

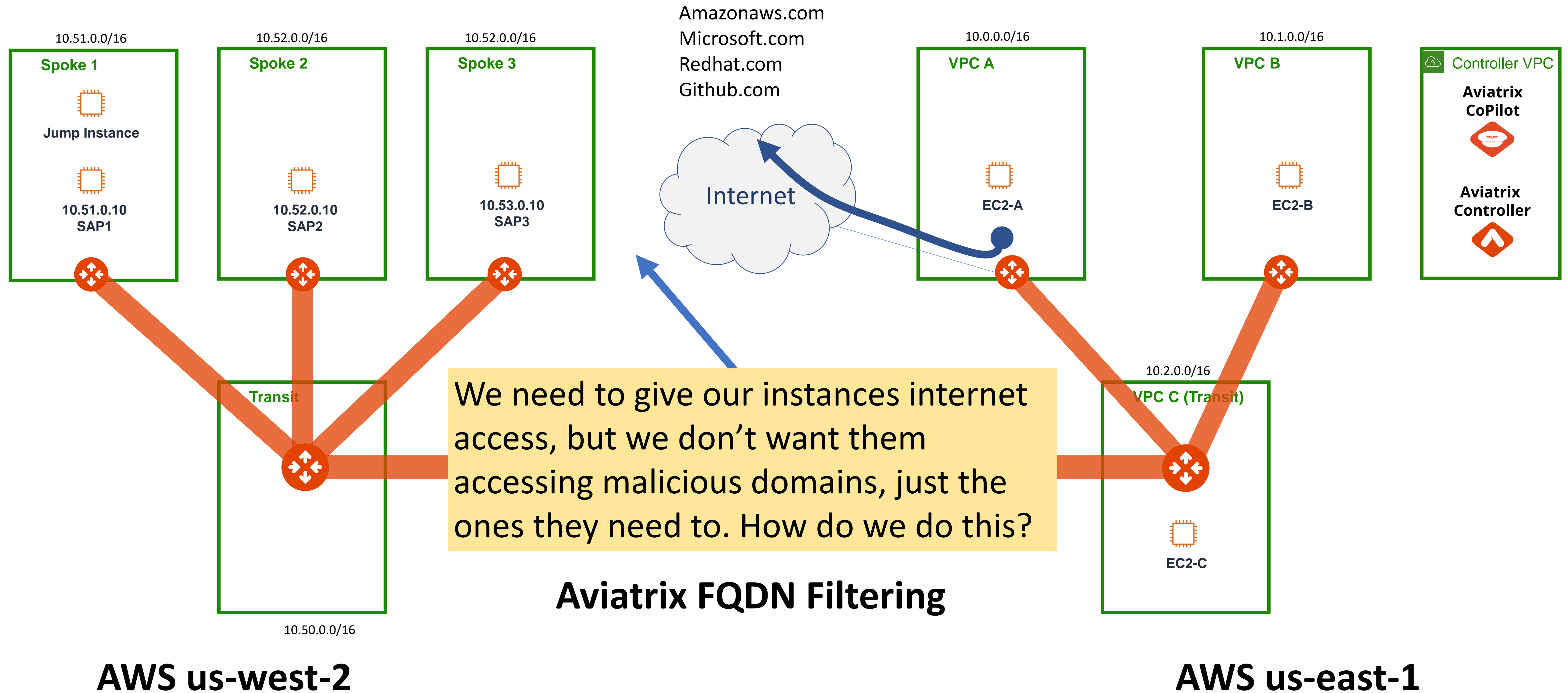
AWS Immersion Day LAB 7

SECURITY: EGRESS FQDN FILTERING

Brad Hedlund
Principal Solutions Architect,
Aviatrix Systems

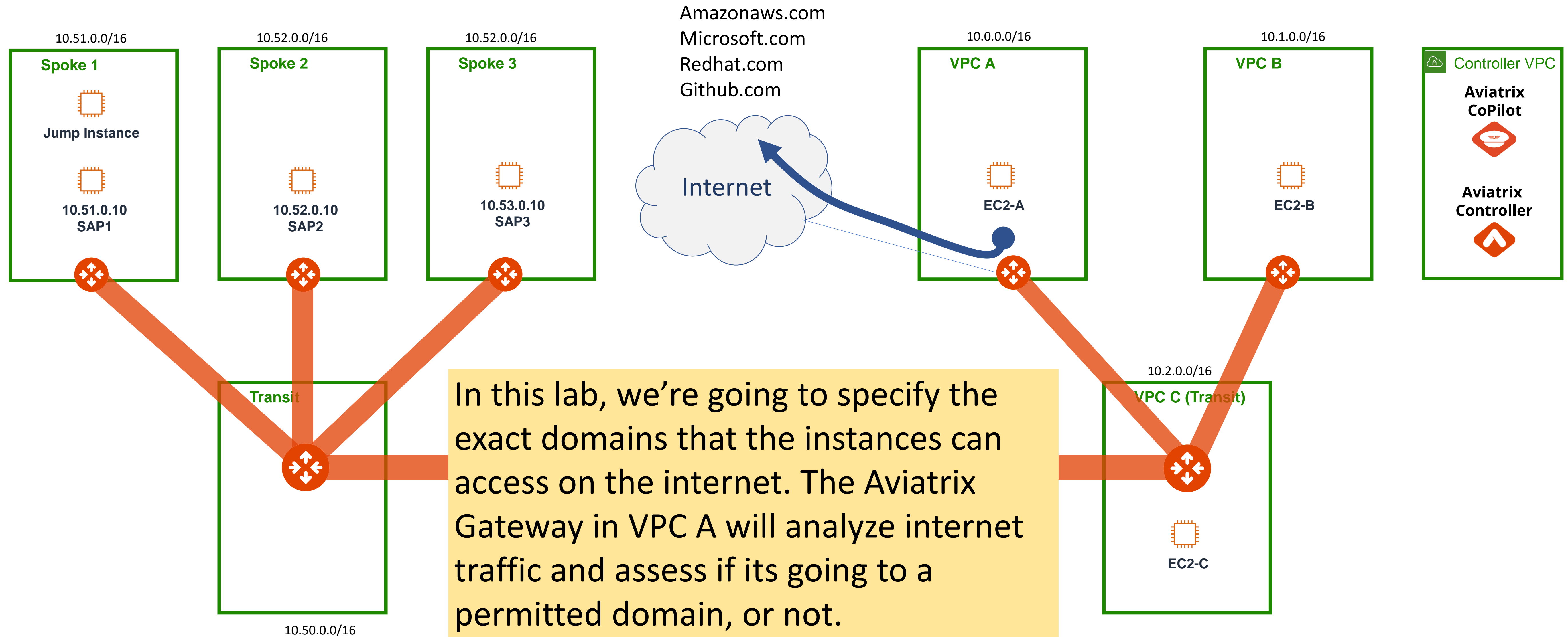
Lab 7 Intro pt.1

Egress FQDN Filtering



Lab 7 Intro pt.2

Egress FQDN Filtering



AWS us-west-2

Aviatrix FQDN Filtering

AWS us-east-1

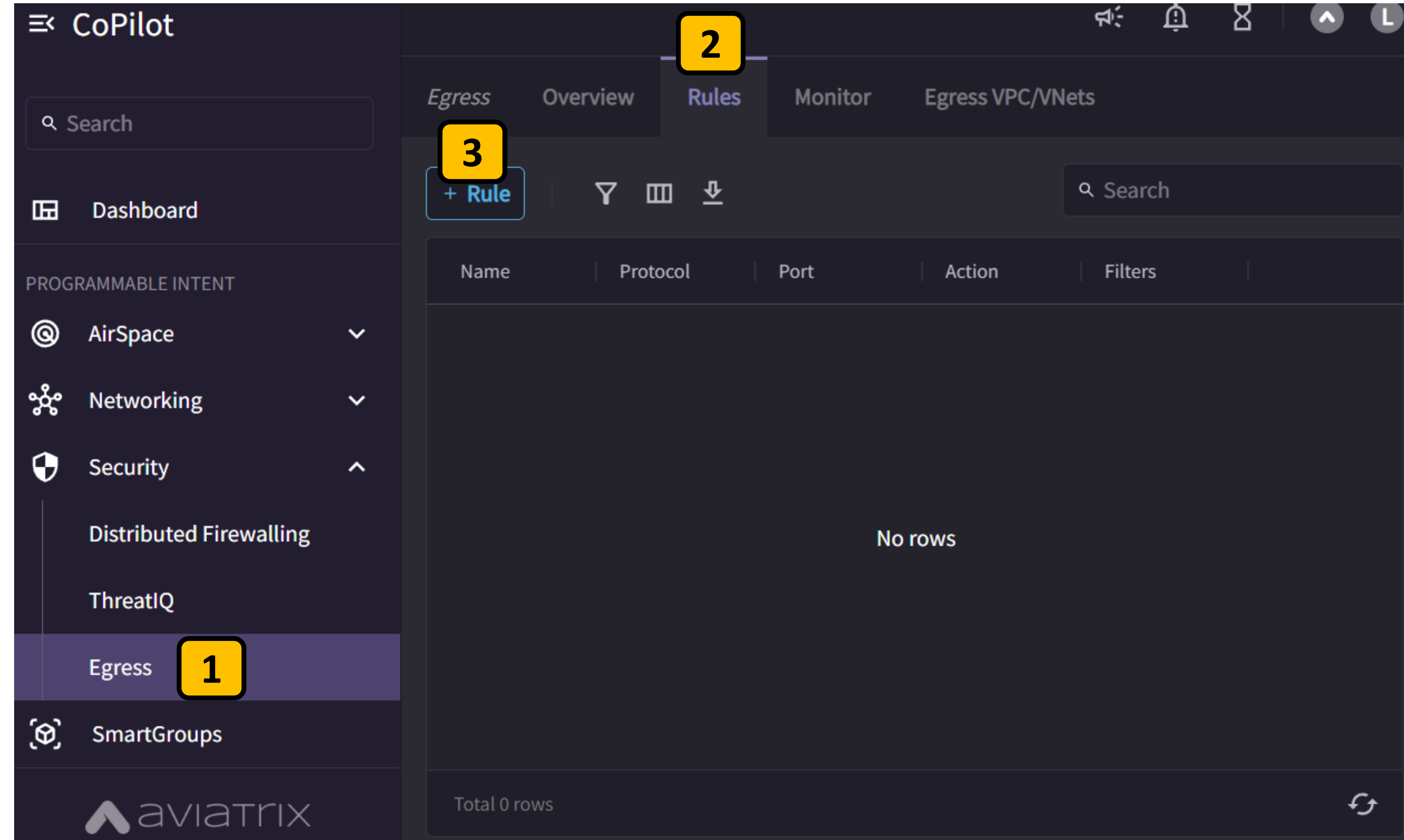
Lab 7: Egress FQDN Filtering: Step 7.0

Create domain filtering rules

To begin, navigate to
Security > Egress **1**

Select Rules **2**

Select +Rule **3**



The screenshot displays the AviaMatrix CoPilot interface. On the left sidebar, the 'Egress' option is highlighted with a yellow box labeled '1'. The main content area has tabs for 'Egress', 'Overview', 'Rules', 'Monitor', and 'Egress VPC/VNets'. The 'Rules' tab is selected, indicated by a yellow box labeled '2'. Within the 'Rules' tab, a '+ Rule' button is highlighted with a yellow box labeled '3'. Below the button is a table with columns: Name, Protocol, Port, Action, and Filters. The table is currently empty, showing 'No rows'. At the bottom of the table, it says 'Total 0 rows'.

