



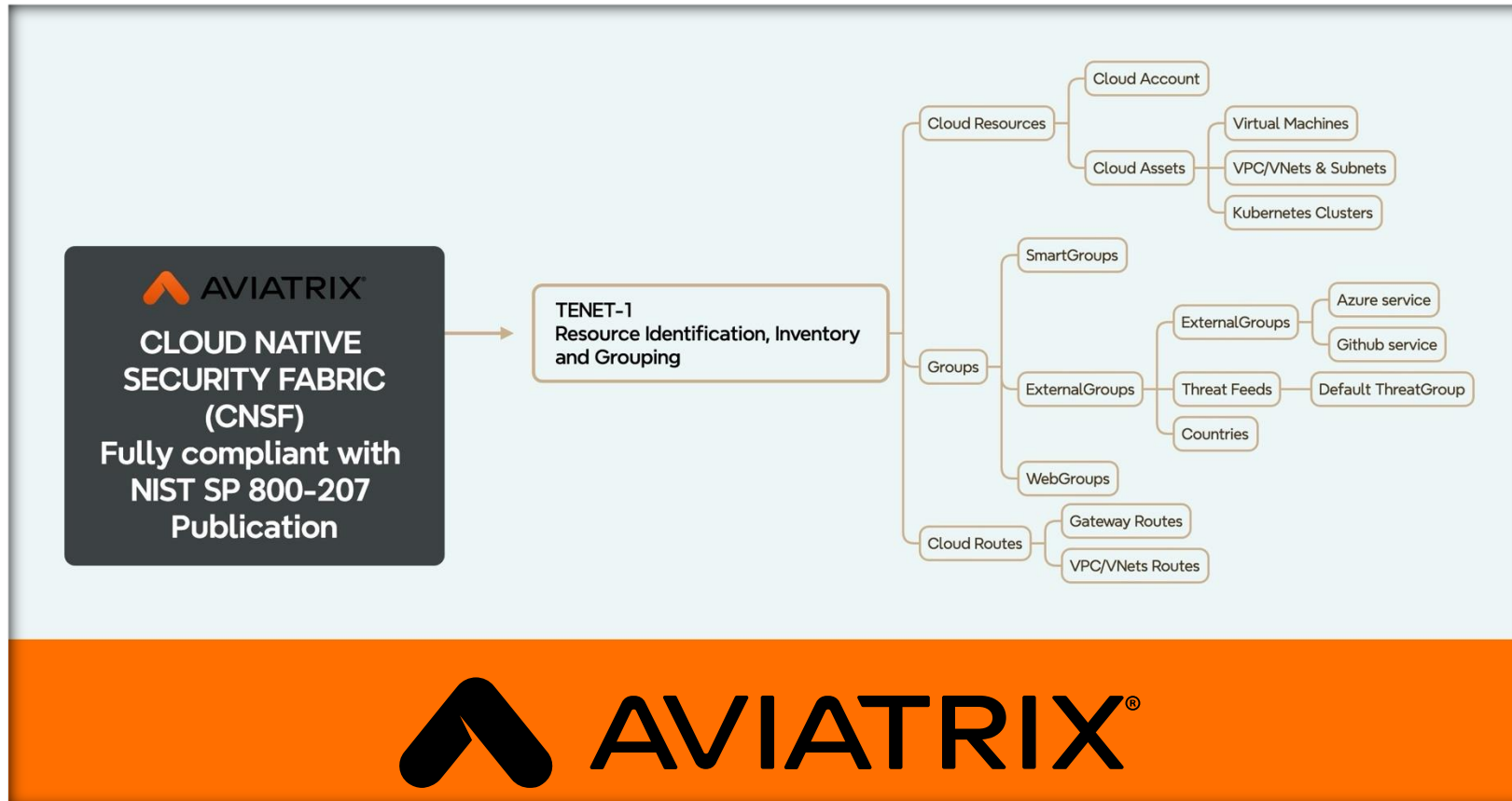
## Tenet-1: Resource Identification, Inventory and Grouping

# 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.

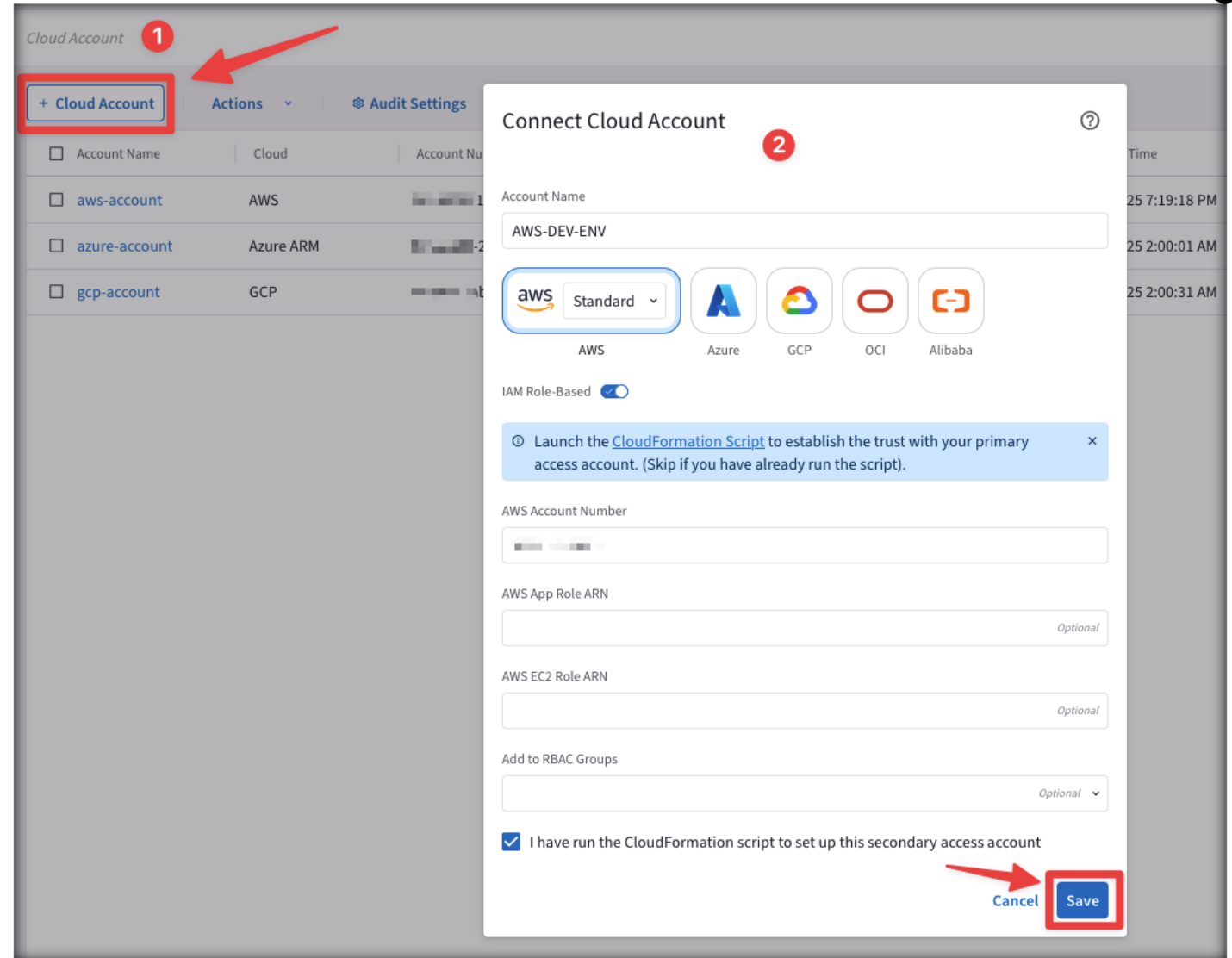
The screenshot displays the Aviatrix CoPilot interface. On the left, the navigation sidebar includes options like Dashboard, Cloud Fabric, Networking, Security, Groups, Cloud Resources (marked with a red box and '1'), Cloud Account (marked with a red box and '2'), Cloud Assets, Monitor, Diagnostics, Administration, and Settings. The main content area is titled 'Cloud Account' and features a '+ Cloud Account' button, 'Actions' dropdown, and 'Audit Settings' link. Below this is a table listing cloud accounts.

<input type="checkbox"/> Account Name	Cloud	Account Number / ID	RBAC Group	Audit Status	Last Audit Time
<input type="checkbox"/> <a href="#">aws-account</a>	AWS	[REDACTED]	admin, <a href="#">+ 1 more</a>	✓ Pass	Jul 19, 2025 7:19:18 PM
<input type="checkbox"/> <a href="#">azure-account</a>	Azure ARM	[REDACTED]	admin, <a href="#">+ 1 more</a>	✓ Pass	Jul 19, 2025 2:00:01 AM
<input type="checkbox"/> <a href="#">gcp-account</a>	GCP	[REDACTED]	admin, <a href="#">+ 1 more</a>	✓ Pass	Jul 19, 2025 2:00:31 AM

# 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 Account 1

+ Cloud Account Actions Audit Settings

Account Name	Cloud	Account Number
aws-account	AWS	...
azure-account	Azure ARM	...
gcp-account	GCP	...

Connect Cloud Account 2

Account Name

AWS-DEV-ENV

aws Standard

AWS Azure GCP OCI Alibaba

IAM Role-Based

Launch the CloudFormation Script to establish the trust with your primary access account. (Skip if you have already run the script).

