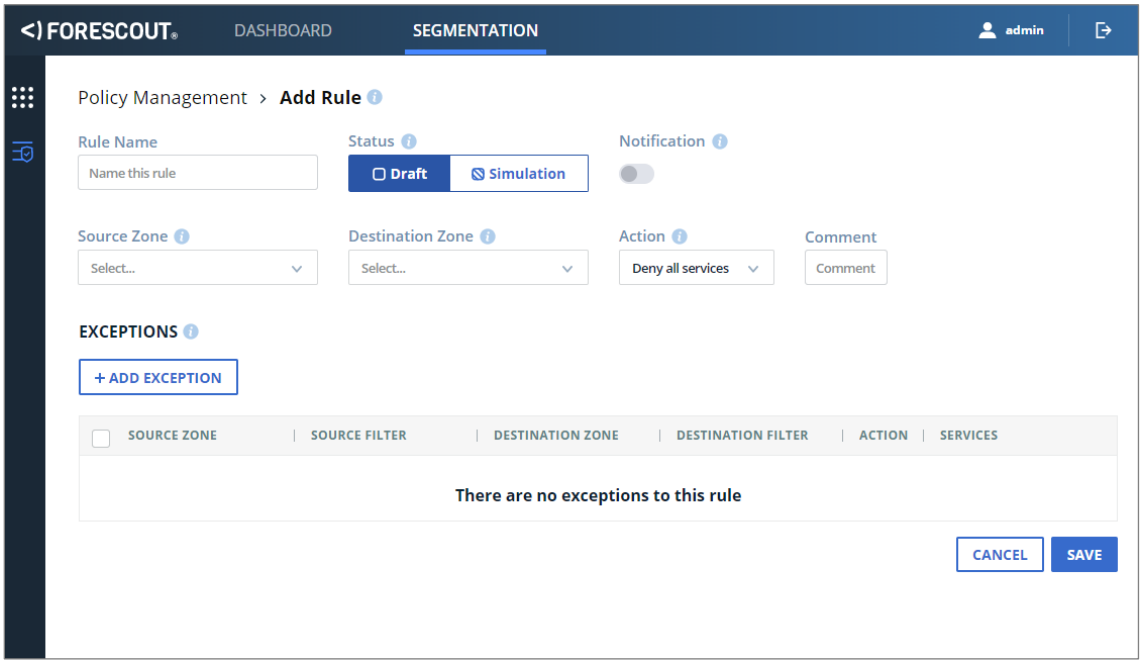
4. Select **Show Me the Rule**.
   - If this traffic did not have a rule, a new rule having a default name is displayed.
   - If a rule already exists for this traffic, the existing rule is displayed.

   The service or traffic patterns you selected are displayed as exceptions to the rule.
5. You can modify the rule and exception fields. See Configure Policy Rules.

Configure Policy Rules

You can change rule fields at any time.

If you save changes to a rule that was in Simulation status, all its previously detected simulated traffic violations are cleared from the matrix.



To configure a policy rule:

1. Name the rule.
   - Rule names are displayed in the eyeSegment Policy page.
   - When a rule in Simulation status with Notification denies traffic, the rule name is written to a device property on both the client and the server.
2. 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-groups.*
   - *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 them to the matrix. Adding the zones enables you to visualize the rule and its violations in the matrix.*
3. 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 matrix, you can see an indication that the traffic between these zones is defined as *Deny* or *Allow*.

4. 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**.
5. To update a device property whenever the device is the source or destination of traffic denied by this rule, select **Notification**. See Send Notifications Based on Policy Results.

   > *This setting is not available when the rule status is* Draft.

6. 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. In 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 a sub-group of, the zones in the rule.

   > *A selected zone includes also all IP addresses in its sub-groups.*

3. Optionally select other groups 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.

Send Notifications Based on Policy Results

Device properties can be set whenever a device is the source or destination of denied traffic, and these properties can trigger a notification event.

The *Traffic Was Denied from This Client* property contain the names of all the eyeSegment policy rules that met the following conditions:

- *Notification* was selected.
- The simulated rule denied traffic from the device.