Lab 7: Egress FQDN Filtering: Step 7.1

Create domain filtering rules

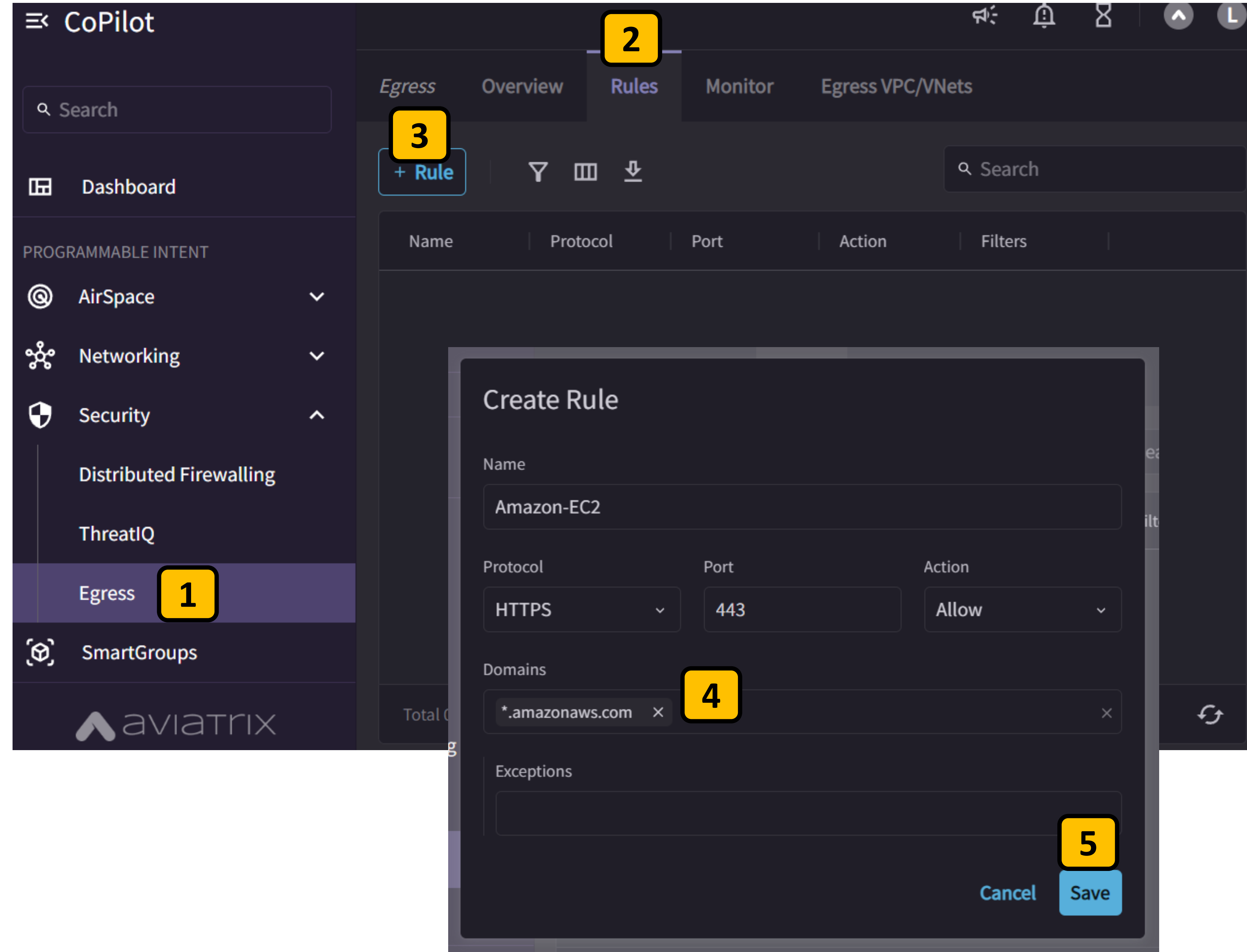
To begin, navigate to
Security > Egress **1**

Select Rules **2**

Select +Rule **3**

Create a rule that allows HTTPS to the
domain *.amazonaws.com **4**

Click Save **5**



The screenshot shows the Aviaatrix CoPilot interface with the following steps highlighted:

- 1**: In the left sidebar, under "PROGRAMMABLE INTENT", the "Egress" option is selected.
- 2**: In the top navigation bar, the "Rules" tab is selected.
- 3**: In the "Rules" tab, the "+ Rule" button is clicked.
- 4**: In the "Create Rule" modal, the "Domains" field contains the entry "*.amazonaws.com".
- 5**: In the "Create Rule" modal, the "Save" button is clicked.

The "Create Rule" modal shows the following configuration:

- Name**: Amazon-EC2
- Protocol**: HTTPS
- Port**: 443
- Action**: Allow
- Domains**: *.amazonaws.com
- Exceptions**: (Empty field)

Lab 7: Egress FQDN Filtering: Step 7.2

Create domain filtering rules

Create additional rules that allow the domains for HTTPS:

***.gitub.com**

***.redhat.com**

1

***.microsoft.com**

Click Save

2

Create Rule

Name

Software-updates

Protocol

Port

Action

HTTPS

443

Allow

Domains

*.github.com

*.redhat.com

*.microsoft.com

1

Exceptions

Cancel

2 Save

Lab 7: Egress FQDN Filtering: Step 7.3

Enable Secure Egress on a spoke Gateway

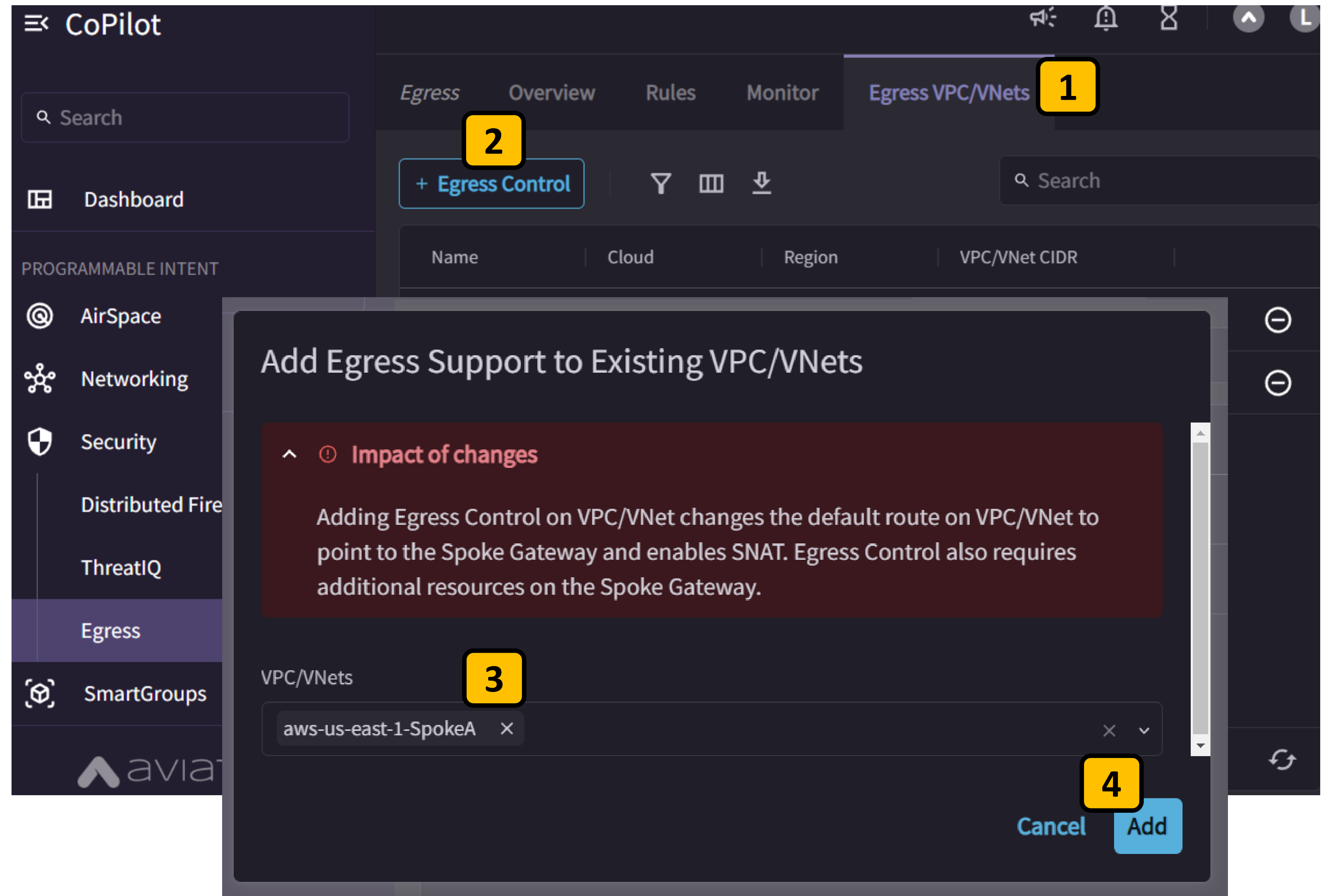
Now let's add Egress Control for the **aws-us-east-1-SpokeA** gateway

Select Egress VPC/VNets **1**

Select +Egress Control **2**

In the popup, select the gateway **aws-us-east-1-SpokeA** **3**

Click Add **4**



Lab 7: Egress FQDN Filtering: Step 7.4

Launch instance in private subnet on VPC A

Now let's launch a new instance in a private subnet in VPC A and test our egress rules we just created.

