

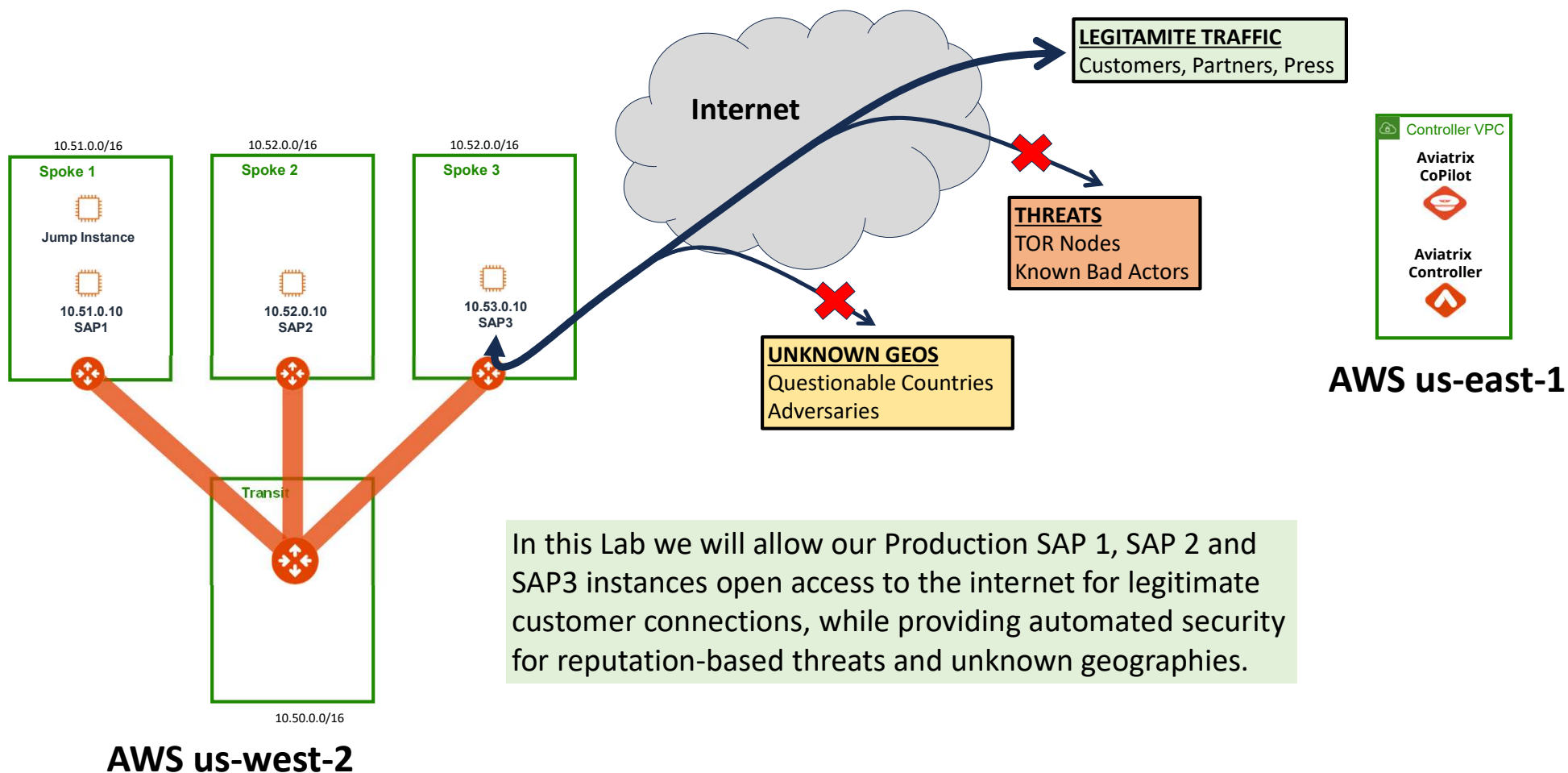
# AWS Immersion Day LAB 4

**SECURITY:** THREAT PREVENTION & GEOBLOCKING

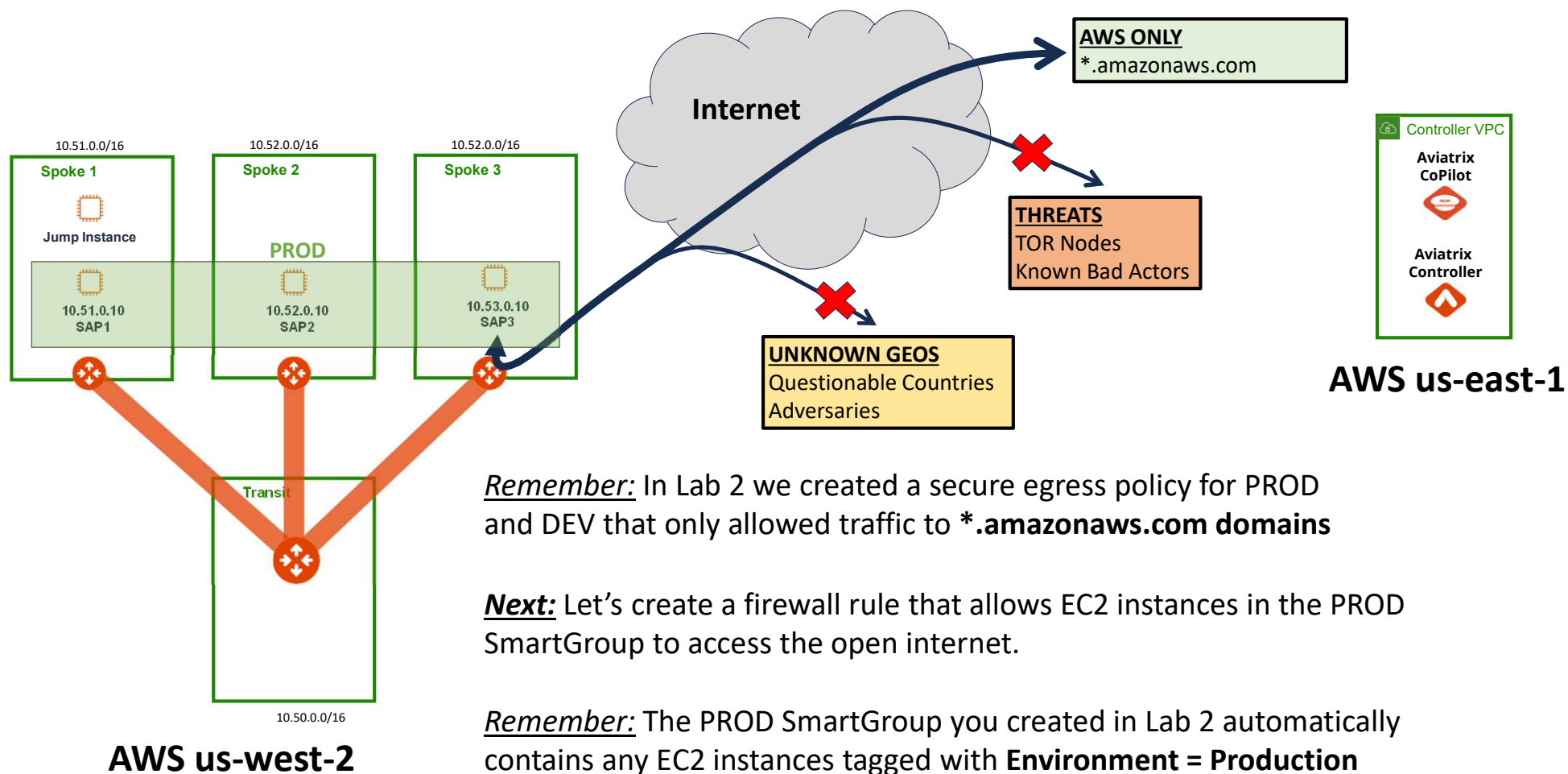
Aviatrix Systems  
Solutions Engineering

