AWS Immersion Day
LAB 4

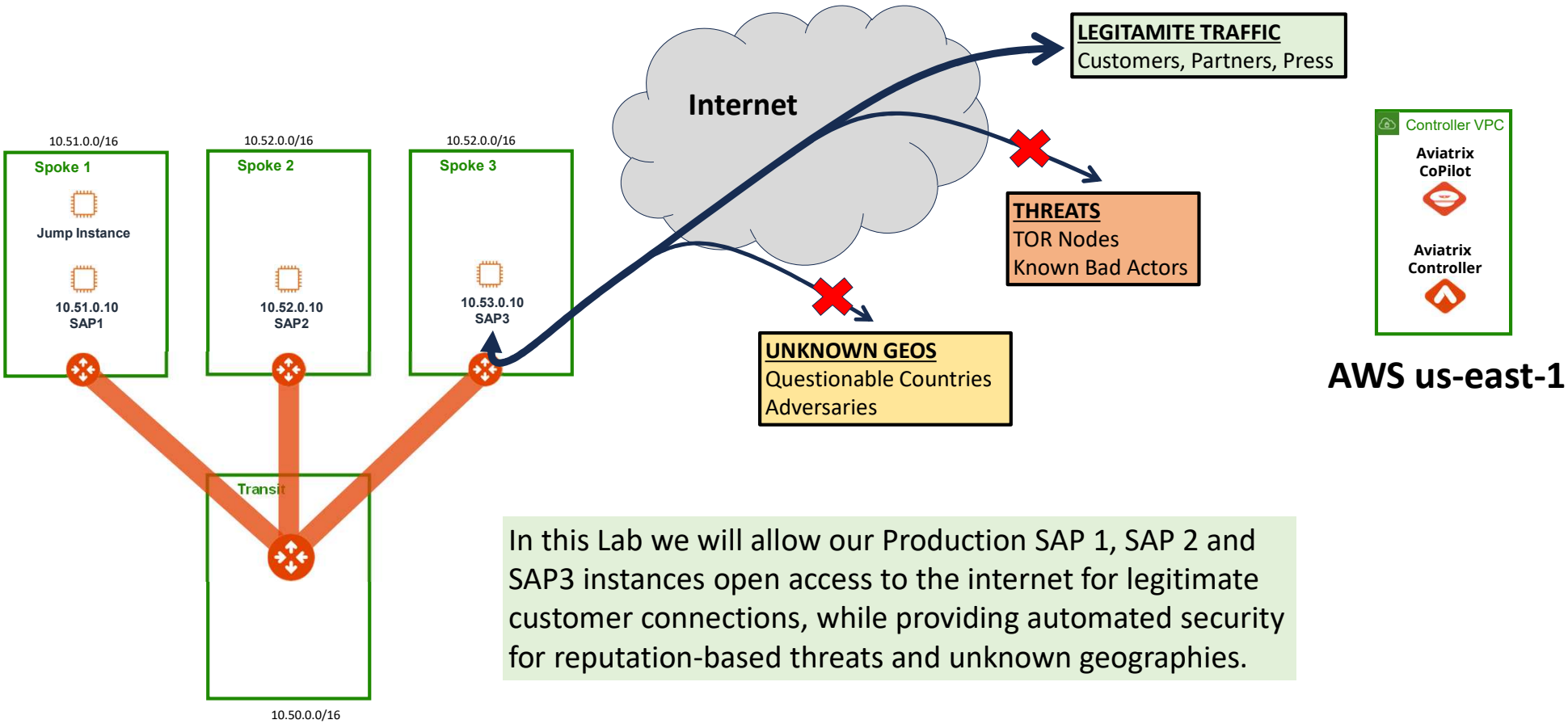
SECURITY: THREAT PREVENTION & GEOBLOCKING

Aviatrix Systems
Solutions Engineering

aviatrix

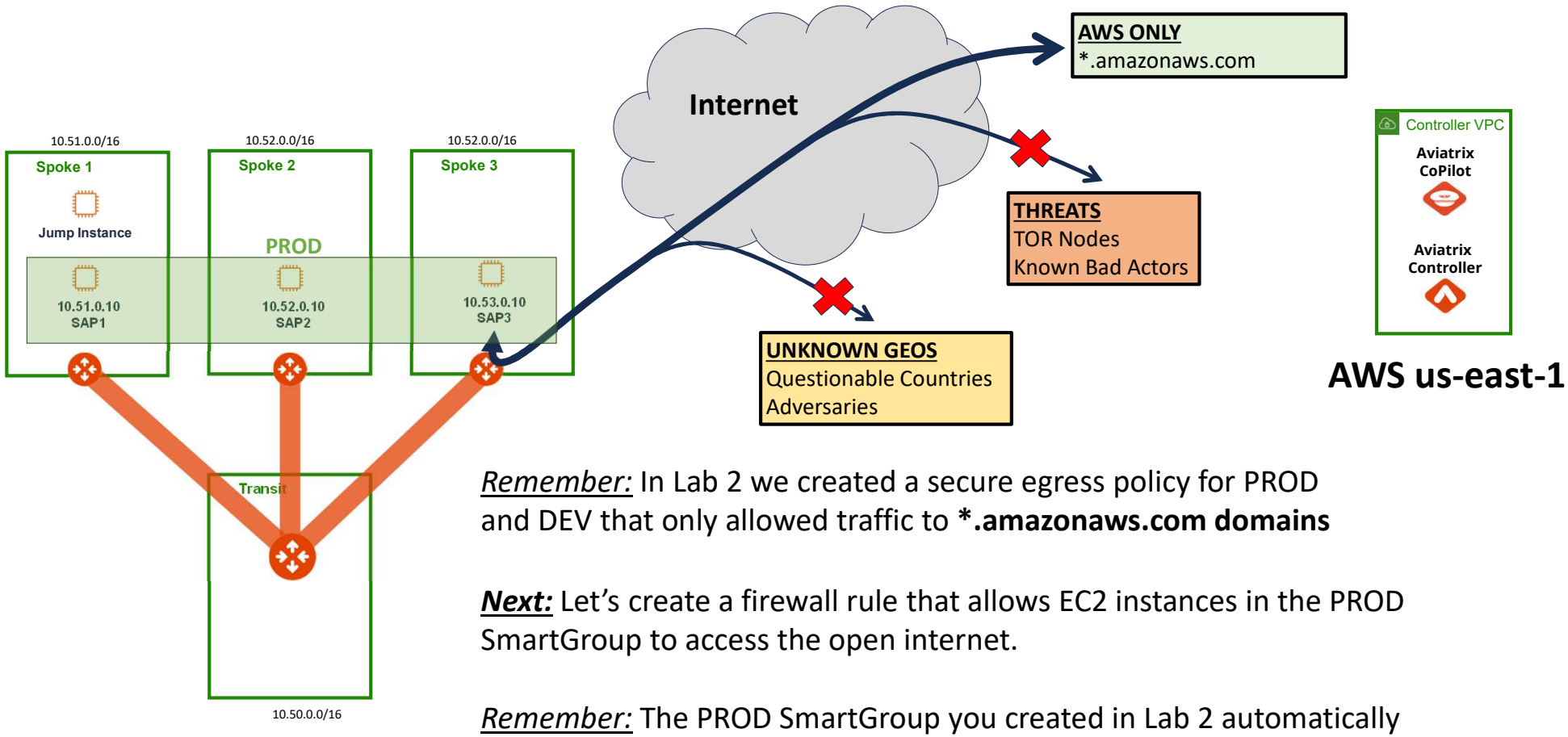
Lab 4 Intro

Distributed Cloud Firewall Threat Prevention & Geo Blocking



In this Lab we will allow our Production SAP 1, SAP 2 and SAP3 instances open access to the internet for legitimate customer connections, while providing automated security for reputation-based threats and unknown geographies.

Lab 4: Current State



Remember: In Lab 2 we created a secure egress policy for PROD and DEV that only allowed traffic to ***.amazonaws.com domains**

Next: Let's create a firewall rule that allows EC2 instances in the PROD SmartGroup to access the open internet.

Remember: The PROD SmartGroup you created in Lab 2 automatically contains any EC2 instances tagged with **Environment = Production**

Lab 4: Threat Prevention: Step 4.1

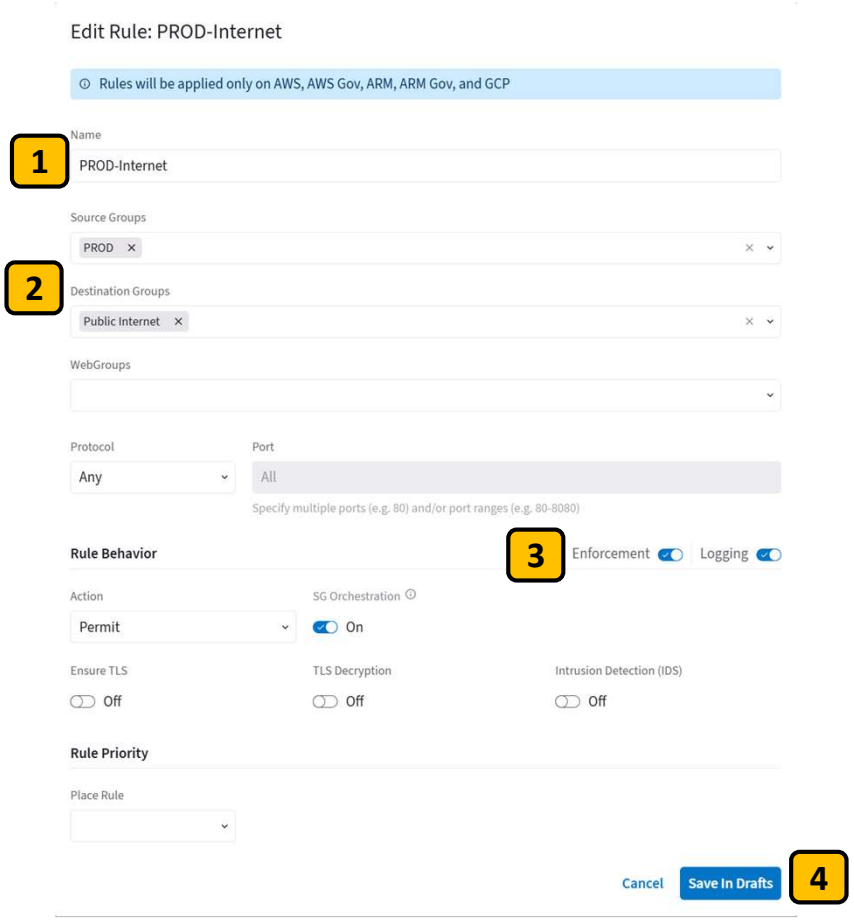
Allow open internet for PROD

Create a new Firewall rule.

