AWS Immersion Day
LAB 3

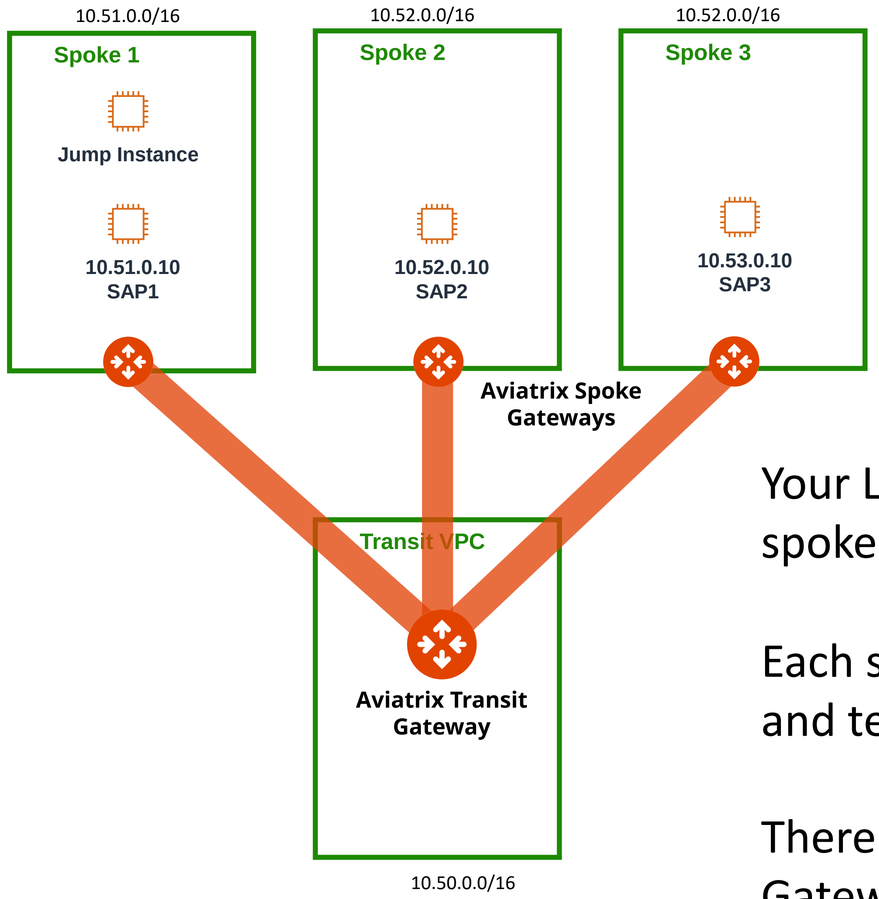
SECURITY: DISTRIBUTED FIREWALL FOR EAST-WEST SECURITY

Brad Hedlund
Principal Solutions Architect,
Aviatrix Systems

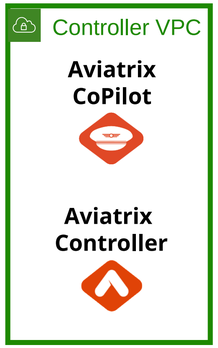
aviatrix

Lab 3 Intro

Distributed Firewall for EAST-WEST



AWS us-west-2



AWS us-east-1

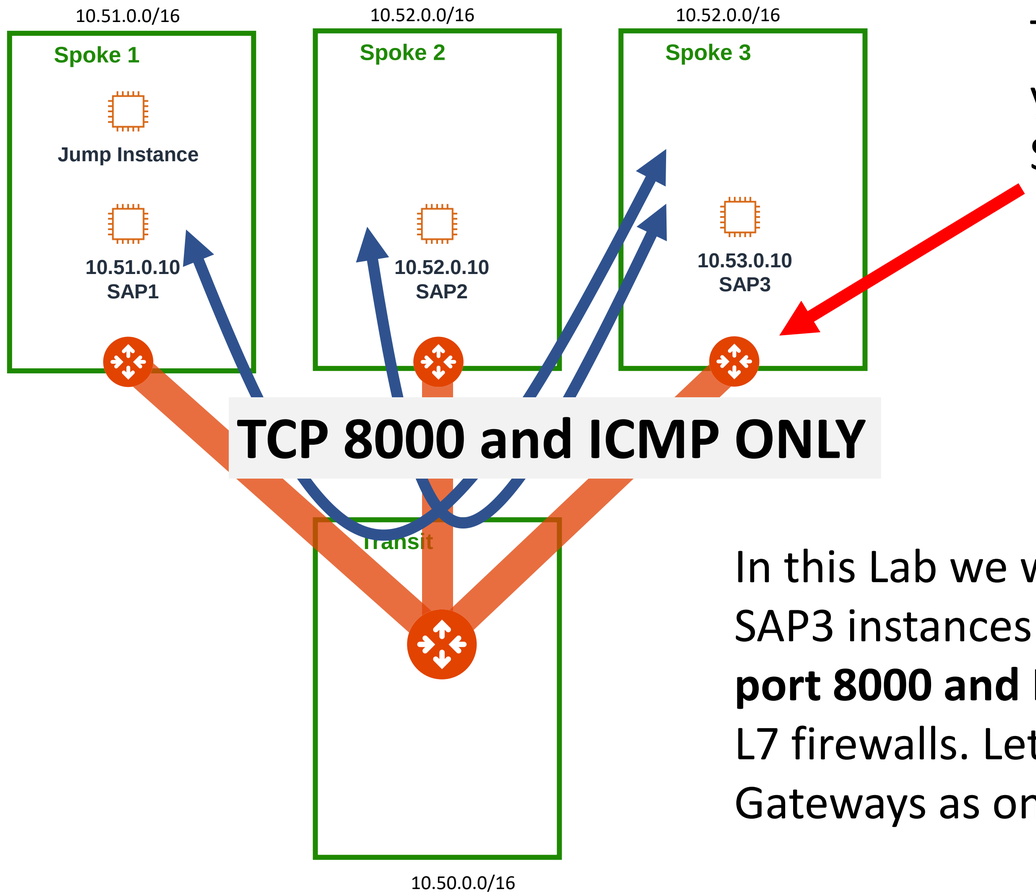
Your Lab account has a full Aviatrix hub-and-spoke architecture deployed in **us-west-2**

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.

