

Deployment Guide

Integrating BloxOne™ Threat Defense with AWS' Route 53

Table of Contents

Table of Contents	1
Introduction	2
Route VPC DNS Traffic to BloxOne Threat Defense	2
Prerequisites	2
Known Limitations	3
Before you get started	3
Configure an AWS VPC	3
Workflow	3
Create or a Identify VPC to Use	3
VPN or Direct connection	4
VPN or Direct Connect Connection External IP	4
NAT Gateway	5
Create a VPC	5
Configure Subnets	7
Create Internet Gateway	11
Create a NAT Gateway	13
Acquire the public IP from the NAT Gateway	21
Create a Route53 Outbound Endpoint	21
Create a Route53 Resolver Rule	25
Add an External Network to BloxOne	29
Add the External Network to a Security Policy	30
Test the Configuration	33
Add TIDE feeds to Route 53 Firewall Domain Lists	33
Prerequisites	34
Known Limitations	34
Workflow	34
Acquire a TIDE API Key	35
Create an AWS Route 53 DNS Firewall domain list	36
Create an AWS Route 53 DNS Firewall Rule Group and Associated Rule	39
Create an S3 Bucket and File	44
Acquire Information for a Lambda function	48
Acquire a TIDE API Call URL	48
Acquire an AWS Route 53 DNS Firewall domain list ID	51
Create a Lambda function	53
Create IAM Policies	59
Test the Lambda Script	68
Automate the script execution via EventBridge	73

Introduction

In addition to its role as a core connectivity technology, DNS offers powerful opportunities for improving your cybersecurity. This document will help you achieve optimal security and performance benefits by effectively integrating the Infoblox BloxOne™ Threat Defense solution with other DNS solutions, specifically the AWS VPC (Virtual Private Cloud) and the AWS Route 53 DNS Firewall.

BloxOne Threat Defense is a cloud-native solution that operates at the DNS level to see threats that other solutions do not and stops attacks earlier in the attack lifecycle. Through extensive automation and ecosystem integration options, it can uplift the effectiveness of the existing security stack, drive efficiencies in SecOps, secure digital and work-from-anywhere efforts and lower the total cost for cybersecurity.

To help you realize these benefits, this document will explain the simple process of routing AWS VPC DNS traffic to BloxOne Threat Defense to effectively protect the VPC while minimizing the need for additional security investments by maximizing the effectiveness of your existing tools.

It also provides guidance on leveraging the TIDE feature of BloxOne Threat Defense to manage threat intelligence and feed it to AWS Route 53 DNS Firewalls to optimize threat detection. TIDE allows you to choose your preferred sources of threat intelligence to be aggregated, normalized, and distributed to AWS DNS Firewalls. TIDE empowers you to identify and manage your own unique blend of threat feeds. Although this document will focus on using TIDE with the AWS DNS Firewall, it can also be used to uplift other solutions throughout your security stack to improve your defense, investigation, and response capabilities.

Route VPC DNS Traffic to BloxOne Threat Defense

This portion of the Deployment guide explains how to forward DNS traffic from an AWS VPC to the BloxOne Threat Defense Cloud.

Prerequisites

The following are prerequisites to route VPC DNS Traffic to BloxOne Threat Defense:

- BloxOne:
 - BloxOne Threat Defense Business Cloud or Advanced subscription
 - A CSP user account with BloxOne Threat Defense administrator permissions
- AWS:
 - A VPC with one of the following:
 - NAT Gateway
 - VPN

- Direct Connect connection
- AWS Security Group/ACL that allows DNS traffic to BloxOne Anycast IPs
 - For a full list of these Anycast IPs please see the Infoblox Documentation portal [here](#)

Note: this guide only covers how to configure a NAT Gateway and does not cover the configuration of an AWS VPN or Direct Connect Connection.

Known Limitations

When forwarding AWS VPC DNS traffic to BloxOne Threat Defense, using Route53's DNSSEC validation will break redirect functionality, BloxOne performs DNSSEC validation.

Before you get started

Configure an AWS VPC

This guide covers how to create and configure an AWS Virtual Private Cloud or VPC with a NAT Gateway. For detailed information on how to configure an AWS VPC please follow the AWS guide located here: <https://docs.aws.amazon.com/vpc/latest/userguide/vpc-getting-started.html>

Workflow

Note: This guide will cover how to configure a VPC with NAT gateway. Alternatively, you may skip section one of the guide if you have already configured a VPC with a NAT Gateway, VPN, or Direct Connect Connection.

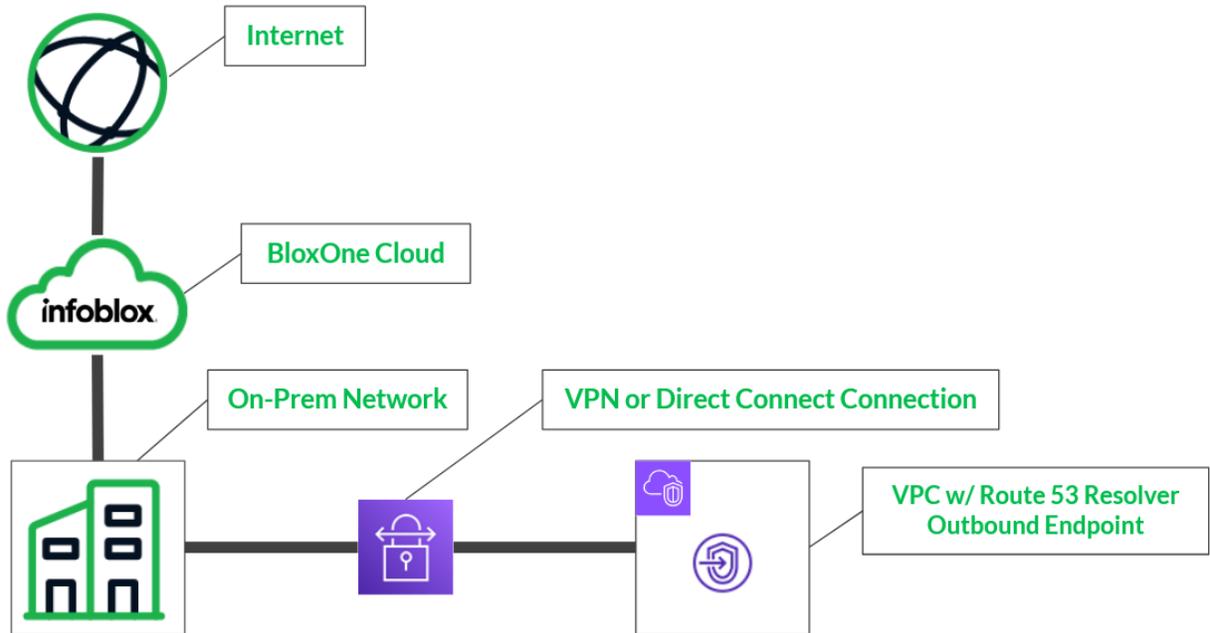
1. Create or identify VPC to use
 - a. (Optional) Create a NAT Gateway
2. Locate the required IP for BloxOne from one of the following:
 - a. VPN connection
 - b. NAT rule
 - c. AWS Direct Connect connection
3. Create a Route 53 Outbound Endpoint
4. Create a Route 53 Resolver rule
5. Create an External Networks that represent your VPC(s) in the Infoblox CSP

Create or a Identify VPC to Use

In order to forward DNS traffic to BloxOne, connectivity to BloxOne's anycast IPs from your VPC must be possible. A full list of the BloxOne anycast IPs are located [here](#). To enable your Outbound endpoint to connect to BloxOne, you will need a VPN, Direct Connect connection, or a NAT gateway. Additionally, you will need to know the public IP of the traffic that will be forwarded to BloxOne. This guide describes a basic topology of each configuration, contains links to AWS guides on how to configure them, and where to look for the public IP(s) needed for the BloxOne configuration. This guide provides an example of how to deploy a VPC with NAT Gateway.

VPN or Direct connection

To configure a VPN, please see the AWS documentation [here](#). To configure the Direct Connect connection, please see the AWS documentation [here](#). The following diagram visually represents the topology of these configurations:

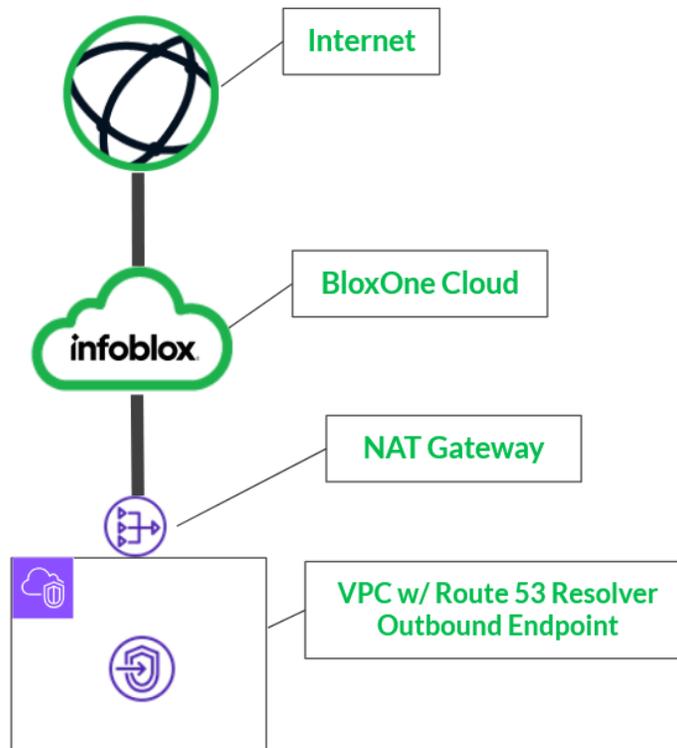


VPN or Direct Connect Connection External IP

Due to the variability of this configuration that can exist in this configuration this guide will not cover how to acquire the external IP of your network(s). Acquire the external IP of your on-premise network, which would be the external IP of the router that is routing for your on-premise network. Once located, store this IP for use later in this guide.

NAT Gateway

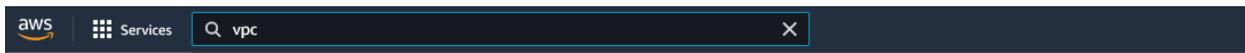
The following diagram visually represents the topology of this configuration:



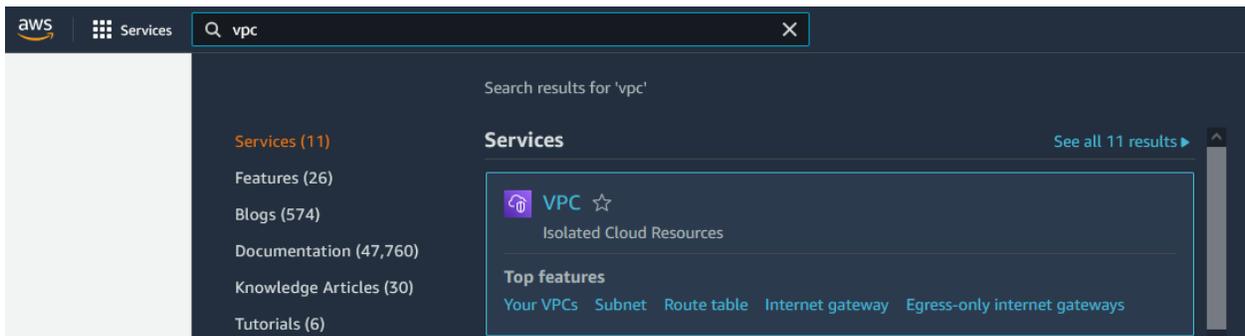
Create a VPC

This is an optional step to configure a VPC, if you have already identified a VPC that you intend to use with this integration, please skip this step. In order to create a VPC, perform the following steps:

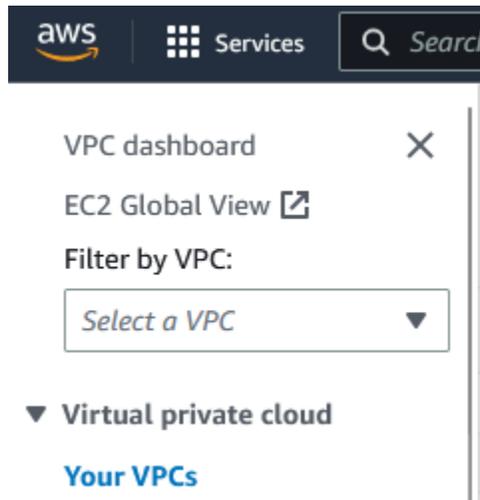
1. Log in to your AWS account. Once logged in, input **VPC** into the *search bar* located at the top of the AWS interface.



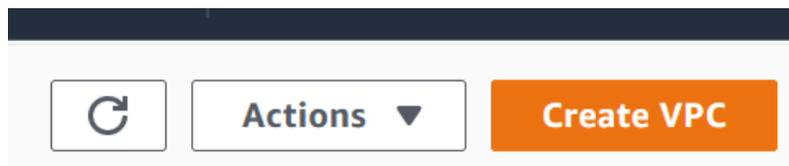
2. Click the text **VPC** in the list that is revealed.



3. On the VPC page, click **Your VPCs** in the left navigation panel.



4. On the top right of the *Your VPCs* page, click the **Create VPC** button.



5. On the Create VPC page, perform the following steps:
 - o In the VPC settings panel, input a **Name tag**.

Name tag - optional

Creates a tag with a key of 'Name' and a value that you specify.

- o Under the *IPv4 CIDR block* header, click the **IPv4 CIDR manual input** bubble.

IPv4 CIDR block [Info](#)

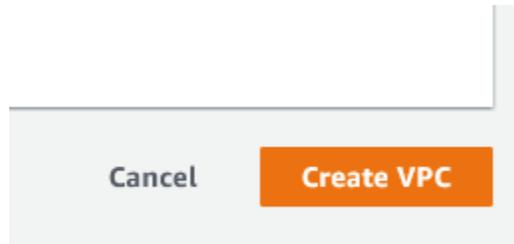
- IPv4 CIDR manual input
- IPAM-allocated IPv4 CIDR block - *new*

- Input an **IPv4 CIDR**. *note, ensure the CIDR chosen is suitable for at least 2 subnets.*

IPv4 CIDR

10.61.0.0/16

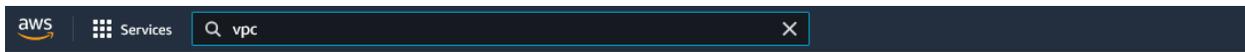
- Keep all other settings as their defaults, and click **Create VPC** to confirm the creation of the VPC.



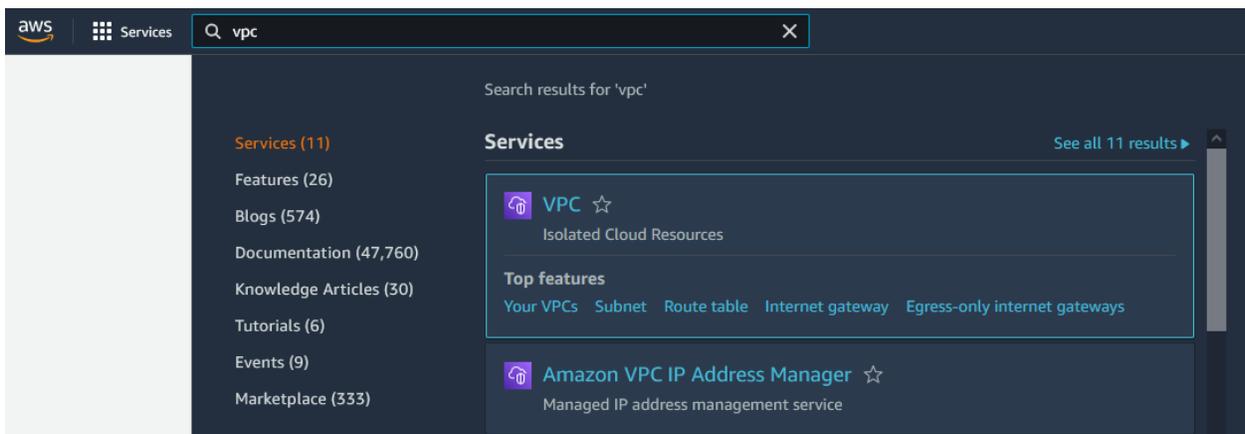
Configure Subnets

To configure a NAT gateway, you will need a Private and Public subnet. To create these subnets, perform the following steps:

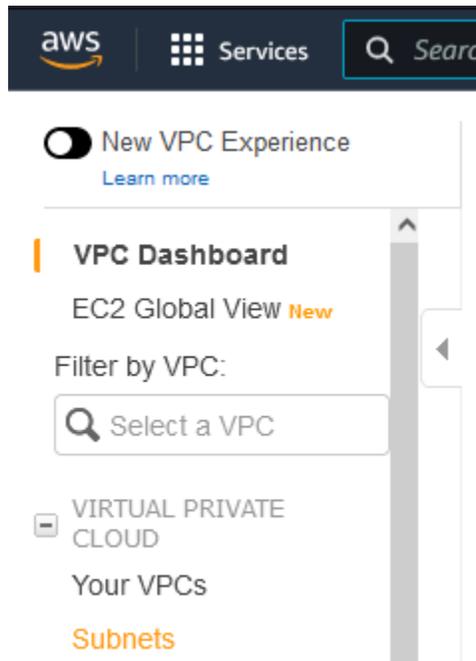
1. Log in to your AWS account. Once logged in, input **VPC** into the *search bar* located at the top of the AWS interface.



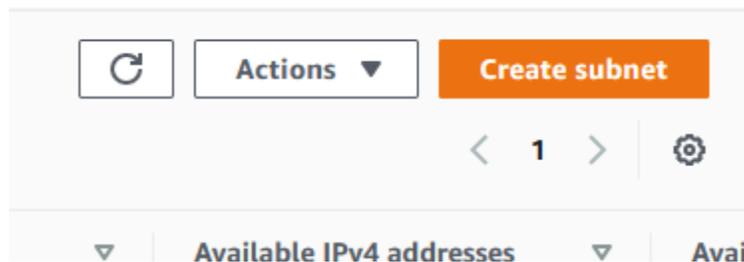
2. Click the text **VPC** in the list that is revealed.