The *Traffic Was Denied to This Server* property contain the names of all the eyeSegment policy rules that met the following conditions:

- *Notification* was selected.
- The simulated rule denied traffic to the device.

This list of rules can be viewed in the Forescout Console.

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, refer to the *eyeSegment Module Configuration Guide*. To access the guide from your Forescout Console after the plugin is installed, select **Tools** > **Options** > **Modules**, select **eyeSegment**, and then select **Help**.

Visualize the eyeSegment Policy in the Matrix

All traffic is evaluated by your eyeSegment policy.

- Traffic denied by an eyeSegment policy rule 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.

Considerations and Troubleshooting

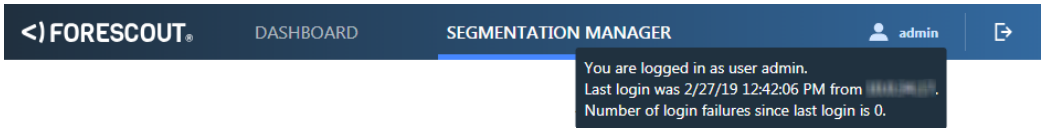
Consider the following when using eyeSegment:

- Web Portal User Security
- Very Little Traffic Data in the Matrix
- Very Little Traffic Data for a Group
- Rules Cannot Be Deleted
- Groups Cannot Be Deleted

Web Portal 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 group defined in the Console.

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.

Very Little Traffic Data for a Group

The traffic data of network devices that are not part of any group is saved in the Internal Network zone.

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

Rules Cannot Be Deleted

When a policy is created in the Console from the eyeSegment Policy Compliance policy template, the names of your eyeSegment policy rules are defined in the conditions. You cannot delete a rule from your eyeSegment policy until the rule name is removed from these policy conditions.

Groups Cannot Be Deleted

The Console Groups Manager does not allow you to delete a group that 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.

Additional Forescout Documentation

For information about other Forescout features and modules, refer to the following resources:

- Documentation Downloads
- Documentation Portal
- Forescout Help Tools

Documentation Downloads

Access documentation downloads from the Forescout Resources Page, or one of two Forescout portals, depending on which licensing mode your deployment is using.

- ***Per-Appliance Licensing Mode*** – Product Updates Portal
- ***Flexx Licensing Mode*** – Customer Portal

Software downloads are also available from these portals.

To identify your licensing mode:

- From the Console, select **Help > About Forescout**.

Forescout Resources Page

The Forescout Resources Page provides links to the full range of technical documentation.

To access the Forescout Resources Page:

- Go to https://www.Forescout.com/company/resources/, select **Technical Documentation,** and search for documents.

Product Updates Portal

The Product Updates Portal provides links to Forescout version releases, Base and Content Modules, and eyeExtend products, as well as related documentation. The portal also provides a variety of additional documentation.

To access the Product Updates Portal:

- Go to https://updates.forescout.com/support/index.php?url=counteract and select the version you want to discover.

Customer Portal

The Downloads page on the Forescout Customer Portal provides links to purchased Forescout version releases, Base and Content Modules, and eyeExtend products, as well as related documentation. Software and related documentation only appear on the Downloads page if you have a license entitlement for the software.

To access documentation on the Forescout Customer Portal:

- Go to https://Forescout.force.com/support/ and select **Downloads**.

Documentation Portal

The Forescout Documentation Portal is a searchable, web-based library containing information about Forescout tools, features, functionality, and integrations.

If your deployment is using Flexx Licensing Mode, you may not have received credentials to access this portal.

To access the Documentation Portal:

- Go to https://updates.forescout.com/support/files/counteract/docs_portal/ and use your customer support credentials to log in.

Forescout Help Tools

Access information directly from the Console.

Console Help Buttons

Use context-sensitive *Help* buttons to access information about tasks and topics quickly.

Forescout Administration Guide

- Select **Forescout Help** from the **Help** menu.

Plugin Help Files

- After installing the plugin, select **Tools** > **Options** > **Modules**, select the plugin, and then select **Help**.

Online Documentation

- Select **Online Documentation** from the **Help** menu to access either the Forescout Resources Page (Flexx licensing) or the Documentation Portal (Per-Appliance licensing).