## Lab 4 Intro

Distributed Cloud Firewall Threat Prevention & Geo Blocking



## Lab 4: Current State





## 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**

Edit Rule: PROD-Internet

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

**1**

Name

PROD-Internet

**2**

Source Groups

PROD

Destination Groups

Public Internet

WebGroups

Protocol

Any

Port

All

Specify multiple ports (e.g. 80) and/or port ranges (e.g. 80-9080)

Rule Behavior

Action

Permit

SG Orchestration

On

Ensure TLS

Off

TLS Decryption

Off

Intrusion Detection (IDS)

Off

Rule Priority

Place Rule

**3**

Enforcement ☒ Logging ☒

Cancel

Save In Drafts

**4**

## Lab 4: Threat Prevention: Step 4.2

Allow open internet for PROD

CoPilot

Security

Distributed Cloud Firewall

FireNet

Firewall

Distributed Cloud Firewall

Rules

Monitor

Detected Intrusions

WebGroups

Settings

+ Rule

Actions

☐
☐
☐

1 New

Discard

Commit

Search

<input type="checkbox"/>	Priority	Name	Source	Destination	WebGroup
<input type="checkbox"/>	0	PROD-Internet	PROD	Public Internet	
<input type="checkbox"/>	1	Allow-TCP-8000	PROD	PROD	
<input type="checkbox"/>	2	Allow-PROD-Ping	PROD	PROD	
<input type="checkbox"/>	3	Allow-AWS	DEV, PROD	Public Internet	Allow-AWS
<input type="checkbox"/>	4	Allow-NTP	DEV, PROD	Public Internet	

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**.

The screenshot shows the AWS Management Console interface. At the top, the 'Oregon' region is selected. The breadcrumb navigation shows 'EC2 > Instances > SAP 3 > Connect to instance'. The main heading is 'Connect to instance' with an 'Info' link. Below this, it says 'Connect to your instance i-0de75c665c140ea1a (SAP3) using any of these options'. There are four tabs: 'EC2 Instance Connect', 'Session Manager' (which is highlighted with a red box), 'SSH client', and 'EC2 serial console'. Under the 'Session Manager' tab, there is a section titled 'Session Manager usage:' with a bulleted list of features. At the bottom right, there are two buttons: 'Cancel' and 'Connect' (which is highlighted with a red box).

aws Services Q 📄 🔔 ? **Oregon**

EC2 IAM CloudFormation VPC AWS Cost Explorer

EC2 > Instances > **SAP 3** > Connect to instance

### Connect to instance [Info](#)

Connect to your instance i-0de75c665c140ea1a (SAP3) 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, a bastion host, or opening any inbound ports.
- 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**

## Lab 4: Threat Prevention: Step 4.4

Confirm open internet access for PROD

Session ID: brad-0a81a0d1bec850995

Instance ID: i-0de75c665c140ea1a

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)

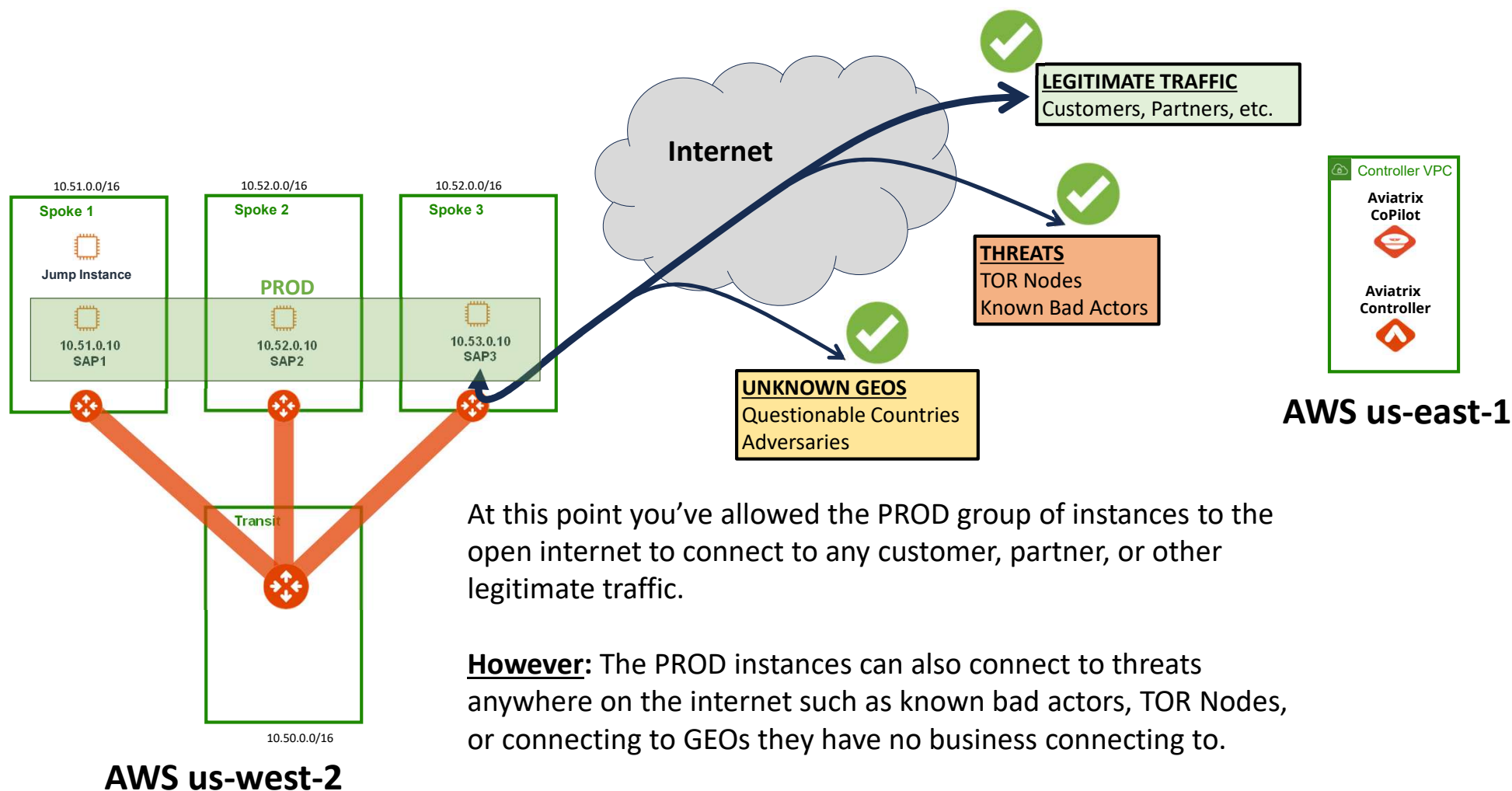
**curl https://google.com** 2

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

```
sh-4.2$ 1 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 ~]$ 2 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 ~]$
```