Name the rule PROD-Internet 1
and allow PROD to access the
Public Internet. 2

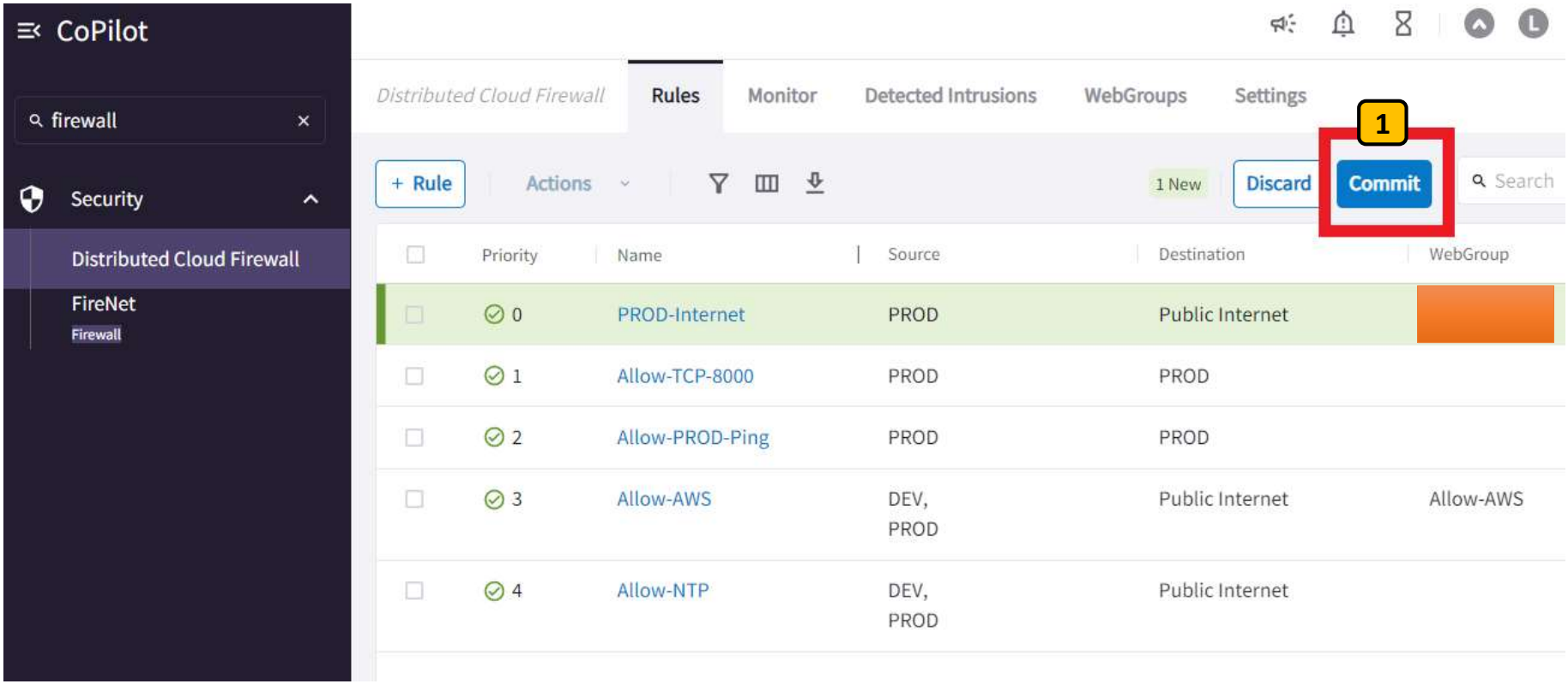
Set Protocol to **Any** and enable Logging and
Permit the traffic. 3

Place the rule on **Top** and click **Save In Drafts** 4



Lab 4: Threat Prevention: Step 4.2

Allow open internet for PROD



Commit the new firewall rule 1

Lab 4: Threat Prevention: Step 4.3

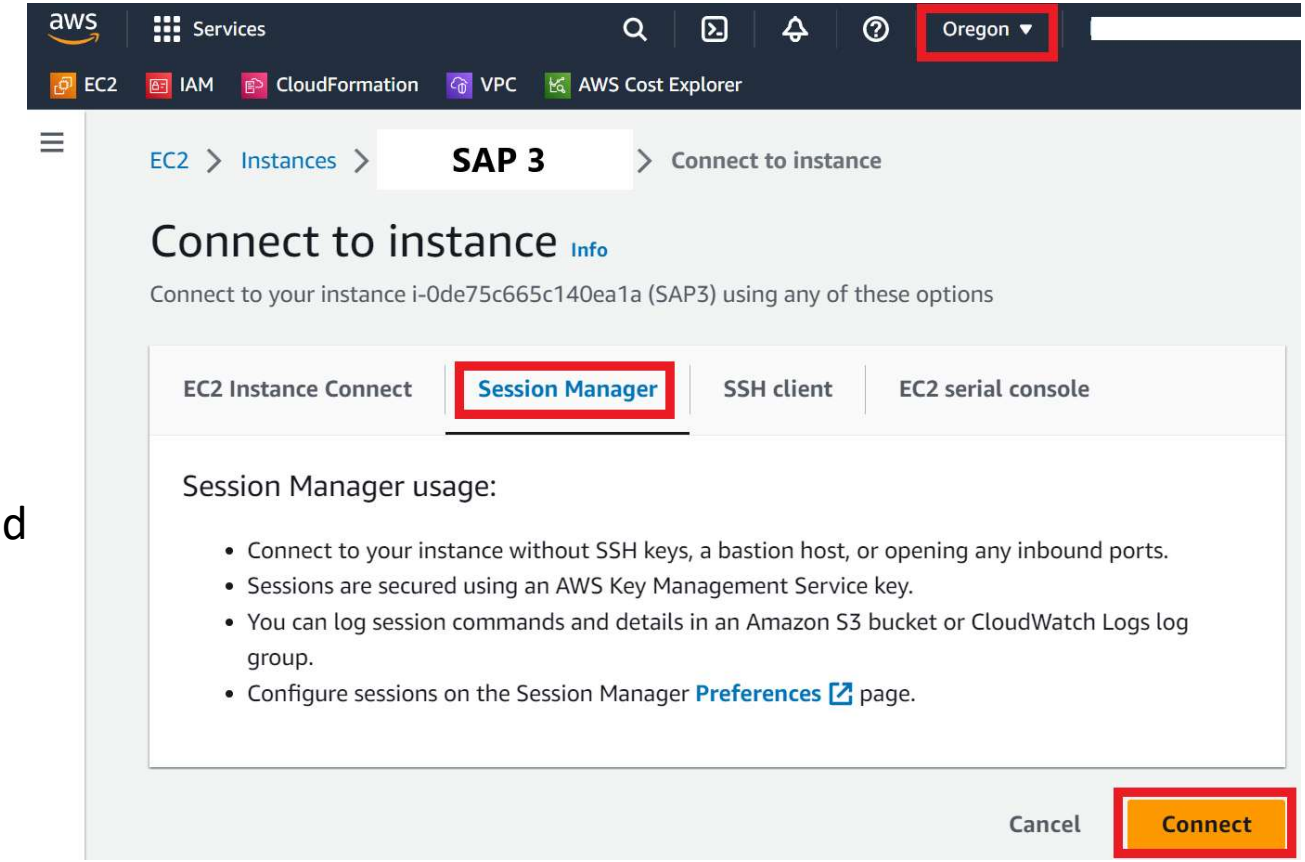
Connect to Console of instance SAP 3 to test your new PROD-Internet rule

Now let's test the new firewall rule.

Connect to the console of instance SAP 3 using Session Manager as you've done in previous labs.

Make sure you're in the Oregon region. Select the SAP 3 instance and click Connect.

Select Session Manager and click **Connect**.



Lab 4: Threat Prevention: Step 4.4

Confirm open internet access for PROD

Login as ec2-user by issuing the command:
sudo su –l ec2-user 1

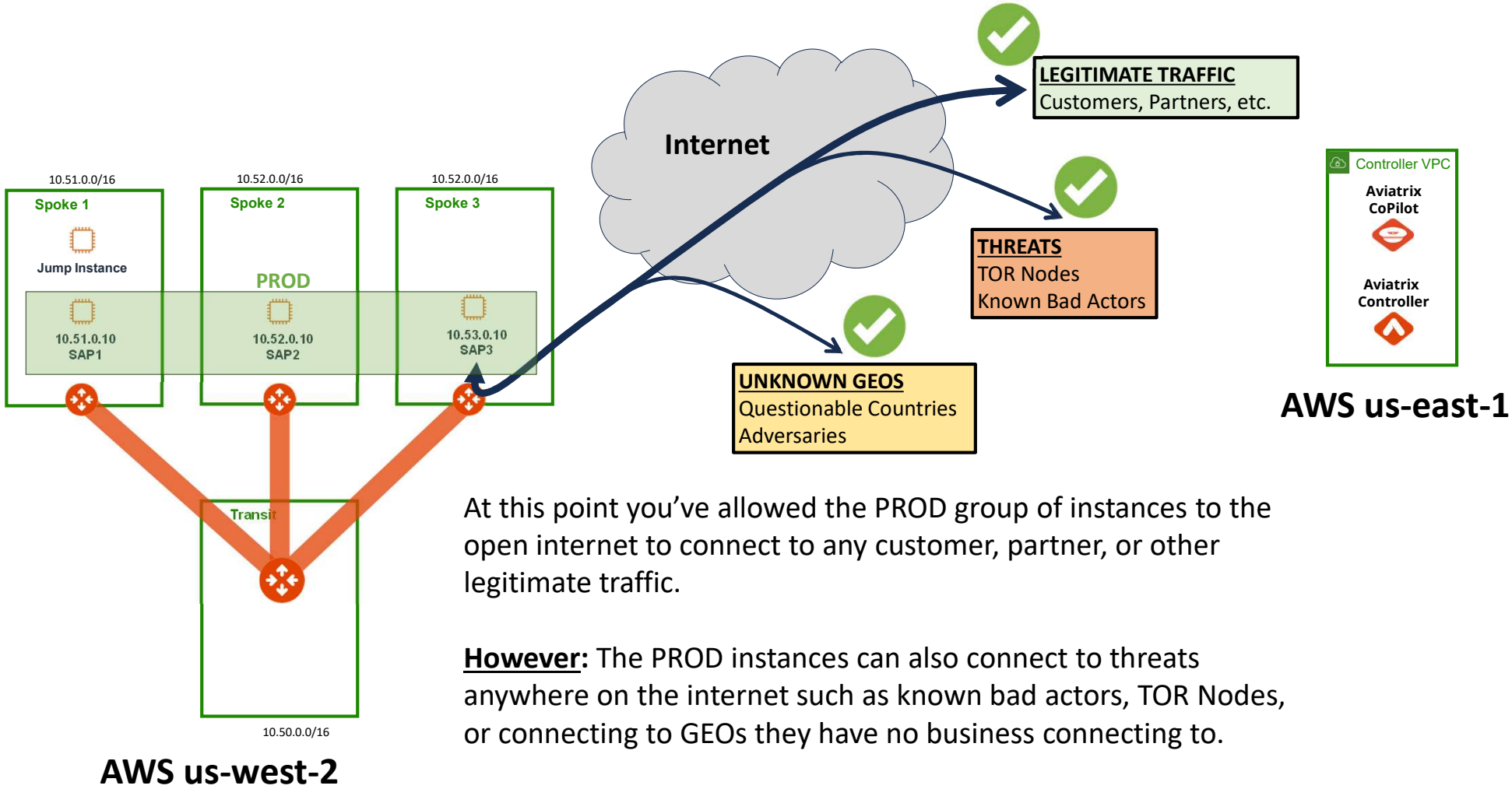
Connect to any website using the curl command (e.g., google.com)
curl https://google.com 2

The curl should return HTML code from the site you connected to.

