



Illumio Core[®]

Version 22.4

Introduction to the Platform

November 2022

14000-300-22.4

Legal Notices

Copyright © 2022 Illumio 920 De Guigne Drive, Sunnyvale, CA 94085. All rights reserved.

The content in this documentation is provided for informational purposes only and is provided "as is," without warranty of any kind, expressed or implied of Illumio. The content in this documentation is subject to change without notice.

Product Version

PCE Version: 22.4

For the complete list of Illumio Core components compatible with Core PCE, see the Illumio Support portal (login required).

For information on Illumio software support for Standard and LTS releases, see [Versions and Releases](#) on the Illumio Support portal.

Resources

Legal information, see <https://www.illumio.com/legal-information>

Trademarks statements, see <https://www.illumio.com/trademarks>

Patent statements, see <https://www.illumio.com/patents>

License statements, see <https://www.illumio.com/eula>

Open source software utilized by the Illumio Core and their licenses, see [Open Source Licensing Disclosures](#)

Contact Information

To contact Illumio, go to <https://www.illumio.com/contact-us>

To contact the Illumio legal team, email us at legal@illumio.com

To contact the Illumio documentation team, email us at doc-feedback@illumio.com

Contents

Chapter 1 Illumio Core Overview	4
About the Illumio Core Platform	4
Workloads	5
Visualization Overview	7
About the Maps	7
Illumination	8
App Group Map	9
Explorer	12
Vulnerability Map	14
Essential Rule Coverage in Illumination and Explorer	15
Chapter 2 Policy Overview	16
Policy Objects	16
Segmentation Templates	17
Services	17
IP Lists	18
Pairing Profiles	18
Virtual Services	19
Virtual Servers	19
Labels and Label Groups	19
How to Create Policy	22
About Rulesets	22
About Rules	23
Rule Writing Examples	23
Custom iptables Rules	26
Rule Search	27

Illumio Core Overview

This chapter contains the following topics:

About the Illumio Core Platform	4
Visualization Overview	7

Illumio is a micro-segmentation product to segment your applications by using the host-based firewall. Illumio uses a allowlist model, which means all traffic is blocked by default. Without a rule, traffic is not allowed to reach the hosts in your environment.

This section introduces the components of the platform and how the platform provides security for your environment.

About the Illumio Core Platform

The Illumio Core consists of two key components — the Policy Compute Engine (PCE) and the Virtual Enforcement Node (VEN).



The PCE is the server side of the Illumio platform. It is the segmentation policy controller and the central manager for the VEN.

The VEN is the agent that is installed on your workloads.

For systems where the agent cannot be installed, you can create unmanaged workloads in the PCE to represent traffic and to use in policy. See the *Security Policy Guide* for more information.

For information about the operating systems supported for the PCE and VEN, see the [OS Support and Package Dependencies](#) pages in the Illumio Support portal.

Workloads

In the Illumio Core, a workload is defined as an OS endpoint where applications and services are running and a VEN resides (when managed). Workloads can be running on bare-metal, in a virtual machine, or as a host platform for containers. Workloads can be running in private datacenters or in cloud environments.

Managed versus Unmanaged Workloads

Managed: When you “pair” a workload with the PCE, the Illumio VEN is installed on it so that the VEN can manage the workload’s native host firewall. A workload that has a VEN installed on it is called a managed workload.

Unmanaged: To create an unmanaged workload, you configure all the details of the workload in the PCE but you do not install a VEN on it, and it is not considered “paired” with the PCE.

How the VEN Runs on Workloads

The VEN has several modes it can run in:

- **Idle:** VEN doesn’t take control of the host-based firewall on the workload and reports a netstat snapshot every 10 minutes.
- **Illuminated:** In build or test mode, the VEN controls the host-based firewall and reports real-time traffic roll ups every 10 minutes to the PCE. Illumio allows all traffic to reach the workload.
- **Enforced:** Only Illumio rules provisioned to the workload are enforced. All other traffic is dropped.

See the *VEN Administration Guide* for more information.

Coexistence mode allows multiple firewalls to coexist, but this is usually for specialized cases and must be enabled on the PCE.

Understanding Illumio Traffic Flows

In the Illumio Core, traffic flows are network traffic in your environment flowing between VENs and other entities in your network.

Traffic flows from the VEN get processed in the PCE by matching them to objects in the following order:

Managed Workloads → Unmanaged Workloads → IP Lists → Unknown

When the PCE can't match the traffic flow to an object, it reports the traffic as unknown and displays a cloud icon in the visualization maps.

Additionally, Illumio divides traffic by its endpoint: traffic provider and traffic consumer.

- **Provider:** The traffic destination

Providers can be any workload, unmanaged workloads, virtual services, or IP addresses that provide a service as specified in the Consumers section of a rule when you define who or what is allowed to communicate with a workload. Providers cannot initiate connections to consumers.

- **Consumer:** The traffic source

Consumers can be groups of workloads, unmanaged workloads, virtual services, or IP addresses that can initiate a connection to a provider or consume a service as specified in the Consumers section of a rule when you define who or what is allowed to communicate with a workload.



NOTE:

In the PCE web console maps, the arrow head points to the provider (destination).

The PCE captures the following types of traffic:

- **Allowed**

- **Reported View:** The reported traffic is allowed because a rule exists to allow it and the rule is provisioned to the workload.
- **Draft View:** The reported traffic is allowed because a rule exists to allow it but the rule is not provisioned to the workload.

- **Potentially Blocked**

- **Reported View:** The PCE is reporting the traffic as potentially blocked because a rule to allow it either doesn't exist or wasn't provisioned to the workload. If the VEN on this workload was moved into enforcement mode, this traffic would be blocked.
- **Draft View:** The PCE is reporting the traffic as potentially blocked because a rule to allow it doesn't exist.

- **Blocked**

- **Reported View:** The VEN is in enforcement mode and a rule doesn't exist or hasn't been provisioned to the workload to allow the traffic.

See the *Visualization Guide* for more information about how the Illumination map displays allowed and blocked traffic.

Visualization Overview

In the PCE web console, you can find the following maps to help you visualize your environment:

- Illumination
- App Group Map
- Explorer
- Vulnerability Map

About the Maps

The maps in the PCE web console provide the following features.

Draft vs Reported in the Maps

In Illumination and the App Group Map, you have two views.

- **Draft:** For existing policy, shows the effect that the policy has on detected traffic flows and turns lines green (or in Explorer reports the traffic as allowed).



