AWS Immersion Day
LAB 3

VISIBILITY: FLOWIQ

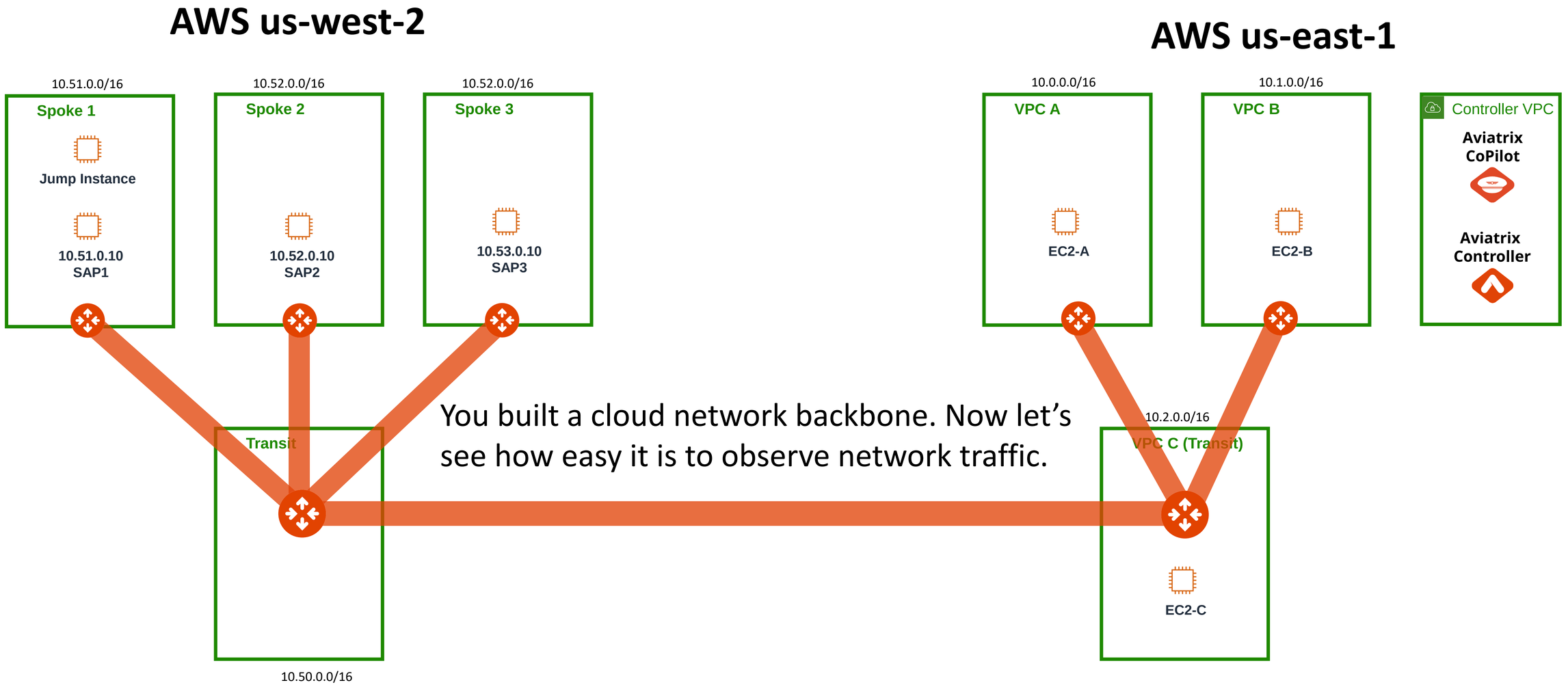
EXAMINE NETWORK TRAFFIC DETAILS WITH EASE