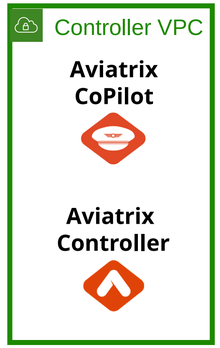
Lab 3 Intro

Distributed Firewall for EAST-WEST



AWS us-west-2

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** !

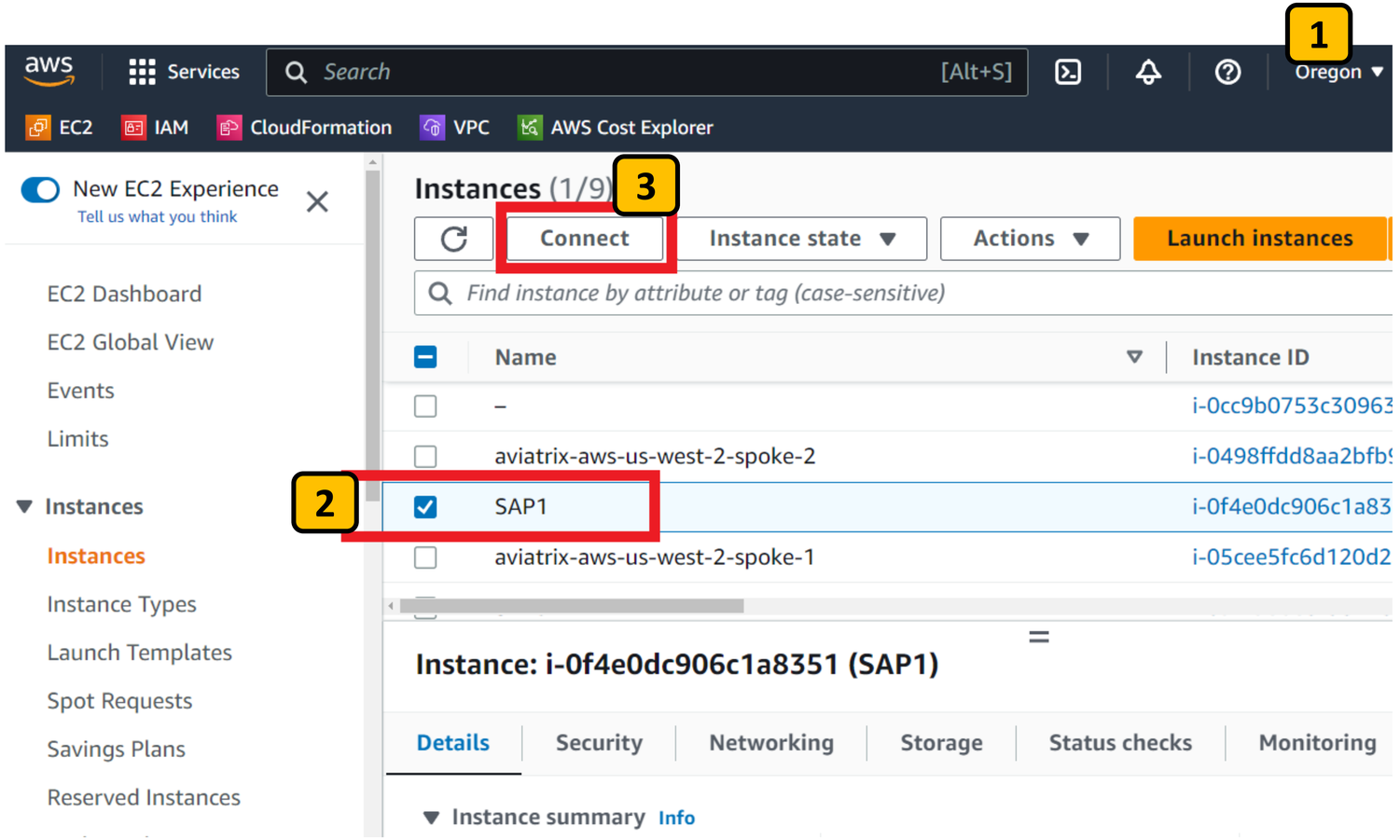
Lab 3: Distributed Firewall: Step 3.1

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



