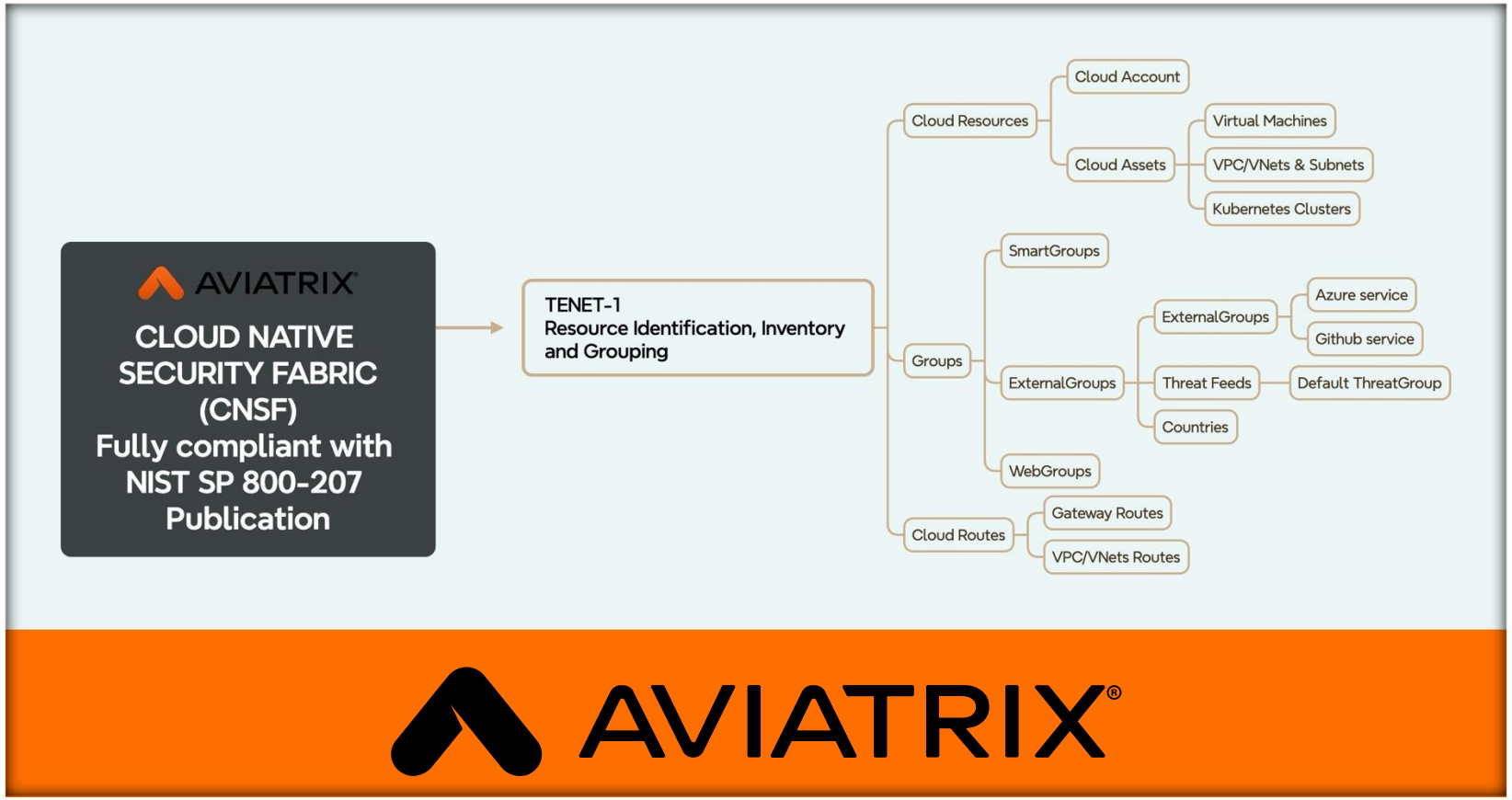
Tenet-1: Resource Identification, Inventory and Grouping

Topics Covered

Tenet from NIST Publication 800-207 - Zero Trust Architecture (ZTA)

The enterprise collects as much information as possible about the current state of assets, network infrastructure and communications and uses it to improve its security posture.

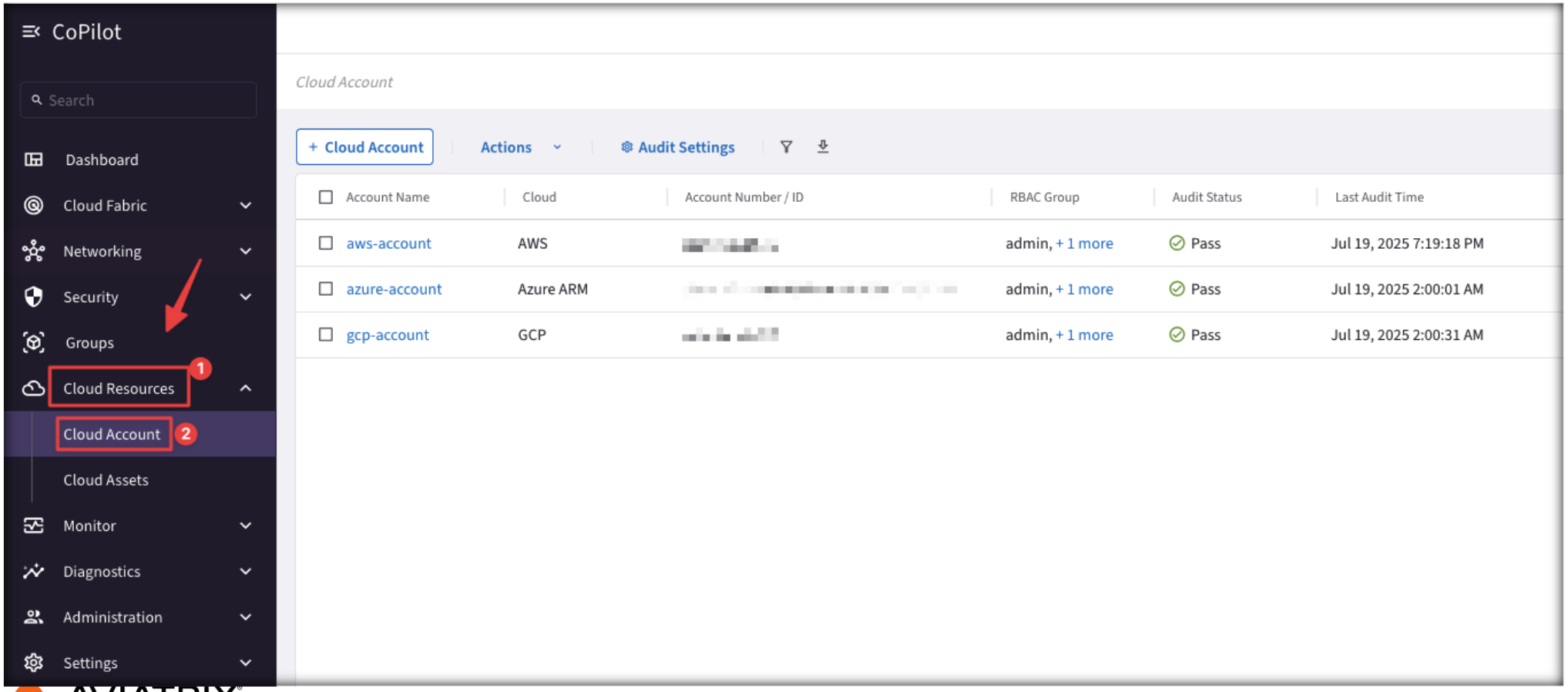


Cloud Resources

Cloud Resources – Cloud Account (part.1)

PATH: *CoPilot > Cloud Resources > Cloud Account*

This section allows you to onboard cloud service provider (CSP) accounts or subscriptions and facilitates the automatic discovery of the existing underlay infrastructure. This includes details such as VPCs/VNets, subnets, routing tables, virtual machines, and Kubernetes clusters, providing a comprehensive overview of your network environment.

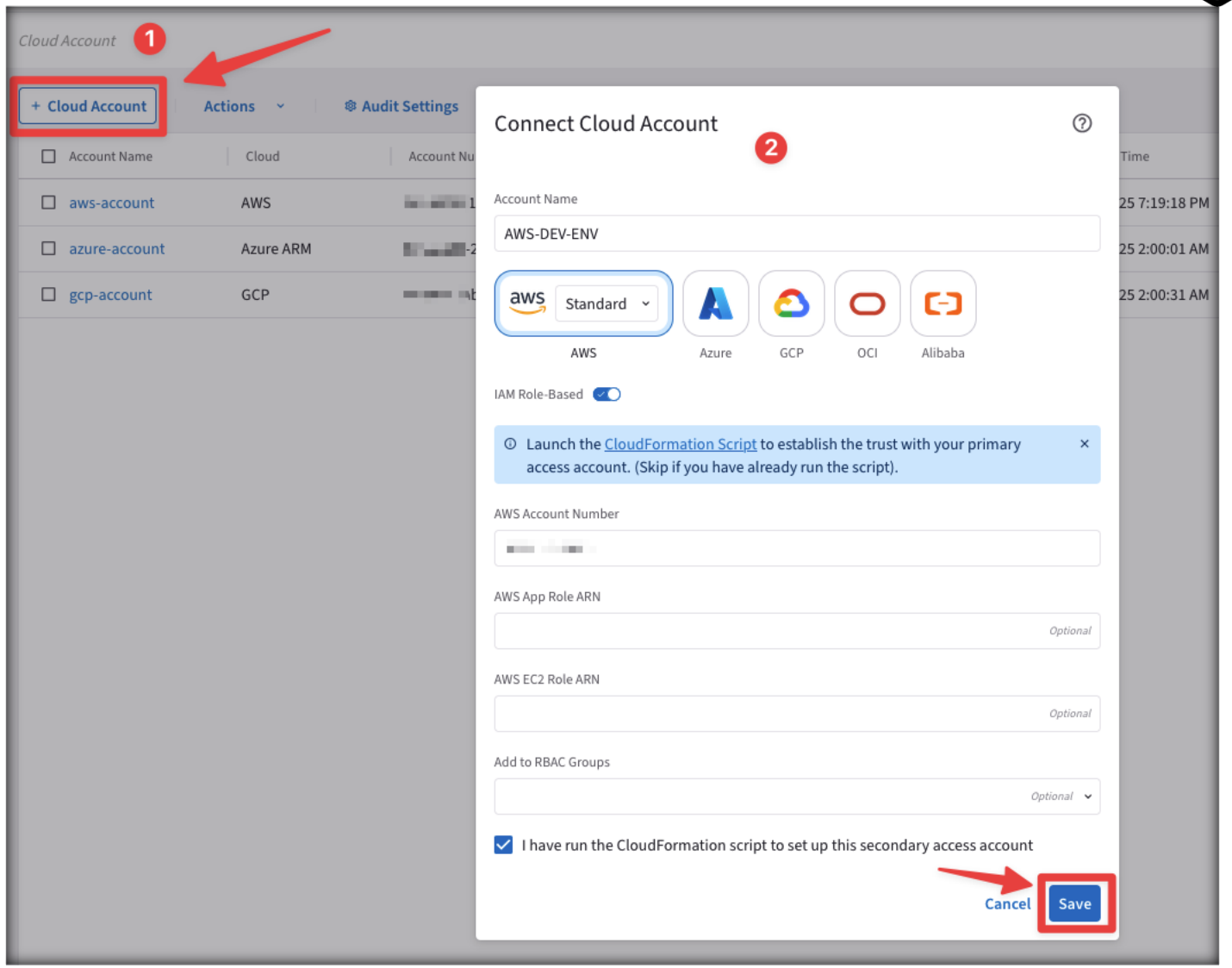


Cloud Resources – Cloud Account (part.2)

Connecting a Cloud Account:

- Click on "***+ Cloud Account***"
- Fill in the required parameters in the provided table.

