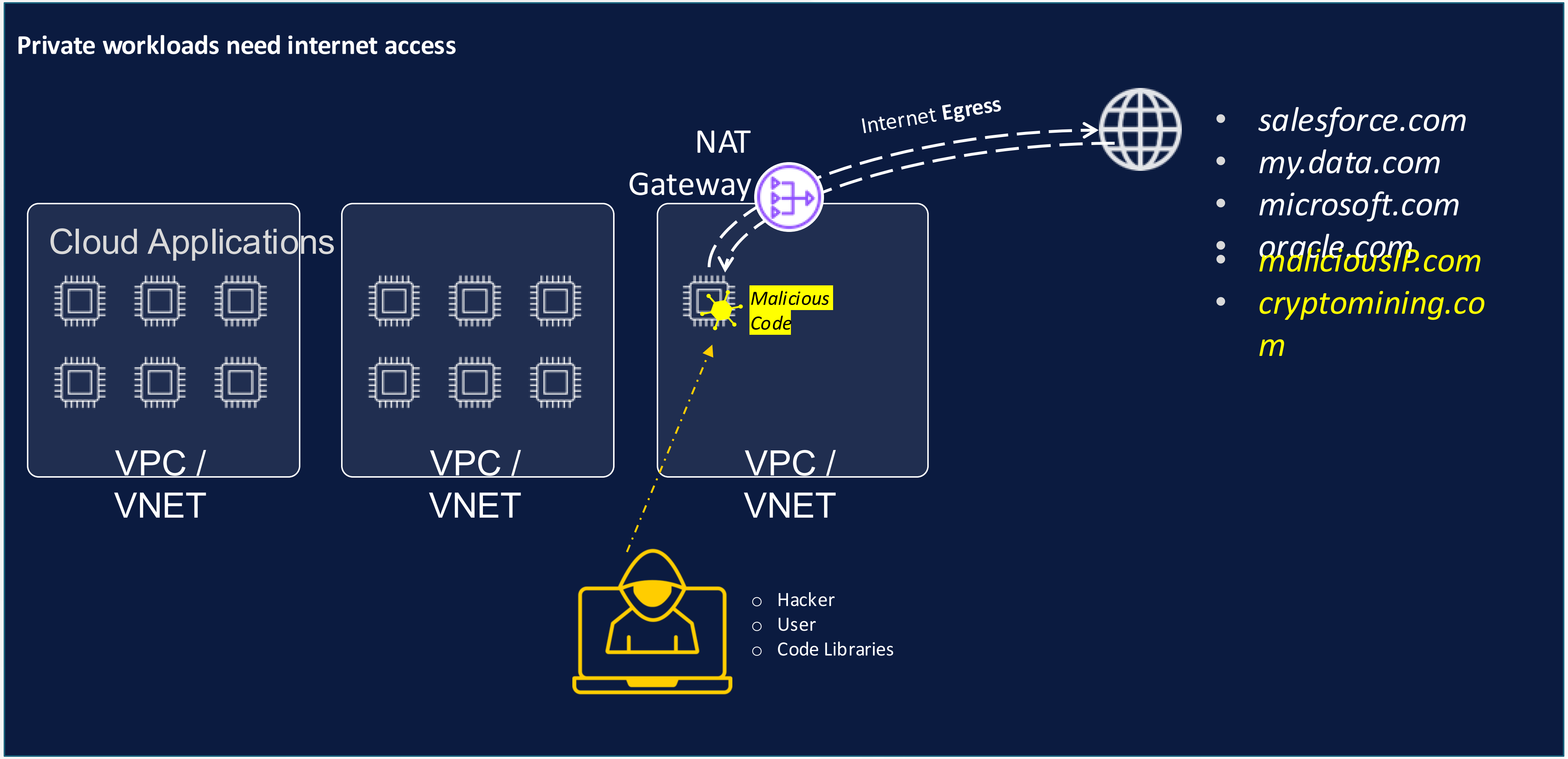
Aviatrix Cloud Firewall (Secure Cloud Egress)

AVIATRIX DCF FOR SECURE CLOUD EGRESS

Cloud Perimeter Security Basics

- SaaS integration
- Patching
- Updates



Private workloads need internet access

- *salesforce.com*
- *my.data.com*
- *microsoft.com*
- *oracle.com*
- *maliciousIP.com*
- *cryptomining.co m*

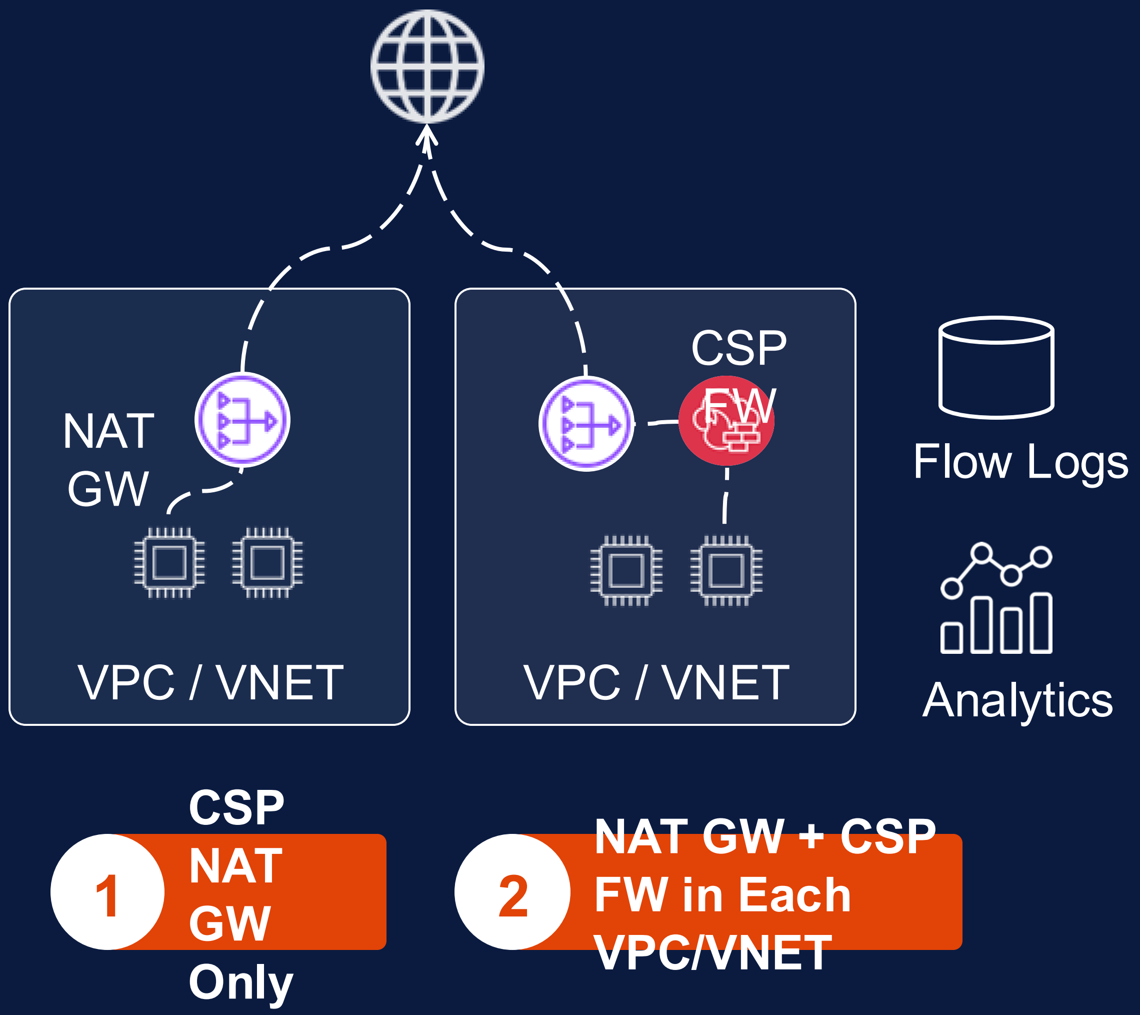
- Hacker
- User
- Code Libraries

Default Architectural Options

1. CSP NAT GW Only
2. NAT GW + CSP FW in Each VPC/VNET

Challenges

- Limited visibility
- High data-processing costs
- Log storage and analytics costs
- No centralized intelligence
- Not multi-cloud capable

