

AWS Immersion Day

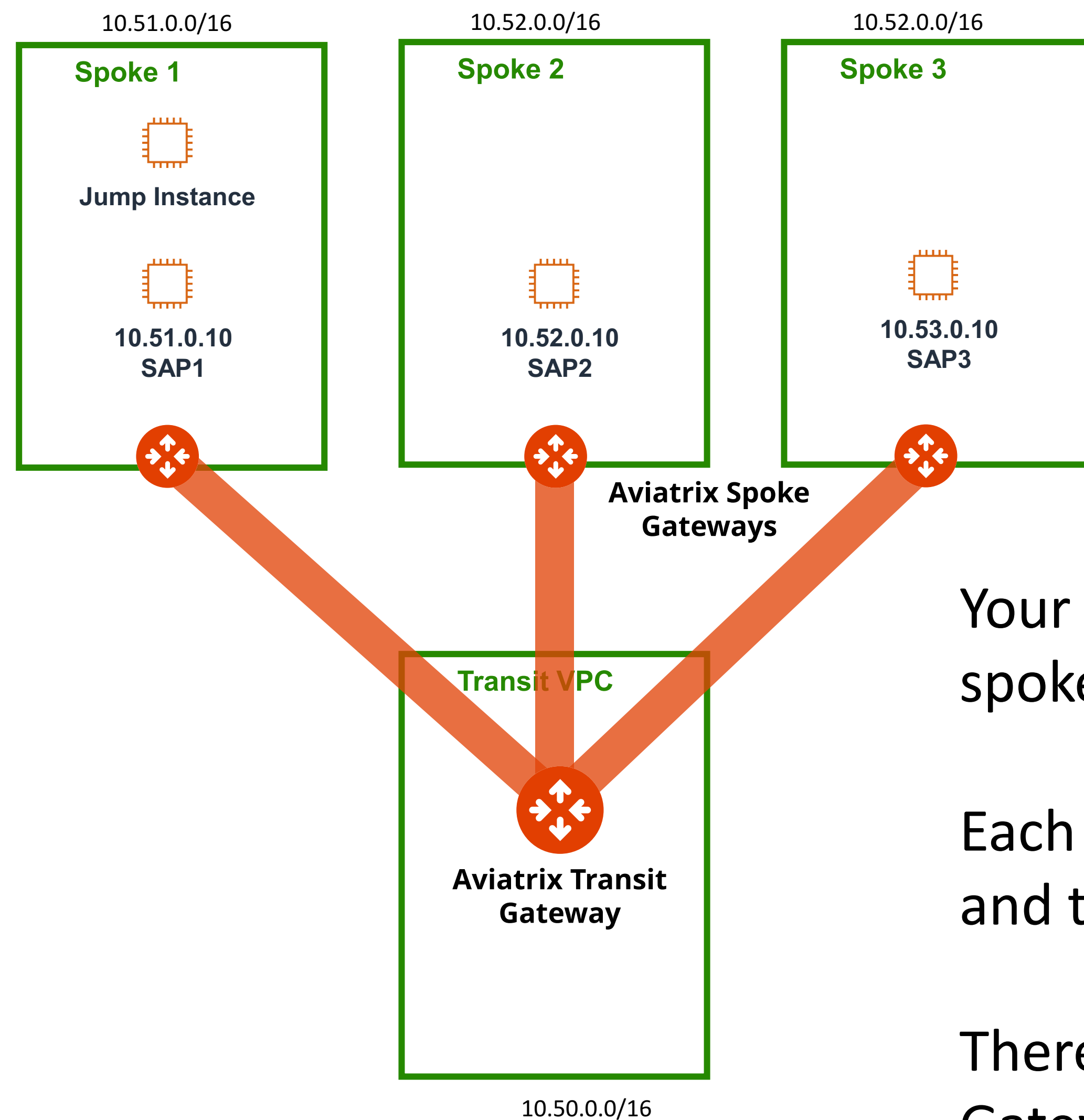
LAB 3

SECURITY: DISTRIBUTED FIREWALL FOR EAST-WEST SECURITY

Ben Biley
Solutions Engineer
Aviatrix Systems

Lab 3 Intro

Distributed Firewall for EAST-WEST

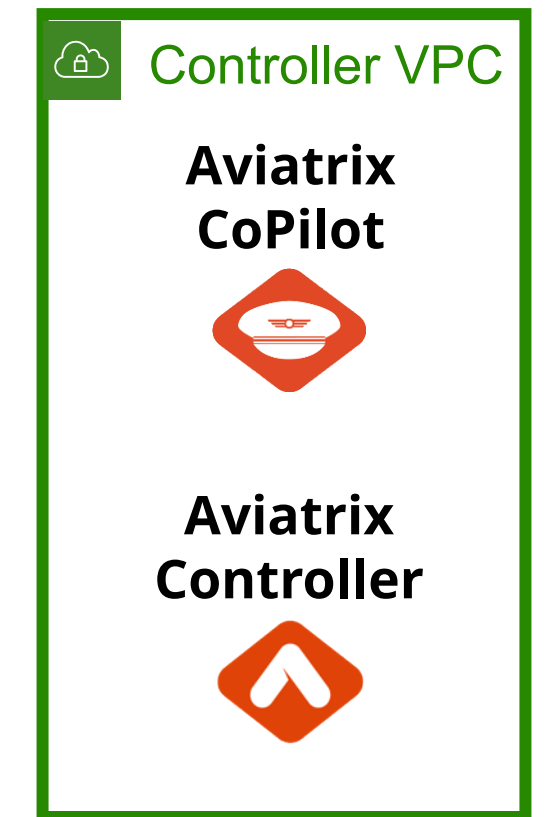


AWS us-west-2

Your Lab account has a full Aviatrix hub-and-spoke architecture deployed in **us-west-2**