NOTE:

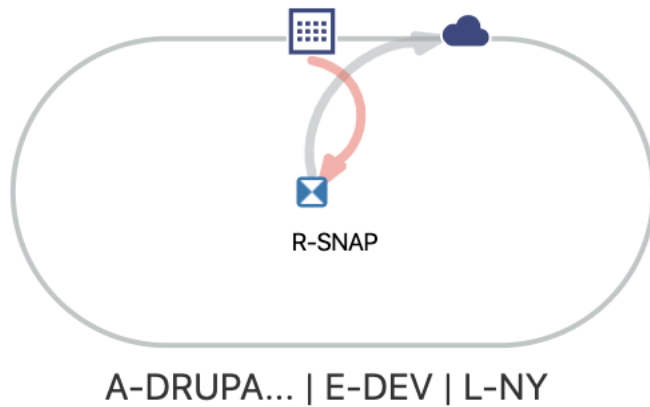
In Core 20.2.0 and later releases, draft view is also available for Explorer.

- **Reported:** Only shows the lines turning green (or in Explorer reported as allowed) after the policy was added, provisioned to the workloads, and a new traffic flow is detected.

See the *Visualization Guide* for more information about how Illumination displays allowed and blocked traffic.

IP Lists and Unknown Traffic

You create IP lists in the PCE to define your subnets, IP ranges, or a set of IP addresses. They are represented as a box containing 12 dots. The PCE web console displays unknown traffic as going to a blue cloud icon.



See the *Security Policy Guide* for more information.

Color Vision Deficiency Filter

In your Profile Settings, the PCE web console includes a Color Vision Deficiency option for customers who are colorblind. To enable this option, click your username in the upper right corner of the console and choose **My Profile**. Select the Color Vision Deficiency option and save the change.

When this option is enabled, green (allowed) traffic displays as blue in Illumination and the App Group Map.

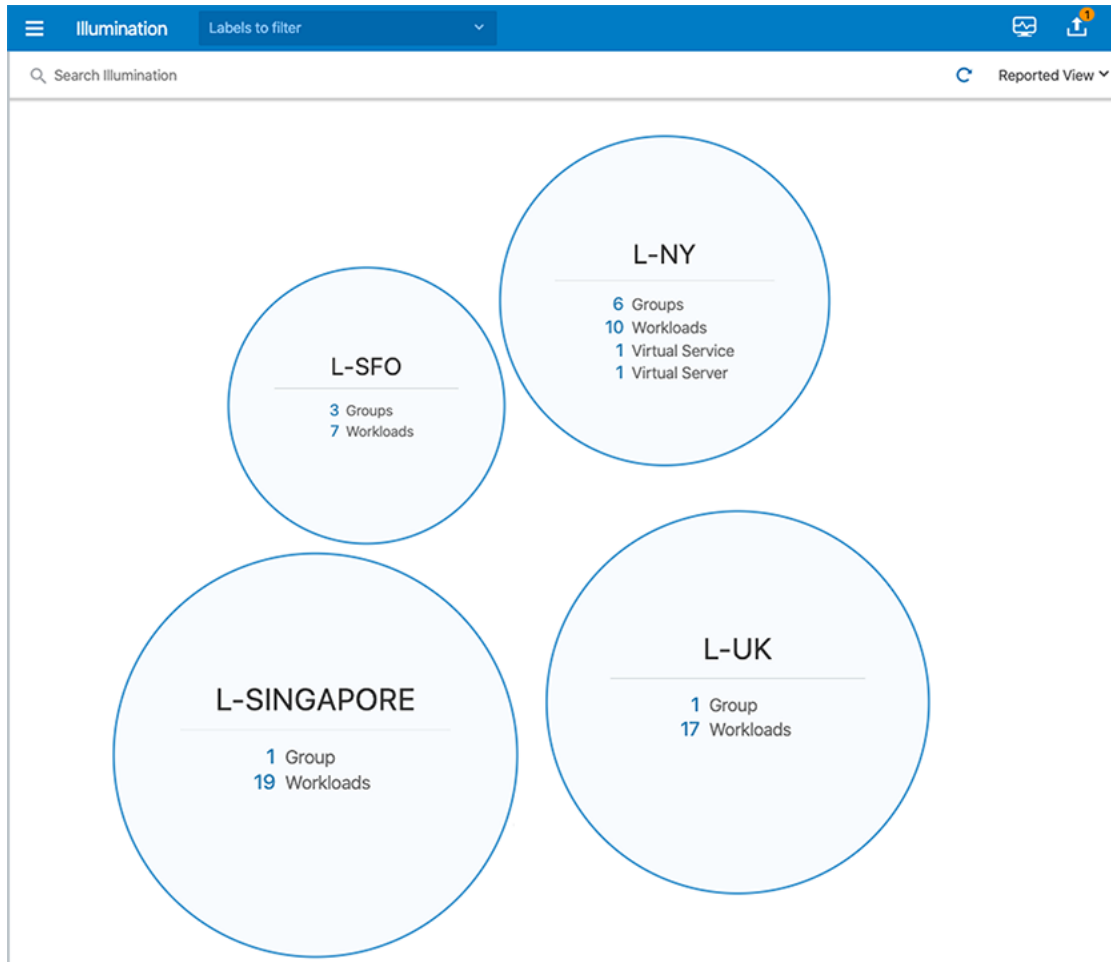
Review Maps Prior to Creating Policy

Before you begin creating policy for your environment, Illumio recommends that you analyze your traffic. You can analyze your traffic by viewing Illumination, the App Group Map, and Explorer. Viewing your traffic in Explorer is a great way to analyze your traffic because the data in it is sortable and exportable, and you can filter the traffic flows that are already impacted by policy.

Illumination

Illumination provides a unique way to reveal the traffic flows in your network and to help you configure policies to secure your applications. Illumination maps the outbound connections from workloads to unknown IP addresses to fully qualified domain names (FQDNs) or DNS-based names. For example, Illumination could display that the outbound connections from a workload are going to maps.google.com instead of hundreds of different IP addresses.

Illumination is organized from a location perspective. Clicking a location bubble in Illumination displays the workloads mapped to that location.