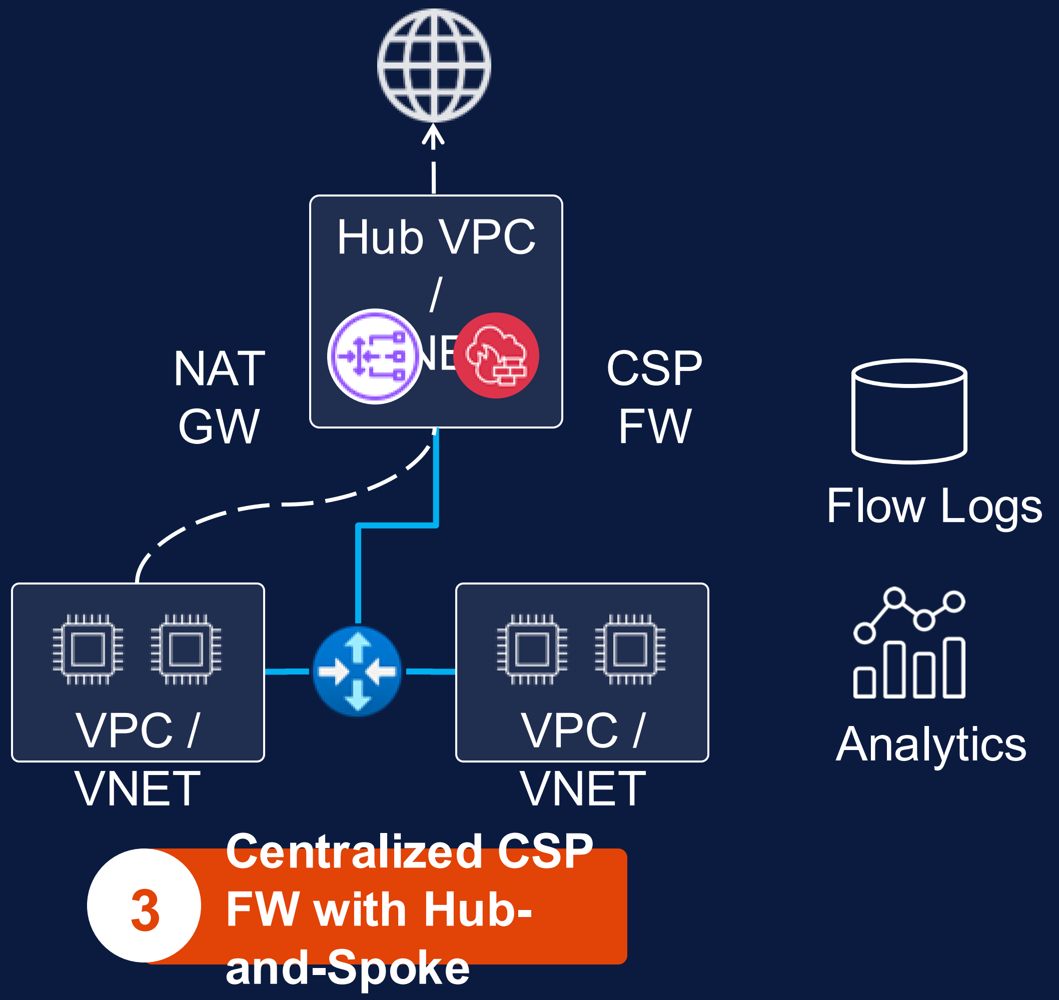


Default Architectural Options

3. Centralized CSP FW with Hub-and-Spoke

Challenges

- Limited visibility
- High data-processing costs
- Log storage and analytics costs
- No intelligence on new resources
- Cannot enforce encryption of data in transit
- Additional troubleshooting issues
- Not multi-cloud capable