Brad Hedlund
Principal Solutions Architect, Aviatrix Systems

aviatrix

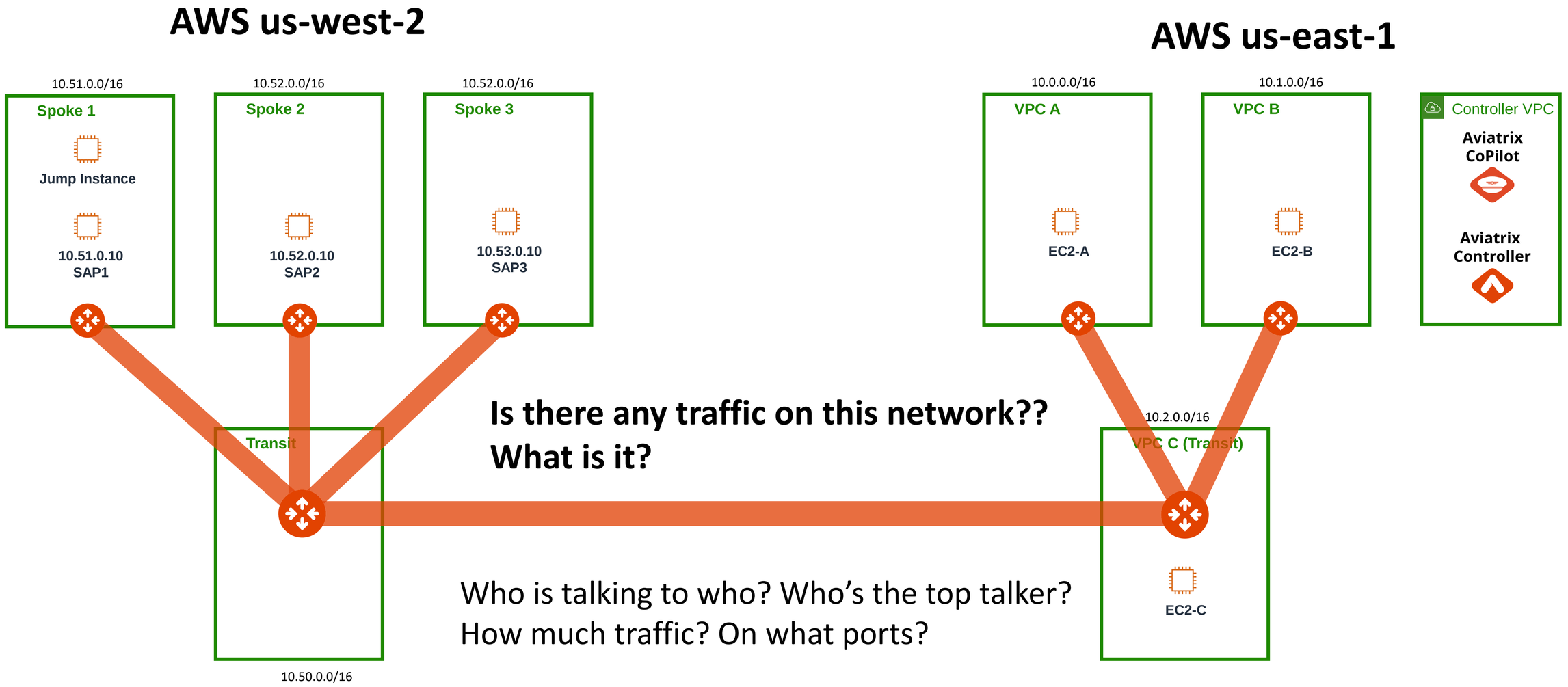
Lab 2 Recap

What you built in the previous lab



Lab 3 Intro

Observe network traffic details



Let's find out… (next)

Lab 3: Step 3.0

Find the top talker in Aviatrix CoPilot FlowIQ dashboard

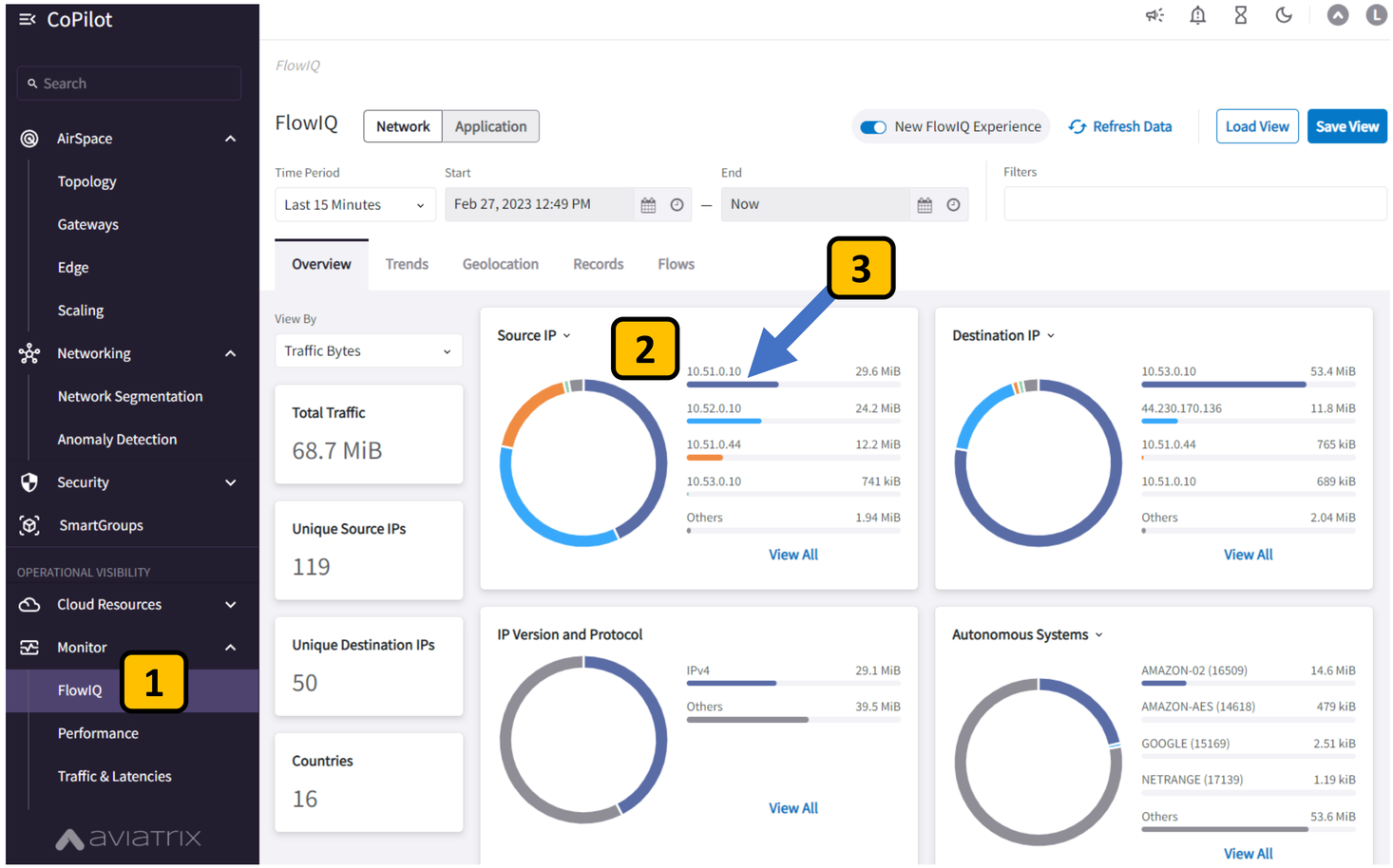
From CoPilot, go to Monitor > **FlowIQ** 1