Each spoke VPC has an Aviatrix Spoke Gateway and test EC2 instances

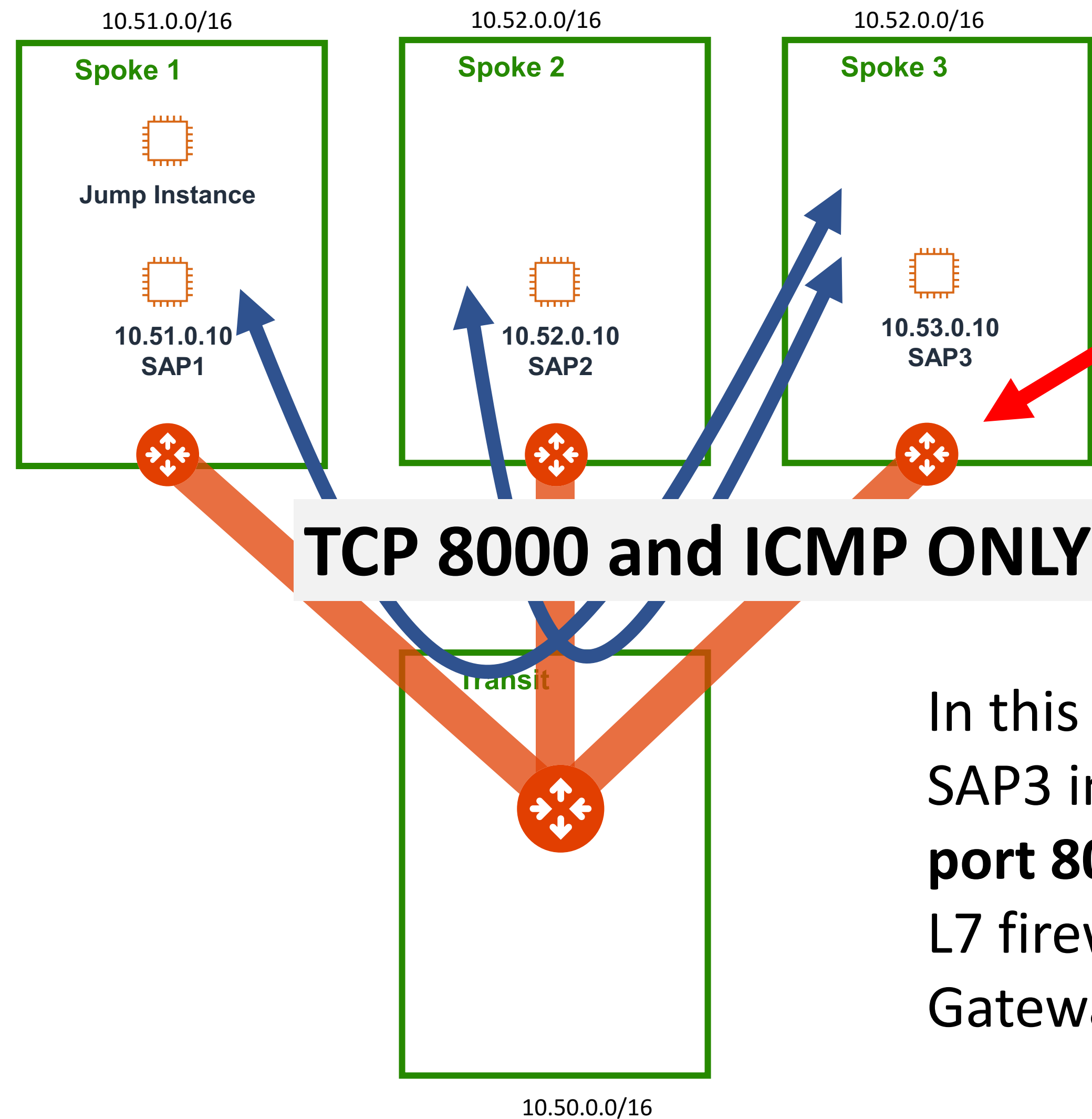
There is a Transit VPC with an Aviatrix Transit Gateway that connects to the Spoke Gateways and forwards traffic between them.



AWS us-east-1

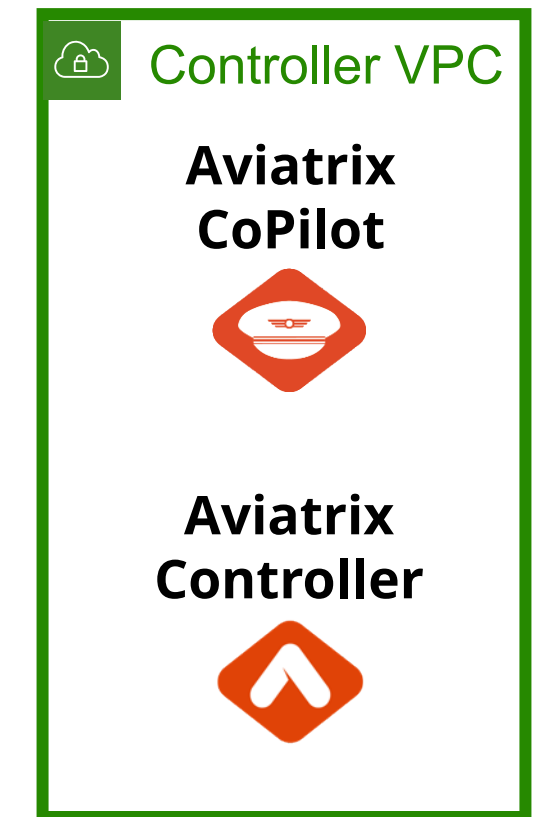
Lab 3 Intro

Distributed Firewall for EAST-WEST



TCP 8000 and ICMP ONLY

The Aviatrix Distributed Cloud Firewall rules you set up in Lab 2 were also deployed to your Spoke gateways in **us-west-2**!



AWS us-east-1

In this Lab we will allow our SAP 1, SAP 2 and SAP3 instances in to communicate **only on TCP port 8000 and ICMP**– without using expensive L7 firewalls. Let's configure the Aviatrix Spoke Gateways as one big **Distributed Firewall** !