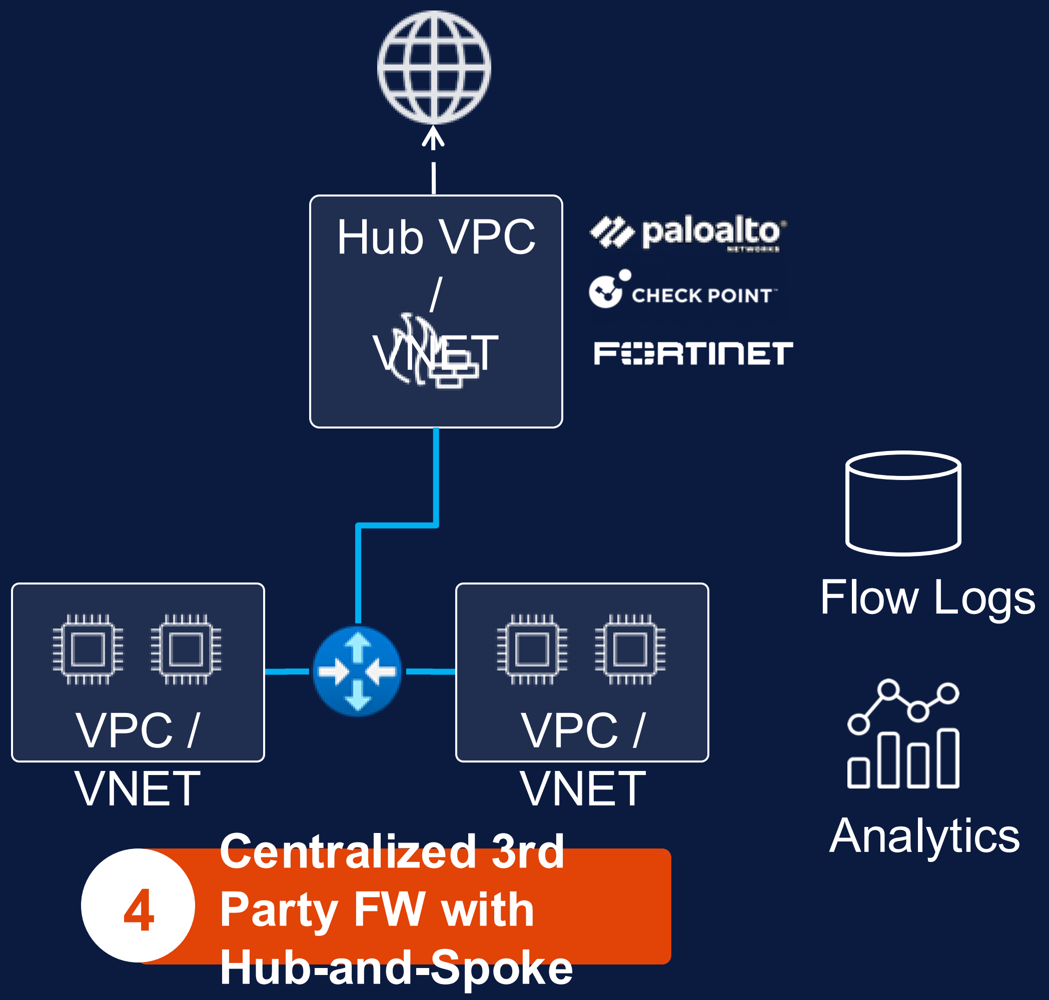
aviatrix

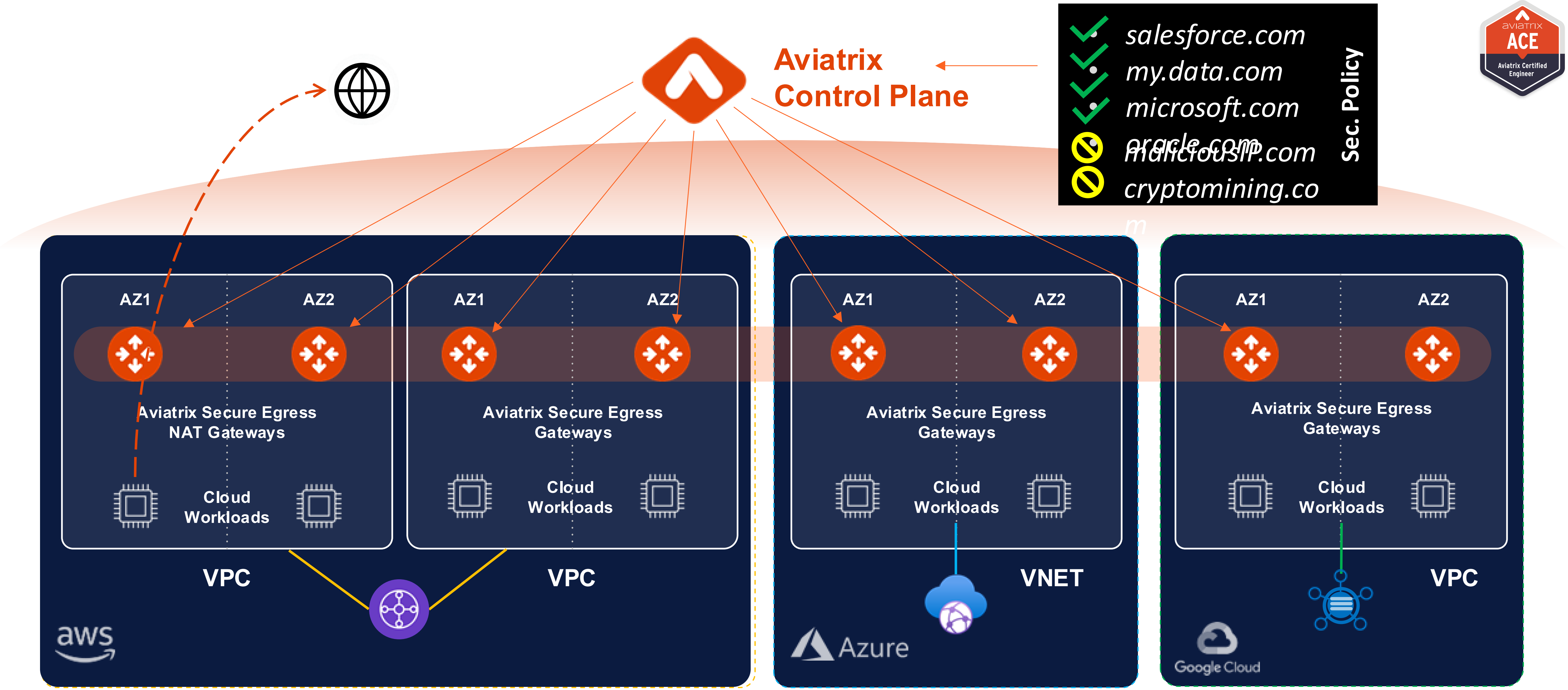
Default Architectural Options

4. Centralized 3rd Party Firewall w/ Hub-and-Spoke

Challenges

- Firewalls not built for cloud: Operational complexity
- Cloud Ops < > Sec Ops Friction
- No centralized network & security intelligence
- Additional troubleshooting issues
- Not multi-cloud deployable





Aviatrix
Control Plane

salesforce.com
my.data.com
microsoft.com
oracle.com
maliciousIP.com
cryptomining.co
m