Aviatrix Gateways send full Netflow v9 to CoPilot so you can see all the traffic flowing through your cloud network.

FlowIQ is the dashboard where you can drill down on this traffic data.

Can you find the top talker? (hint) 2

Click on the first IP address listed in the Source IP widget. Copilot will drill down showing all traffic from that IP 3



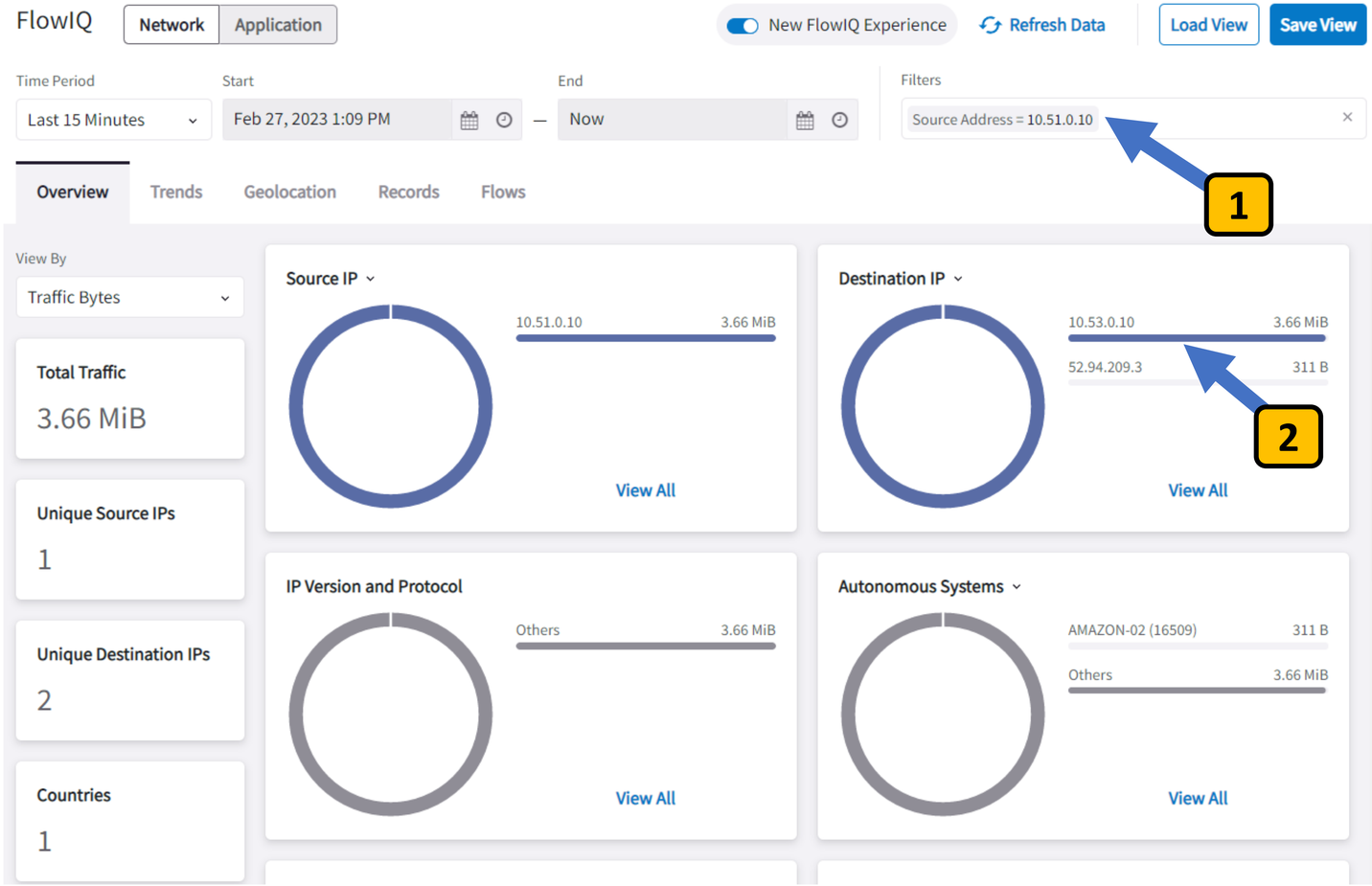
Lab 3: Step 3.1

Find who the top talker is talking to (the most)?