Session ID: brad-0a81a0d1bec850995 Instance ID: i-0de75c665c140ea1a

```
sh-4.2$
sh-4.2$ sudo su -l ec2-user
Last login: Tue Aug 15 23:05:56 UTC 2023 on pts/1
[ec2-user@ip-10-53-0-10 ~]$
[ec2-user@ip-10-53-0-10 ~]$
[ec2-user@ip-10-53-0-10 ~]$
[ec2-user@ip-10-53-0-10 ~]$ curl https://google.com
<HTML><HEAD><meta http-equiv="content-type" content="text/html;charset=utf-8">
<TITLE>301 Moved</TITLE></HEAD><BODY>
<H1>301 Moved</H1>
The document has moved
<A HREF="https://www.google.com/">here</A>.
</BODY></HTML>
[ec2-user@ip-10-53-0-10 ~]$
[ec2-user@ip-10-53-0-10 ~]$
[ec2-user@ip-10-53-0-10 ~]$
[ec2-user@ip-10-53-0-10 ~]$
```

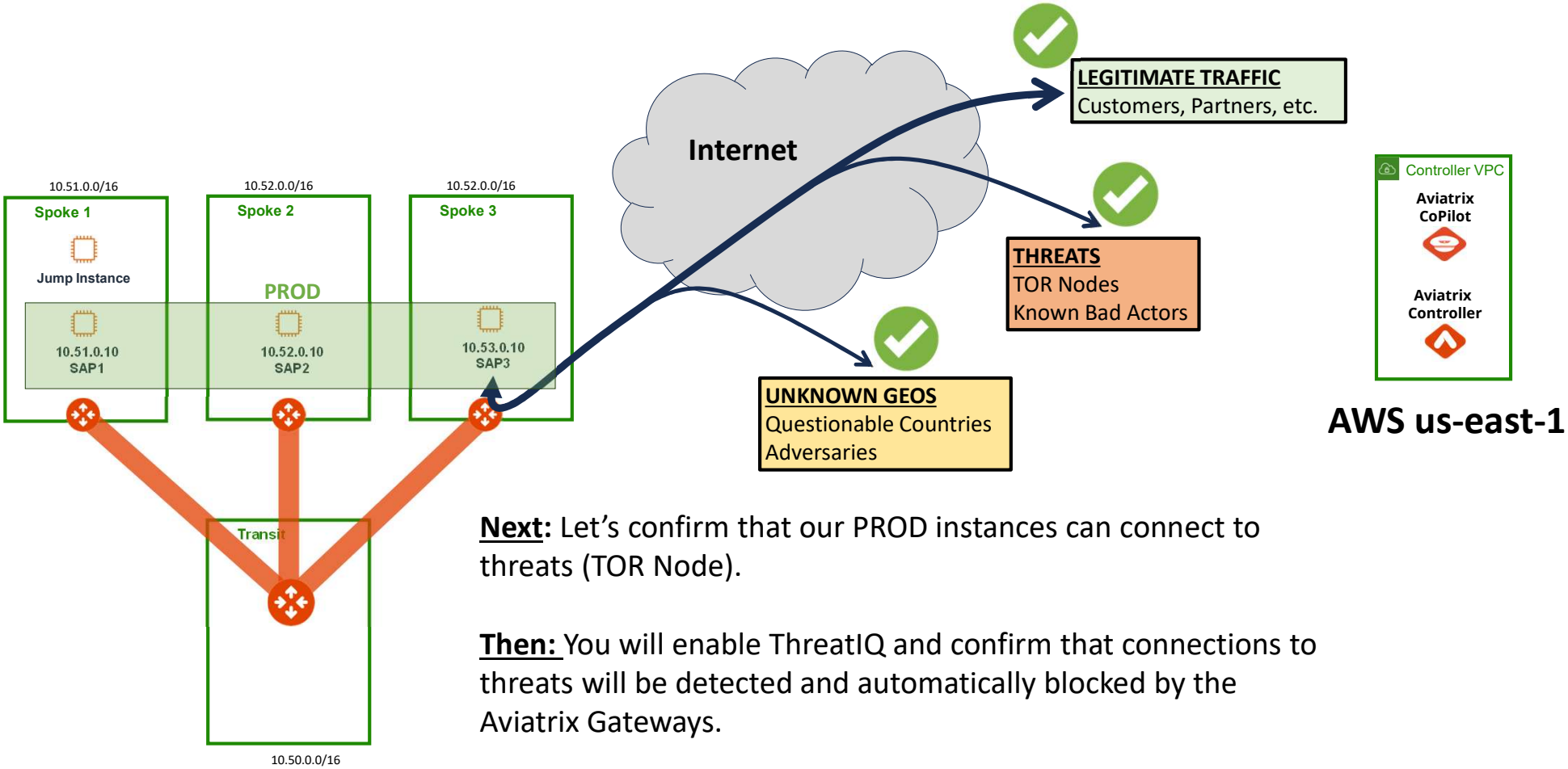
Lab 4: Checkpoint 1: Current State



At this point you've allowed the PROD group of instances to the open internet to connect to any customer, partner, or other legitimate traffic.

<u>However</u>: The PROD instances can also connect to threats anywhere on the internet such as known bad actors, TOR Nodes, or connecting to GEOs they have no business connecting to.

Lab 4: Checkpoint 1: Current State



Next: Let's confirm that our PROD instances can connect to threats (TOR Node).

Then: You will enable ThreatIQ and confirm that connections to threats will be detected and automatically blocked by the Aviatrix Gateways.

Lab 4: Threat Prevention: Step 4.5

Investigate an abuse IP

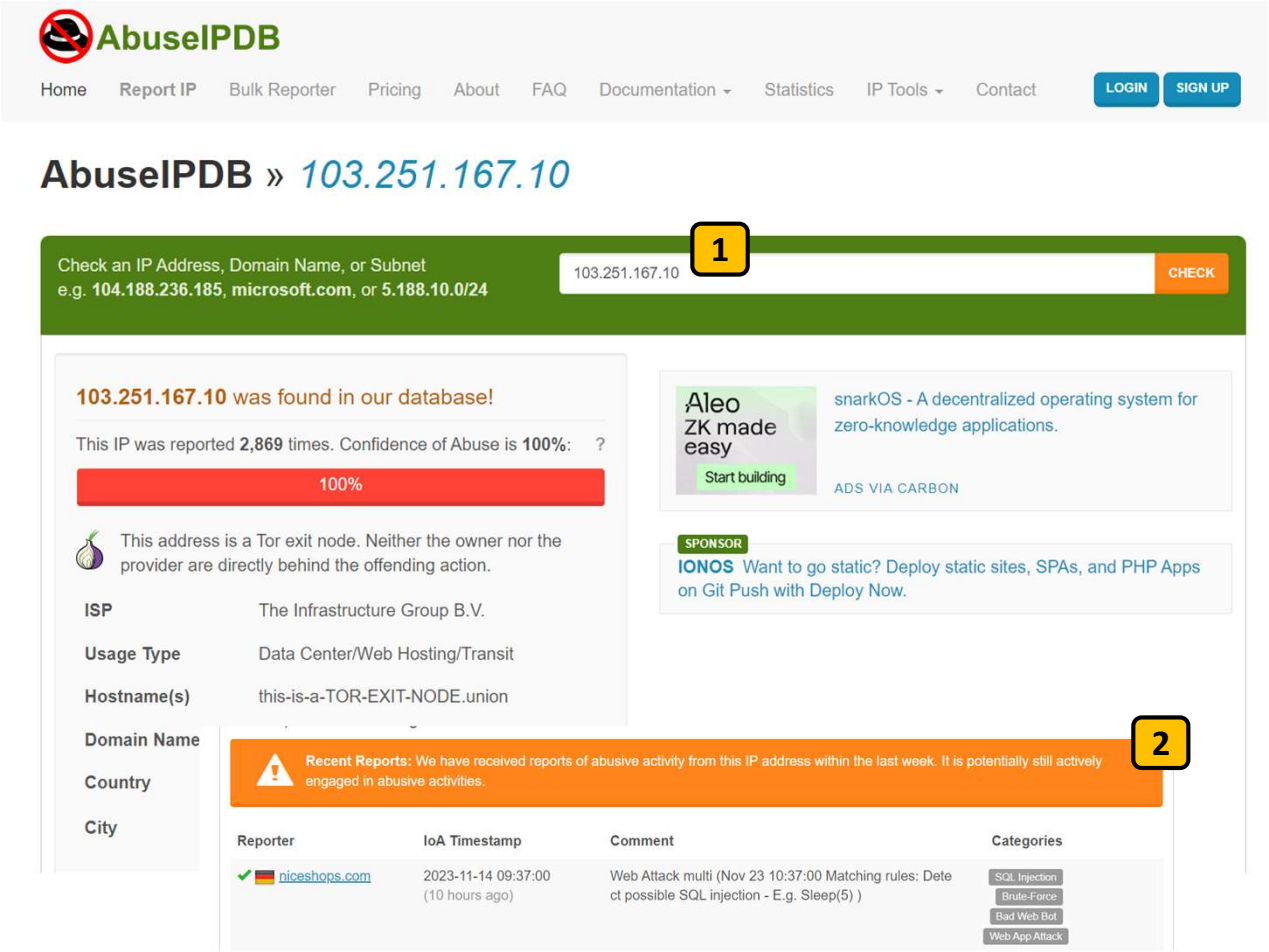
Open a browser tab to the website: http://abuseipdb.com

Check the following IP address: **103.251.167.10** 1

Confirm this IP has been found in the database, scroll down and read the recent reports about it. 2

This IP is a TOR Node and it's been reported doing questionable activity as you can see.