AWS Account Number

AWS App Role ARN

AWS EC2 Role ARN

Add to RBAC Groups

I have run the CloudFormation script to set up this secondary access account

Cancel Save

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

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

CoPilot

Search

Dashboard

Cloud Fabric

Networking

Security

Groups

Cloud Resources

Cloud Account

Cloud Assets

Monitor

Diagnostics

Administration

Settings

Cloud Assets

Virtual Machines

VPC/VNets & Subnets

Kubernetes Clusters

Actions

Filter

Grid

Download

Search

Name	Cloud	Region	Availability Zone	IP Address	Tags	SmartGroups	Aviatrix Manag
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

1

Search

<input type="checkbox"/> Name ↑	Cloud ▼ ↑	Region	Availability Zone	IP Address	Tags	SmartGroups	Aviatrix Managed ↓
<input type="checkbox"/> aviatrix-engineering-aws-spoke-qa	AWS	us-east-2	us-east-2a	10.5..., + 6 more	Aviatrix-Created-Resource:..., + 4 more		Gateways
<input type="checkbox"/> aviatrix-operations-aws-landing-zone	AWS	us-east-1	us-east-1a	10.7..., + 1 more	Aviatrix-Created-Resource:..., + 4 more		Gateways
<input type="checkbox"/> aviatrix-operations-aws-spoke-k8s	AWS	us-east-1	us-east-1a	10.1..., + 1 more	Aviatrix-Created-Resource:..., + 4 more		Gateways
<input type="checkbox"/> aviatrix-transit-aws-us-east-1	AWS	us-east-1	us-east-1a	10.1..., + 3 more	Aviatrix-Created-Resource:..., + 4 more		Gateways
<input type="checkbox"/> aviatrix-transit-aws-us-east-2	AWS	us-east-2	us-east-2a	10..., + 15 more	Aviatrix-Created-Resource:..., + 4 more		Gateways
<input type="checkbox"/> 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
<input type="checkbox"/> 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
<input type="checkbox"/> accounting-app-qa	AWS	us-east-1	us-east-1a	10.1.3.10	Application: crm, + 9 more	Accenture_Demo, app, + 7 more	Yes
<input type="checkbox"/> 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
<input type="checkbox"/> 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
<input type="checkbox"/> 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
<input type="checkbox"/> engineering-app-qa	AWS	us-east-2	us-east-2a	10.5.3.10	Application: engineering app, + 9 more	Accenture_Demo, + 7 more	Yes
<input type="checkbox"/> engineering-web-dev	AWS	us-east-2	us-east-2a	10.5.2.10	Application: engineering app, + 9 more	Accenture_Demo, + 6 more	Yes
<input type="checkbox"/> ng_1	AWS	us-east-1	us-east-1a	10..., + 19 more	Name: ng_1, + 10 more		Yes
<input type="checkbox"/> 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
<input type="checkbox"/> AviatrixController-migrated-2025-05-23T02-51-28	AWS	us-west-2	us-west-2a	172..., + 1 more	Aviatrix-Created-Resource:..., + 8 more		No
<input type="checkbox"/> AviatrixCoPilot	AWS	us-west-2	us-west-2a	172..., + 1 more	Name: AviatrixCoPilot, + 4 more		No
<input type="checkbox"/> grafana-demo	AWS	us-west-2	us-west-2a	172..., + 1 more	Department: 550 Solution..., + 6 more		No

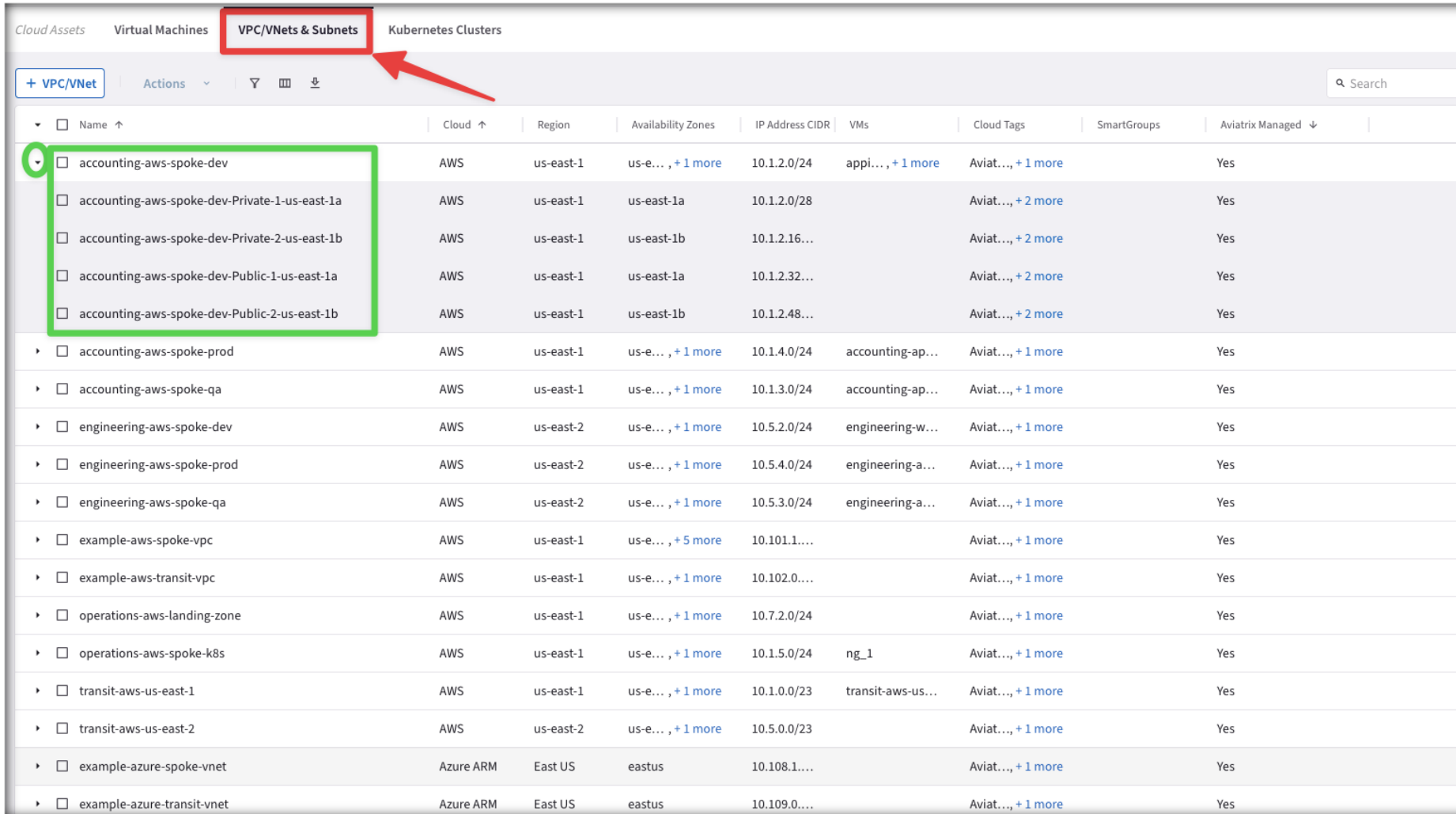
A VM can be marked as *Aviatrix managed* where:

- **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.



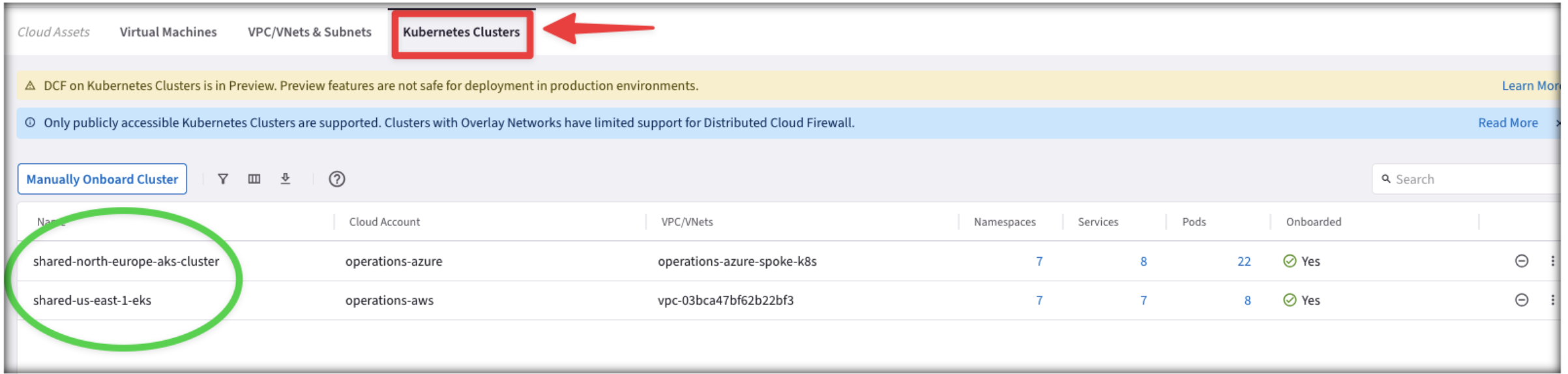
Name	Cloud	Region	Availability Zones	IP Address CIDR	VMs	Cloud Tags	SmartGroups	Aviatrix Managed
<input type="checkbox"/> accounting-aws-spoke-dev	AWS	us-east-1	us-e... , + 1 more	10.1.2.0/24	appli..., + 1 more	Aviat..., + 1 more		Yes
<input type="checkbox"/> accounting-aws-spoke-dev-Private-1-us-east-1a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



Name	Cloud Account	VPC/VNets	Namespaces	Services	Pods	Onboarded
shared-north-europe-aks-cluster	operations-azure	operations-azure-spoke-k8s	7	8	22	✓ Yes
shared-us-east-1-eks	operations-aws	vpc-03bca47bf62b22bf3	7	7	8	✓ Yes

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

Discovery of Kubernetes Resources
Preview

Control the discovery of Kubernetes Resources on your Cloud Accounts.