When clicked on the top Source IP in the previous step, CoPilot built a filter for you on the fly, to focus on traffic from that IP 1

Now you can see the top destination our top talker is talking to. 2

Click on the top Destination IP to refine our filter more. 2



Lab 3: Step 3.2

Find who the top talker is talking to (the most)?

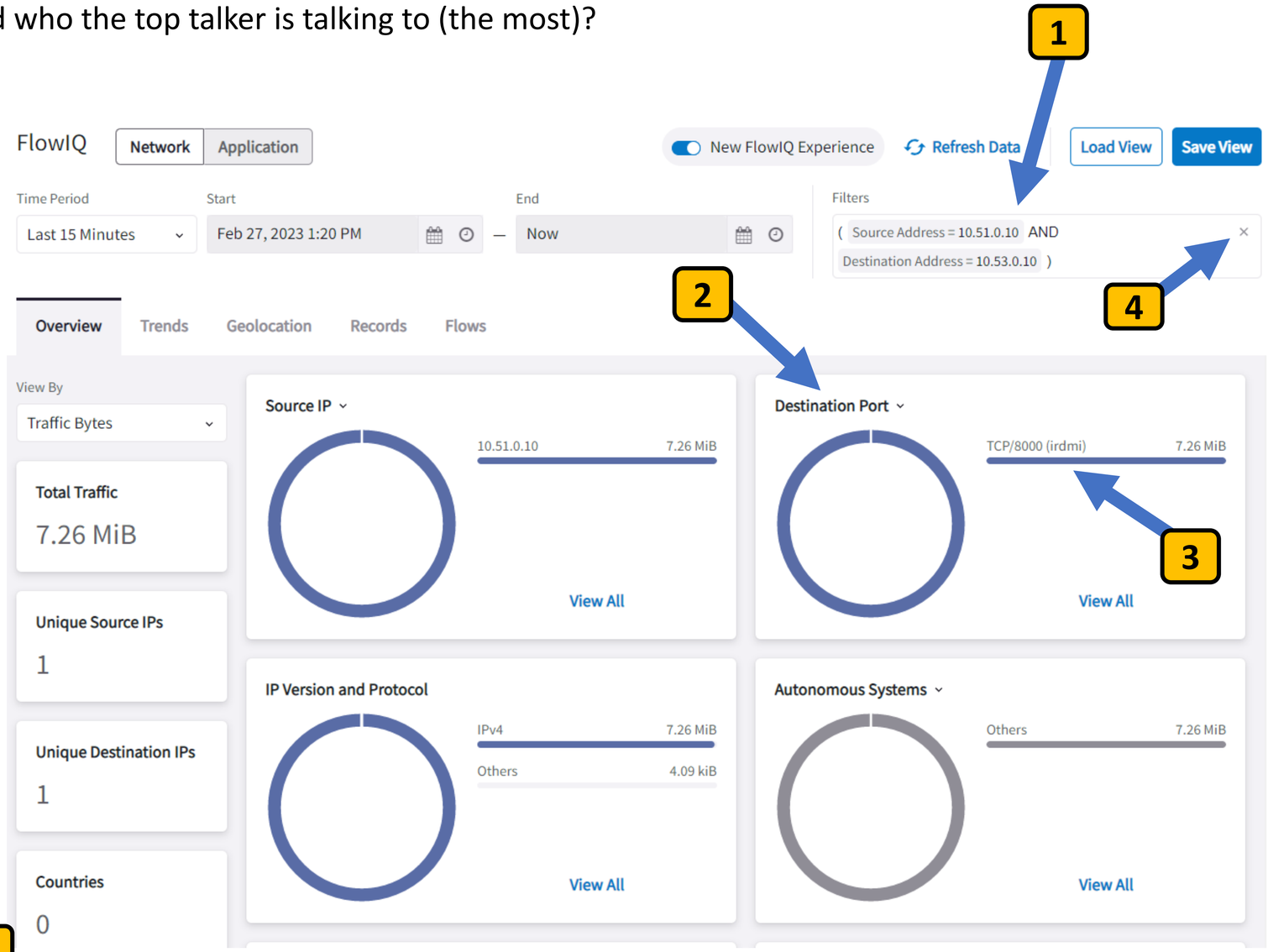
When you clicked the top Destination IP in the previous step, CoPilot expanded the filter for you, to focus on traffic between these two IPs 1

What port number are they talking on?