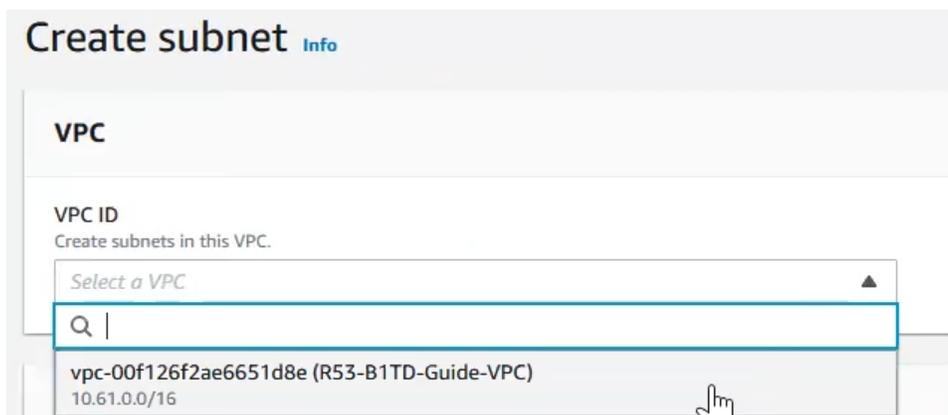
3. In the left navigation panel of the VPC page, click **Subnets**.



4. Click the **Create subnet** button located on the top right of the Subnets page. *Note that this will be a public subnet intended for external traffic via the NAT Gateway.*



5. On the *Create Subnet* page perform the following steps:
 - o Select the **VPC** that you would like to associate with this Subnet via the *VPC ID* dropdown menu.



- In the Subnet settings panel that is revealed, input a **Subnet name**.

Subnet settings

Specify the CIDR blocks and Availability Zone for the subnet.

Subnet 1 of 1

Subnet name

Create a tag with a key of 'Name' and a value that you specify.

R53-B1TD-Guide-Pub-Subnet

The name can be up to 256 characters long.

- Select an **Availability Zone** via the Availability Zone dropdown menu.

Availability Zone [Info](#)

Choose the zone in which your subnet will reside, or let Amazon choose one for you.

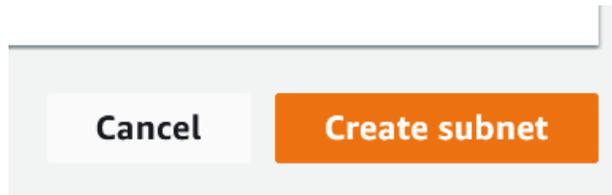
US East (N. Virginia) / us-east-1a

- Input an IPv4 CIDR via the **IPv4 CIDR block**. *Note pick a range that allows remaining IPs in the VPC as a second Subnet will be created later in this guide.*

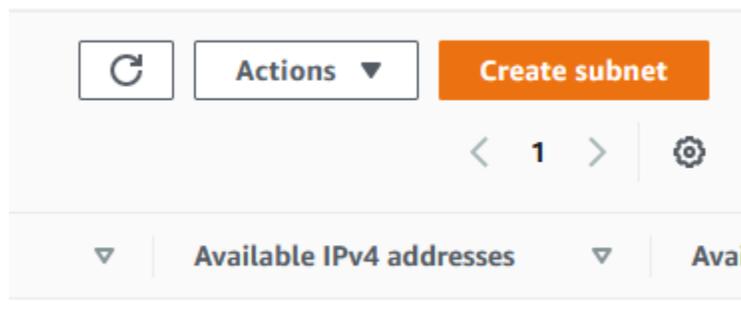
IPv4 CIDR block [Info](#)

10.61.10.0/24

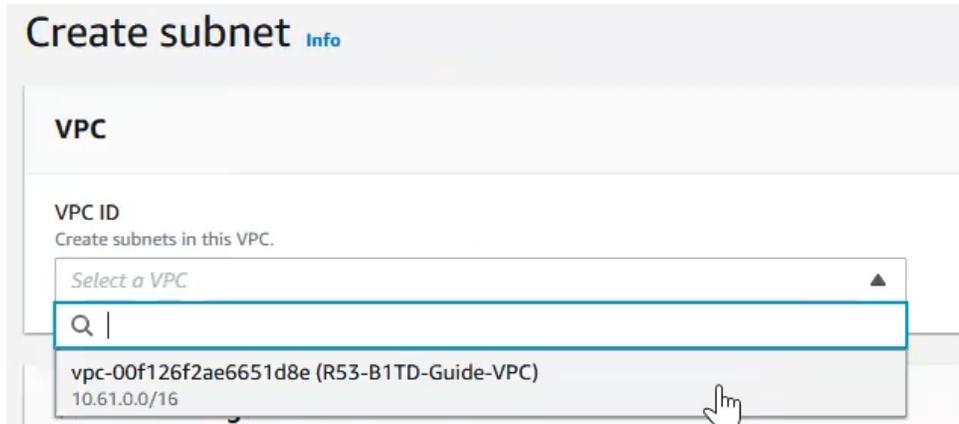
- Click **Create subnet** to confirm the creation of the subnet.



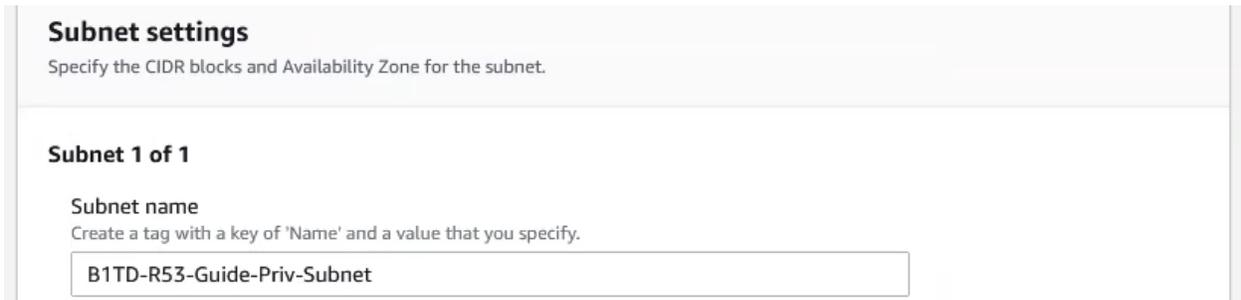
6. Click the **Create subnet** button located on the top right of the Subnets page. *Note that this will be a private subnet intended for internal traffic.*



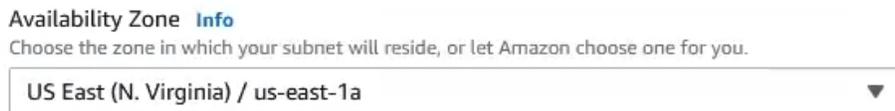
7. On the *Create Subnet* page perform the following steps:
 - o Select the same **VPC** that you selected with the previously created Subnet via the *VPC ID* dropdown menu.



- o In the Subnet settings panel that is revealed, input a **Subnet name**.



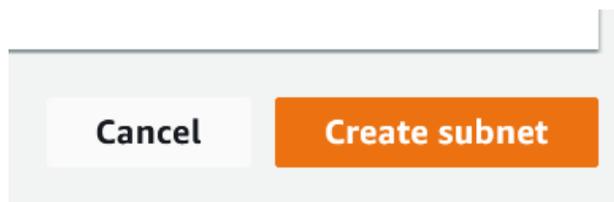
- o Select an **Availability Zone** via the Availability Zone dropdown menu.



- o Input an IPv4 CIDR via the **IPv4 CIDR block**. Note pick a range that allows remaining IPs in the VPC as a second Subnet will be created later in this guide.



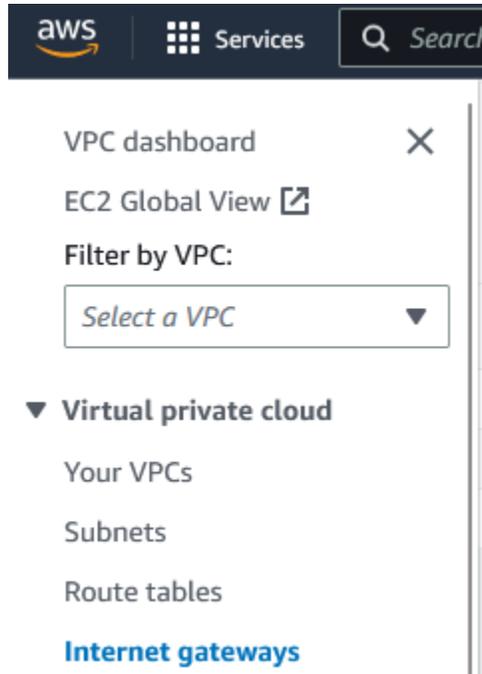
- o Click **Create subnet** to confirm the creation of the subnet.



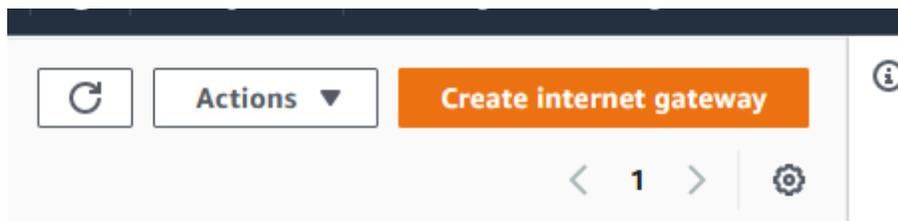
Create Internet Gateway

In addition to the previous subnets, an Internet Gateway is also required to create a NAT Gateway. In order to create an Internet Gateway, perform the following steps:

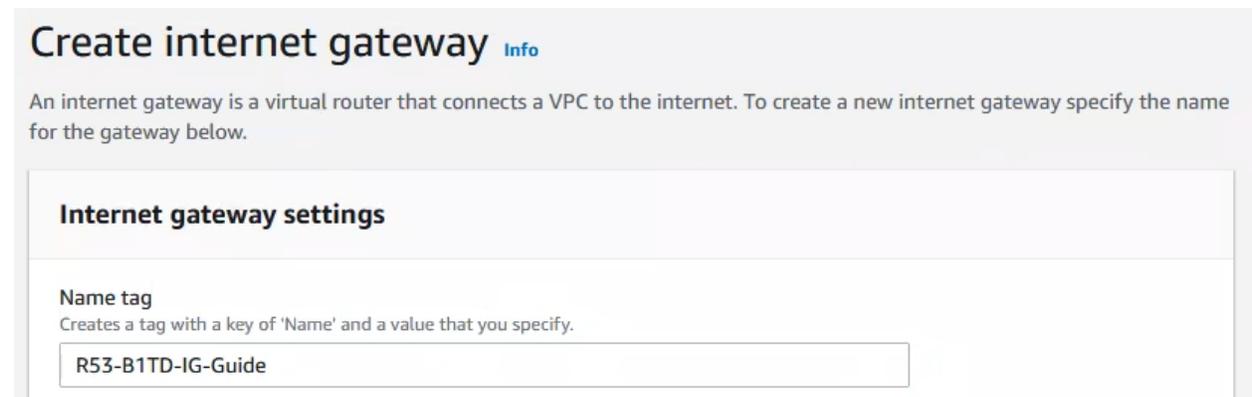
1. In the left navigation panel of the Subnets page, click **Internet Gateways**.



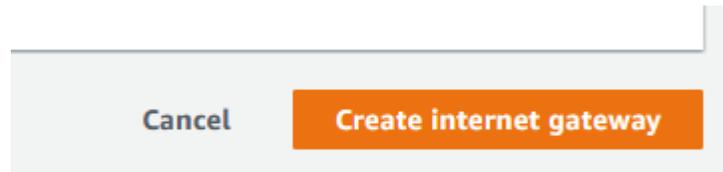
2. On the **Internet Gateways** page, click **Create internet gateway**.



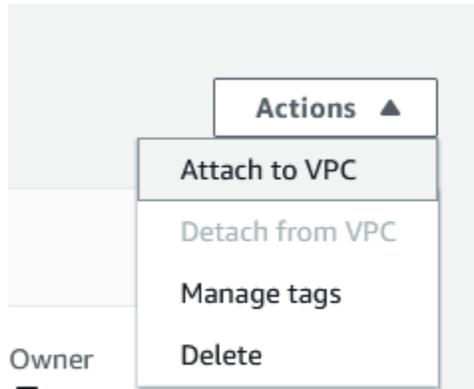
3. On the Create internet gateway page, input a **Name tag**.



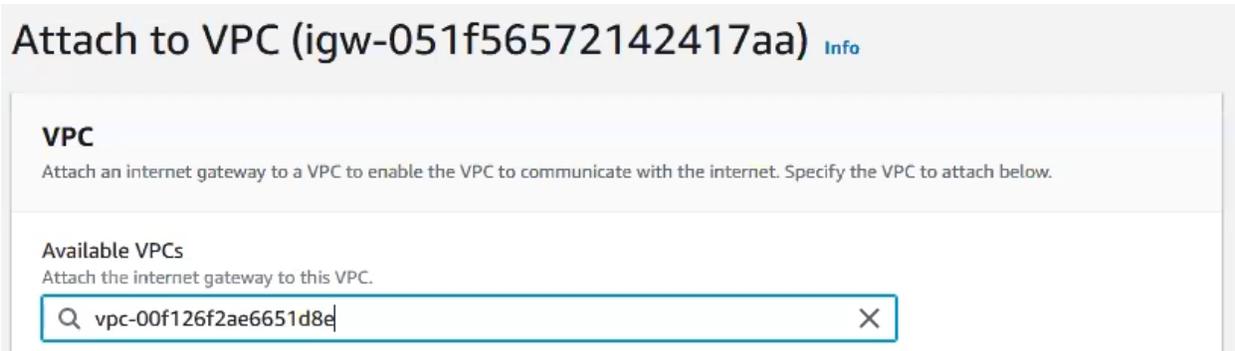
- Click **Create internet gateway** to confirm the creation of the Internet Gateway.



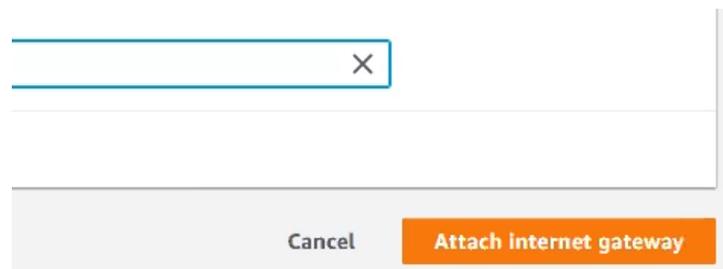
- Once on the newly created Internet Gateway's page, click the **Actions** button. Then, click **Attach to VPC**.



- On the *Attach to VPC* page, select the VPC you intend to use with this integration via the **Available VPCs** dropdown.



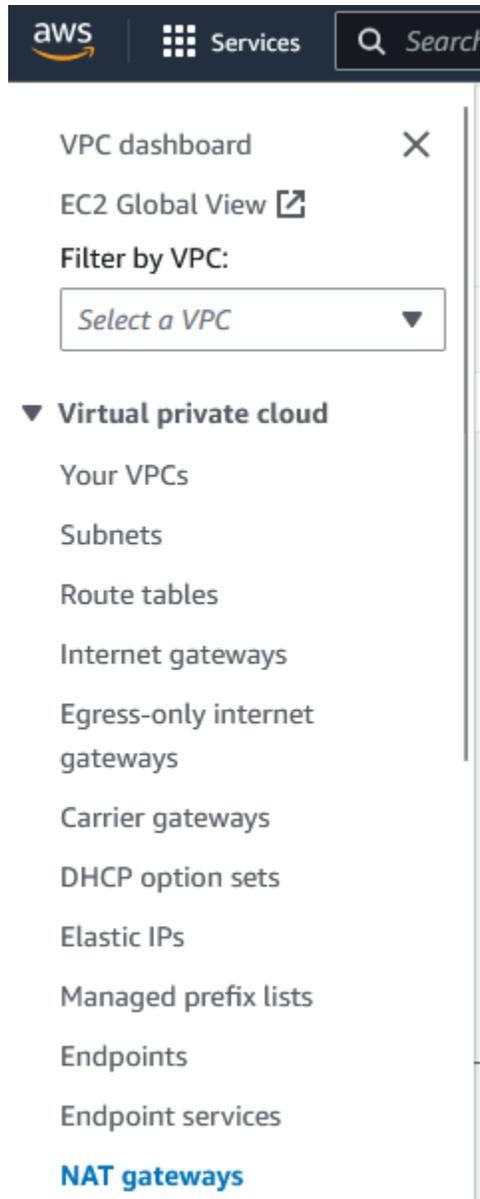
- Click the **Attach internet gateway** button to confirm the operation.



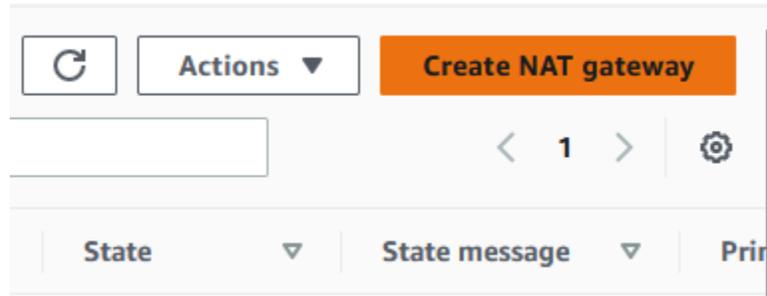
Create a NAT Gateway

In order to create NAT Gateway, perform the following steps:

1. In the left navigation panel of the Internet Gateways page, click **NAT Gateways**.

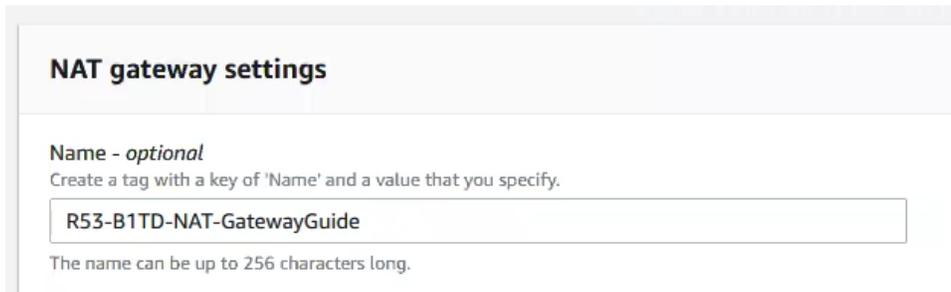


- On the NAT Gateways page, click **Create NAT gateway**.



- On the NAT gateway settings page perform the following steps:

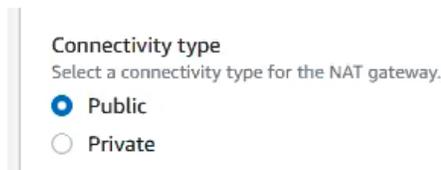
- Input a **Name**.



- Select the **Public subnet** that was created earlier in this guide via the **Subnet** dropdown.