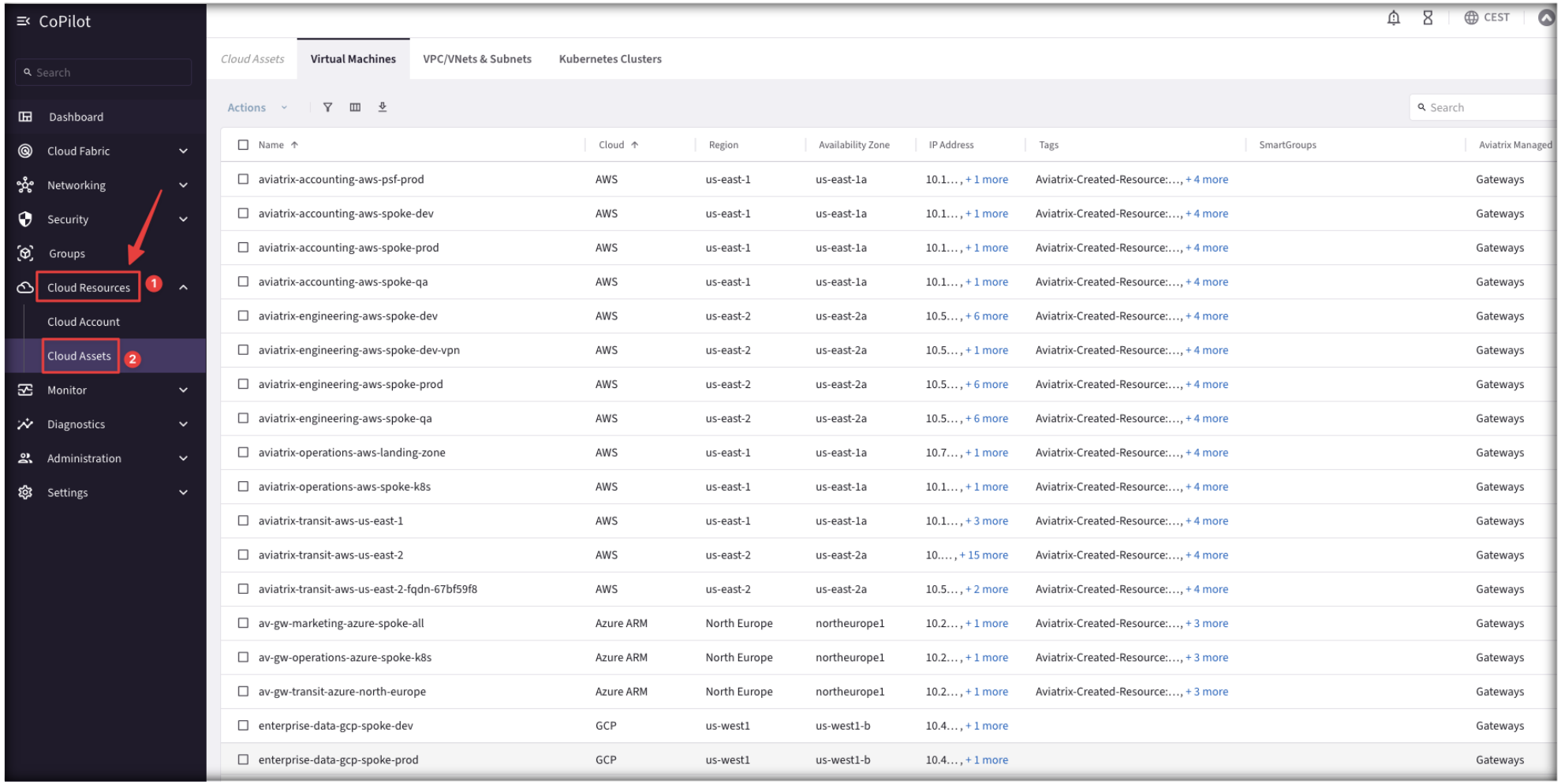
- After onboarding a cloud account, you can:
  - Edit settings by clicking the Edit icon on the account's row.
  - Audit the account via the Actions or the ellipsis menu.
  - Update the IAM policy for AWS accounts through the Actions menu.



Cloud Resources – Cloud Assets (part.1)

PATH: *CoPilot > Cloud Resources > Cloud Assets*

This section offers full visibility into the cloud environment, including instances, Kubernetes clusters, VPCs, and subnets.



Name	Cloud	Region	Availability Zone	IP Address	Tags	SmartGroups	Aviatrix Managed
aviatrix-accounting-aws-psf-prod	AWS	us-east-1	us-east-1a	10.1..., + 1 more	Aviatrix-Created-Resource:..., + 4 more		Gateways
aviatrix-accounting-aws-spoke-dev	AWS	us-east-1	us-east-1a	10.1..., + 1 more	Aviatrix-Created-Resource:..., + 4 more		Gateways
aviatrix-accounting-aws-spoke-prod	AWS	us-east-1	us-east-1a	10.1..., + 1 more	Aviatrix-Created-Resource:..., + 4 more		Gateways
aviatrix-accounting-aws-spoke-qa	AWS	us-east-1	us-east-1a	10.1..., + 1 more	Aviatrix-Created-Resource:..., + 4 more		Gateways
aviatrix-engineering-aws-spoke-dev	AWS	us-east-2	us-east-2a	10.5..., + 6 more	Aviatrix-Created-Resource:..., + 4 more		Gateways
aviatrix-engineering-aws-spoke-dev-vpn	AWS	us-east-2	us-east-2a	10.5..., + 1 more	Aviatrix-Created-Resource:..., + 4 more		Gateways
aviatrix-engineering-aws-spoke-prod	AWS	us-east-2	us-east-2a	10.5..., + 6 more	Aviatrix-Created-Resource:..., + 4 more		Gateways
aviatrix-engineering-aws-spoke-qa	AWS	us-east-2	us-east-2a	10.5..., + 6 more	Aviatrix-Created-Resource:..., + 4 more		Gateways
aviatrix-operations-aws-landing-zone	AWS	us-east-1	us-east-1a	10.7..., + 1 more	Aviatrix-Created-Resource:..., + 4 more		Gateways
aviatrix-operations-aws-spoke-k8s	AWS	us-east-1	us-east-1a	10.1..., + 1 more	Aviatrix-Created-Resource:..., + 4 more		Gateways
aviatrix-transit-aws-us-east-1	AWS	us-east-1	us-east-1a	10.1..., + 3 more	Aviatrix-Created-Resource:..., + 4 more		Gateways
aviatrix-transit-aws-us-east-2	AWS	us-east-2	us-east-2a	10...., + 15 more	Aviatrix-Created-Resource:..., + 4 more		Gateways
aviatrix-transit-aws-us-east-2-fqdn-67bf59f8	AWS	us-east-2	us-east-2a	10.5..., + 2 more	Aviatrix-Created-Resource:..., + 4 more		Gateways
av-gw-marketing-azure-spoke-all	Azure ARM	North Europe	northeurope1	10.2..., + 1 more	Aviatrix-Created-Resource:..., + 3 more		Gateways
av-gw-operations-azure-spoke-k8s	Azure ARM	North Europe	northeurope1	10.2..., + 1 more	Aviatrix-Created-Resource:..., + 3 more		Gateways
av-gw-transit-azure-north-europe	Azure ARM	North Europe	northeurope1	10.2..., + 1 more	Aviatrix-Created-Resource:..., + 3 more		Gateways
enterprise-data-gcp-spoke-dev	GCP	us-west1	us-west1-b	10.4..., + 1 more			Gateways
enterprise-data-gcp-spoke-prod	GCP	us-west1	us-west1-b	10.4..., + 1 more			Gateways

Cloud Resources – Cloud Assets (part.2)

PATH: *CoPilot > Cloud Resources > Cloud Assets >* ***Virtual Machines***

Complete visibility of all virtual machines across the entire multicloud environment.

Cloud Assets | **Virtual Machines** | VPC/VNets & Subnets | Kubernetes Clusters

Actions | Search

Name	Cloud	Region	Availability Zone	IP Address	Tags	SmartGroups	Aviatrix Managed
aviatrix-engineering-aws-spoke-qa	AWS	us-east-2	us-east-2a	10.5..., + 6 more	Aviatrix-Created-Resource:..., + 4 more		Gateways
aviatrix-operations-aws-landing-zone	AWS	us-east-1	us-east-1a	10.7..., + 1 more	Aviatrix-Created-Resource:..., + 4 more		Gateways
aviatrix-operations-aws-spoke-k8s	AWS	us-east-1	us-east-1a	10.1..., + 1 more	Aviatrix-Created-Resource:..., + 4 more		Gateways
aviatrix-transit-aws-us-east-1	AWS	us-east-1	us-east-1a	10.1..., + 3 more	Aviatrix-Created-Resource:..., + 4 more		Gateways
aviatrix-transit-aws-us-east-2	AWS	us-east-2	us-east-2a	10...., + 15 more	Aviatrix-Created-Resource:..., + 4 more		Gateways
aviatrix-transit-aws-us-east-2-fqdn-67bf59f8	AWS	us-east-2	us-east-2a	10.5..., + 2 more	Aviatrix-Created-Resource:..., + 4 more		Gateways
accounting-app-prod	AWS	us-east-1	us-east-1a	10.1.4.10	Application: crm, + 9 more	app, crm-app, crm-dev-web, + 5 more	Yes
accounting-app-qa	AWS	us-east-1	us-east-1a	10.1.3.10	Application: crm, + 9 more	Accenture_Demo, app, + 7 more	Yes
accounting-web-dev	AWS	us-east-1	us-east-1a	10.1.2.10	Application: crm, + 9 more	Accenture_Demo, crm-app, + 6 more	Yes
appiq-example-destination	AWS	us-east-1	us-east-1a	10.1.2.5	Application: appiq, + 9 more	app, crm-prod, crm-qa-app, + 2 more	Yes
engineering-app-prod	AWS	us-east-2	us-east-2a	10.5.4.10	Application: engineering app, + 9 more	App-Frontend, Huss-App-FE, + 6 more	Yes
engineering-app-qa	AWS	us-east-2	us-east-2a	10.5.3.10	Application: engineering app, + 9 more	Accenture_Demo, + 7 more	Yes
engineering-web-dev	AWS	us-east-2	us-east-2a	10.5.2.10	Application: engineering app, + 9 more	Accenture_Demo, + 6 more	Yes
ng_1	AWS	us-east-1	us-east-1a	10...., + 19 more	Name: ng_1, + 10 more		Yes
transit-aws-us-east-1-az1-fw1@172.64.1.114	AWS	us-east-1	us-east-1a	10.1..., + 4 more	Aviatrix-Created-Resource:..., + 1 more		Yes
AviatrixController-migrated-2025-05-23T02-51-28	AWS	us-west-2	us-west-2a	172...., + 1 more	Aviatrix-Created-Resource:..., + 8 more		No
AviatrixCoPilot	AWS	us-west-2	us-west-2a	172...., + 1 more	Name: AviatrixCoPilot, + 4 more		No
grafana-demo	AWS	us-west-2	us-west-2a	172...., + 1 more	Department: 550 Solution... , + 6 more		No

A VM can be marked as *Aviatrix managed* where:

- **Aviatrix managed = Yes** Indicates the VM is behind an Aviatrix Gateway; that is, it exists in a VPC/VNet where an Aviatrix gateway is deployed.
- **Aviatrix managed = No** Indicates the VM exists in a VPC/VNet where no Aviatrix gateways exist.
- **Aviatrix managed = Gateways** Indicates the VM exists in an Aviatrix Gateway (Transit, Spoke, or Specialty/Other)

Cloud Resources – Cloud Assets (part.3)

PATH: *CoPilot > Cloud Resources > Cloud Assets >* ***VPC/Vnets & Subnets***

Full visibility of all VPCs and their associated subnets.