Click on the top “Destination IP” drop down and select “Destination Port” 2

What TCP/UDP port number is used the most? 3

Clear your filter to see all traffic again 4



Lab 3: Step 3.3

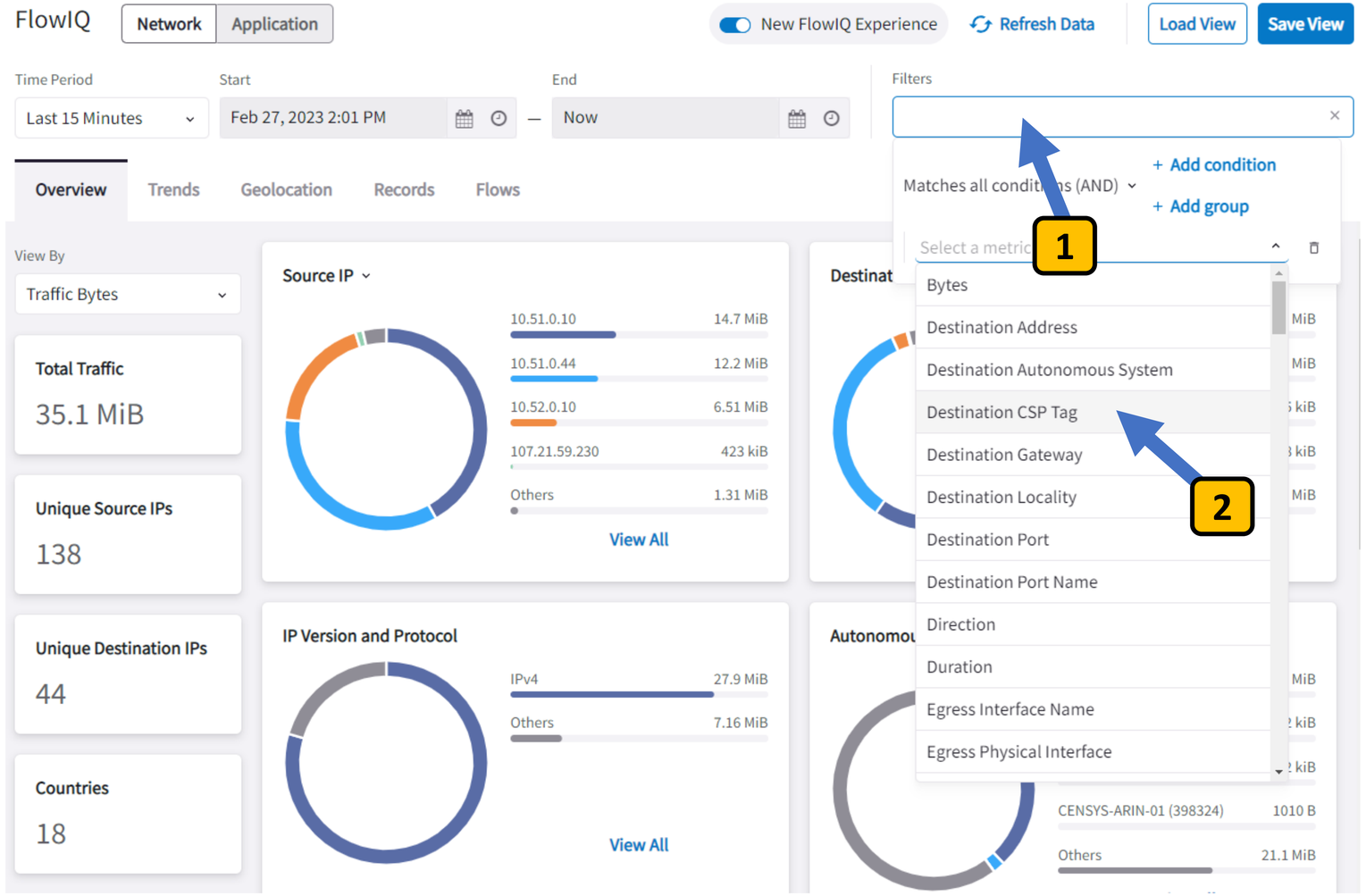
Filter traffic using native CSP Tags

CoPilot knows about all of instances in your cloud and what tags have been applied to them.

You can use these tags to drill down on traffic without thinking about IP addresses.