Status

☒ Enabled

Disable



# Groups

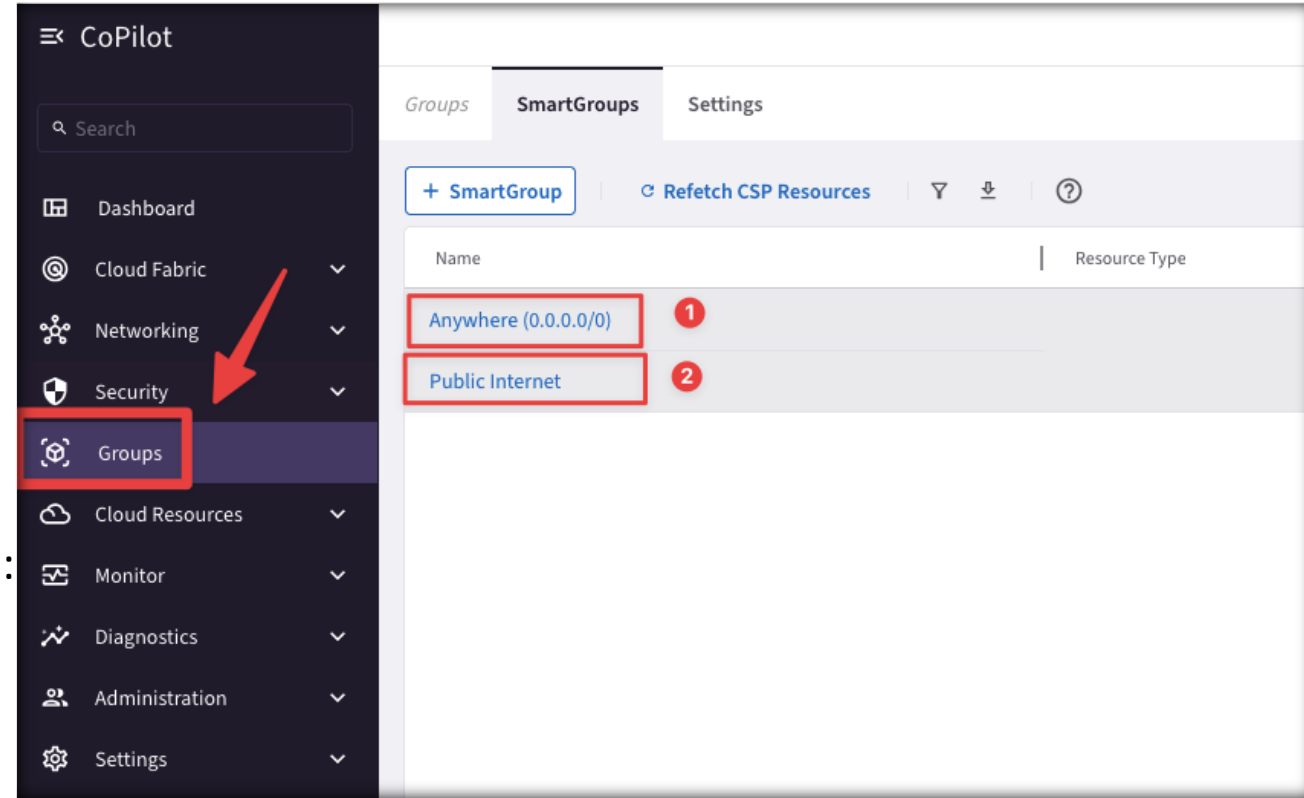
# Groups

- ❑ 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.

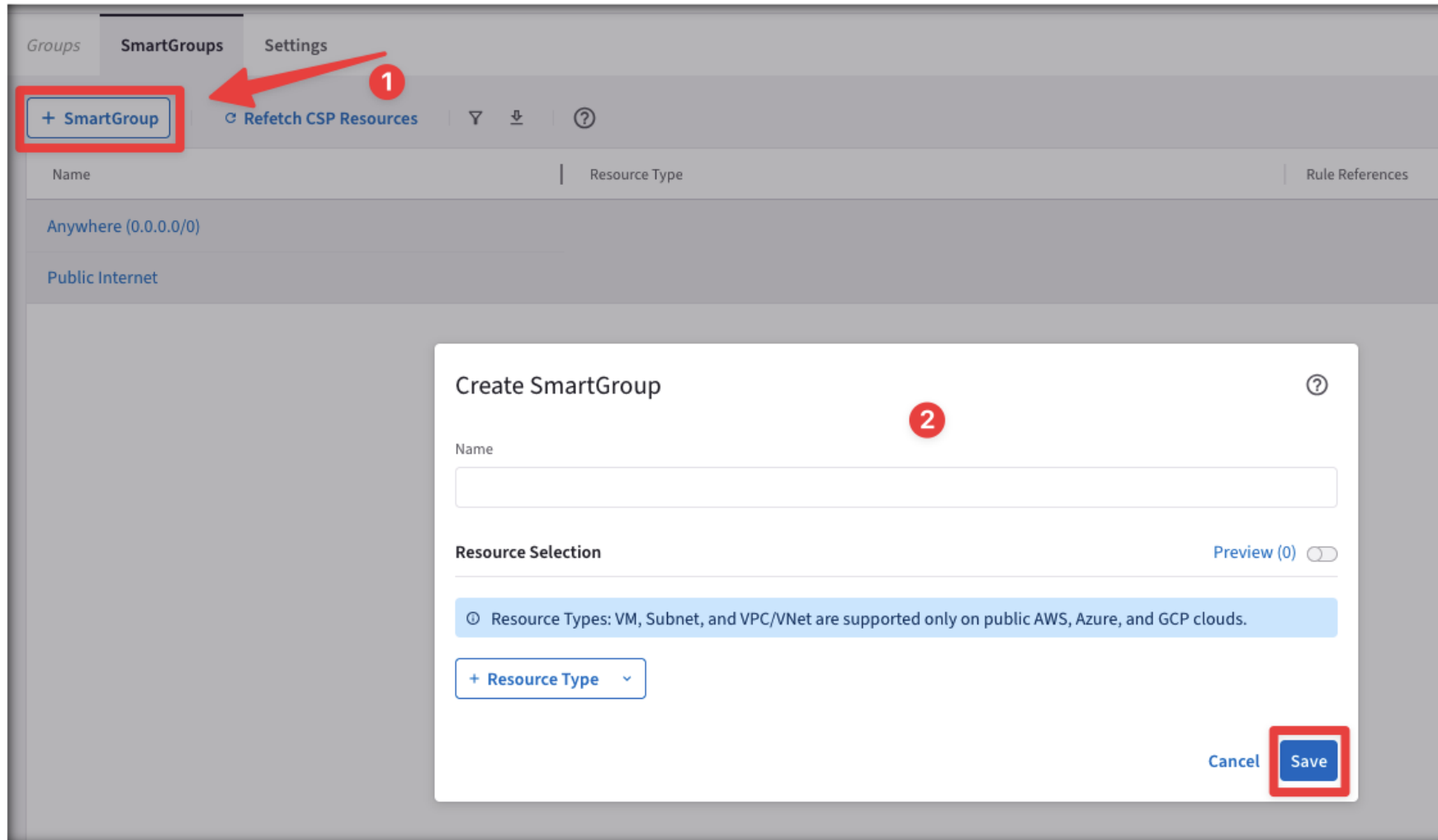
**CAVEAT:** These system-defined SmartGroups cannot be deleted.



**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.

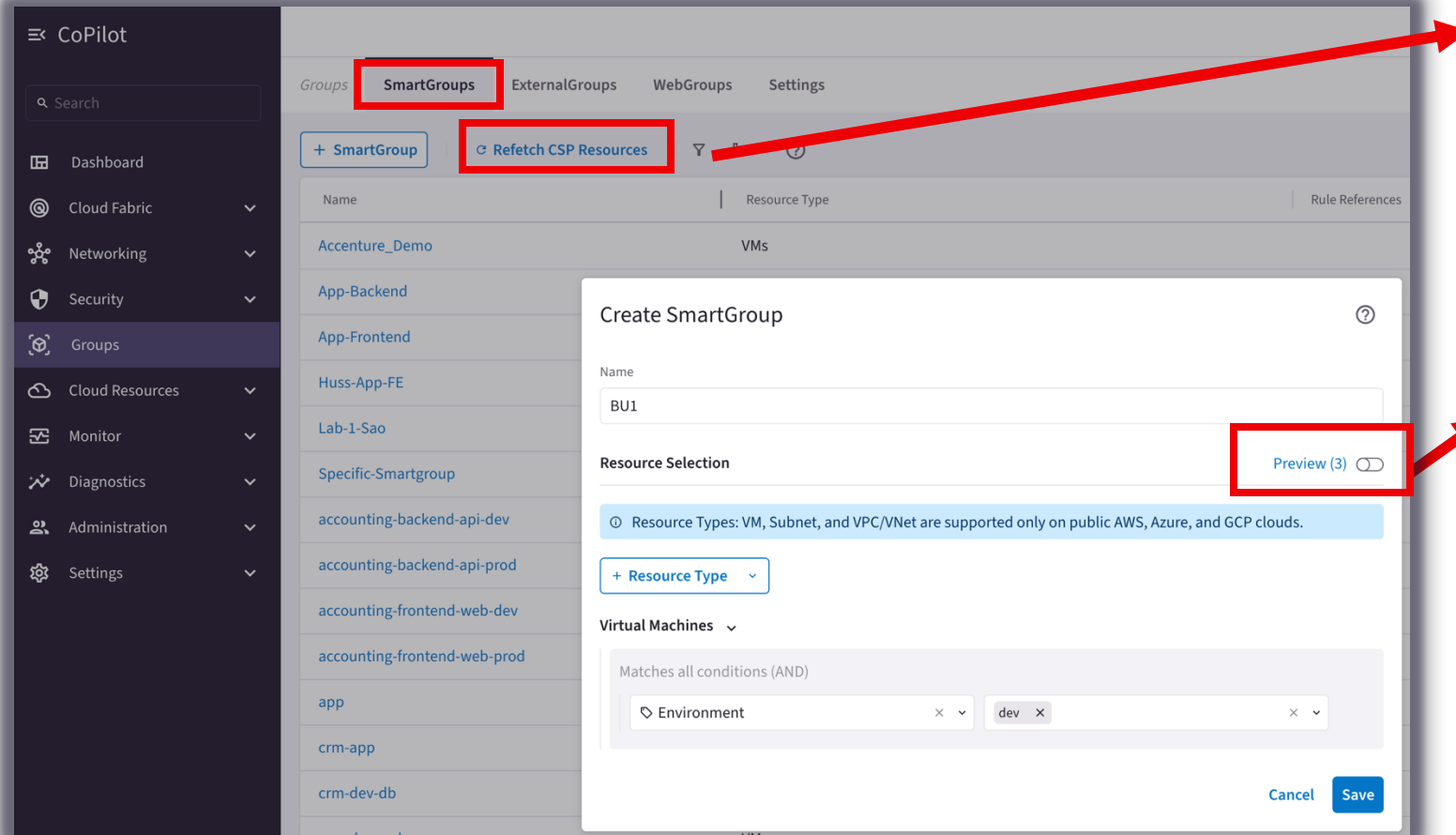
# Groups – SmartGroups (part.1)

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

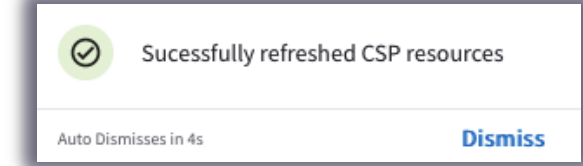


The screenshot shows the 'SmartGroups' tab in the Aviatrix interface. A red box highlights the '+ SmartGroup' button, and a red arrow points to it with a red circle containing the number '1'. Below this, a table lists existing SmartGroups: 'Anywhere (0.0.0.0/0)' and 'Public Internet'. A 'Create SmartGroup' modal is open, with a red circle containing the number '2' next to its title. The modal includes a 'Name' input field, a 'Resource Selection' section with a 'Preview (0)' toggle, and a blue informational box stating: 'Resource Types: VM, Subnet, and VPC/VNet are supported only on public AWS, Azure, and GCP clouds.' At the bottom of the modal, there is a '+ Resource Type' dropdown and 'Cancel' and 'Save' buttons. The 'Save' button is highlighted with a red box.