This is not an IP you want connecting to your PROD instances!



Lab 4: Threat Prevention: Step 4.6

Connect to the abuse IP

From your Console session on instance SAP 3, connect to the abuse IP using curl:

curl http://103.251.167.10 1

Note: (HTTP …. Not HTTPS)

```
[ec2-user@ip-10-53-0-10 ~]$
[ec2-user@ip-10-53-0-10 ~]$
[ec2-user@ip-10-53-0-10 ~]$
[ec2-user@ip-10-53-0-10 ~]$ curl http://103.251.167.10
```

1

Lab 4: Threat Prevention: Step 4.7

Connect to the abuse IP

The instance should successfully connect to the abuse IP.

It returns HTML code telling us that it's a TOR Node. 1

This is obviously not good.

How can we easily and quickly shut this down while still providing open internet access?

Let's see what Aviatrix can do about it…

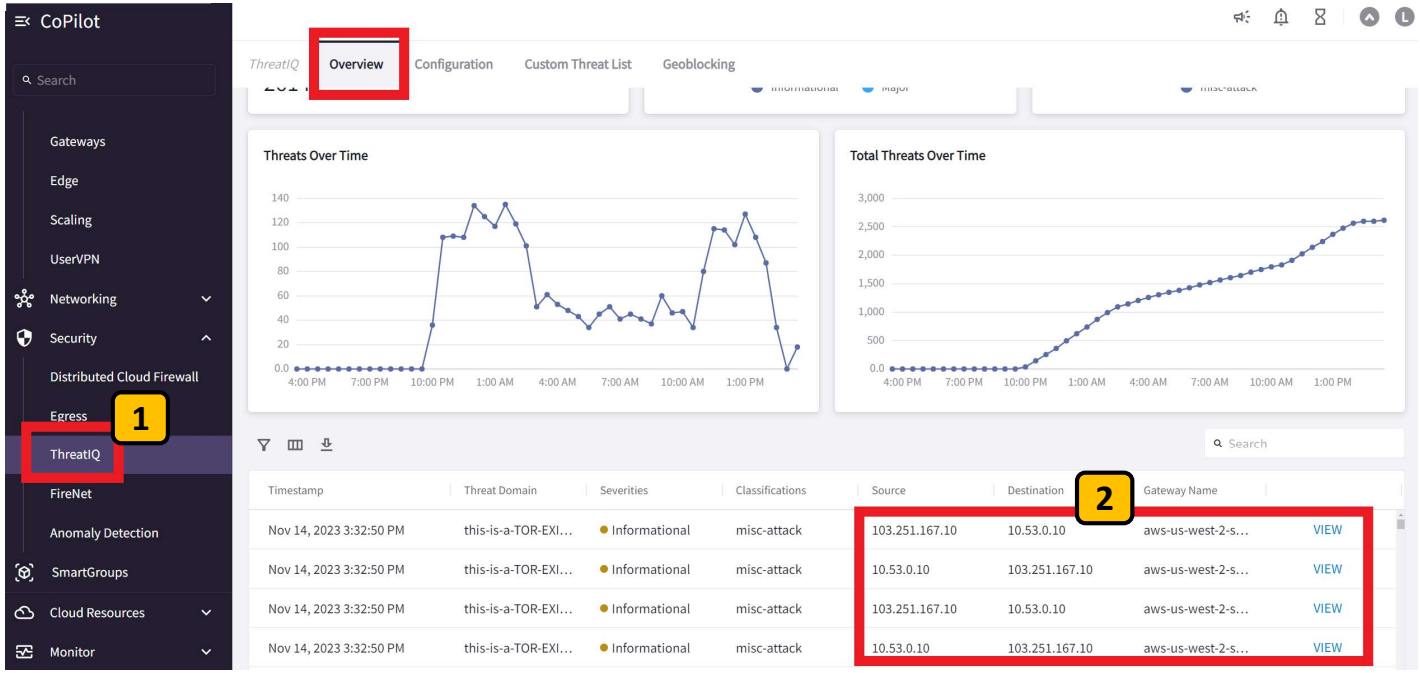
```
<p>
That being said, if you still have a complaint about the router,  you may
email the <a href="mailto:FIXME_YOUR_EMAIL_ADDRESS">maintainer</a>. If
complaints are related to a particular service that is being abused, I will
consider removing that service from my exit policy, which would prevent my
router from allowing that traffic to exit through it. I can only do this on an
IP+destination port basis, however. Common P2P ports are
already blocked.</p>

<p>
You also have the option of blocking this IP address and others on
the Tor network if you so desire. The Tor project provides a <a
href="https://check.torproject.org/torbulkexitlist">web service</a>
to fetch a list of all IP addresses of Tor exit nodes that allow exiting to a
specified IP:port combination, and an official <a
href="https://dist.torproject.org/tordnsel/">DNSRBL</a> is also available to
determine if a given IP address is actually a Tor exit server. Please
be considerate
when using these options. It would be unfortunate to deny all Tor users access
to your site indefinitely simply because of a few bad apples.</p>

</main>
</body>
</html>
[ec2-user@ip-10-53-0-10 ~]$
```

Lab 4: Threat Prevention: Step 4.8

Observe the threat in ThreatIQ



CoPilot is always watching your traffic for threats in ThreatIQ

Go to **ThreatIQ** under Security 1

Look for the threat connection from your curl in ThreatIQ 2

Note: It may take a few minutes for ThreatIQ to acknowledge and display the threat.

Lab 4: Threat Prevention: Step 4.9

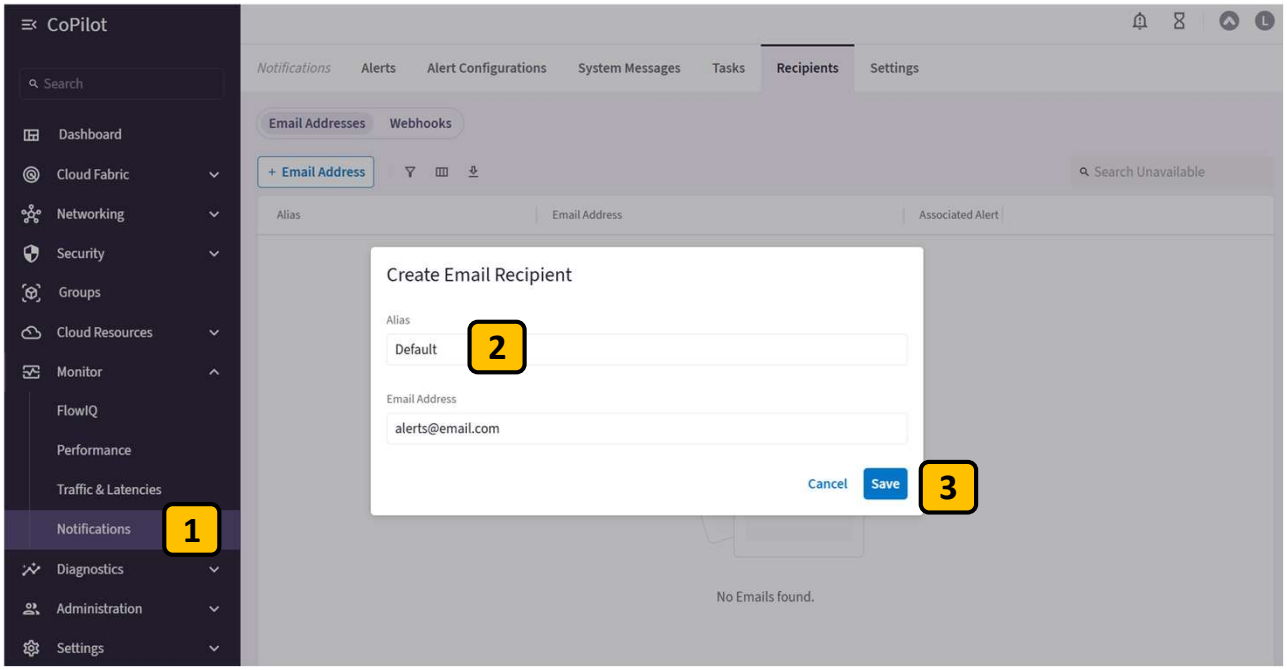
Enable threat alerting in ThreatIQ

We need to specify a recipients list for our alert configuration.

Click on **Monitor > Notifications > Recipients** and choose **+Email Address** 1

In the dialogue box enter **Default** as the Alias and use an email address of alerts@email.com 2

Click **Save** 3



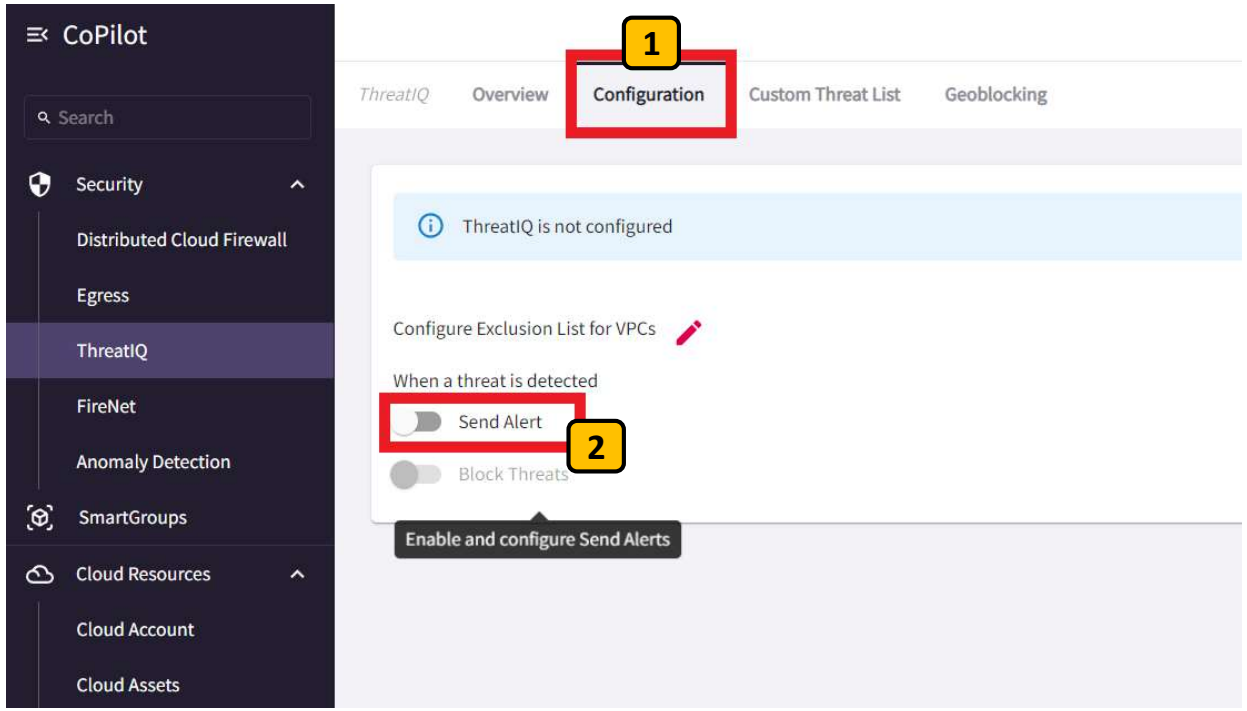
Lab 4: Threat Prevention: Step 4.10

Enable threat alerting in ThreatIQ

To protect our PROD instances, lets begin by enable alerts when ThreatIQ sees a threat connection.