Sec. Policy

AZ1 AZ2

Aviatrix Secure Egress
NAT Gateways

Cloud
Workloads

VPC

AZ1 AZ2

Aviatrix Secure Egress
Gateways

Cloud
Workloads

VPC

aws

AZ1 AZ2

Aviatrix Secure Egress
Gateways

Cloud
Workloads

VNET

Azure

AZ1 AZ2

Aviatrix Secure Egress
Gateways

Cloud
Workloads

VPC

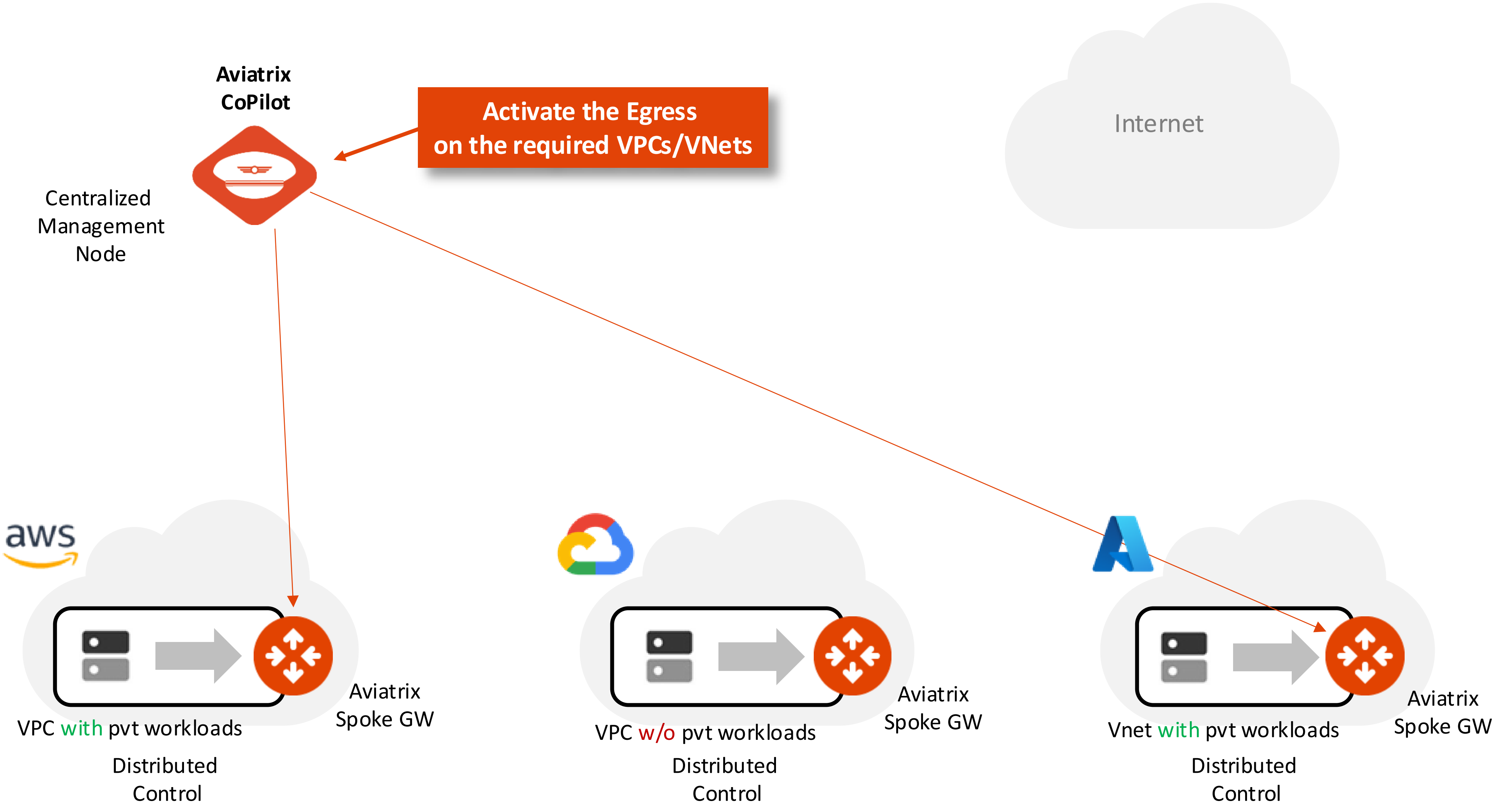
Google Cloud

Distributed Perimeter

1:1 Replacement of NAT GW

Centralized Management, Visibility, and Control

Aviatrix Cloud Perimeter Security

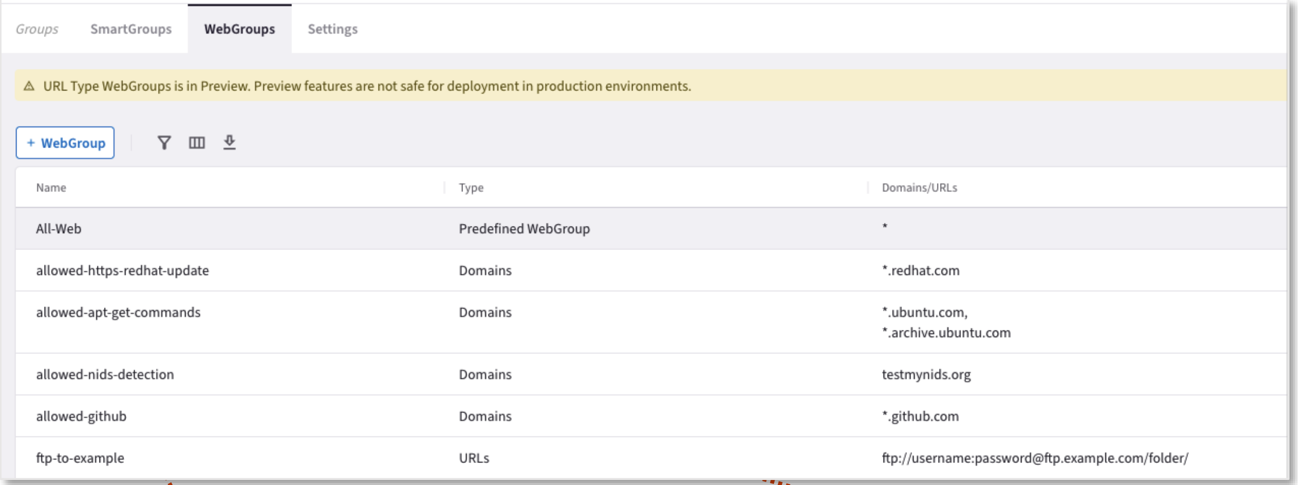


Aviatrix Cloud Perimeter Security

Aviatrix CoPilot

Centralized Management Node

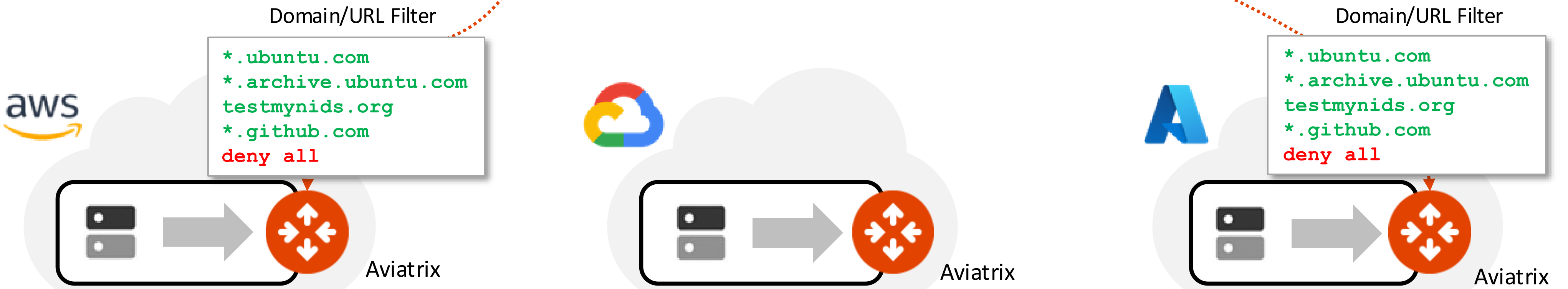
Egress Filtering Policies with **WebGroups** inserted into **DCF rules**



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

Name	Type	Domains/URLs
All-Web	Predefined WebGroup	*
allowed-https-redhat-update	Domains	*.redhat.com
allowed-apt-get-commands	Domains	*.ubuntu.com, *.archive.ubuntu.com
allowed-nids-detection	Domains	testmynids.org
allowed-github	Domains	*.github.com
ftp-to-example	URLs	ftp://username:password@ftp.example.com/folder/

Internet



Domain/URL Filter

```
*.ubuntu.com
*.archive.ubuntu.com
testmynids.org
*.github.com
deny all
```

VPC with pvt workloads

Aviatrix Spoke GW

Distributed Control

VPC w/o pvt workloads

Aviatrix Spoke GW

Distributed Control

Domain/URL Filter

```
*.ubuntu.com
*.archive.ubuntu.com
testmynids.org
*.github.com
deny all
```

Vnet with pvt workloads

Aviatrix Spoke GW

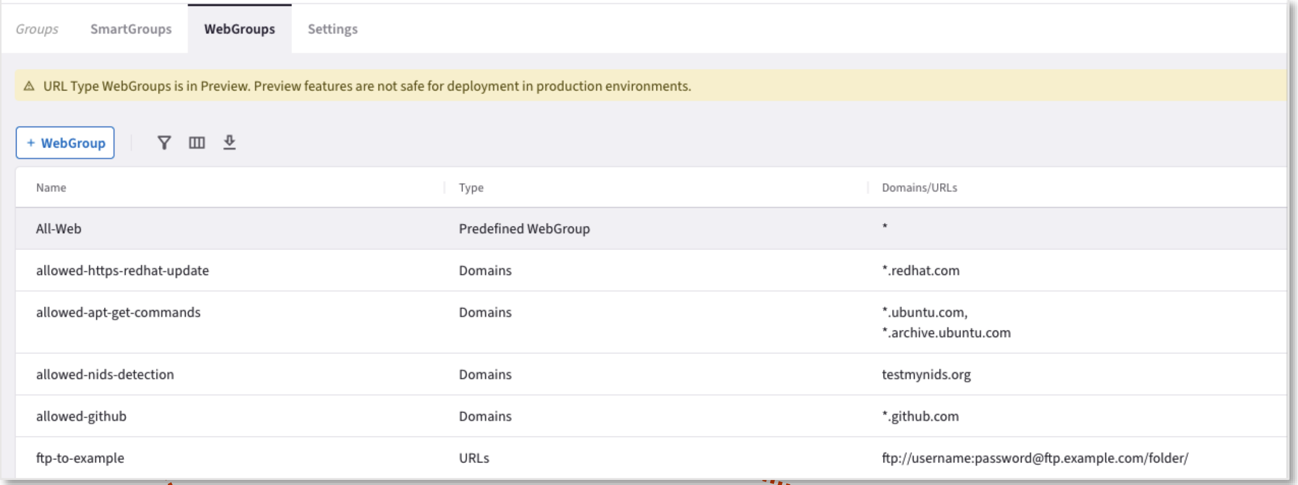
Distributed Control

Aviatrix Cloud Perimeter Security

Aviatrix CoPilot

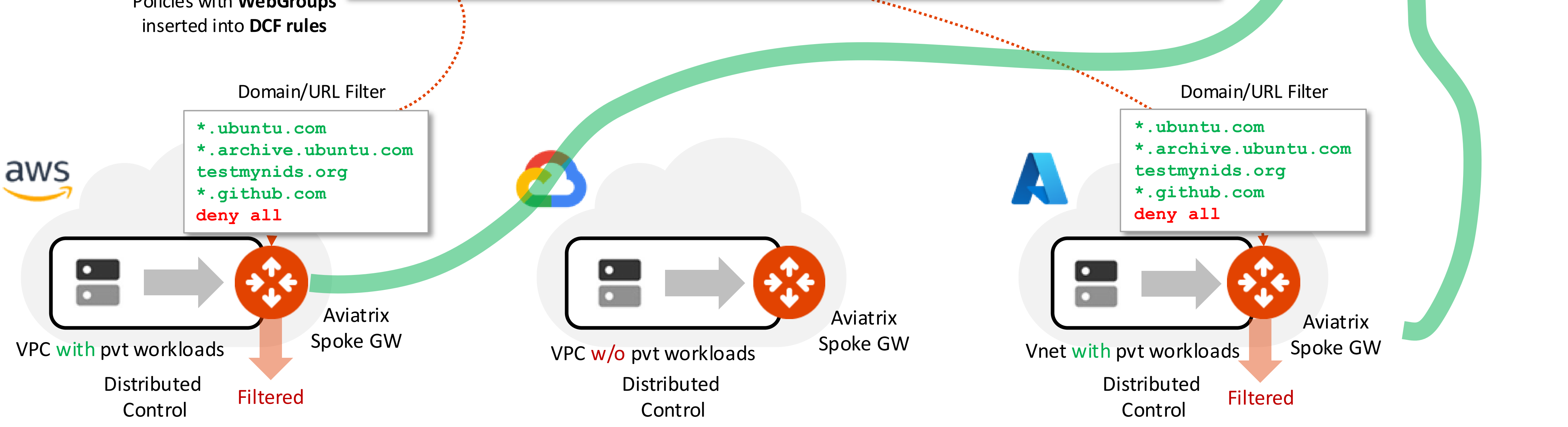
Centralized Management Node

Egress Filtering Policies with **WebGroups** inserted into **DCF rules**



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

Name	Type	Domains/URLs
All-Web	Predefined WebGroup	*
allowed-https-redhat-update	Domains	*.redhat.com
allowed-apt-get-commands	Domains	*.ubuntu.com, *.archive.ubuntu.com
allowed-nids-detection	Domains	testmynids.org
allowed-github	Domains	*.github.com
ftp-to-example	URLs	ftp://username:password@ftp.example.com/folder/