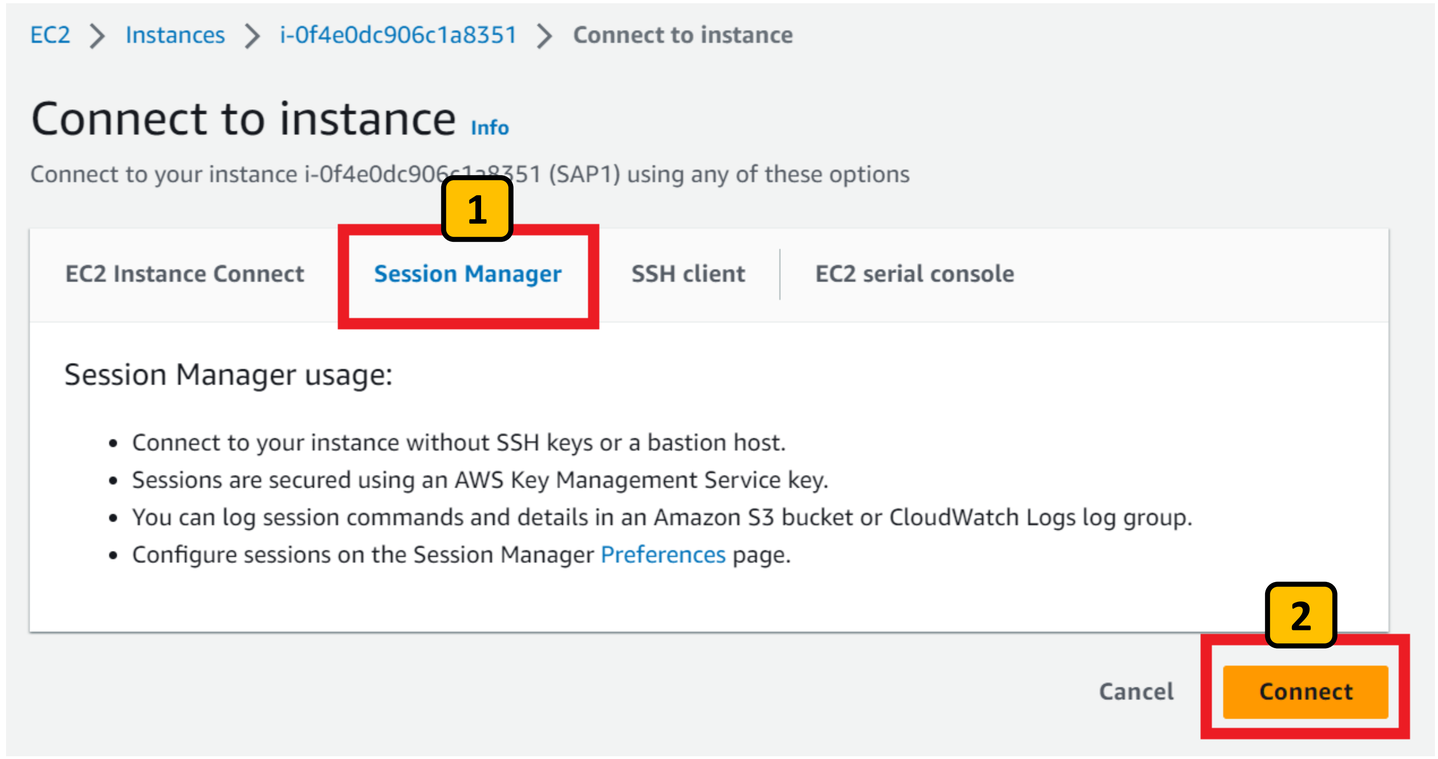
Lab 3: Distributed Firewall: Step 3.2

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



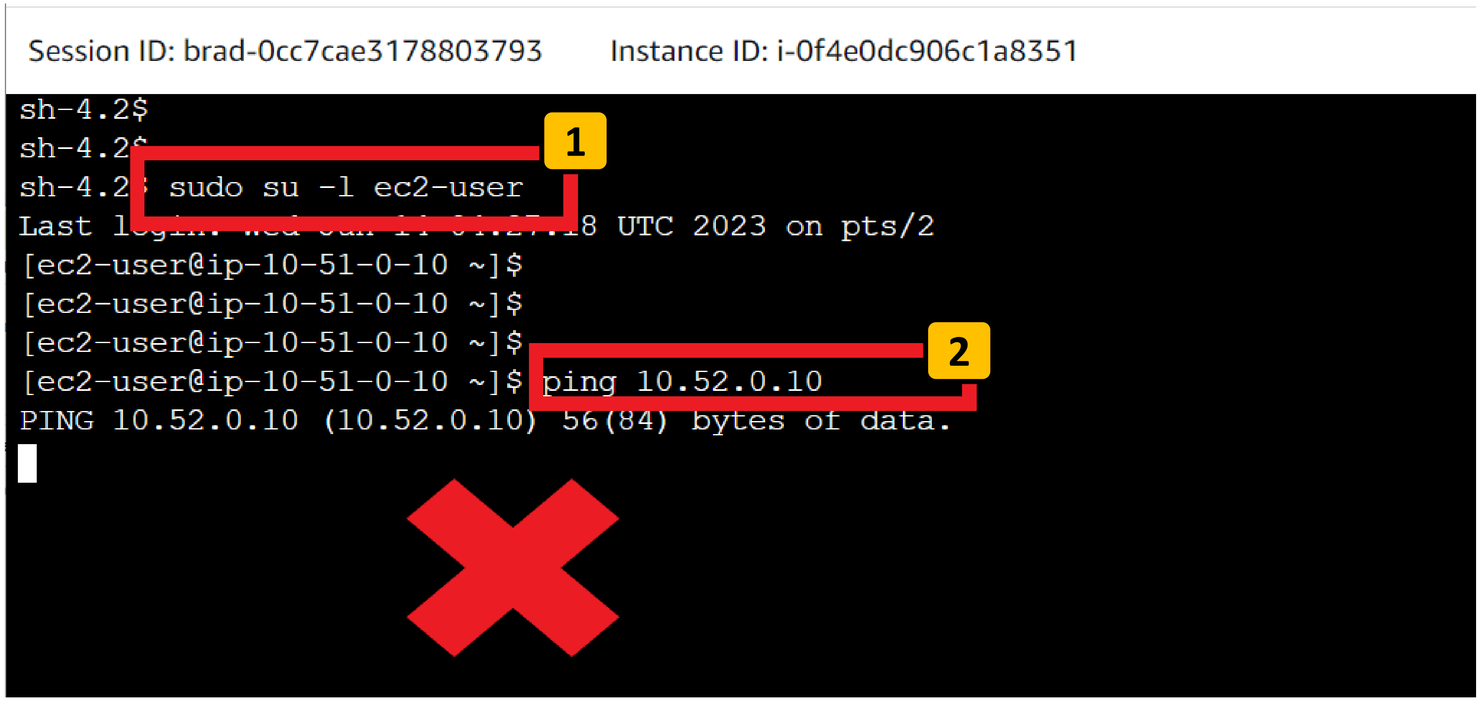
Lab 3: Distributed Firewall: Step 3.3

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.



