

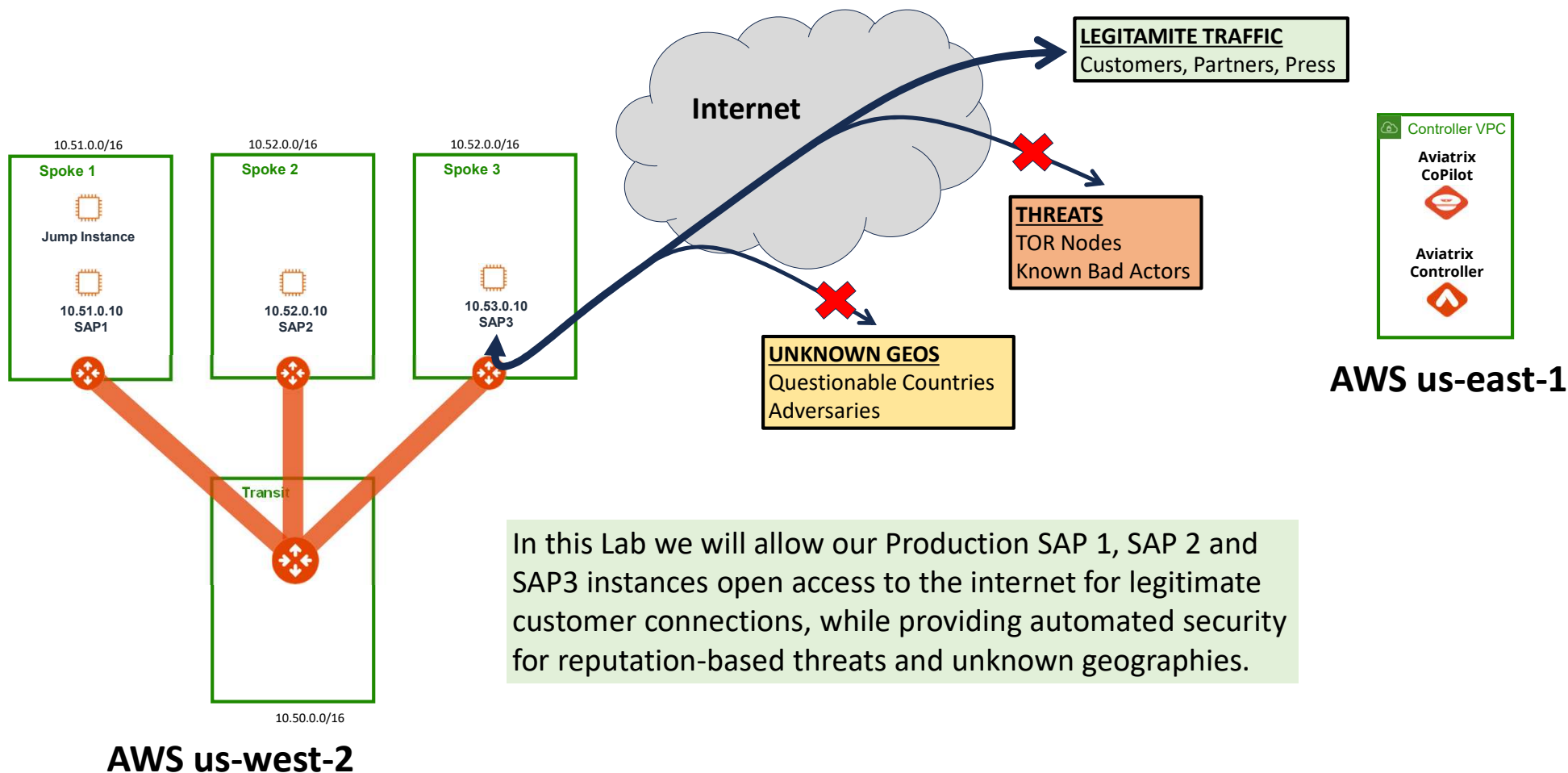
AWS Immersion Day LAB 4

SECURITY: THREAT PREVENTION & GEOBLOCKING

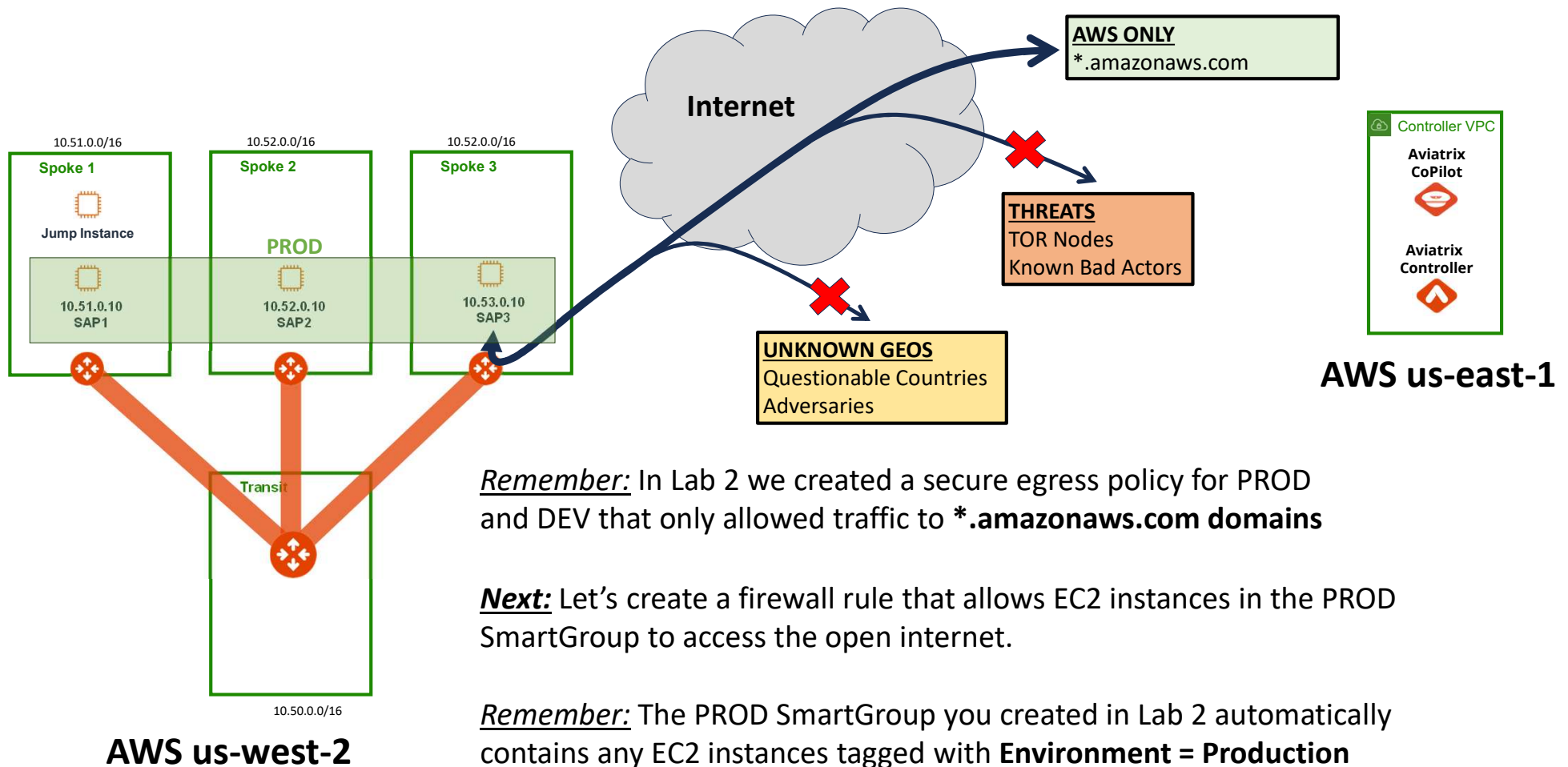
Ben Biley
Solutions Engineer
Aviatrix Systems