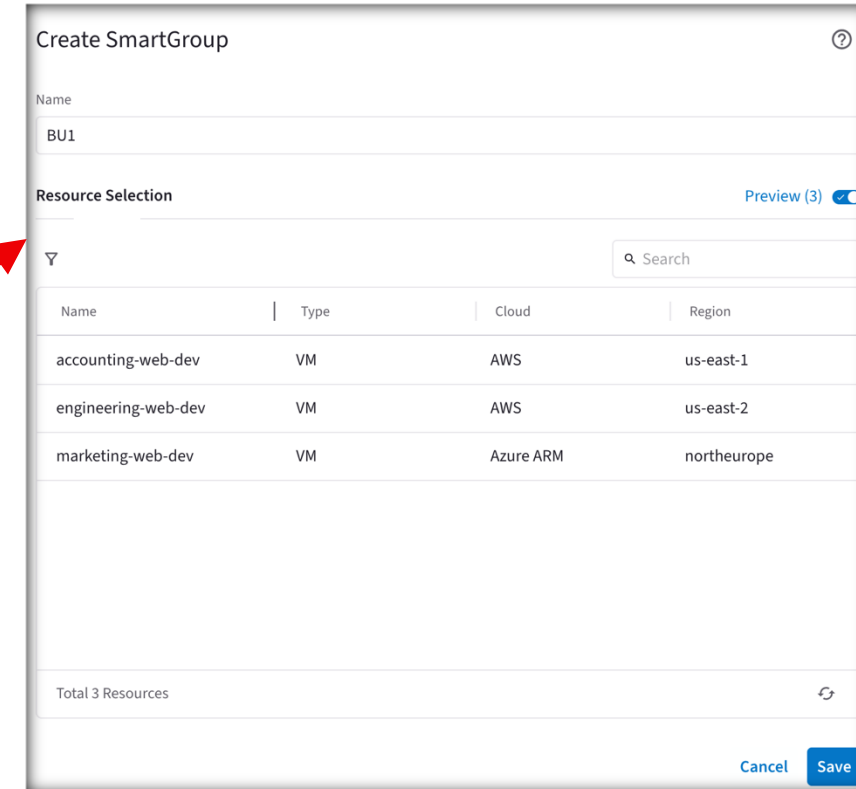
# Groups – SmartGroups (part.2)



The screenshot shows the CoPilot interface with the 'Groups' section selected in the sidebar. The 'SmartGroups' tab is active, and the 'Refetch CSP Resources' button is highlighted. A red arrow points from this button to a success message box on the right.



Successfully refreshed CSP resources  
Auto Dismisses in 4s  
[Dismiss](#)



Create SmartGroup

Name: BU1

Resource Selection Preview (3) ☒

Name	Type	Cloud	Region
accounting-web-dev	VM	AWS	us-east-1
engineering-web-dev	VM	AWS	us-east-2
marketing-web-dev	VM	Azure ARM	northeurope

Total 3 Resources

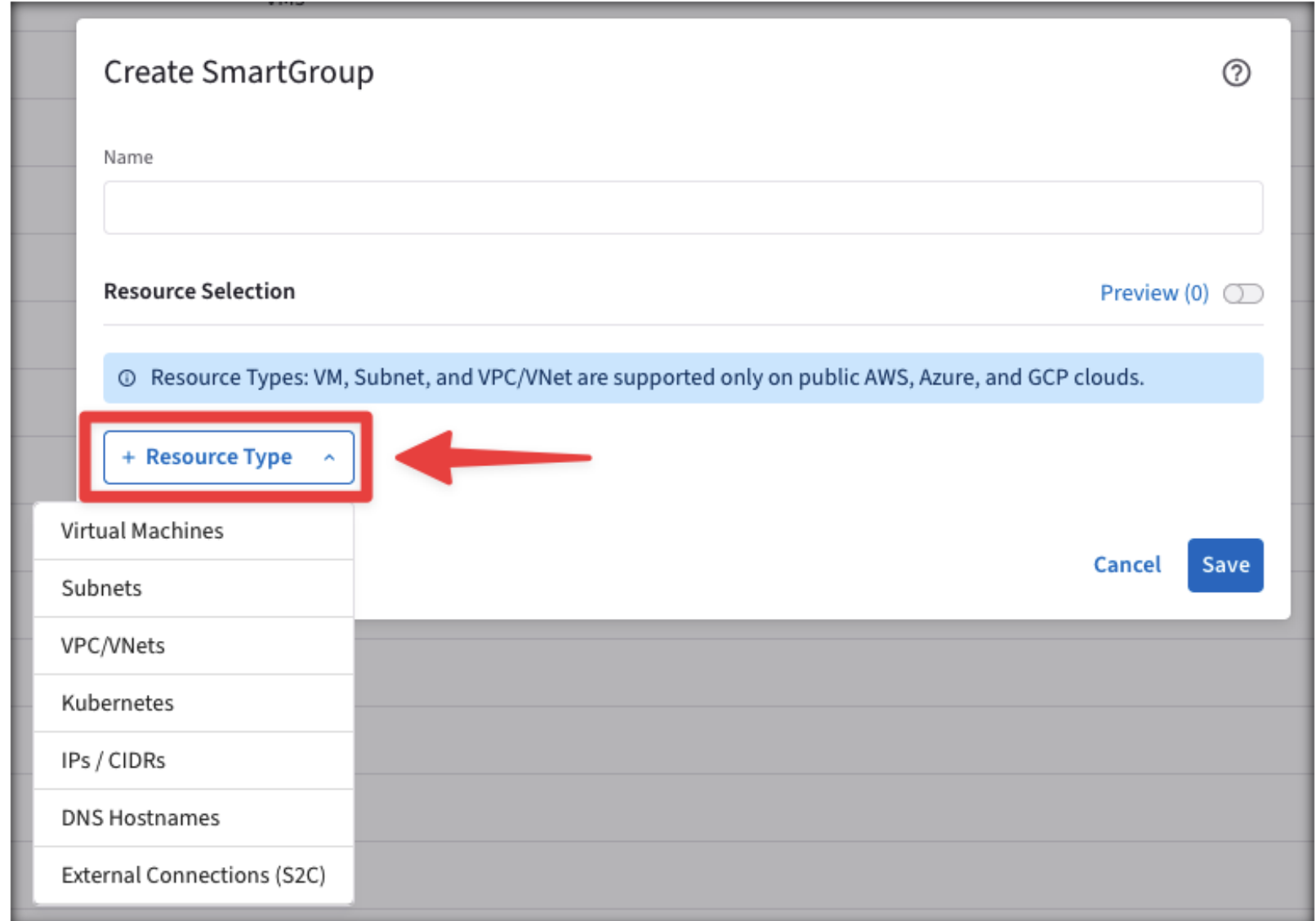
[Cancel](#) [Save](#)

- 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)



Create SmartGroup

Name

Resource Selection

Preview (0)

Resource Types: VM, Subnet, and VPC/VNet are supported only on public AWS, Azure, and GCP clouds.

+ Resource Type

- Virtual Machines
- Subnets
- VPC/VNets
- Kubernetes
- IPs / CIDRs
- DNS Hostnames
- External Connections (S2C)

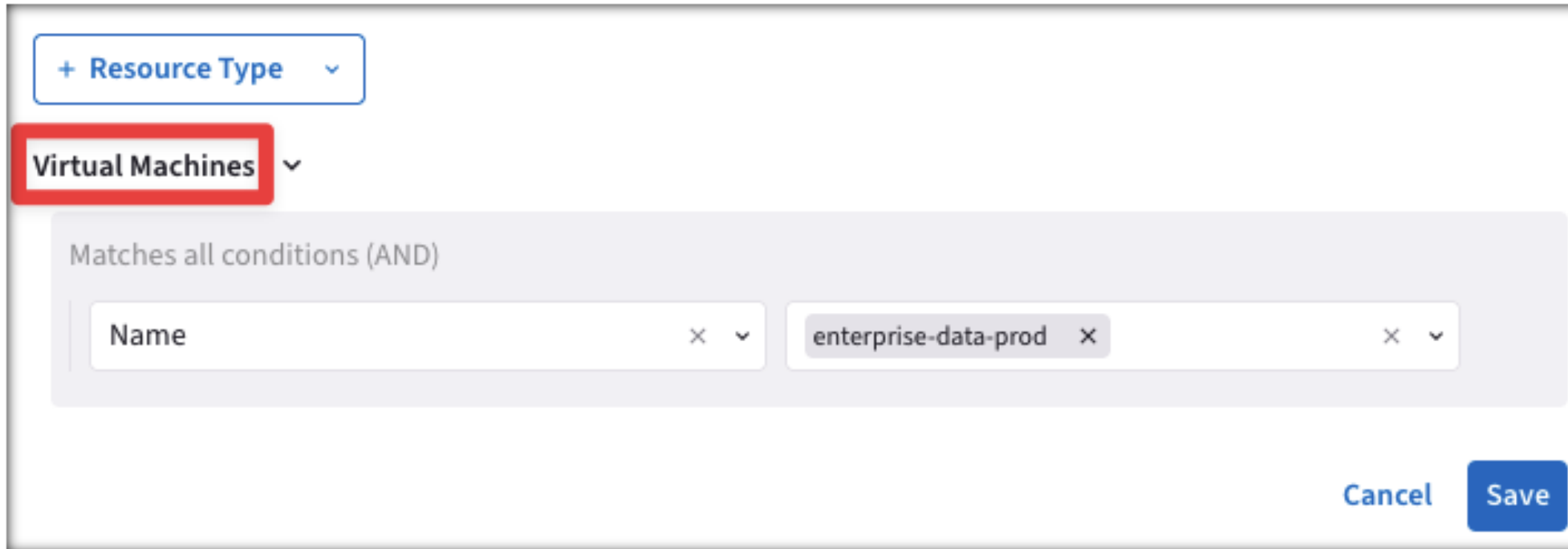
Cancel Save

# Groups – SmartGroups (part.4)

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

1) Virtual Machine:

- **Name** → symbolic name of the interested instance



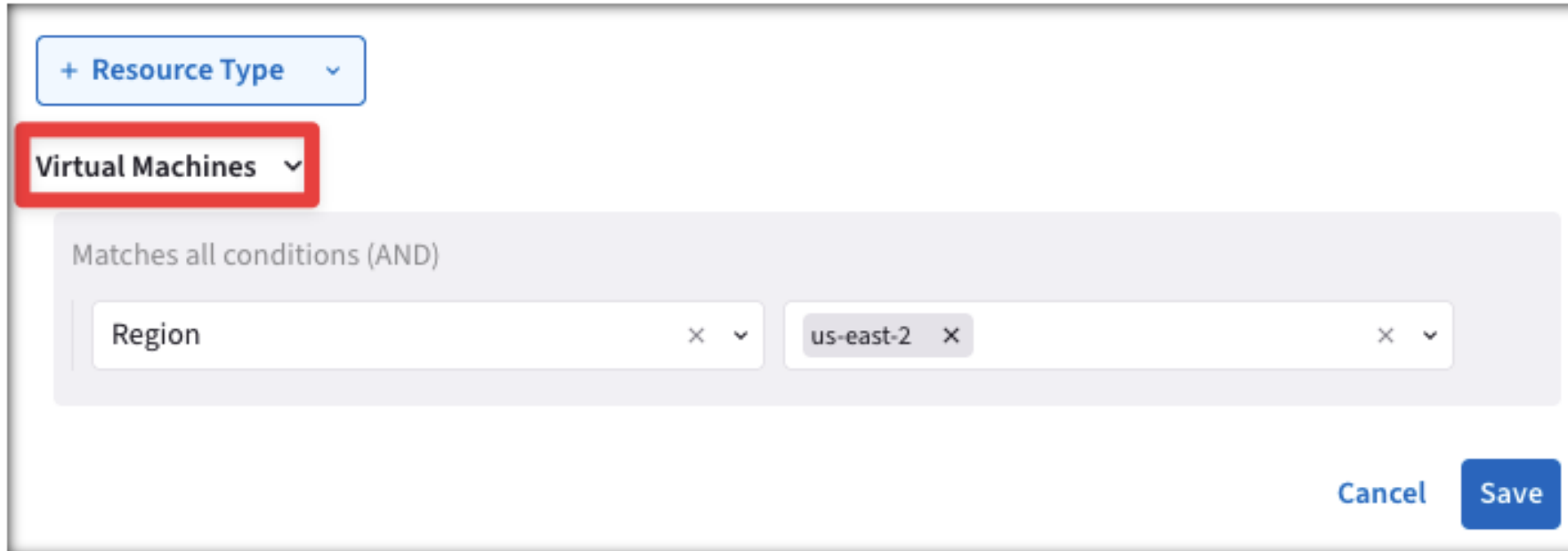
The screenshot shows a configuration window for a SmartGroup. At the top left, there is a button labeled "+ Resource Type" with a dropdown arrow. Below it, a dropdown menu is open, showing "Virtual Machines" with a dropdown arrow; this menu is highlighted with a red rectangular border. Below the dropdown, a light gray box contains the text "Matches all conditions (AND)". Inside this box, there are two input fields. The first field is labeled "Name" and has a dropdown arrow. The second field contains the text "enterprise-data-prod" and has a dropdown arrow. Both fields have a small 'x' icon to their right. At the bottom right of the window, there are two buttons: "Cancel" and "Save".

# Groups – SmartGroups (part.5)

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

1) Virtual Machine:

- **Region** → region's identifier

The image shows a user interface for configuring a SmartGroup. At the top left, there is a button labeled "+ Resource Type" with a dropdown arrow. Below it, a dropdown menu is open, showing "Virtual Machines" with a dropdown arrow; this menu is highlighted with a red rectangular border. Below the dropdown, a light gray box contains the text "Matches all conditions (AND)". Inside this box, there are two filter conditions: "Region" followed by a close button (x) and a dropdown arrow, and "us-east-2" followed by a close button (x) and a dropdown arrow. At the bottom right of the interface, there are two buttons: "Cancel" and "Save".

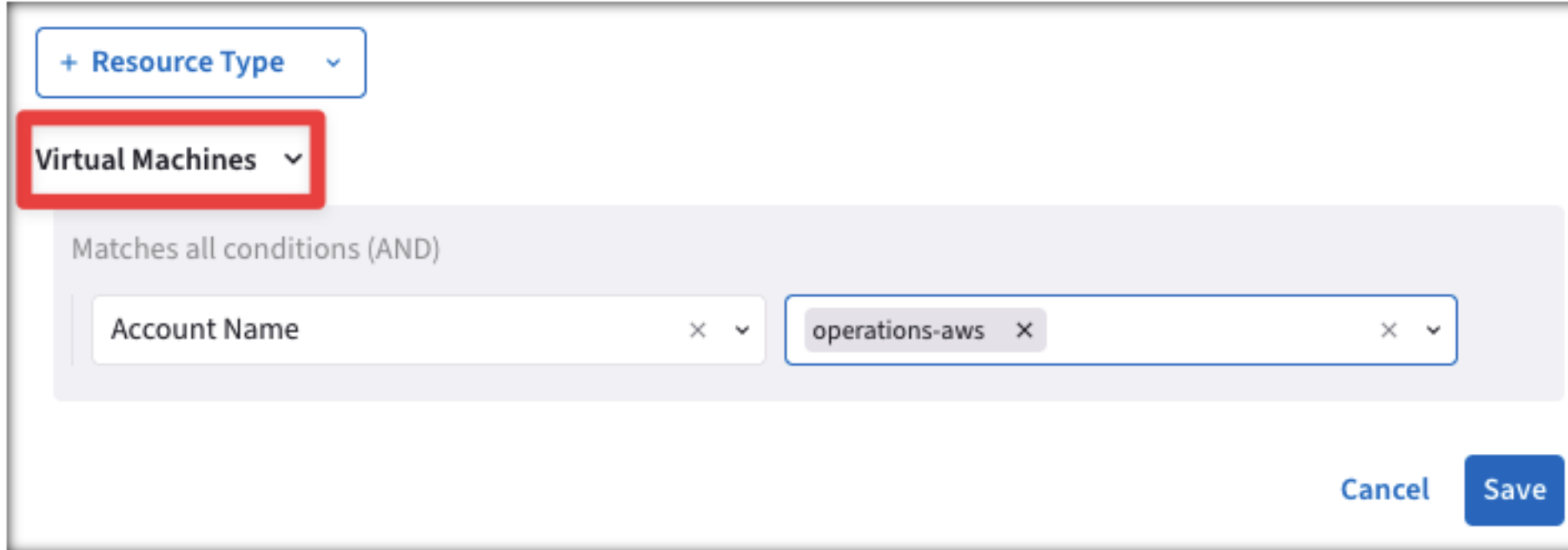


# Groups – SmartGroups (part.6)

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

1) Virtual Machine:

- **Account Name** → The name of your account or subscription

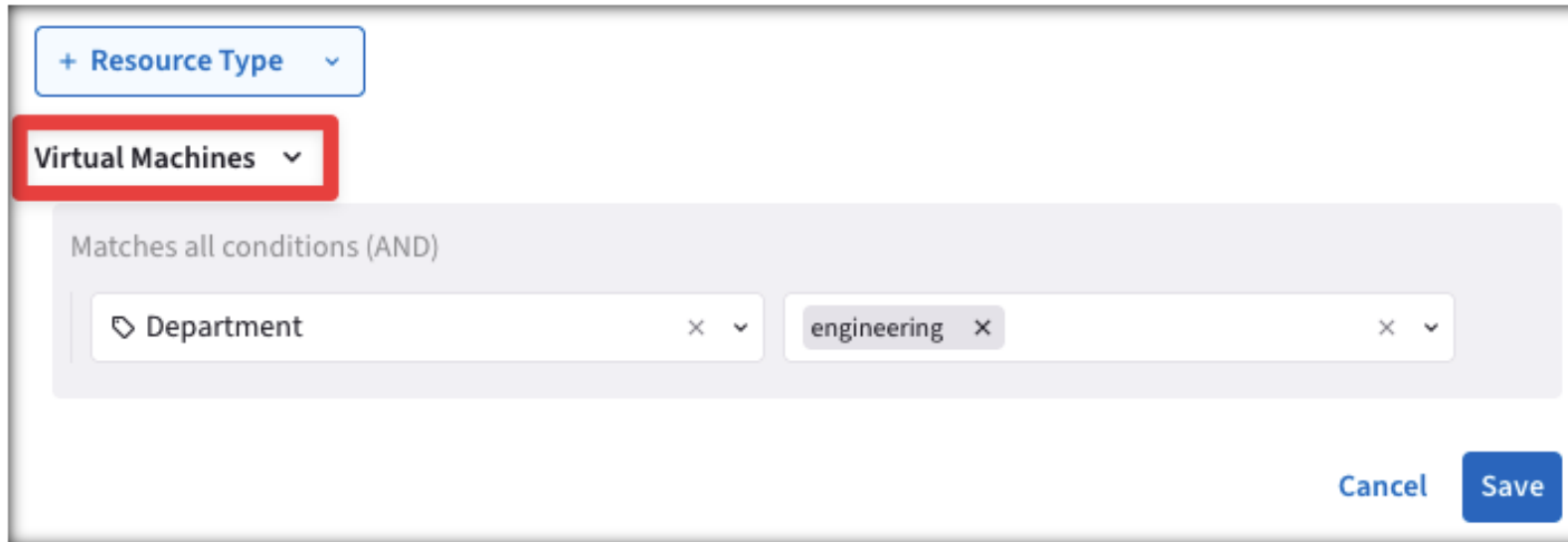


The screenshot shows a configuration window for a SmartGroup. At the top left, there is a button labeled "+ Resource Type" with a dropdown arrow. Below it, a dropdown menu is open, showing "Virtual Machines" with a dropdown arrow; this menu is highlighted with a red rectangular border. Below the dropdown, the text "Matches all conditions (AND)" is displayed. Underneath this text, there are two input fields. The first field is labeled "Account Name" and has a dropdown arrow. The second field contains the text "operations-aws" and has a dropdown arrow. Both fields have a small "x" icon to their right, indicating they can be removed. At the bottom right of the window, there are two buttons: "Cancel" and "Save".

# Groups – SmartGroups (part.7)

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

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

The screenshot shows a web interface for creating a SmartGroup. At the top left is a button labeled "+ Resource Type" with a dropdown arrow. Below it, a dropdown menu is open, showing "Virtual Machines" with a dropdown arrow; this menu is highlighted with a red rectangular border. Below the dropdown is a light gray box containing the text "Matches all conditions (AND)". Inside this box are two filter tags: "Department" with a dropdown arrow and an 'x' to remove it, and "engineering" with an 'x' to remove it. At the bottom right of the interface are two buttons: "Cancel" and "Save".