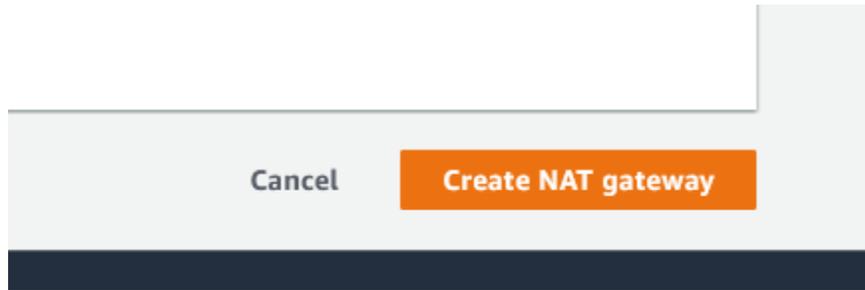
- Under the Connectivity type header, click the **Public** bubble.



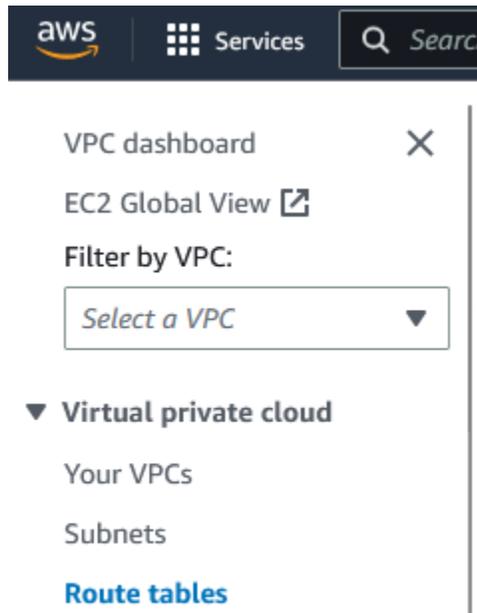
- Select an existing Elastic IP via the **Elastic IP allocation ID** dropdown or allocate a new Elastic IP via the **Allocate Elastic IP** button.



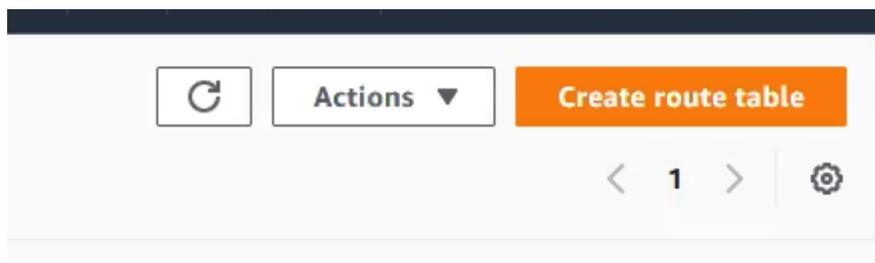
- Click **Create NAT gateway** to confirm the creation of the NAT gateway.



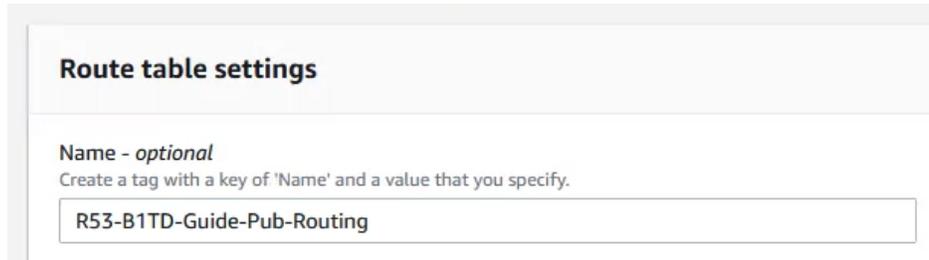
4. In the left navigation panel of the Nat Gateways page, click **Route Tables**.



5. In the top right of the *Route tables* page, click the **Create route table** button. Note that this routing table will be used for routing between the public subnet and the Internet Gateway created earlier in this guide.



6. On the Create Route table page, give the Route table a **Name**.



Route table settings

Name - *optional*
Create a tag with a key of 'Name' and a value that you specify.

R53-B1TD-Guide-Pub-Routing

7. Then, assign the **VPC** that you created the subnets in earlier in this guide.



VPC
The VPC to use for this route table.

vpc-00f126f2ae6651d8e (R53-B1TD-Guide-VPC)

8. Then, click the **Create route table** to confirm the creation of the route table.



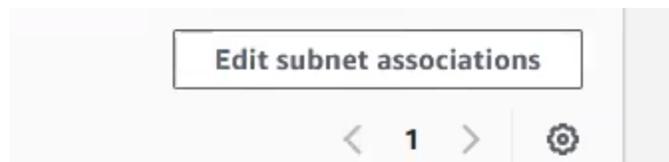
Cancel Create route table

9. In the newly created *Route table*, click the **Subnet associations** tab located near the bottom of the page.



Routes Subnet associations Edge associations

10. In the *Explicit subnet associations* panel, click the **Edit subnet associations** button.



Edit subnet associations

< 1 > ⚙

11. In the **Available subnets** panel, select the public subnet that was created earlier in this guide.



Available subnets (1/2)

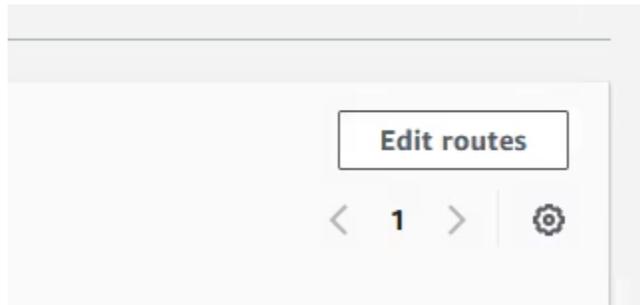
Filter subnet associations

<input type="checkbox"/>	Name	Subnet ID
<input checked="" type="checkbox"/>	R53-B1TD-Guide-Pub-Subnet	subnet-0ee4c30837f6d21be
<input type="checkbox"/>	B1TD-R53-Guide-Priv-Subnet	subnet-019b593ee4da75f07

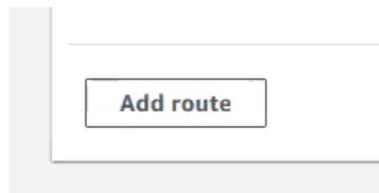
12. Click **Save association** to confirm the subnet association.



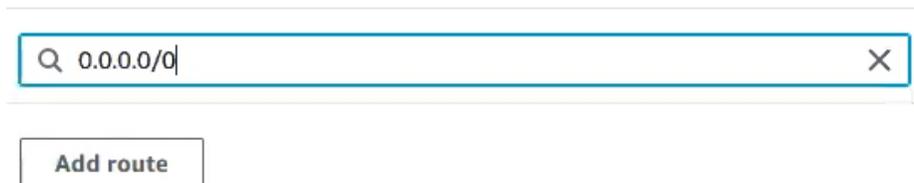
13. On the Route table's primary page, click **Edit routes** located in the Routes panel.



14. On the Edit routes page, click the **Add route** button.



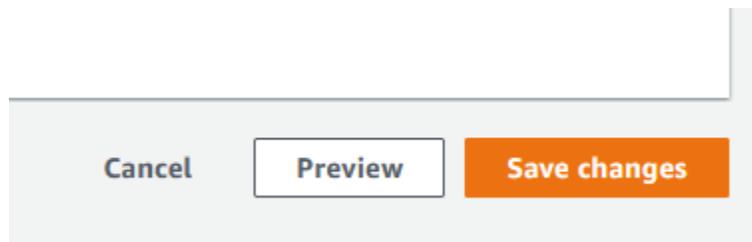
15. In the new route's *Destination* textbox, input the wildcard address **0.0.0.0/0**.



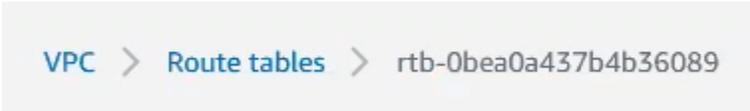
16. In the new route's *Target* textbox, input the ID of the **Internet Gateway** that was created earlier in this guide.



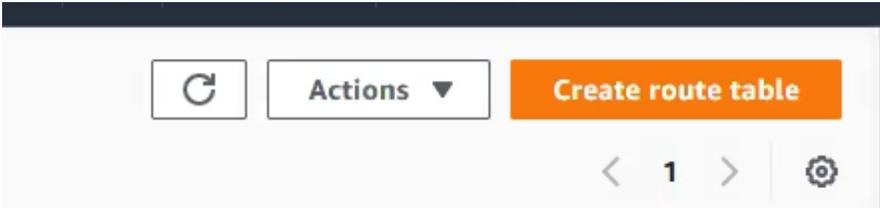
17. Click the **Save changes** button to confirm the changes to the routing table.



18. On the top of the *Route table's* page, click **Route tables** to return to the Route tables page.



19. In the top right of the *Route tables* page, click the **Create route table** button. *Note that this routing table will be used for routing between the subnet and the NAT Gateway created earlier in this guide.*



20. On the Create Route table page, give the Route table a **Name**.

Name - optional
Create a tag with a key of 'Name' and a value that you specify.

21. Then, assign the VPC that you created the subnets in on *pages 6-8*.

VPC
The VPC to use for this route table.

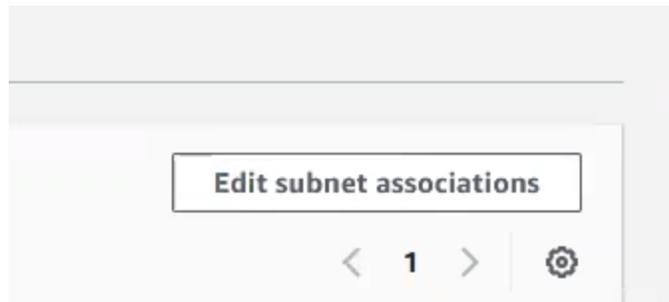
22. Then, click the **Create route table** to confirm the creation of the route table.



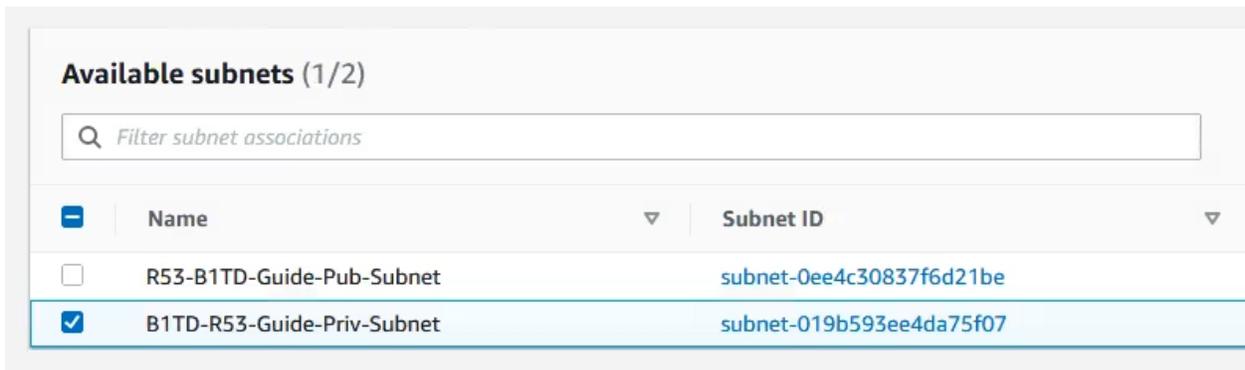
23. In the newly created *Route table*, click the **Subnet associations** tab located near the bottom of the page.



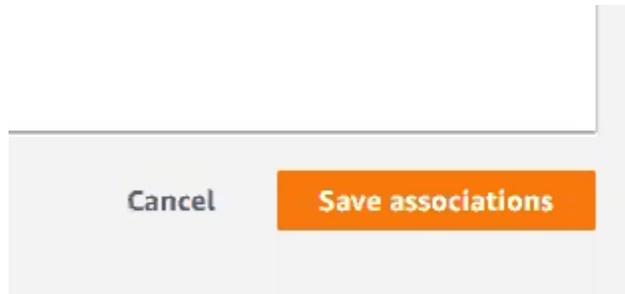
24. In the *Explicit subnet associations* panel, click the **Edit subnet associations** button.



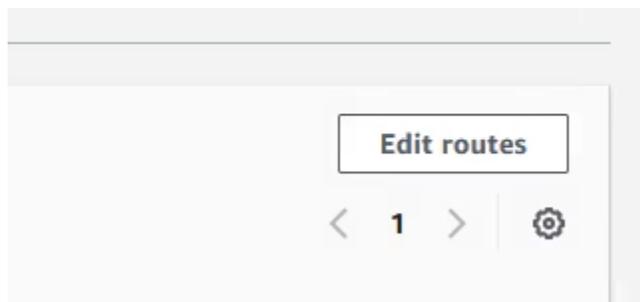
25. In the **Available subnets** panel, select the private subnet that was created earlier in the guide.



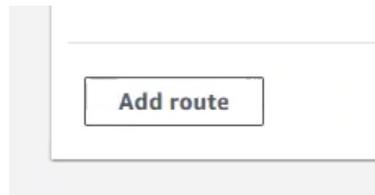
26. Click **Save association** to confirm the subnet association.



27. On the Route table's primary page, click **Edit routes** located in the Routes panel.



28. On the Edit routes page, click the **Add route** button.



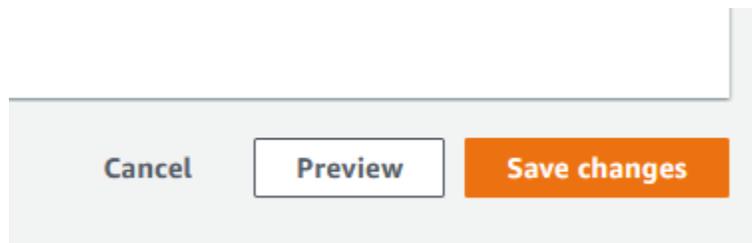
29. In the new route's *Destination* textbox, input the wildcard address **0.0.0.0/0**.

A screenshot of a search-style input field with a magnifying glass icon on the left and an 'X' icon on the right. The text "0.0.0.0/0" is entered into the field.

30. In the new route's *Target* textbox, input the ID of the **NAT Gateway** that was created earlier in this guide.

A screenshot of a search-style input field with a magnifying glass icon on the left and an 'X' icon on the right. The text "nat-0ce1197724a3adbdf" is entered into the field.

31. Click the **Save changes** button to confirm the changes to the routing table.



32. In the **Available subnets** panel, select the private subnet that was created on *pages 10-11*.

Available subnets (1/2)		
<input type="text" value="Filter subnet associations"/>		
<input type="checkbox"/>	Name	Subnet ID
<input type="checkbox"/>	R53-B1TD-Guide-Pub-Subnet	subnet-0ee4c30837f6d21be
<input checked="" type="checkbox"/>	B1TD-R53-Guide-Priv-Subnet	subnet-019b593ee4da75f07

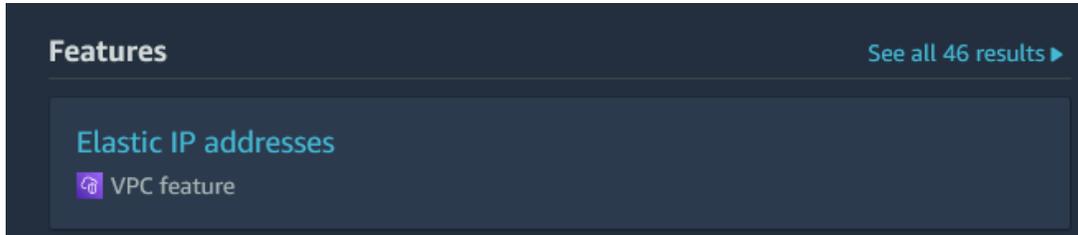
Acquire the public IP from the NAT Gateway

To acquire the external IP of a NAT Gateway, perform the following steps:

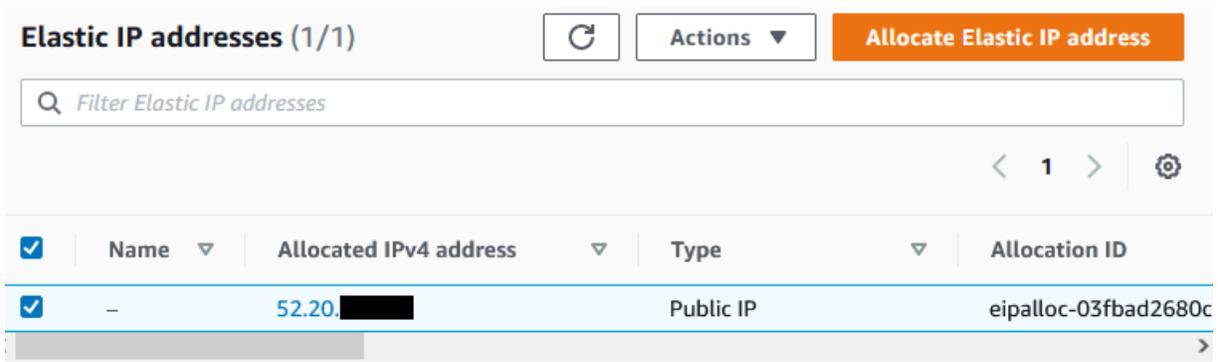
1. In the *AWS Management Console*, input **Elastic IP** into the search bar.



2. Click the text **Elastic IP addresses** in the list that is revealed.



3. Once on the Elastic IP addresses page, locate the Elastic IP of the NAT Gateway you've configured for your VPC. Copy and **save** this IP to another location for use later. *Note: the IP will be located in the **Allocated IPv4 address** column.*



Create a Route53 Outbound Endpoint

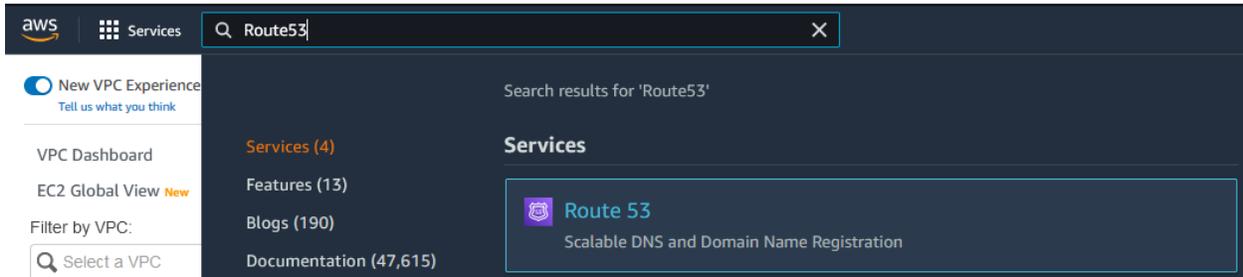
In order to forward DNS traffic from an AWS VPC, you must create an Outbound Endpoint. An outbound endpoint is an AWS feature that allows DNS traffic from a VPC to be forwarded to an IP or Domain. To create an Outbound Endpoint, perform the following steps:

1. Log in to your AWS account. Once logged in, input **Route53** into the *search bar* located at the top of the AWS interface.