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. **1**

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

~~Allow this traffic to access any domain using the default Any Web WebGroup.~~ **3** Leave WebGroups Blank*

Set Protocol to **Any** and enable Logging and Permit the traffic. **4**

Place the rule on **Top** and click **Save In Drafts** **6**

* There is currently a bug with L7 rules not generating Netflow records, that will be fixed in the next release.

CoPilot

firewall

Security

Distributed Cloud Firewall

FireNet

Firewall

+ Rule

Rules

Monitor

Create Rule

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

Name

PROD-Internet

Source SmartGroups

PROD

Destination SmartGroups

Public Internet

WebGroups

Protocol

Any

Port

All

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

Rule Behavior

Action

Permit

SG Orchestration

Off

Ensure TLS

Off

TLS Decryption

Off

Intrusion Detection (IDS)

Off

Enforcement

On

Logging

On

Rule Priority

Place Rule

Top

Cancel

Save In Drafts

Lab 4: Threat Prevention: Step 4.1

Allow open internet for PROD

CoPilot

firewall

Security

Distributed Cloud Firewall

FireNet

Firewall

Distributed Cloud Firewall
Rules
Monitor
Detected Intrusions
WebGroups
Settings

+ Rule
Actions
1 New
Discard
Commit
Search

	Priority	Name	Source	Destination	WebGroup
<input checked="" 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 4.2

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' (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:

- 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.

At the bottom right, there are two buttons: 'Cancel' and 'Connect' (highlighted with a red box).

Lab 4: Threat Prevention: Step 4.3

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)