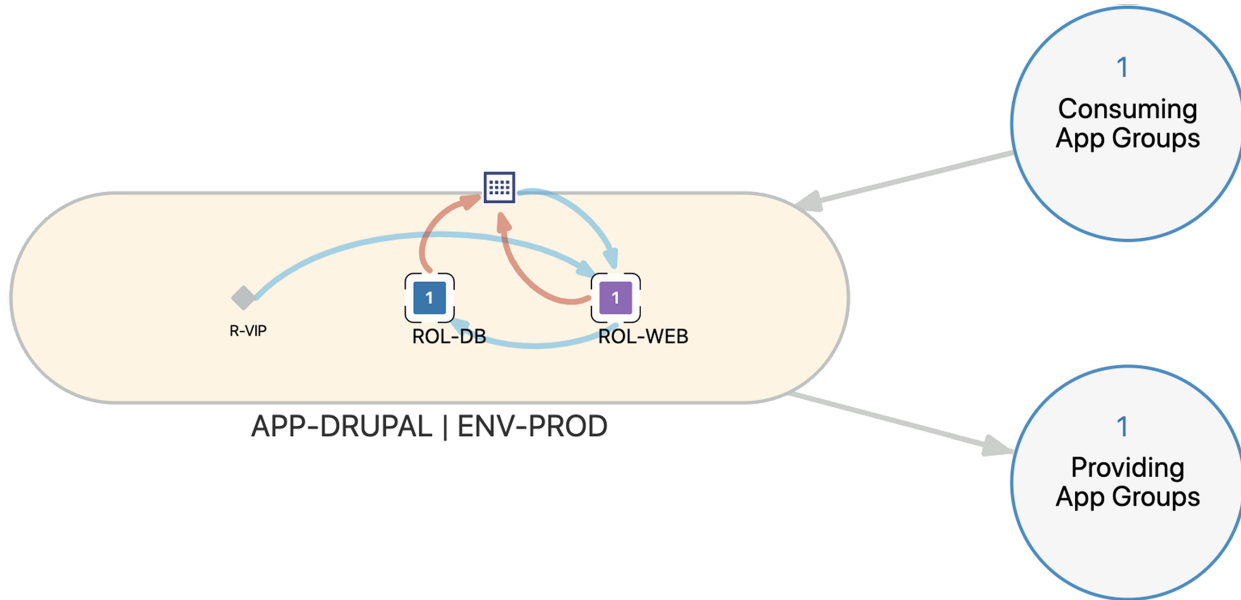


See the *Visualization Guide* for more information.

App Group Map

The App Group Map provides a way to view traffic to and from specific applications. Usually, customers prefer using this map when they want traffic information for specific applications. The App Group Map is especially valuable because it displays traffic flows from Consuming App Groups to your applications.

The Consuming App Groups bubble includes all app groups that your application is providing services to. The Providing App Groups bubble includes all services your application is consuming. Clicking the number in a Consuming App Groups bubble or Providing App Groups bubble allows you to review information about a specific app group communicating with your application or determine if the application is communicating outbound with another application.



Clicking a Consuming App Group or Providing App Group displays the traffic between the target application and the Consuming or Providing App Group. You no longer see the intra-scope traffic within the application. Clicking a traffic line displays the details of the traffic across that line.

The screenshot shows the 'App Group Map - Reported View' interface. On the left, a sidebar displays details for a 'ROLE-TO-ROLE' connection between 'ROL-DC' and 'ROL-WEB'. It lists two services: 'httpd' (80 TCP) and 'S-SSH' (22 TCP). Under 'Consumers', it lists 'ROL-DC', 'CSA-ACTIVEDIRECTORY', and 'LOC-NY'. Under 'Providers', it lists 'ROL-WEB', 'APP-DRUPAL', 'ENV-PROD', and 'LOC-NY'. The 'Last Detected' time is 11/01/2019, 11:01:25. A 'View RuleSets' link is also present.

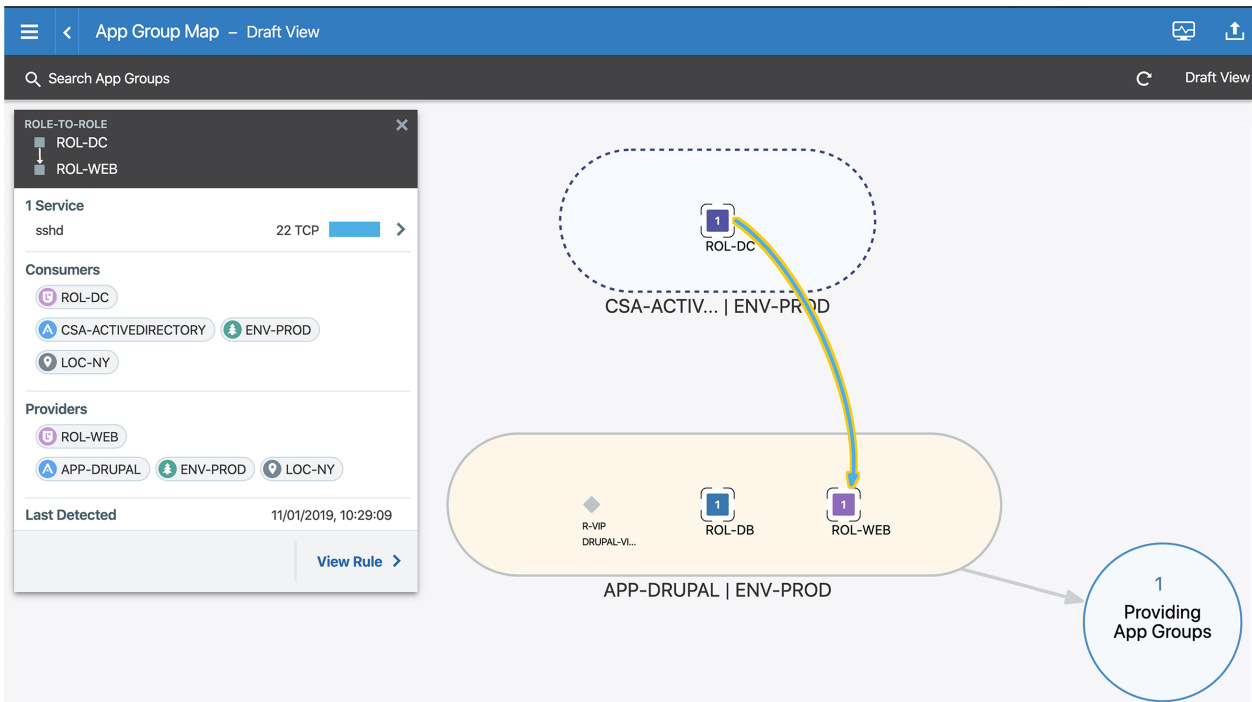
The main map area shows a dashed box around 'ROL-DC' (part of 'CSA-ACTIV... | ENV-PROD') and a solid box around 'APP-DRUPAL | ENV-PROD' containing 'R-VIP DRUPAL-VI...', 'ROL-DB', and 'ROL-WEB'. A thick orange arrow points from 'ROL-DC' to 'ROL-WEB'. A callout bubble on the right indicates '1 Providing App Groups'.



TIP:
Select the Consuming App Groups bubble and click the red lines around it to see the ports and protocols that require rules.

By default, the App Group Map displays your traffic from inside your application and to and from IP lists and unknown traffic.

In this example, the traffic flow 22 TCP displays the reported service as sshd. To distinguish between reported services and service objects, Illumio recommends you adopt a label naming convention. See [Labels and Label Groups](#) for more information.