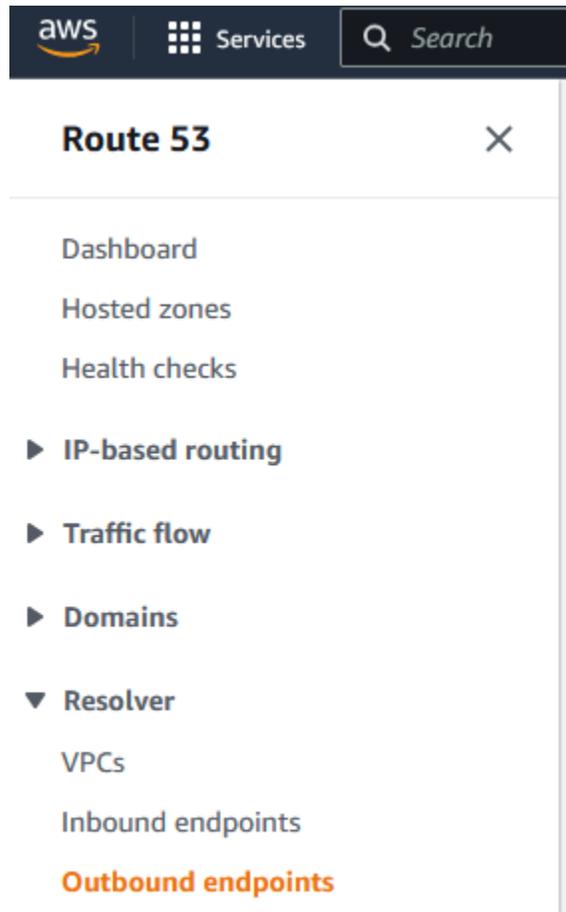


AWS Management Console

2. Click the text **Route 53** in the list that is revealed.



3. In the *Route 53* navigation pane, click **Outbound endpoints** located under the *Resolver* header.



4. On the *Outbound endpoints* page, click **Create outbound endpoint**.



5. On the *Create outbound endpoint* page, input the following data:
- Give the Outbound Endpoint a **Name**.

General settings for outbound endpoint

Endpoint name
A friendly name lets you easily find your endpoint on the dashboard.

The endpoint name can have up to 64 characters. Valid characters: a-z, A-Z, 0-9, space, _ (underscore), and - (hyphen)

- Select the **VPC** you would like to associate with the Outbound Endpoint via the dropdown.

VPC in the Region: us-east-1 (N. Virginia) [Info](#)

All outbound DNS queries will flow through this VPC on the way from other VPCs. You can't change this value after you create an endpoint.

- Select the **Security group** you would like to associate with this Outbound Endpoint by using the dropdown.

Security group for this endpoint [Info](#)

A security group controls access to this VPC. The security group that you choose must include one or more outbound rules. You can't change this value after you create an endpoint.

- Select **IPv4** as the Endpoint Type via the dropdown.

Endpoint Type

Route 53 Resolver endpoints support IPv4, IPv6, and Dual-stack IP addresses. For a Dual-stack connection one endpoint can use both IPv4 and IPv6 addresses to connect to a VPC.

- Under the *IP address #1* header, select the **Availability Zone** you would like to use for this Outbound Endpoint. *Note that this is the IP clients will send DNS requests to, any additional IP addresses entered will act as redundant to the first one to improve availability.*

▼ IP address #1 Remove IP address

Availability Zone [Info](#)
The Availability Zone that you choose for outbound DNS queries must be configured with a subnet.

- Select the private **Subnet** associated with the Availability zone.

Subnet Info

The subnet that you choose must have an available IP address. Only IPv4 addresses are supported.

subnet-01e5ce32d0b7ac987 (B1TD-R53-Guide-Subnet) (10.6... ▼

- Choose an **IP address** for the Outbound Endpoint. You may choose to allow AWS to choose one automatically, or input one manually.

IP address Info

For outbound DNS queries, you can either let the service choose an IP address for you from the available IP addresses in the subnet, or you can specify the IP address yourself.

- Use an IP address that is selected automatically
- Use an IP address that you specify

- Under the *IP address #2* header, select the **Availability Zone** you would like to use for this Outbound Endpoint. *Note that this is the IP clients will send DNS requests to.*

▼ **IP address #2**

Remove IP address

Availability Zone Info

The Availability Zone that you choose for outbound DNS queries must be configured with a subnet.

us-east-1e ▼

- Select the private **Subnet** associated with the Availability zone.

Subnet Info

The subnet that you choose must have an available IP address. Only IPv4 addresses are supported.

subnet-01e5ce32d0b7ac987 (B1TD-R53-Guide-Subnet) (10.6... ▼

- Choose an **IP address** for the Outbound Endpoint. You may choose to allow AWS to choose one automatically, or input one manually.

IP address Info

For outbound DNS queries, you can either let the service choose an IP address for you from the available IP addresses in the subnet, or you can specify the IP address yourself.

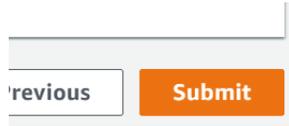
- Use an IP address that is selected automatically
- Use an IP address that you specify

- (Optional) If desired, input additional IP addresses via the **Add another IP address** button.

- Use an IP address that you specify

Add another IP address

- (Optional) Input **Tags** if desired.
- Click **Submit** to finish the creation of the Outbound Endpoint.



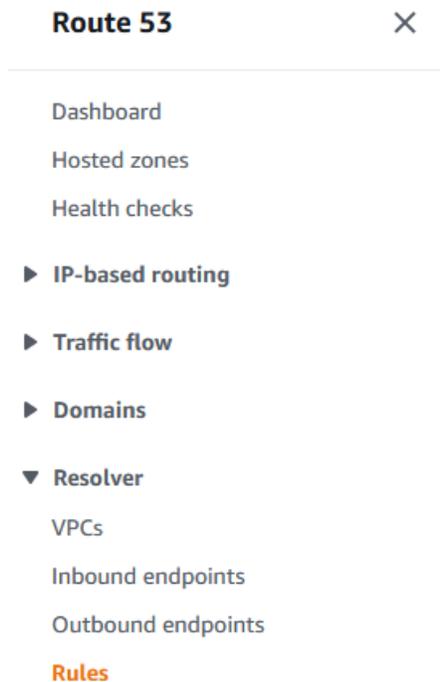
- If the creation of the Outbound Endpoint was successful, you will now see the newly created outbound endpoint on the Outbound endpoints page.

Outbound endpoints (1) Info					
		View details	Edit	Delete	Create outbound endpoint
<input type="text"/>					< 1 > ⚙️
ID	Name	Status	Host VPC	IP addresses	
○ rslvr-out-d457d2	R53-B1TD-Guide-Endpoint	✔️ Operational	vpc-04b2cd3b...	2	

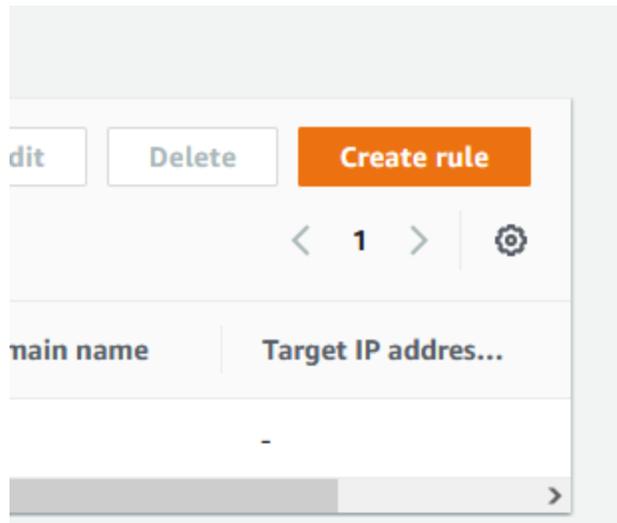
Create a Route53 Resolver Rule

In order to forward traffic to BloxOne Threat Defense you must configure a resolver rule which allows Route 53 to forward traffic to IP addresses defined within. To create a Resolver rule, perform the following steps:

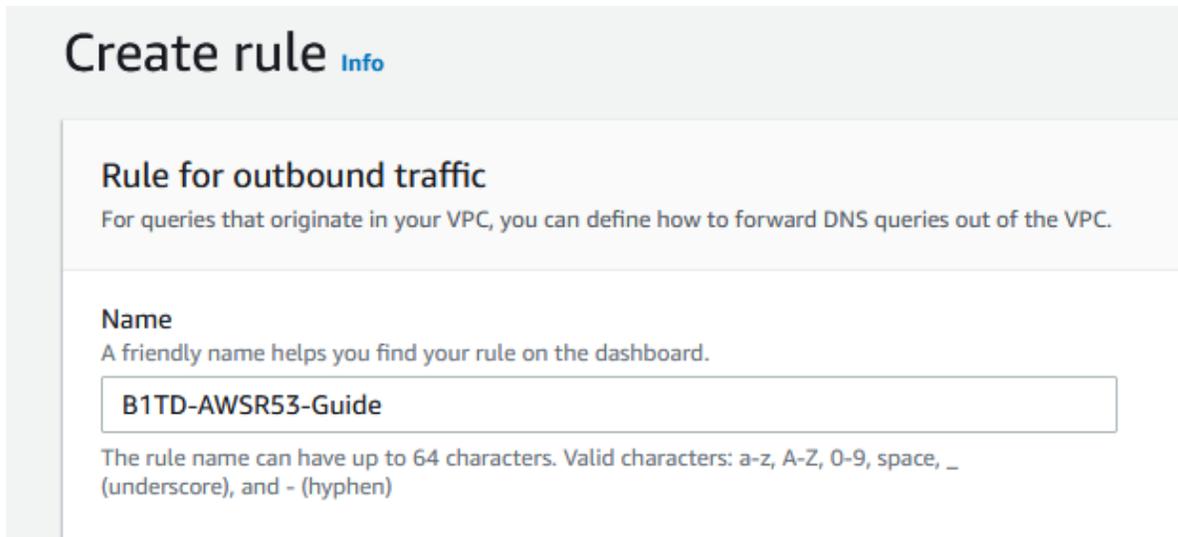
1. In the *Route 53 navigation panel*, click **Rules** located under the *Resolver* header.



2. On the *Rules* page, click **Create rule**.



3. Configure the new rule:
 - o Give the rule a **Name**.



- o Set the *Rule type* as **Forward**.

Rule type [Info](#)

Choose **Forward** to forward DNS queries to the IP addresses that you specify in **Target IP addresses** section near the bottom of this page. Choose **System** to have Resolver handle queries for a specified subdomain. You can't change this value after you create a rule.

Forward ▼

- In the *Domain name* text field input the character '.' without quotations.

Domain name Info

DNS queries for this domain name are forwarded to the IP address that you specify in the **Target IP addresses** section near the bottom of the page. If a query matches multiple rules (example.com and www.example.com), outbound DNS queries are routed using the rule that contains the most specific domain name (www.example.com). You can't change this value after you create a rule.

- Select any **VPC(s)** that you would like this rule to apply to via the dropdown menu located under the *VPCs that use this rule* header.

VPCs that use this rule - optional Info

You can associate this rule with as many VPCs as you want. To remove a VPC, choose the X for that VPC.

Choose VPC ▼ ↻

vpc-04b2cd3b612959c0a (VPC-R53-B1TD-Guide) X

- Select the **Outbound endpoint** that was created earlier via the dropdown menu.

Outbound endpoint Info

Resolver uses the outbound endpoint to route DNS queries to the IP addresses that you specify in the **Target IP addresses** section near the bottom of this page.

rslvr-out-d457d27664bd46a38 (R53-B1TD-Guide-Endpoint) ▼

- In the *First Target IP address text field*, input the address **52.119.40.100**. Additionally, input **53** in the *Port* text field

Target IP addresses Info

DNS queries are forwarded to the following IPv4 addresses:

IP address	Port	
<input type="text" value="52.119.40.100"/>	<input type="text" value="53"/>	<input type="button" value="Remove target"/>
<input type="button" value="Add target"/>		

- Click **Add target** to input another IP address.

- In the second Target IP addresses field input the IP **103.80.5.100**. Additionally, input **53** in the *Port* text field

- Click **Submit** to confirm the creation of the rule.

- If the creation of the rule was successful, you will now see the new rule in the list of *Rules*.

Rules (2) [Info](#) [Details](#) [Edit](#) [Delete](#) [Create rule](#)

🔍

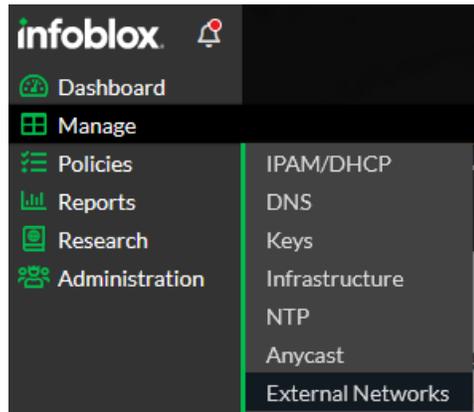
< 1 > ⚙️

	Name	ID	Status	Outbound c
○	Internet Resolver	rslvr-autodefined-rr-internet-resolver	✔️ Compl...	-
○	B1TD-AWSR53-Guide	rslvr-rr-3c52779069404ddf9	✔️ Compl...	rslvr-out-d4

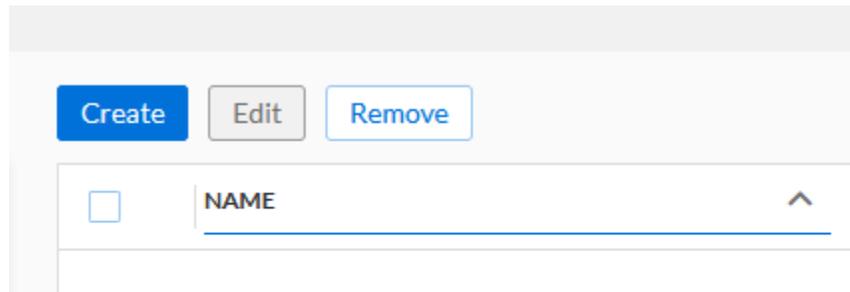
Add an External Network to BloxOne

In order for BloxOne to protect your network, you must input an External Network into your CSP. To do this, perform the following steps.

1. Log in to the Infoblox CSP. Once logged in, navigate to the External Networks page. Highlight Manage, then click on **External Networks** in the list that is revealed.



2. Create a new External Network. Click **Create** located on the top left of the External Networks page.



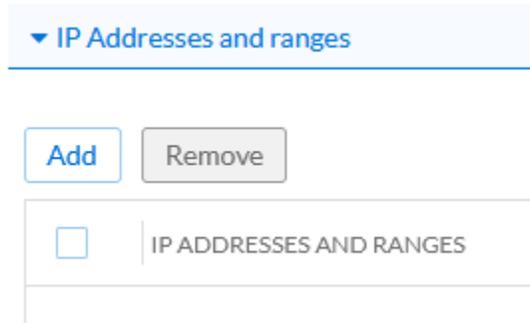
3. In the *Add New Network Panel* that is revealed, input the following:
 - Give the new External Network a **Name**.

*Network Name

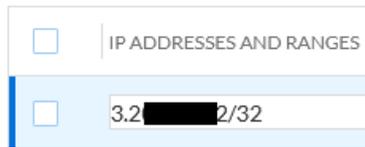
- (Optional) If desired, input a **Description**.

Description

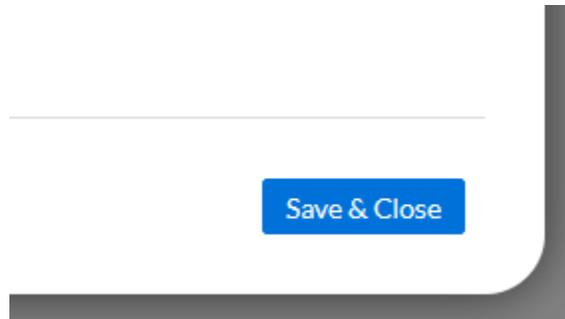
- Click the **Add** button located in the *IP Addresses and ranges* section.



- Input the **External IP** acquired from your NAT Gateway, or On-prem network.



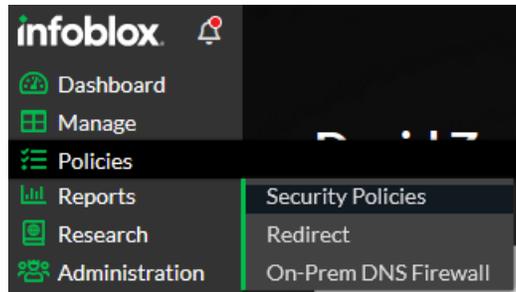
- Click **Save & Close** to confirm the creation of the new External Network.



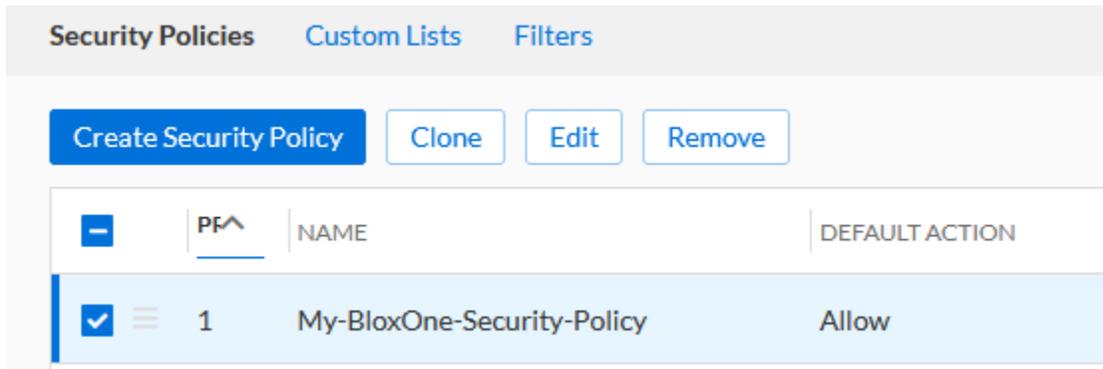
Add the External Network to a Security Policy

In order to apply a security policy to your AWS VPC, Perform the following steps.