Cloud Assets | Virtual Machines | VPC/VNets & Subnets | Kubernetes Clusters

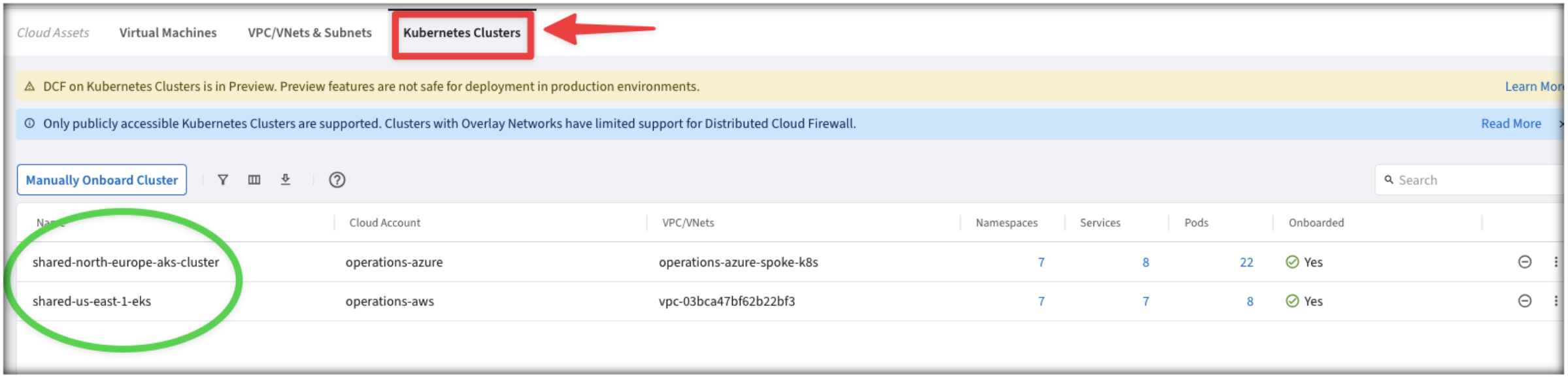
+ VPC/VNet | Actions | Search

Name	Cloud	Region	Availability Zones	IP Address CIDR	VMs	Cloud Tags	SmartGroups	Aviatrix Managed
accounting-aws-spoke-dev	AWS	us-east-1	us-e… , + 1 more	10.1.2.0/24	appi… , + 1 more	Aviat…, + 1 more		Yes
accounting-aws-spoke-dev-Private-1-us-east-1a	AWS	us-east-1	us-east-1a	10.1.2.0/28		Aviat…, + 2 more		Yes
accounting-aws-spoke-dev-Private-2-us-east-1b	AWS	us-east-1	us-east-1b	10.1.2.16…		Aviat…, + 2 more		Yes
accounting-aws-spoke-dev-Public-1-us-east-1a	AWS	us-east-1	us-east-1a	10.1.2.32…		Aviat…, + 2 more		Yes
accounting-aws-spoke-dev-Public-2-us-east-1b	AWS	us-east-1	us-east-1b	10.1.2.48…		Aviat…, + 2 more		Yes
accounting-aws-spoke-prod	AWS	us-east-1	us-e… , + 1 more	10.1.4.0/24	accounting-ap…	Aviat…, + 1 more		Yes
accounting-aws-spoke-qa	AWS	us-east-1	us-e… , + 1 more	10.1.3.0/24	accounting-ap…	Aviat…, + 1 more		Yes
engineering-aws-spoke-dev	AWS	us-east-2	us-e… , + 1 more	10.5.2.0/24	engineering-w…	Aviat…, + 1 more		Yes
engineering-aws-spoke-prod	AWS	us-east-2	us-e… , + 1 more	10.5.4.0/24	engineering-a…	Aviat…, + 1 more		Yes
engineering-aws-spoke-qa	AWS	us-east-2	us-e… , + 1 more	10.5.3.0/24	engineering-a…	Aviat…, + 1 more		Yes
example-aws-spoke-vpc	AWS	us-east-1	us-e… , + 5 more	10.101.1.…		Aviat…, + 1 more		Yes
example-aws-transit-vpc	AWS	us-east-1	us-e… , + 1 more	10.102.0.…		Aviat…, + 1 more		Yes
operations-aws-landing-zone	AWS	us-east-1	us-e… , + 1 more	10.7.2.0/24		Aviat…, + 1 more		Yes
operations-aws-spoke-k8s	AWS	us-east-1	us-e… , + 1 more	10.1.5.0/24	ng_1	Aviat…, + 1 more		Yes
transit-aws-us-east-1	AWS	us-east-1	us-e… , + 1 more	10.1.0.0/23	transit-aws-us…	Aviat…, + 1 more		Yes
transit-aws-us-east-2	AWS	us-east-2	us-e… , + 1 more	10.5.0.0/23		Aviat…, + 1 more		Yes
example-azure-spoke-vnet	Azure ARM	East US	eastus	10.108.1.…		Aviat…, + 1 more		Yes
example-azure-transit-vnet	Azure ARM	East US	eastus	10.109.0.…		Aviat…, + 1 more		Yes

Cloud Resources – Cloud Assets (part.4)

PATH: *CoPilot > Cloud Resources > Cloud Assets >* ***Kubernetes Clusters***

Full visibility of all clusters of Kubernetes containers.



CAVEAT: On the *Groups > Settings* tab, enable the Discovery of Kubernetes Resources feature. This allows for discovery of Kubernetes clusters in your cloud accounts.

Groups

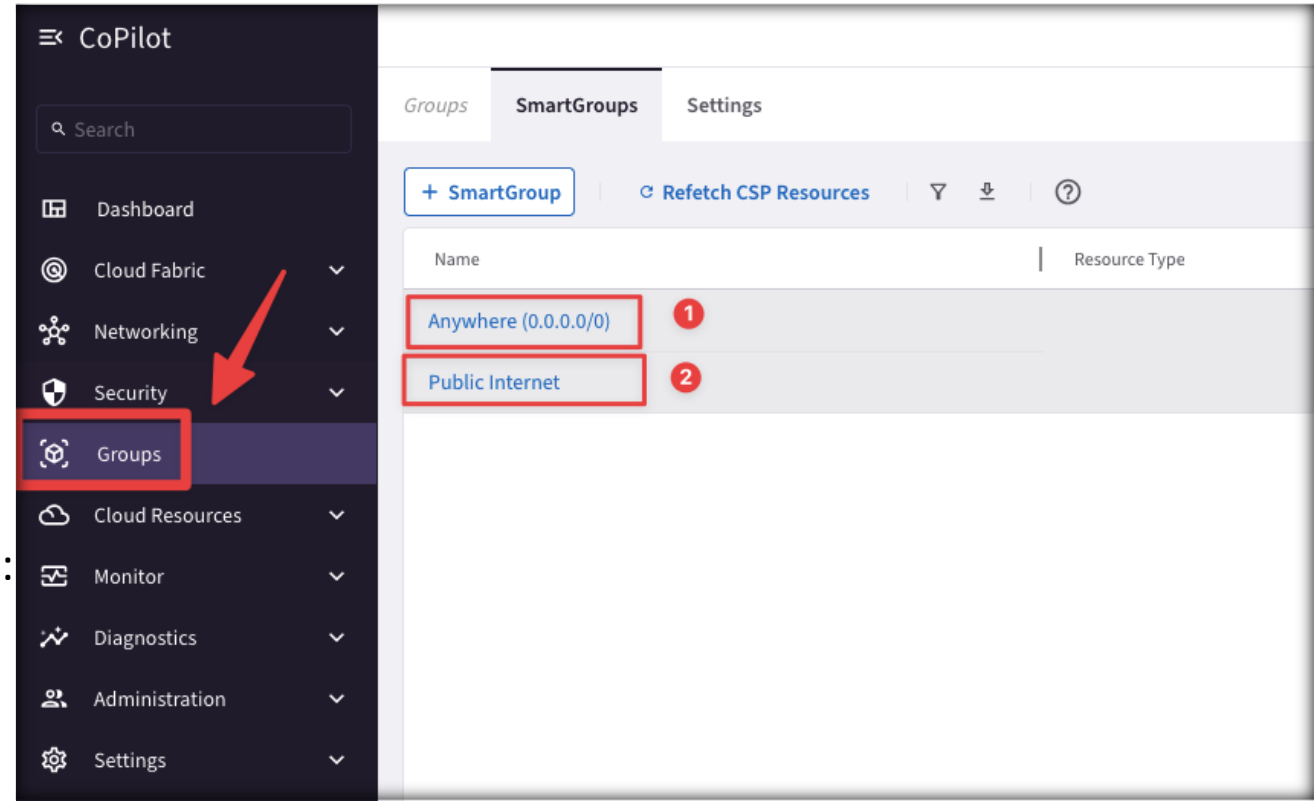
Groups

- In CoPilot, **GROUPS** are versatile constructs for organizing and managing Aviatrix resources across multicloud environments. They enable logical grouping of resources by subscription, cloud account, region, or VPC/VNet, supporting various organizational structures.

CAVEAT: Only the SmartGroups tab is visible before enabling the Distributed Cloud Firewall.

- CoPilot includes two default **system-defined SmartGroups**:
  - **Anywhere (0.0.0.0/0):** Represents all IP addresses and CIDR ranges.
  - **Public Internet:** Covers non-RFC 1918 IP ranges, i.e., public Internet addresses.

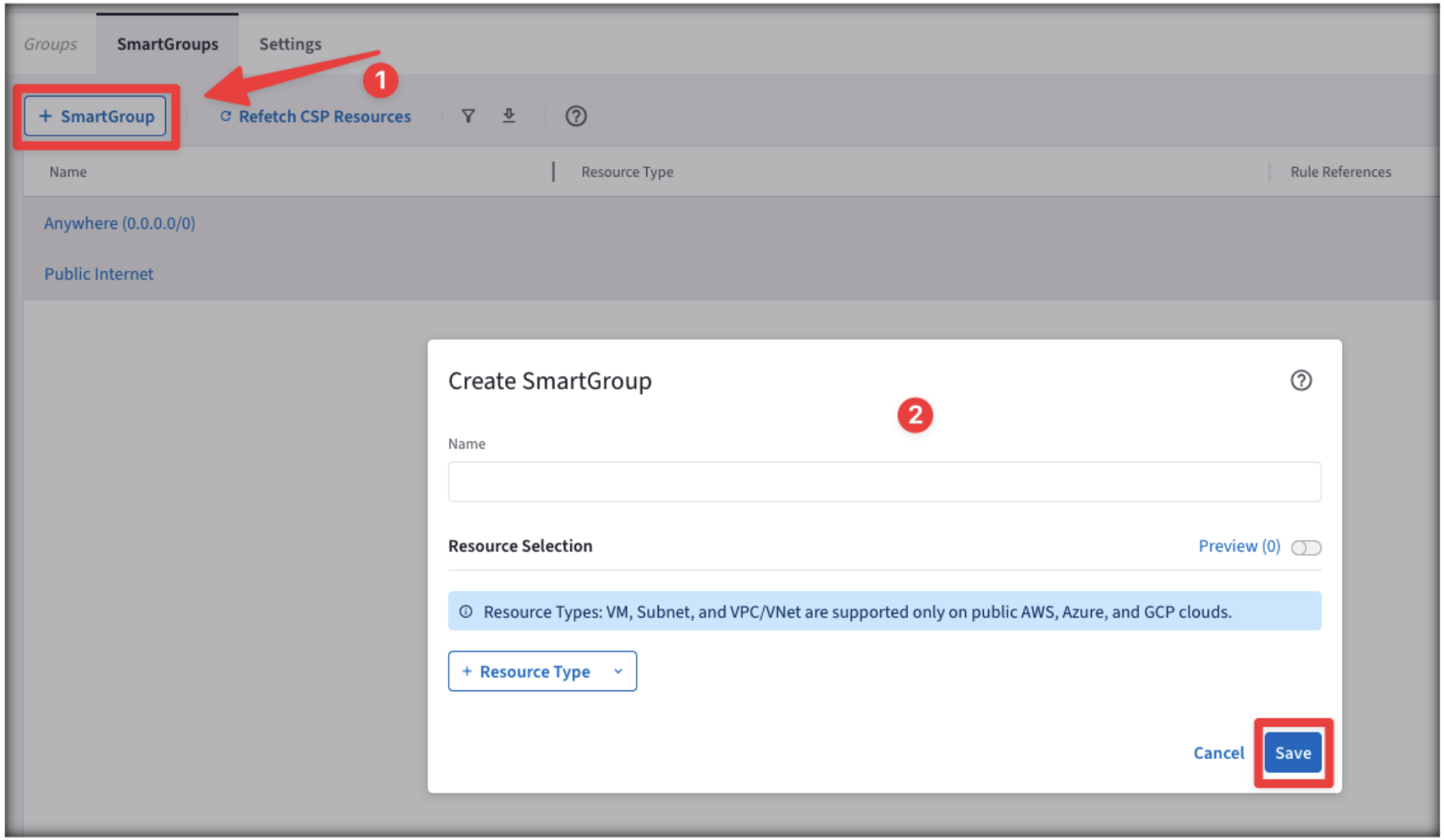
CAVEAT: These system-defined SmartGroups cannot be deleted.