TIP:
Create services that you can reuse in rules to make creating policy more efficient. See the *Security Policy Guide* for more information.

See the *Visualization Guide* for more information.

To globally include or exclude the location in all App Group Maps, set the App Group Type. Including the location displays a separate App Group Map for each location. Typically, you don't need to include the location especially when the same applications span multiple locations. (You must be a PCE global administrator to set the App Group Type.)

App Group Type

Description
App Groups are created automatically based on Workload labels and the App Group Type setting. App Groups can be configured to require two or three matching labels.

App Group Type

Application | Environment
Two Workload labels required to match. (Location label is ignored.)

Application | Environment | Location
Three Workload labels required to match

Explorer

The Explorer provides a historical view of your traffic flows. Use Explorer to search for different traffic combinations to and from any application. The information you obtain from Explorer helps you add the necessary policy for your applications. See the *Visualization Guide* for more information.

You can choose the way that Explorer displays traffic flow data:

- View the traffic flows your applications send and receive in tabular form or as parallel coordinates. When you view your traffic flows in tabular form, you can export your queries to CSV to analyze offline.
- View traffic flow data for "Consumers or Providers" or "Consumers and Providers." When you choose "Consumers or Providers," Explorer displays the inbound and outbound traffic you specified in the Include field.
- Use the "Draft View" or "Reported View" to view traffic flows. Having access to both views allows you to determine what traffic flows the Illumio Core will allow or block after provisioning your policy.

When you query Explorer, you will mostly want to look for Potentially blocked under Reported Policy or draft view - blocked traffic while building your policies.

Traffic Displayed for “Consumers Or Providers” and Draft View

The screenshot shows the Explorer interface with the following settings:

- View:** Consumers Or Providers
- Include:** Select Included Consumers Or Providers
- Exclude:** Select Excluded Consumers Or Providers
- Services:** Consumers And Providers
- Time:** Last Day
- Reported Policy:** All Policy States
- Format:** Table
- Draft View:** A dropdown menu is open, showing options: Reported View, Draft View, and All Draft (which is selected).



TIP:

- To help determine what policy to add for your applications, query Explorer for potentially blocked traffic by using the Reported Policy field or Draft view.
- To reduce the amount of traffic flows to analyze, exclude services or consumers.


The screenshot shows the Explorer interface with the following settings:

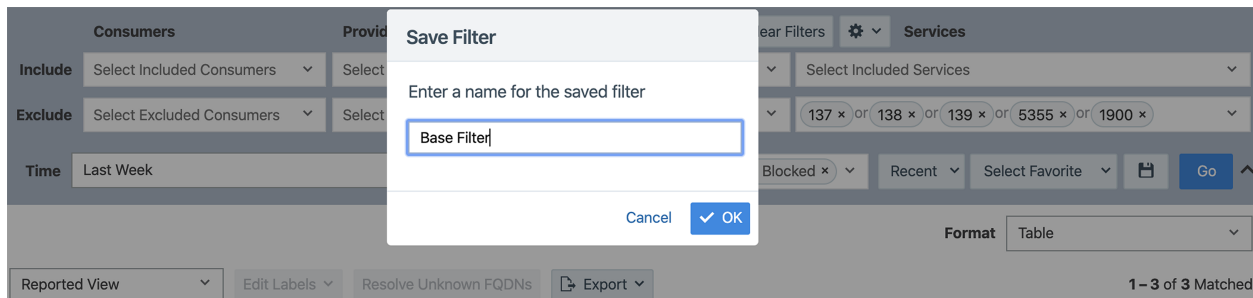
- View:** Consumers
- Providers:** DRUPAL, E-PROD
- Include:** Select Included Consumers
- Exclude:** Select Excluded Consumers
- Services:** Select Included Services
- Time:** Last Week
- Reported Policy:** Potentially Blocked
- Format:** Table

Reported Policy	Connection State	Consumer	Consumer Applications	Provider	Provider Labels	Port/Process [User]	Flows	First Detected	Last Detected
Potentially Blocked by Consumer	Timed Out	DC1 192.168.6.10	R-DC A-CSA-ACTIVEDIRECTORY E-PROD L-NY	DRUPAL-VIP 192.168.2.221 Unicast	R-VIP A-DRUPAL E-PROD L-NY	80 TCP iexplore.exe [HOME\greg]	7	11/26/2019 09:45:52	11/26/2019 09:45:52
Potentially Blocked by Consumer	Timed Out	WIN7-V4-PC 192.168.4.45	R-DESKTOP A-SYSTEMS E-PROD L-NY	DRUPAL-VIP 192.168.2.221 Unicast	R-VIP A-DRUPAL E-PROD L-NY	80 TCP chrome.exe [HOME\greg]	8	11/26/2019 09:30:35	11/26/2019 09:30:35
Potentially Blocked by Provider	Closed	DRUPAL-VIP 192.168.2.5	R-VIP A-DRUPAL E-PROD L-NY	drupal.home.lab 192.168.2.21 Unicast	R-WEB A-DRUPAL E-PROD L-NY	80 TCP httpd [root]	10697	11/25/2019 19:06:12	11/26/2019 09:36:05
Potentially Blocked by Provider	Closed	drupal.home.lab 192.168.2.21	R-WEB A-DRUPAL E-PROD L-NY	db.home.lab 192.168.2.22 Unicast	R-DB A-DRUPAL E-PROD L-NY	3306 TCP mysqld [mysql]	13	11/26/2019 09:30:54	11/26/2019 09:46:06
Potentially Blocked	Active	DRUPAL-VIP 192.168.2.5	R-VIP A-DRUPAL	drupal.home.lab 192.168.2.21	R-WEB A-DRUPAL	ICMP	10	11/26/2019 09:08:59	11/26/2019 09:39:05

Saving Explorer Filters

You can configure Explorer to filter out traffic flows that don't require policy. For example, Windows environments typically utilize protocols that generate a lot of traffic flows but don't require policy in most cases. You can save an Explorer query that excludes those protocols.

To save a filter, create your query with the excluded traffic flows, click the save  icon, and enter a name.



For example, you could create a base filter that excludes all three netbios ports, LLMNR (dnscache or link local multicast name resolution), and uPNP. To access a saved filter, select it from the **Select Favorite** drop-down menu.