AWS us-west-2

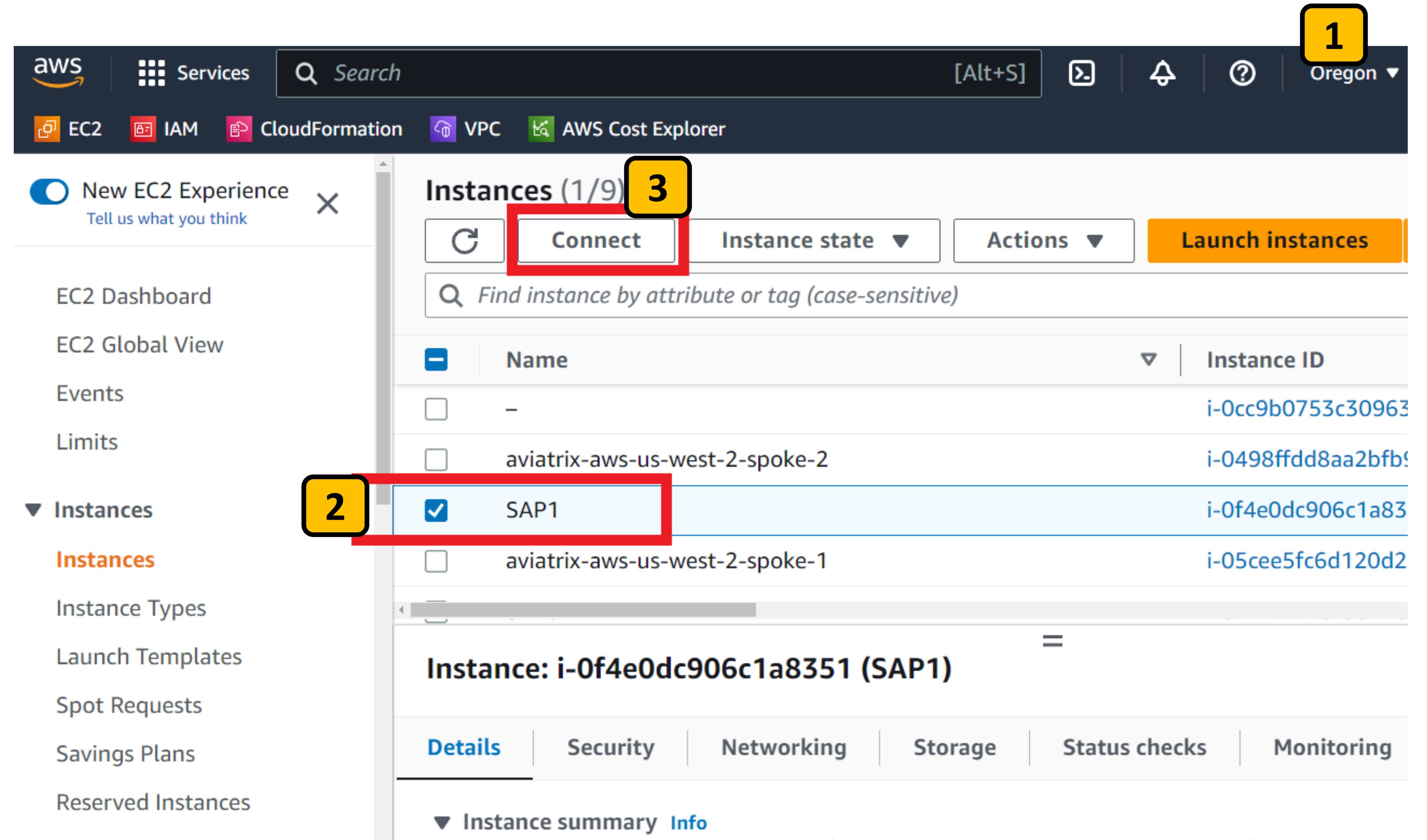
Lab 3: Distributed Firewall: Step 3.1

Connect to CLI of SAP 1 Instance

Switch your AWS Console to the us-west-2 **Oregon** region. **1**

Go to the EC2 section of the AWS Console and select the **SAP 1** instance. **2**

Click **Connect**. **3**



The screenshot shows the AWS Management Console interface. At the top, the region is set to Oregon (us-west-2), indicated by a yellow box with the number 1. The left sidebar shows the navigation menu with 'Instances' selected. The main content area displays a list of EC2 instances. The 'SAP1' instance is selected, highlighted with a red box and a yellow box with the number 2. Above the instance list, the 'Connect' button is highlighted with a red box and a yellow box with the number 3. The 'Launch instances' button is also visible in the top right corner.

Name	Instance ID
-	i-0cc9b0753c30963
aviatrix-aws-us-west-2-spoke-2	i-0498ffdd8aa2bfb9
<input checked="" type="checkbox"/> SAP1	i-0f4e0dc906c1a83
aviatrix-aws-us-west-2-spoke-1	i-05cee5fc6d120d2

Instance: i-0f4e0dc906c1a8351 (SAP1)

Details | Security | Networking | Storage | Status checks | Monitoring

▼ Instance summary [Info](#)