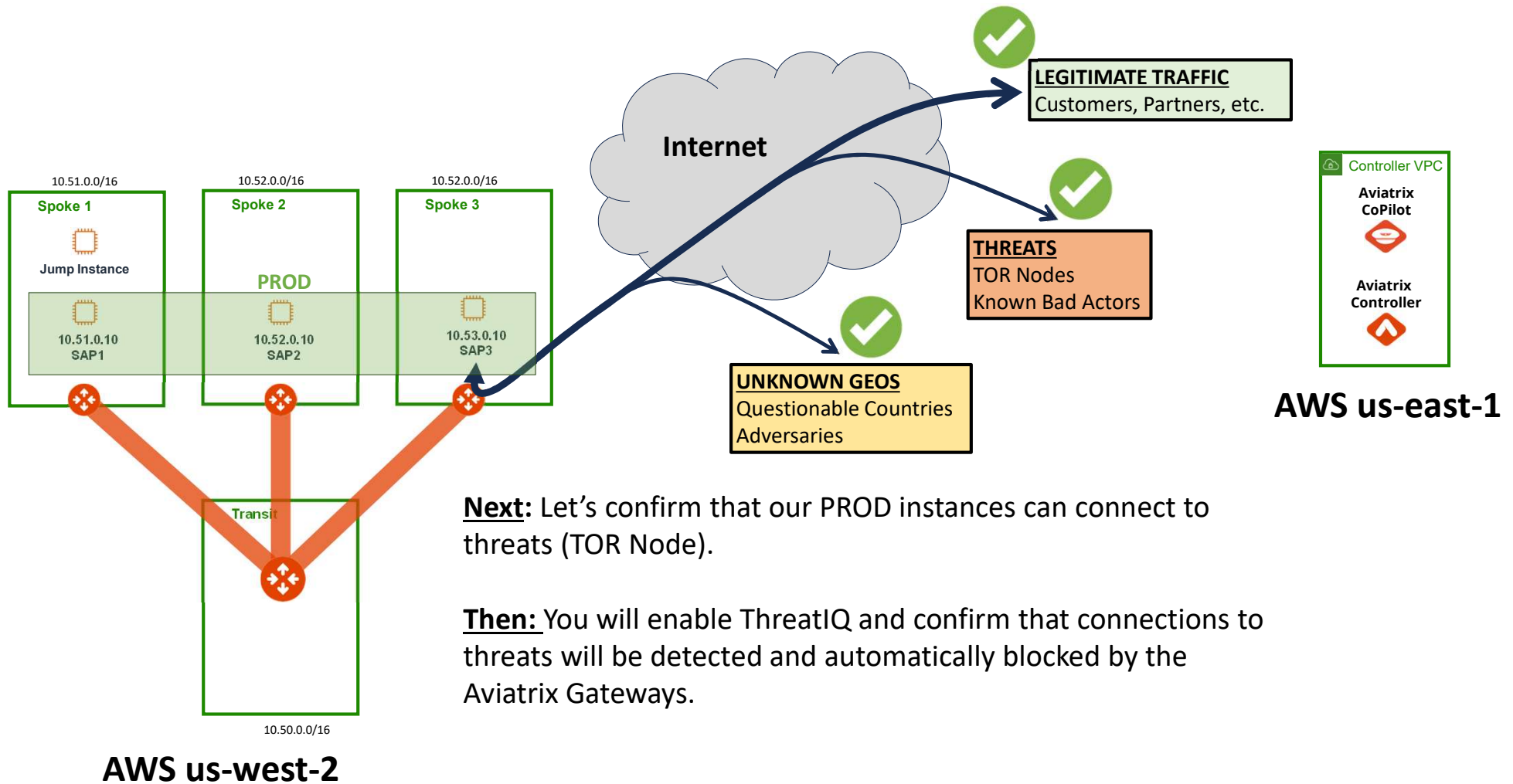


## Lab 4: Checkpoint 1: Current State





## Lab 4: Checkpoint 1: Current State



## 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!**



**AbuseIPDB** » [103.251.167.10](#)

Check an IP Address, Domain Name, or Subnet  
e.g. 104.188.236.185, microsoft.com, or 5.188.10.0/24

103.251.167.10 **1** **CHECK**

**103.251.167.10 was found in our database!**


This IP was reported **2,869** times. Confidence of Abuse is **100%**: ?

**100%**

 This address is a Tor exit node. Neither the owner nor the provider are directly behind the offending action.

ISP: The Infrastructure Group B.V.  
Usage Type: Data Center/Web Hosting/Transit  
Hostname(s): this-is-a-TOR-EXIT-NODE.union  
Domain Name:  
Country:  
City:

**Recent Reports:** We have received reports of abusive activity from this IP address within the last week. It is potentially still actively engaged in abusive activities.

Reporter	IoA Timestamp	Comment	Categories
 <a href="#">niceshops.com</a>	2023-11-14 09:37:00 (10 hours ago)	Web Attack multi (Nov 23 10:37:00 Matching rules: Detected possible SQL injection - E.g. Sleep(5) )	<ul style="list-style-type: none"> <li>SQL Injection</li> <li>Brute-Force</li> <li>Bad Web Bot</li> <li>Web App Attack</li> </ul>

**2**

**Aleo**  
ZK made easy  
Start building

**snarkOS** - A decentralized operating system for zero-knowledge applications.  
ADS VIA CARBON

**SPONSOR**  
**IONOS** Want to go static? Deploy static sites, SPAs, and PHP Apps on Git Push with Deploy Now.



## 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 Aviaatrix 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>

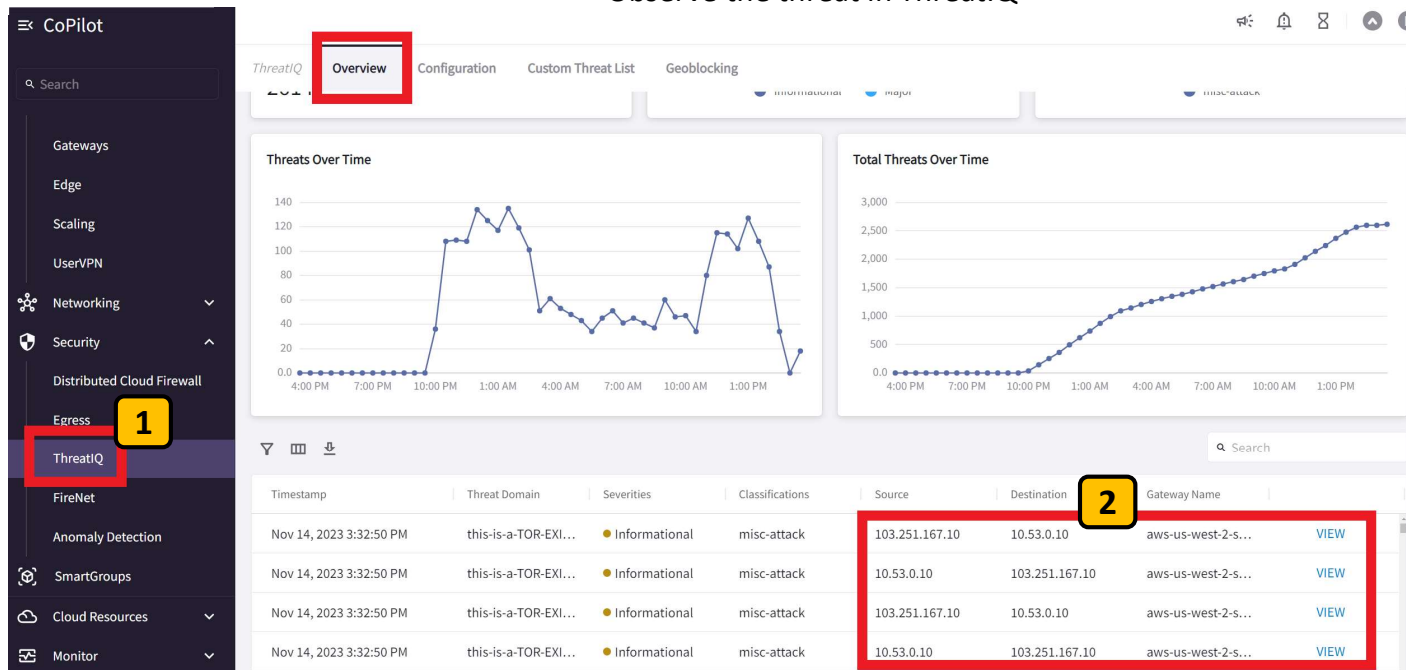
<p>
You also have the option of blocking this IP address and others on
the Tor network if you so desire. The Tor project provides a <a
href="https://check.torproject.org/torbulkexitlist">web service</a>
to fetch a list of all IP addresses of Tor exit nodes that allow exiting to a
specified IP:port combination, 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

