Cloud Resource Identification, Inventory and Grouping

Topics Covered

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

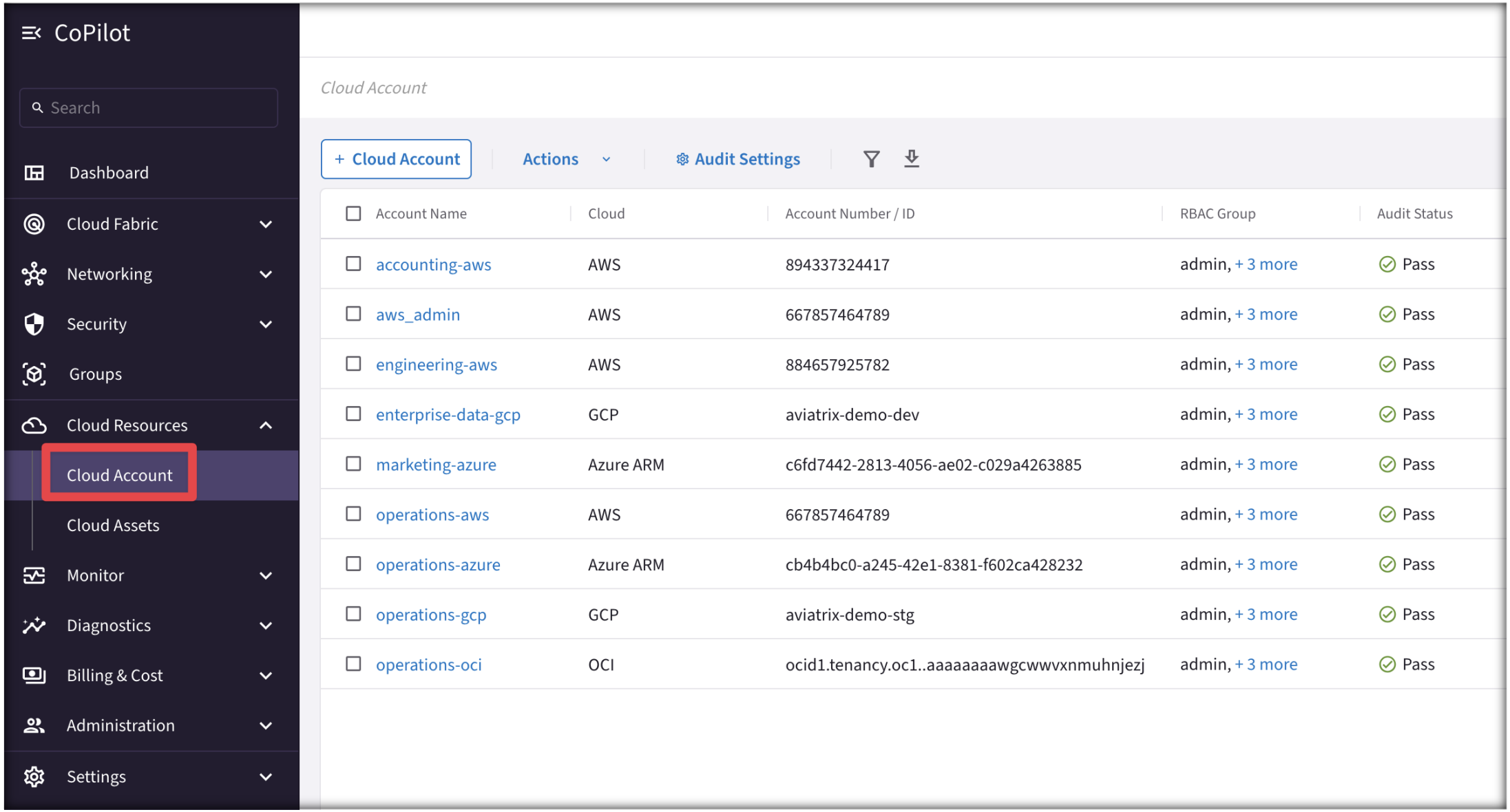
The enterprise collects as much information as possible about the current state of assets, network infrastructure and communications and uses it to improve its security posture.