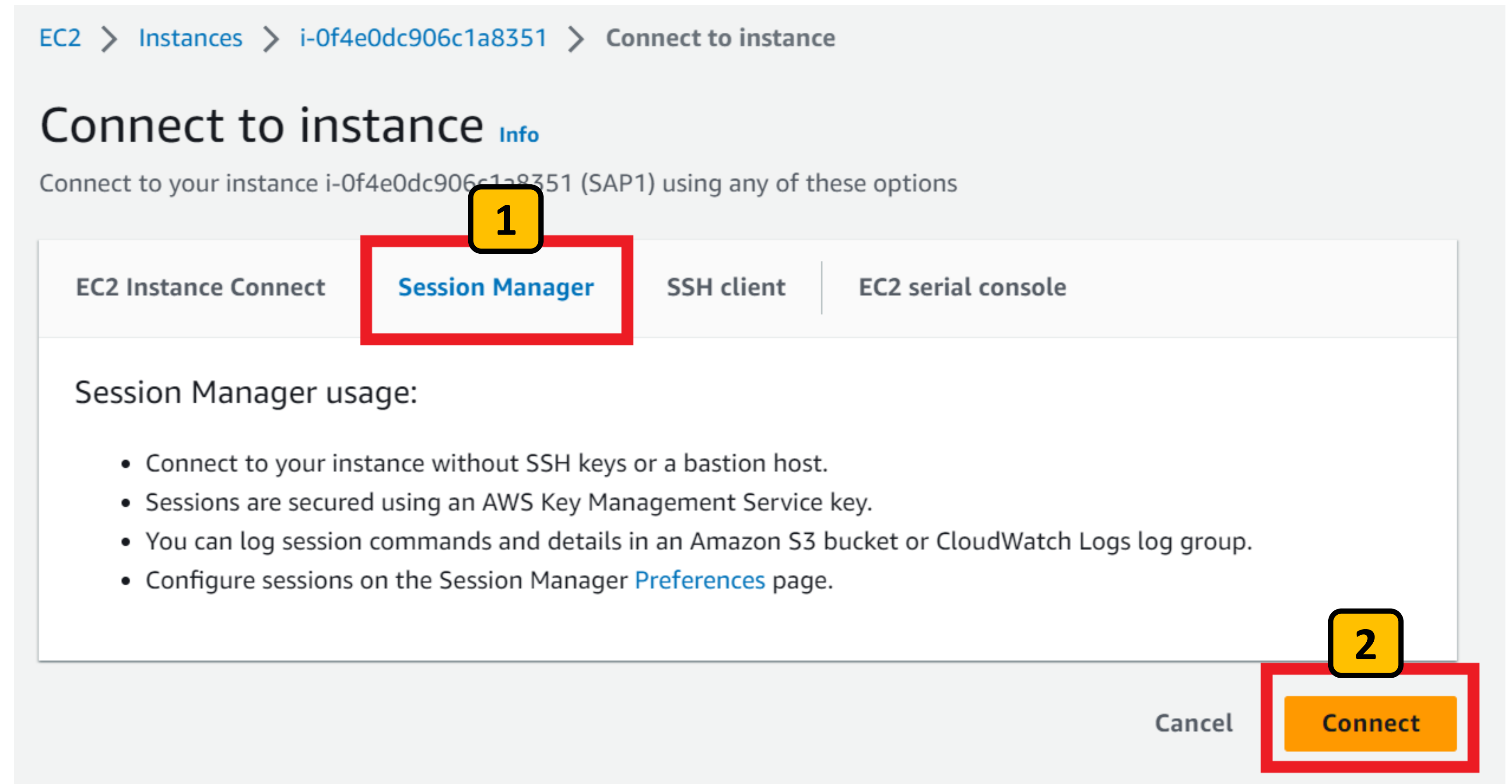
Lab 3: Distributed Firewall: Step 3.2

Connect to CLI of SAP 1 Instance

Select the **Session Manager** tab. **1**

Click Connect. **2**

This will open a new browser tab giving you a CLI session on this instance



EC2 > Instances > i-Of4e0dc906c1a8351 > Connect to instance

Connect to instance [Info](#)

Connect to your instance i-Of4e0dc906c1a8351 (SAP1) using any of these options

1

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 **2** **Connect**

Lab 3: Distributed Firewall: Step 3.3

Test PING does not work without firewall rule

Login as ec2-user by issuing the command:

sudo su -l ec2-user 1

Try to PING the SAP2 instance by issuing the command:

ping 10.52.0.10 2


The ping should fail because our Distributed Cloud Firewall from Lab 2 does not have a rule that allows it.

```

Session ID: brad-0cc7cae3178803793    Instance ID: i-0f4e0dc906c1a8351

sh-4.2$
sh-4.2$ sudo su -l ec2-user 1
Last login: Wed Jan 11 01:27:18 UTC 2023 on pts/2
[ec2-user@ip-10-51-0-10 ~]$
[ec2-user@ip-10-51-0-10 ~]$
[ec2-user@ip-10-51-0-10 ~]$ ping 10.52.0.10 2
PING 10.52.0.10 (10.52.0.10) 56(84) bytes of data.

```



Lab 3: Distributed Firewall: Step 3.4

Create firewall rule for PING

Create a Distributed Firewall Rule that allows the SmartGroup **PROD** to ping **PROD**

Name the rule Allow-PROD-Ping **1**

Set the source to PROD, and the destination to PROD. **2**

Set Protocol to ICMP **3**

Enable Enforce and Logging **4**

Set Rule to Top and **Save In Drafts** **5**

Create Rule

Rules will be applied only on AWS, AWS Gov, ARM, ARM Gov, and GCP

Name

Allow-PROD-Ping

Source SmartGroups

PROD

Destination SmartGroups

PROD

WebGroups

Protocol

ICMP

Rule Behavior

Enforcement

Logging

Action

Permit

SG Orchestration

On

Ensure TLS

Off

TLS Decryption

Off

Intrusion Detection (IDS)

Off

Rule Priority

Place Rule

Top

Cancel

Save In Drafts

Lab 3: Distributed Firewall: Step 3.5

Create rule for TCP 8000

Create another Distributed Firewall Rule that allows the SmartGroup **PROD** to connect on TCP 8000 to **PROD**

Name the rule Allow-TCP-8000 **1**

Set the source to PROD, and the destination to PROD. **2**

Set Protocol to TCP and Port to 8000 **3**

Enable Enforce and Logging **4**

Set Rule to Top and **Save In Drafts** **5**

Create Rule

Rules will be applied only on AWS, AWS Gov, ARM, ARM Gov, and GCP

Name

Allow-TCP-8000

Source SmartGroups

PROD

Destination SmartGroups

PROD

WebGroups

Protocol

TCP

Port

8000

Specify multiple ports (e.g. 80) and/or port ranges (e.g. 80-8080)

Rule Behavior

Enforcement

Logging

Action

Permit

SG Orchestration

On

Ensure TLS

Off

TLS Decryption

Off

Intrusion Detection (IDS)

Off

Rule Priority

Place Rule

Top

Cancel

Save In Drafts

Lab 3: Distributed Firewall: Step 3.6

Commit east-west rules

Distributed Firewalling
Rules
Policy Monitor
Detected Intrusions
WebGroups
Settings

+ Rule
Actions
Filter
List
Download
2 New
Discard
Commit
Search

<input type="checkbox"/>	Priority	Name	Source	Destination	WebGroup	Protocol	Ports	
<input type="checkbox"/>	0	Allow-TCP-8000	PROD	PROD		TCP	8000	↑↓ ✎ ⋮
<input type="checkbox"/>	1	Allow-PROD-Ping	PROD	PROD		ICMP		↑↓ ✎ ⋮
<input type="checkbox"/>	2	Allow-AWS	DEV, PROD	Public Internet	Allow-AWS	TCP	443	↑↓ ✎ ⋮
<input type="checkbox"/>	3	Allow-NTP	DEV, PROD	Public Internet		UDP	123	↑↓ ✎ ⋮

Commit your new Distributed Firewall Rules 1

Lab 3: Distributed Firewall: Step 3.7

Test that ping works now with east-west rule

Go back the console session of the SAP1 instance you opened earlier or open it again.