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**

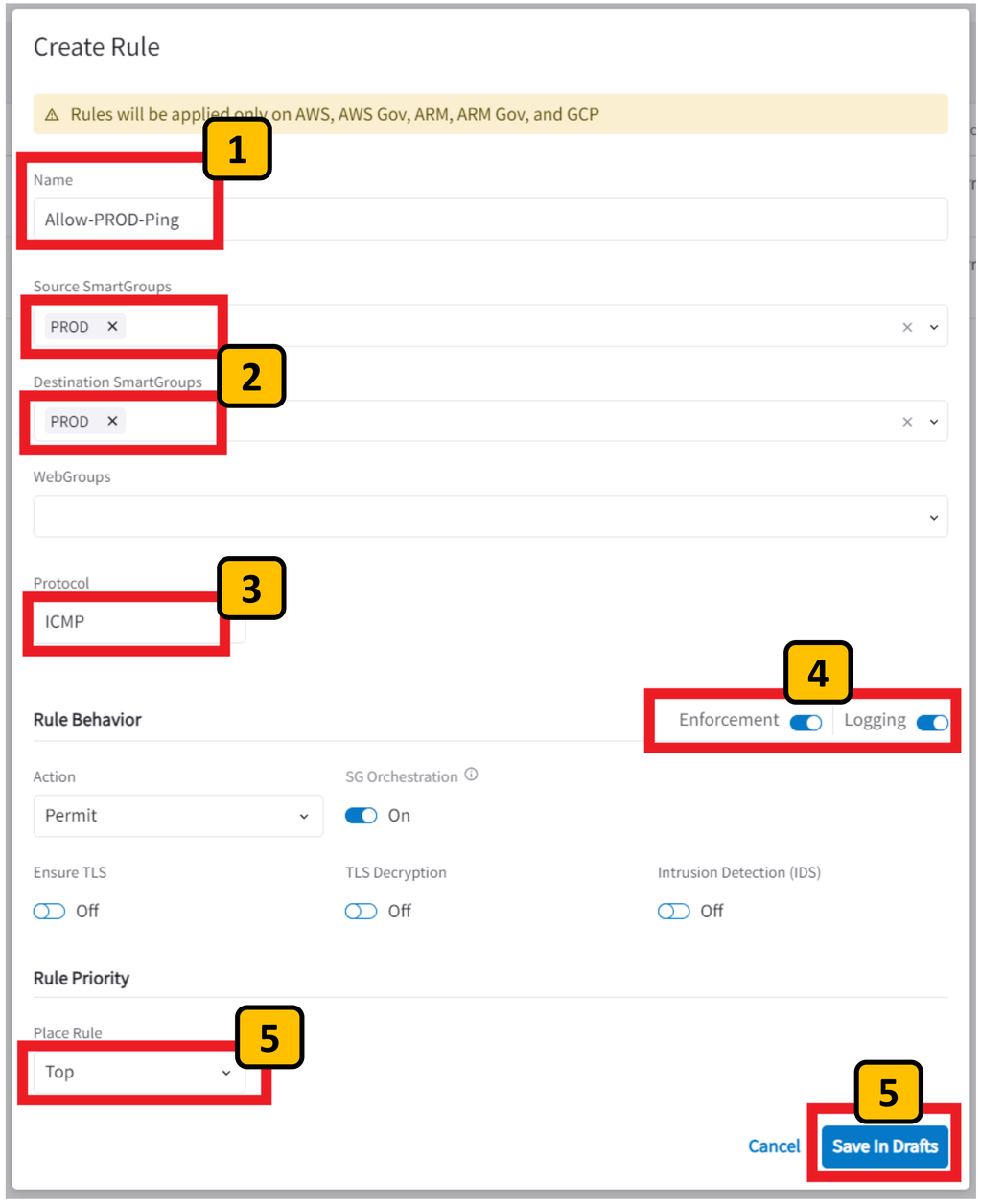
Name the rule Allow-PROD-Ping 1

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



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**

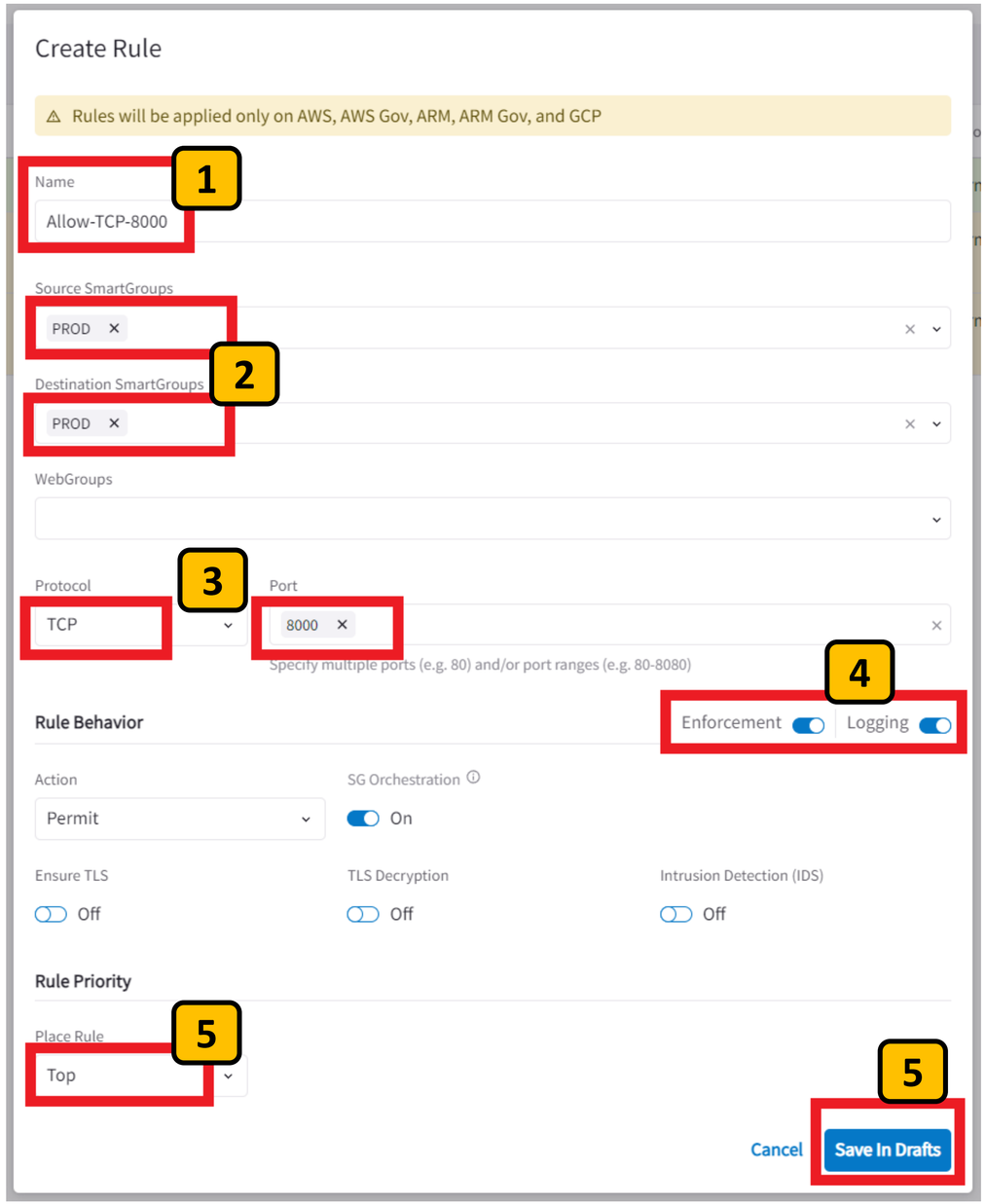
Name the rule Allow-TCP-8000 1

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

Set Protocol to TCP and Port to 8000 3