- Asset Inventory using Aviatrix CoPilot Asset Inventory
- Resources identification using tags and other attributes
- Kubernetes Clusters discovery
- Resource Grouping using Aviatrix SmartGroups

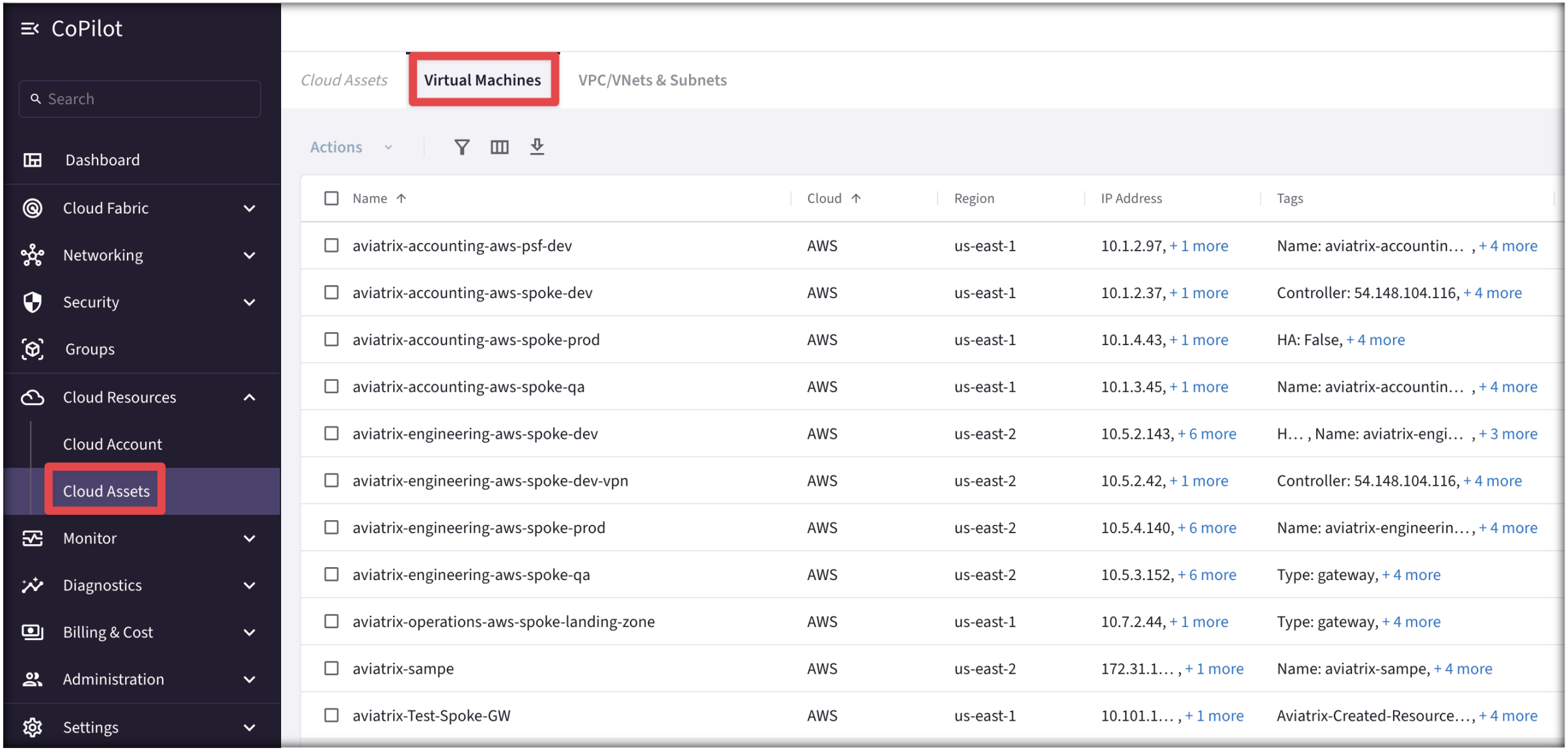
Use Cases:

Zero Trust Network Access (Cloud Firewalling	Secure B2B Connectivity	Secure High-Performance Data Connectivity for LLMS	Secure High-Performance Datacenter Edge	Cloud Visibility and Tooling