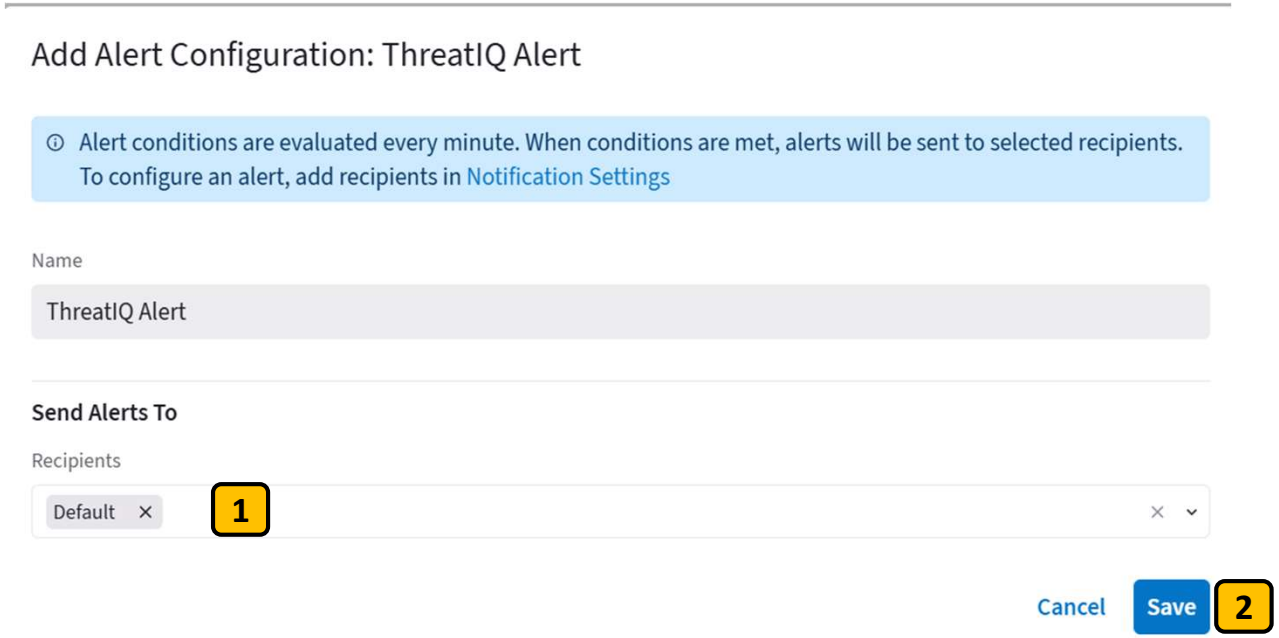
Go to the **Configuration** tab in ThreatIQ 1

Enable the **Send Alert** switch. 2



Lab 4: Threat Prevention: Step 4.11

Enable threat alerting in ThreatIQ



In the configuration pop-up click **Send Alert To** and select the email address you created earlier to receive alerts. 1

Then **Confirm**. 2

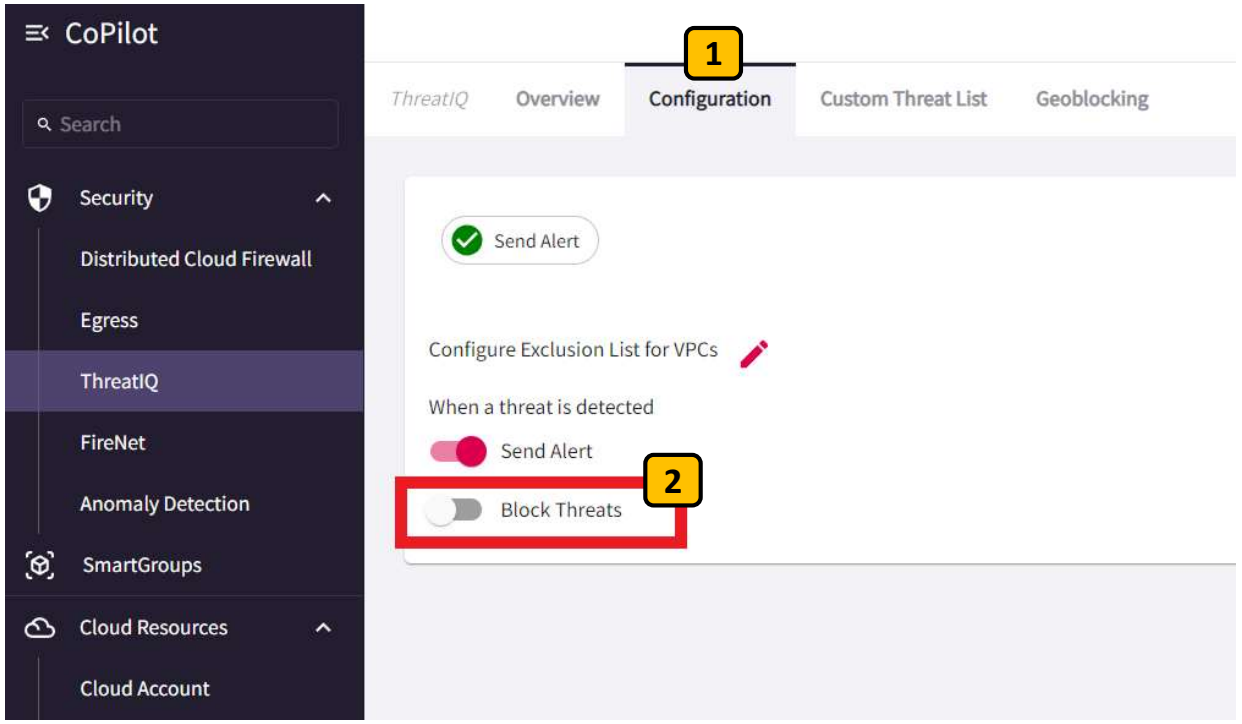
Lab 4: Threat Prevention: Step 4.12

Enable threat BLOCKING in ThreatIQ

Next, let's tell CoPilot to automatically block the threats when they're observed.

Go to the **Configuration** tab in ThreatIQ 1

Enable the **Block Threats** switch. 2



Lab 4: Threat Prevention: Step 4.13

Enable threat BLOCKING in ThreatIQ

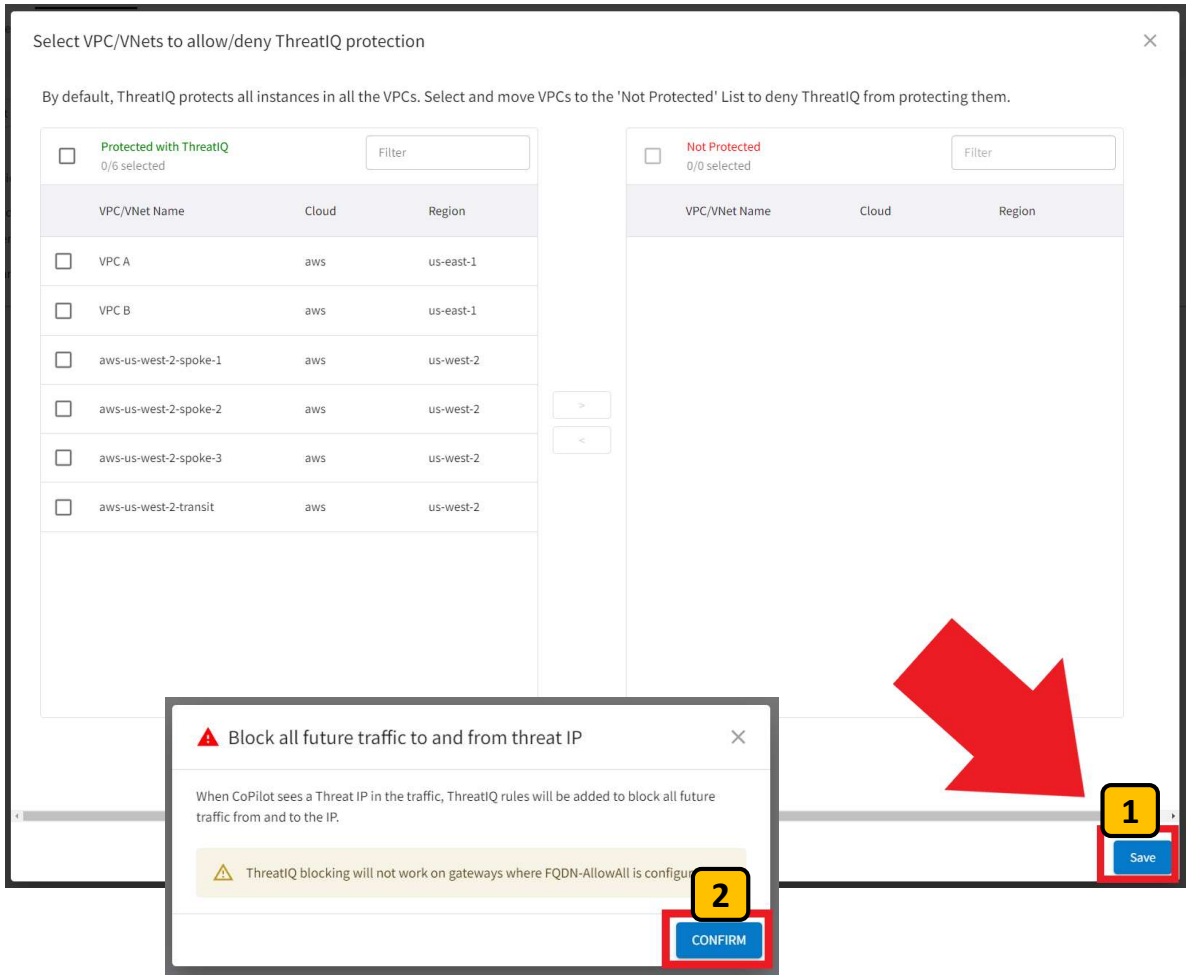
You can select which VPCs will have threat blocking enabled.

By default, all VPCs will be protected.

Let's keep it that way for now.