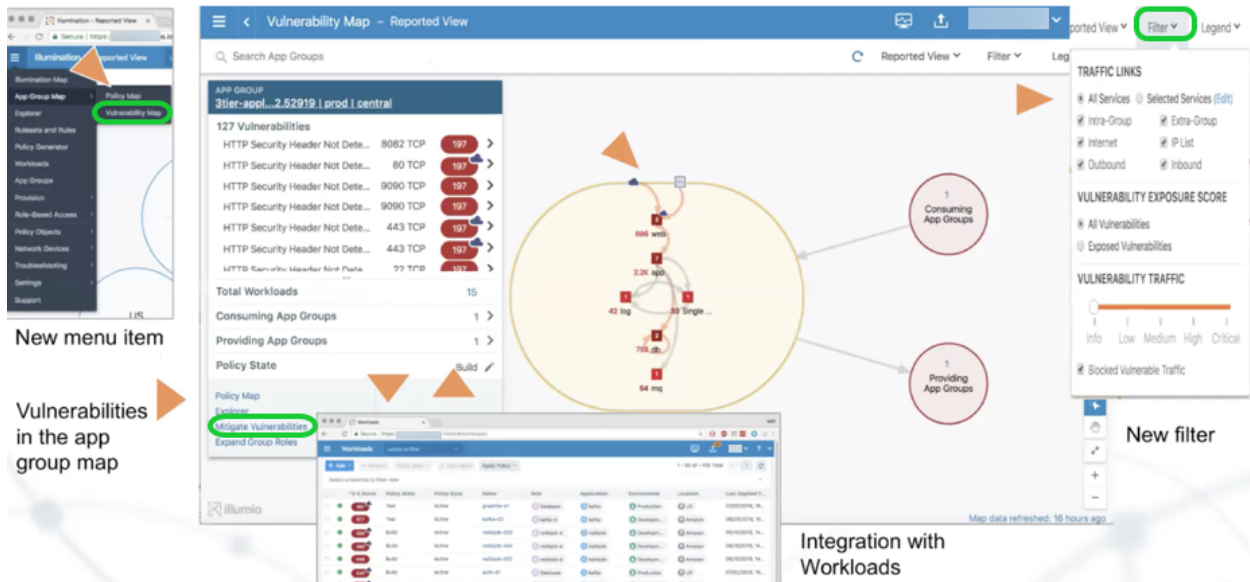
NOTE:

Saved filters include the consumers, providers, time, and reported policy type specified in the Explorer query. Make sure to set them as part of creating a saved filter.

Vulnerability Map

Vulnerability management and micro-segmentation are foundational security controls of a successful cybersecurity strategy. Vulnerability Maps combines Illumio's Application Dependency Map with vulnerability data from Qualys Cloud Platform to provide insights into the exposure of vulnerabilities and attack paths across your applications running in data centers and clouds.

It integrates application-dependencies and network flows with the vulnerabilities on the host that are exposed on communicating ports.



See the *Visualization Guide* for more information.

Essential Rule Coverage in Illumination and Explorer

Illumination and Explorer's draft view, flows allowed by essential service rules are reported as **Allowed** rather than **Blocked**. If an essential service rule allows a flow, the user-interface marks the flow as **Allowed** and displays that rule when the flow is selected.

IPSec-related essential service rules are still not considered in Illumination and Explorer as these rules are only enabled when workloads have SecureConnect or Machine Authentication rules that apply to them.

Policy Overview

This chapter contains the following topics:

Policy Objects	16
How to Create Policy	22

At a high level, policies are configurable sets of rules that protect network assets from threats and disruptions. The Illumio Core relies on policy to secure communications between workloads. This section introduces you to the elements (objects) of a policy and introduces you to creating your own policy to protect your environment.

Policy Objects

To help you create and update policy, you can create policy objects in the PCE. Policy objects include Segmentation Templates, services, IP lists, labels, label groups, user groups, virtual services, and virtual servers.

Some policy objects must be provisioned before any changes to them take effect on your workloads. See the *Security Policy Guide* for more information.

Segmentation Templates

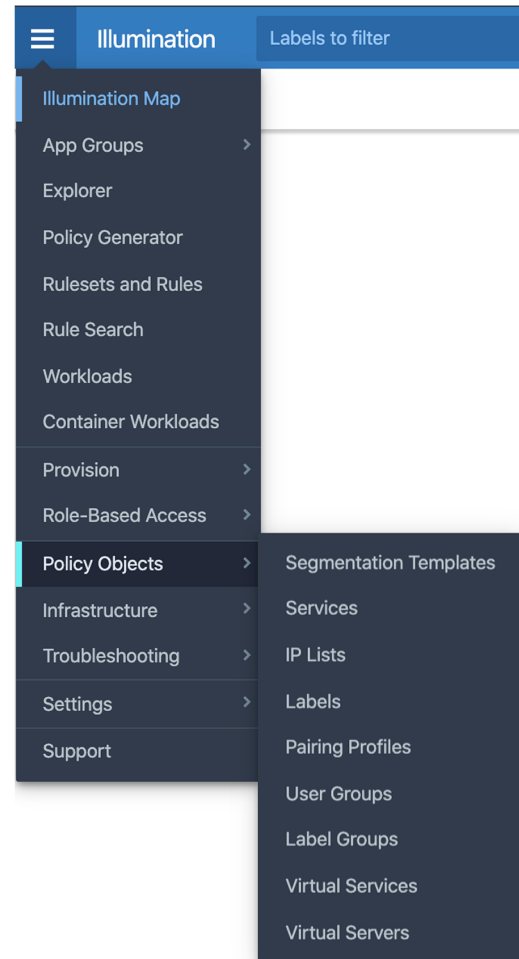
Segmentation Templates provide prepackaged, tested security policies that provide all the segmentation rules needed for common enterprise applications. They can include services, rulesets, rules, labels, and IP lists.

To use Segmentation Templates, log into your Support account and download them from the Illumio Tools Catalog. See the *Security Policy Guide* for more information.

Services

When you add a service to the PCE, you can specify multiple ports and protocols for the service and you can use it in multiple rules. When you update that service, the update applies to every rule where the service is added.

For example, if you update a service in the PCE by modifying its ports, every rule that includes that service will automatically include the updated ports.



TIP:

Adding services to the PCE is not required because you can specify them in your rules when you create policy. However, creating a list of common services that you can reuse in rules makes creating policy faster and more efficient.

When the PCE analyzes traffic flows, it might display a service as a service object in the maps. If a service object doesn't exist, the VEN might report the service that it detected when it captured the traffic flow or report the service as unknown.

See the *Security Policy Guide* for more information.

Windows Processed-Based Services

You can add Windows services to the PCE for specific processes running on Windows workloads.

IP Lists

IP lists allow you to define allowlists of trusted IP address, IP address ranges, or CIDR blocks that you want to allow into your datacenter and to be able to access workloads and applications in your network. Illumio recommends including IP lists in your rule-sets and rules to cover traffic flows from workloads that don't have installed VENs. For managed workloads (hosts with installed VENs), you should create policy by specifying the workloads' labels.