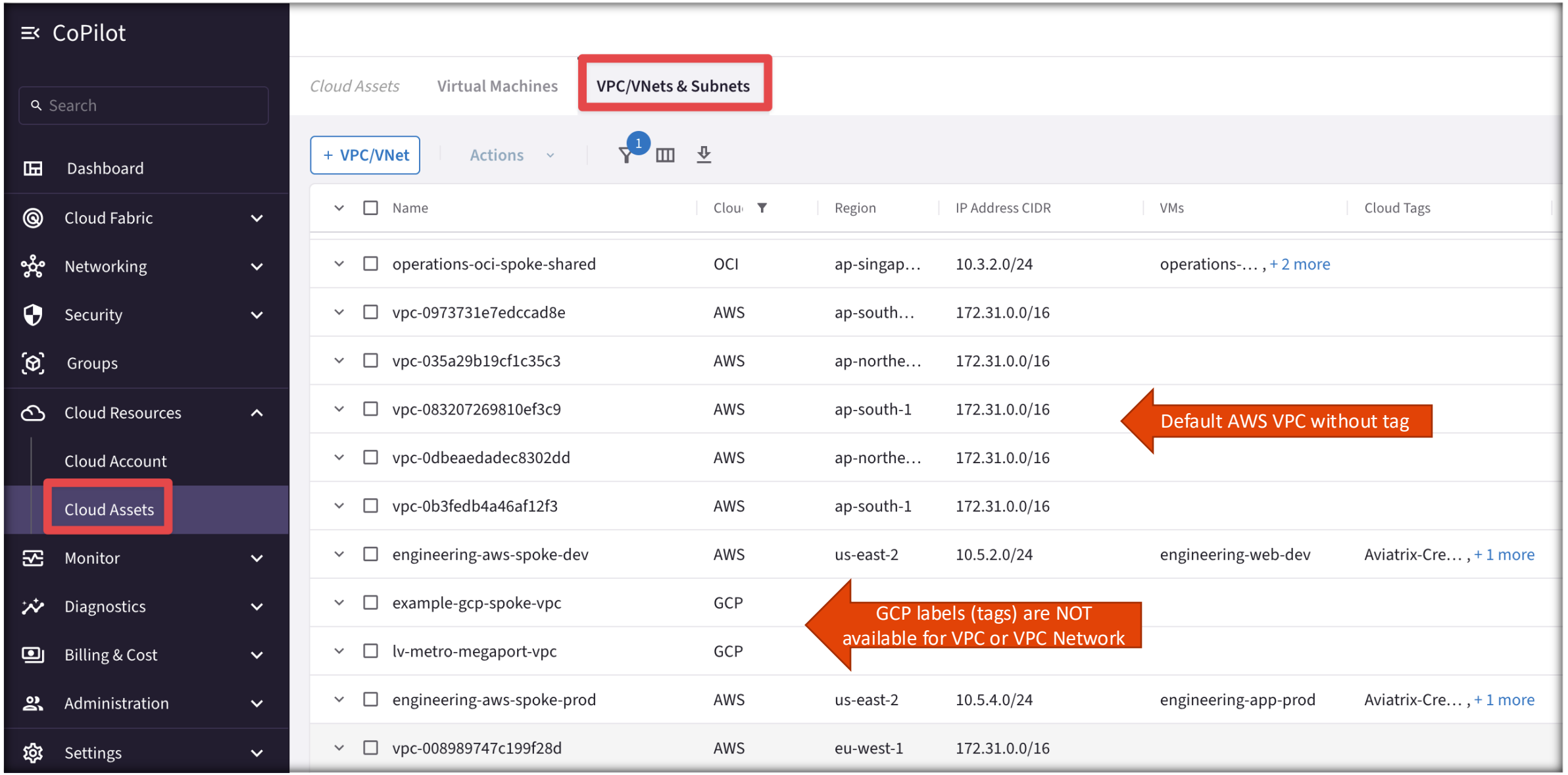
CSP Cloud Accounts Inventory



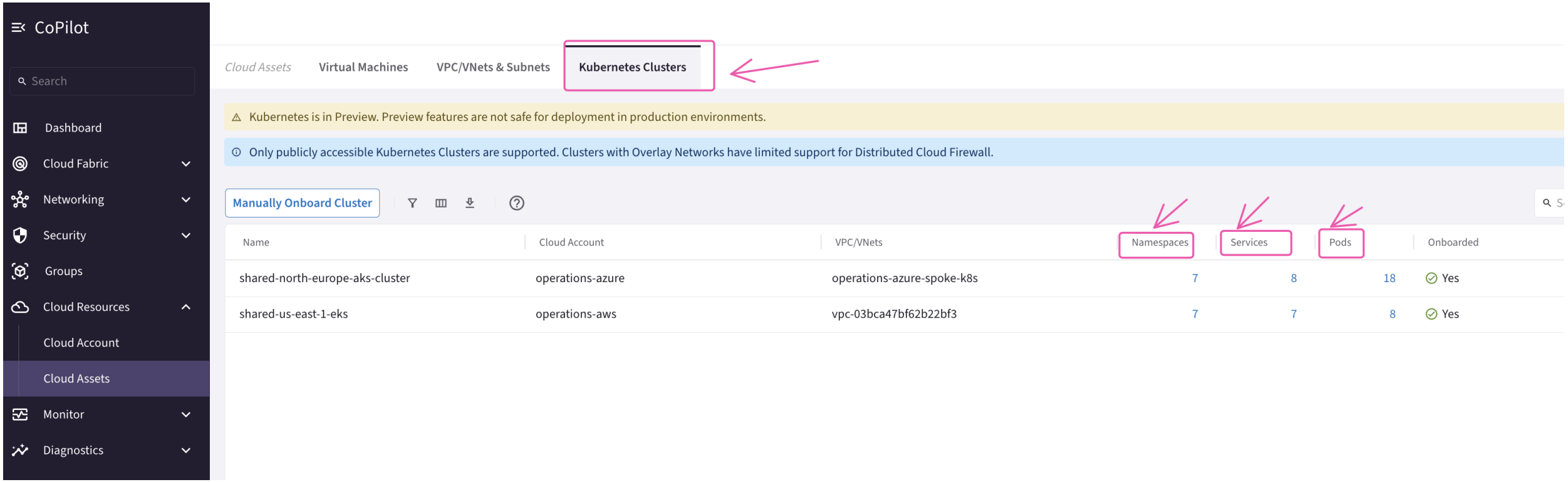
CSP Assets Inventory



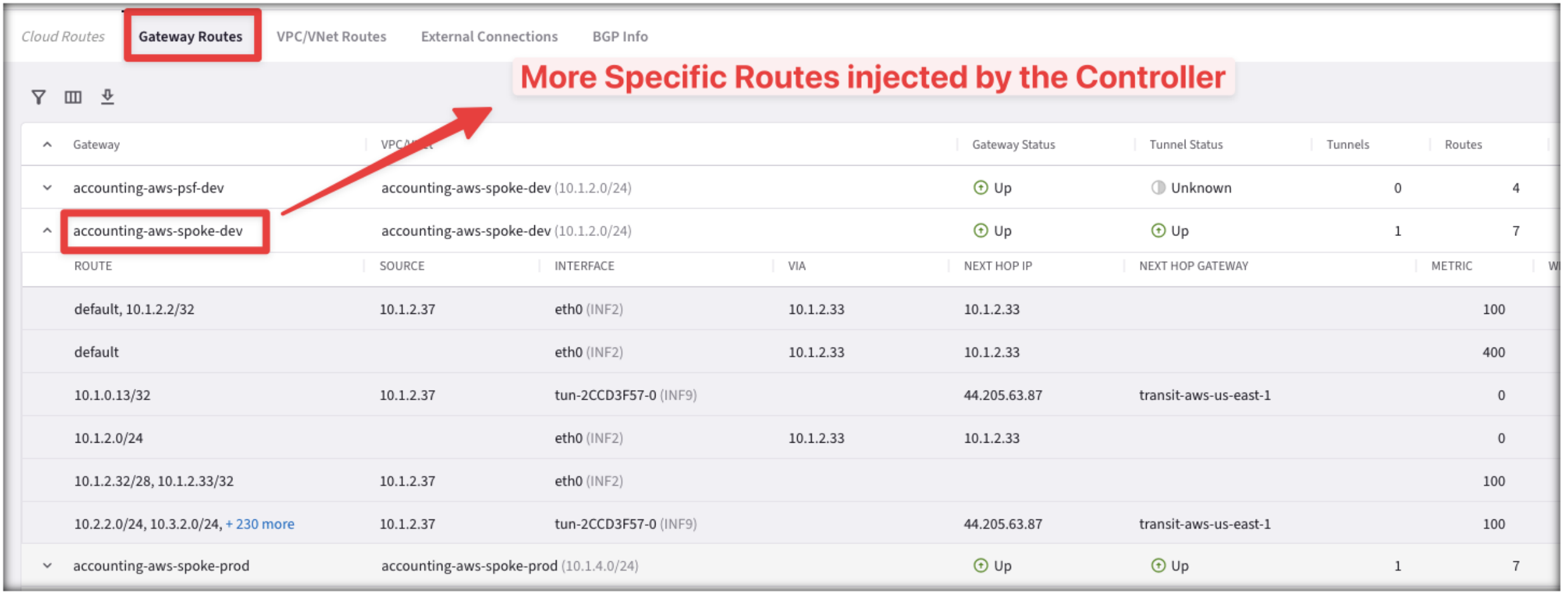
CSP Assets Inventory



Kubernetes Assets Inventory



Global Routing Inventory (i.e Cloud Routes): Aviatrix Gateways' RTBs

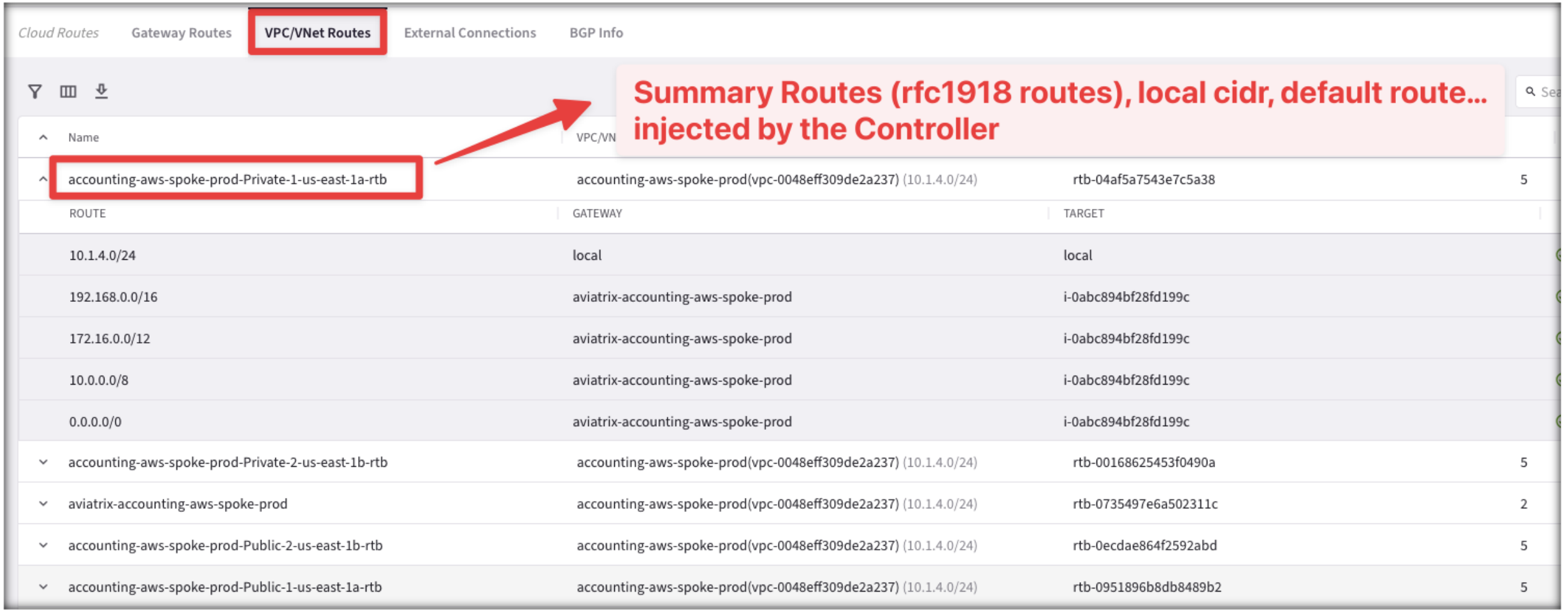


Gateway	VPC/VNet	Gateway Status	Tunnel Status	Tunnels	Routes
accounting-aws-psf-dev	accounting-aws-spoke-dev (10.1.2.0/24)	Up	Unknown	0	4