Click **Save**. 1

Then **Confirm**. 2

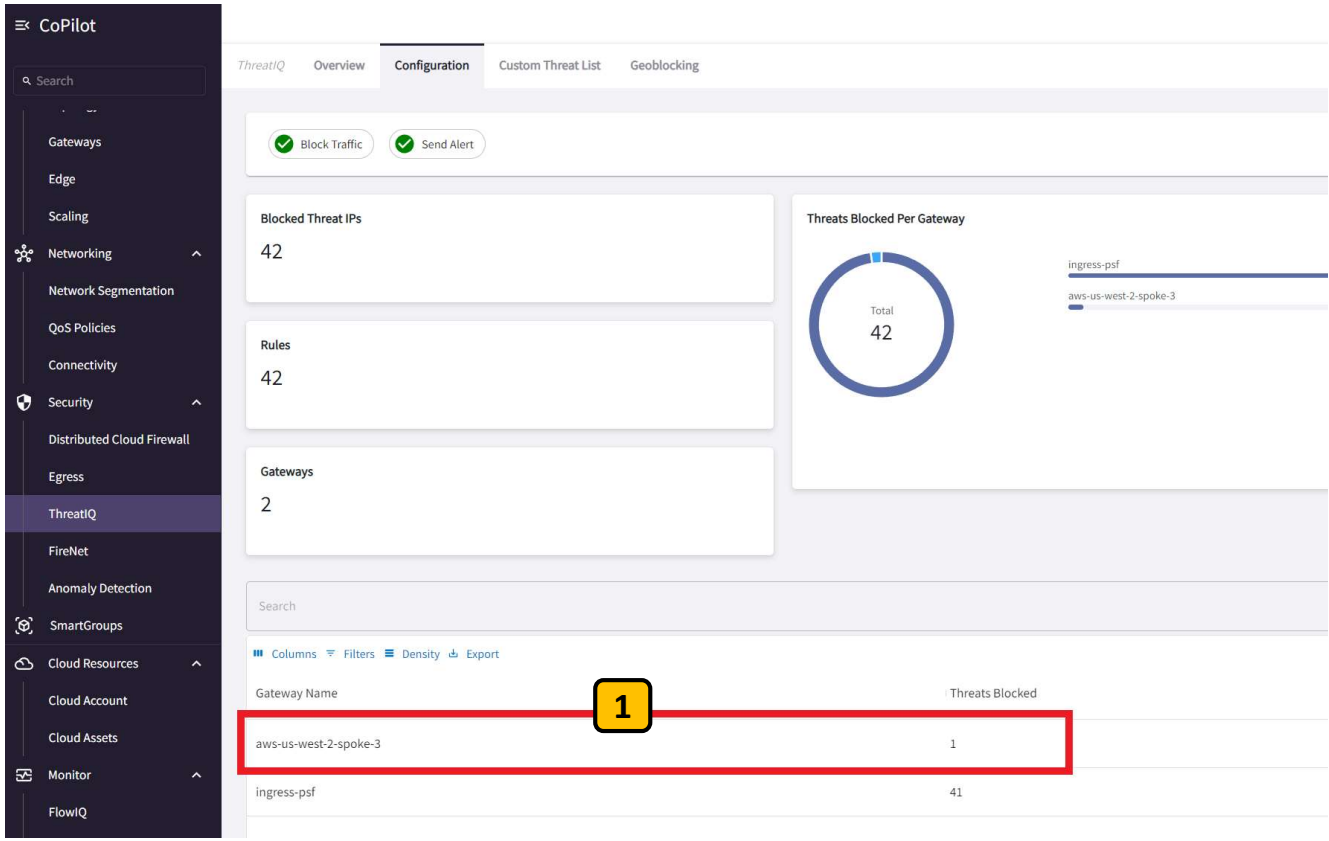


Lab 4: Threat Prevention: Step 4.14

View threat BLOCKING in ThreatIQ

Once enabled, CoPilot will begin blocking any new threat IPs that have been detected.

On the Configuration tab you will see how many threats have been blocked and on which Aviatrix Gateway. 1



Lab 4: Threat Prevention: Step 4.15

Observe and confirm threat blocking

Go back the Console session of instance SAP 3.
(Note: you will need to close and open the connection or else you may get an open TCP socket from your prior connection)

Reconnect to the threat IP using curl: 1

curl http://103.251.167.10

Session ID: Participant-012cbf264a1e61a71 Instance ID: i-01f3d833a2a47c0d3

```
[ec2-user@ip-10-53-0-10 ~]$
[ec2-user@ip-10-53-0-10 ~]$
[ec2-user@ip-10-53-0-10 ~]$ curl http://103.251.167.10
```

1

Lab 4: Threat Prevention: Step 4.16

Connect to the abuse IP

The instance should successfully connect to the abuse IP again.

It returns HTML code telling us that it's a TOR Node. 1

Now that threat blocking is enabled, CoPilot will witness these connections again and configure drop rules on your Aviatrix Gateway for the threat IP.

Connect a few times and wait a few minutes…

```
<p>
That being said, if you still have a complaint about the router,  you may
email the <a href="mailto:abuse@august.tw">maintainer</a>. If
complaints are related to a particular service that is being abused, I will
consider removing that service from my exit policy, which would pre
router from allowing that traffic to exit through it. I can only  an
IP+destination port basis, however. Common P2P ports a
already blocked.</p>

<p>
You also have the option of blo  s and  on
the Tor network if you so desire. The Tor project provides  <a
href="https://check.torproject.org/  ">web service</a>
to fetch a list of all IP addresses of Tor exit nodes that allow exiting to a
specified IP:port combination, and an official <a
href="https://dist.torproject.org/tordnsel/">DNSRBL</a> is also available to
determine if a given IP address is actually a Tor exit server. Please
be considerate
when using these options. It would be unfortunat  Tor users access
to your site indefinitely simply because of a fe  bad apples.</p>

</main>
</body>
</html>
[ec2-user@ip-10-53-0-10 ~]$
```

Lab 4: Threat Prevention: Step 4.17

Observe and confirm threat blocking

Session ID: Participant-012cbf264a1e61a71 Instance ID: i-01f3d833a2a47c0d3

```
[ec2-user@ip-10-53-0-10 ~]$
[ec2-user@ip-10-53-0-10 ~]$
[ec2-user@ip-10-53-0-10 ~]$
[ec2-user@ip-10-53-0-10 ~]$ curl http://103.251.167.10
curl: (28) Failed to connect to 103.251.167.10 port 80 after 131203 ms: Couldn't connect to server
[ec2-user@ip-10-53-0-10 ~]$
```

1

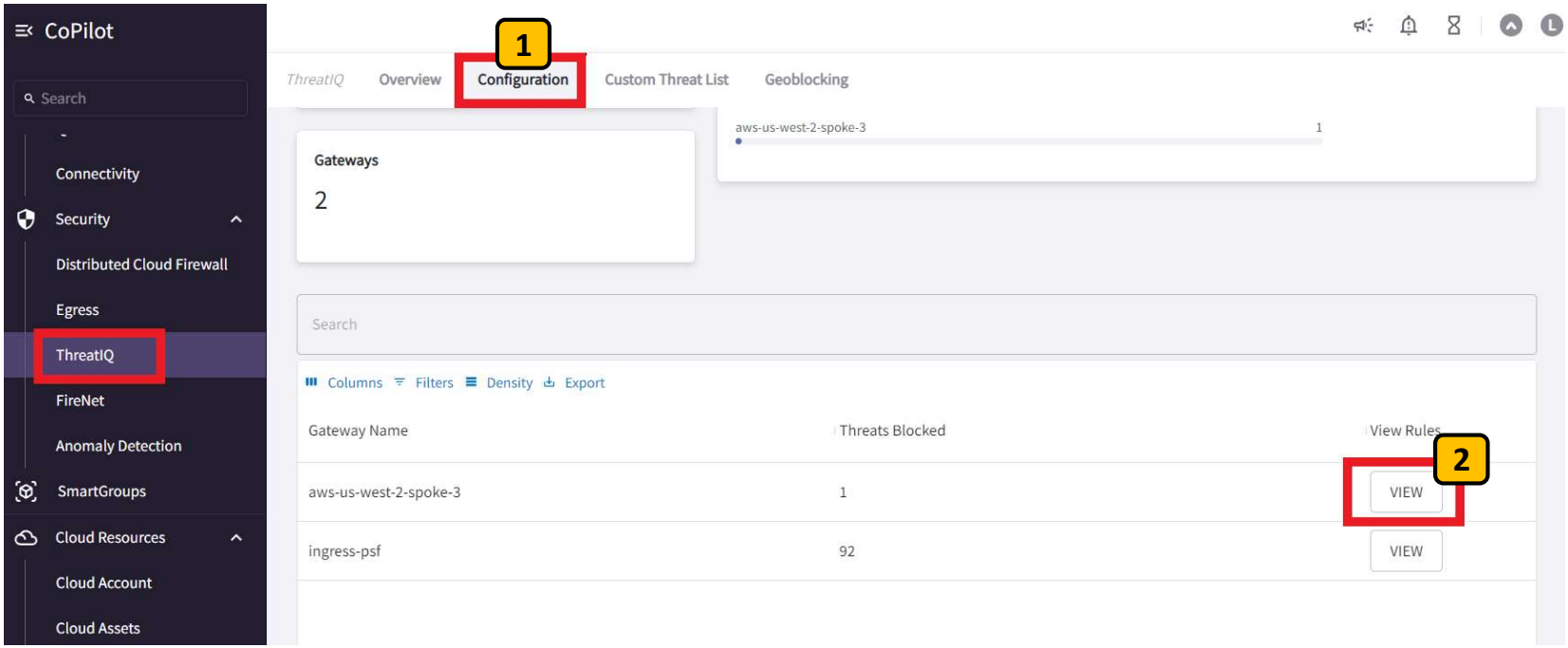
BLOCKED

After a few minutes of you should being to see your connections to this threat IP fail. 1

Aviatrix CoPilot has detected the threat connection and automatically blocked it as you've requested!