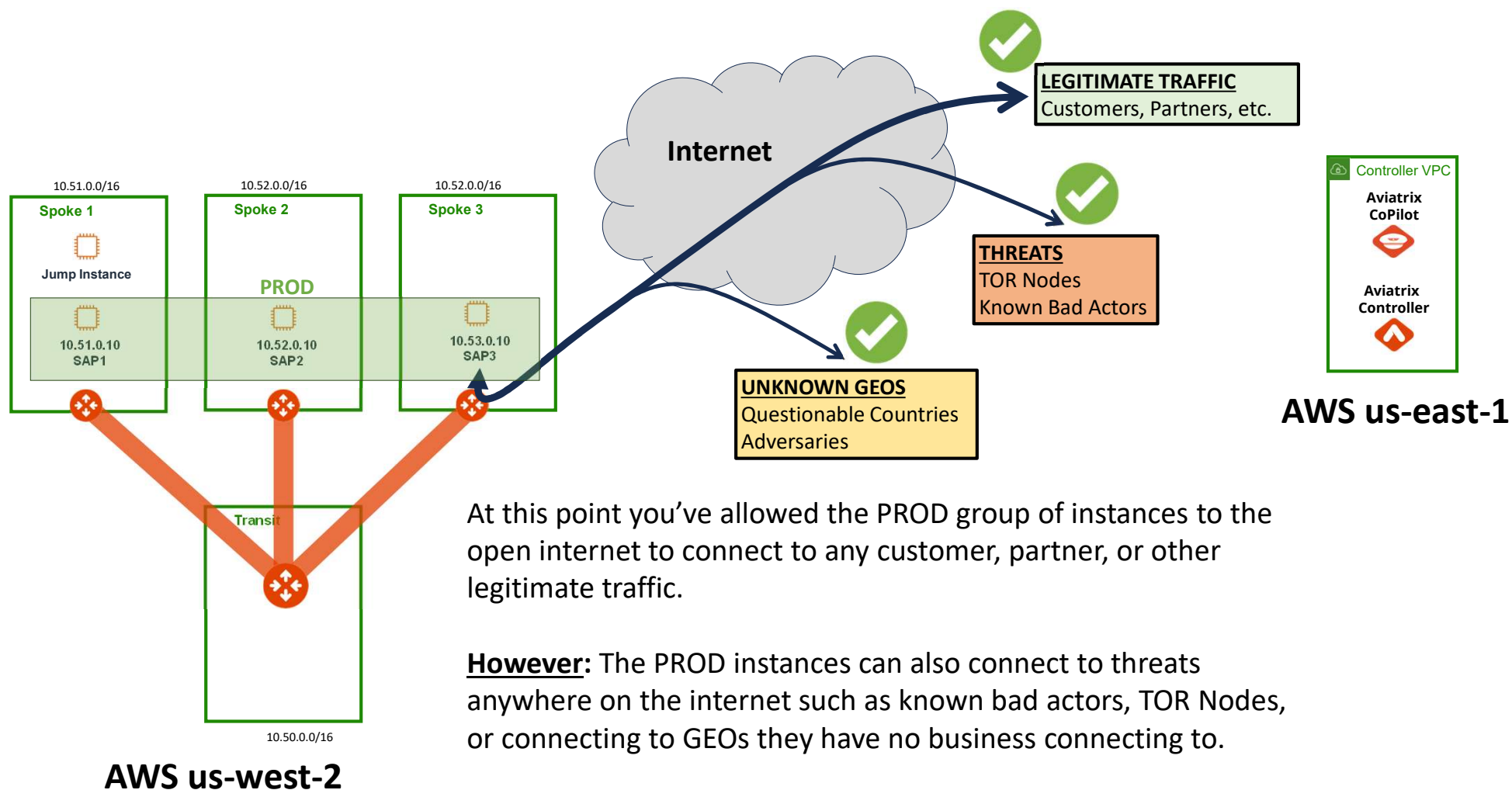
curl https://google.com 2

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

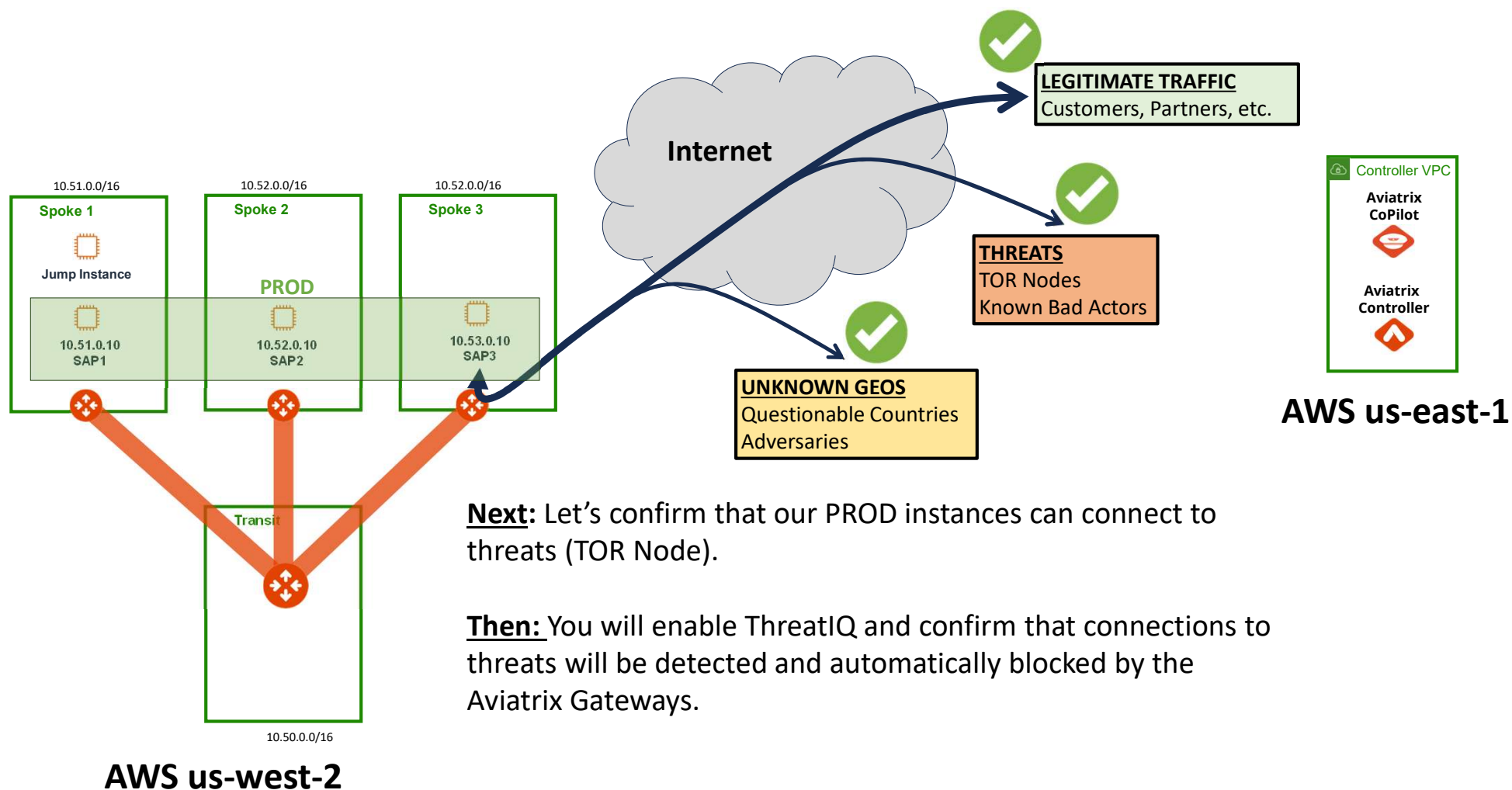
```
sh-4.2$ sudo su -l ec2-user 1
Last login: Tue Aug 15 23:05:56 UTC 2023 on pts/1
[ec2-user@ip-10-53-0-10 ~]$
[ec2-user@ip-10-53-0-10 ~]$
[ec2-user@ip-10-53-0-10 ~]$ curl https://google.com 2
<HTML><HEAD><meta http-equiv="content-type" content="text/html; charset=utf-8">
<TITLE>301 Moved</TITLE></HEAD><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 4.4

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
 niceshops.com	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"> SQL Injection Brute-Force Bad Web Bot Web App Attack

SPONSOR

Aleo ZK made easy
Start building

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

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

2



Lab 4: Threat Prevention: Step 4.5

Connect to the abuse IP

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

curl http://184.105.48.40 **1**

Note: (HTTP Not HTTPS)

Session ID: brad-0e2fe1f2e50a521a3

Instance ID: i-0de75c665c140ea1a