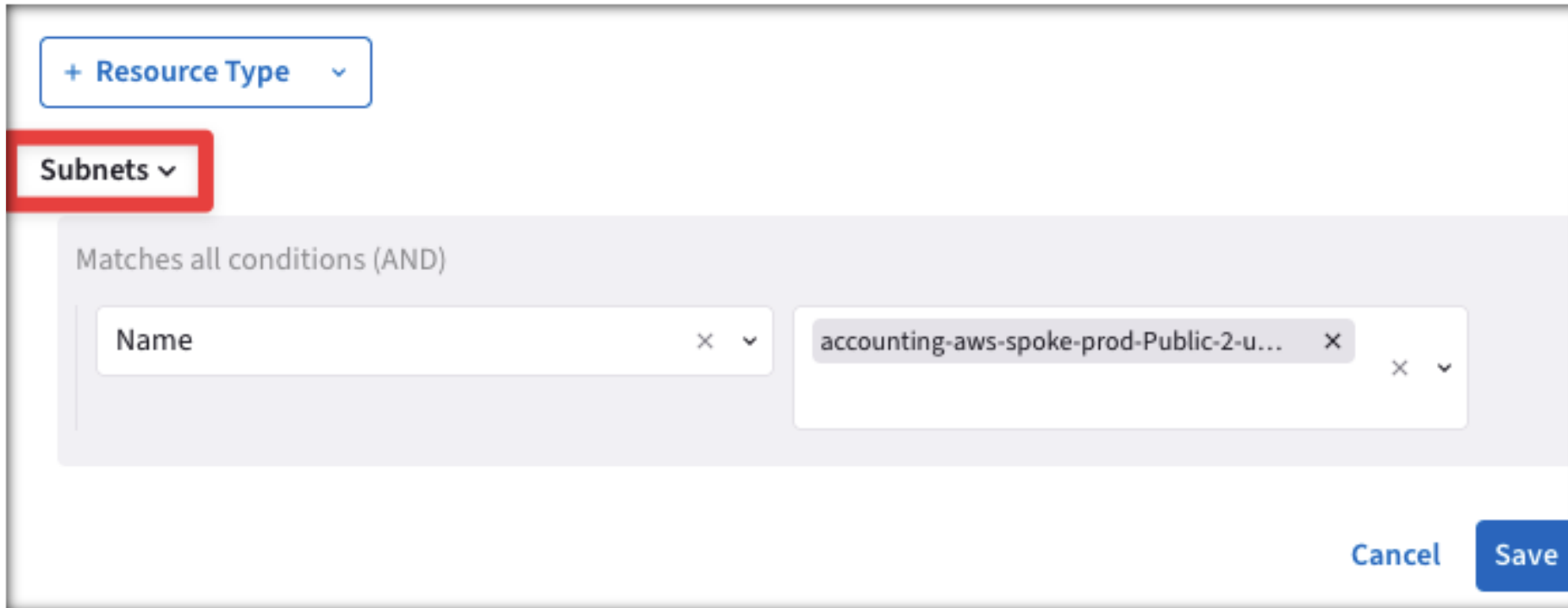
**Recommended method**

# Groups – SmartGroups (part.8)

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

2) Subnets:

- Name → subnet's name



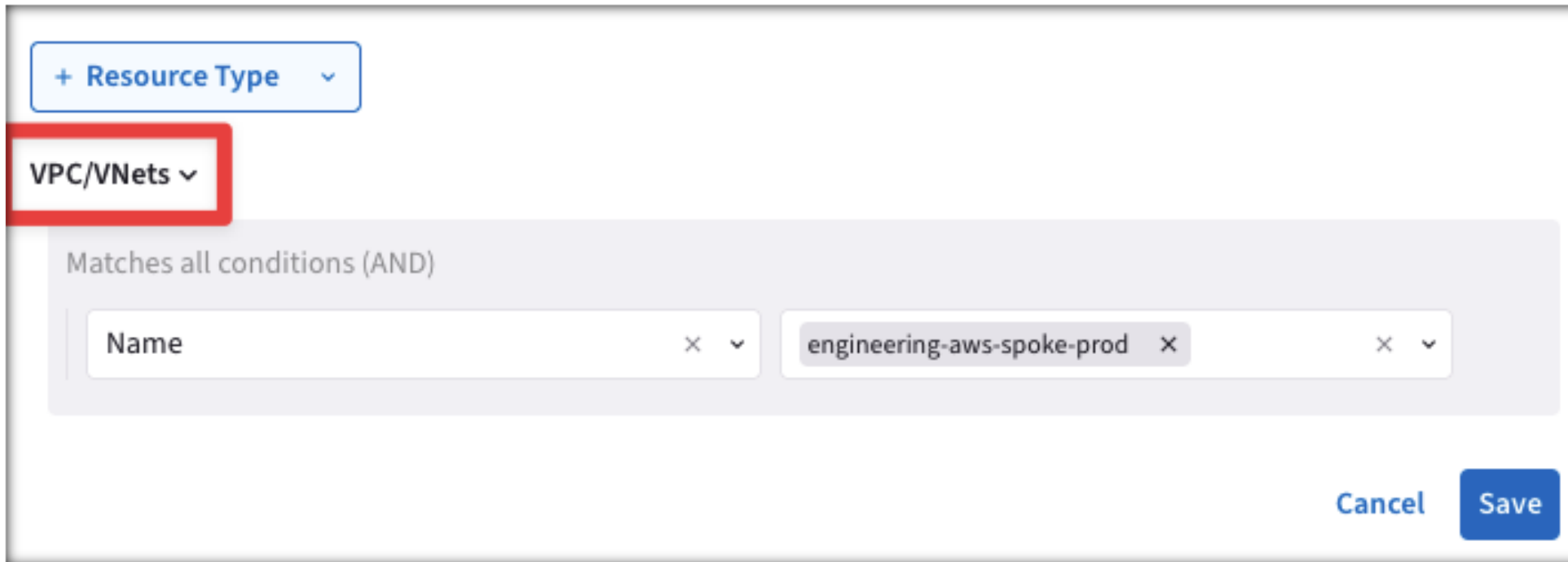
The screenshot shows the configuration interface for a SmartGroup. At the top left, there is a button labeled "+ Resource Type" with a dropdown arrow. Below it, the "Subnets" resource type is selected and highlighted with a red box. The main configuration area is titled "Matches all conditions (AND)". It contains a single condition: "Name" is equal to "accounting-aws-spoke-prod-Public-2-u...". The condition is displayed in a light gray box with a search bar on the left and a value field on the right. The value field contains the text "accounting-aws-spoke-prod-Public-2-u..." and has a dropdown arrow. At the bottom right of the interface, there are "Cancel" and "Save" buttons.

# Groups – SmartGroups (part.9)

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

3) VPC/VNets:

- Name → VPC's name



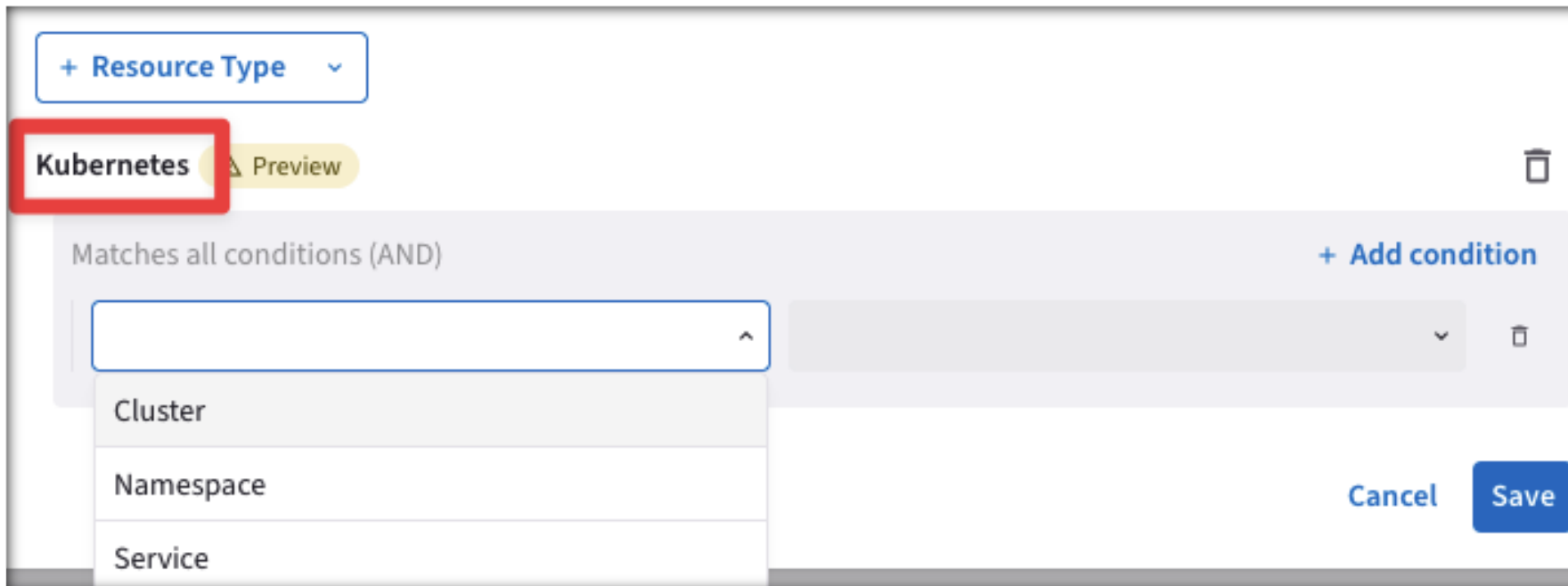
The screenshot shows a configuration window for a SmartGroup. At the top left, there is a button labeled "+ Resource Type" with a dropdown arrow. Below it, a dropdown menu is open, showing "VPC/VNets" with a dropdown arrow; this menu is highlighted with a red rectangular box. Below the dropdown, a light gray box contains the text "Matches all conditions (AND)". Inside this box, there are two search criteria: "Name" and "engineering-aws-spoke-prod". Each criterion is in a white box with a close button (X) and a dropdown arrow. At the bottom right of the window, there are two buttons: "Cancel" and "Save".

# Groups – SmartGroups (part.10)


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

4) Kubernetes:

- **Cluster**
- **Namespace**
- **Service**

The image shows a screenshot of a web interface for configuring a SmartGroup. At the top, there is a button labeled "+ Resource Type" with a dropdown arrow. Below it, a red rectangle highlights the "Kubernetes" option, which is also labeled as a "Preview". To the right of "Kubernetes" is a trash icon. Below this, a light gray box contains the text "Matches all conditions (AND)" and a "+ Add condition" button. Inside this box, there is a dropdown menu currently showing an empty field with an upward arrow. Below the dropdown, a list of options is visible: "Cluster", "Namespace", and "Service". To the right of the dropdown menu is another trash icon. At the bottom right of the interface are "Cancel" and "Save" buttons.