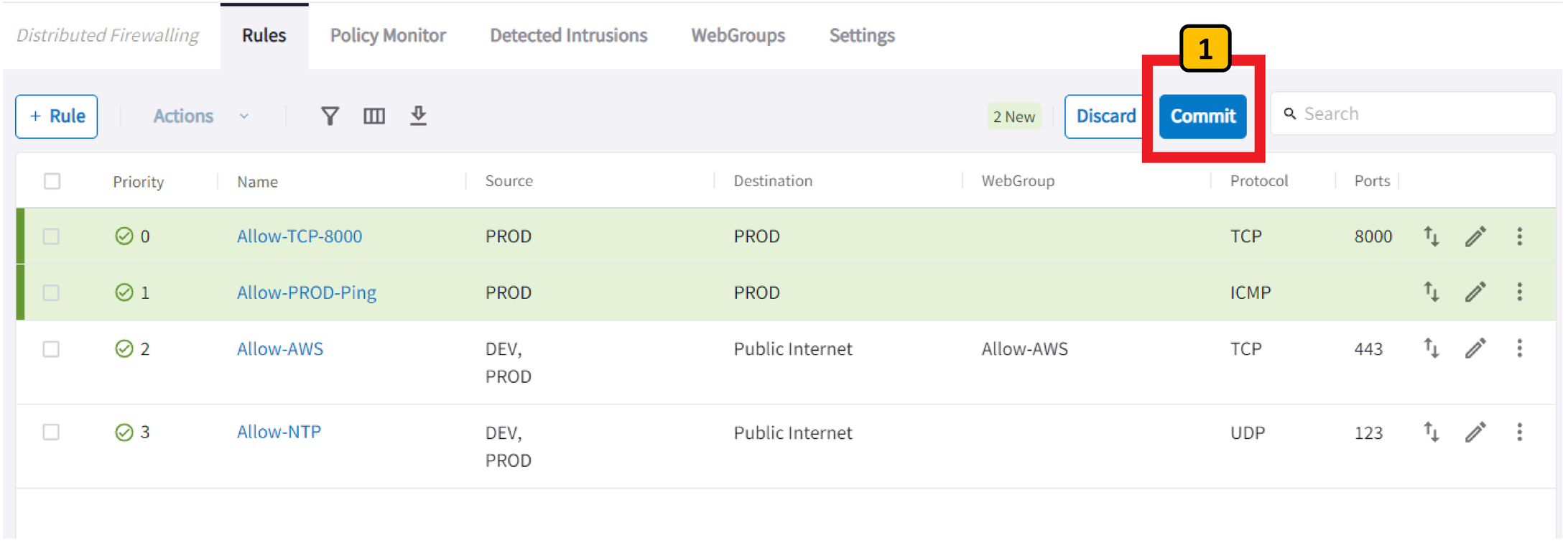
Enable Enforce and Logging 4

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



Lab 3: Distributed Firewall: Step 3.6

Commit east-west rules



Commit your new Distributed Firewall Rules 1

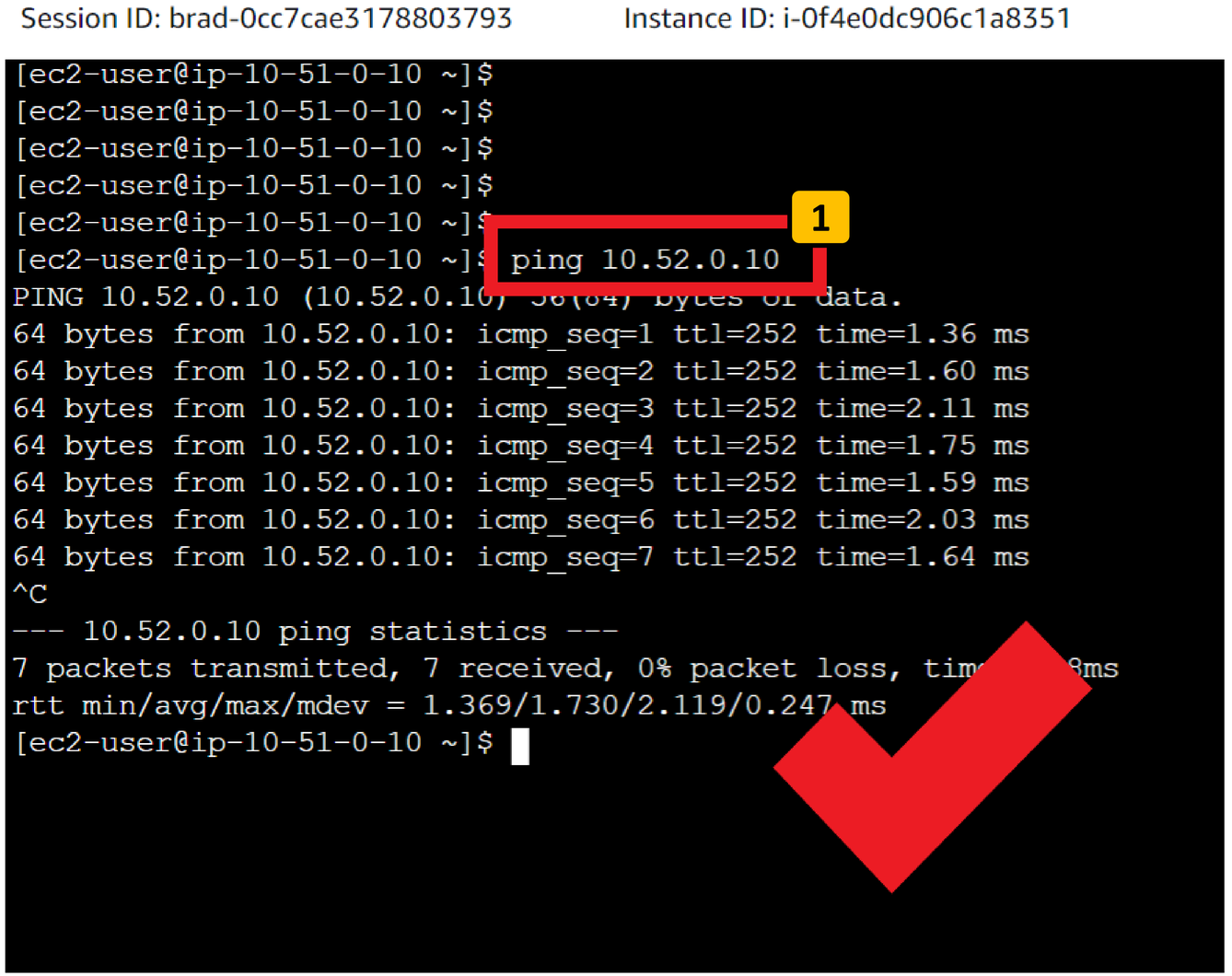
Lab 3: Distributed Firewall: Step 3.7

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.