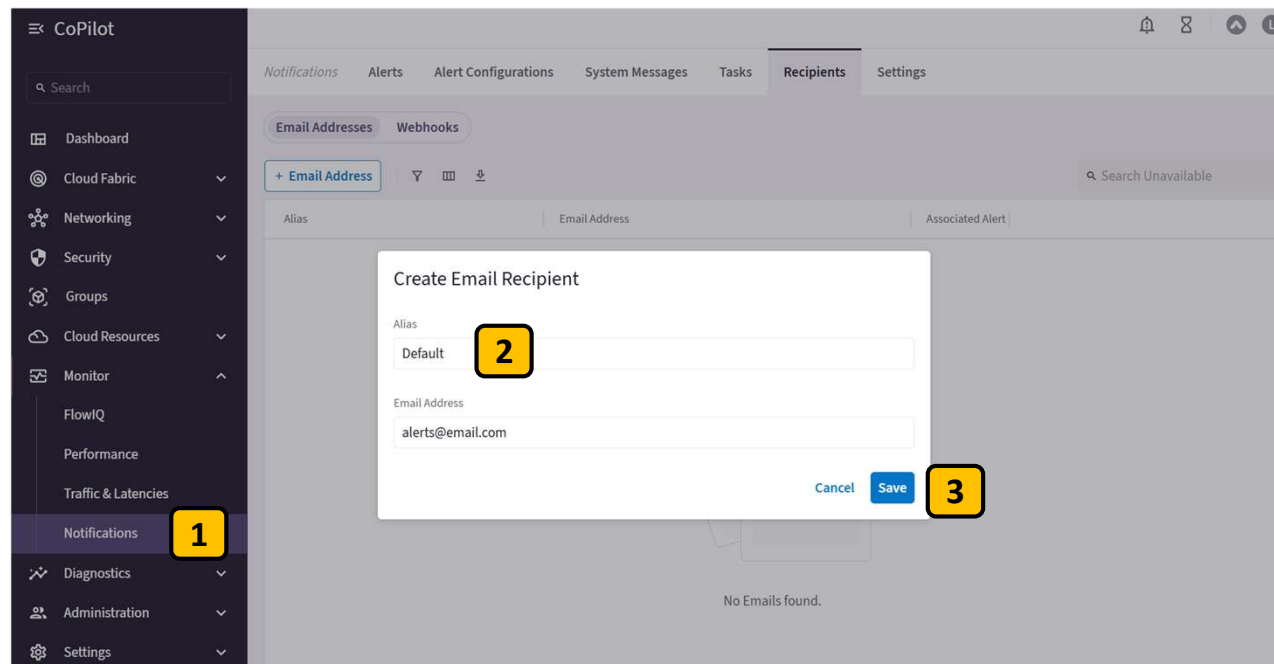
Enable threat alerting in ThreatIQ

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](mailto:alerts@email.com) **2**

Click **Save** **3**





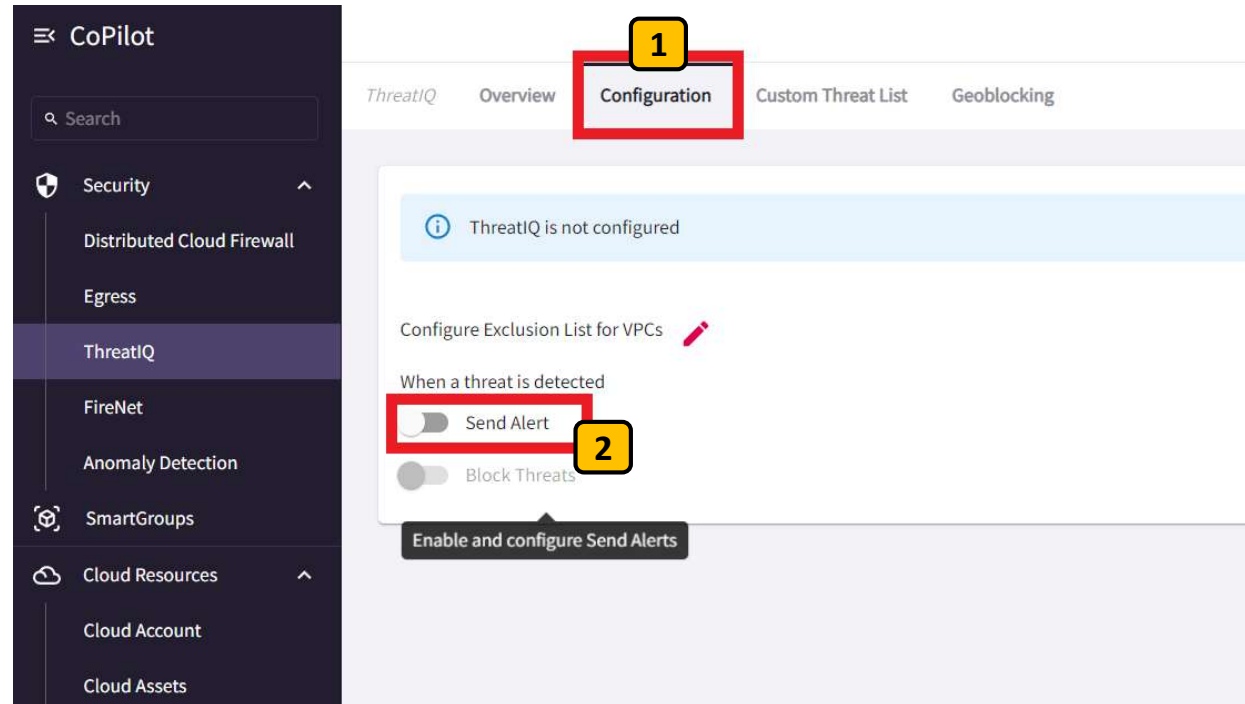
## Lab 4: Threat Prevention: Step 4.10

Enable threat alerting in ThreatIQ

To protect our PROD instances, let's begin by enabling 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

### Add Alert Configuration: ThreatIQ Alert

ⓘ Alert conditions are evaluated every minute. When conditions are met, alerts will be sent to selected recipients. To configure an alert, add recipients in [Notification Settings](#)