Lab 4: Threat Prevention: Step 4.18

Observe and confirm threat blocking



Go to the Configuration tab of ThreatIQ to view the blocks that have happened. 1

Find the aws-us-west-2-spoke-3 gateway with threats blocked and click **View** 2

Lab 4: Threat Prevention: Step 4.19

Observe and confirm threat blocking

aws-us-west-2-spoke-3

Columns Filters Density Export

Source IP	Destination IP	Port	Protocol	Description	Action	Delete
103.251.167.10/32	n/a	ALL	ALL	ipset rule	force-drop	

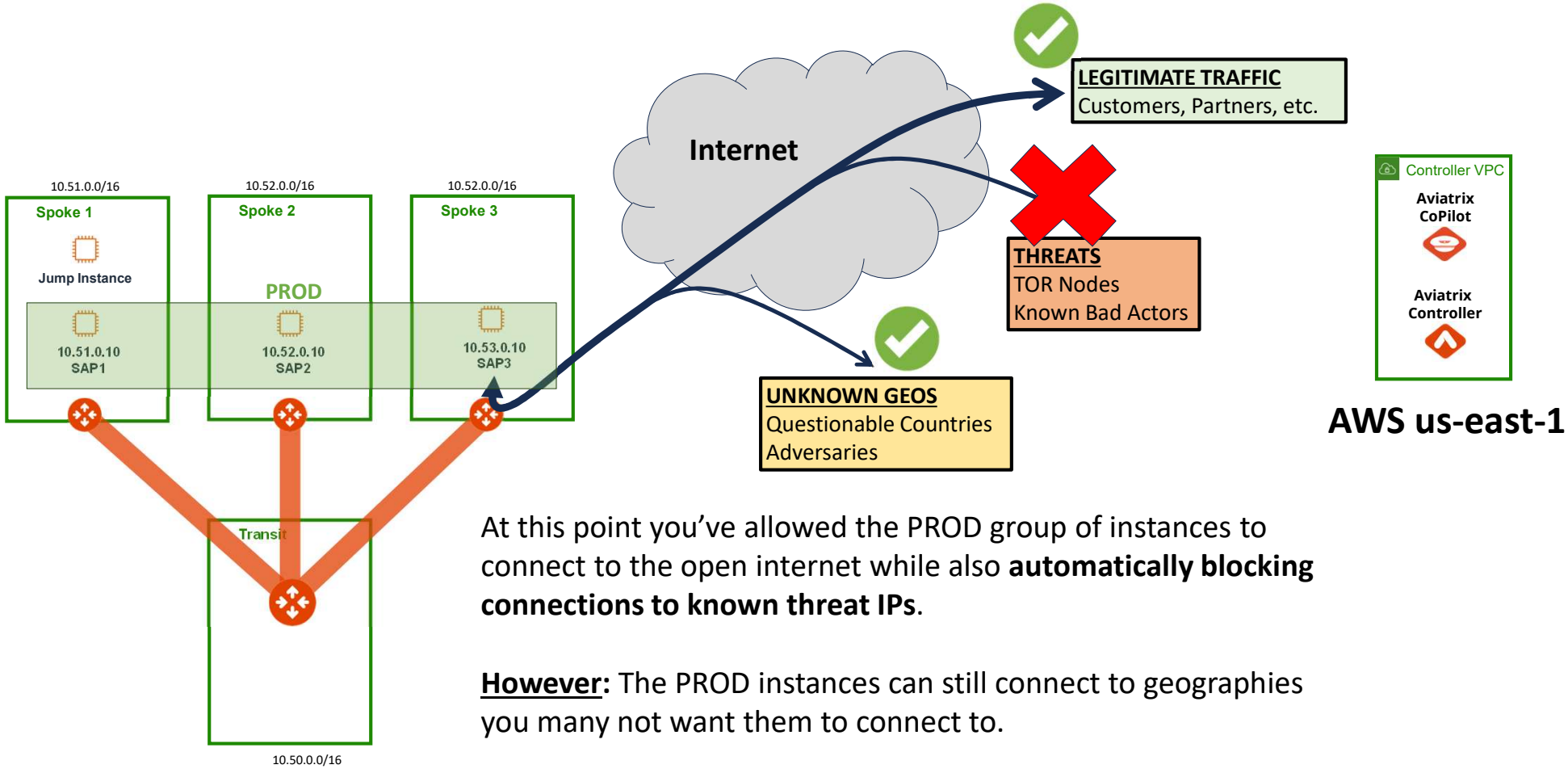
1 1

You should see the threat IP you connected to listed in a drop rule configured on this Aviatrix Gateway handing internet traffic for the instance SAP 3 1

Imagine this happening at 3am. You can continue to sleep while CoPilot protects your network.

Nobody will need to page you to wake up and write a firewall rule at 3am!

Lab 4: Checkpoint 2: Current State



At this point you've allowed the PROD group of instances to connect to the open internet while also **automatically blocking connections to known threat IPs**.

<u>However</u>: The PROD instances can still connect to geographies you many not want them to connect to.