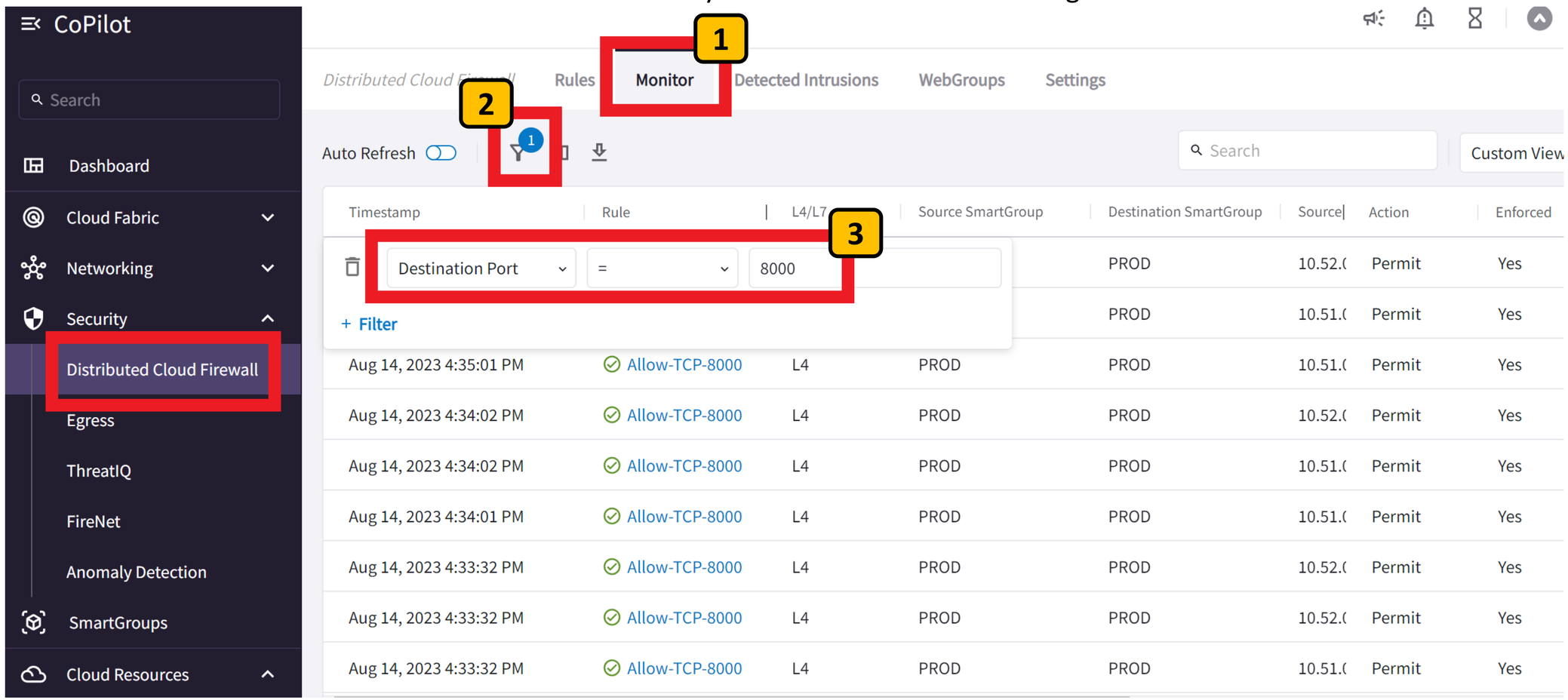
Try to PING the SAP2 instance by issuing the command:
ping 10.52.0.10 1