+ Resource Type ▾

**Kubernetes** Preview 

Matches all conditions (AND) + Add condition

Cluster

Namespace

Service

Cancel Save

# 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



The screenshot shows a configuration interface for a SmartGroup. At the top, there is a button labeled '+ Resource Type' with a dropdown arrow. Below it, a red rectangular box highlights the text 'IPs / CIDRs'. Underneath this, there is a horizontal input field containing three entries: '10.1.20.45/32', '10.1.20.46/32', and '192.168.0.0/16'. Each entry has a small 'x' icon to its right for removal. A larger 'x' icon is at the far right of the input field. Below the input field, the text 'Supports multiple IPs and CIDRs' is displayed.

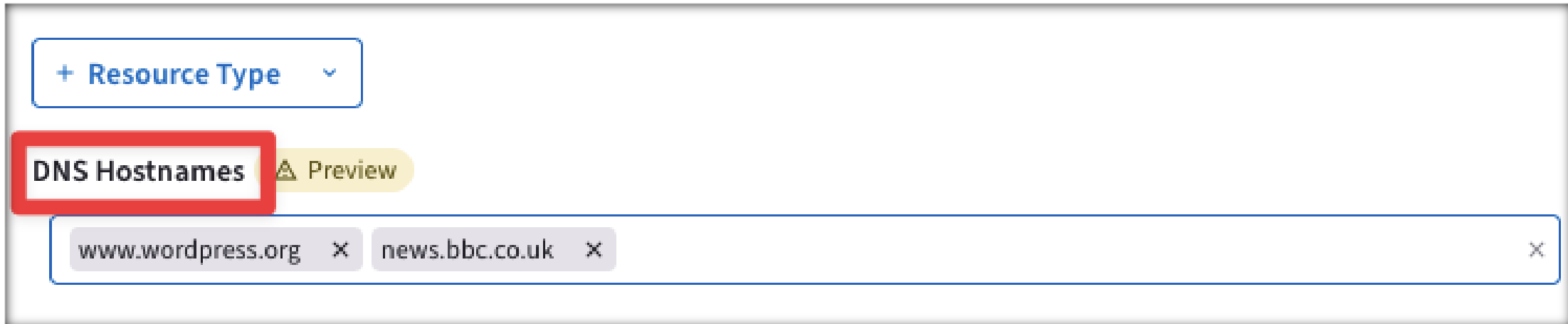
# Groups – SmartGroups (part.12)

❑ 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*.



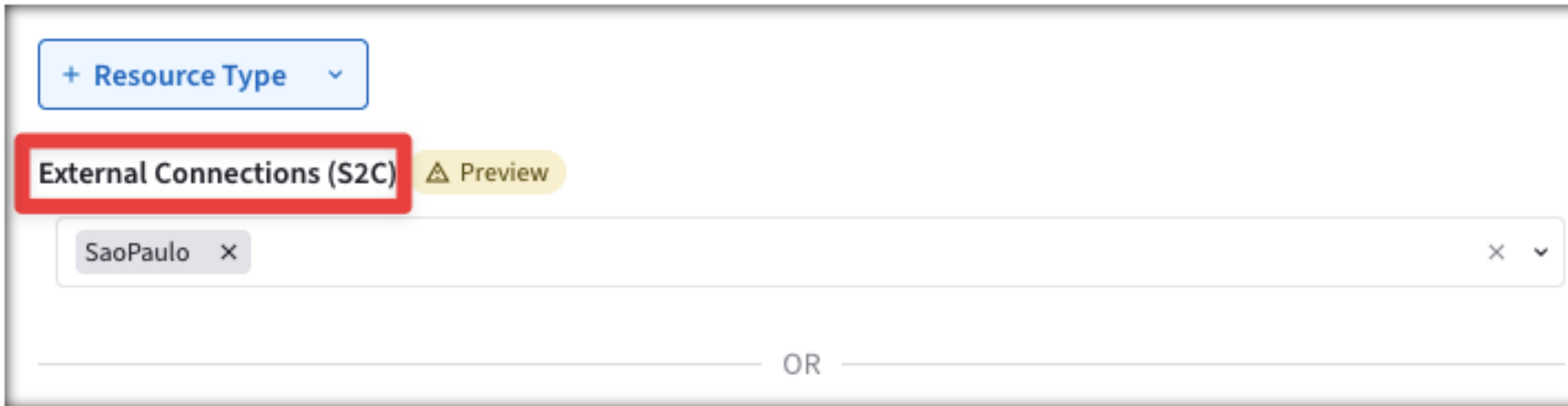
The screenshot shows a configuration interface for a SmartGroup. At the top, there is a button labeled "+ Resource Type" with a dropdown arrow. Below this, the "DNS Hostnames" tab is selected and highlighted with a red border. To the right of the tab is a "Preview" button. Below the tabs is a large text input field containing two domain names: "www.wordpress.org" and "news.bbc.co.uk". Each domain name has a small "x" icon to its right, indicating it can be removed. A larger "x" icon is at the far right of the input field.

# 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.



+ Resource Type ▾

External Connections (S2C) Preview

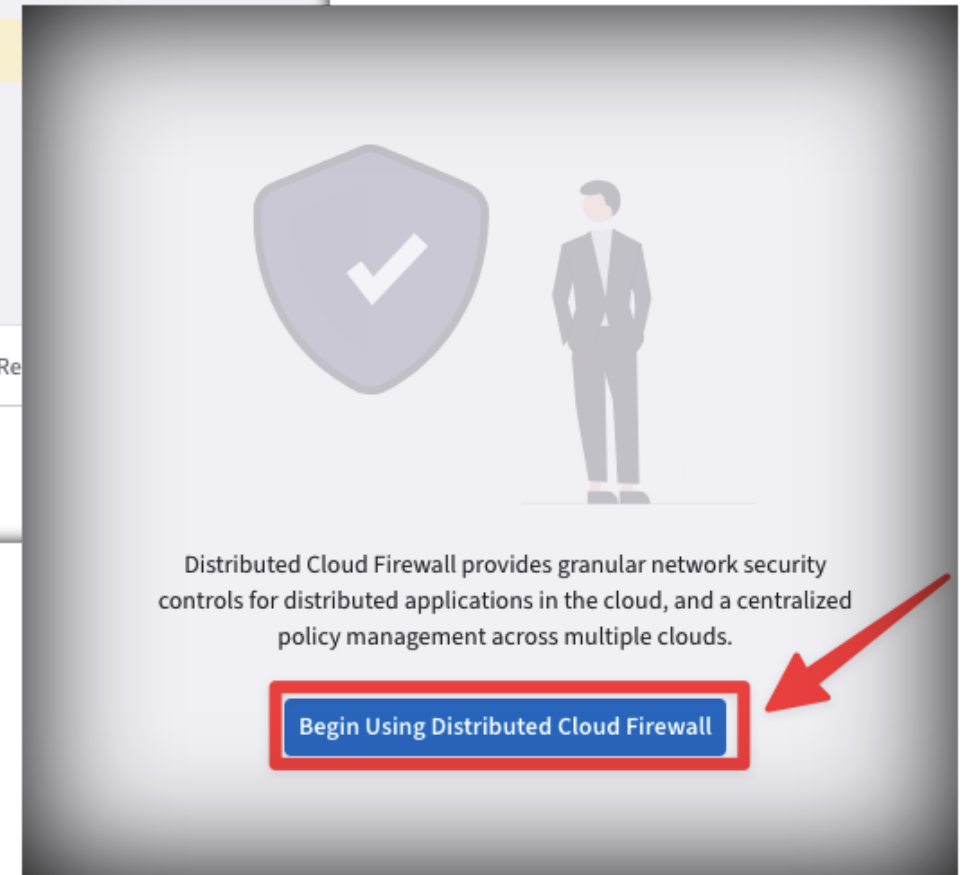
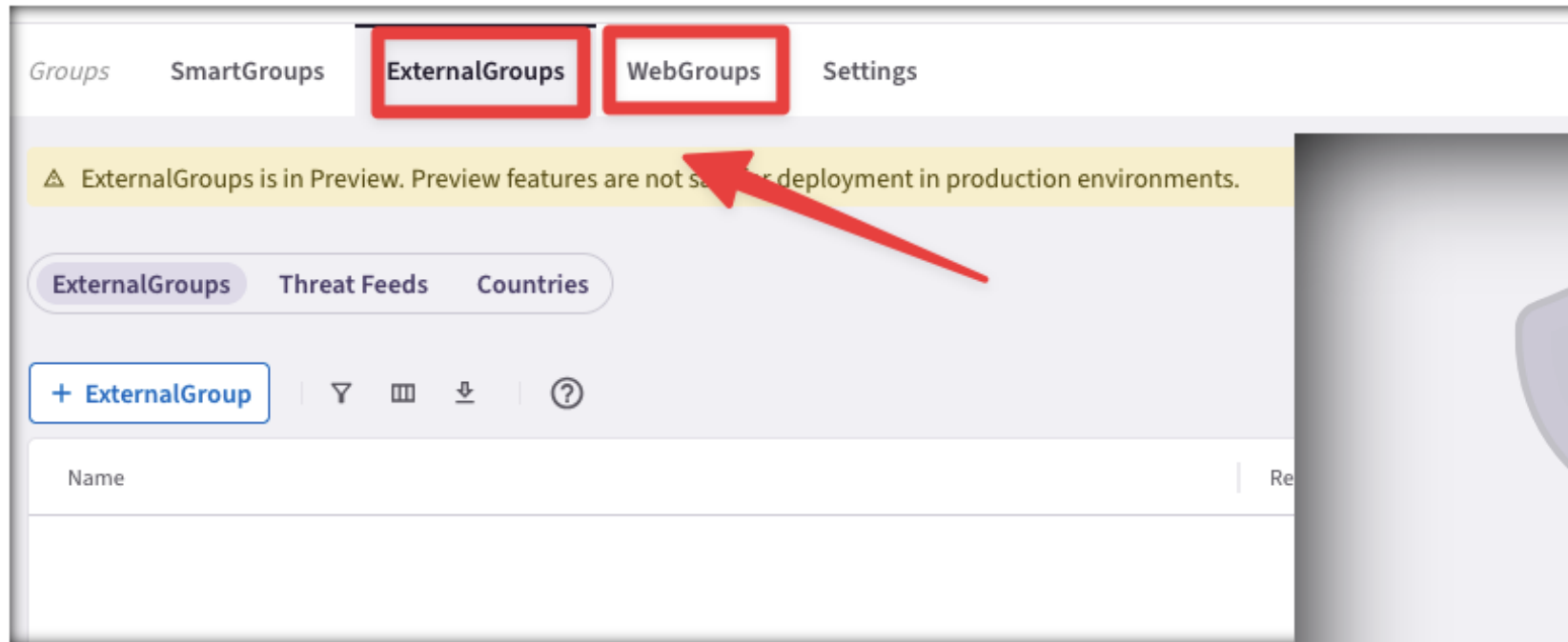
SaoPaulo X