NOTE:

Creating policy using IP lists has the following limitations:

- Because IP lists consist of static IP addresses, policy created from them is not adaptive like policy you create by using labels. See the *Security Policy Guide* for an overview of using IP Lists in your policy. For a description of how Illumio policy is adaptive, see the *Security Policy Guide*.
- You cannot use an IP list in policy when the global consumer in the extra-scope rule has an installed VEN. IP lists do not program the out-bound side of rules for consumers.

Pairing Profiles

A pairing profile is a configuration that allows you to apply certain properties to workloads as they pair with the PCE, such as applying labels, setting workload policy state, and more. You can create pairing profiles for specific workload deployments.

However, Illumio customers often use generic pairing profiles for most of their workload deployments and update the workload labels after VEN installation.

When using a generic pairing profile, be sure that it contains generic default labels.

This way, you can easily identify newly managed workloads that need updated labels.

See the *VEN Installation and Upgrade Guide* for information on how to use pairing profiles.

Generic Label Example

- R-ONBOARDING
- A-ONBOARDING,
- E-ONBOARDING
- L-ONBOARDING

Virtual Services

You add virtual services to the PCE to create policy for multi-tenant applications and containers. Using virtual services, you can label services on a workload and add rules for specific services (not the entire workload).

For example, you have two databases in your environment that each run the same service on ports 1433 TCP and 3306 TCP. The databases are used by different applications. A workload can have only one set of labels. To create separate policy for each database application, you can uniquely label the database services on each workload based on their application.

See the *Security Policy Guide* for more information.

Virtual Servers

Virtual servers are imported from configured load balancers. You can label the virtual IPs (VIPs) imported from load balancers and include them in policy. In the Illumio Core, you can enforce policy on the load balancer itself to restrict inbound access to the VIP. See the *Security Policy Guide* for more information.

Labels and Label Groups

At a high level, policies are configurable sets of rules that protect network assets from threats and disruptions. The Illumio Core relies on policy to secure communications between workloads. Illumio policy uses a multidimensional label system to sort and describe the function of workloads. By describing workload functionally, policy statements are clear and unambiguous. Illumio users assign four-dimensional labels to their workloads to identify their roles, applications, environments, and locations. Creating policy by using labels is preferable over creating policy based on IP lists because policy created from IP lists is not adaptive like policy created by using labels.

You can create labels in several places in the PCE web console and the Illumio Core REST API. For example, go to **Policy Objects > Labels** from the main menu, or you can create them on the Workloads page.

In addition to labels, Illumio Core includes label groups, which are useful groupings of labels of the same type.

**IMPORTANT:**

When you use a label group in a ruleset scope or a rule, the label group is expanded into multiple scopes or rules, respectively. Therefore, be aware that using multiple label groups in a policy can cause that policy to contain a large number of rules.

See the *Security Policy Guide* for an explanation of how labels groups work.

How the Label Types Affect Policy

The combination of the four label types defines the boundary of your “firewall” when applying application segmentation to your environment. When applying labels to your workloads, the labels define the boundaries for your policy.

Understanding how these labels affect policy is important:

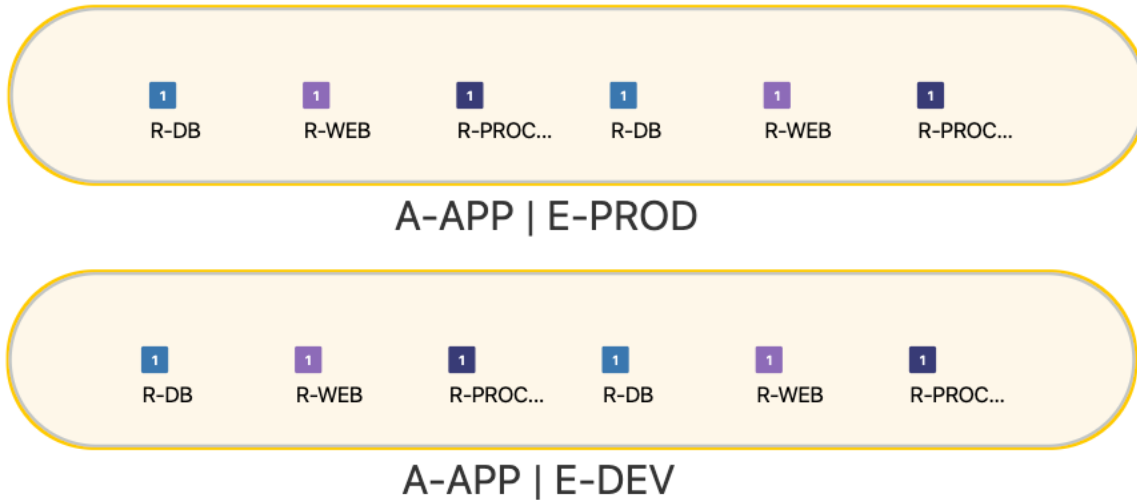
- **Role:** Defines the primary role of a workload based on the application label. In some cases, the role of a workload might be generic because the application has only one role.
- **Application:** Defines the primary application running on a workload. If a workload is running multiple applications, contact an Illumio Professional Services representative to discuss these scenarios.
- **Environment:** Defines the environment an application is operating in; such as, production, QA, test, development, or staging.
- **Location:** Defines where the workload is located; such as, in a specific datacenter or region.

**NOTE:**

When adding labels to rules, the PCE calculates policy in the following way: labels use an OR between the same label type and an AND between different label types.

Labeling Example

The following labeling example shows a three-tiered application that consists of four web servers, four intermediate servers, and four database servers in a production environment and a development environment:



Create this policy...	To have this workload affect...
For A-APP in E-PROD assign the ALL label for location	The policy only affects the workloads with the labels A-APP and E-PROD and the A-APP workloads in the E-DEV environment are not affected.
For the R-WEB role in the A-APP application in the E-PROD environment on port 443 TCP	Allows inbound traffic to the R-WEB role for A-APP in the E-PROD environment, but does not allow traffic to access the R-DB or R-Processing tiers.

Label Naming Recommendations

Illumio recommends you adopt a label design strategy and consistently follow it.

- Apply the same label naming convention for all object types in the PCE.
- Use a prefix of the label type in your label design strategy.
- Consistently use the same case (upper or lower) for all label names.

See the *Application Ringfencing Tutorial* for more recommendations about how to set up labeling.

Label Naming Examples

This example shows how a prefix for label type and uppercase are used for label names:

- R-WEB
- A-HRM
- E-PROD
- L-NY

This example shows how the same naming strategy is applied for other objects in the PCE, such as IP lists, services, and label groups:

- S-SNMP (SNMP services)
- IPL-USER_SUBNETS (IP list for user subnets)
- LGE-ALL ("Label Group Environment" for all environments)

How to Create Policy

Illumio users assign four-dimensional labels to their workloads to identify their roles, applications, environments, and locations. Users specify labels in ruleset scopes and in the providers and consumers components of rules, which allows the workloads in their environments to communicate with each other. Together, labeling workloads and creating the corresponding rulesets and rules define the security policies for workloads. The PCE converts these label-based security policies into the appropriate rules for the OS-level firewalls of the workloads.