```
[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://184.105.48.40
```

1

Lab 4: Threat Prevention: Step 4.6

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...

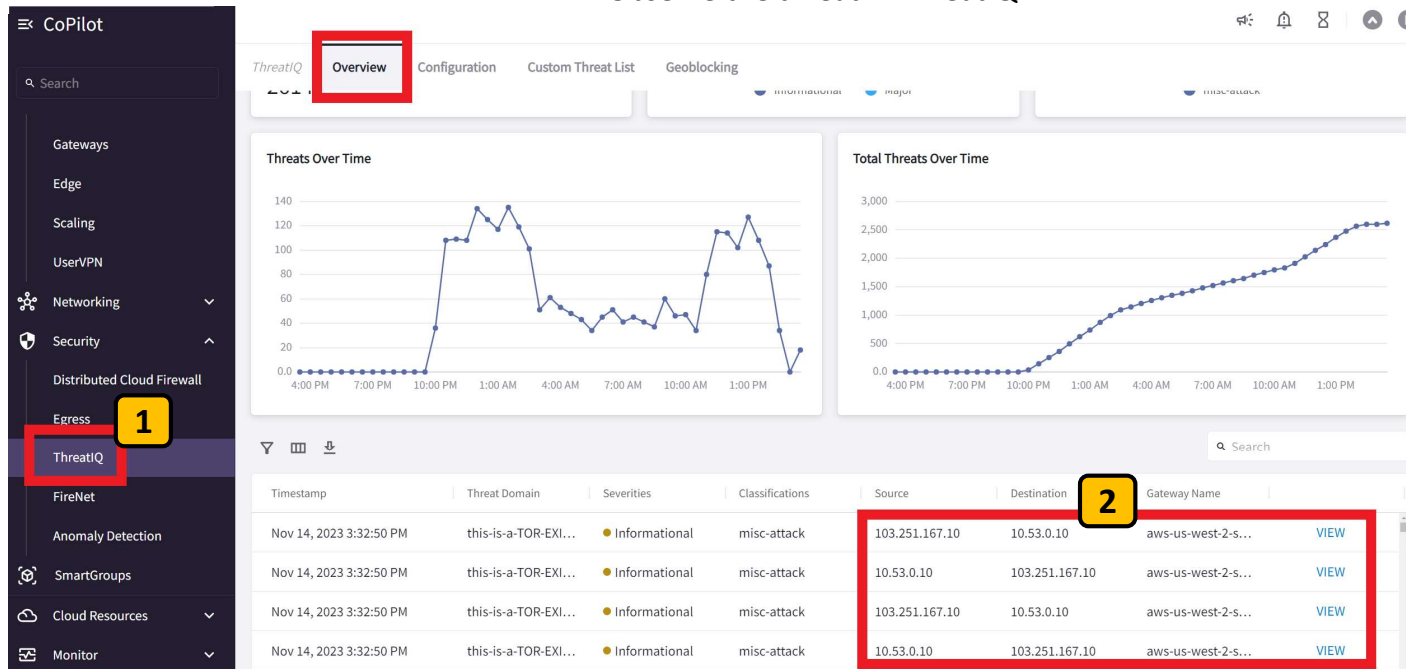
```
<p>
That being said, if you still have a complaint about the router, you may
email the <a href="mailto:abuse@august.tw">maintainer</a>. If
complaints are related to a particular service that is being abused, I will
consider removing that service from my exit policy, which would prevent my
router 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 access and blocking 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 4.7

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.



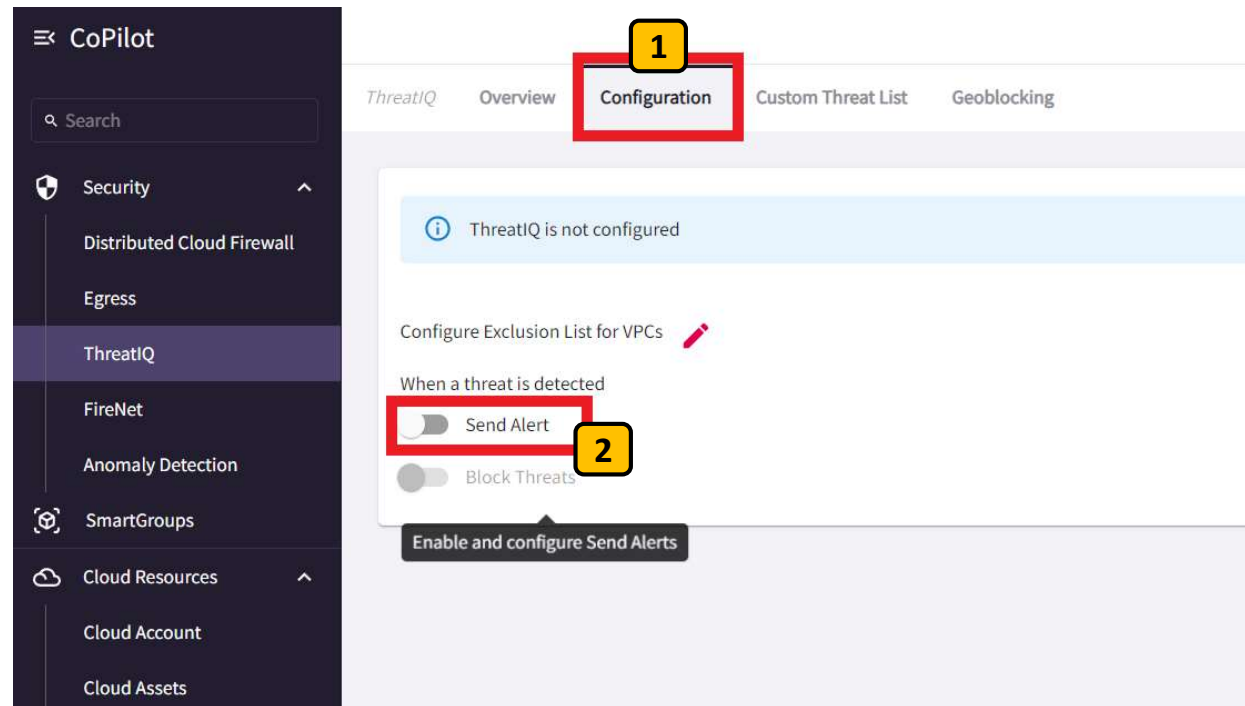
Lab 4: Threat Prevention: Step 4.8

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 4.9

Enable threat alerting in ThreatIQ

Notification Settings'. At the bottom right, there is a blue 'CONFIRM' button. Two yellow numbered callouts are present: '1' points to the 'Add Recipient(s)' box, and '2' points to the 'CONFIRM' button." data-bbox="73 245 942 603"/>

ThreatIQ Configuration

Define Alert

Name of the Alert

ThreatIQ Alert

Condition

Select a Metric (e.g. Rate, Status)

Threat IP Detected

An Alert will be sent when a threat is detected.

Add Recipient(s)

alerts@email.com

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](#)