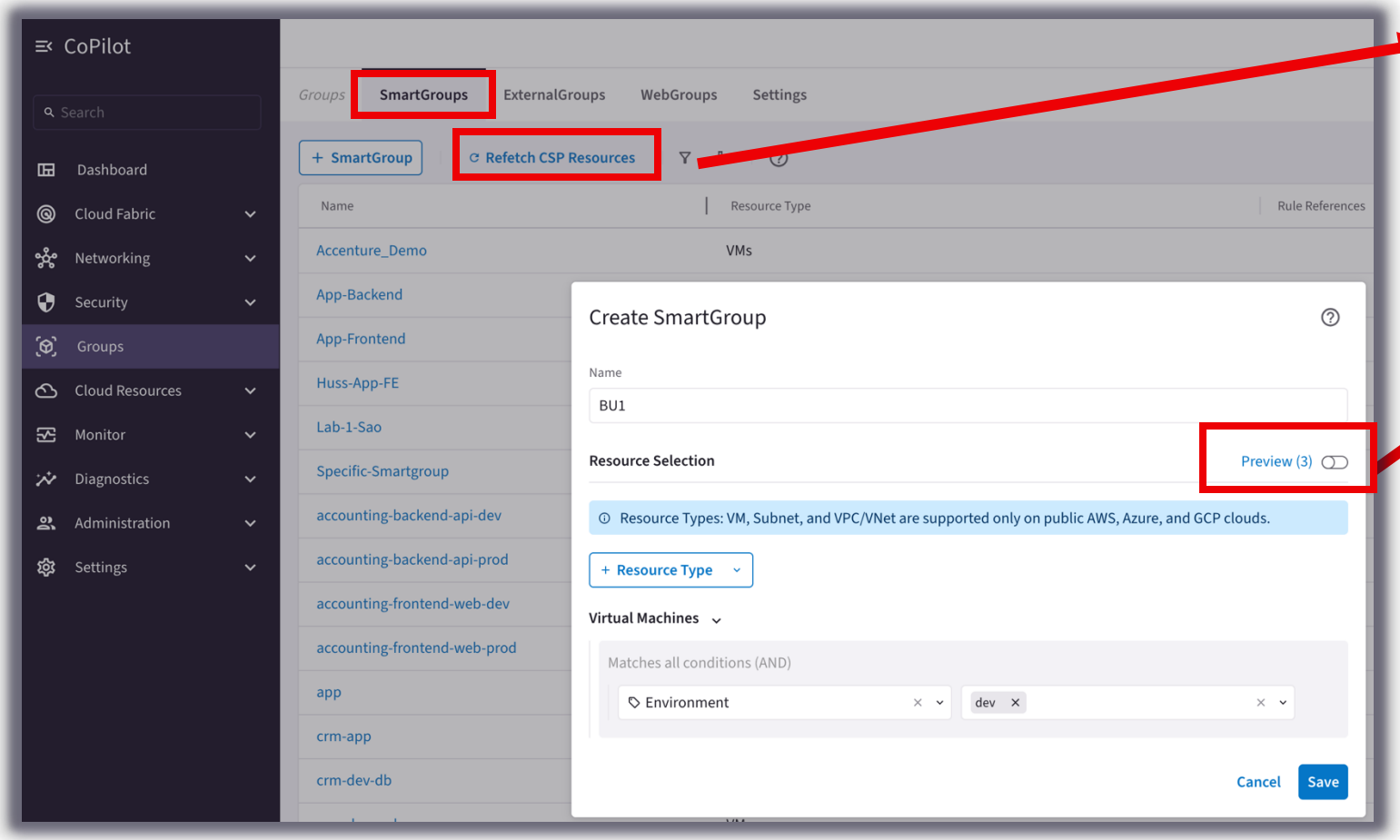
Purpose of the SmartGroup: To identify the L3 information required for the Distributed Cloud Firewall rule. You can configure policies to filter traffic between applications residing in the SmartGroups.

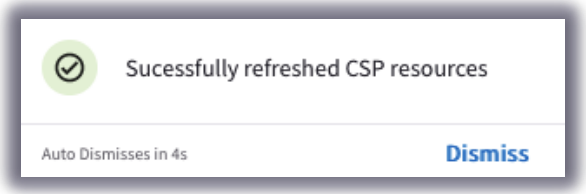
Groups – SmartGroups (part.1)

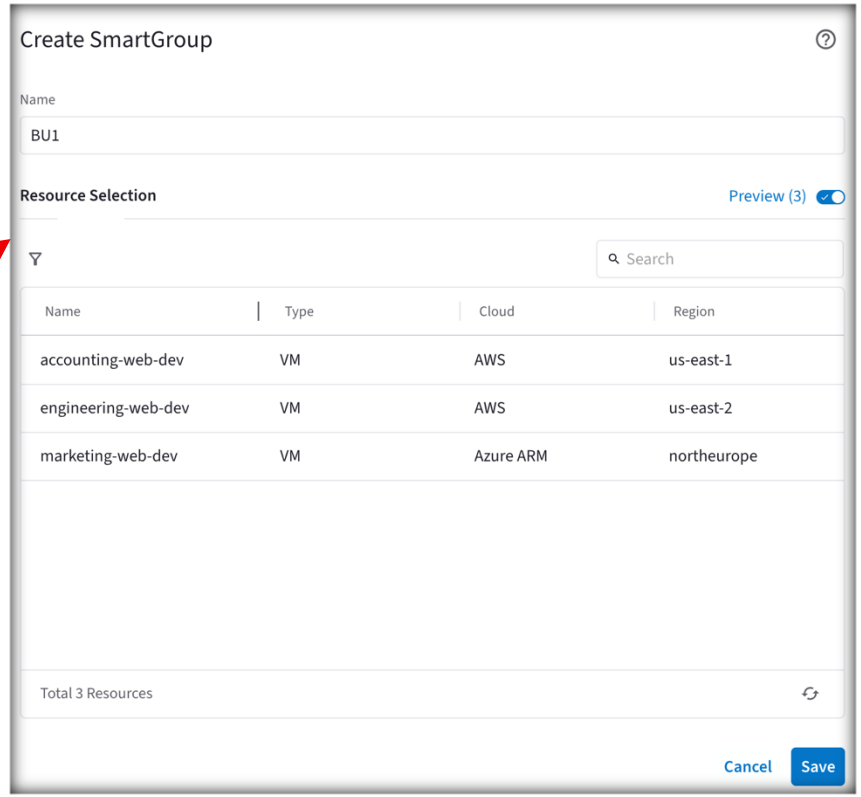
- A SmartGroup is a logical grouping used by the Aviatrix Distributed Cloud Firewall to filter traffic between applications within the group.



Groups – SmartGroups (part.2)





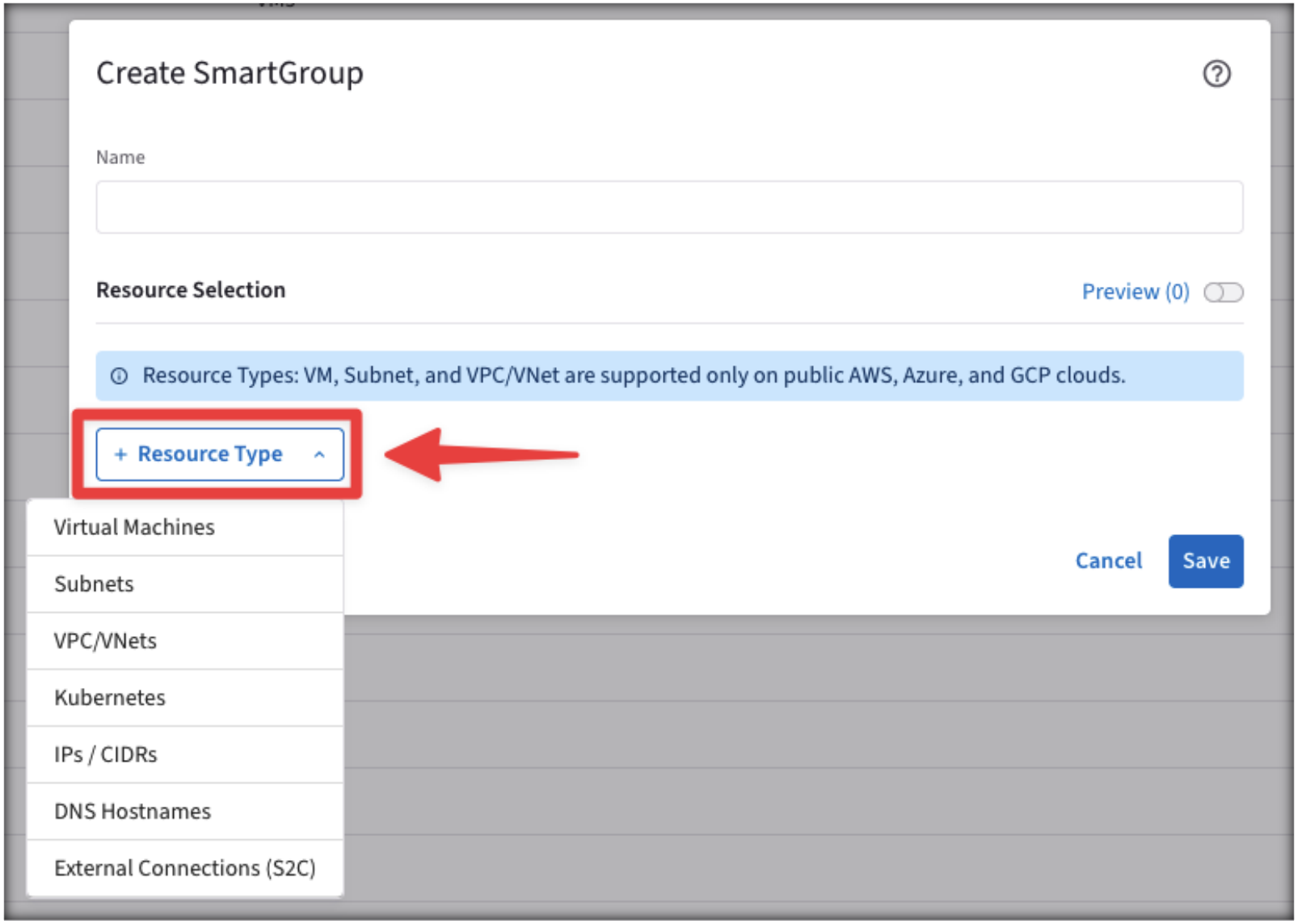


- Controller polls the CSPs to retrieve inventory (about VPCs, instances etc.) every **15 minutes** (can be modified)
- CoPilot queries Controller every **1 hour** (can be modified)
- On-demand refresh of tags is available

Groups – SmartGroups (part.3)

- A SmartGroup can be defined based on **7 Resource Types**:

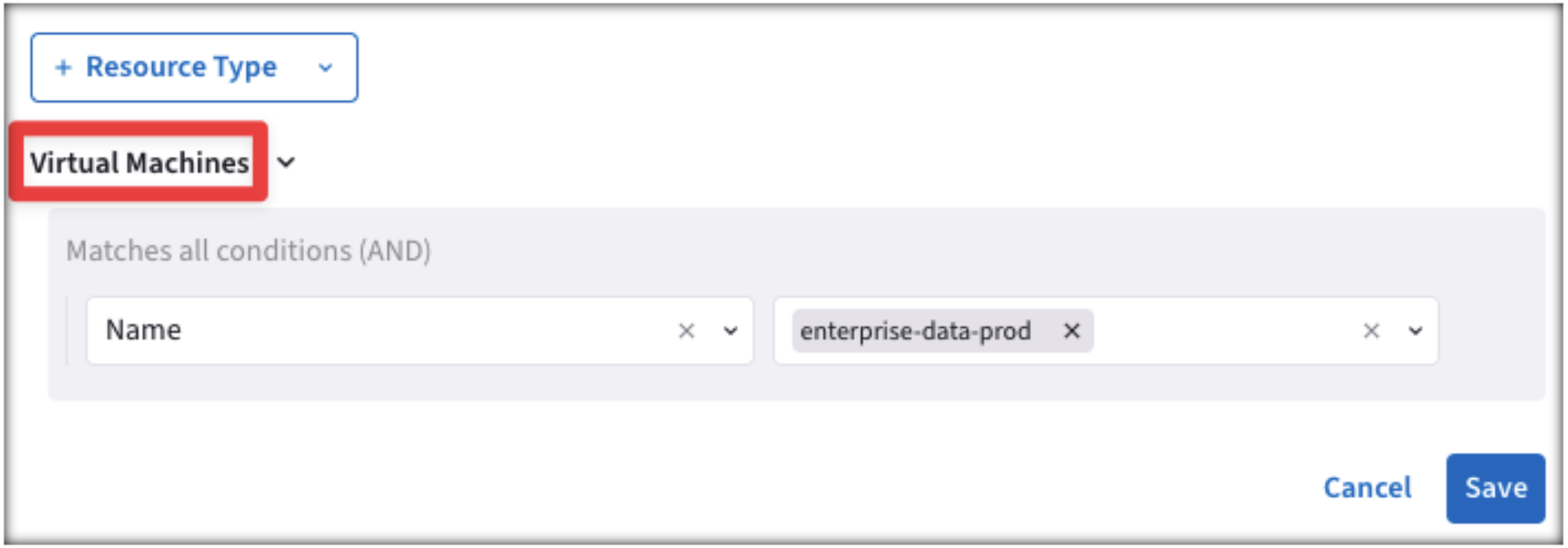
1) Virtual Machines
2) Subnets
3) VPC/Vnets
4) Kubernetes
5) IPs / CIDRs
6) DNS Hostnames
7) External Connections (S2C)