Let's address this issue using Geo-blocking…

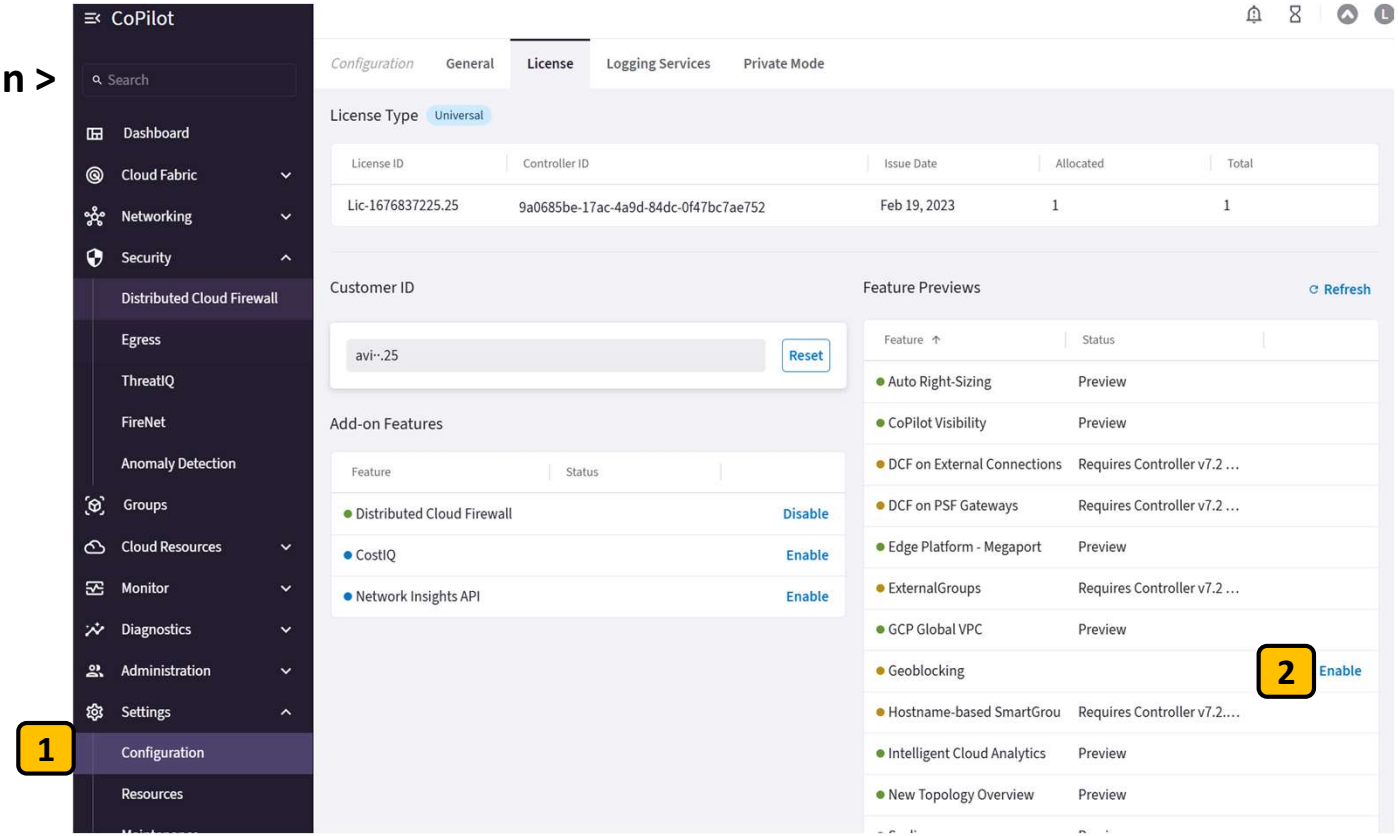
Lab 4: Threat Prevention: Step 4.20

Enable Geoblocking

1 Click on **Settings > Configuration > License**

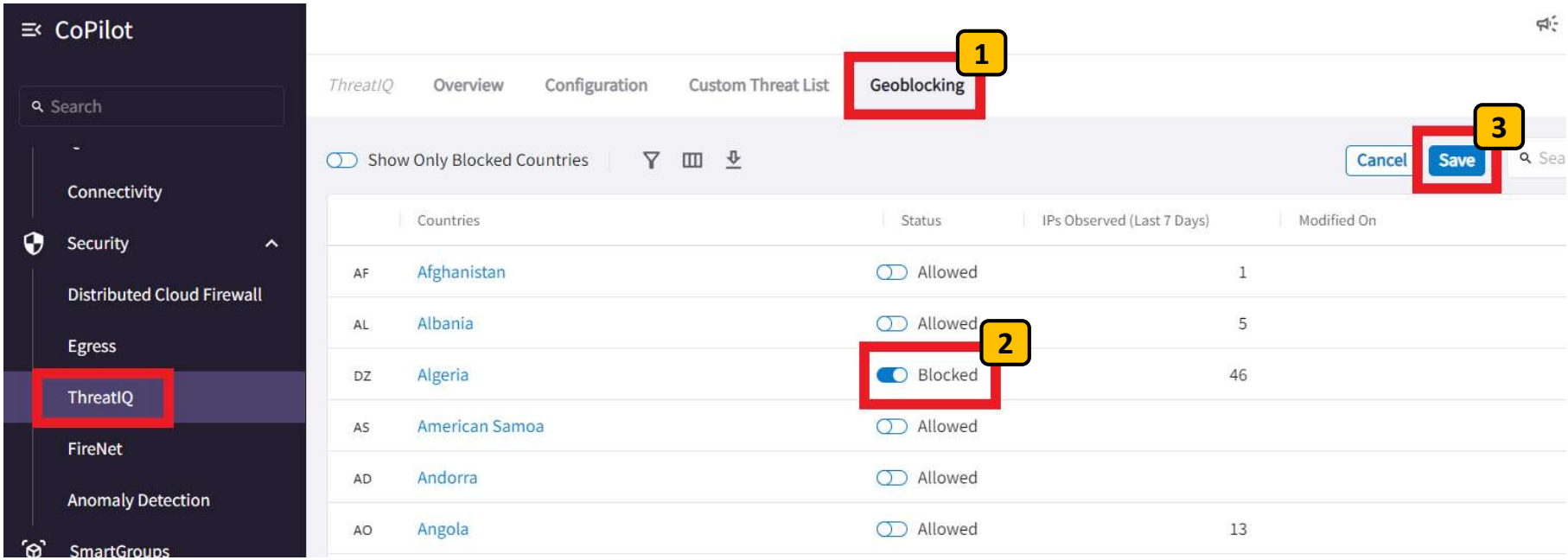
2 Then enable **Geoblocking**

3 On the PopUp Click on **Enable Geoblocking**



Lab 4: Threat Prevention: Step 4.21

Block geographies using Geoblocking



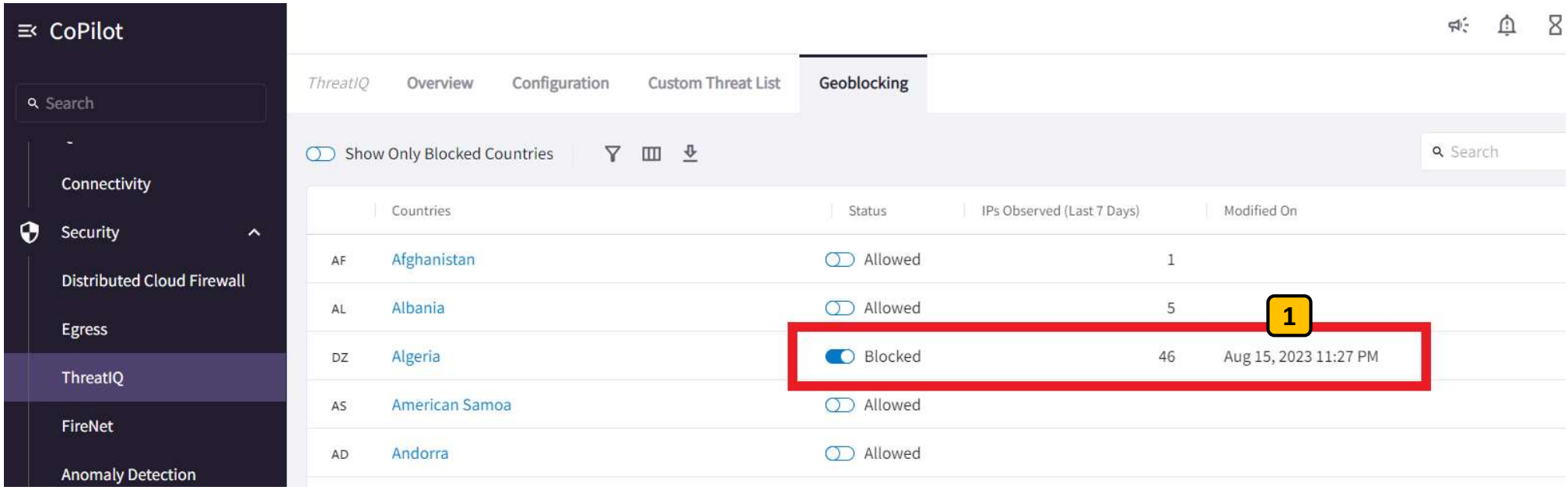
Go to the **Geoblocking** tab of ThreatIQ and you will see a long list of countries and how many IPs have been observed from them on your network. 1

Pick a country to block by clicking the Allowed switch to change it to Blocked 2

Click **Save**. 3

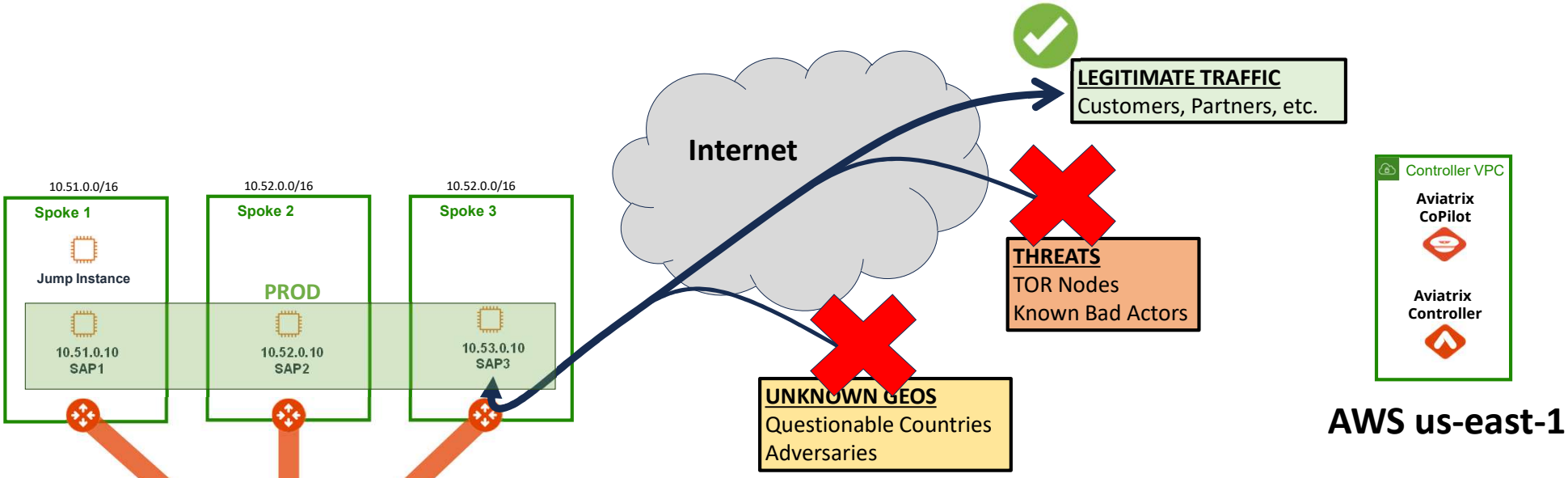
Lab 4: Threat Prevention: Step 4.22

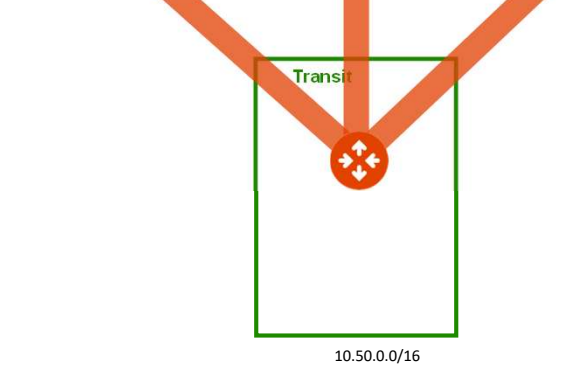
Block geographies using Geoblocking



Any new connections from the chosen country will be detected by CoPilot and subsequently blocked, just like you observed with the threat IP. 1

Lab 4: Complete: Current State





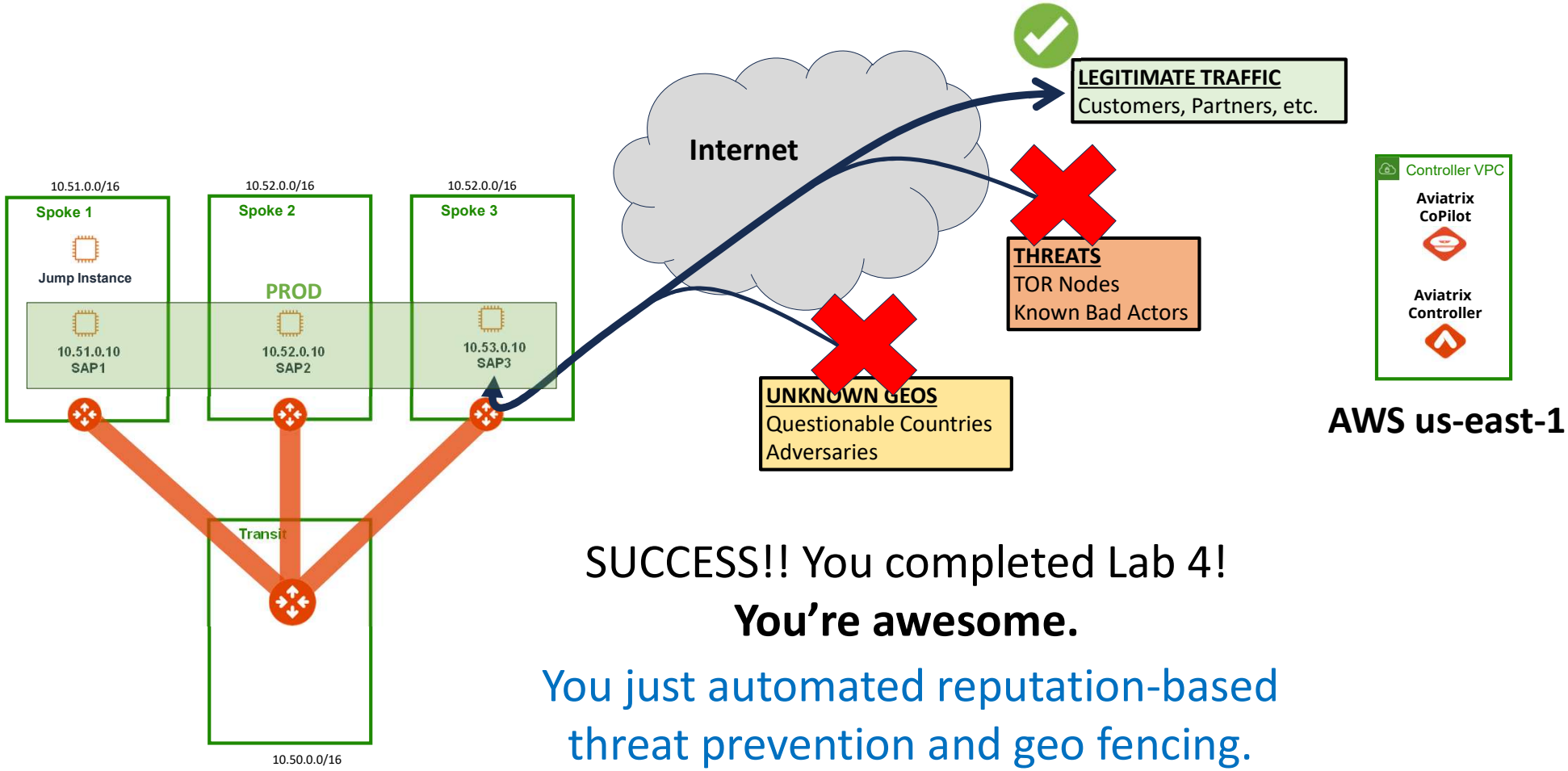
AWS us-west-2

At this point you've allowed the PROD group of instances to connect to the open internet while also **automatically blocking connections to known threat IPs … AND … automatically blocking chosen geographies!**

Super easy, right?

The easier it is to setup security, the more likely it is your network will be properly secured.

Lab 4: Success



AWS us-west-2

AWS us-east-1

SUCCESS!! You completed Lab 4!

You're awesome.

You just automated reputation-based threat prevention and geo fencing.

How cool is that??