accounting-aws-spoke-dev	accounting-aws-spoke-dev (10.1.2.0/24)	Up	Up	1	7

ROUTE	SOURCE	INTERFACE	VIA	NEXT HOP IP	NEXT HOP GATEWAY	METRIC
default, 10.1.2.2/32	10.1.2.37	eth0 (INF2)	10.1.2.33	10.1.2.33		100
default		eth0 (INF2)	10.1.2.33	10.1.2.33		400
10.1.0.13/32	10.1.2.37	tun-2CCD3F57-0 (INF9)		44.205.63.87	transit-aws-us-east-1	0
10.1.2.0/24		eth0 (INF2)	10.1.2.33	10.1.2.33		0
10.1.2.32/28, 10.1.2.33/32	10.1.2.37	eth0 (INF2)				100
10.2.2.0/24, 10.3.2.0/24, + 230 more	10.1.2.37	tun-2CCD3F57-0 (INF9)		44.205.63.87	transit-aws-us-east-1	100

accounting-aws-spoke-prod	accounting-aws-spoke-prod (10.1.4.0/24)	Up	Up	1	7

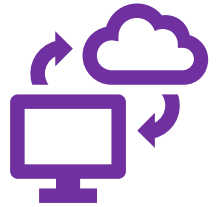
Global Routing Inventory (i.e Cloud Routes): CSPs' Routers RTBs



Aviatrix Smart Group

An Aviatrix Smart Group identifies a group of resources with similar policy requirements confined in the same logical container.