Groups – SmartGroups (part.4)

- A SmartGroup can be defined based on **7 Resource Types**:

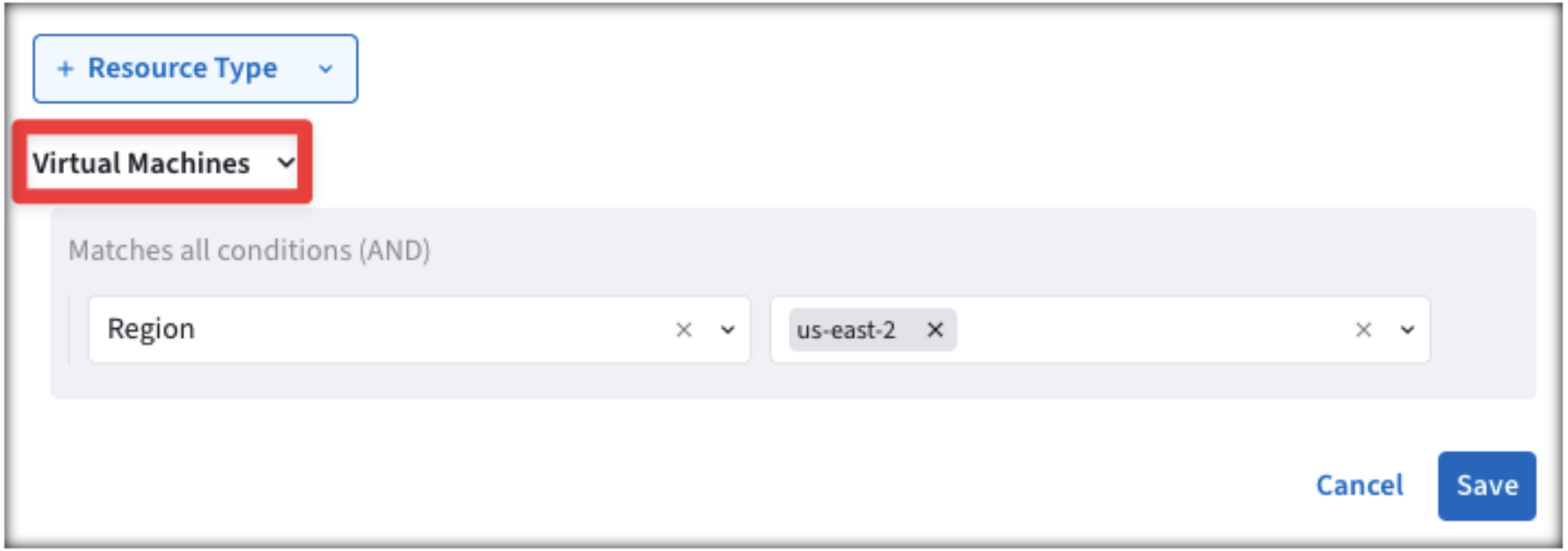
1) Virtual Machine:
   - **Name → symbolic name of the interested instance**



Groups – SmartGroups (part.5)

- A SmartGroup can be defined based on **7 Resource Types**:

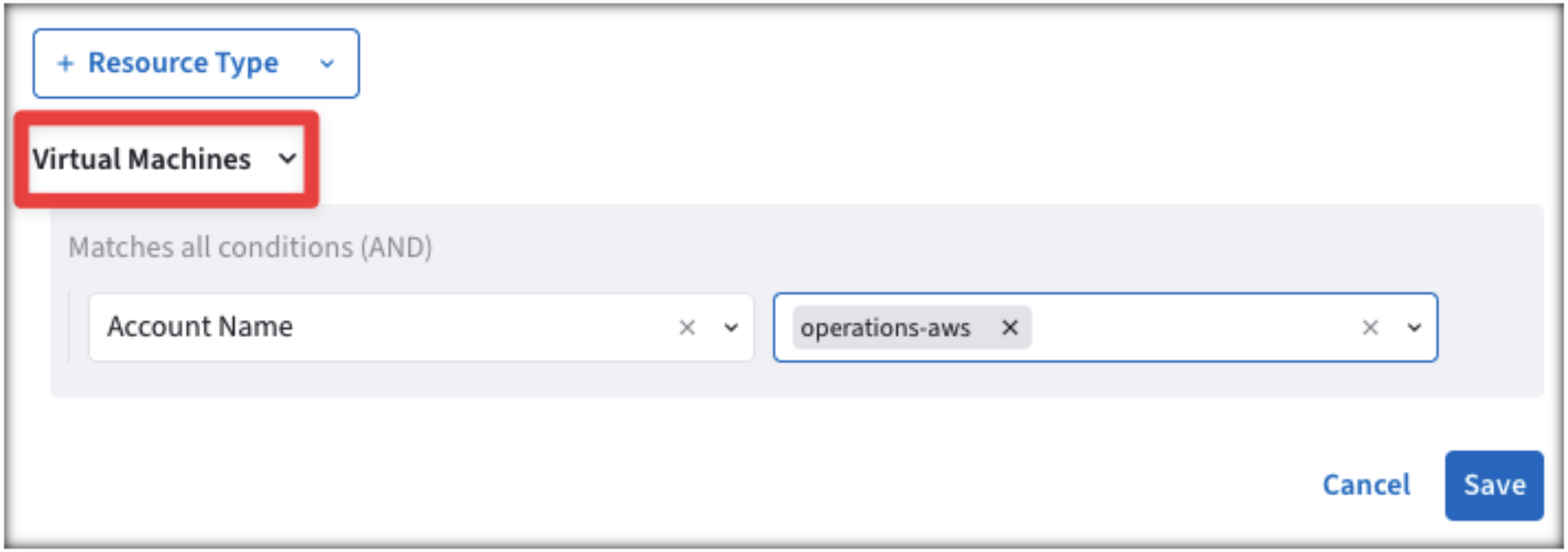
1) Virtual Machine:
   - **Region → region's identifier**



Groups – SmartGroups (part.6)

- A SmartGroup can be defined based on **7 Resource Types**:

1) Virtual Machine:
   - **Account Name → The name of your account or subscription**



Groups – SmartGroups (part.7)

- A SmartGroup can be defined based on **7 Resource Types**:

1) Virtual Machine:
   - **CSP Tag → Value**

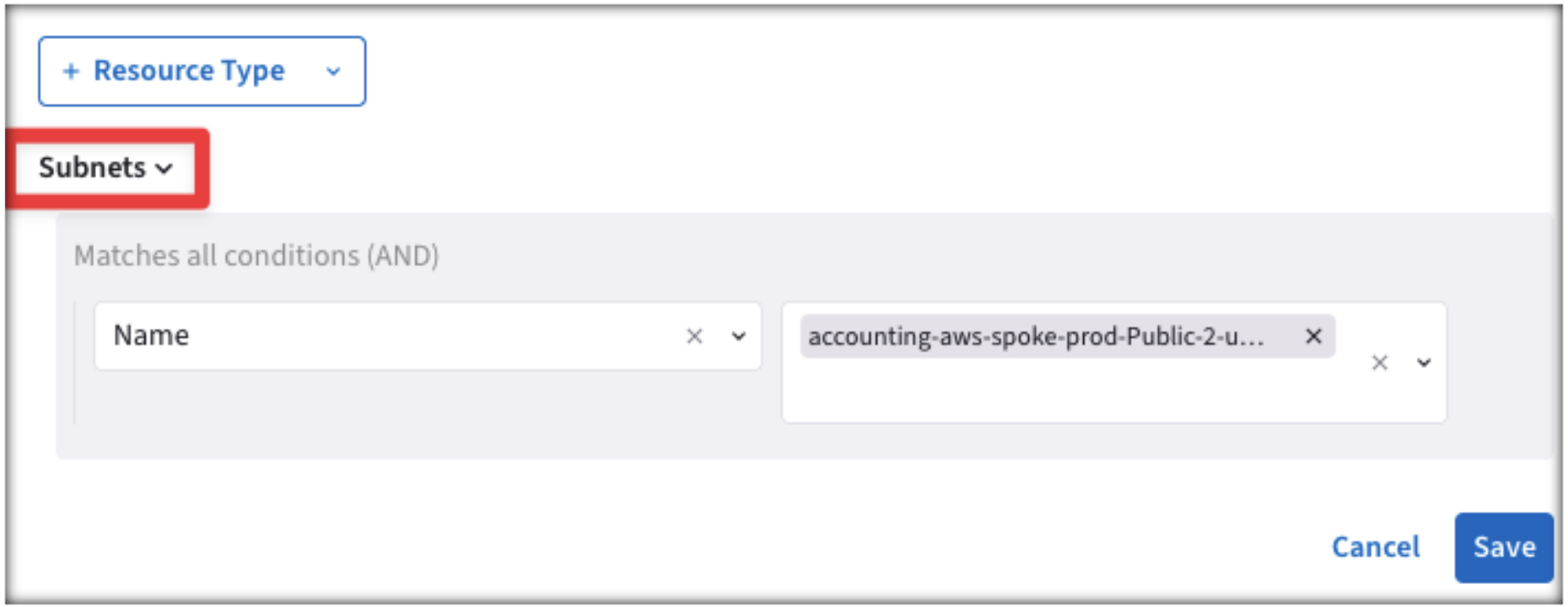
Recommended method

Groups – SmartGroups (part.8)

- A SmartGroup can be defined based on **7 Resource Types**:

2) Subnets:

   - **Name → subnet's name**



Groups – SmartGroups (part.9)

- A SmartGroup can be defined based on **7 Resource Types**:

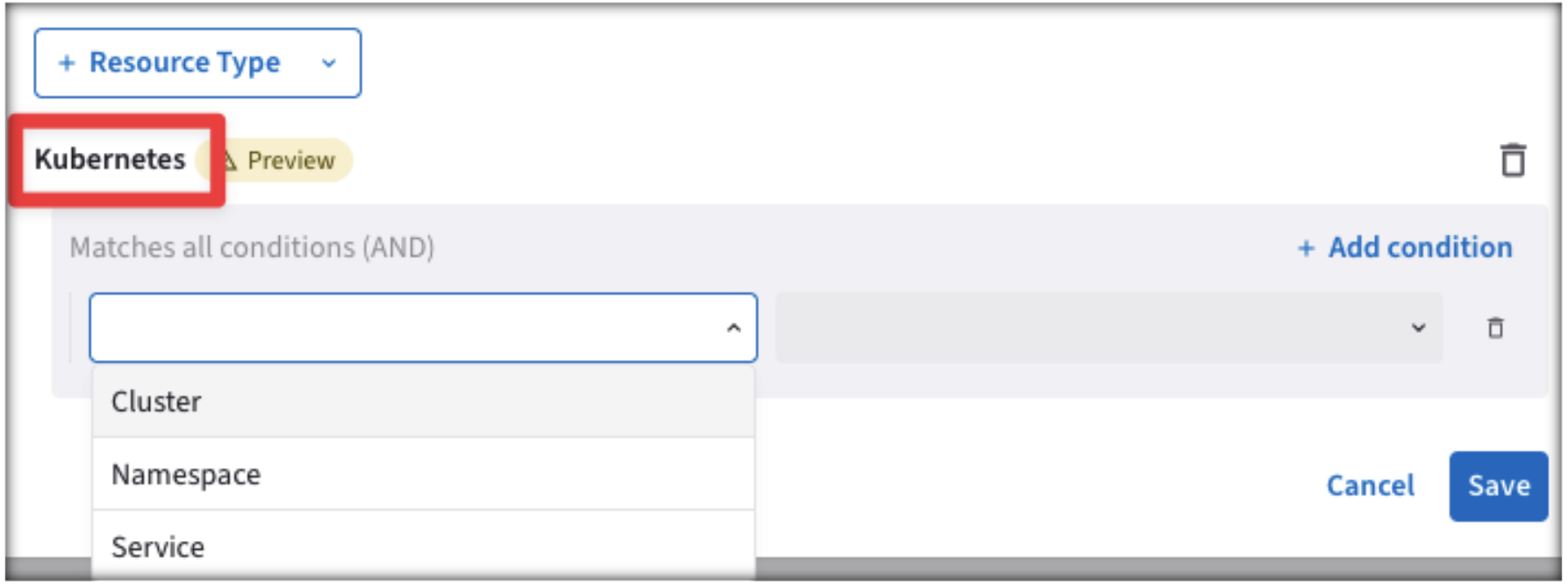
3) VPC/VNets:

- **Name → VPC's name**

Groups – SmartGroups (part.10)

- A SmartGroup can be defined based on **7 Resource Types**:

4) Kubernetes:
   - **Cluster**
   - **Namespace**
   - **Service**



Groups – SmartGroups (part.11)

- A SmartGroup can be defined based on **7 Resource Types**:

5) IPs / CIDRS:

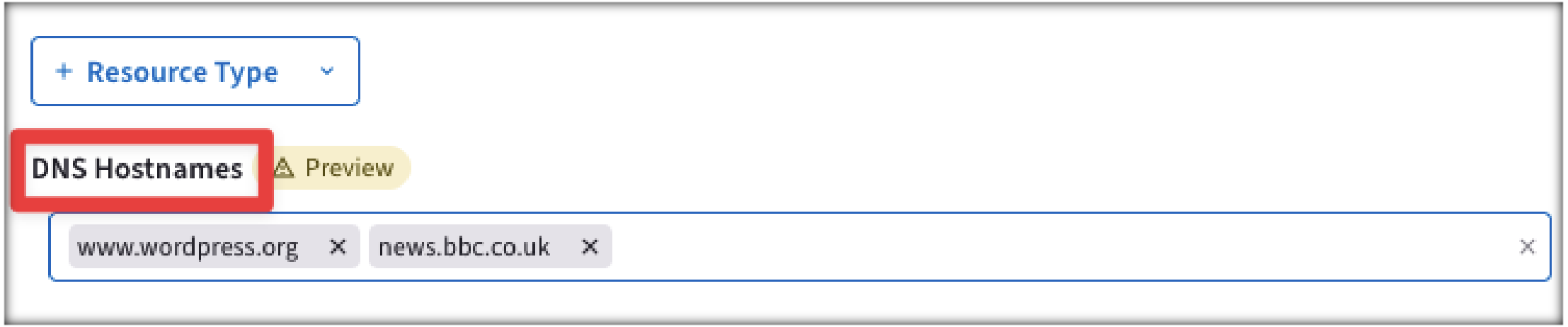
   - **For resources that are not tagged, you can directly specify IP addresses or CIDRs**

Groups – SmartGroups (part.12)

- A SmartGroup can be defined based on **7 Resource Types**:

6) DNS Hostnames:
   - **Enter Fully Qualified Domain Names**

CAVEAT: Ensure that the DNS server you want to use for resolving hostnames is selected on the DNS Server for Hostname Resolution card under *Groups > Settings*.



Groups – SmartGroups (part.13)

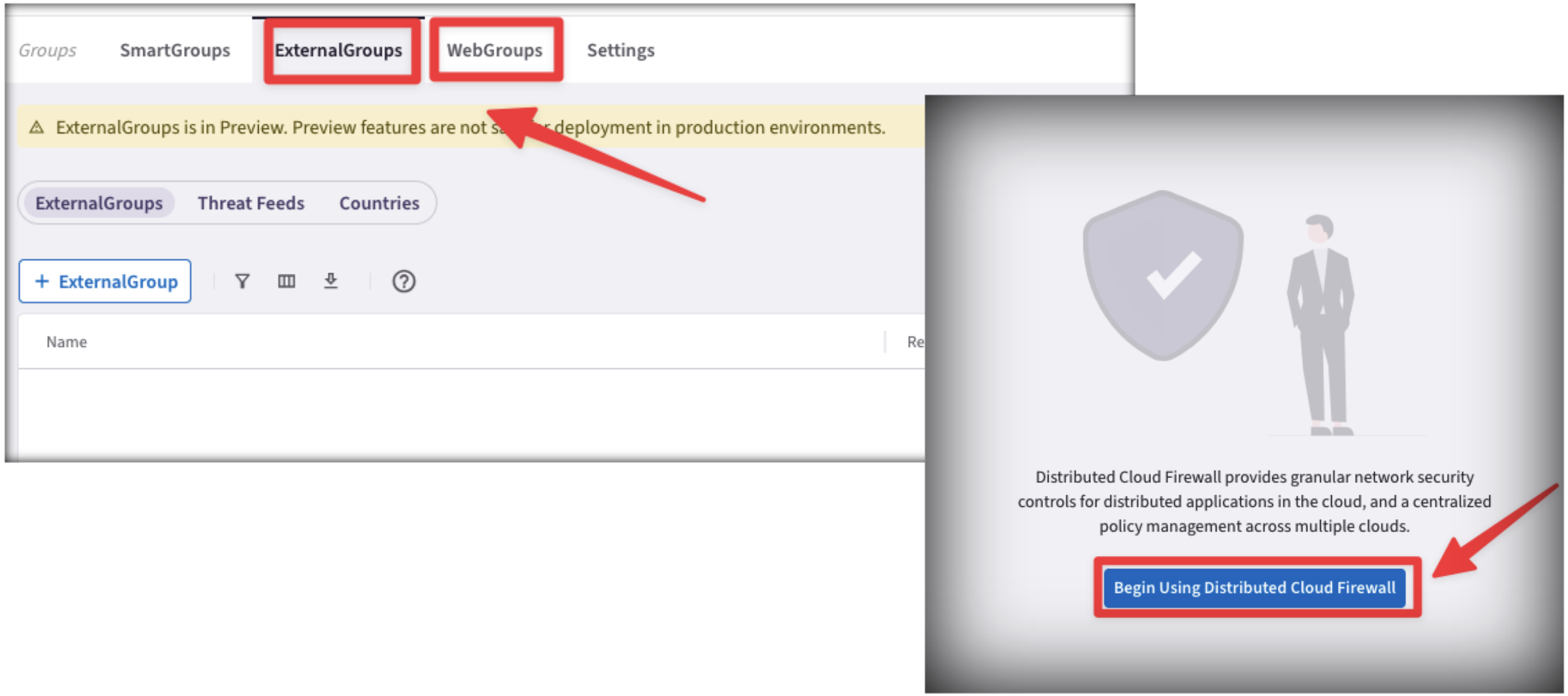
- A SmartGroup can be defined based on **7 Resource Types**:

7) External Connections (S2C):

   - **Select pre-existing external connection. An External Connection SmartGroup will resolve to either the remote CIDRs defined for a static route external connection, or the BGP-advertised CIDRs for BGP-based external connections.**

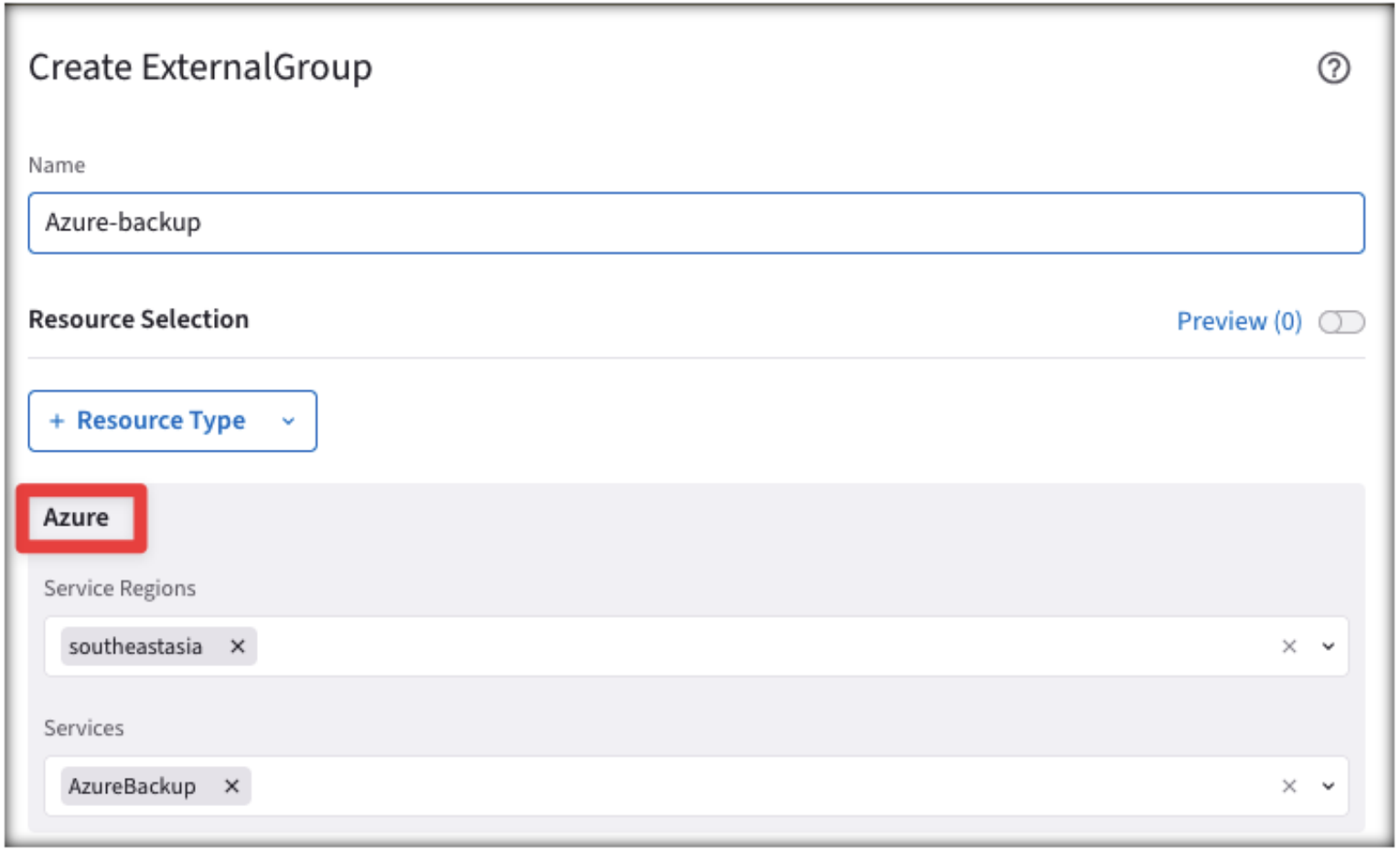
Groups – ExternalGroups & WebGroups

- Once the Distributed Cloud Firewall feature is enabled, two additional tabs—**External Groups and Web Groups**—will automatically appear under the Groups section.



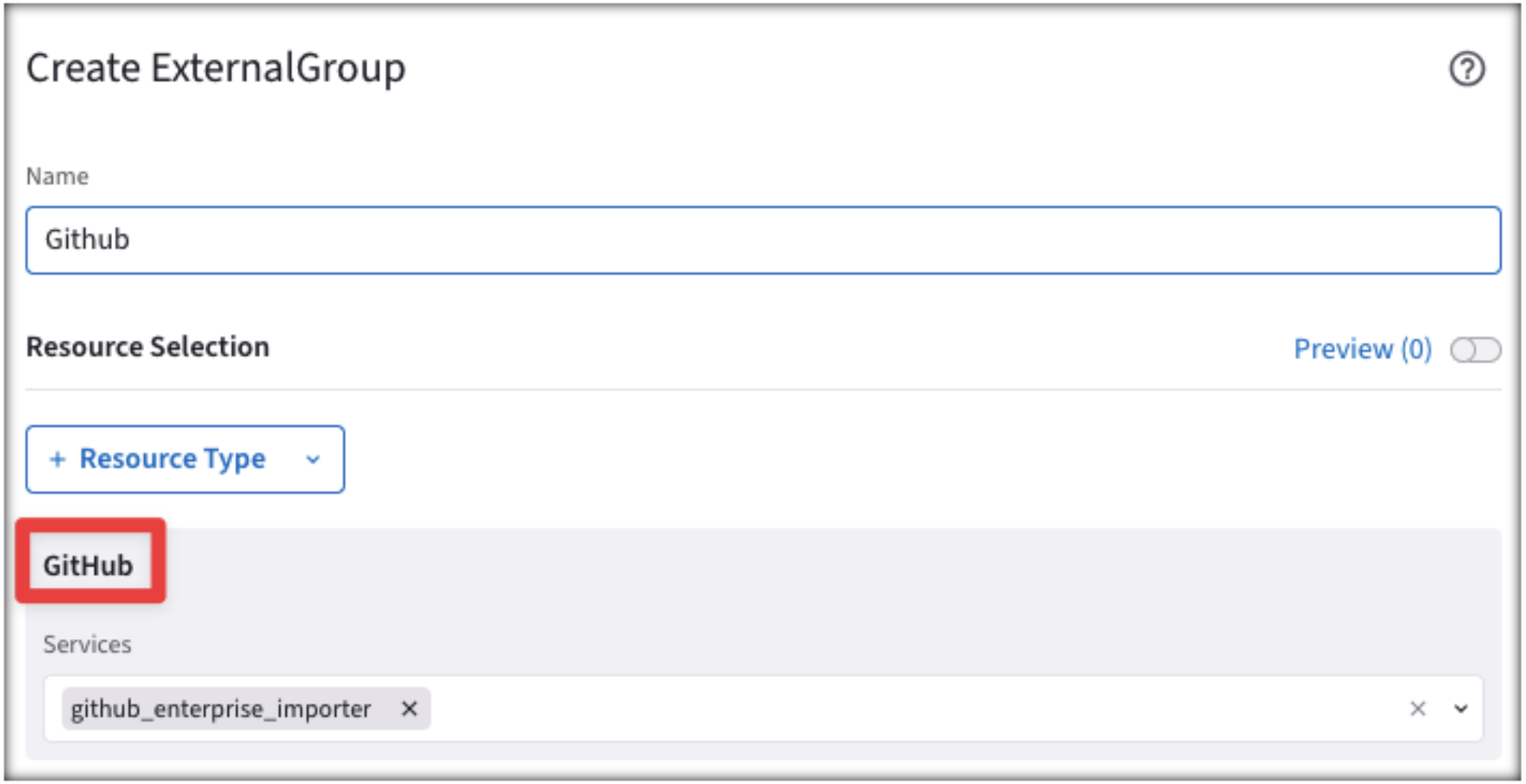
Groups – ExternalGroups – Azure (SaaS-based service)