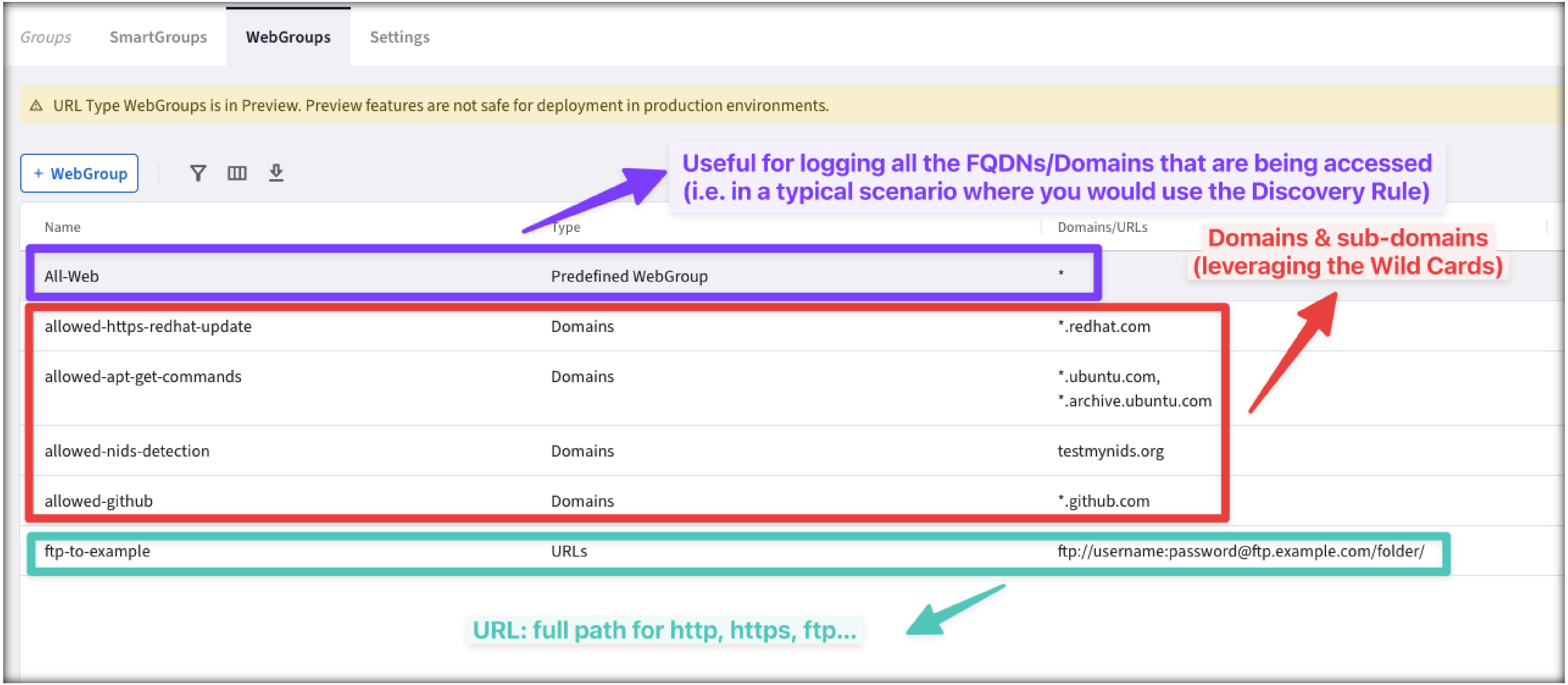
Domain/URL Filter

```
*.ubuntu.com
*.archive.ubuntu.com
testmynids.org
*.github.com
deny all
```

Domain/URL Filter

```
*.ubuntu.com
*.archive.ubuntu.com
testmynids.org
*.github.com
deny all
```

WebGroups Definition



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

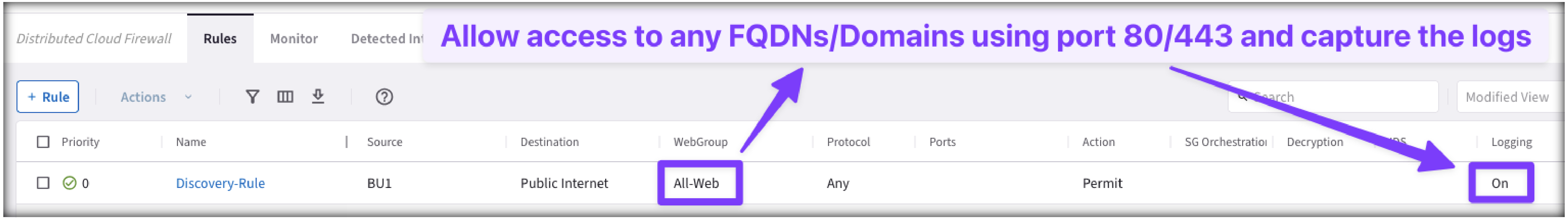
Name	Type	Domains/URLs
All-Web	Predefined WebGroup	*
allowed-https-redhat-update	Domains	*.redhat.com
allowed-apt-get-commands	Domains	*.ubuntu.com, *.archive.ubuntu.com
allowed-nids-detection	Domains	testmynids.org
allowed-github	Domains	*.github.com
ftp-to-example	URLs	ftp://username:password@ftp.example.com/folder/

Useful for logging all the FQDNs/Domains that are being accessed (i.e. in a typical scenario where you would use the Discovery Rule)

Domains & sub-domains (leveraging the Wild Cards)

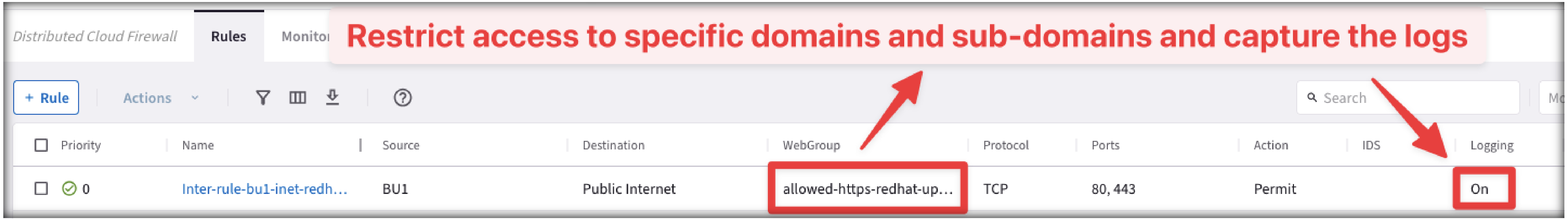
URL: full path for http, https, ftp...