CONFIRM

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

Then **Confirm.** **2**

Lab 4: Threat Prevention: Step 4.10

Create a Notification Recipient for detected Threats

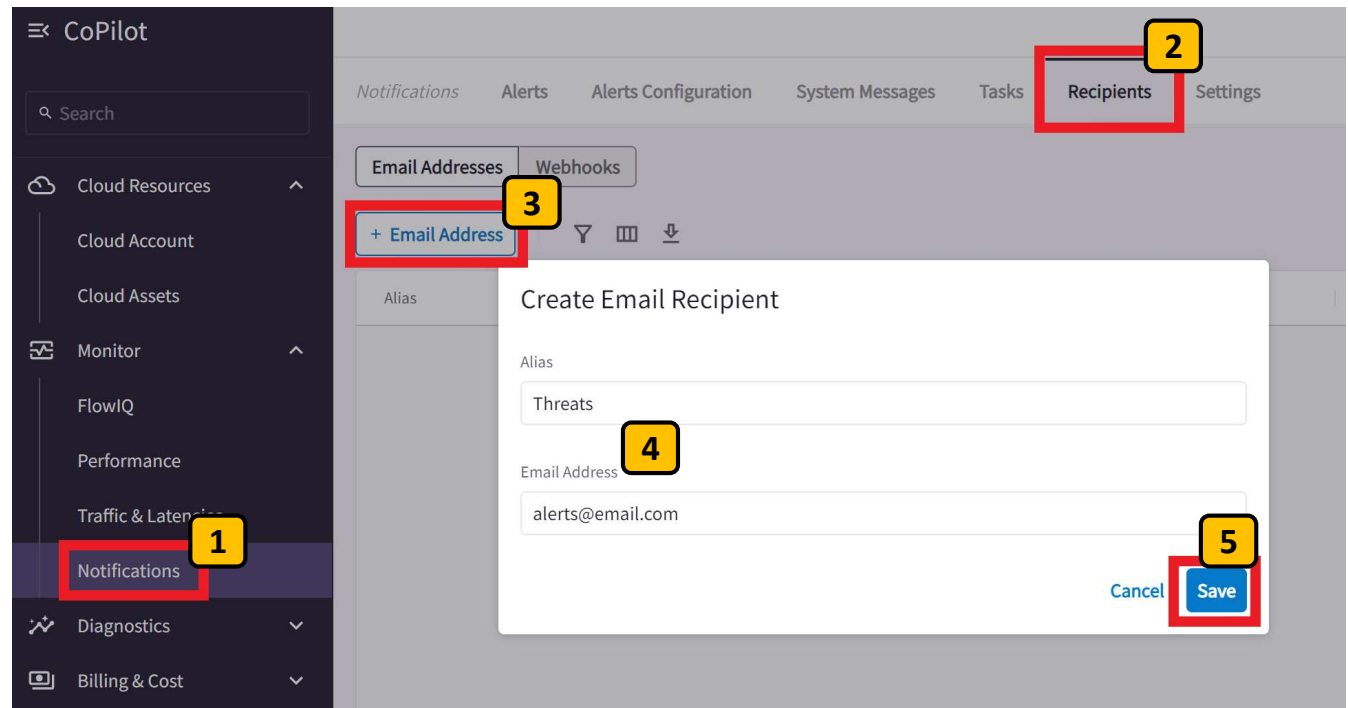
From the CoPilot UI select the **Notifications** section under Monitor. **1**

Select the **Recipients** tab. **2**

Click **+ Email Address** button to add an email recipient. **3**

Name the Alias Threats and provide an email address. **4**

Click **Save**. **5**



Note: In a real word production deployment you can also create Webhook recipients to be ingested by anything that accepts Webhooks, like a Slack channel or your favorite SIEM system.



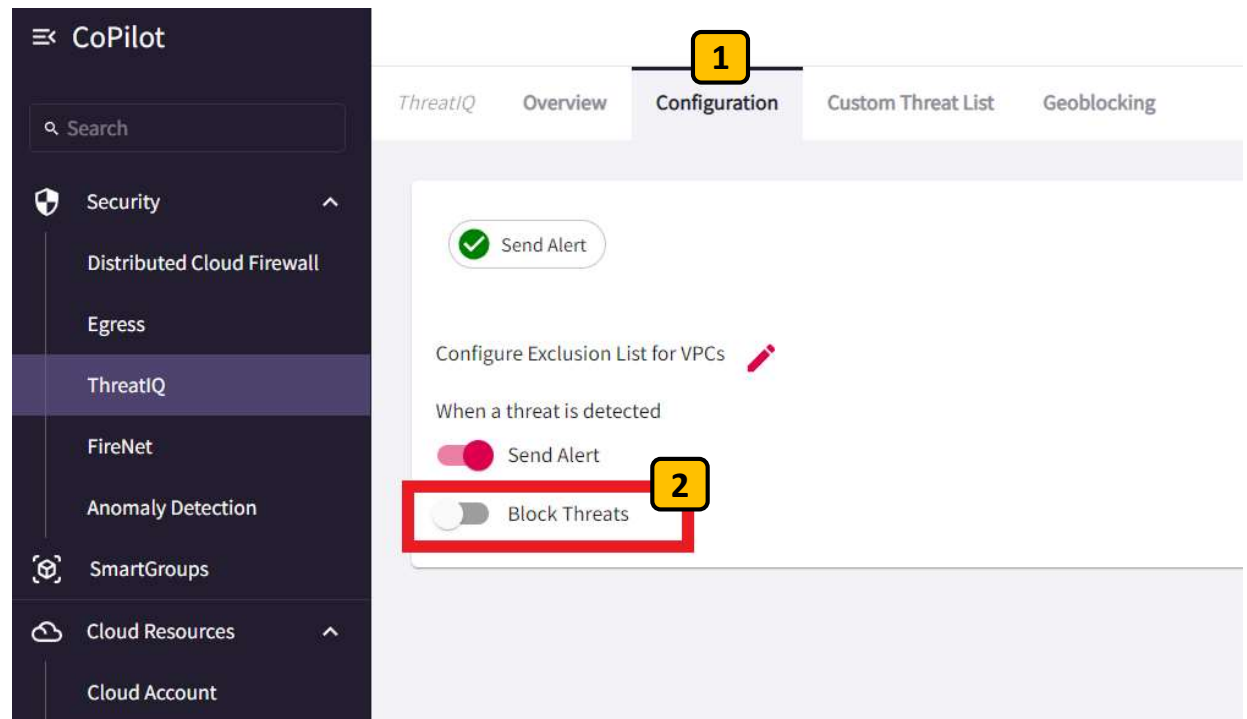
Lab 4: Threat Prevention: Step 4.11

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 4.11

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**

The screenshot shows the 'Select VPC/VNets to allow/deny ThreatIQ protection' dialog. It has two columns: 'Protected with ThreatIQ' (0/6 selected) and 'Not Protected' (0/0 selected). The 'Protected with ThreatIQ' column contains a table with the following data:

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

Below the table are '>' and '<' buttons. A red arrow points to the 'Save' button in the bottom right corner, which is labeled with a yellow box containing the number '1'. A confirmation dialog is overlaid on top of the main dialog, titled 'Block all future traffic to and from threat IP'. It contains the text: 'When CoPilot sees a Threat IP in the traffic, ThreatIQ rules will be added to block all future traffic from and to the IP.' Below this is a yellow warning box that says: 'ThreatIQ blocking will not work on gateways where FQDN-AllowAll is configured'. At the bottom of the dialog is a blue 'CONFIRM' button, which is labeled with a yellow box containing the number '2'.