- The members of a SmartGroup can be classified using *different* methods:
  - CSP Tag
  - Subnets
  - VPC/Vnets
  - Kubernetes
  - Hostnames
  - External Connections (S2C)



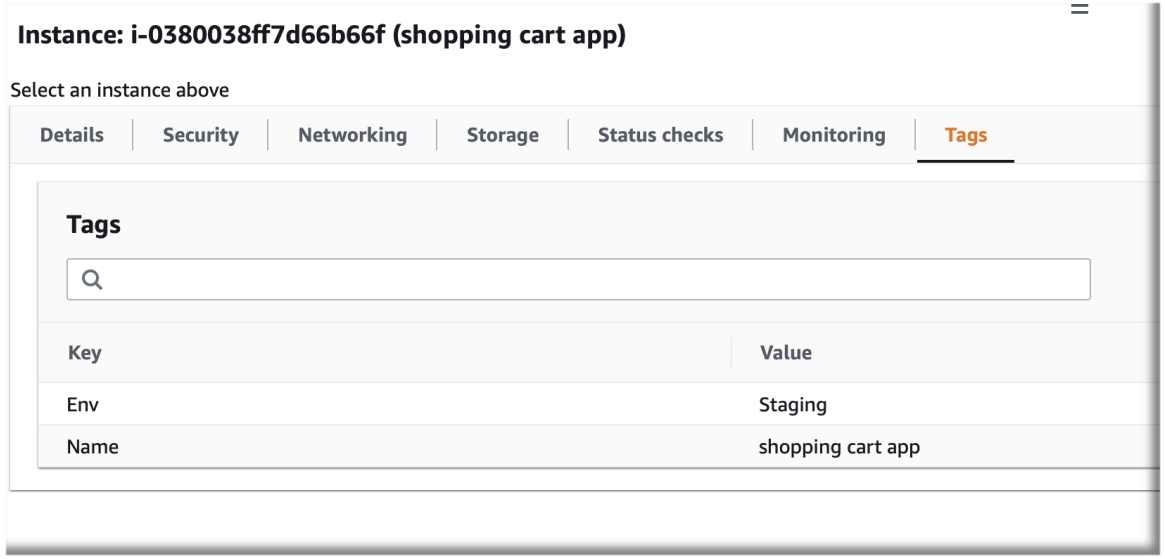
Classification Methods

CSP Tags (recommended)

- Tags are assigned to:
  - Instance
  - VPC/VNET
  - Subnet
- Tags are {Key, Value} pairs
- Example: A shopping cart app can be tagged with:

  {Key: Env, Value: Staging}

  {Key: Name, Value: Shopping cart app}



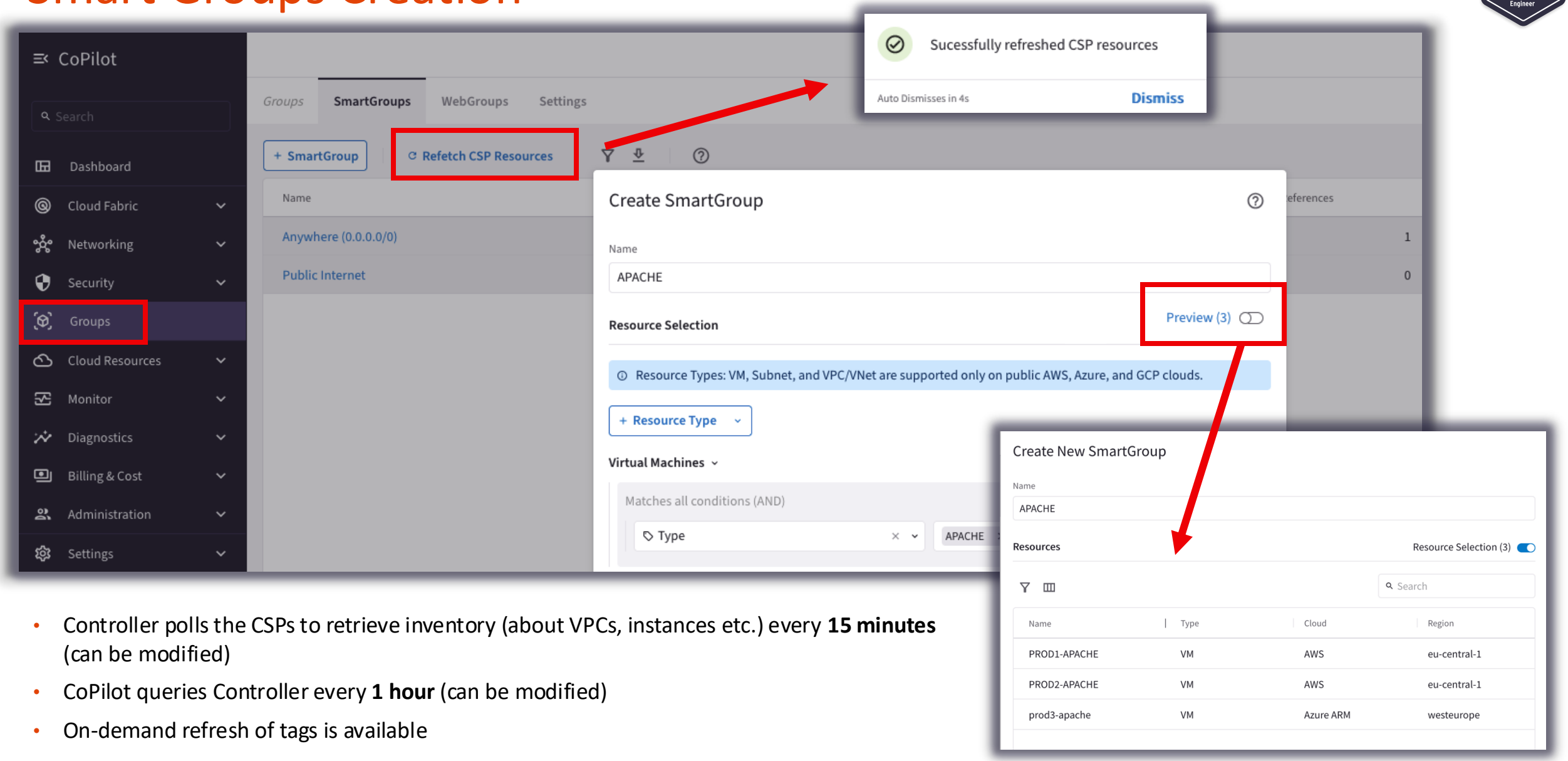
Resource attribute

- Region Name, Account Name

IP Prefixes

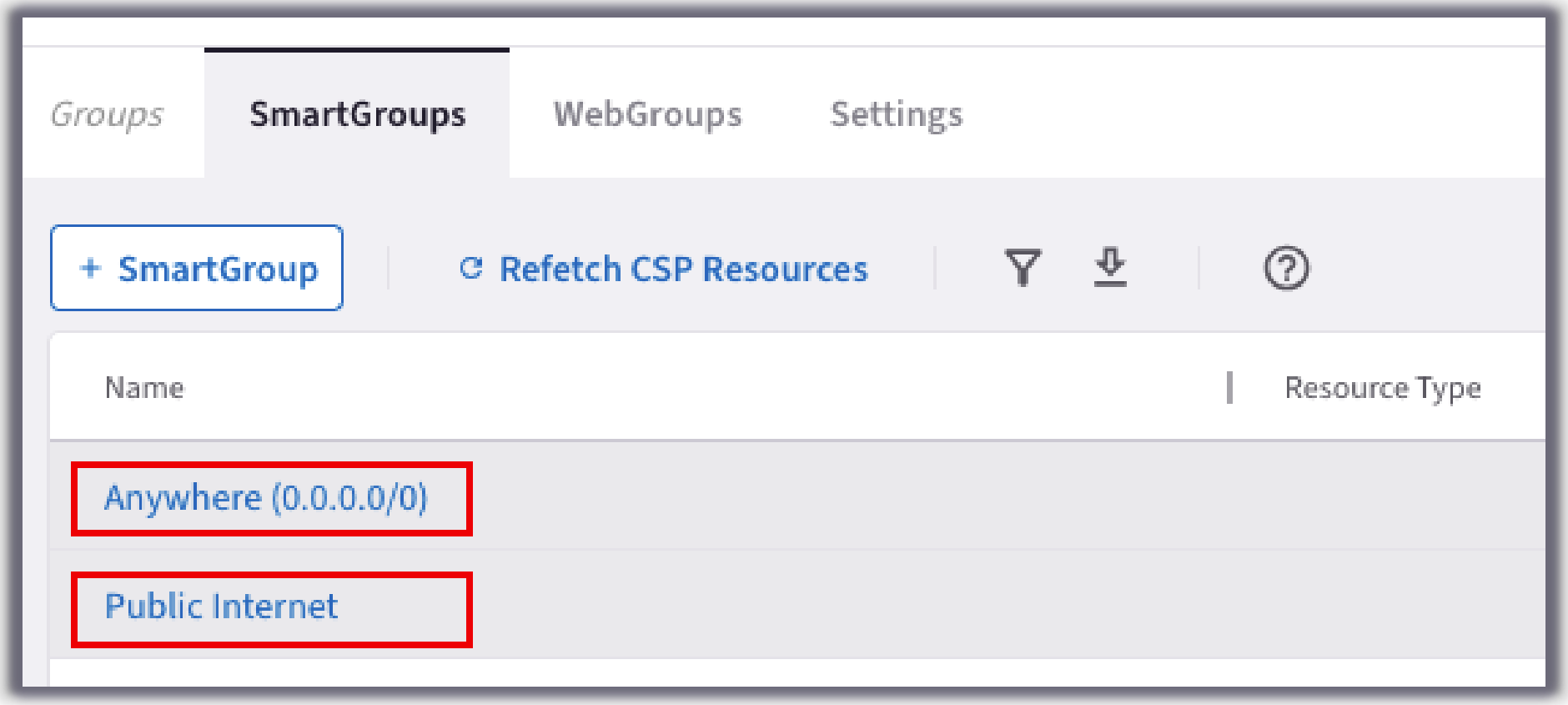
- CIDR

Smart Groups Creation



- 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

Pre-defined Smart Groups



- **Anywhere (0.0.0.0/0)** → RFC1918 routes + Default Route (IGW)
- **Public Internet** → Default Route (IGW)

“Public Internet” SmartGroups Members (31 CIDRS Members)

Type	SmartGroups	IP/CIDRs
CIDR	Public Internet	0.0.0.0/5
CIDR	Public Internet	8.0.0.0/7
CIDR	Public Internet	11.0.0.0/8
CIDR	Public Internet	12.0.0.0/6
CIDR	Public Internet	16.0.0.0/4
CIDR	Public Internet	32.0.0.0/3
CIDR	Public Internet	64.0.0.0/2
CIDR	Public Internet	128.0.0.0/3
CIDR	Public Internet	160.0.0.0/5
CIDR	Public Internet	168.0.0.0/6
CIDR	Public Internet	172.0.0.0/12

Total 31 Destination Entities

Type	SmartGroups	IP/CIDRs
CIDR	Public Internet	172.0.0.0/12
CIDR	Public Internet	172.32.0.0/11
CIDR	Public Internet	172.64.0.0/10
CIDR	Public Internet	172.128.0.0/9
CIDR	Public Internet	173.0.0.0/8
CIDR	Public Internet	174.0.0.0/7
CIDR	Public Internet	176.0.0.0/4
CIDR	Public Internet	192.0.0.0/9
CIDR	Public Internet	192.128.0.0/11
CIDR	Public Internet	192.160.0.0/13
CIDR	Public Internet	192.169.0.0/16

Total 31 Destination Entities

Type	SmartGroups	IP/CIDRs
CIDR	Public Internet	192.169.0.0/16
CIDR	Public Internet	192.170.0.0/15
CIDR	Public Internet	192.172.0.0/14
CIDR	Public Internet	192.176.0.0/12
CIDR	Public Internet	192.192.0.0/10