- Azure Services: IP addresses of Microsoft Azure services categorized by Service and Region



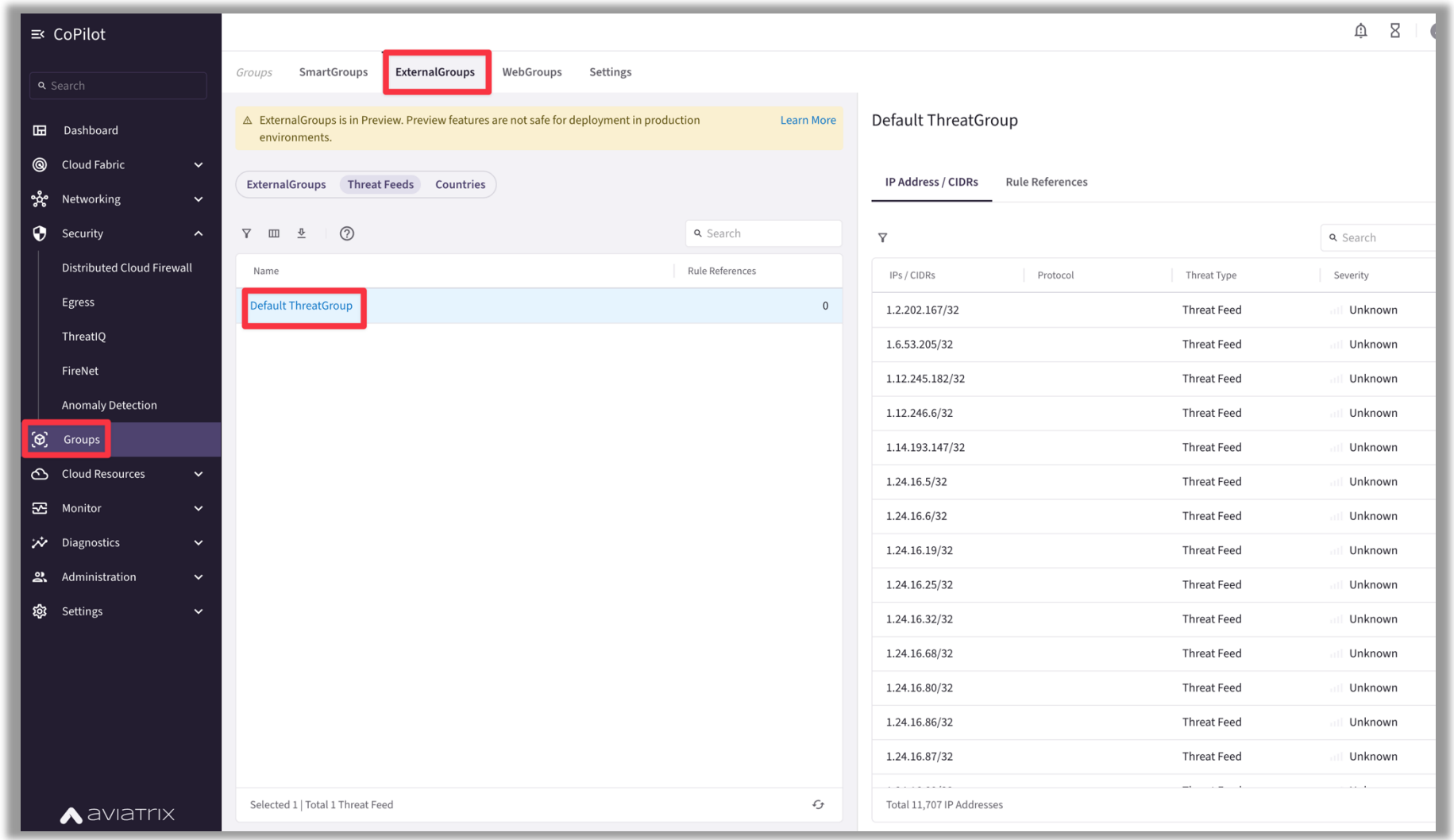
Groups – ExternalGroups – Github (SaaS-based service)

- GitHub Services: IP addresses of GitHub services categorized by service



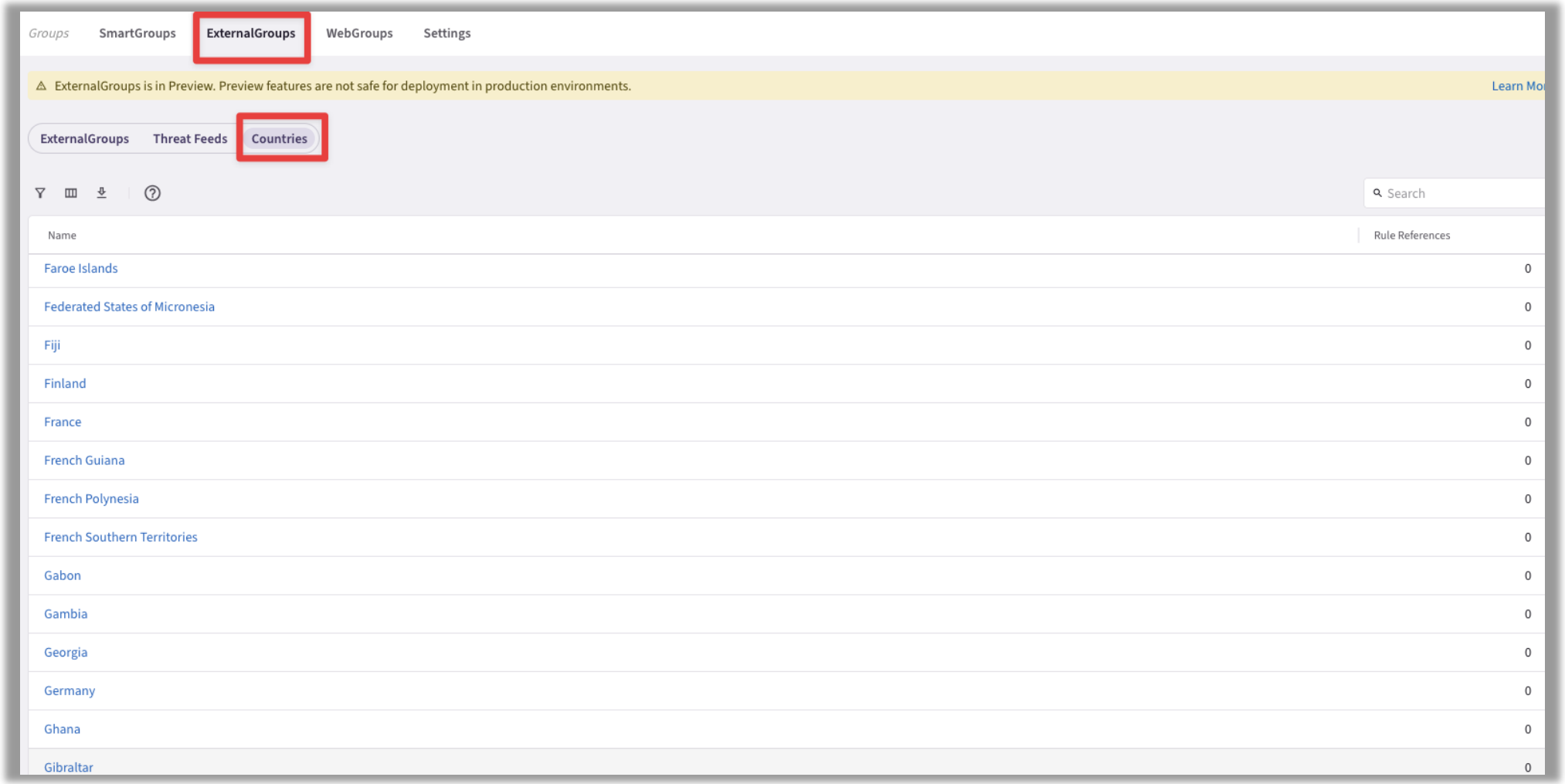
Groups – ExternalGroups – Threat Feeds

- The Default ThreatGroup, provided by third-party **ProofPoint**, is a malicious IP database used for threat prevention by cross-referencing internal IPs against known bad reputations.



Groups – ExternalGroups – Countries

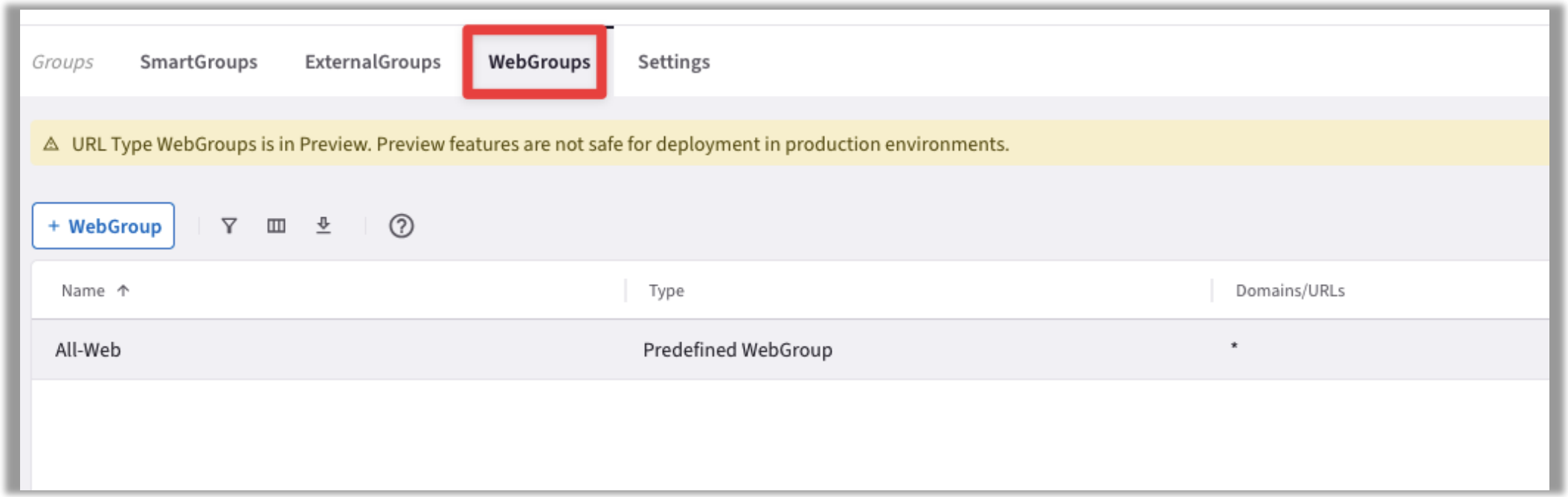
- The **'Countries'** sub-category lists the countries that can be used within DCF rules.