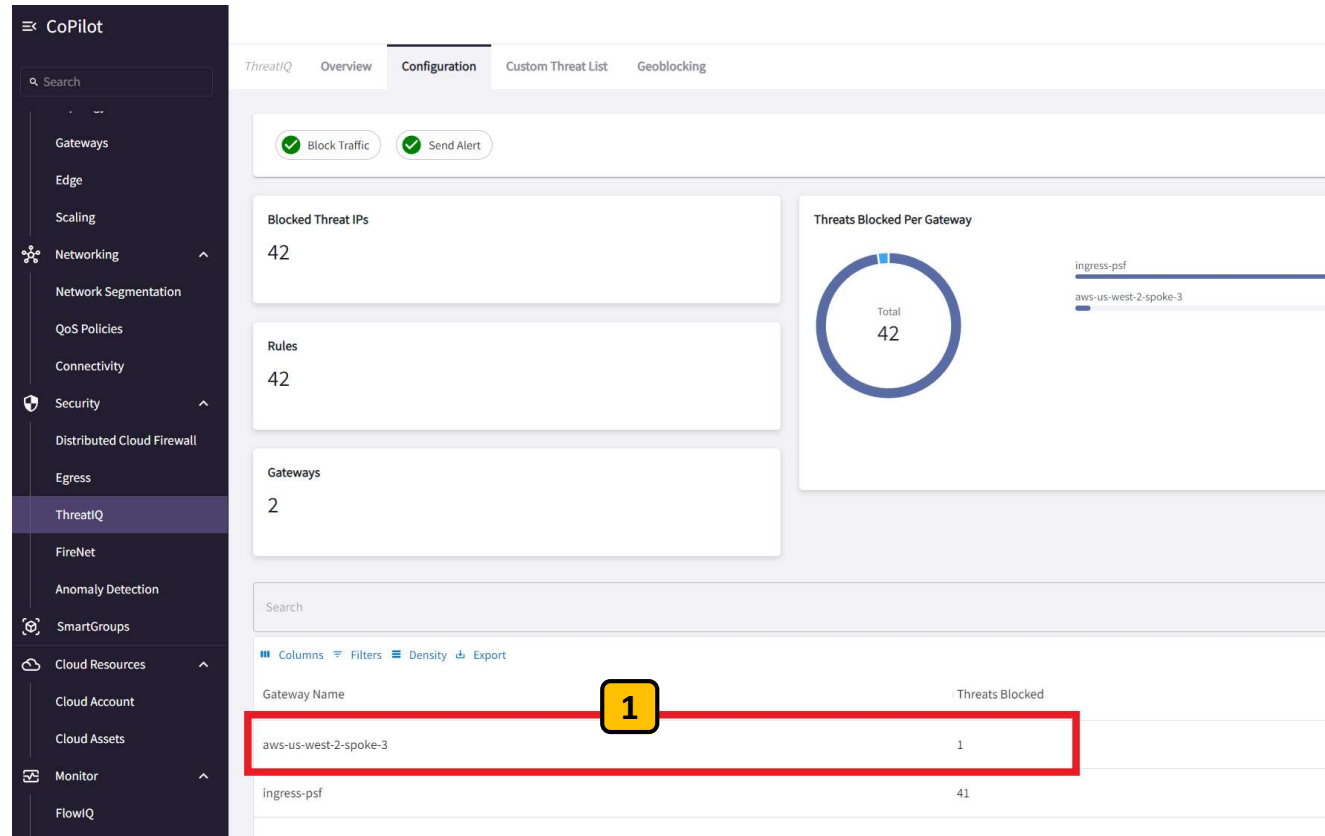


Lab 4: Threat Prevention: Step 4.12

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 Aviaatrix Gateway. **1**





Lab 4: Threat Prevention: Step 4.13

Observe and confirm threat blocking

Go back the Console session of instance SAP 3.

Reconnect to the threat IP using curl:

curl http://103.251.167.10 1

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 4.9

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 ~]$
```

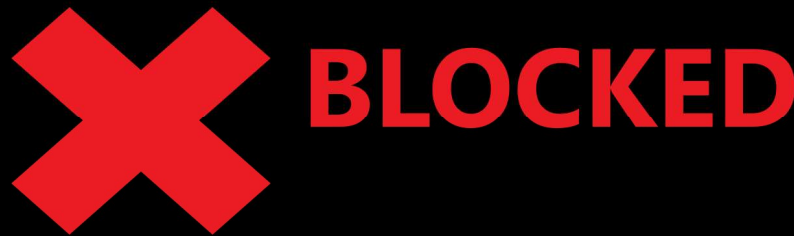
Lab 4: Threat Prevention: Step 4.14

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 ~]$
```