Try to PING the SAP2 instance by issuing the command:

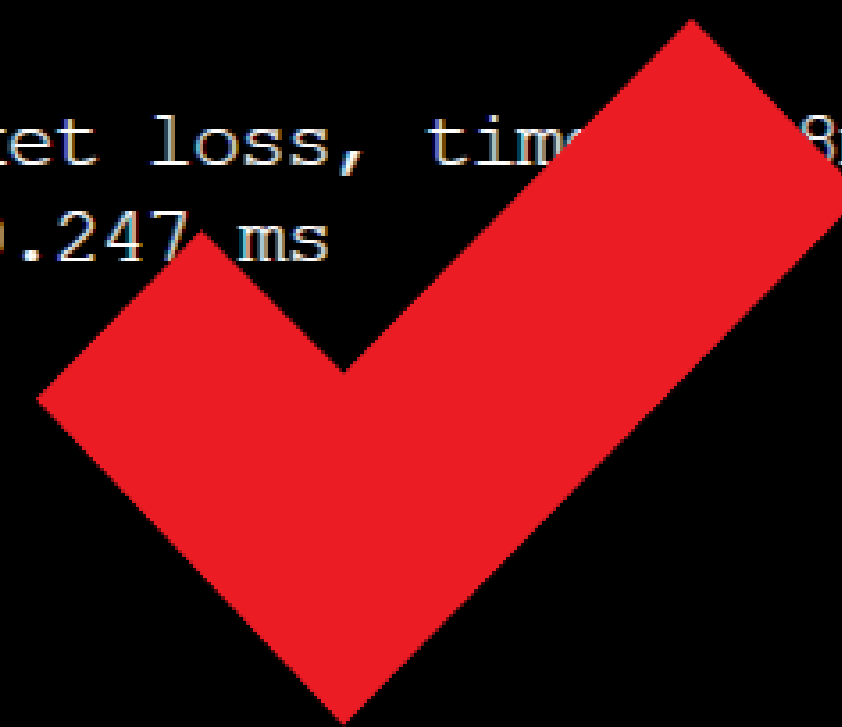
ping 10.52.0.10 1

The ping should work now because your Distributed Firewall now allows these two instances in the PROD group to ping.

Session ID: brad-0cc7cae3178803793

Instance ID: i-0f4e0dc906c1a8351

```
[ec2-user@ip-10-51-0-10 ~]$
[ec2-user@ip-10-51-0-10 ~]$
[ec2-user@ip-10-51-0-10 ~]$
[ec2-user@ip-10-51-0-10 ~]$
[ec2-user@ip-10-51-0-10 ~]$ ping 10.52.0.10
PING 10.52.0.10 (10.52.0.10) 56(84) bytes of data:
64 bytes from 10.52.0.10: icmp_seq=1 ttl=252 time=1.36 ms
64 bytes from 10.52.0.10: icmp_seq=2 ttl=252 time=1.60 ms
64 bytes from 10.52.0.10: icmp_seq=3 ttl=252 time=2.11 ms
64 bytes from 10.52.0.10: icmp_seq=4 ttl=252 time=1.75 ms
64 bytes from 10.52.0.10: icmp_seq=5 ttl=252 time=1.59 ms
64 bytes from 10.52.0.10: icmp_seq=6 ttl=252 time=2.03 ms
64 bytes from 10.52.0.10: icmp_seq=7 ttl=252 time=1.64 ms
^C
--- 10.52.0.10 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 8ms
rtt min/avg/max/mdev = 1.369/1.730/2.119/0.247 ms
[ec2-user@ip-10-51-0-10 ~]$
```



Lab 3: Distributed Firewall: Step 3.8

Verify traffic on TCP 8000 is flowing

The screenshot shows the Aviaatrix CoPilot interface. On the left sidebar, the 'Distributed Cloud Firewall' option is highlighted. The main panel shows the 'Monitor' tab of the Distributed Cloud Firewall. A filter is applied: 'Destination Port = 8000'. The table below shows traffic logs for the 'Allow-TCP-8000' rule.

Timestamp	Rule	L4/L7	Source SmartGroup	Destination SmartGroup	Source	Action	Enforced
Aug 14, 2023 4:35:01 PM	Allow-TCP-8000	L4	PROD	PROD	10.51.0.1	Permit	Yes
Aug 14, 2023 4:34:02 PM	Allow-TCP-8000	L4	PROD	PROD	10.52.0.1	Permit	Yes
Aug 14, 2023 4:34:02 PM	Allow-TCP-8000	L4	PROD	PROD	10.51.0.1	Permit	Yes
Aug 14, 2023 4:34:01 PM	Allow-TCP-8000	L4	PROD	PROD	10.51.0.1	Permit	Yes
Aug 14, 2023 4:33:32 PM	Allow-TCP-8000	L4	PROD	PROD	10.52.0.1	Permit	Yes
Aug 14, 2023 4:33:32 PM	Allow-TCP-8000	L4	PROD	PROD	10.52.0.1	Permit	Yes
Aug 14, 2023 4:33:32 PM	Allow-TCP-8000	L4	PROD	PROD	10.51.0.1	Permit	Yes