Launch an Amazon Linux t2.micro instance in **us-east-1**, in **VPC A**, in the **VPC A Private Subnet** **1**

Under Advanced Details, assign it to the IAM instance profile **Ec2RoleForSSM** **2**

▼ Network settings
Info

VPC - required
Info

vpc-02a5168593a0435a0 (VPC A)
10.0.0.0/16
▼

Subnet
Info

1

subnet-0c4312f7a06c52c5a
VPC A Private Subnet
VPC: vpc-02a5168593a0435a0
Owner: 797818187282
Availability Zone: us-east-1a
IP addresses available: 251
CIDR: 10.0.2.0/24)
▼

Create new subnet

▼ Advanced details
Info

Purchasing option
Info

☐ Request Spot Instances
Request Spot Instances at the Spot price, capped at the On-Demand price

Domain join directory
Info

Select
▼

IAM instance profile
Info

2

Ec2RoleForSSM
arn:aws:iam::797818187282:instance-profile/Ec2RoleForSSM
▼

Lab 7: Egress FQDN Filtering: Step 7.5

Access the new instances terminal

Once your instance is in the running state, access its console using **Session Manager**. **1**

Login as ec2-user with the command `sudo su -l ec2-user` **2**

Instances (1/9) Info

Find instance by attribute or tag (case-sensitive)

Instance state = running

Clear filters

	Name	Instance ID	Instance state
<input type="checkbox"/>	aviatrix-aws-us-east-1-Sp...	i-0670208877c0cbaba	Running
<input checked="" type="checkbox"/>	egress-test	i-061b59fdd009aa7c7	Running
<input type="checkbox"/>	AviaatrixController	i-0f559469cc702b230	Running
<input type="checkbox"/>	aviatrix-aws-		

Connect to instance Info

Connect to your instance i-061b59fdd009aa7c7 (egress-test) using any of these options

EC2 Instance Connect

Session Manager

SSH client

EC2 serial console

Session Manager usage:

- Connect to your instance without SSH keys or a bastion host.
- Sessions are secured using an AWS Key Management Service key.
- You can log session commands and details in an Amazon S3 bucket or CloudWatch Logs log group.
- Configure sessions on the Session Manager [Preferences](#) page.

Cancel

Connect

Session ID: brad-0b93adefc7ee7dee0 Instance ID: i-061b59fdd009aa7c7

```
sh-5.2$
sh-5.2$
sh-5.2$ sudo su -l ec2-user

[ec2-user@ip-10-0-2-219 ~]$
[ec2-user@ip-10-0-2-219 ~]$
[ec2-user@ip-10-0-2-219 ~]$
[ec2-user@ip-10-0-2-219 ~]$
[ec2-user@ip-10-0-2-219 ~]$
```

Lab 7: Egress FQDN Filtering: Step 7.5

Test your domain rules

Let's test our *.amazonaws.com rule by running an update for Amazon Linux.

Run an update with the command
sudo yum update -y 1

Test a connection to www.github.com using the command
curl https://www.github.com -v 2

Test a connection to google.com using the command
curl https://google.com -v 3

```
[ec2-user@ip-10-0-2-219 ~]$
[ec2-user@ip-10-0-2-219 ~]$ sudo yum update -y
Last metadata expiration check: 0:07:36 ago on Wed Apr 12 01:16:21 2023.
Dependencies resolved.
Nothing to do.
Complete!
[ec2-user@ip-10-0-2-219 ~]$
```