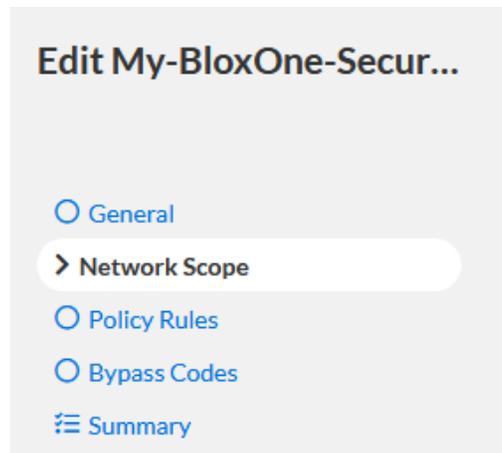
1. In the Infoblox CSP, Navigate to the Security Policy page. Highlight Policies, then click on **Security Policy** in the list that is revealed.



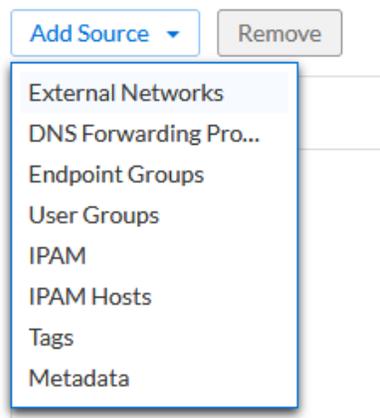
2. Once on the Security Policies page, locate the security policy that you would like to add your AWS VPC to. Click the **checkbox** associated with the Security Policy. Then, click **Edit**.



3. On the panel that is revealed, click **Network Scope** in the left navigation panel.



4. On the *Network Scope* page, click **Add Source**. Then, click **External Networks** in the list that is revealed.



5. In the Available External Networks panel of the Security Policy, click the **arrow** associated with the External network that you've created in the previous section.

Manage External Networks

AVAILABLE EXTERNAL N...	SELECTED
B1TD-R53-Guide-Ext-Net	No external networks selected

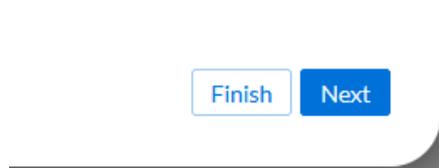
Buttons: Cancel, Save, Back, Finish, Next

6. After the External network has been moved from the *AVAILABLE* panel to the *SELECTED* panel, click **Save**.

AVAILABLE EXTERNAL N...	SELECTED
No external networks available	B1TD-R53-Guide-Ext-Net

Buttons: Cancel, Save

7. Finally, click **Finish**, then **Save & Close** to confirm the changes to your Security Policy.



Test the Configuration

To verify that your DNS traffic is successfully being forwarded to BloxOne perform the following steps:

1. Access a device contained within your AWS VPC. *Note, select a device that can perform a Dig or nslookup command.*
2. Open a Command prompt.
3. Use the **Dig**, or **nslookup** command to resolve a malicious domain that is contained within the security policy this device is protected by.
 - o In the example screenshot I use the dig command to a domain called goal.com which is contained in the security policy that is assigned to my AWS VPC. The domain is resolved to a BloxOne redirect as per the policies' configuration.

```
[ec2-user@ip-10-65-1-23 ~]$ dig goal.com

; <<>> DiG 9.11.4-P2-RedHat-9.11.4-26.P2.amzn2.5.2 <<>> goal.com
; global options: +cmd
; Got answer:
; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 34905
; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

; OPT PSEUDOSECTION:
; EDNS: version: 0, flags; udp: 4096
; QUESTION SECTION:
;goal.com.                IN      A

; ANSWER SECTION:
goal.com.                0      IN      A      3.215.231.251

; Query time: 11 msec
; SERVER: 10.65.0.2#53(10.65.0.2)
; WHEN: Wed Dec 15 20:19:28 UTC 2021
; MSG SIZE rcvd: 53
```

Add TIDE feeds to Route 53 Firewall Domain Lists

This portion of the Deployment guide will guide you on how to add Infoblox TIDE feeds to your AWS Route 53 DNS Firewall domain list. Please note that by utilizing an AWS Route 53 firewall, charges will be incurred from AWS. Infoblox does not charge extra for the use of TIDE, however a BloxOne Threat Defense Advanced license is required for this feature.

Prerequisites

The following are prerequisites to add TIDE feeds to AWS' DNS Firewall domain list:

- BloxOne:
 - BloxOne Threat Defense Advanced subscription
 - A CSP user account with BloxOne Threat Defense administrator permissions
- AWS:
 - A Preconfigured VPC

Known Limitations

By default, AWS Route53 DNS Firewall allows adding up to 100,000 domains per list. If you need to publish more entries, please contact AWS. Please note that by default the script used in this guide will overwrite any existing Domains in the AWS Route 53 DNS Firewall domain list with Replace via the `import_firewall_domains` function. Additionally, note that the AWS Route 53 DNS Firewall domain list only accepts domain names, one line at a time. For more information on AWS Route Firewall domain lists, please see the AWS documentation [here](#).

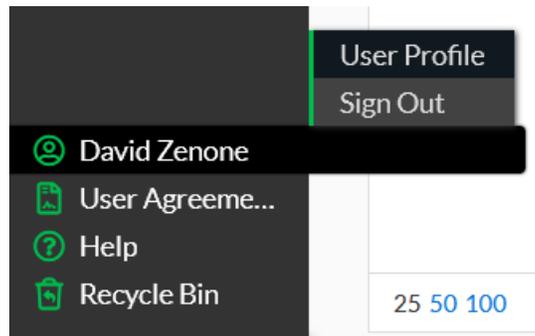
Workflow

1. Acquire a TIDE API Key.
2. Create an AWS Route 53 DNS Firewall domain list or use an existing one.
3. Create a rule group or use an existing one.
 - a. Assign the AWS Route 53 DNS Firewall domain list to the rule group.
 - b. Create a rule and associate that rule with your VPC.
4. Create an S3 Bucket.
 - a. Create a simple text file in the S3 bucket.
 - b. Save the S3 Bucket name and file name for use in the Lambda function's environment variables.
5. Acquire parameters for a Lambda function.
 - a. Acquire a TIDE API Call URL.
 - b. Acquire an AWS Route 53 DNS Firewall domain list ID.
6. Create a Lambda function.
 - a. Input environment variables.
7. Create IAM Policies.
8. Test the Lambda function.
9. Create an AWS EventBridge Schedule.

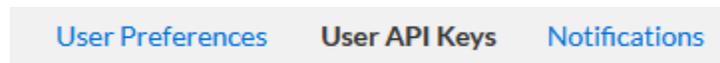
Acquire a TIDE API Key

To input TIDE feeds into an AWS Route 53 DNS Firewall, you must first acquire a TIDE API key from the Infoblox CSP. As mentioned in the prerequisites, a BloxOne Threat Defense Advanced license is required for TIDE feeds. In order to acquire a TIDE API key, perform the following steps:

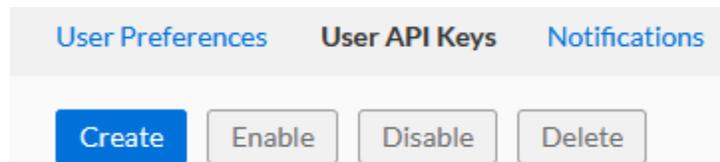
1. Log into the Infoblox CSP. Once logged in, highlight your **username** located in the bottom left of the navigation panel, then click on **User Profile** in the list that is revealed.



2. On the *User Profile* page, click the **User API Keys** tab located at the top of the page.



3. Click the **Create** button to begin creating an API key.



4. On the Create Service API Key panel that is revealed. Give the API Key a **Name**.

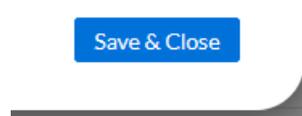
Create User API Key

*Name

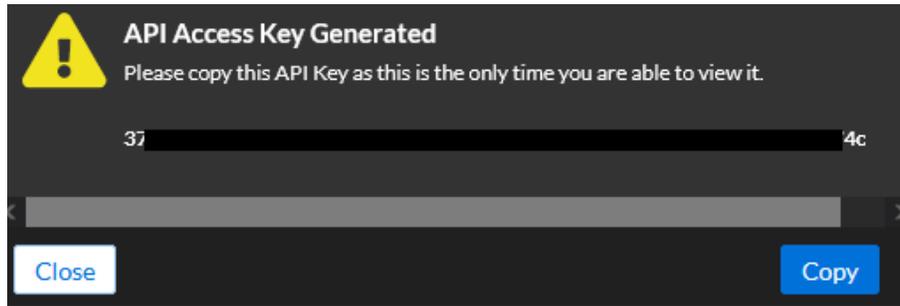
5. (Optional) Change the API Keys expiration date by changing the **Expires at** field.

Expires at 

6. Click **Save & Close** to confirm the creation of the API key.



7. After clicking Save & Close, a *dialog box* will appear. **Copy** the API key from this dialog box and save it to a text file for use later. *Please note that once you close this dialog box, the API key will no longer be accessible.*



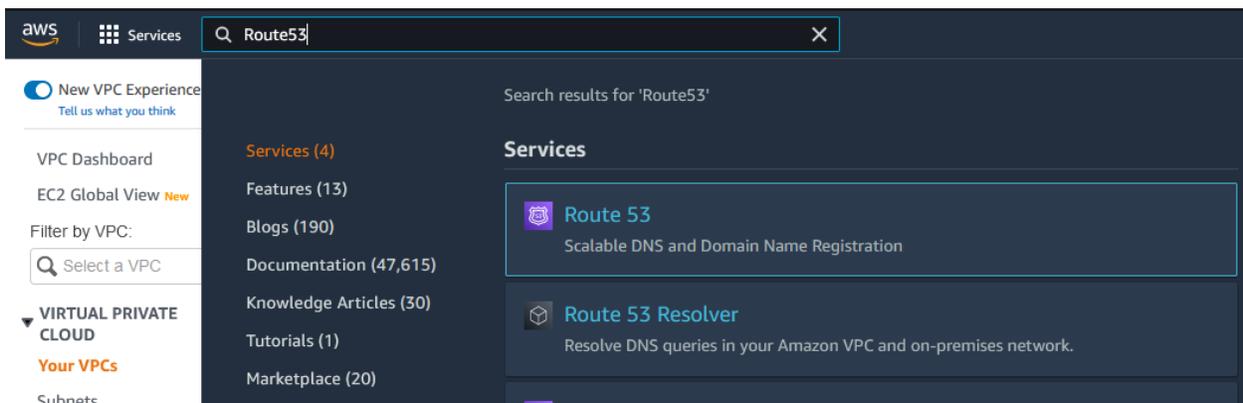
Create an AWS Route 53 DNS Firewall domain list

In order to use an Infoblox Tide feed an AWS Route 53 Firewall domain list must be used. This list contains domains that are either blocked or allowed. If you have an existing AWS R53 Domain list, you may use that one instead of creating a new one. If you would like to use an existing one, please skip this section. If you would like to create a new one, perform the following steps:

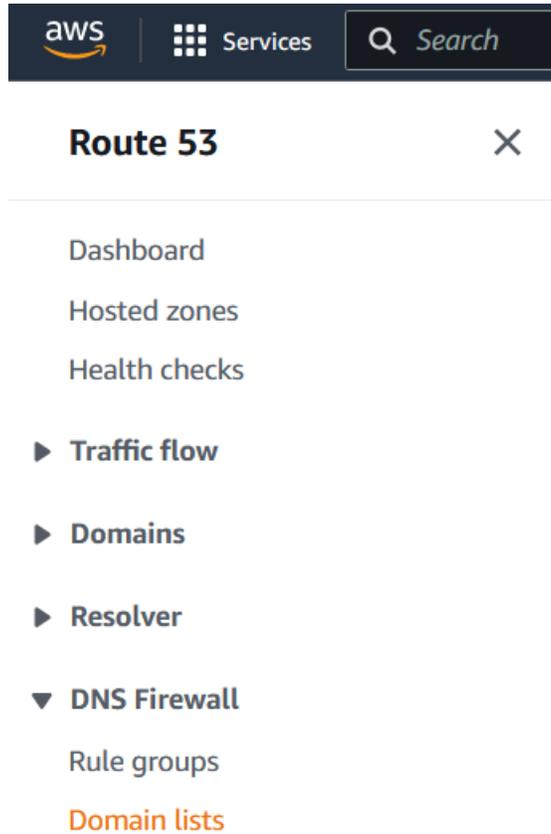
1. Log in to your AWS account. Once logged in, input **Route53** into the *search bar* located at the top of the AWS interface.



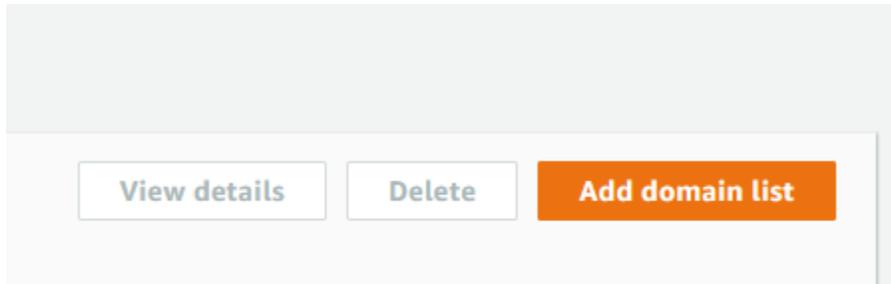
2. Click the text **Route 53** in the list that is revealed.



3. In the *Route 53 navigation pane*, click **Domain List** located under the *DNS Firewall* header.



4. On the *Domain Lists* page, in the *Owned domain lists* panel click **Add domain list**.

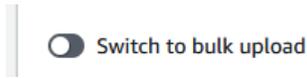


5. On the *Add domain list* page, input the following information:
- Give the domain list a **Name**.

Domain list name

The name must have 1-128 characters. Valid characters: A-Z, a-z, 0-9, -(hyphen), and _(underscore).

- (Optional) If desired, you may input a bulk list of domains to the domain list via the **Switch to bulk upload** toggle switch and an *S3 bucket*.



- Input one or more domains in the **Enter one domain per line** text box. *Note, you may only input one domain per line*

Enter one domain per line

- (Optional) If desired, add tags via the **Add tag** button

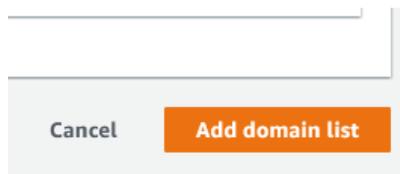
Tags

No tags associated with the resource.

Add tag

You can add 50 more tags.

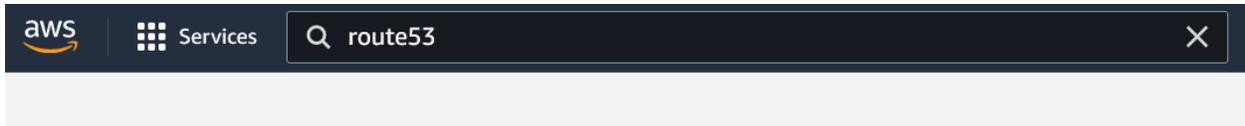
- Click the **Add domain list** button to confirm the creation of the domain list



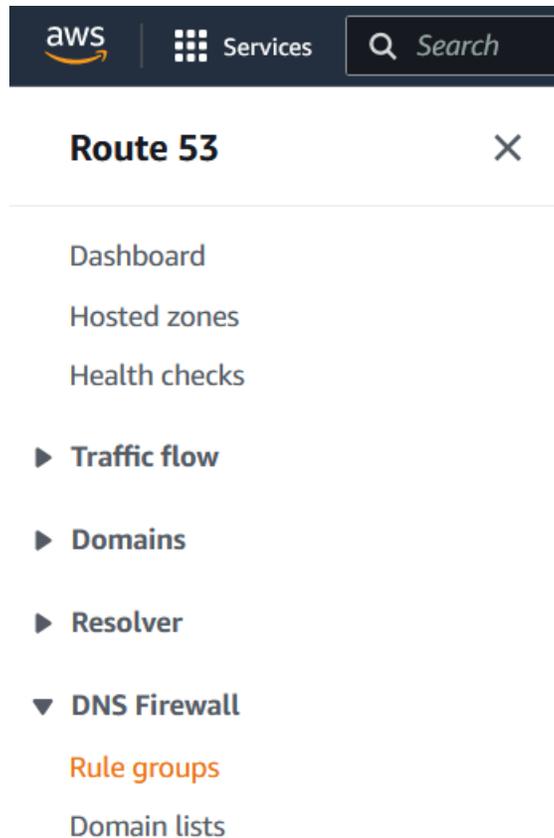
Create an AWS Route 53 DNS Firewall Rule Group and Associated Rule

To determine what actions are taken by the AWS R53 DNS Firewall, a Rule group must be created. This rule group contains rules that define if domains contained in an AWS R53 domain name list are blocked or allowed. If you have an existing AWS R53 rule group, you may use that one instead of creating a new one. If you would like to use an existing one, please skip this section. If you would like to create a new one, perform the following steps:

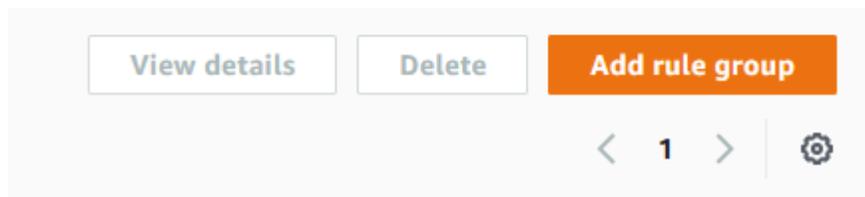
1. On the AWS Interface, input **Route53** into the *search bar* located at the top of the page.



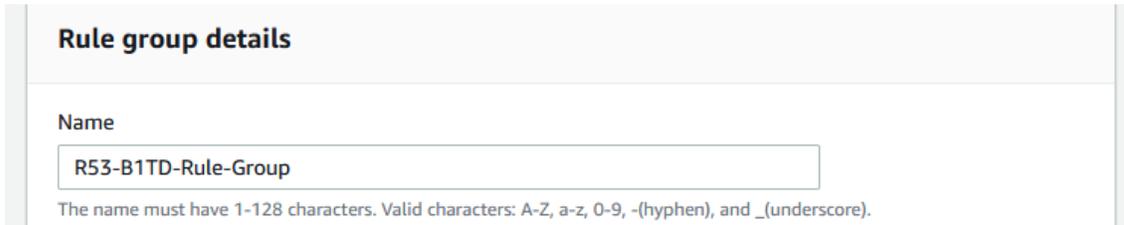
2. In the *Route 53 navigation pane*, click **Rule groups** located under the *DNS Firewall* header.