Groups – WebGroups (part.1)

PATH: CoPilot > Groups > WebGroups

- WebGroups define Domains and URLs that assists in filtering (and providing security to) Internet-bound traffic.



System-Defined WebGroup: *All-Web*
When you navigate to *Security > Distributed Cloud Firewall > WebGroups*, a system-defined WebGroup, 'All-Web', has already been created for. <u>This predefined WebGroup cannot be deleted</u>.
This is an "allow-all" WebGroup that you must select in a Distributed Cloud Firewall rule if you do not want to limit the Internet-bound traffic for that rule, but you still want to log the FQDNs that are being accessed.

Groups – WebGroups (part.2)

- Creating a WebGroup

Groups | SmartGroups | ExternalGroups | **WebGroups** | Settings

⚠ URL Type WebGroups is in Preview. Preview features are not safe for deployment in production environments.

+ WebGroup

Name	Type
allowed-internet-http	Domains
allow-internet-https	Domains
allowed-nids-detection	Domains
All-Web	Predefined WebGroup
Sample-WebGroup	Domains

Create WebGroup

⚠ URL Type WebGroups is in Preview. Preview features are not safe for deployment in production environments. Lear…

Name: allowed-internet-http

Type: Domains / URLs Preview

Domains/URLs: *.ubuntu.com

Cancel | Save

Create WebGroup

⚠ URL Type WebGroups is in Preview. Preview features are not safe for deployment in production environments. Lear…

Name: FieldEng

Type: Domains / URLs Preview

Domains/URLs: github.com/AviatrixFieldEng/

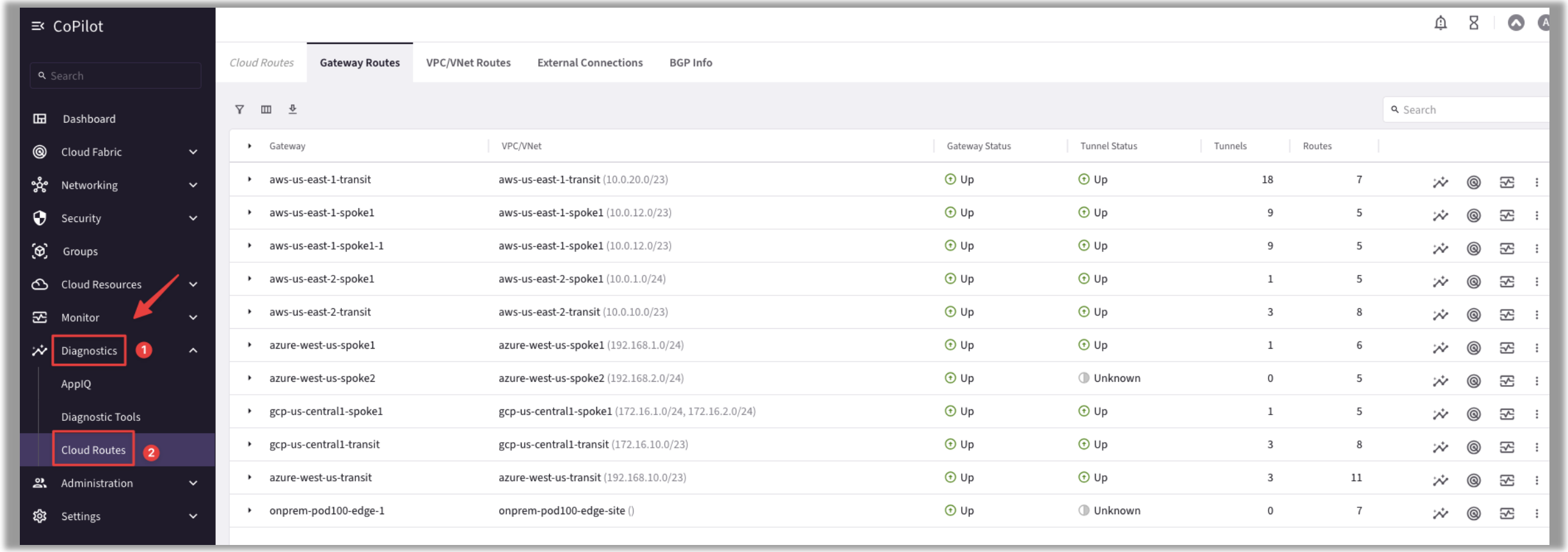
Cancel | Save

Cloud Routes

Cloud Routes

- **PATH**: *CoPilot > Diagnostics > Cloud Routes* or typing **Cloud Routes** in the navigation search.

- In Cloud Routes, you can view routing information for managed resources across your **Aviatrix CNSF**, including multicloud and on-premises (external/Site-to-Cloud) connections, with or without Aviatrix Edge. This enables cloud engineers to access all routing data centrally, without logging into individual cloud provider consoles.



Cloud Routes – Gateway Routes

- **PATH**: *CoPilot > Diagnostics > Cloud Routes* > Gateway Routes
- The Gateway Routes tab shows tunnel information for all Aviatrix gateways managed by the Controller across clouds
- <u>Gateways routes represent the "more specific" routes injected by the Aviatrix Controller using SD-Networking</u>

Cloud Routes | **Gateway Routes** | VPC/VNet Routes | External Connections | BGP Info

Search

Gateway	VPC/VNet	Gateway Status	Tunnel Status	Tunnels	Routes
aws-us-east-1-transit	aws-us-east-1-transit (10.0.20.0/23)	Up	Up	18	7
aws-us-east-1-spoke1	aws-us-east-1-spoke1 (10.0.12.0/23)	Up	Up	9	5

ROUTE	SOURCE	INTERFACE	VIA	NEXT HOP IP	NEXT HOP GATEWAY	METRIC	WEIGHT	STATUS
default		eth0 (INF2)	10.0.12.65	10.0.12.65		400		Up
10.0.12.0/23		eth0 (INF2)	10.0.12.65	10.0.12.65		0		Up
10.0.12.64/26, 10.0.12.65/32	10.0.12.126	eth0 (INF2)				100		Up
10.0.20.79/32	10.0.12.124	tun-0A001444-0 (INF13)		10.0.20.68	aws-us-east-1-transit	0	1	Up
10.0.20.79/32	10.0.12.124	tun-0A001447-0 (INF10)		10.0.20.71	aws-us-east-1-transit	0	1	Up
10.0.20.79/32	10.0.12.124	tun-0A001451-0 (INF11)		10.0.20.81	aws-us-east-1-transit	0	1	Up

aws-us-east-1-spoke1-1	aws-us-east-1-spoke1 (10.0.12.0/23)	Up	Up	9	5
aws-us-east-2-spoke1	aws-us-east-2-spoke1 (10.0.1.0/24)	Up	Up	1	5
aws-us-east-2-transit	aws-us-east-2-transit (10.0.10.0/23)	Up	Up	3	8

Cloud Routes – VPC/Vnets Routes

- **PATH**: *CoPilot > Diagnostics > Cloud Routes* > Gateway Routes
- The VPC/VNet Routes tab shows the routing tables for all VPC/VNet/VCNs in any cloud providers
- VPC/VNet routes represent the routes within the VPC router, typically including RFC1918 addresses

Cloud Routes | Gateway Routes | **VPC/VNet Routes** | External Connections | BGP Info

Search

Name	VPC/VNet	Route Table ID	Routes	Route Status
aws-us-east-1-spoke1-Public-2-us-east-1b-rtb	aws-us-east-1-spoke1(vpc-062df7dccb55b4e75) (10.0.12.0/23)	rtb-0e2c7eb3300fae8fa	5	Up
aws-us-east-1-spoke1-Private-1-us-east-1a-rtb	aws-us-east-1-spoke1(vpc-062df7dccb55b4e75) (10.0.12.0/23)	rtb-02313d032d812cc55	4	Up
ROUTE	GATEWAY	TARGET		
10.0.12.0/23	local	local		Active
192.168.0.0/16	aviatrix-aws-us-east-1-spoke1	i-08f996a30c4f3e781		Active
172.16.0.0/12	aviatrix-aws-us-east-1-spoke1	i-08f996a30c4f3e781		Active
10.0.0.0/8	aviatrix-aws-us-east-1-spoke1	i-08f996a30c4f3e781		Active
aviatrix-aws-us-east-1-spoke1	aws-us-east-1-spoke1(vpc-062df7dccb55b4e75) (10.0.12.0/23)	rtb-07dc78301741ab2ca	3	Up
aws-us-east-1-spoke1-Private-2-us-east-1b-rtb	aws-us-east-1-spoke1(vpc-062df7dccb55b4e75) (10.0.12.0/23)	rtb-0bec61841f8c75c32	4	Up
aws-us-east-1-spoke1-Public-1-us-east-1a-rtb	aws-us-east-1-spoke1(vpc-062df7dccb55b4e75) (10.0.12.0/23)	rtb-048ac2d2ebeb7c70a	5	Up
aws-us-east-1-transit-Public-rtb	aws-us-east-1-transit(vpc-0cc023ddffdf960fb) (10.0.20.0/23)	rtb-0cdf52348c88a7329	2	Up
aws-us-east-1-transit-Private-rtb	aws-us-east-1-transit(vpc-0cc023ddffdf960fb) (10.0.20.0/23)	rtb-03e475fd5a0b8c001	1	Up

Cloud Routes – External Connections

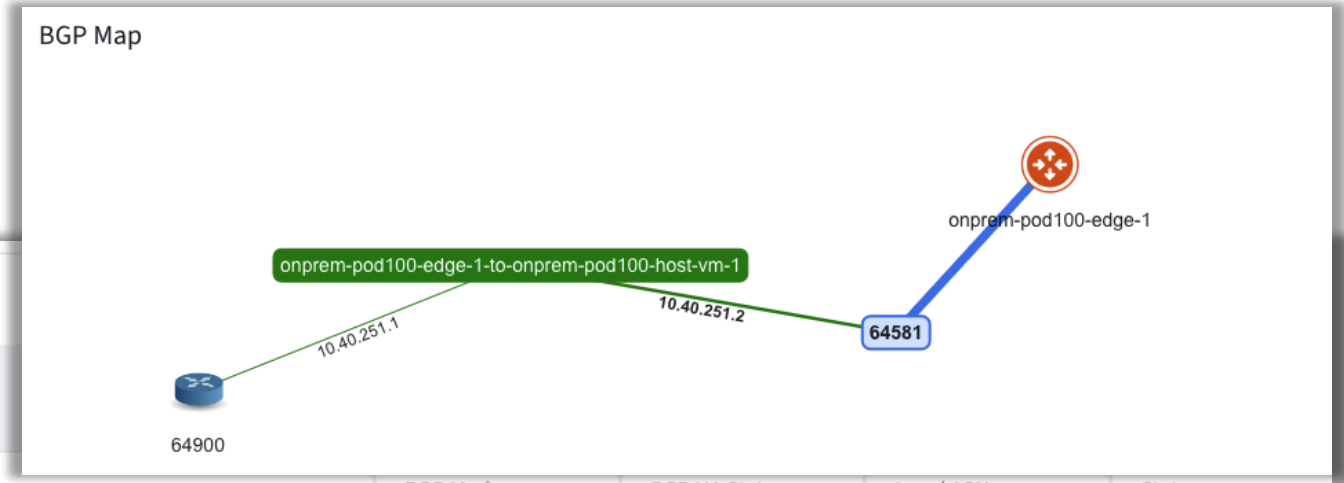
- **PATH**: *CoPilot* > *Diagnostics* > *Cloud Routes* > External Connections

- The External Connections tab shows data center, branch offices, partner site connections into the cloud.

Cloud Routes – External Connections

- **PATH**: *CoPilot* > *Diagnostics* > *Cloud Routes* > External Connections

- The BGP Info tab shows BGP connections from on-prem into the cloud. On this tab you can:
  - View advertised routes being sent to the remote site.
  - View learned routes that are being received from the remote site.



Cloud Routes | Gateway Routes | VPC/VNet Routes | External Connections | **BGP Info**

Gateway	VPC/VNet	BGP Mode	BGP HA Status	Local ASN	Status
onprem-pod100-edge-1	()	Enabled	activemesh	64581	Established

Connection Name	Remote AS Number	Neighbor IP	Local IP	Neighbor Status
onprem-pod100-edge-1-to-onprem-pod100-host-vm-1(10.4…	64900	10.40.251.1	10.40.251.2	Established

AVIATRIX CLOUD COFFE BREAK

Next: Tenet-2 Distributed and Embedded Security