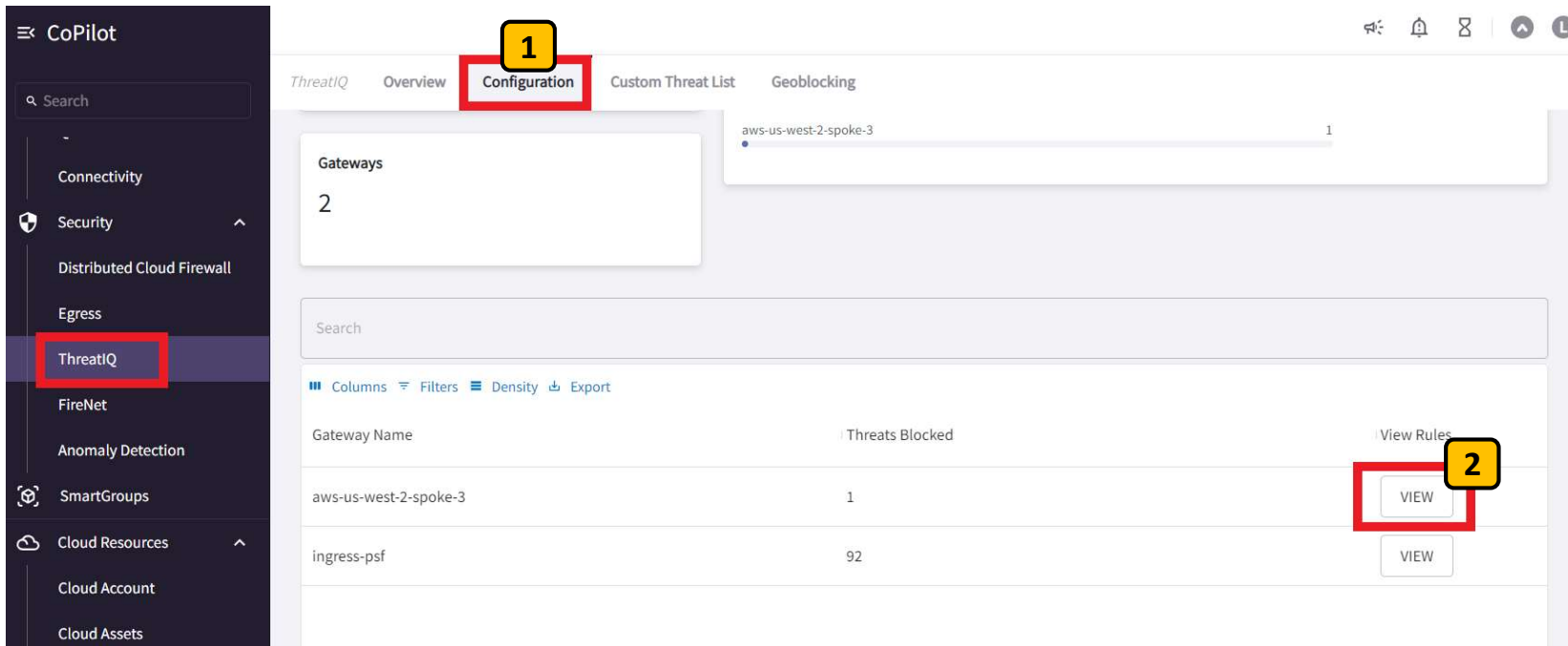


After a few minutes of you should
being to see your connections to
this threat IP fail. **1**

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

Lab 4: Threat Prevention: Step 4.15

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 camera icon), 'Cloud Resources' (with a cloud icon), 'Cloud Account', and 'Cloud Assets'. The main area 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 tabs, there's a 'Gateways' section with a list showing 'aws-us-west-2-spoke-3' and a count of '1'. Below that is a search bar and 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' column for the first row has a 'VIEW' button highlighted with a red box and a yellow '2' in a box.

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 4.16

Observe and confirm threat blocking

aws-us-west-2-spoke-3

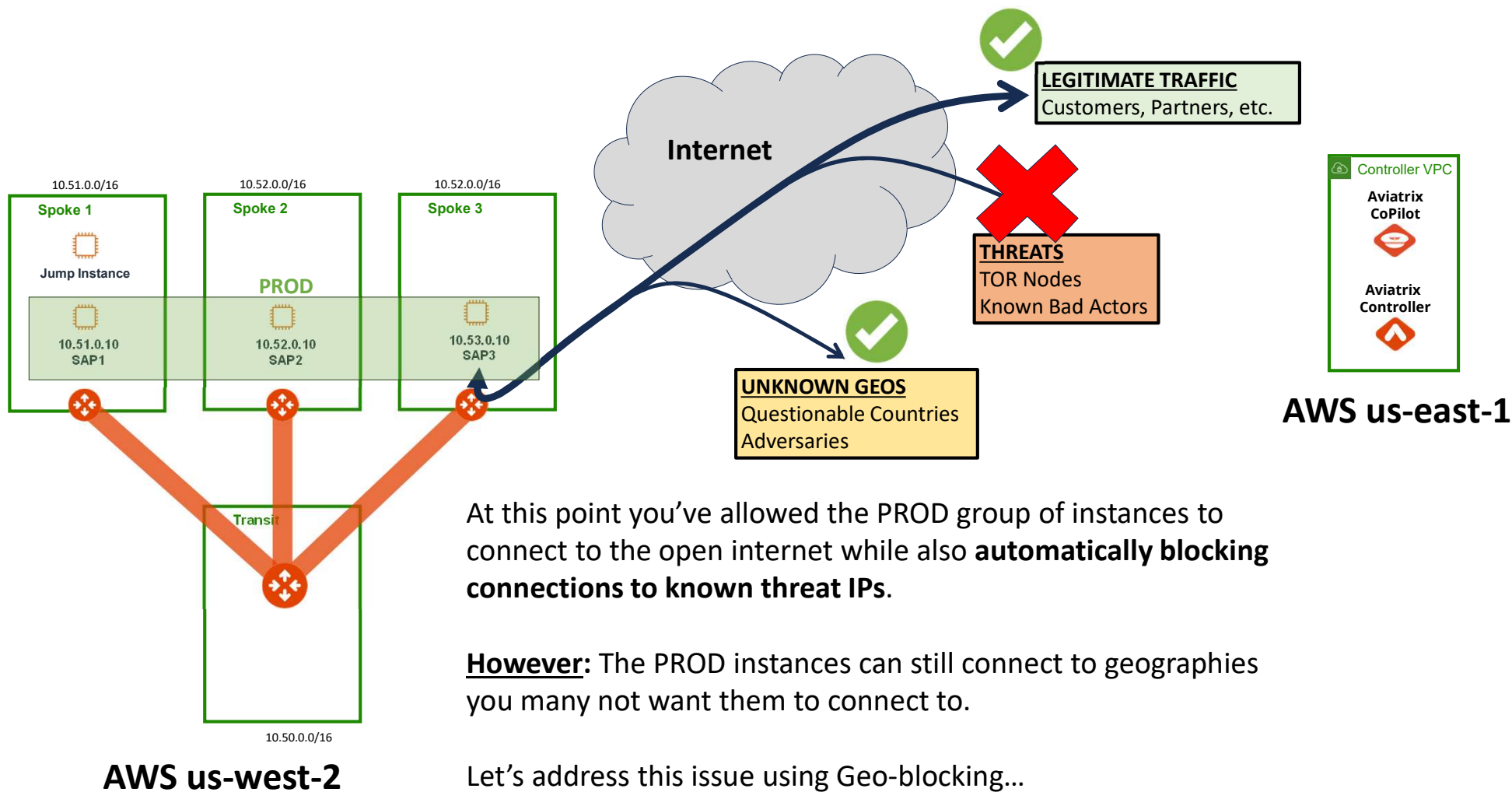
Source IP	Destination IP	Port	Protocol	Description	Action	Delete
103.251.167.10/32	n/a	ALL	ALL	ipset rule	force-drop	