3. On the *Rule groups* page, click **Add rule group**.



- On the Add rule group page perform the following steps:
 - In the Rule group details panel, give the rule group a **Name**.



Rule group details

Name

R53-B1TD-Rule-Group

The name must have 1-128 characters. Valid characters: A-Z, a-z, 0-9, -(hyphen), and _(underscore).

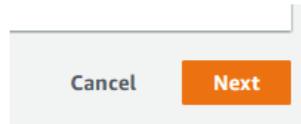
- (Optional) If desired, give the Rule group a **Description**.



Description - optional

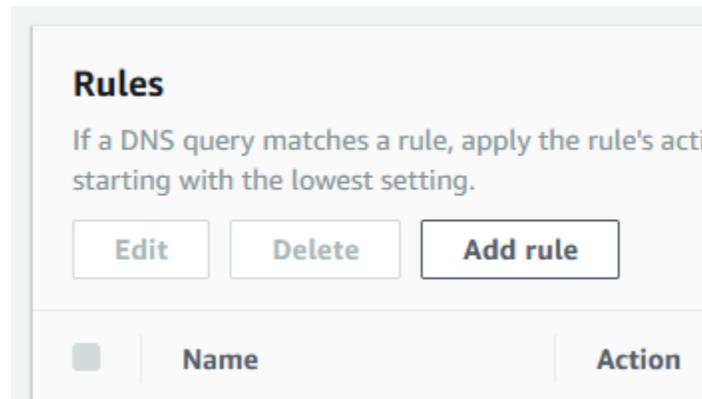
The description can have 1-256 characters.

- Click **Next**



Cancel Next

- Click the **Add Rule** button located near the top of the *Rules* panel to begin adding a rule.



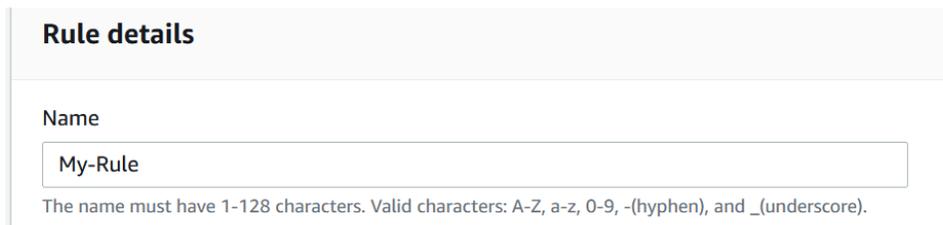
Rules

If a DNS query matches a rule, apply the rule's action starting with the lowest setting.

Edit Delete Add rule

	Name	Action
--	------	--------

- Give the rule a **Name**.



Rule details

Name

My-Rule

The name must have 1-128 characters. Valid characters: A-Z, a-z, 0-9, -(hyphen), and _(underscore).

- (Optional) If desired, give the rule a **Description**.

Description - optional

The description can have 1-256 characters.

- In the *Domain list* panel, select **Add my own domain list**.

Domain list

Domain list
You can choose your own domain list or an AWS managed domain list. [See Amazon Route 53 DNS Firewall pricing for AWS managed domain lists.](#) You can't change the domain list of a rule after you create the rule.

Add my own domain list
Use this option to create or migrate your own domain list.

Add AWS managed domain list
These are subscribed domain lists provided by Amazon.

- In the *Choose or create a new domain list* drop-down menu, select the **domain list** you intend to add TIDE feeds to.

Choose or create a new domain list

- In the Action panel, select the action that will be taken when this rule is triggered by selecting the **action** in the *Choose an action to take when a DNS query fits the matches* drop-down, and the associated bubbles.

Action

Choose an action to take when a DNS query fits the matches

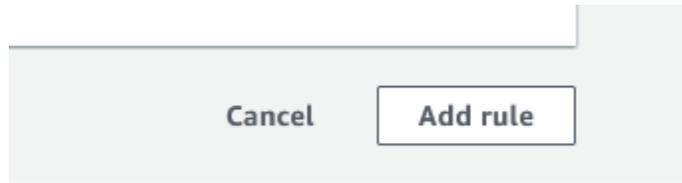
Select a response to send for the BLOCK action

NODATA
Indicates that this query was successful, but there is no response available for the query.

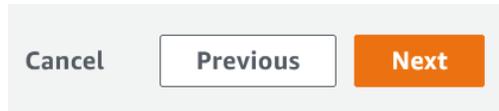
NXDOMAIN
Indicates that the domain name that's in the query doesn't exist.

OVERRIDE
Provides a custom override response to the query.

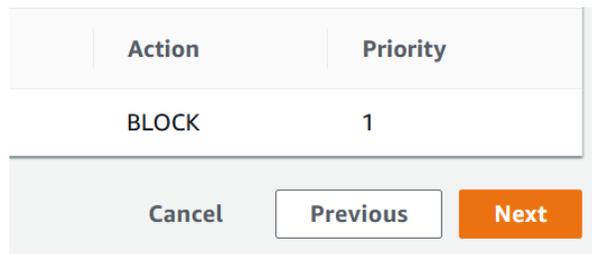
- Click the **Add rule** button to confirm the creation of the rule.



- Click **Next**.



- Click **Next**.



- (Optional) If desired, add Tags to the rule group via the **Add tag** button.

Add tags - optional Info

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

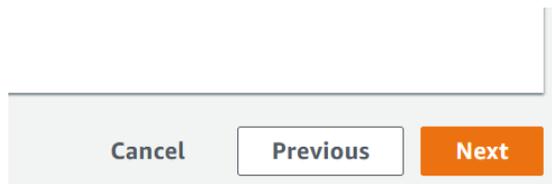
Tags

No tags associated with the resource.

Add tag

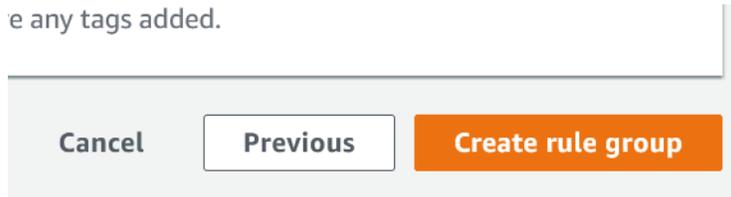
You can add 50 more tags.

- Click **Next**

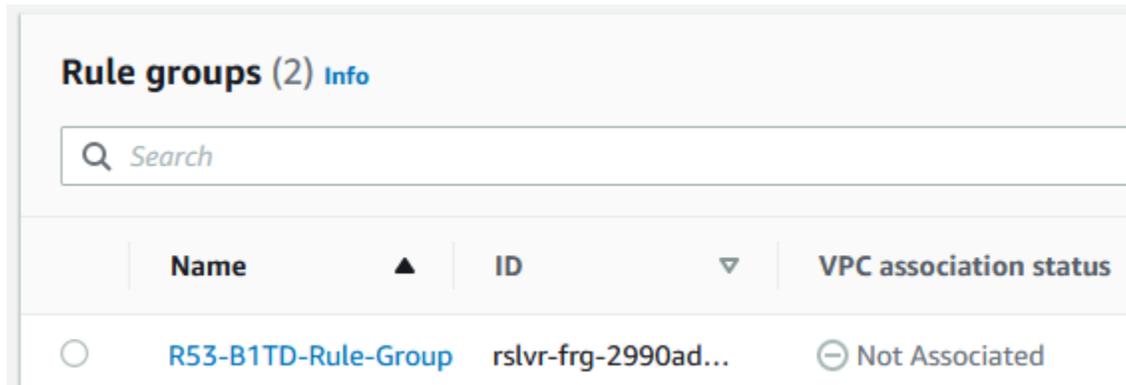


- Review the rule groups settings, then click **Create rule group** to confirm the creation of the rule group.

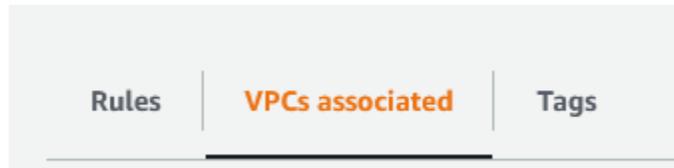
...e any tags added.



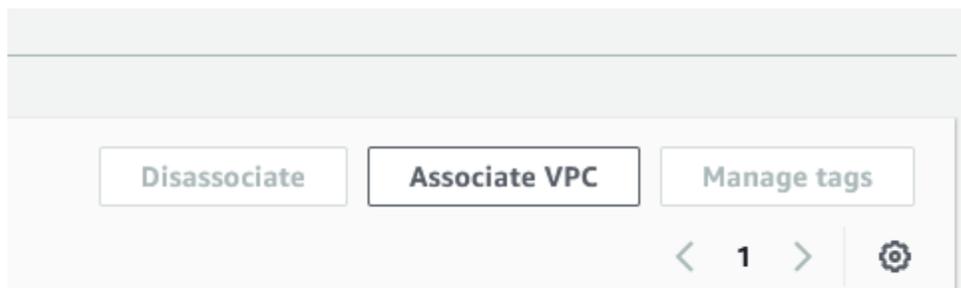
5. This *Rule group* must be associated with a VPC in order to take action on domains contained in your domain list. In order to associate the rule group to a VPC click the rule group you've just created by clicking the **rule group** located in the rule group panel.



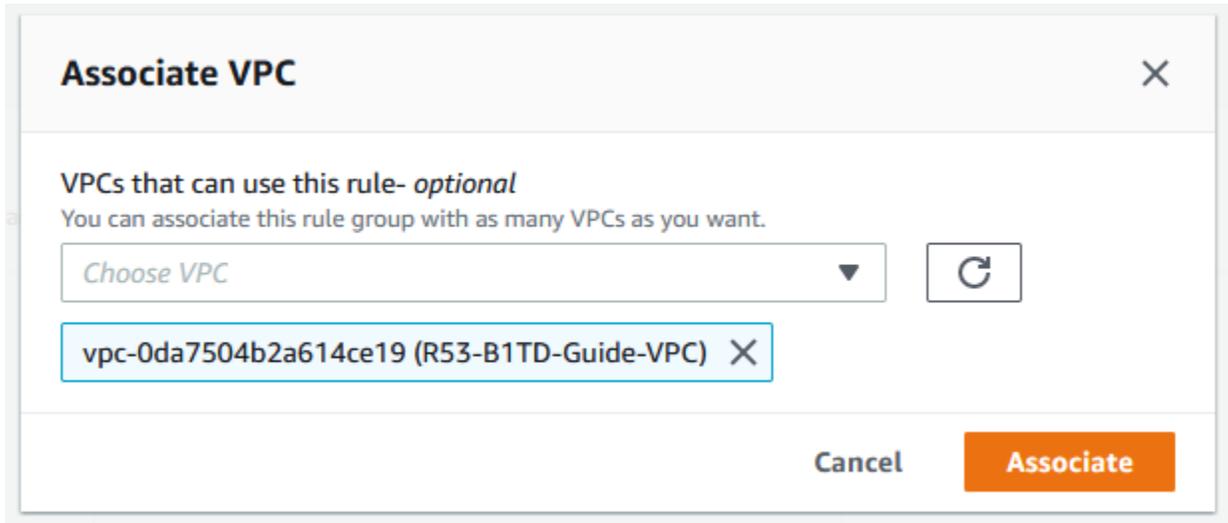
6. Near the bottom of the *rule group's* page, click the **VPCs Association** tab.



7. Click the Associate VPC button located in the **VPCs associated** panel.



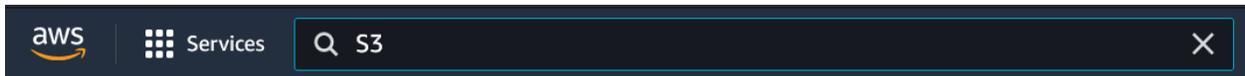
8. In the *Associate VPC* panel **select** a VPC via the *Choose VPC drop-down*, then Click **Associate**.



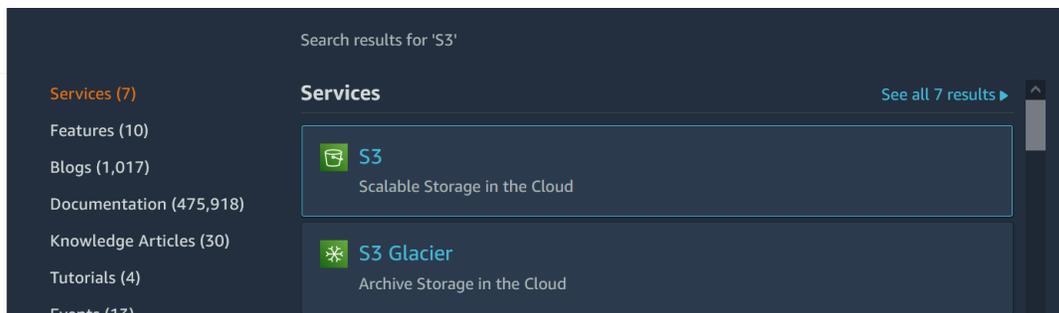
Create an S3 Bucket and File

In order to add domains to an AWS Route 53 domain list, a S3 bucket, and a simple text file are required. The file acts as an interim location, allowing for the transferring of IOC data sourced from the TIDE API, into the domain list that has been specified. In order to create an S3 bucket and file, perform the following steps:

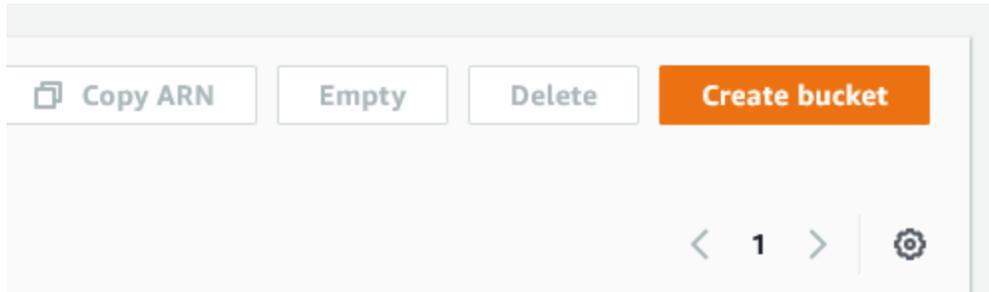
1. Input **S3** into the *search bar* located at the top of the AWS interface.



2. Locate and click on **S3** to navigate to the *Amazon S3* page.



3. On the *S3 Amazon* page, click **Create bucket**.



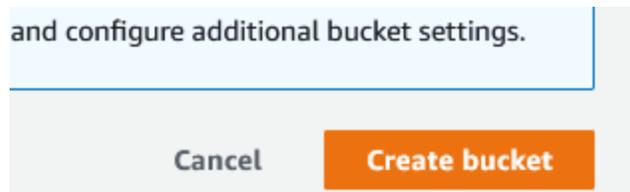
4. On the *Create bucket* page perform the following steps:
 - Give the bucket a **name**. *Note: save this name to a text file for use later in this guide*

A screenshot of the 'General configuration' section of the AWS 'Create bucket' page. The title 'General configuration' is in bold. Below it, the 'Bucket name' label is followed by a text input field containing 'r53-bitd-bucket'. Below the input field, there is a note: 'Bucket name must be unique and must not contain spaces or uppercase letters. [See rules for bucket naming](#) '. The entire section is enclosed in a light gray border.

- Select the **AWS region** you intend to use via the AWS Region drop-down.

A screenshot of the 'AWS Region' dropdown menu. The label 'AWS Region' is above a dropdown box that currently displays 'US East (N. Virginia) us-east-1' with a downward-pointing arrow on the right side.

- (Optional) If desired, configure any additional settings. Once you are done configuring the bucket, click **Create bucket**.



- On the *Buckets* page, scroll down to the Buckets panel. Locate and click on the **S3 bucket** you've just created.

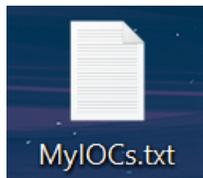
Buckets (22) [Info](#)

Buckets are containers for data stored in S3. [Learn more](#)

< 1 >

	Name ▲	AWS Region ▼	Access ▼	Creation date ▼
<input type="radio"/>	firewall-querylogs	US west (N. California) us-west-1	Objects can be public	July 25, 2021, 10:02:21 (UTC-07:00)
<input type="radio"/>	firewalllist	US West (Oregon) us-west-2	Bucket and objects not public	July 26, 2021, 15:24:49 (UTC-07:00)
<input type="radio"/>	hw3-md-76	US East (N. Virginia) us-east-1	Objects can be public	July 2, 2018, 13:48:48 (UTC-07:00)
<input type="radio"/>	infobloxsplunktest	US West (N. California) us-west-1	Bucket and objects not public	September 11, 2020, 08:02:10 (UTC-07:00)
<input type="radio"/>	r53-bitd-bucket	US East (N. Virginia) us-east-1	Bucket and objects not public	January 5, 2022, 09:26:04 (UTC-08:00)

- On your desktop, create a simple **text file** with no content.



- In the *Objects* panel of Bucket's page click **Upload**.

Objects (0)

Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 inventory](#) to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. [Learn more](#)

< 1 >

- Locate and **upload** the simple text file created in this section. You may do this via the **Drag and Drop** feature, or the **Add files** button.

Files and folders (1 Total, 0 B)

All files and folders in this table will be uploaded.

9. Click **Upload** located at the bottom of the page. *Note: Save the name of the file to a text file for use later in this guide.*

Drag and drop files and folders you want to upload here, or choose **Add files**, or **Add folders**.

Files and folders (1 Total, 0 B)
All files and folders in this table will be uploaded.

< 1 >

<input type="checkbox"/>	Name	Folder	Type
<input type="checkbox"/>	MyIOCs.txt	-	text/plain

Destination

Destination
[s3://r53-bitd-bucket](#)

▶ **Destination details**
Bucket settings that impact new objects stored in the specified destination.

▶ **Permissions**
Grant public access and access to other AWS accounts.

▶ **Properties**
Specify storage class, encryption settings, tags, and more.