OR



# 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

## Create ExternalGroup

Name

Azure-backup

Resource Selection

Preview (0)

+ Resource Type

Azure

Service Regions

southeastasia

Services

AzureBackup

# Groups – ExternalGroups – Github (SaaS-based service)

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

## Create ExternalGroup ?

Name

Resource Selection Preview (0) ☐

+ Resource Type ▾

**GitHub**

Services

github\_enterprise\_importer × ▾

# 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.

The screenshot shows the Aviatrix CoPilot interface. On the left is a dark sidebar with a search bar and a menu including Dashboard, Cloud Fabric, Networking, Security, Groups (highlighted with a red box), Cloud Resources, Monitor, Diagnostics, Administration, and Settings. The main content area has tabs for Groups, SmartGroups, ExternalGroups (highlighted with a red box), WebGroups, and Settings. A yellow warning banner states: "ExternalGroups is in Preview. Preview features are not safe for deployment in production environments." Below this are sub-tabs for ExternalGroups, Threat Feeds, and Countries. The ExternalGroups tab shows a table with columns Name and Rule References. The "Default ThreatGroup" is listed and highlighted with a red box, showing 0 rule references. The Threat Feeds tab is active, showing a table with columns IP Address / CIDs, Protocol, Threat Type, and Severity. It lists 11 threat feeds, all of type "Threat Feed" with "Unknown" severity. At the bottom, it states "Total 11,707 IP Addresses".

IPs / CIDs	Protocol	Threat Type	Severity
1.2.202.167/32		Threat Feed	Unknown
1.6.53.205/32		Threat Feed	Unknown
1.12.245.182/32		Threat Feed	Unknown
1.12.246.6/32		Threat Feed	Unknown
1.14.193.147/32		Threat Feed	Unknown
1.24.16.5/32		Threat Feed	Unknown
1.24.16.6/32		Threat Feed	Unknown
1.24.16.19/32		Threat Feed	Unknown
1.24.16.25/32		Threat Feed	Unknown
1.24.16.32/32		Threat Feed	Unknown
1.24.16.68/32		Threat Feed	Unknown
1.24.16.80/32		Threat Feed	Unknown
1.24.16.86/32		Threat Feed	Unknown
1.24.16.87/32		Threat Feed	Unknown

# Groups – ExternalGroups – Countries

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

GroupsSmartGroupsExternalGroupsWebGroupsSettings

⚠ ExternalGroups is in Preview. Preview features are not safe for deployment in production environments.[Learn More](#)

ExternalGroupsThreat FeedsCountries

⌵☰⬇️?

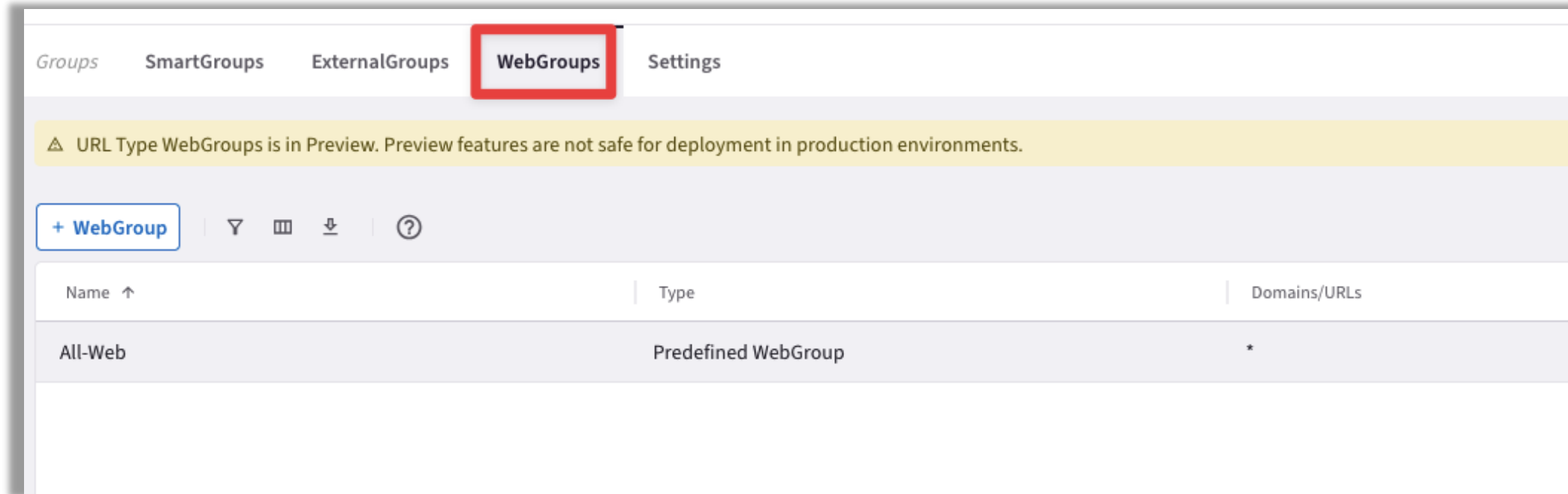
Search

Name	Rule References
<a href="#">Faroe Islands</a>	0
<a href="#">Federated States of Micronesia</a>	0
<a href="#">Fiji</a>	0
<a href="#">Finland</a>	0
<a href="#">France</a>	0
<a href="#">French Guiana</a>	0
<a href="#">French Polynesia</a>	0
<a href="#">French Southern Territories</a>	0
<a href="#">Gabon</a>	0
<a href="#">Gambia</a>	0
<a href="#">Georgia</a>	0
<a href="#">Germany</a>	0
<a href="#">Ghana</a>	0
<a href="#">Gibraltar</a>	0

# 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. This predefined WebGroup cannot be deleted.





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. [Lear...](#)

**+ 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

Type  
☒ Domains ☐ URLs Preview

Domains/URLs  
 


[Cancel](#) [Save](#)

Create WebGroup 

⚠ URL Type WebGroups is in Preview. Preview features are not safe for deployment in production environments. [Lear...](#)

Name

Type  
☐ Domains ☒ URLs Preview

Domains/URLs  
 

[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.

CoPilot

Dashboard

Cloud Fabric

Networking

Security

Groups

Cloud Resources

Monitor

Diagnostics 1

AppIQ

Diagnostics Tools

Cloud Routes 2

Administration

Settings

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

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	
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	
azure-west-us-spoke1	azure-west-us-spoke1 (192.168.1.0/24)	Up	Up	1	6	
azure-west-us-spoke2	azure-west-us-spoke2 (192.168.2.0/24)	Up	Unknown	0	5	
gcp-us-central1-spoke1	gcp-us-central1-spoke1 (172.16.1.0/24, 172.16.2.0/24)	Up	Up	1	5	
gcp-us-central1-transit	gcp-us-central1-transit (172.16.10.0/23)	Up	Up	3	8	
azure-west-us-transit	azure-west-us-transit (192.168.10.0/23)	Up	Up	3	11	
onprem-pod100-edge-1	onprem-pod100-edge-site ()	Up	Unknown	0	7	

# 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
- ❑ Gateways routes represent the “more specific” routes injected by the Aviatrix Controller using SD-Networking

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-062df7dcc55b4e75) (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-062df7dcc55b4e75) (10.0.12.0/23)	rtb-02313d032d812cc55	4	Up																				
<table><tr><th>ROUTE</th><th>GATEWAY</th><th>TARGET</th><th></th></tr><tr><td>10.0.12.0/23</td><td>local</td><td>local</td><td>Active</td></tr><tr><td>192.168.0.0/16</td><td>aviatrix-aws-us-east-1-spoke1</td><td>i-08f996a30c4f3e781</td><td>Active</td></tr><tr><td>172.16.0.0/12</td><td>aviatrix-aws-us-east-1-spoke1</td><td>i-08f996a30c4f3e781</td><td>Active</td></tr><tr><td>10.0.0.0/8</td><td>aviatrix-aws-us-east-1-spoke1</td><td>i-08f996a30c4f3e781</td><td>Active</td></tr></table>					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
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-062df7dcc55b4e75) (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-062df7dcc55b4e75) (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-062df7dcc55b4e75) (10.0.12.0/23)	rtb-048ac2d2ebeb7c70a	5	Up																				
aws-us-east-1-transit-Public-rtb	aws-us-east-1-transit(vpc-0cc023ddfd960fb) (10.0.20.0/23)	rtb-0cdf52348c88a7329	2	Up																				
aws-us-east-1-transit-Private-rtb	aws-us-east-1-transit(vpc-0cc023ddfd960fb) (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   Gateway Routes   VPC/VNet Routes <b>External Connections</b> BGP Info								
<div> <span>▼</span> <span>☰</span> <span>⬇</span> </div>								
Name	VPC/VNet	BGP Status		Status	Tunnel Status		HA Status	
<div> <span>▼</span> onprem-pod100-edge-1-to-onprem-pod100-host-vm-1 </div>	()	<span>✔</span> Enabled		<span>⬆</span> Up	<span>⬆</span> Up		<span>⛔</span> Disabled	
Tunnel Name	Gateway	IP Address	Peer IP Address	Tunnel Protocol	Cert Based External	Tunnel Status	HA Status	Modified
tunnel-onprem-pod100-edge-1	onprem-pod100-edge-1	10.40.251.2	10.40.251.1	N/A(LAN)		<span>⬆</span> Up	<span>✔</span> Active	

- ### BGP Map
- 
- The BGP Map diagram illustrates the following connections:
- AS 64900** (blue router icon) is connected to **onprem-pod100-edge-1-to-onprem-pod100-host-vm-1** (green box) via a green line labeled **10.40.251.1**.
  - onprem-pod100-edge-1-to-onprem-pod100-host-vm-1** (green box) is connected to **AS 64581** (blue box icon) via a green line labeled **10.40.251.2**.
  - AS 64581** (blue box icon) is connected to **onprem-pod100-edge-1** (red router icon) via a blue line.



AVIATRIX®

# AVIATRIX CLOUD COFFE BREAK





**Next: Tenet-2 Distributed and  
Embedded Security**