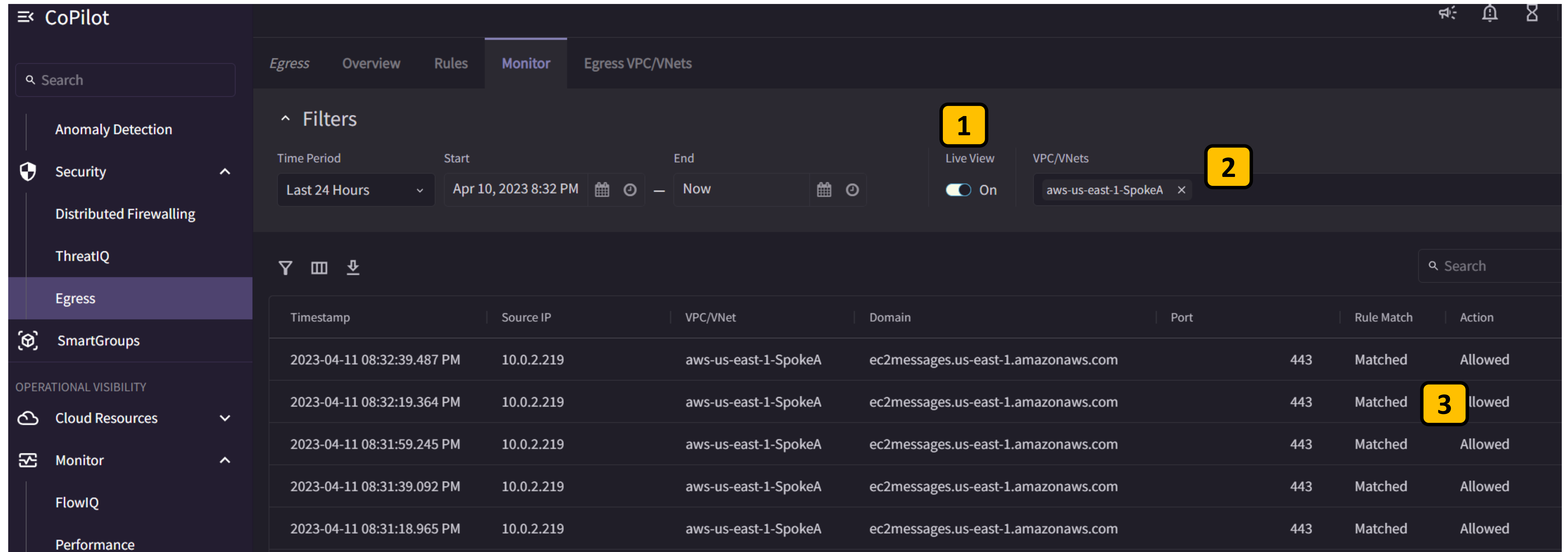
```
[ec2-user@ip-10-0-2-219 ~]$
[ec2-user@ip-10-0-2-219 ~]$ curl https://www.github.com -v
* Trying 140.82.114.3:443...
* Connected to www.github.com (140.82.114.3) port 443 (#0)
* ALPN: offers h2,http/1.1
* TLSv1.3 (OUT), TLS handshake, Client hello (1):
* CAfile: /etc/pki/tls/certs/ca-bundle.crt
* CPath: none
* TLSv1.3 (IN), TLS handshake, Server hello (2):
* TLSv1.3 (IN), TLS handshake, Encrypted Extensions (8):
* TLSv1.3 (IN), TLS handshake, Certificate (11):
* TLSv1.3 (IN), TLS handshake, CERT verify (15):
* TLSv1.3 (IN), TLS handshake, Finished (20):
```

```
[ec2-user@ip-10-0-2-219 ~]$ curl https://google.com -v
* Trying 142.251.16.101:443...
* Connected to google.com (142.251.16.101) port 443 (#0)
* ALPN: offers h2,http/1.1
* TLSv1.3 (OUT), TLS handshake, Client hello (1):
* CAfile: /etc/pki/tls/certs/ca-bundle.crt
* CPath: none
* OpenSSL SSL_connect: SSL_ERROR_SYSCALL in connection to google.com:443
* Closing connection 0
curl: (35) OpenSSL SSL_connect: SSL_ERROR_SYSCALL in connection to google.com:443
[ec2-user@ip-10-0-2-219 ~]$
```

Did you get the results that you expected??

Lab 7: Egress FQDN Filtering: Step 7.5

View domain access activity in real time



The screenshot shows the AWS CloudTrail console with the 'Egress' section selected in the left sidebar. The 'Monitor' tab is active, and the 'Live View' toggle is turned on. The 'VPC/VNets' dropdown is set to 'aws-us-east-1-SpokeA'. The table displays traffic logs with the following columns: Timestamp, Source IP, VPC/VNet, Domain, Port, Rule Match, and Action.