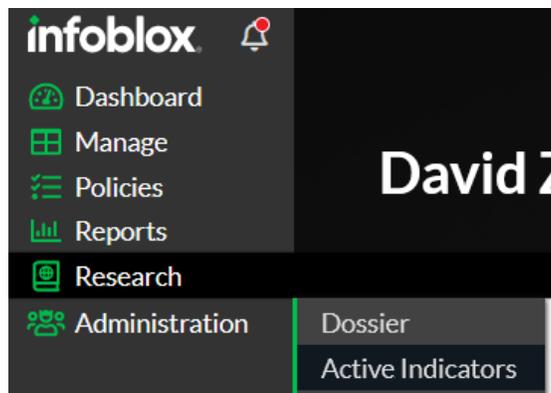
Acquire Information for a Lambda function

In order to download TIDE feeds a Lambda function is used. This lambda function requires parameters specific to your environment. To acquire these parameters, perform the steps in following subsections:

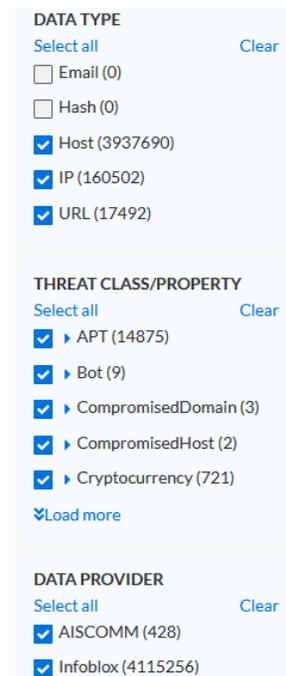
Acquire a TIDE API Call URL

The lambda function that will be created in this guide requires an API call to acquire feeds from BloxOne. Please note that it is possible to return a large data set via a TIDE API call. By default, AWS Route53 DNS Firewall allows adding up to 100.000 domains per list. If you need to publish more entries, please contact AWS. To create a TIDE API call, perform the following steps:

1. Log into the Infoblox CSP. Once logged in, highlight *Research* located in the bottom left of the navigation panel, then click on **Active Indicators** in the list that is revealed.



2. Here you can see the list of *Active indicators*. Due to the quantity of data, it is suggested to filter the API call. Click **Clear** for each section, until all sections are unchecked.



3. Under the *DATA TYPE* header, click the **checkbox** associated with the **Host** data type.

Data Type	
Select all	Clear
<input type="checkbox"/> Email	(4)
<input type="checkbox"/> Hash	(7,951)
<input checked="" type="checkbox"/> Host	(20,509,844)
<input type="checkbox"/> IP	(124,171)
<input type="checkbox"/> URL	(225,432)

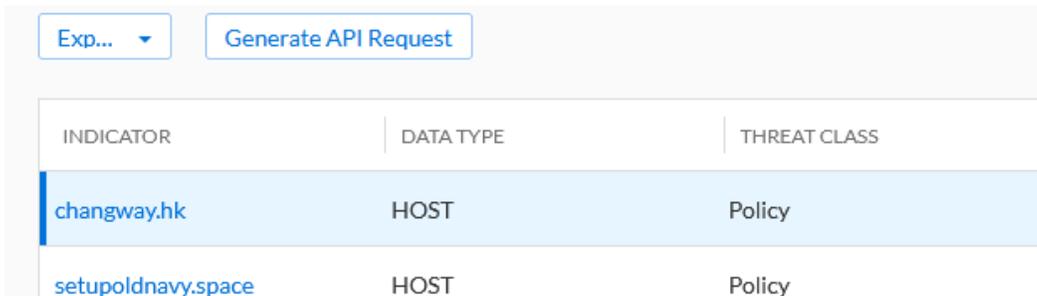
4. Under the *THREAT CLASS/PROPERTY* header, click the **checkboxes** associated with the **Threat Class / Properties** you would like to add to your AWS Route 53 Domain Firewall list. *Note that it is suggested to only select one threat class/property per lambda function as duplicates may occur for domains that are associated with one or more threat class/property. Route 53 DNS Domain lists do not allow duplicate entries.*

Threat Class/Property	
Select all	Clear
<input type="checkbox"/> ▶ APT	(8,210)
<input type="checkbox"/> ▶ Bot	(5)
<input type="checkbox"/> ▶ CompromisedDomain	(2)
<input type="checkbox"/> ▶ CompromisedHost	(9)
<input type="checkbox"/> ▶ Cryptocurrency	(2,008)
<input type="checkbox"/> ▶ DNSTunnel	(3)
<input checked="" type="checkbox"/> ▶ ExploitKit	(985)

5. Click **Apply Filter** to apply the selected filter.

Data Type	
Select all	Clear
<input type="checkbox"/> Email	(4)
<input type="checkbox"/> Hash	(7,951)
<input checked="" type="checkbox"/> Host	(20,509,844)

6. At the top of the *Active Indicators* page, click **Generate API request**. Note this will create a simple API call for the IOC defined, this API call can be modified further with additional parameters.

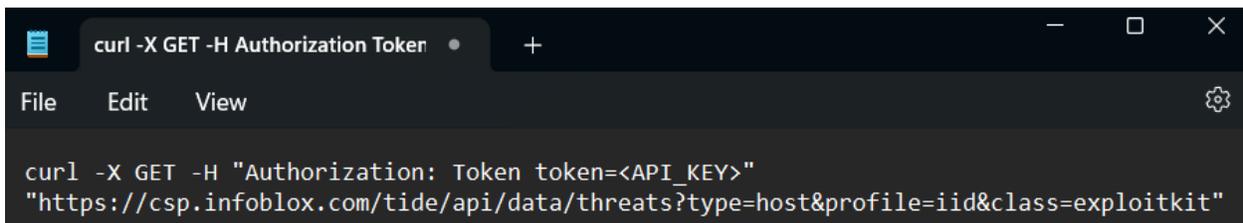


INDICATOR	DATA TYPE	THREAT CLASS
changway.hk	HOST	Policy
setupoldnavy.space	HOST	Policy

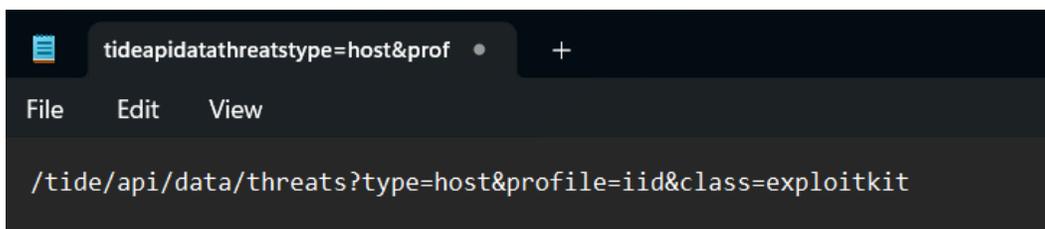
7. **Copy** the API call in the dialog box that has been revealed.



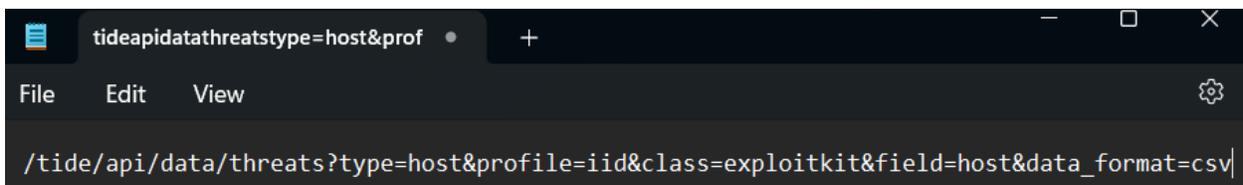
8. **Paste** the API call to a text editor of your choice.



9. Modify the API call by **deleting** all text until `/tide/`. Additionally, keep all following text except for the closing quotation mark.



10. Append the text `&field=host&data_format=csv` to the end of the string. Note these parameters tell the API to only retrieve the *Host* field, and to return it in a *CSV* format.



- (Optional) **Add** additional parameters to specify which IOCs will be imported. For more information on the parameters accepted by the TIDE API, please see the TIDE documentation located [here](#). *Note, If you choose to import a large quantity of IOCs, the transfer of data may take a very long time.*
 - In the example screenshot, the API call has been altered to only acquire IOCs from a 30 day period via the text `&period=30d`. The call has also been altered to only accept 20 domains via the text `&rlimit=20`.

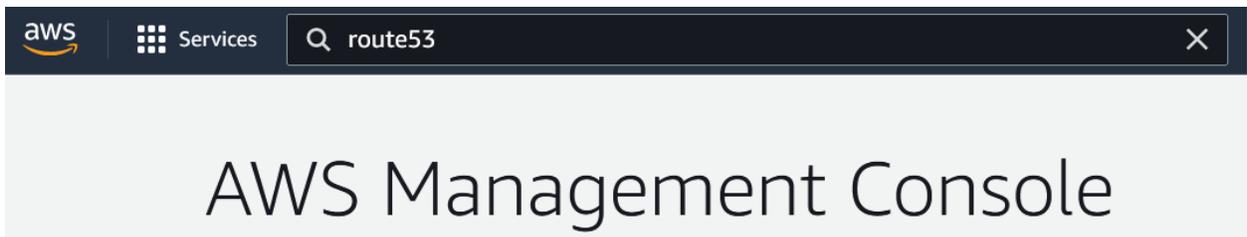


- Save this API call for use later.

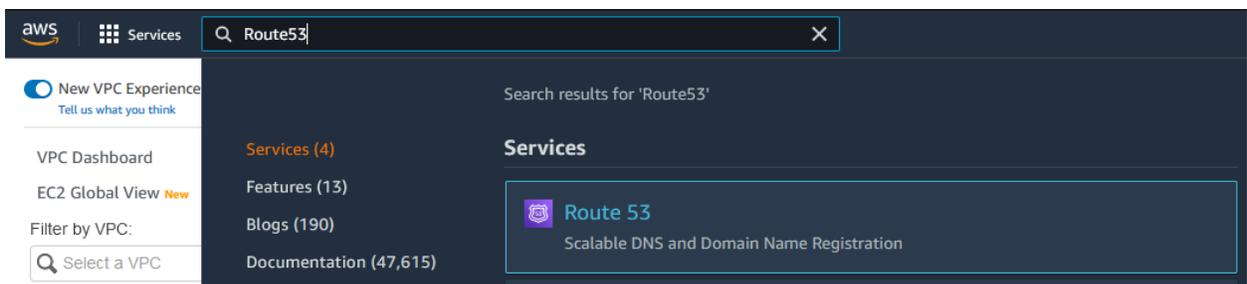
Acquire an AWS Route 53 DNS Firewall domain list ID

To acquire an AWS Route 53 DNS Firewall domain list ID, perform the following steps:

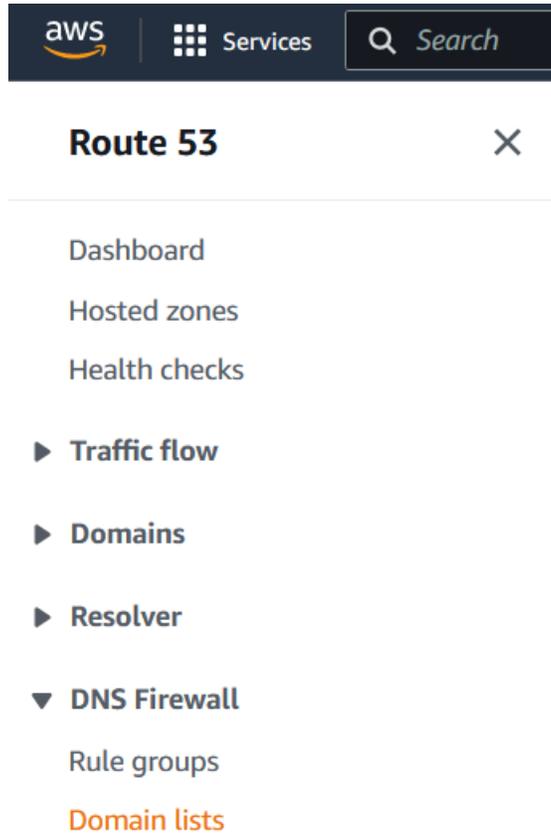
- Log in to your AWS account. Once logged in, input **Route53** into the *search bar* located at the top of the AWS interface.



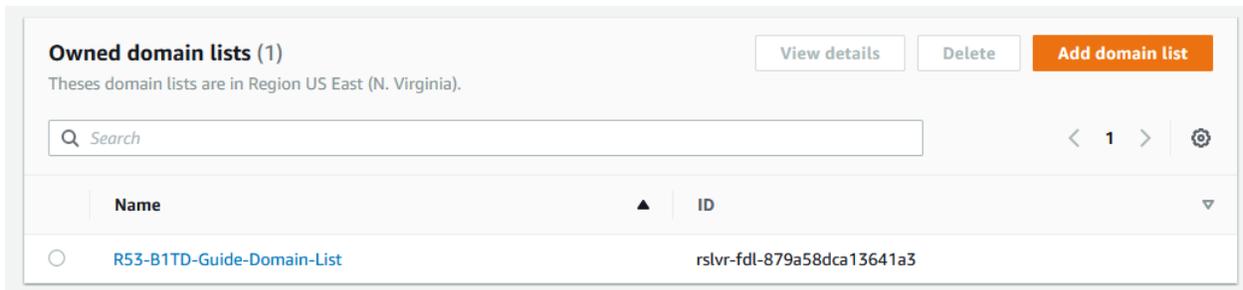
- Click the text **Route 53** in the list that is revealed.



3. In the *Route 53 navigation pane*, click **Domain List** located under the *DNS Firewall* header.



4. On the *Domain Lists* page, in the *Owned domain lists* panel locate the Domain list you intend to add TIDE IOCs to. **Copy** the ID and **Save** it to a text file for use later. *Note, in the example screenshot the Domain list ID is rslvr-fdl-879a58dca13641a3.*



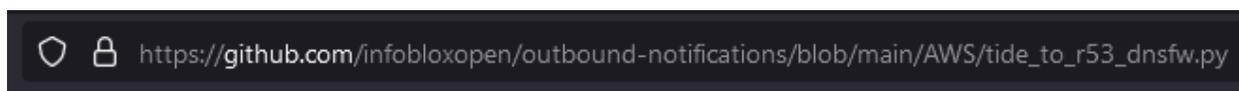
Create a Lambda function

To import TIDE feeds into the AWS Route 53 Domain list, API calls must be made. This is easily done via a previously created Python script which can be added to AWS as a Lambda function.

Please note that the script replaces any existing domains in the domain list it is interacting with. If desired, you may alter the script to append instead of replace.

To download this script, perform the following steps:

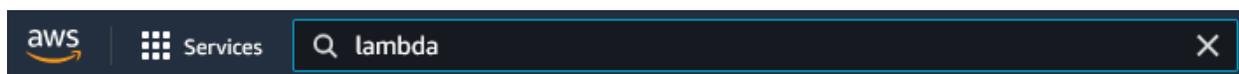
1. Navigate to https://github.com/infobloxopen/outbound-notifications/blob/main/AWS/tide_to_r53_dnsfw.py in your web browser of choice.



2. Copy the Python script and save it to a text file.

```
56 lines (48 sloc) 1.61 KB
1  # (c) Vadim Pavlov
2  # 2021-09-17
3  # lambda function to import IoCs from TIDE to AWS Route 53 Firewall
4  import json, os, urllib3, logging, boto3
5  from pprint import pprint
6  logging.basicConfig(level = logging.INFO, force=True)
7  search = os.environ['SEARCH']
8  APIkey = os.environ['CSP_API_KEY']
9  dnsFWListId = os.environ['DNSFW_LISTID']
10 s3Bucket = os.environ['S3BUCKET']
11 s3File = os.environ['S3FILE']
12 s3URL = "s3://" + s3Bucket + "/" + s3File
13 print (s3URL)
14 baseUrl = 'https://csp.infoblox.com'
15 authH = ('Authorization: Token token=' + APIkey)
16 tideREST = urllib3.PoolManager(timeout=30.0)
17
18 s3 = boto3.client('s3')
19 r53 = boto3.client('route53resolver')
20
21 def lambda_handler(event, context):
22     # TODO implement
23
24     try:
25         r = tideREST.request('GET', baseUrl+search, headers=authH)
26         if (r.status==200):
27             #print("ioc:", r.data[5:])
28             s3r = s3.put_object(
29                 Body=r.data[5:],
30                 Bucket=s3Bucket,
31                 Key=s3File,
32             )
33             ##add error handling
34             r53=r53.Import_firewall_domains(
35                 FirewallDomainListId=dnsFWListId,
36                 Operation='REPLACE',
37                 DomainFileUrl=s3URL
38             )
39             ##add error handling
40             pprint(r53r)
41
42     except Exception as e:
43         print("send(..) failed executing tideREST.request(..):", e)
```

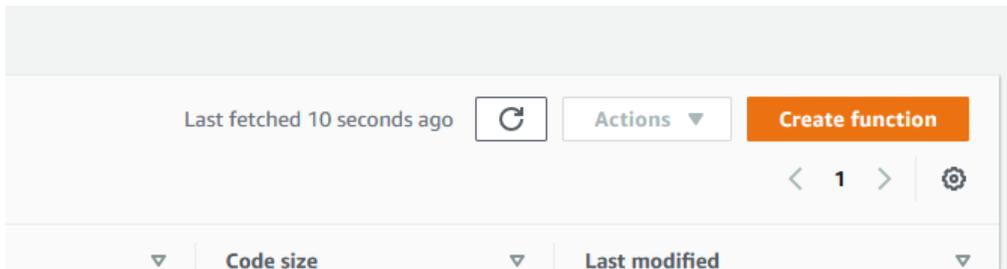
1. Back in the AWS console, input **Lambda** into the *search bar* located at the top of the AWS interface.



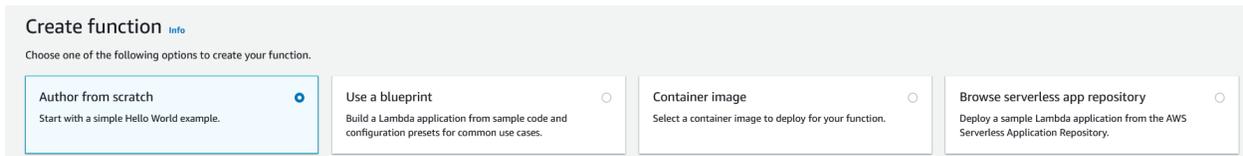
2. Locate and click on **Lambda** to navigate to the *Lambda* page.



3. On the *AWS Lambda functions* page, click **Create function**.



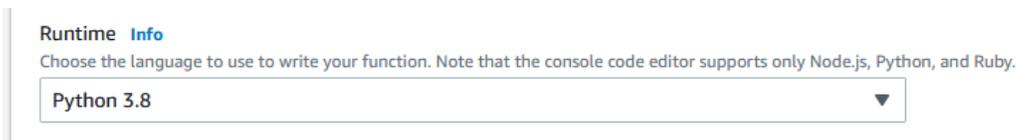
4. On the *Create function* page, configure the following settings:
 - Click the **Author from scratch** bubble.



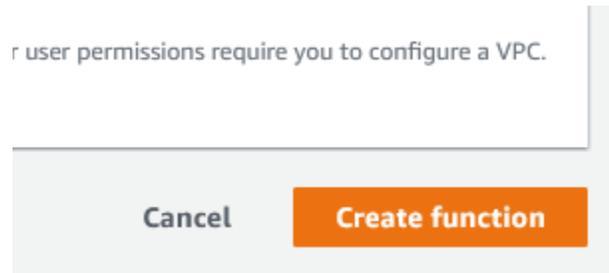
- Give the Function a **name**.