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



Lab 3: Distributed Firewall: Step 3.8

Verify traffic on TCP 8000 is flowing



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

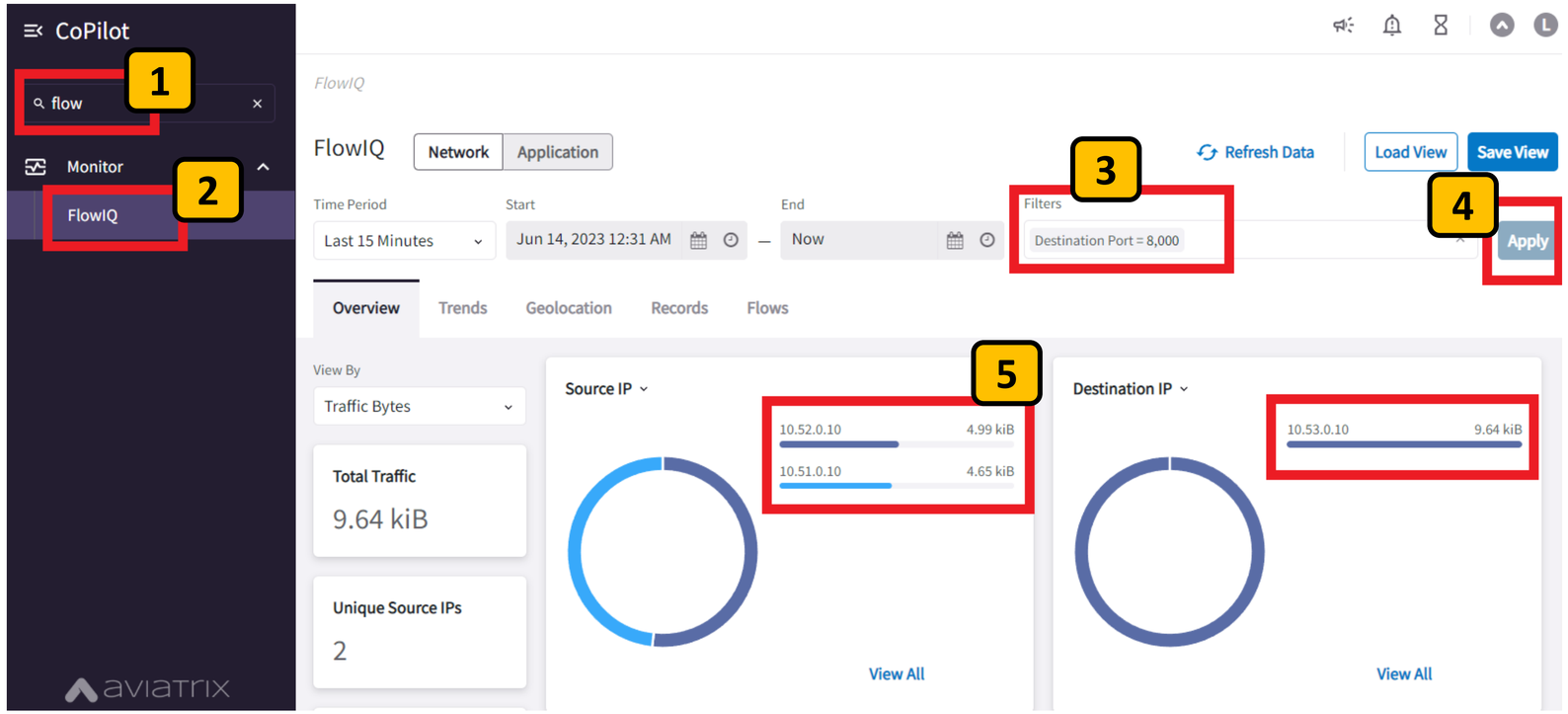
Click the **Filter icon**. 2

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

Select the **FlowIQ** search result 2

Filter for **Destination Port = 8000** 3

Click **Apply** 4

Observe the top talker on TCP 8000 5

Lab 3: EXTRA CREDIT: Troubleshooting

Troubleshoot connectivity issue

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

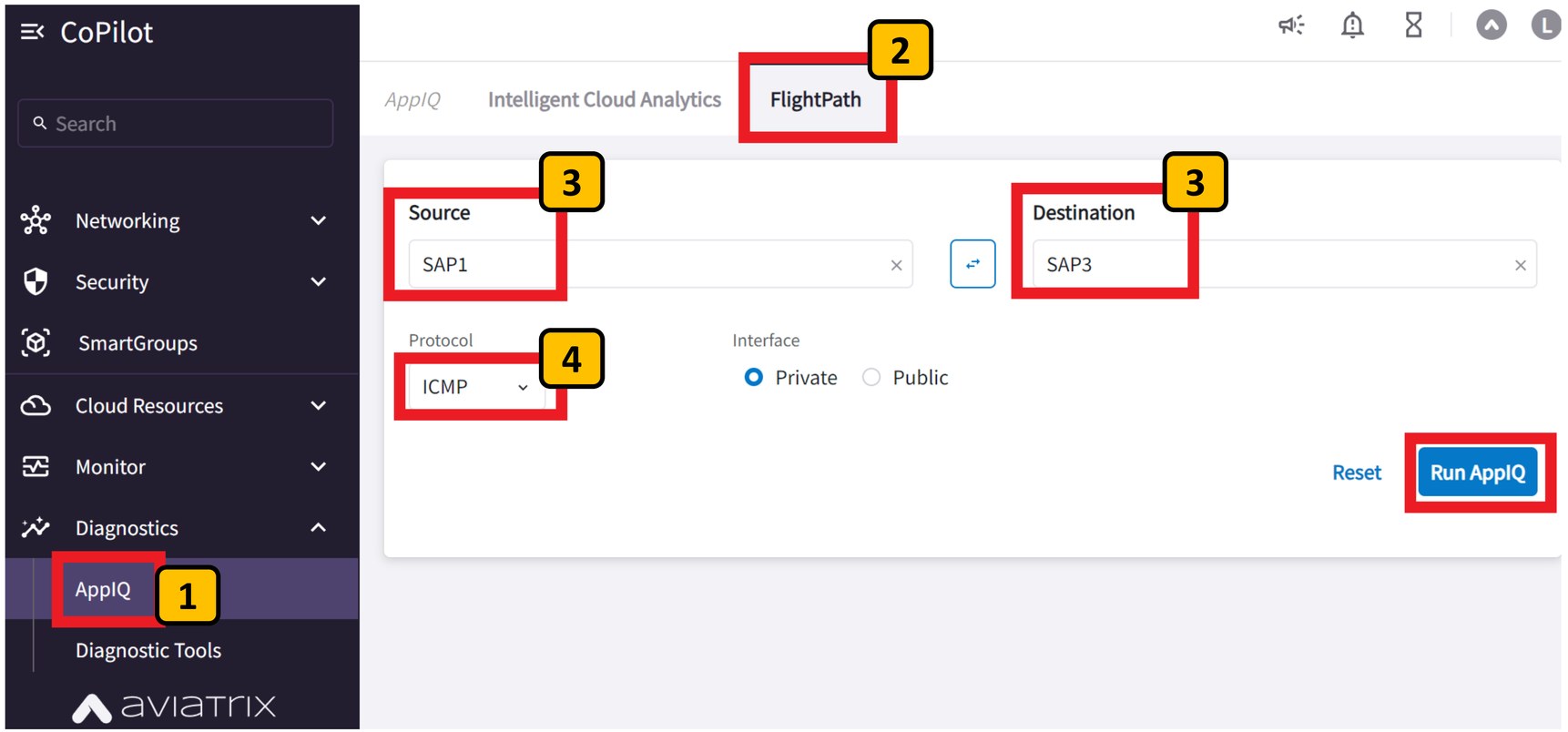
Try to PING the SAP3 instance by issuing the command:
ping 10.53.0.10 1