Name

ThreatIQ Alert

Send Alerts To

Recipients

Default ×

1

× ▼

Cancel

Save

2

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

Then **Confirm.** 2





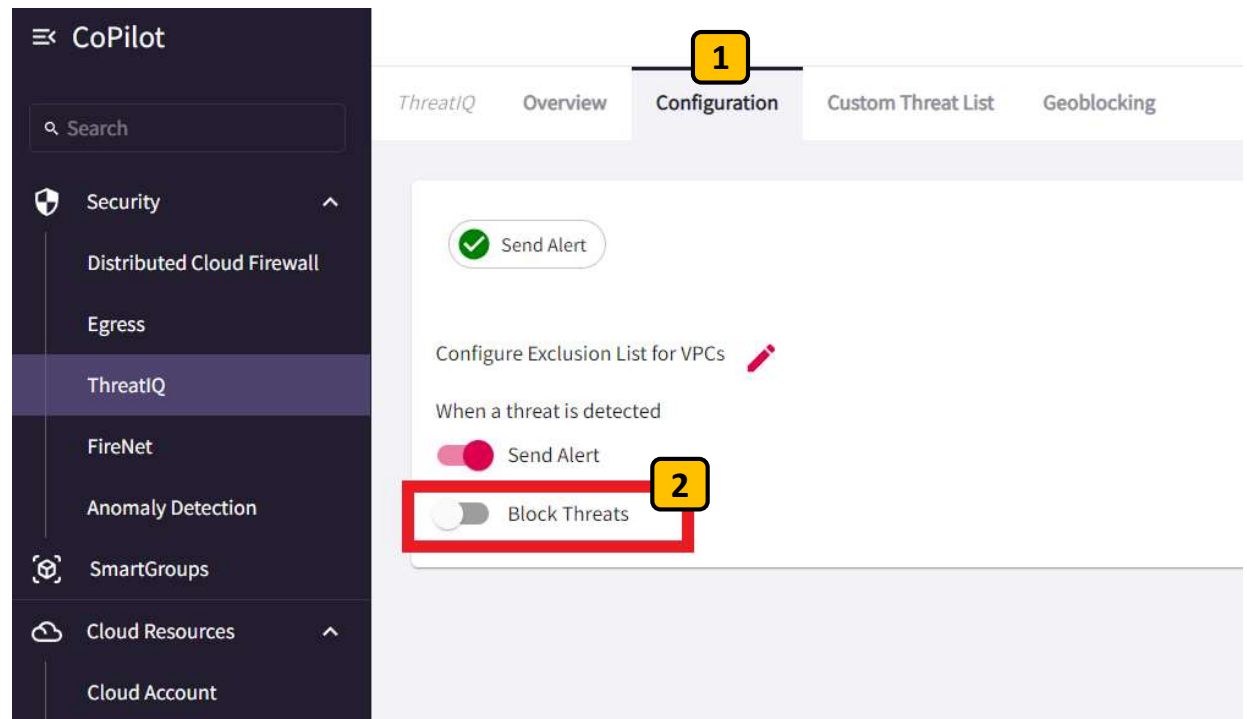
## Lab 4: Threat Prevention: Step 4.12

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**

Select VPC/VNets to allow/deny ThreatIQ protection

By default, ThreatIQ protects all instances in all the VPCs. Select and move VPCs to the 'Not Protected' List to deny ThreatIQ from protecting them.

☐ Protected with ThreatIQ  
0/6 selected

VPC/VNet Name	Cloud	Region
<input type="checkbox"/> VPC A	aws	us-east-1
<input type="checkbox"/> VPC B	aws	us-east-1
<input type="checkbox"/> aws-us-west-2-spoke-1	aws	us-west-2
<input type="checkbox"/> aws-us-west-2-spoke-2	aws	us-west-2
<input type="checkbox"/> aws-us-west-2-spoke-3	aws	us-west-2
<input type="checkbox"/> aws-us-west-2-transit	aws	us-west-2

☐ Not Protected  
0/0 selected

VPC/VNet Name	Cloud	Region
---------------	-------	--------

**Block all future traffic to and from threat IP**

When CoPilot sees a Threat IP in the traffic, ThreatIQ rules will be added to block all future traffic from and to the IP.

ThreatIQ blocking will not work on gateways where FQDN-AllowAll is configured

2 CONFIRM

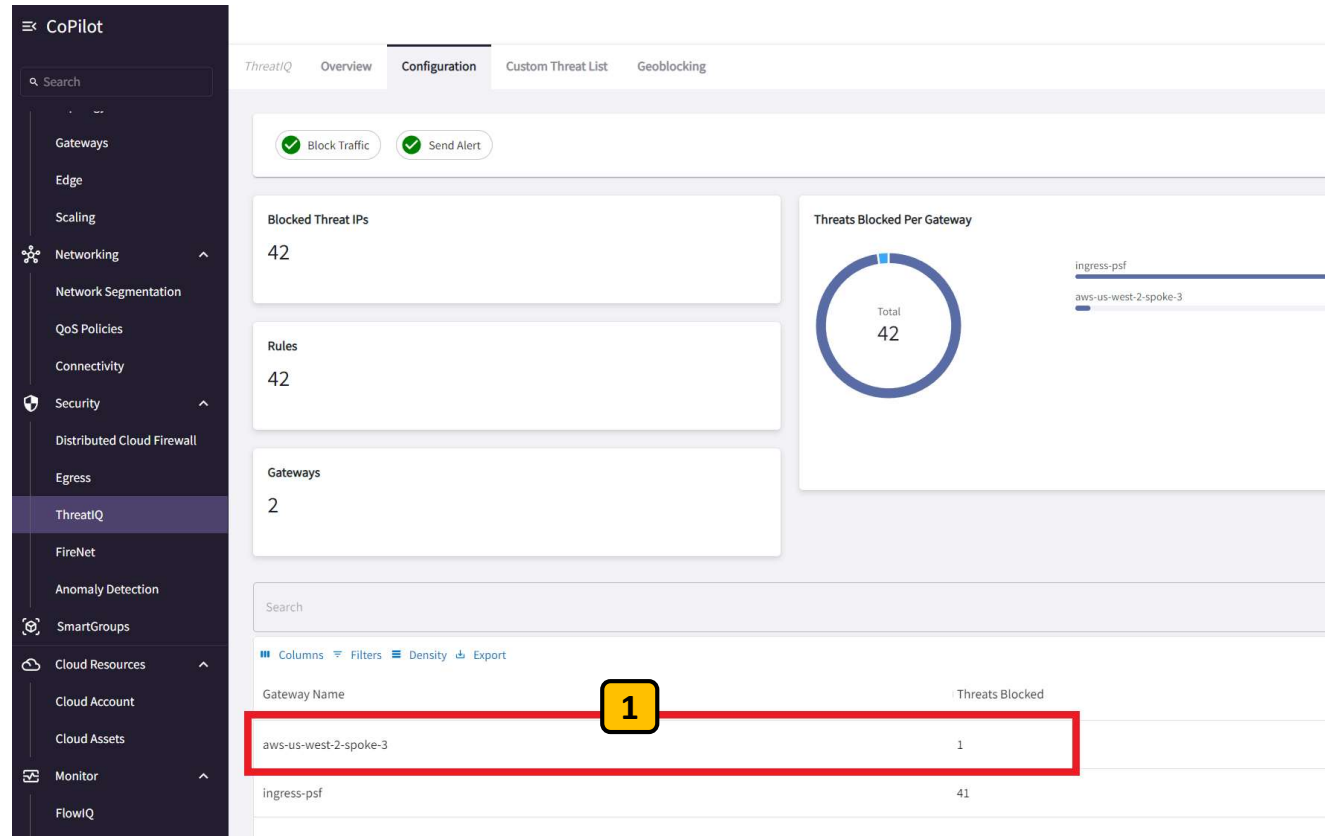


## Lab 4: Threat Prevention: Step 4.14

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
```

## 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**

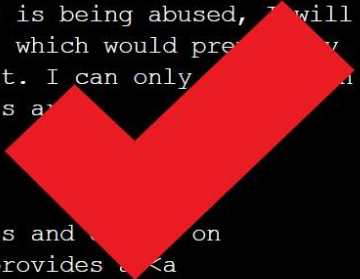
Now that threat blocking is enabled, CoPilot will witness these connections again and configure drop rules on your Aviatrix Gateway for the threat IP.

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 prevent my
router from allowing that traffic to exit through it. I can only block on an
IP+destination port basis, however. Common P2P ports are already blocked.</p>

<p>
You also have the option of blocking Tor exit nodes and Tor users on
the Tor network if you so desire. The Tor project provides a <a
href="https://check.torproject.org/exit-addresses">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/torndnsel/">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 if 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 4.17

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 ~]$
```