Go to the **Monitor** of your Distributed Cloud Firewall **1**

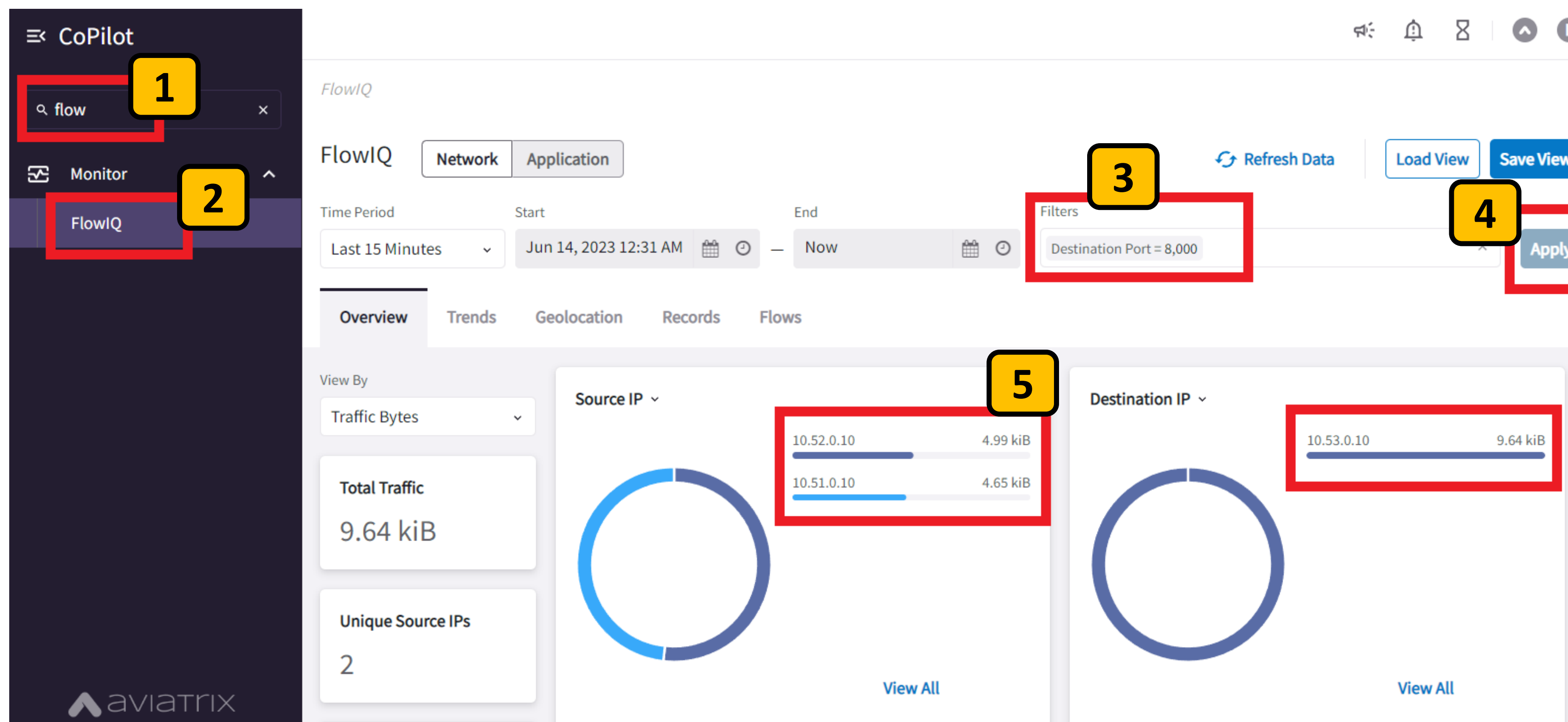
Click the **Filter icon**. **2**

Search for traffic where the **Destination Port = 8000** **3**

Observe the sessions that have now been flowing between PROD instances on TCP 8000

Lab 3: Distributed Firewall: Step 3.9

Inspect traffic details for TCP 8000 in FlowIQ



Type **flow** in the CoPilot search bar (1)

Click **Apply** (4)

Select the **FlowIQ** search result (2)

Observe the top talker on TCP 8000 (5)

Filter for **Destination Port = 8000** (3)

Lab 3: **EXTRA CREDIT:** Troubleshooting

Troubleshoot connectivity issue

Go back the console session of the SAP1 instance you opened earlier or open it again.

Try to PING the SAP3 instance by issuing the command:

ping 10.53.0.10 1

This ping *SHOULD* work because your Distributed Cloud Firewall now allows these two instances in the PROD group to ping.

Why is this not working???

Let's use CoPilot to troubleshoot...