WebGroups Attached to the DCF Rule



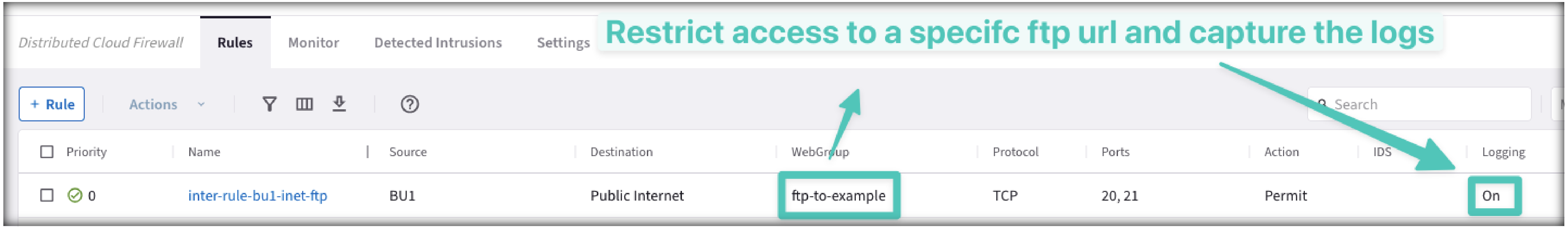
Allow access to any FQDNs/Domains using port 80/443 and capture the logs

□ Priority	Name	Source	Destination	WebGroup	Protocol	Ports	Action	SG Orchestratio	Decryption	IDS	Logging
□ ✓ 0	Discovery-Rule	BU1	Public Internet	All-Web	Any		Permit				On



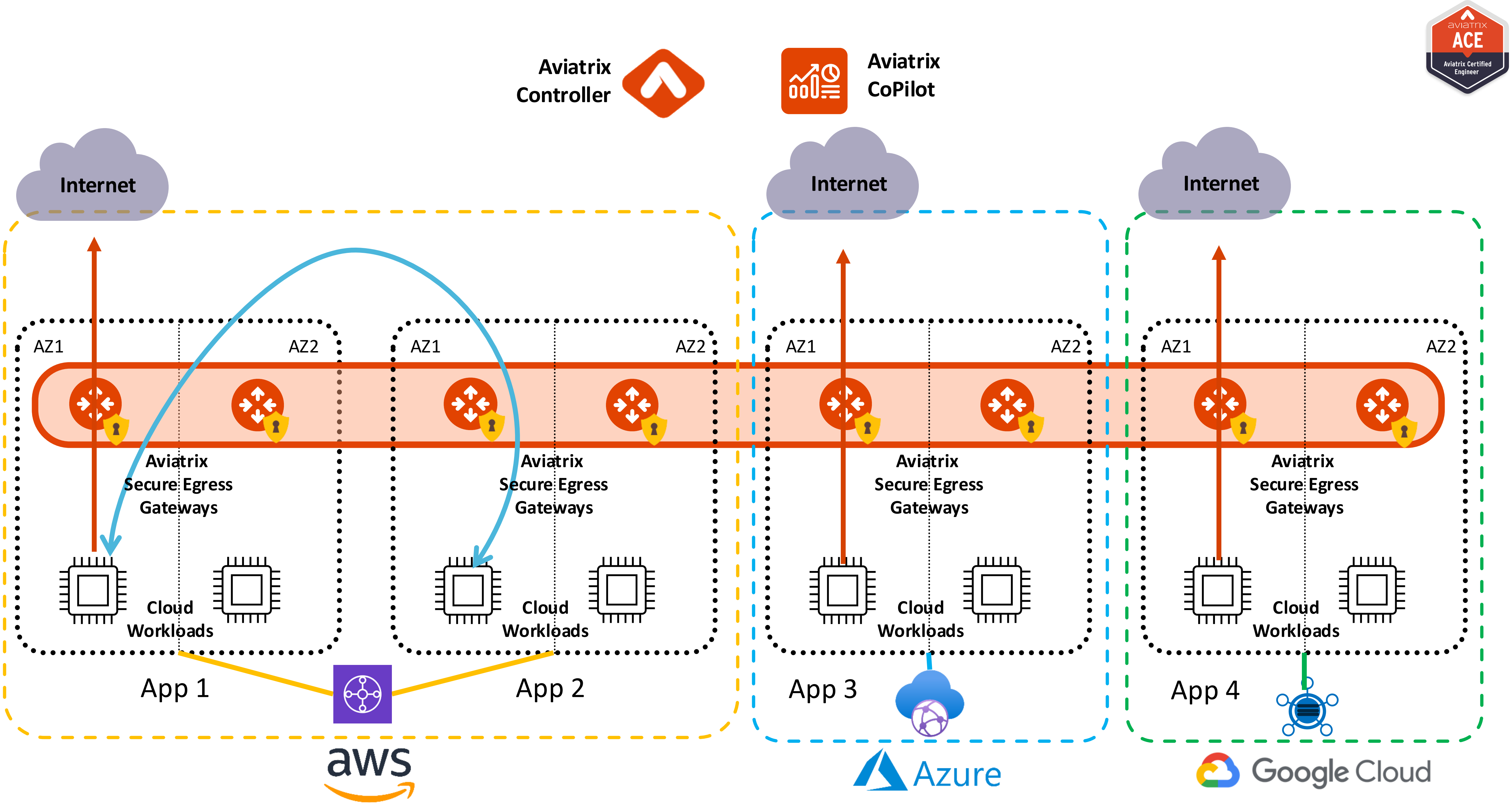
Restrict access to specific domains and sub-domains and capture the logs

□ Priority	Name	Source	Destination	WebGroup	Protocol	Ports	Action	IDS	Logging
□ ✓ 0	Inter-rule-bu1-inet-redh…	BU1	Public Internet	allowed-https-redhat-up…	TCP	80, 443	Permit		On



Restrict access to a specifc ftp url and capture the logs

□ Priority	Name	Source	Destination	WebGroup	Protocol	Ports	Action	IDS	Logging
□ ✓ 0	inter-rule-bu1-inet-ftp	BU1	Public Internet	ftp-to-example	TCP	20, 21	Permit		On