CIDR	Public Internet	193.0.0.0/8
CIDR	Public Internet	194.0.0.0/7
CIDR	Public Internet	196.0.0.0/6
CIDR	Public Internet	200.0.0.0/5
CIDR	Public Internet	208.0.0.0/4
CIDR	Public Internet	224.0.0.0/3

Total 31 Destination Entities

“Anywhere” SmartGroups Members (1 CIDR Member behind the scene)

Type	SmartGroups	IP/CIDRs
CIDR	Anywhere (0.0.0.0/0)	0.0.0.0/0

Total 1 Destination Entity

Asset Inventory with SmartGroups

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

Actions

Name	Cloud	Region	IP Address	CSP Tags	Aviatrix Managed	SmartGroups
dc-metro-equinix-host-vm-1	GCP	us-west1	10.50.25… , + 1 more		No	
dc-metro-equinix-test-vm	GCP	us-west1	10.50.25… , + 1 more		No	
engineering-app-dev	AWS	us-east-2	10.5.2.10	Department: e… , + 8 more	Yes	Dev, dev
engineering-app-prod	AWS	us-east-2	10.5.4.10	Department: e… , + 8 more	Yes	prod
engineering-app-qa	AWS	us-east-2	10.5.3.10	Division: Soluti… , + 8 more	Yes	qa
enterprise-data-dev	GCP	us-west1	10.4.2.10	environment: d… , + 8 more	No	dev-data
enterprise-data-gcp-spok…	GCP	us-west1	10.4.2.2, + 1 more		Gateways	
enterprise-data-gcp-spok…	GCP	us-west1	10.4.4.2, + 1 more		Gateways	
enterprise-data-gcp-spok…	GCP	us-west1	10.4.3.2, + 1 more		Gateways	
enterprise-data-prod	GCP	us-west1	10.4.4.10	infrastructure: … , + 8 more	No	prod-data
enterprise-data-qa	GCP	us-west1	10.4.3.10	terraform: true, + 8 more	No	qa-data
gcp-workload	GCP	us-west1	10.4.2.10	department: FF… , + 6 more	No	

Aviatrix Certified Engineer (ACE)
https://aviatrix.com/ACE

COMMUNITY
https://community.aviatrix.com