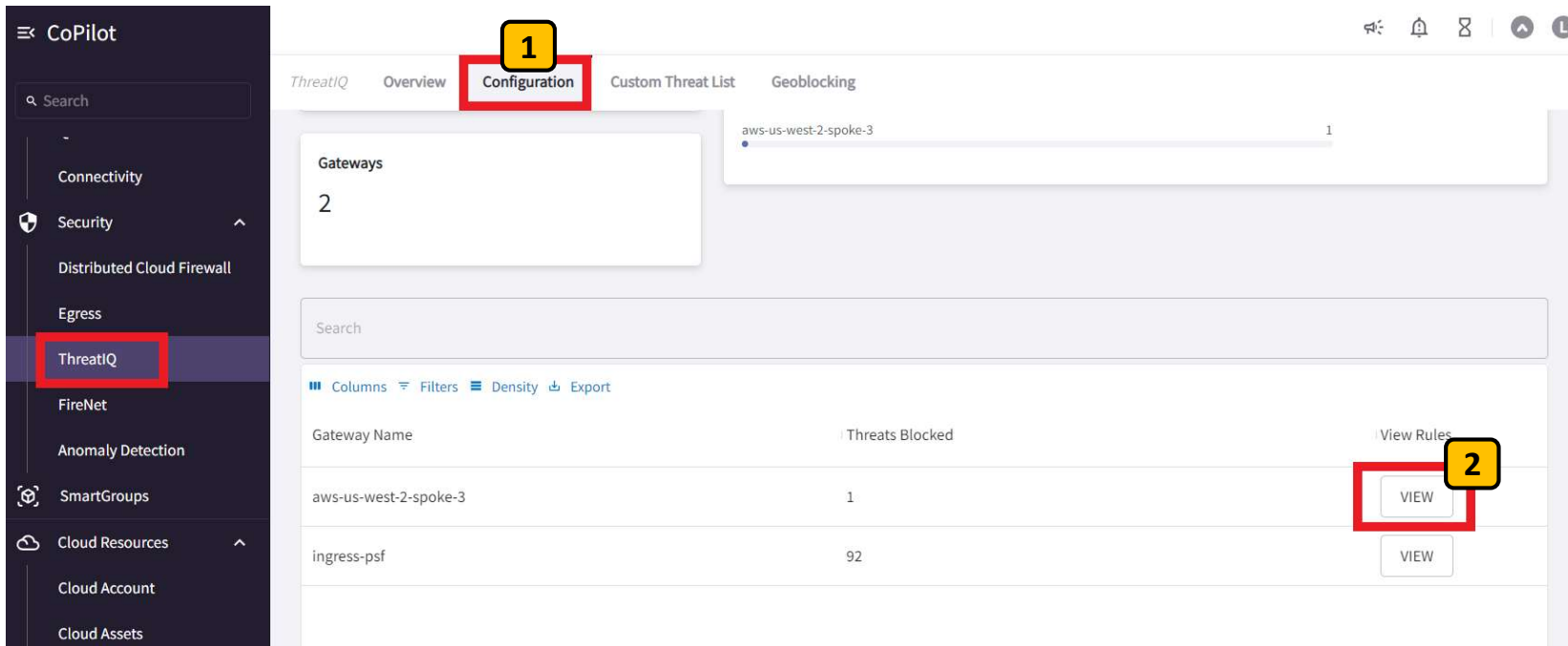


After a few minutes of you should  
being to see your connections to  
this threat IP fail. **1**

Aviaatrix 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



The screenshot shows the Aviaatrix ThreatIQ interface. On the left is a dark sidebar with a 'CoPilot' header and a search bar. Below the search bar are several menu items: 'Connectivity', 'Security' (with a shield icon), 'Distributed Cloud Firewall', 'Egress', 'ThreatIQ' (highlighted with a red box and a yellow '1' in a box), 'FireNet', 'Anomaly Detection', 'SmartGroups' (with a network icon), 'Cloud Resources' (with a cloud icon), 'Cloud Account', and 'Cloud Assets'. The main panel has tabs for 'ThreatIQ', 'Overview', 'Configuration' (highlighted with a red box and a yellow '1' in a box), 'Custom Threat List', and 'Geoblocking'. Below the 'Configuration' tab, there's a 'Gateways' section showing '2' gateways. A search bar is present. Below that is a table with columns 'Gateway Name', 'Threats Blocked', and 'View Rules'. The table has two rows: 'aws-us-west-2-spoke-3' with 1 threat blocked, and 'ingress-psf' with 92 threats blocked. The 'View Rules' button for the 'aws-us-west-2-spoke-3' row is highlighted with a red box and a yellow '2' in a box.

Gateway Name	Threats Blocked	View Rules
aws-us-west-2-spoke-3	1	<a href="#">VIEW</a>
ingress-psf	92	<a href="#">VIEW</a>