Aviatrix Controller

Aviatrix CoPilot

aviatrix ACE Aviatrix Certified Engineer

Internet

Internet

Internet

AZ1

AZ2

AZ1

AZ2

AZ1

AZ2

AZ1

AZ2

Aviatrix Secure Egress Gateways

Aviatrix Secure Egress Gateways

Aviatrix Secure Egress Gateways

Aviatrix Secure Egress Gateways

Cloud Workloads

Cloud Workloads

Cloud Workloads

Cloud Workloads

App 1

App 2

App 3

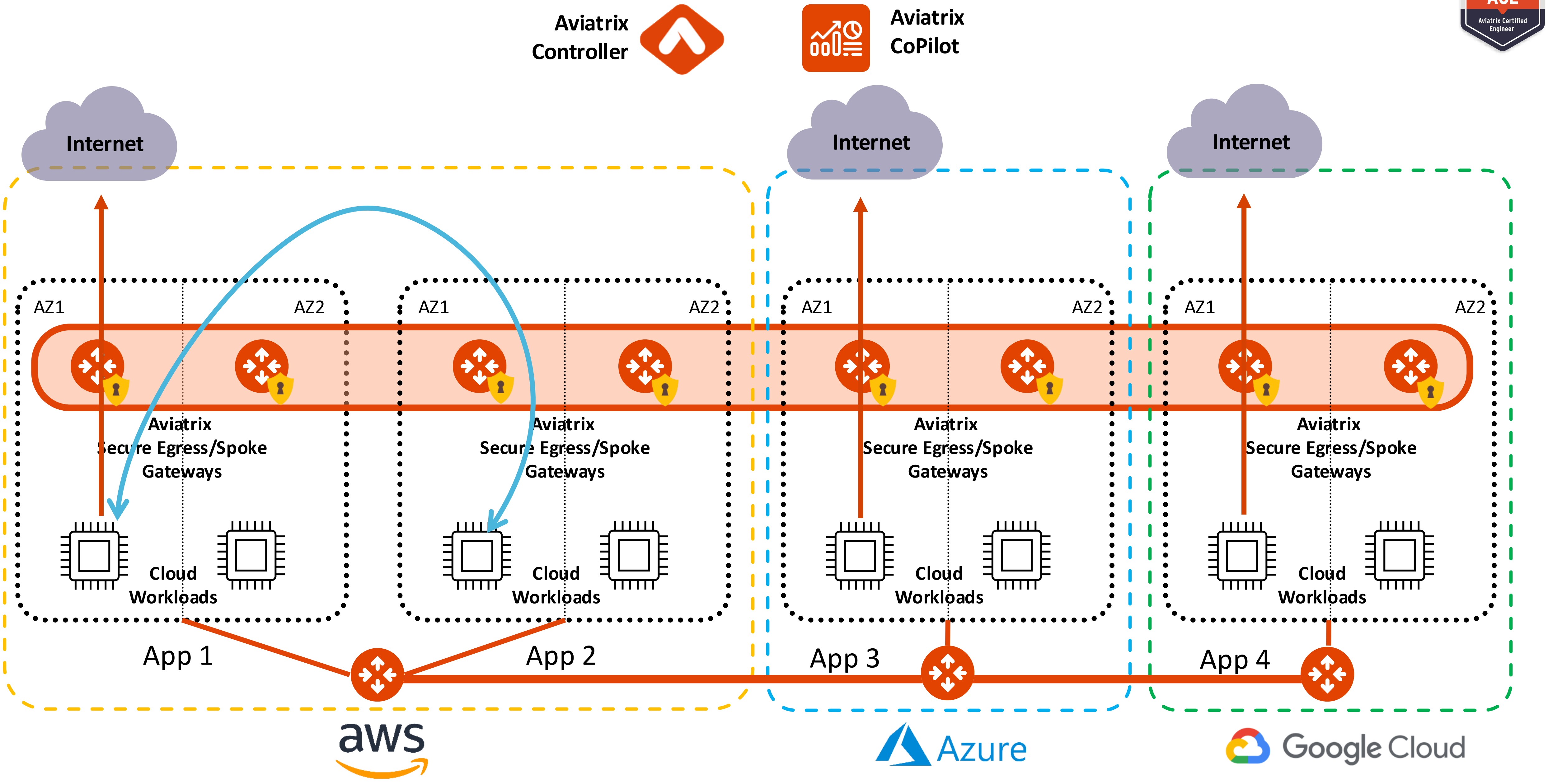
App 4

aws

Azure

Google Cloud

aviatrix®



Aviatrix Controller

Aviatrix CoPilot

Internet

Internet

Internet

AZ1

AZ2

AZ1

AZ2

AZ1

AZ2

AZ1

AZ2

Aviatrix Secure Egress/Spoke Gateways

Aviatrix Secure Egress/Spoke Gateways

Aviatrix Secure Egress/Spoke Gateways

Aviatrix Secure Egress/Spoke Gateways

Cloud Workloads

Cloud Workloads

Cloud Workloads

Cloud Workloads

App 1

App 2

App 3

App 4

aws

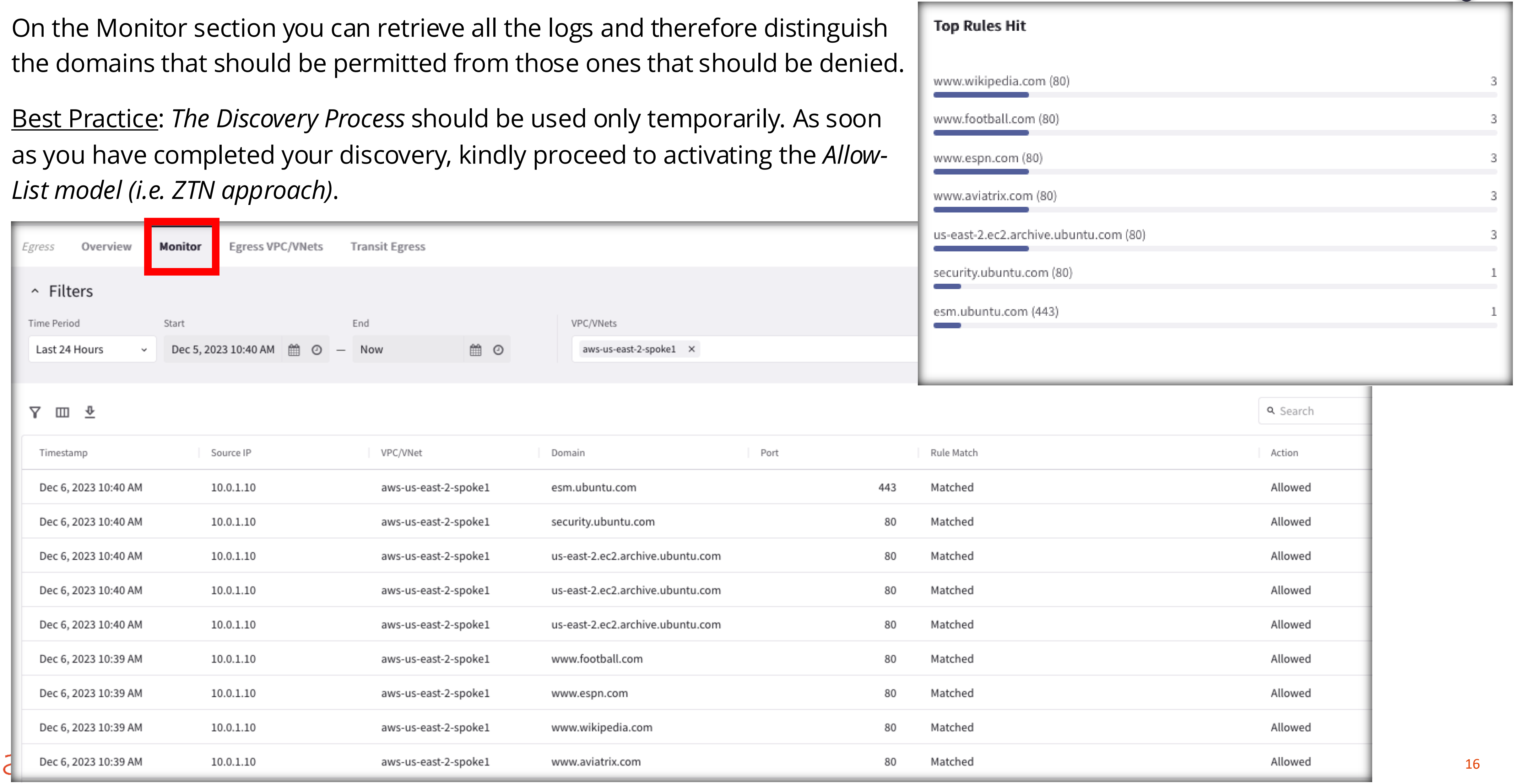
Azure

Google Cloud

aviatrix

Monitor

- On the Monitor section you can retrieve all the logs and therefore distinguish the domains that should be permitted from those ones that should be denied.
- Best Practice: *The Discovery Process* should be used only temporarily. As soon as you have completed your discovery, kindly proceed to activating the *Allow-List model (i.e. ZTN approach)*.



Time Period: Last 24 Hours

Start: Dec 5, 2023 10:40 AM

End: Now

VPC/VNets: aws-us-east-2-spoke1

Timestamp	Source IP	VPC/VNet	Domain	Port	Rule Match	Action
Dec 6, 2023 10:40 AM	10.0.1.10	aws-us-east-2-spoke1	esm.ubuntu.com	443	Matched	Allowed
Dec 6, 2023 10:40 AM	10.0.1.10	aws-us-east-2-spoke1	security.ubuntu.com	80	Matched	Allowed
Dec 6, 2023 10:40 AM	10.0.1.10	aws-us-east-2-spoke1	us-east-2.ec2.archive.ubuntu.com	80	Matched	Allowed
Dec 6, 2023 10:40 AM	10.0.1.10	aws-us-east-2-spoke1	us-east-2.ec2.archive.ubuntu.com	80	Matched	Allowed
Dec 6, 2023 10:40 AM	10.0.1.10	aws-us-east-2-spoke1	us-east-2.ec2.archive.ubuntu.com	80	Matched	Allowed
Dec 6, 2023 10:39 AM	10.0.1.10	aws-us-east-2-spoke1	www.football.com	80	Matched	Allowed
Dec 6, 2023 10:39 AM	10.0.1.10	aws-us-east-2-spoke1	www.espn.com	80	Matched	Allowed
Dec 6, 2023 10:39 AM	10.0.1.10	aws-us-east-2-spoke1	www.wikipedia.com	80	Matched	Allowed
Dec 6, 2023 10:39 AM	10.0.1.10	aws-us-east-2-spoke1	www.aviatrix.com	80	Matched	Allowed

Top Rules Hit

www.wikipedia.com (80)	3
www.football.com (80)	3
www.espn.com (80)	3
www.aviatrix.com (80)	3
us-east-2.ec2.archive.ubuntu.com (80)	3
security.ubuntu.com (80)	1
esm.ubuntu.com (443)	1

Aviatrix Kubernetes Firewall
Kubernetes Aware Firewall

Securing Kubernetes Clusters

Aviatrix Kubernetes Firewall

Provide a Scalable and Secure Fabric on which to safely deploy and run Kubernetes workloads with high developer velocity.