Timestamp	Source IP	VPC/VNet	Domain	Port	Rule Match	Action
2023-04-11 08:32:39.487 PM	10.0.2.219	aws-us-east-1-SpokeA	ec2messages.us-east-1.amazonaws.com	443	Matched	Allowed
2023-04-11 08:32:19.364 PM	10.0.2.219	aws-us-east-1-SpokeA	ec2messages.us-east-1.amazonaws.com	443	Matched	Allowed
2023-04-11 08:31:59.245 PM	10.0.2.219	aws-us-east-1-SpokeA	ec2messages.us-east-1.amazonaws.com	443	Matched	Allowed
2023-04-11 08:31:39.092 PM	10.0.2.219	aws-us-east-1-SpokeA	ec2messages.us-east-1.amazonaws.com	443	Matched	Allowed
2023-04-11 08:31:18.965 PM	10.0.2.219	aws-us-east-1-SpokeA	ec2messages.us-east-1.amazonaws.com	443	Matched	Allowed

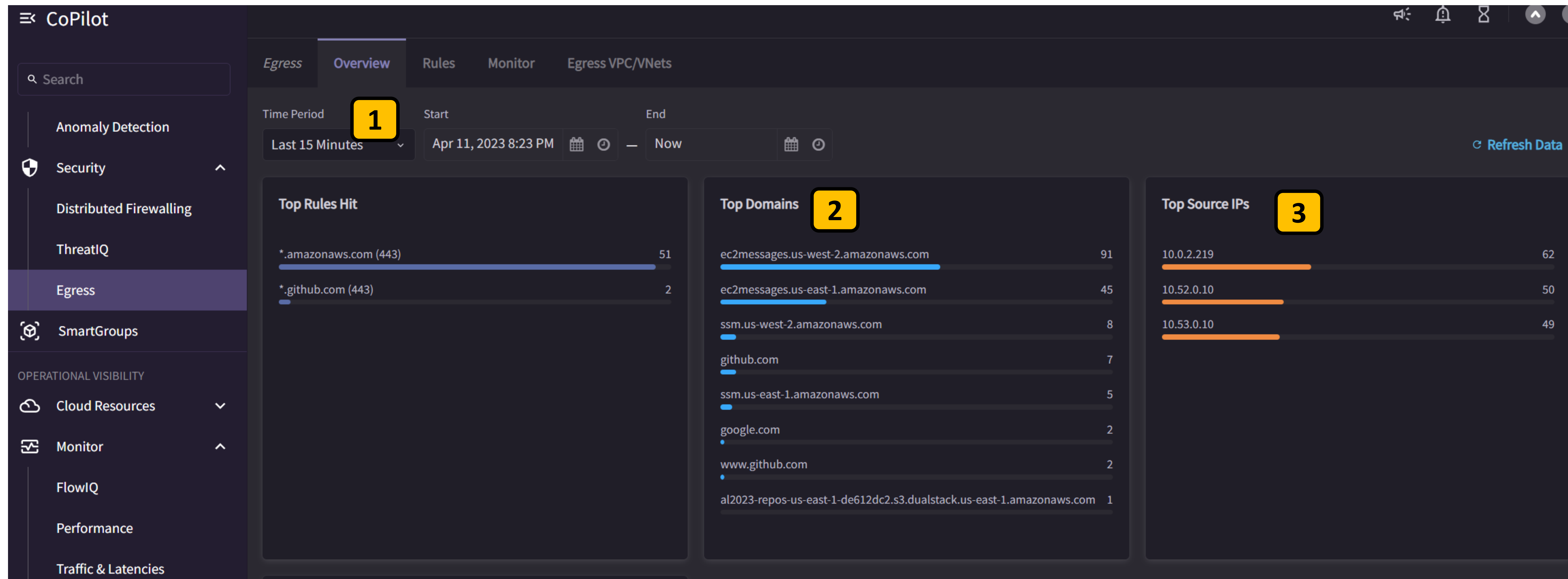
Select the Monitor tab and enable **Live View** **1**

Select the gateway aws-us-east-1-SpokeA gateway in the VPC/Vnets dropdown **2**

Observe the domain-based traffic in real time and notice Rule Match and Action columns. **3**

Lab 7: Egress FQDN Filtering: Step 7.5

View domain access activity in real time



Select the Overview tab and select the Last 15 Minutes of history **1**

Observe the summary top accessed domains **2**

Observe the top talkers of this domain-based Egress traffic. **3**

Lab 7 Success

Egress FQDN Filtering