Session ID: MasterKey-04317290154b074ef

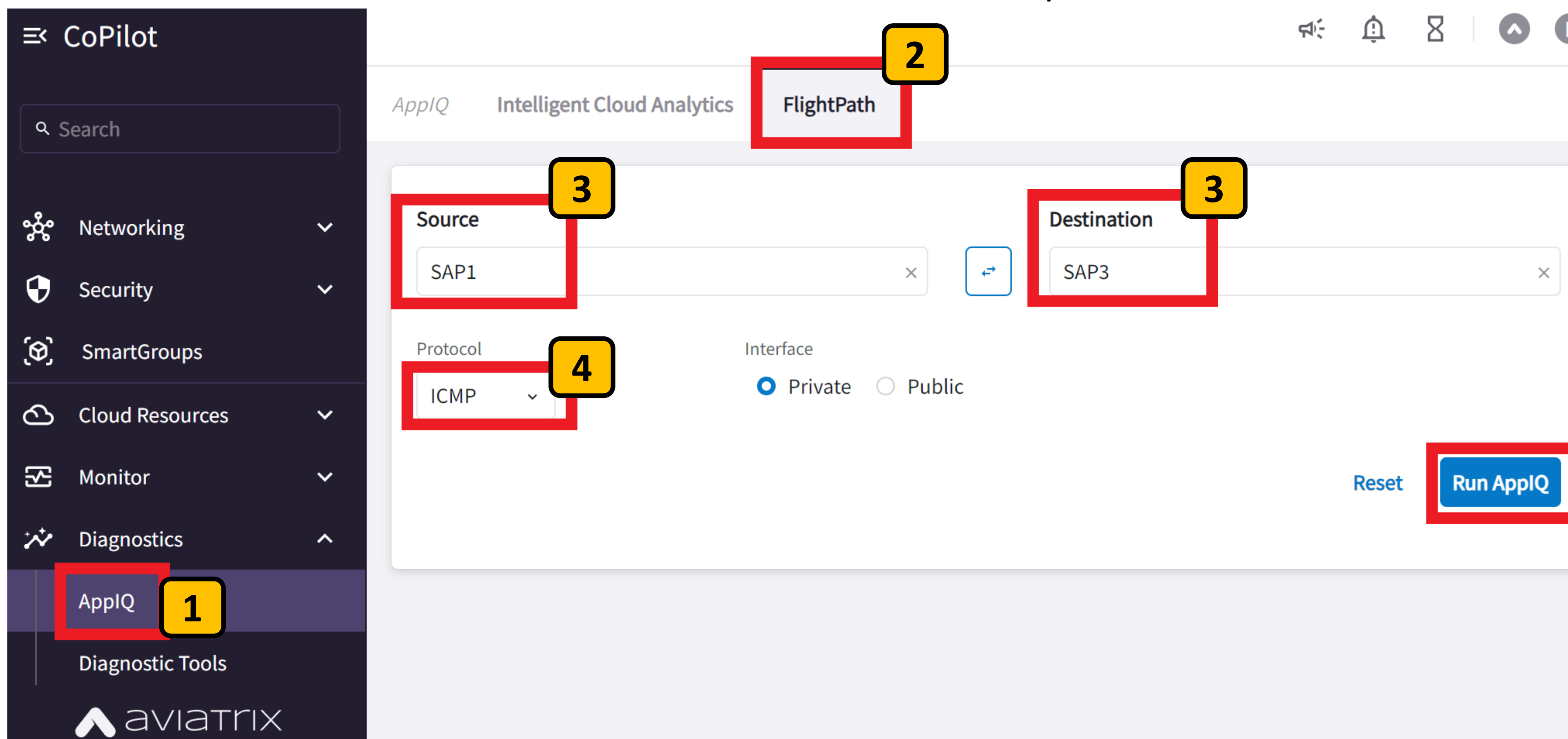
Instance ID: i-05a44a91c82c8ab4d

```
[ec2-user@ip-10-51-0-10 ~]$
[ec2-user@ip-10-51-0-10 ~]$
[ec2-user@ip-10-51-0-10 ~]$
[ec2-user@ip-10-51-0-10 ~]$ 1
[ec2-user@ip-10-51-0-10 ~]$ ping 10.53.0.10
PING 10.53.0.10 (10.53.0.10) 56(84) bytes of data.
```



Lab 3: EXTRA CREDIT: Troubleshooting

Troubleshoot connectivity issue



From the CoPilot navigation select **ApplQ** under **Diagnostics**. 1

Select the **FlightPath** tab. 2

Select **SAP1** as the Source and **SAP3** as the Destination. 3

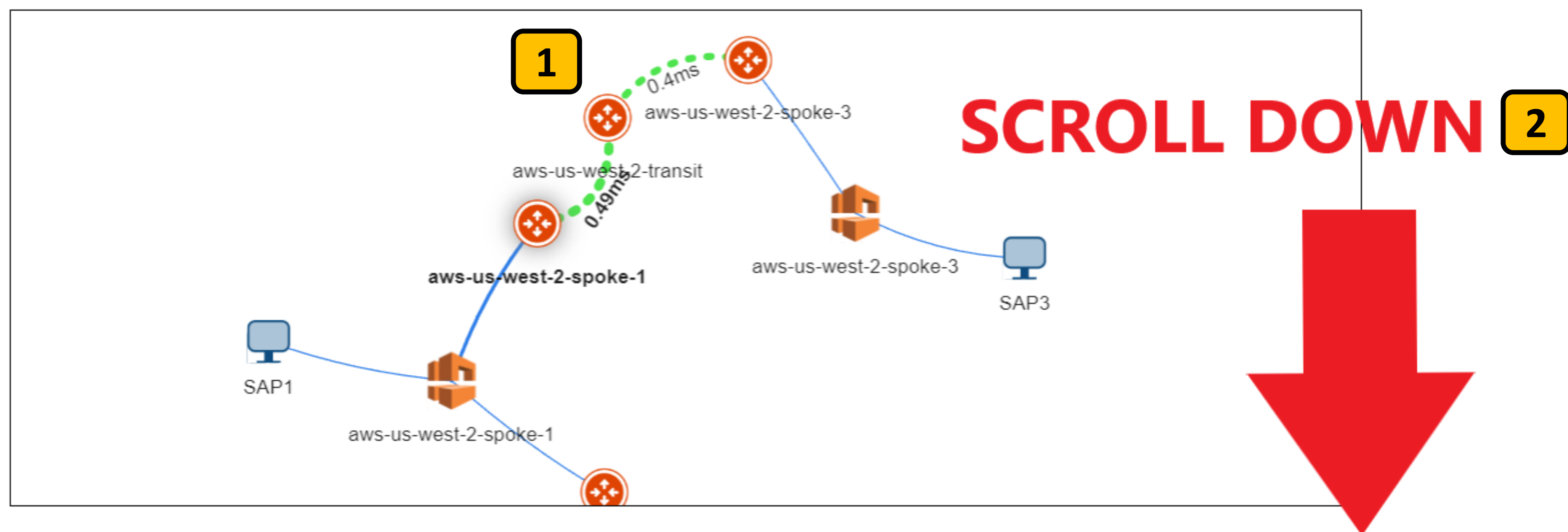
Select **ICMP** as the Protocol and click **Run ApplQ** 4

Lab 3: EXTRA CREDIT: Troubleshooting

Troubleshoot connectivity issue



ApplQ Report for SAP1 => SAP3



Observe the topology between these instances and the latency. 1

Scroll down and view all of the details in the complete report. 2

Did CoPilot find the problem?? What was it??

Lab 3: EXTRA CREDIT: Troubleshooting

Troubleshoot connectivity issue

Fix the issue that CoPilot found in the ApplQ report.