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

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

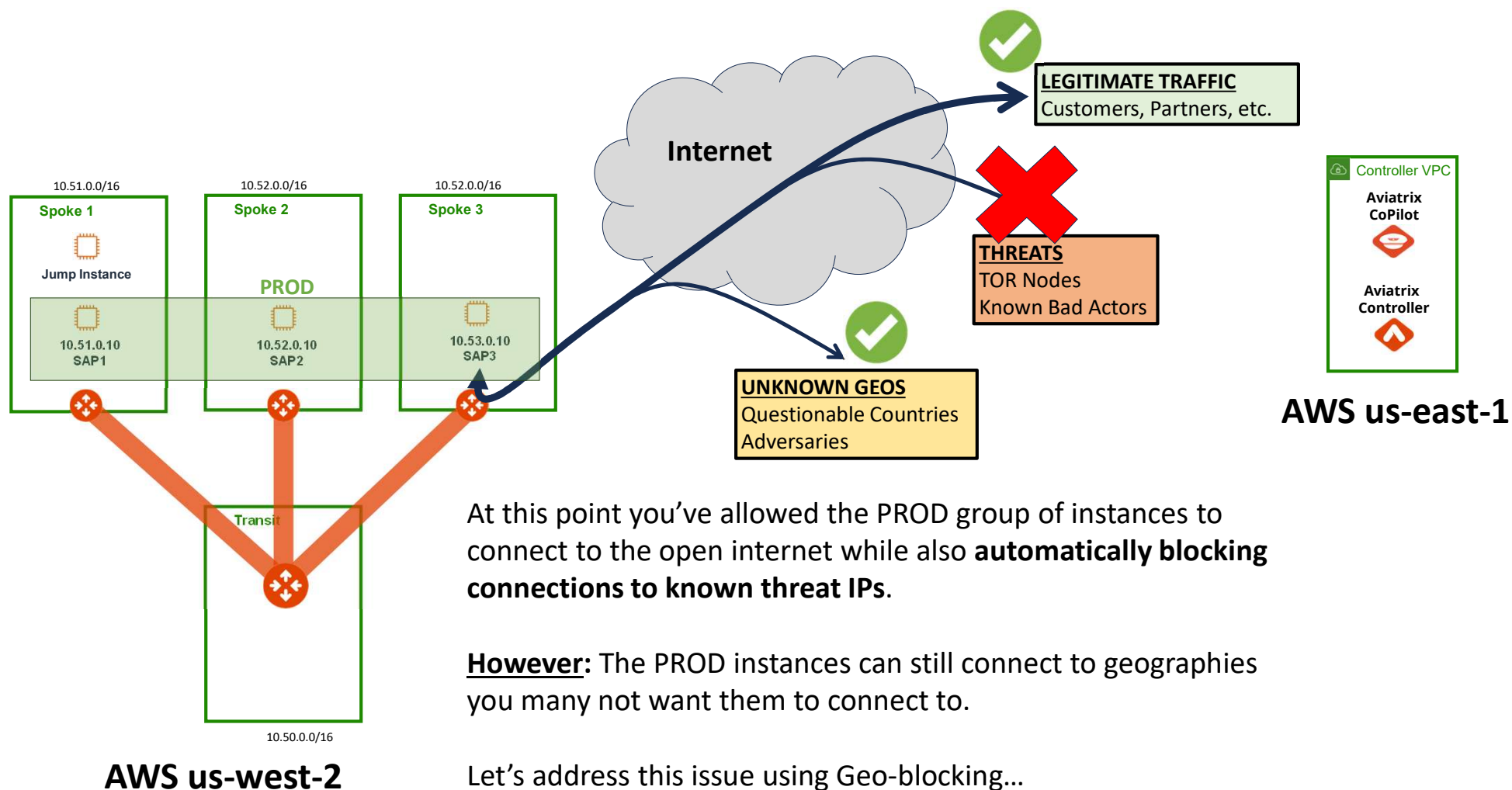
You should see the threat IP you connected to listed in a drop rule configured on this Aviaatrix Gateway handing internet traffic for the instance SAP 3

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





## 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**

⚠ Geoblocking is in Preview. Preview features are not safe for deployment in production environments.



Geoblocking

Geoblocking allows you to select countries to block IP traffic coming into and coming from the country. When Geoblocking is enabled for a country, a tag-based security policy is implemented on each gateway to deny traffic for IP addresses associated with the country.

All gateways in your VPC/VNets will block.

Cancel

Enable Geoblocking

3

CoPilot

Search

Dashboard

Cloud Fabric

Networking

Security

Distributed Cloud Firewall

Egress

ThreatIQ

FireNet

Anomaly Detection

Groups

Cloud Resources

Monitor

Diagnostics

Administration

Settings

Configuration

Resources

Configuration General License Logging Services Private Mode

License Type Universal

License ID	Controller ID	Issue Date	Allocated	Total
Lic-1676837225.25	9a0685be-17ac-4a9d-84dc-0f47bc7ae752	Feb 19, 2023	1	1

Customer ID

avi-25

Reset

Add-on Features

Feature	Status
Distributed Cloud Firewall	Disable
CostIQ	Enable
Network Insights API	Enable

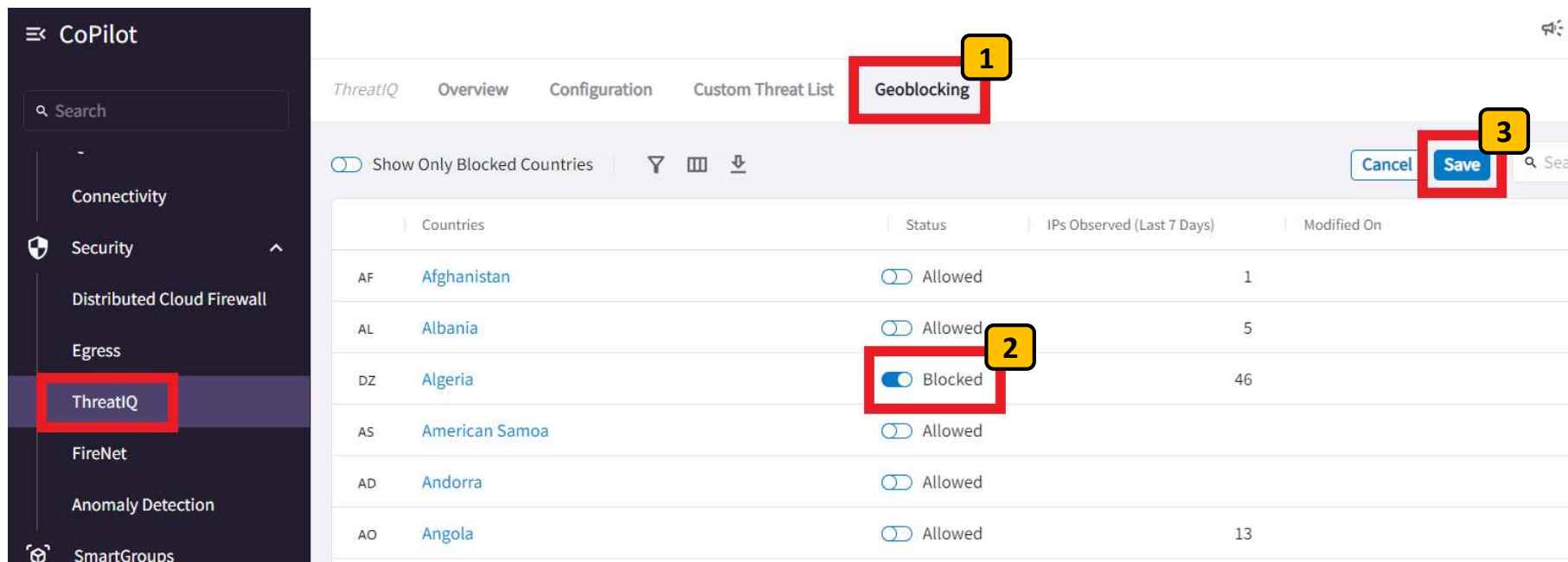
Feature Previews

Refresh

Feature	Status
Auto Right-Sizing	Preview
CoPilot Visibility	Preview
DCF on External Connections	Requires Controller v7.2 ...
DCF on PSF Gateways	Requires Controller v7.2 ...
Edge Platform - Megaport	Preview
ExternalGroups	Requires Controller v7.2 ...
GCP Global VPC	Preview
Geoblocking	Enable
Hostname-based SmartGrou	Requires Controller v7.2....
Intelligent Cloud Analytics	Preview
New Topology Overview	Preview

## Lab 4: Threat Prevention: Step 4.21

Block geographies using Geoblocking



The screenshot shows the Aviaatrix ThreatIQ interface. On the left, the 'ThreatIQ' menu item is highlighted. The main panel displays the 'Geoblocking' tab. A table lists countries with their status (Allowed or Blocked) and the number of IPs observed in the last 7 days. The 'Algeria' row is highlighted, and its status is 'Blocked'. The 'Save' button is visible in the top right corner.