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…

Lab 3: EXTRA CREDIT: Troubleshooting

Troubleshoot connectivity issue



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

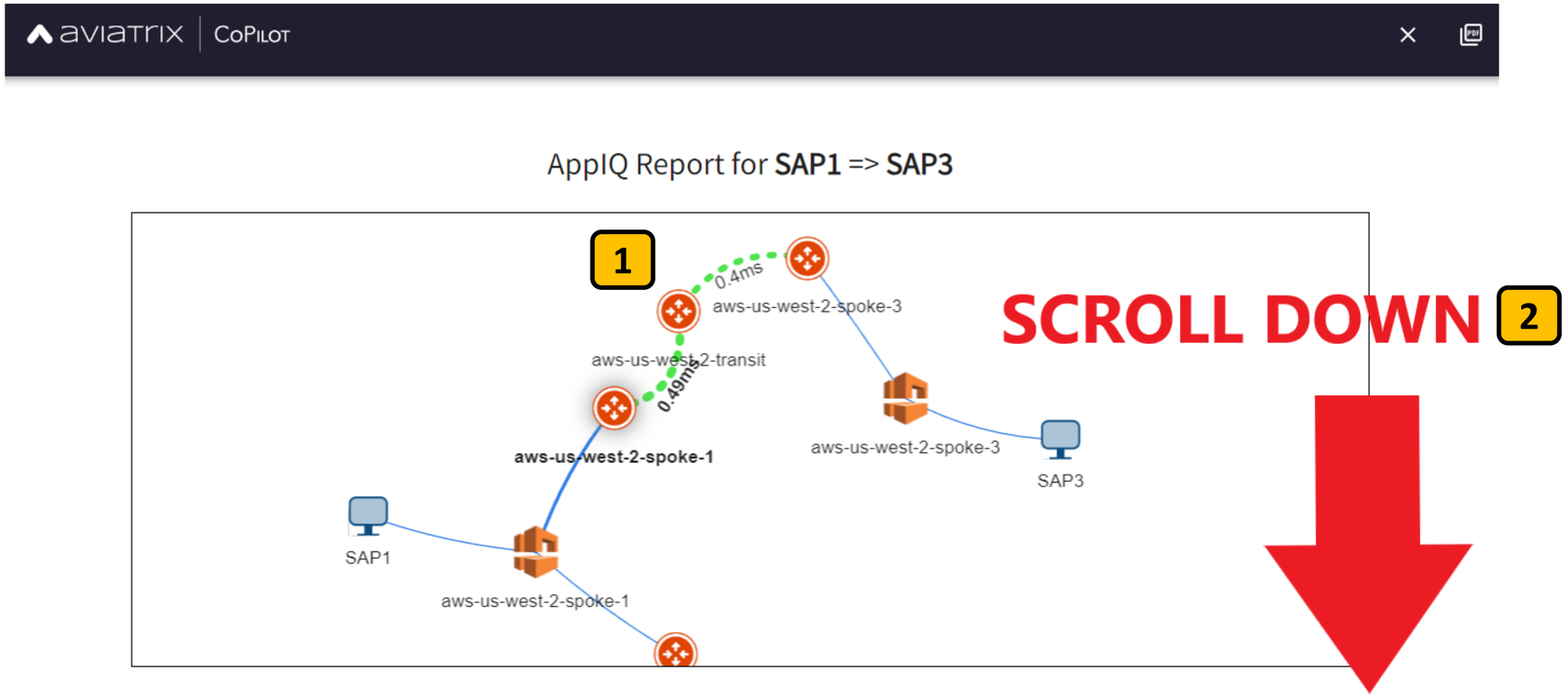
Select the **FlightPath** tab. 2

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

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

Lab 3: EXTRA CREDIT: Troubleshooting

Troubleshoot connectivity issue



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

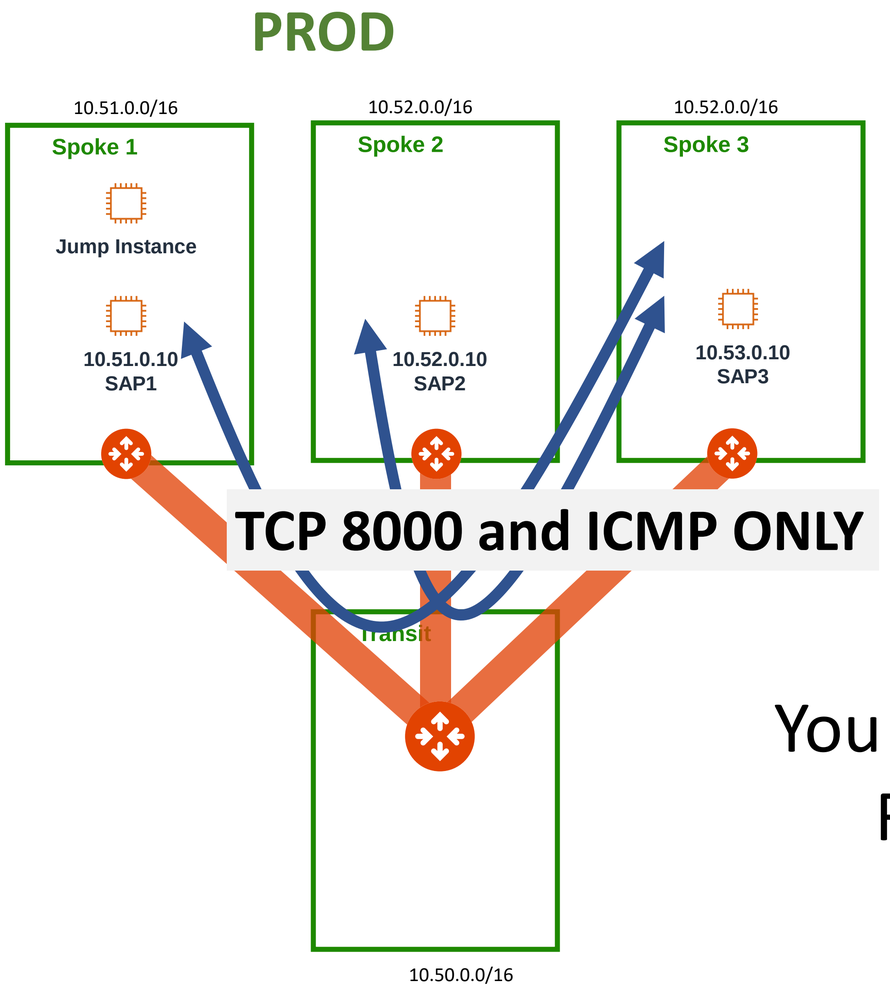
Fix the issue that CoPilot found in the AppIQ report.

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

Lab 3 Success

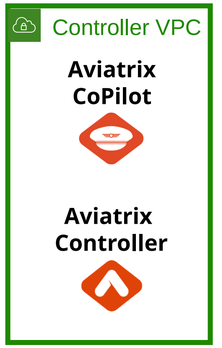
Distributed Firewall EAST-WEST security



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??