From the SAP1 CLI: Try to PING the SAP3 instance again by issuing the command:

ping 10.53.0.10 **1**

Does your ping work now? **2**

Session ID: MasterKey-0de433d888dbda49c

Instance ID: i-05a44a91c82c8ab4d

```
[ec2-user@ip-10-51-0-10 ~]$  
[ec2-user@ip-10-51-0-10 ~]$  
[ec2-user@ip-10-51-0-10 ~]$  
[ec2-user@ip-10-51-0-10 ~]$ ping 10.53.0.10
```

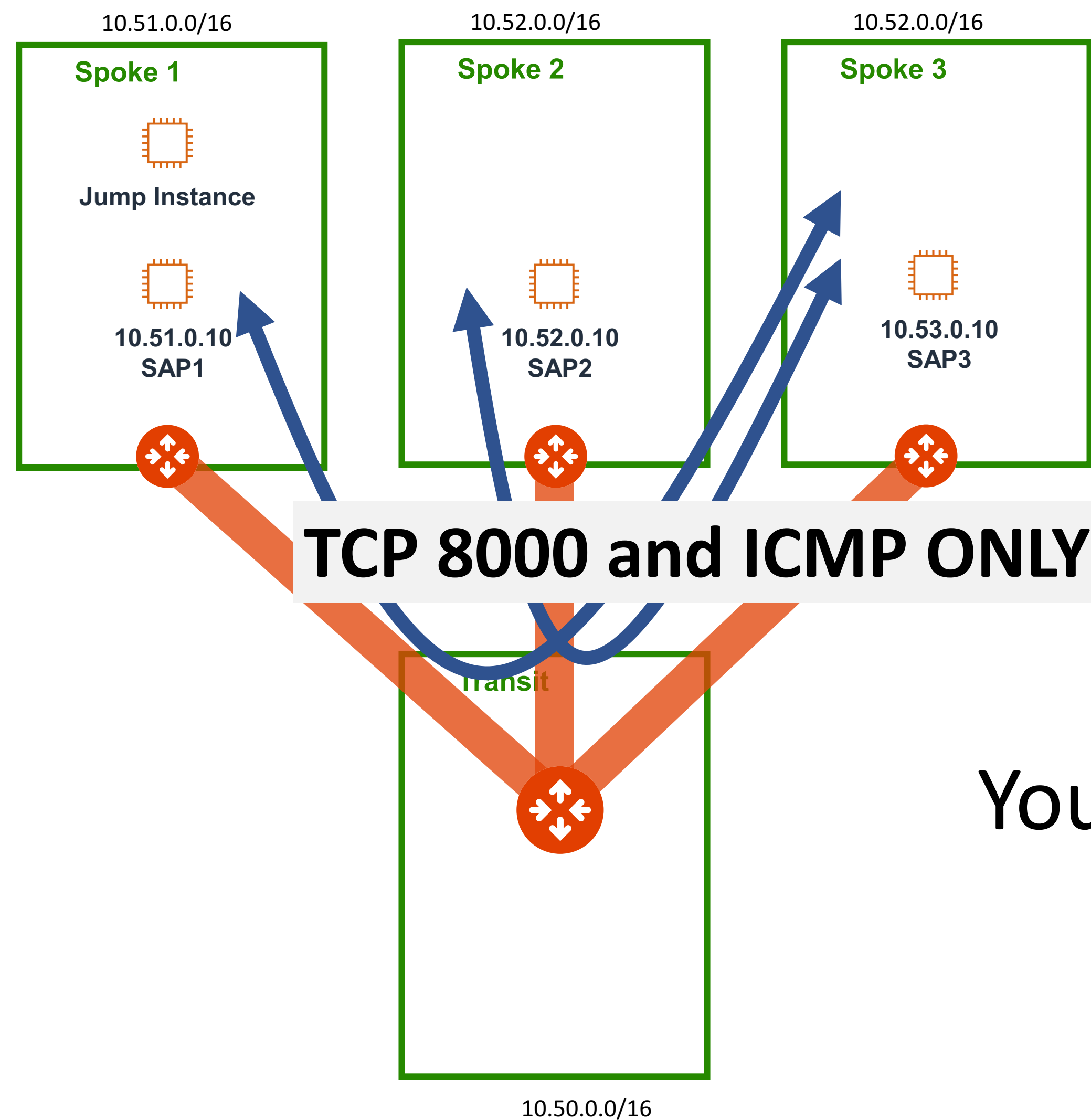
1

2 **???**

Lab 3 Success

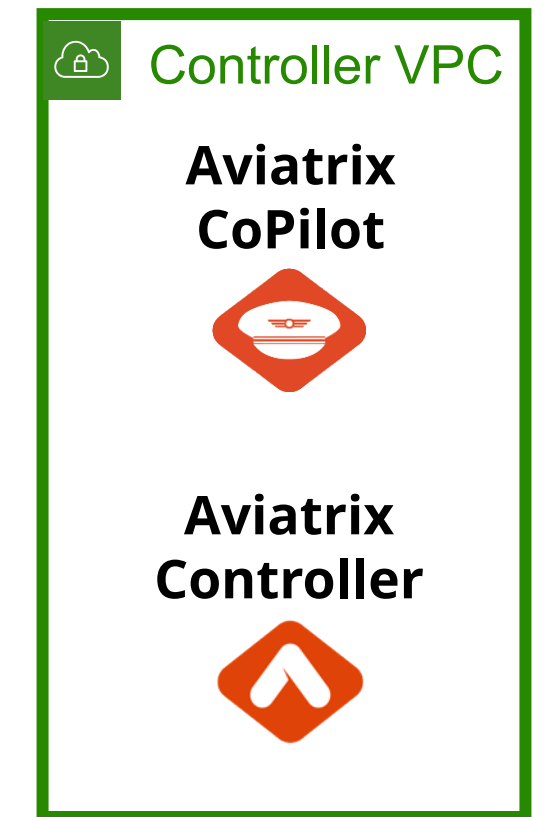
Distributed Firewall EAST-WEST security

PROD



AWS us-west-2

SUCCESS!! You completed Lab 3!
You're awesome.



AWS us-east-1

You just deployed a Distributed Cloud
Firewall for East-West filtering.
How cool is that??