Countries	Status	IPs Observed (Last 7 Days)	Modified On
AF <a href="#">Afghanistan</a>	Allowed	1	
AL <a href="#">Albania</a>	Allowed	5	
DZ <a href="#">Algeria</a>	Blocked	46	
AS <a href="#">American Samoa</a>	Allowed		
AD <a href="#">Andorra</a>	Allowed		
AO <a href="#">Angola</a>	Allowed	13	

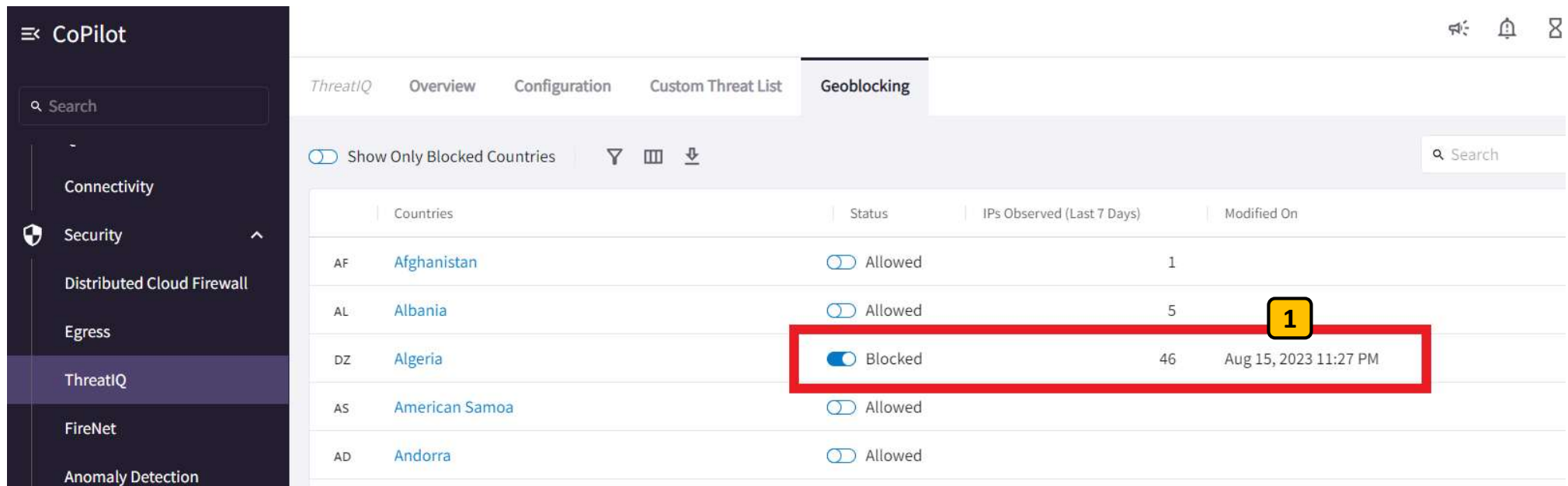
Go to the **Geoblocking** tab of ThreatIQ and you will see a long list of countries and how many IPs have been observed from them on your network. **1**

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

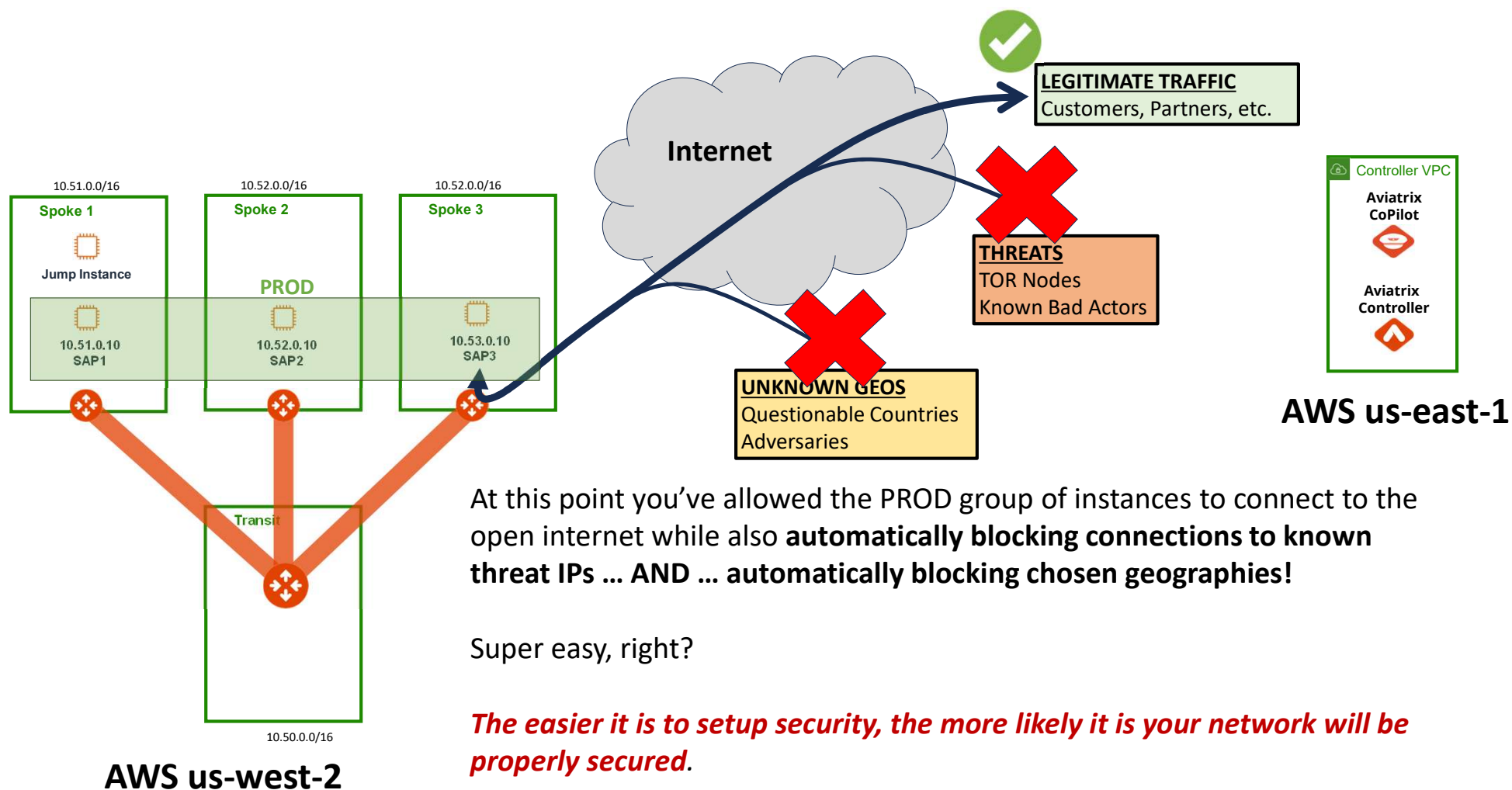


The screenshot shows the Aviaatrix ThreatIQ Geoblocking interface. The left sidebar contains the 'CoPilot' menu with options: Connectivity, Security (expanded), Distributed Cloud Firewall, Egress, ThreatIQ (selected), FireNet, and Anomaly Detection. The main panel displays the 'Geoblocking' tab with a table of countries. The table has columns: Countries, Status, IPs Observed (Last 7 Days), and Modified On. The row for 'Algeria' (DZ) is highlighted with a red box, and a yellow box with the number '1' is placed next to the 'Blocked' status.

Countries	Status	IPs Observed (Last 7 Days)	Modified On
AF <a href="#">Afghanistan</a>	<input type="checkbox"/> Allowed	1	
AL <a href="#">Albania</a>	<input type="checkbox"/> Allowed	5	
DZ <a href="#">Algeria</a>	<input checked="" type="checkbox"/> Blocked	46	Aug 15, 2023 11:27 PM
AS <a href="#">American Samoa</a>	<input type="checkbox"/> Allowed		
AD <a href="#">Andorra</a>	<input type="checkbox"/> Allowed		

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



## Lab 4: Success