About Rulesets

Every ruleset has three main components: the scope, intra-scope rules, and extra-scope rules.

The ruleset scope is defined by an Application label, Environment label, and a Location label. It defines which workloads are impacted by the rules within the ruleset. Any workloads that have the labels specified in the ruleset scope are covered by the policy.

See the *Security Policy Guide* for more information.

All | All | All Scopes

Think carefully before creating a ruleset scope that includes all applications, all environments, and all locations (often referred to as an All | All | All scope). For example, if you created a ruleset with an All | All | All scope and added an intra-scope rule for All Workloads | All Services | All Workloads, you could inadvertently allow all traffic between all workloads on all ports on every Illumio managed workload.

Typically, the use of an All | All | All scope is mainly used for globally-consumed outbound core services. Some core services, such as vulnerability scanners, Active Directory, and backup solutions, generate a lot of outbound connections to your workloads; therefore, creating their policy with an All | All | All scope is more efficient than creating it individually in each application's ruleset.

About Rules

Within a ruleset, you add rules. Rules define the communication allowed between applications or entities impacted by the ruleset scope or between different scopes. You create rules from the provider's perspective and the PCE automatically programs the outbound rules using the labels on the consumer side of the policy. Specifying IP lists in the consumer component of a rule creates inbound (provider side) only rules.

- Intra-scope rules apply to the workloads inside the ruleset scope. They are bound by the scope on the consumer and provider side; therefore, all rules written apply only to the scope.
- Extra-scope rules apply to workloads outside the ruleset scope. The provider side of an extra-scope rule is bound to the scope.

**NOTE:**

IP Lists in rules do not affect labels and can be included in the same rule.

**IMPORTANT:**

Illumio recommends that you do not use more than one label type when including multiple labels in a rule. For example, customers often consider adding multiple Applications labels with an Environment label. However, be very cautious before creating this type of policy.

See the *Security Policy Guide* for more information.

Global Consumers

Extra-scope rules include global consumers. In an extra-scope rule, global consumers are not bound to the scope; therefore, you can use as many labels as you need in the Global Consumers section. If you do not specify a label in Global Consumers, the PCE uses "All" by default.

The Global Consumers section is the only part of the ruleset where the specified labels apply outside the ruleset scope.

Be very careful using the All Workloads object in the Global Consumer side of an extra-scope rule because the rule will impact every workload with an installed VEN in your environment.

Rule Writing Examples

In these examples, the scope specifies A-DRUPAL, E-PROD, and All Locations.

Intra-scope Ringfence Rule

Intra-scope rule 1 specifies All Workloads, All Services, and All Workloads for the providers, providing service, and consumers of the rule. This type of rule is called a ringfence rule. A ringfence rule allows all workloads within the scope to communicate with each other on all protocols. Creating an intra-scope ringfence rule eliminates the need to restrict access between workloads that have the same labels.

Adding a ringfence rule is a quick way to create policy. A ringfence rule secures communication so you only have to track traffic to your application from consumers outside the ruleset scope.

Ruleset - A-DRUPAL | E-PROD

Summary | **Scopes and Rules** | Duplicate Ruleset

Viewing draft version Up to date [View the active version.](#)

Scopes A-DRUPAL | E-PROD | All Locations

Status	Application	Environment	Location
<input type="checkbox"/>	A-DRUPAL	E-PROD	All Locations

Rules 3 Total

1 Intra-Scope Rule

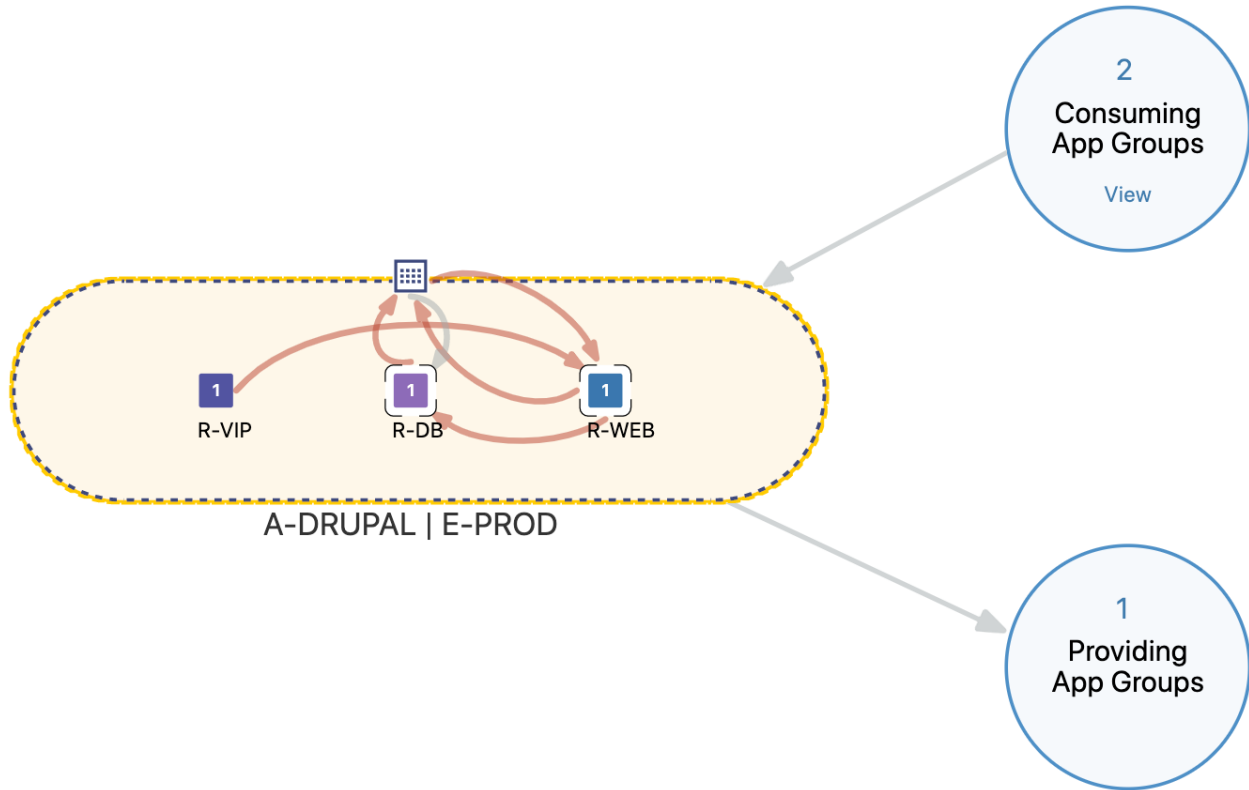
No.	Provision Status	Status	Providers	Providing Service	Consumers	Note
1	Enabled	<input checked="" type="checkbox"/>	All Workloads	All Services	All Workloads	

2 Extra-Scope Rules

No.	Provision Status	Status	Providers	Providing Service	Global Consumers	Note
1	Enabled	<input checked="" type="checkbox"/>	R-WEB	22 TCP	IPL-HOME-SN	

To visualize how an intra-scope ringfence rule works, see the same example depicted in the App Group Map.