What we hear from customers about Kubernetes challenges

- Scalability issues due to IP address exhaustion and overlap
- Sub-par and inefficient Egress security due to ephemeral and dynamic nature of Kubernetes Lower developer velocity due to security, governance and compliance needs
- Complex implementation for Network segmentation and Zero Trust
- Complex multi-cluster secure networking across zones, regions and multi-cloud for modern apps.
- Inadequate network observability and troubleshooting
- High cost from suboptimal Compute usage, Network Firewall, NAT GW, IP address, Egress, etc.

Network Security for Kubernetes

Key Use Cases

- Multi-cluster security without worrying about IP address overlap or exhaustion
- Kubernetes resource (cluster, namespaces, pods, service, nodes) based egress security to guard against breaches, command and control and exfiltration
- Network segmentation and observability based on Kubernetes resources, VMs and cloud services to stop lateral movement and help achieve compliance.
- Zero Trust Security

High Level Concept

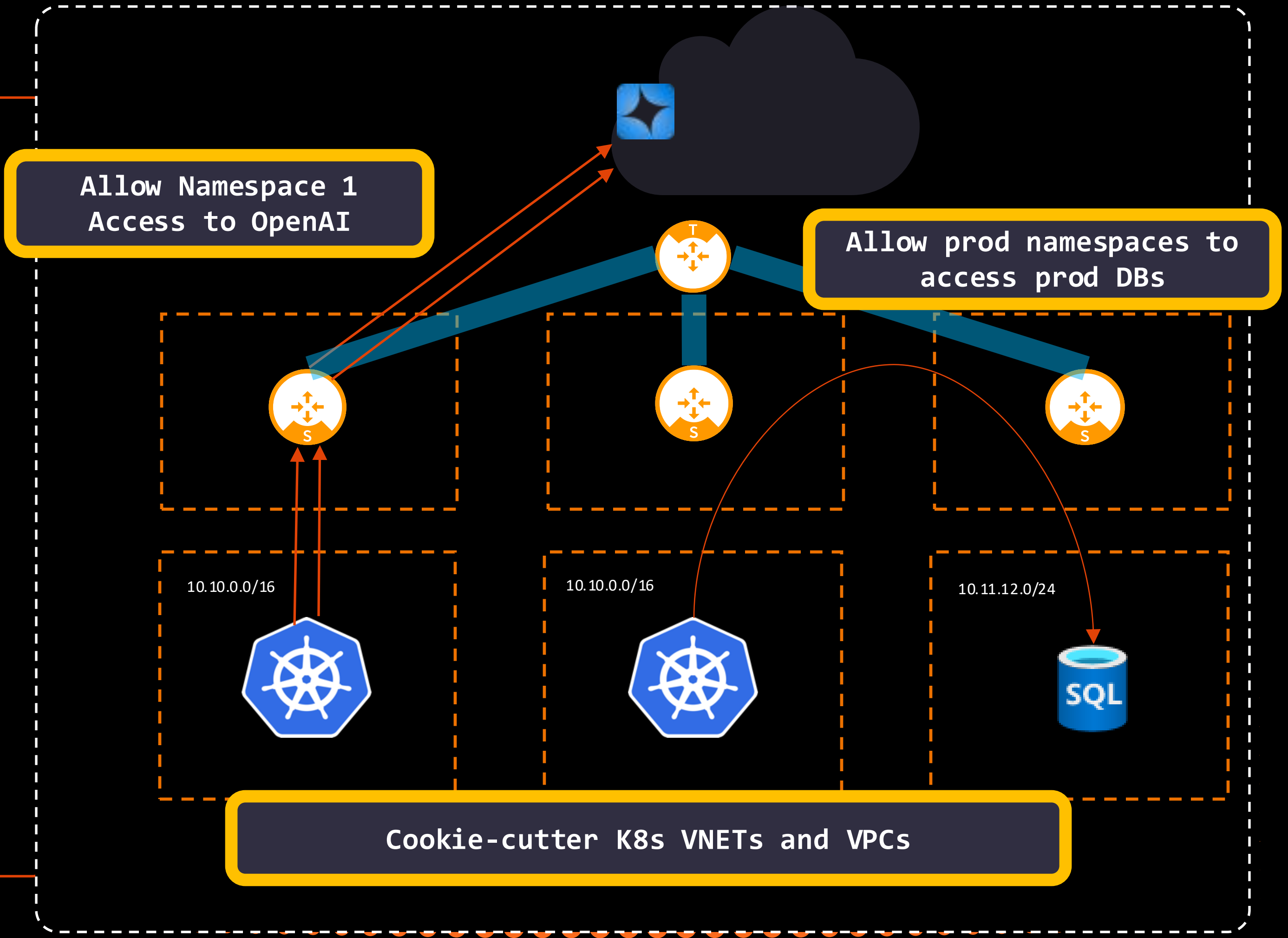
- Aviatrix Controller connects to all API servers across multi-cloud deployments
- Customer can define declarative KRM based policies using smart groups
- Aviatrix Controller listens to etcd changes and reconciles smart groups
- The reconciled rules gets rapidly actualized in the right Aviatrix Gateways for enforcement

SHIPPING TODAY

DCF for Kubernetes

Problem: Kubernetes often hosts multiple applications and lacks effective egress and cluster-to-cluster controls

- Pod and namespace level firewall policy
- Egress L7 policy enforcement
- East-West L4 segmentation
- Enables repeatable K8s deployments without IP address exhaustion
- AKS/EKS/GKE with native CNIs



Allow Namespace 1 Access to OpenAI
Allow prod namespaces to access prod DBs
T
S
S
S
10.10.0.0/16
10.10.0.0/16
10.11.12.0/24
SQL
Cookie-cutter K8s VNETs and VPCs

AVIATRIX

Demo

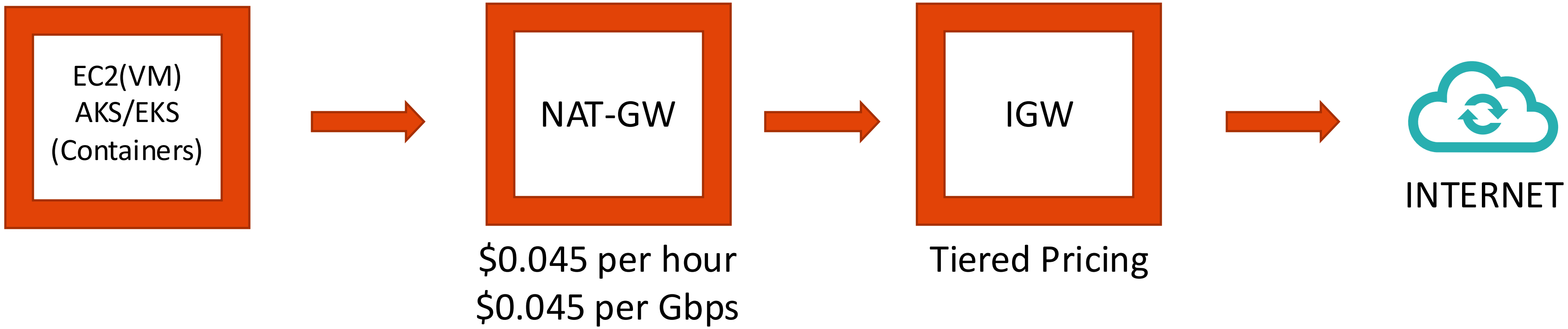
https://www.youtube.com/watch?v=F22bJEUAaoc

Cloud Perimeter Security – LAB Time

- Lab Progress is counted towards the cert
- Everyone will get their own lab pod
- Work in Groups / Breakout – Instructor will create breakouts
- No help will be provided by the instructor to complete the lab
- Group members should discuss and help each other
- You have 1 hour
- Use hints and Aviatrix documentation
- LABs will be destroyed after 6 hours automatically at the completion of course

Cloud Perimeter Security – Secure Egress Advantages

1. Cost saving → https://aviatrix.com/tco-calculator/
2. Enhanced Security
3. Deep Monitoring Logging
4. Easy management and troubleshooting



EC2(VM)
AKS/EKS
(Containers)

NAT-GW

IGW

INTERNET

$0.045 per hour
$0.045 per Gbps

Tiered Pricing

Reference: https://aws.amazon.com/vpc/pricing/
https://aws.amazon.com/ec2/pricing/on-demand/

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

COMMUNITY
https://community.aviatrix.com