Click the Filters box, then click Select a metric. 1

From the drop-down pick Destination CSP Tag 2



Lab 3: Step 3.4

Filter traffic using native CSP Tags

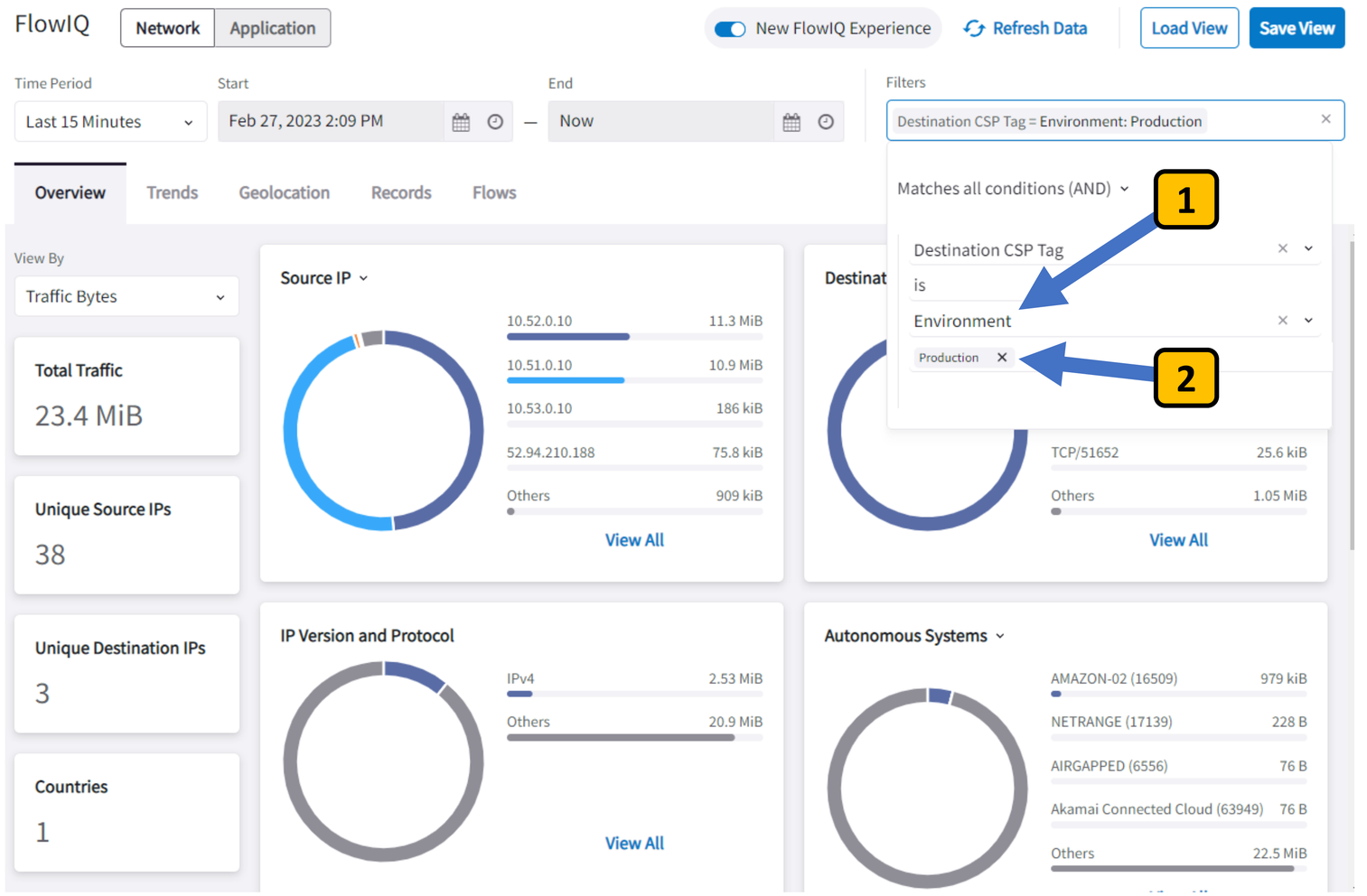
Select the tag name **Environment** 1

Select the tag value to **Production** 2

I just want to see my production traffic. I don't want to think about which IP ranges to filter on.

Presto! You are now seeing all traffic destined to any instance with the tag **Environment = Production**

As new instances are launched with that tag, their traffic will be displayed here too.