In the App Group Map, the A-DRUPAL | E-PROD app group has a ring around it. The traffic inside the ring is the intra-scope traffic and the Consuming App Groups are the app groups connecting to the application from outside the scope.



Extra-scope Rules

The extra-scope rule below has one Application label (A-SYSTEMS) in the Global Consumers section. This rule allows inbound traffic for All Roles, All Environments, and All Locations for A-SYSTEMS to the A-DRUPAL | E-PROD environment in All Locations. Be aware that this extra-scope rule does not prevent A-SYSTEMS | E-DEV from accessing the E-PROD application.

Scopes A-DRUPAL E-PROD All Locations + - ▾							
Status	Application	Environment	Location				
<input type="checkbox"/>							
Rules + ▾ - ▾ ▾ ▾ 3 Total							
1 Intra-Scope Rule + Reorder Rules							1-1 of 1 Total
No.	Provision Status	Status	Providers	Providing Service	Consumers	Note	
1	Enabled	<input checked="" type="checkbox"/>	All Workloads	All Services	All Workloads	✎ ▾	
2 Extra-Scope Rules + Reorder Rules							1-2 of 2 Total
No.	Provision Status	Status	Providers	Providing Service	Global Consumers	Note	
1	Enabled	<input checked="" type="checkbox"/>	R-WEB	22 TCP	A-SYSTEMS	✎ ▾	

The following example shows a better way to write the extra-scope rule because it restricts inbound traffic from the R-SNAP role, the A-SYSTEMS application, and the E-PROD environment in all locations.

No.	Provision Status	Status	Providers	Providing Service	Global Consumers	Note
1	MODIFICATION PENDING	Enabled	R-WEB	22 TCP	R-SNAP E-PROD A-SYSTEMS	

The following example shows an extra-scope rule with two Application, one Role, and one Environment labels. The PCE translates this Global Consumer side rule as follows:

R-SNAP | A-HRM | E-PROD | All Locations

R-SNAP | A-SYSTEMS | E-PROD | All Locations

This rule is problematic because none of the A-HRM workloads have an R-SNAP label assigned to them; therefore, none of the A-HRM workloads are configured to access to R-WEB role for the defined ruleset scope.

If access to the R-WEB role by All Roles from either application is acceptable, simply remove the Role label. However, if you need Role-specific access, divide this rule into two rules as shown in this example:

No.	Provision Status	Status	Providers	Providing Service	Global Consumers
1	MODIFICATION PENDING	Enabled	R-WEB	22 TCP	R-SNAP A-HRM E-PROD A-SYSTEMS

Custom iptables Rules

For Linux workloads only, you can add custom iptables rules to rulesets. In the Illumio Core, these rules provide the ability to program custom iptables rules needed for your applications. Custom iptables rules help preserve any configured iptables from native Linux host configurations by allowing you to include them with the rules for your policy.

The following example shows an iptables rule that redirects incoming 2222 TCP requests to 22 TCP for the workloads defined in the Receivers section of the rule.

1 Custom iptables Rule

Provision Status	Status	Receivers	IP Version	iptables Rules applied to Scope
	Enabled	All Workloads	IPv4	-t nat -A PREROUTING -p tcp -m tcp --dport 2222 -j REDIRECT --to-ports 22

After provisioning, these rules operate on your workloads in all modes except idle mode. Your workloads do not have to be in enforcement mode for iptables rules to operate.

See the *Security Policy Guide* for more information.

Rule Search

By default, Rule Search shows you all the draft rules in the PCE.

The screenshot shows the Rule Search interface with the following table of results:

Providers	Providing Service	Consumers	Extra	Ruleset	Note
All Workloads	All Services	All Workloads		A-DRUPAL E-PROD	
Any (0.0.0.0 and ::0)	ICMP ICMP, ICMPv6	All Workloads		Default	
All Workloads	All Services	All Workloads		A-DRUPAL E-DEV	
All Workloads	ICMP ICMP, ICMPv6	Any (0.0.0.0 and ::0)		Default	
All Workloads	All Services	All Workloads		A-SYSTEMS E-DEV L-NY	

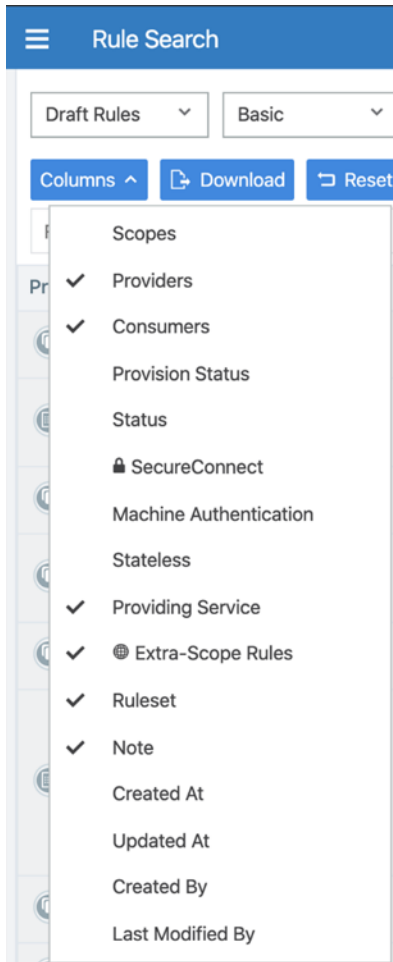
You can use Rule Search to find rules assigned to any object type. From the **Filter by Labels and Rule attributes** drop-down list, select the object types that you want to restrict your search to. To download your search query, click the **Download** button.

The following example shows how to search for rules that include port 22 TCP. The search returns results for all draft rules.

The screenshot shows the Rule Search interface with the search filter 'Port: 22 TCP' applied. The table of results is as follows:

Providers	Providing Service	Consumers	Extra	Ruleset
R-WEB	22 TCP	IPL-HOME-SN	Extra	A-DRUPAL E-PROD

To add columns so that you can view more rule details, click the **Columns** button:



See the *Security Policy Guide* for more information.