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

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

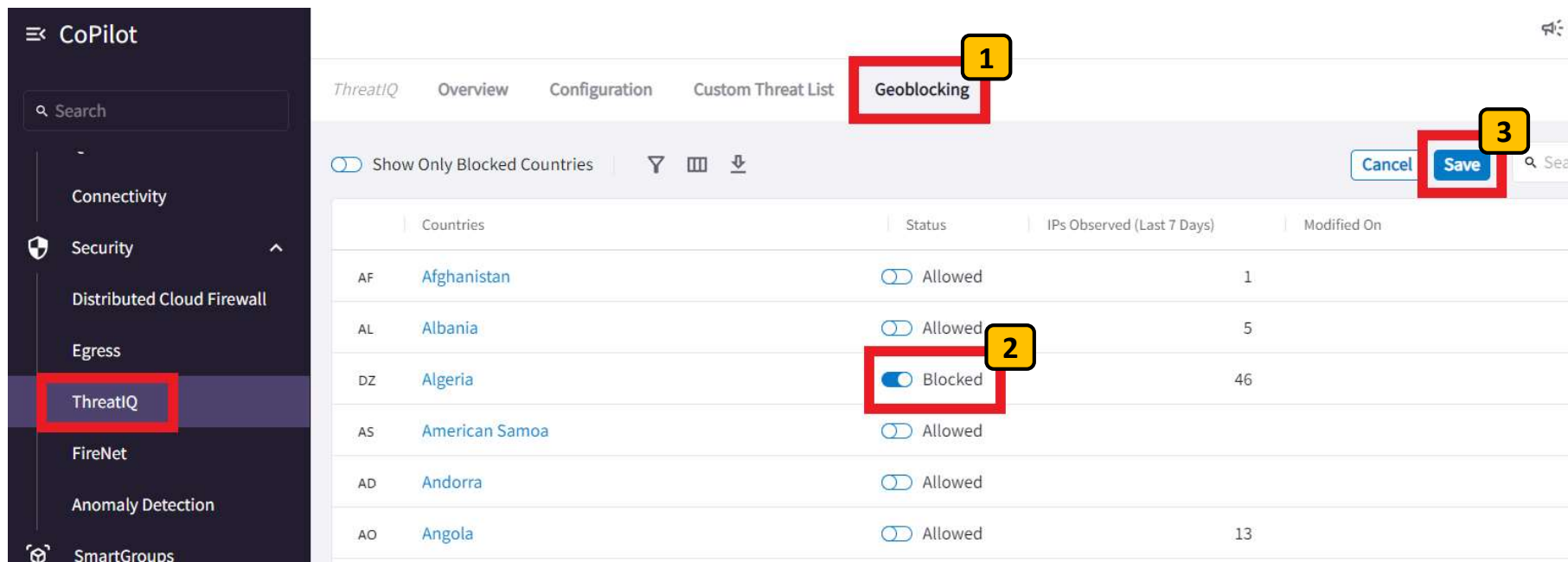
Nobody will need to page you to wake up and write a firewall rule at 3am!

Lab 4: Checkpoint 2: Current State



Lab 4: Threat Prevention: Step 4.17

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 Afghanistan	Allowed	1	
AL Albania	Allowed	5	
DZ Algeria	Blocked	46	
AS American Samoa	Allowed		
AD Andorra	Allowed		
AO Angola	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 4.18

Block geographies using Geoblocking

CoPilot

Search

Connectivity

Security

Distributed Cloud Firewall

Egress

ThreatIQ

FireNet

Anomaly Detection

ThreatIQ Overview Configuration Custom Threat List **Geoblocking**

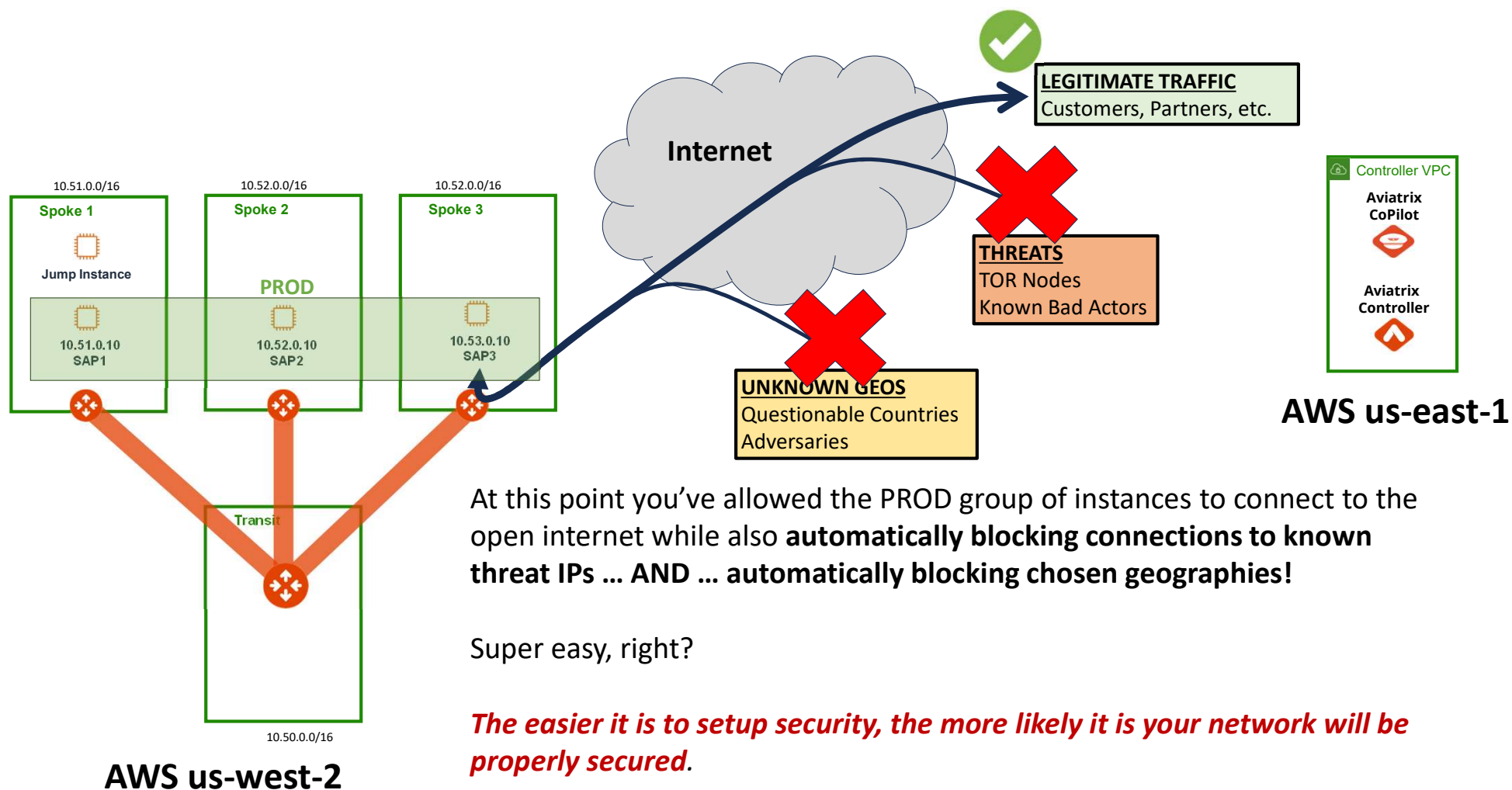
Show Only Blocked Countries

Search

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