Lab 3: Step 3.5

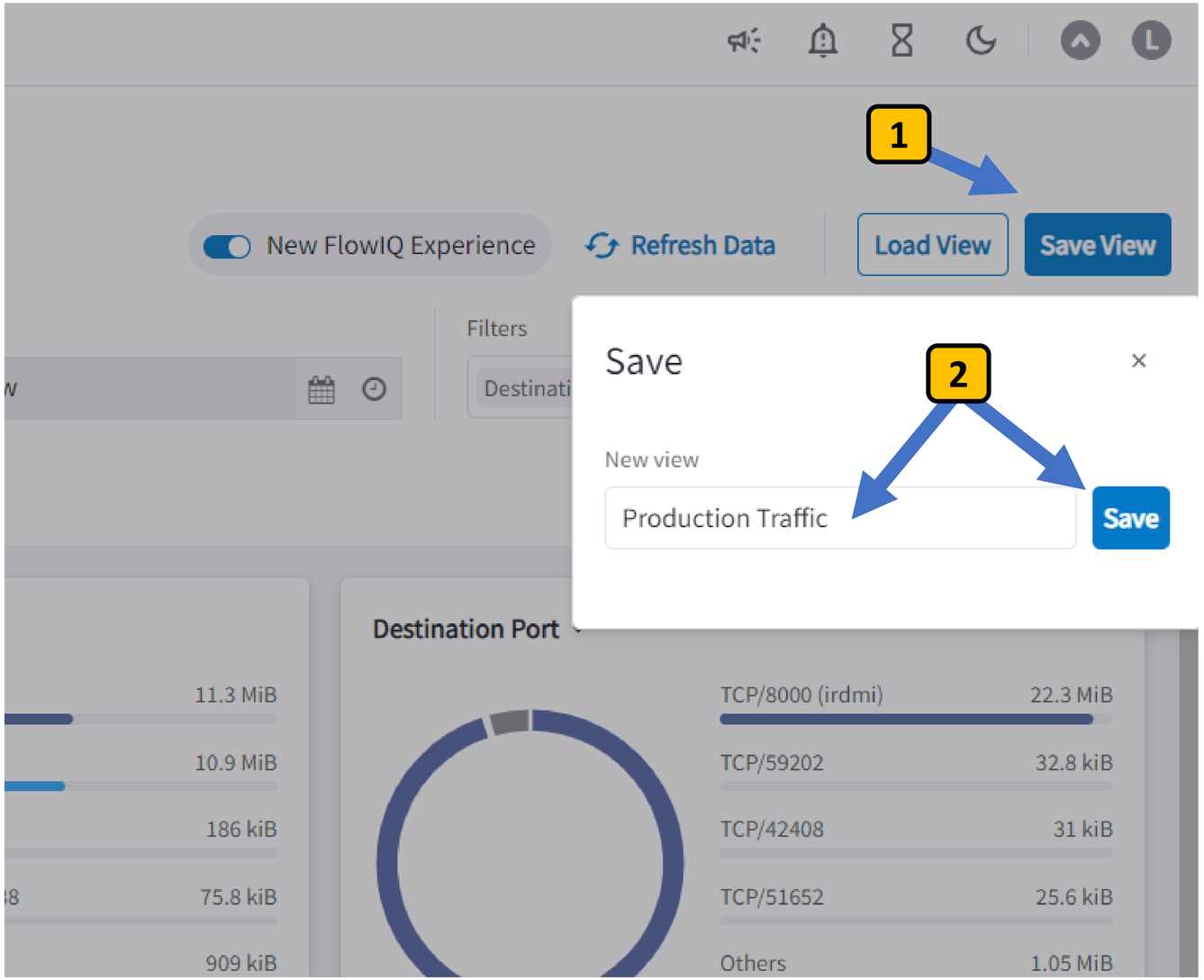
Save your filter view

When you create a useful filter in FlowIQ you can save it to use again later.

Let’s save our Production traffic (using CSP tags) view.

Click **Save View** 1

Give the filter a name and click **Save** 2



Lab 3: Step 3.6

What countries is your cloud network talking to?

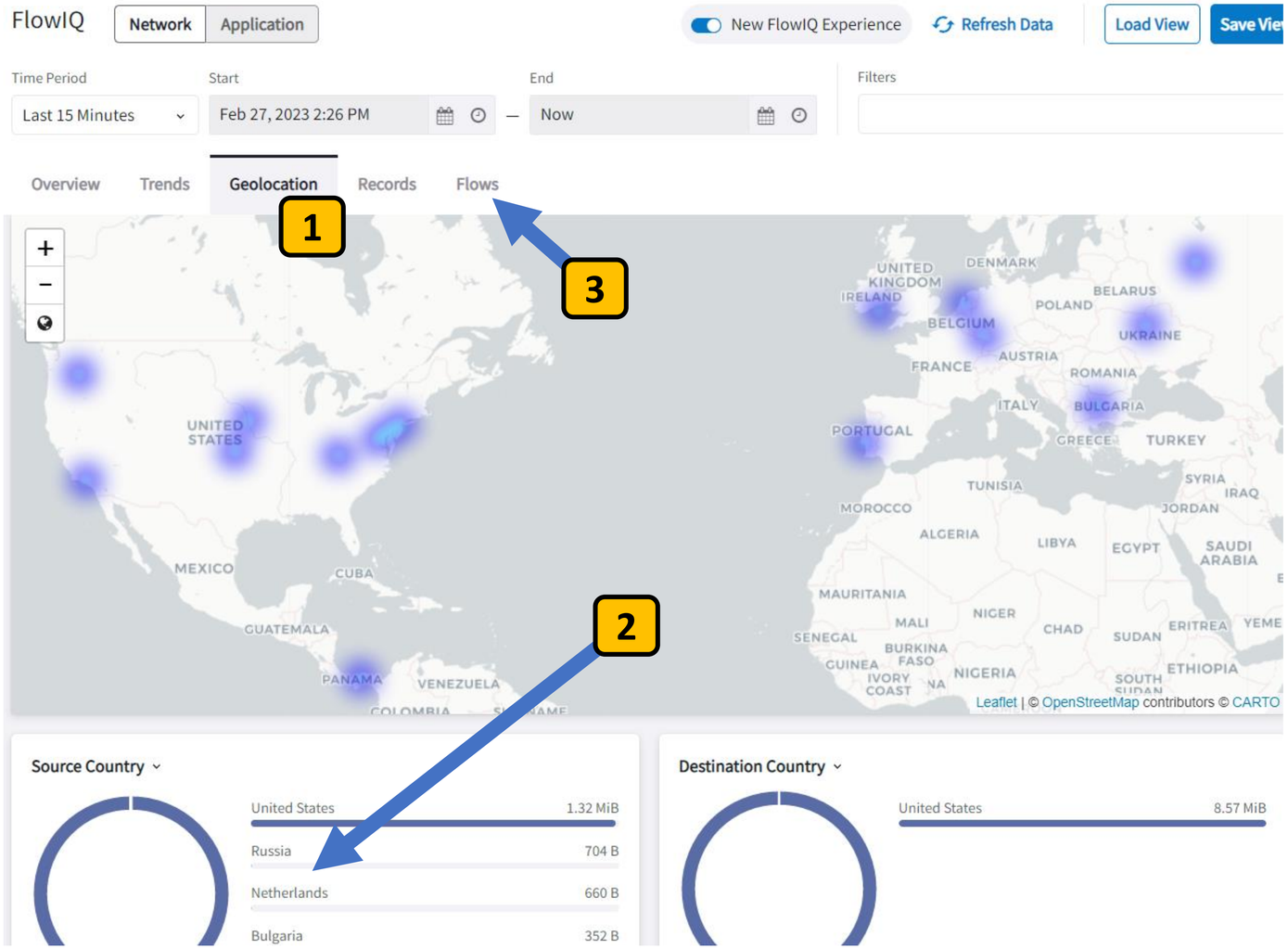
FlowIQ can geolocate the public IP addresses communicating with instances in your network.

Click the Geolocation tab in FlowIQ 1

Click a **Source Country** to build a filter so you can drill down on just that country. 2

With the filter created, select the Overview or Trends or Records tab.

Notice your filter persists across views until you clear it.



Lab 3: Step 3.7

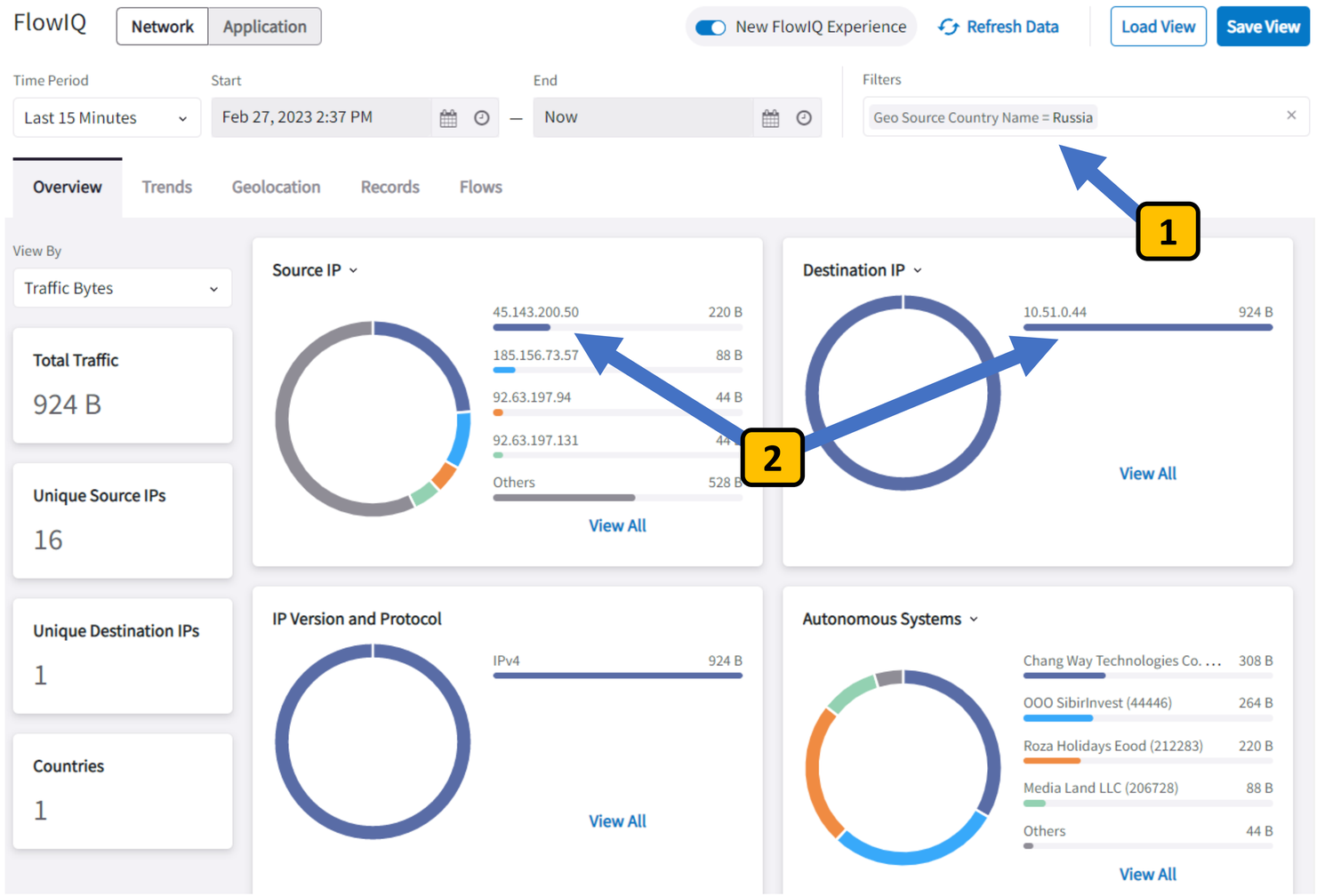
What are the traffic details for these countries?

In the previous step, I clicked on Russia.

By doing that, FlowIQ built a filter to show me only traffic from Russia talking to my cloud network. 1

Then I clicked on the Overview tab to get a quick breakdown of the top talker from Russia, and what IP in my network it's talking to. 2

Note: You can have CoPilot tell your Gateways to block traffic from any country automatically!



Lab 3 Completed

Observe network traffic details

You were able to get deep visibility of traffic on your network, all right out of the box in Aviatrix CoPilot.

You didn’t have build a mousetrap to collect and visualize your network traffic. Aviatrix has built that solution for you (*that works the same way in any cloud*).