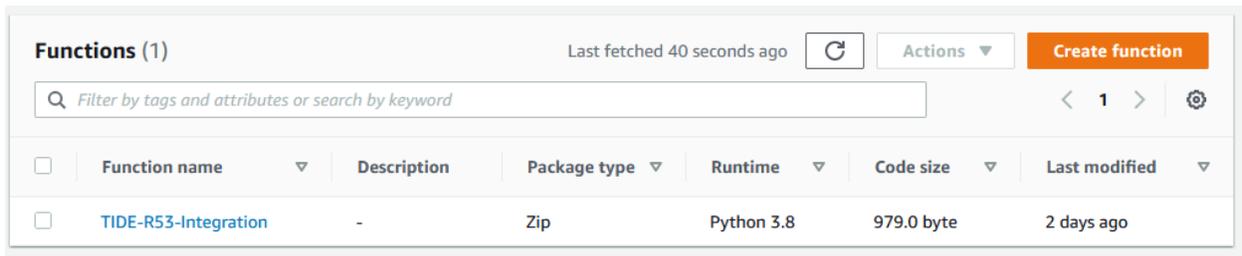
5. Select **Python 3.8** via the *Runtime* drop-down menu.



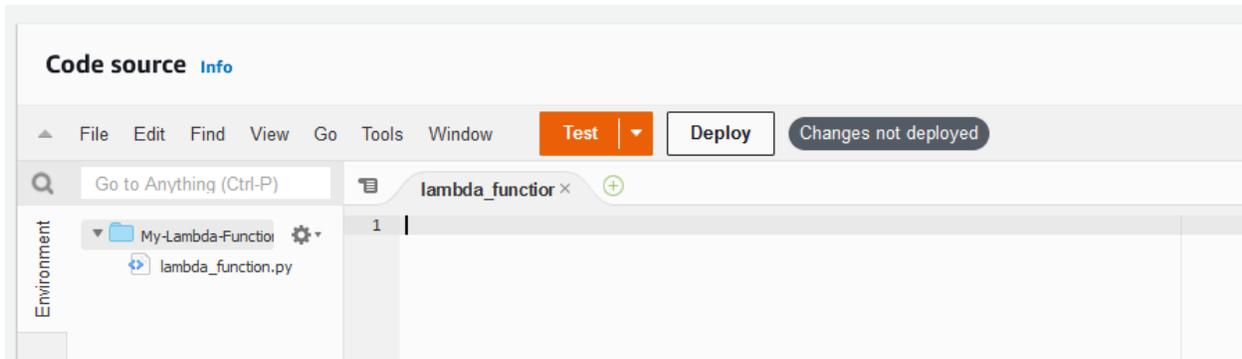
- Keep all other settings as their default and click **Create function**.



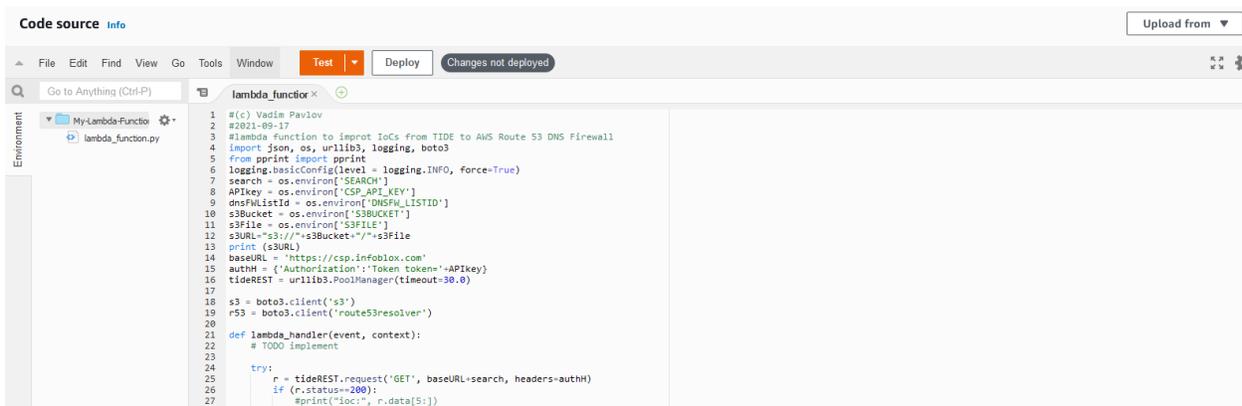
- On the *Functions* page, locate and click the **Lambda function** you've just created.



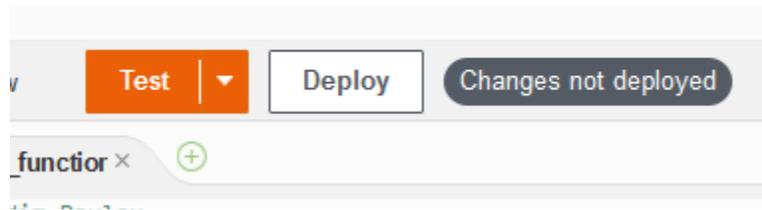
- Once on the Lambda function's page, **delete** all text located in the code editor.



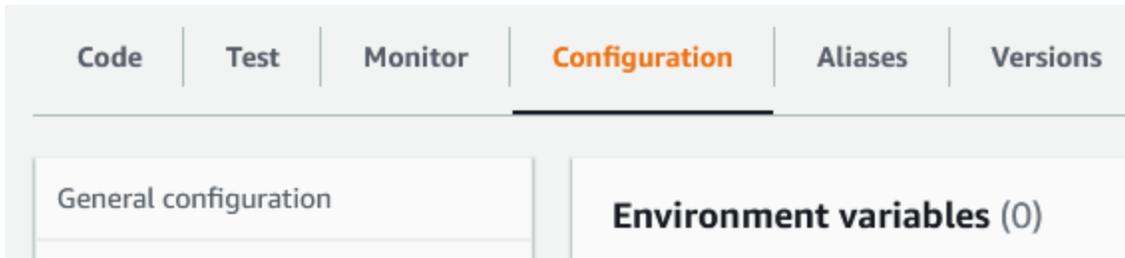
- Paste the code acquired previously in this section on page 36.



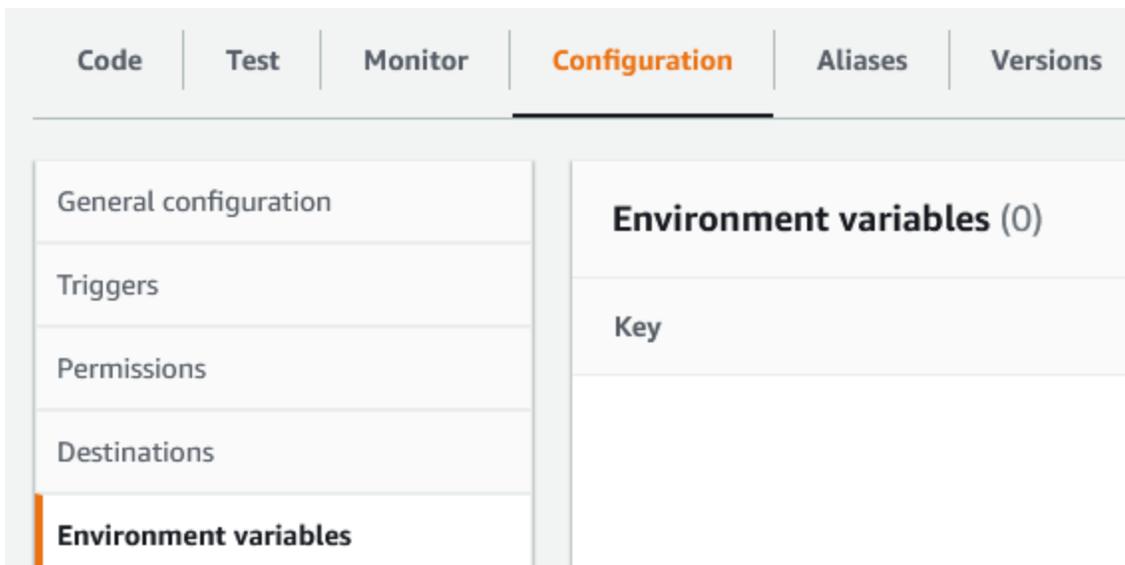
10. To deploy the code, click the **Deploy** button located above the code editor.



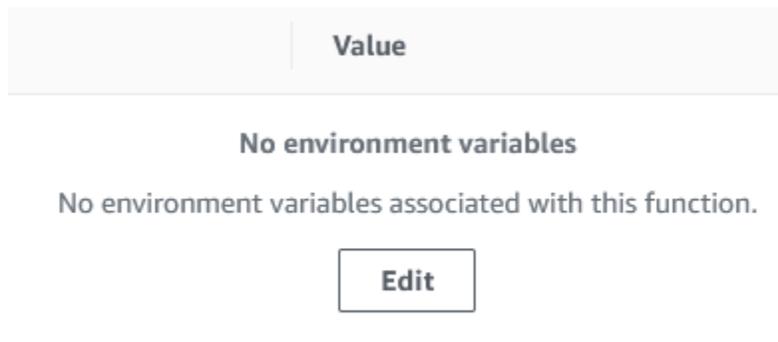
11. On the Lambda function's page, click the **Configuration** tab.



12. On the *Configuration* page, click **Environment variables** in the navigation panel.



13. Edit the *Environment Variables* by clicking the **Edit** button located in the middle of the Environment variables panel.



14. On the Edit environment variables page, click **Add environment variable**.

Edit environment variables

Environment variables

You can define environment variables as key-value pairs that are accessible from your function code. These are useful to store configuration settings without the need to change function code. [Learn more](#) 

There are no environment variables on this function.

Add environment variable

15. In the first *Environment Variable*, input **CSP_API_KEY** in the **Key** text field.

Key

CSP_API_KEY

16. Input the **CSP API key** that was acquired on [pages 35-36](#) in the **Value** text field.

Value

My-API-Key-Here

17. Click **Add environment variable** to add an additional environment variable.

Add environment variable

18. In the second *Environment Variable*, input **DNSFW_LISTID** in the **Key** text field.

Key

DNSFW_LISTID

19. Input the **AWS Route 53 DNS Firewall domain list ID** that was acquired on [page 49](#) in the **Value** text field.

Value

My-DNSFW-List-ID-Here

20. Click **Add environment variable** to add an additional environment variable.

Add environment variable

21. In the third *Environment Variable*, input **S3BUCKET** in the **Key** text field.

Key

S3BUCKET

22. Input the **S3 Bucket name** that was created on [page 43](#) in the **Value** text field.

Value

My-S3-Bucket-Name-Here

23. Click **Add environment variable** to add an additional environment variable.

Add environment variable

24. In the fourth *Environment Variable*, input **S3FILE** in the **Key** text field.

Key

S3FILE

25. Input the **S3 file name** that was created on [page 45](#) in the **Value** text field.

Value

My-S3-File-Name-Here

26. Click **Add environment variable** to add an additional environment variable.

Add environment variable

27. In the fifth *Environment Variable*, input **SEARCH** in the **Key** text field.

Key

SEARCH

28. Input the **TIDE API call** that was created on [pages 46-48](#) in the **Value** text field.

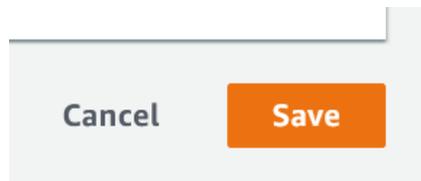
Value

My-TIDE-API-Call-Here

- After inputting all of your environment variables, they should look similar to this screenshot:

Key	Value	
CSP_API_KEY	37c867c1da1d9507c92c4ca020290b76	Remove
DNSFW_LISTID	rslvr-fdl-879a58dca13641a3	Remove
S3BUCKET	r53-bitd-bucket	Remove
S3FILE	MyIOCs.txt	Remove
SEARCH	/tide/api/data/threats?type=host&class	Remove
Add environment variable		

29. Click **Save** to confirm the addition of the newly created environment variables.



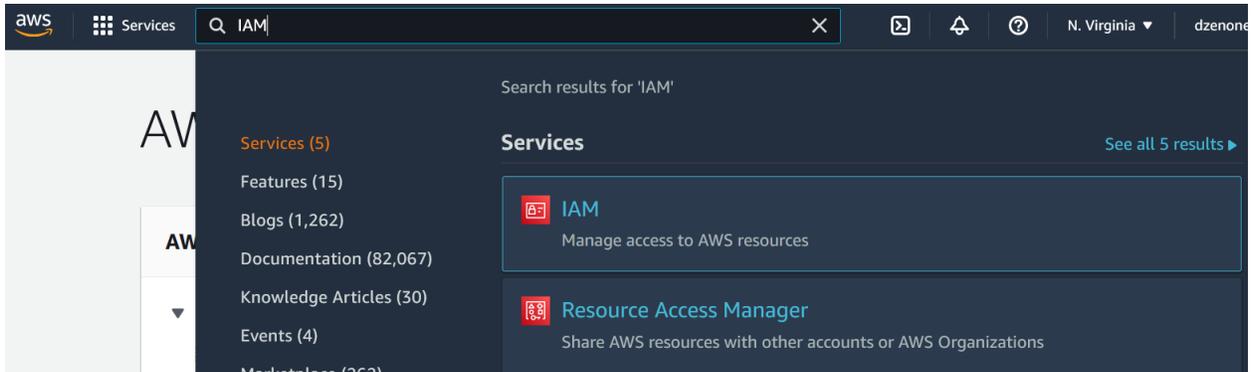
Create IAM Policies

In order to run the Lambda script, the script must have permission to interact with the varying AWS components that are called. To give permissions to the Lambda script, perform the following steps:

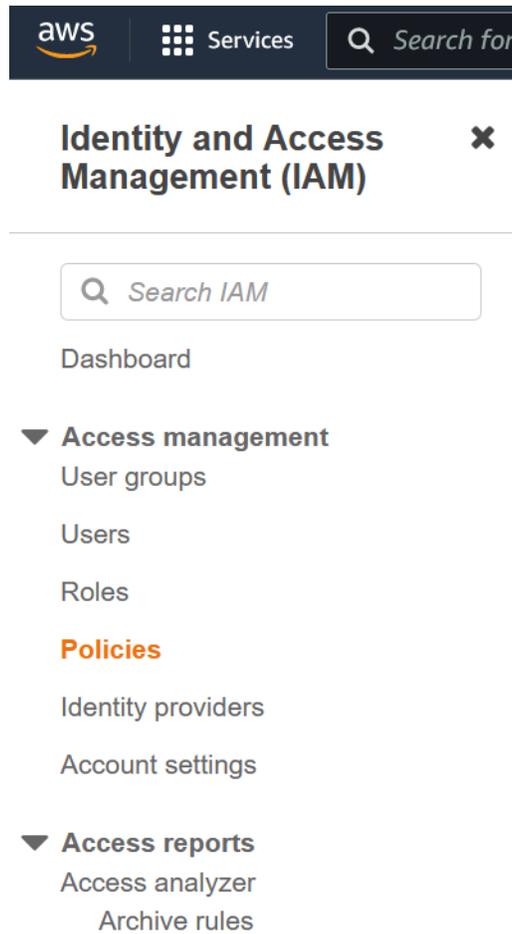
1. Input **IAM** into the *search bar* located at the top of the AWS interface.



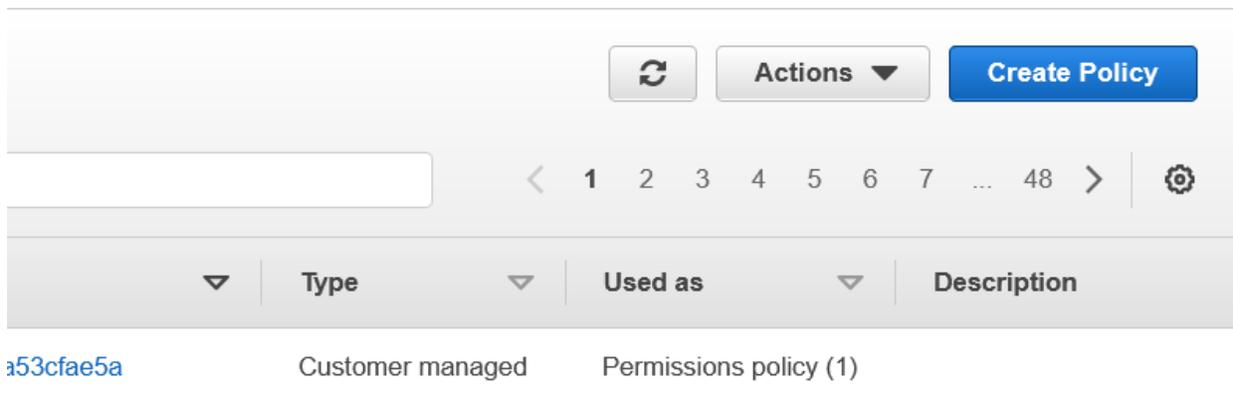
2. Locate and click on **IAM** to navigate to the IAM page.



3. In the IAM navigation pane, click **Policies** located under the *Access management* header.



4. Two policies are required for this integration, first create a policy to allow the Lambda script to interact with the AWS Route 53 DNS Firewall domain list. On the *Policies* page, click **Create Policy** located on the top right of the page.



5. On the *Create Policy* page, click the **JSON** button.



6. **Copy** the following JSON code:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "route53resolver:CreateFirewallRule",
        "route53resolver:CreateFirewallRuleGroup",
        "route53resolver:CreateFirewallDomainList",
        "route53resolver:ListFirewallRules",
        "route53resolver:ListFirewallDomains",
        "route53resolver:GetFirewallDomainList",
        "route53resolver:UpdateFirewallDomains",
        "route53resolver:GetFirewallRuleGroup",
        "route53resolver>DeleteFirewallDomainList",
        "route53resolver:ListFirewallDomainLists",
        "route53resolver:ImportFirewallDomains"
      ],
      "Resource": "*"
    }
  ]
}
```

7. Replace all code in the JSON text box with the code copied from the previous step.

Policy editor

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Sid": "VisualEditor0",
6       "Effect": "Allow",
7       "Action": [
8         "route53resolver:CreateFirewallRule",
9         "route53resolver:CreateFirewallRuleGroup",
10        "route53resolver:CreateFirewallDomainList",
11        "route53resolver:ListFirewallRules",
12        "route53resolver:ListFirewallDomains",
13        "route53resolver:GetFirewallDomainList",
14        "route53resolver:UpdateFirewallDomains",
15        "route53resolver:GetFirewallRuleGroup",
16        "route53resolver>DeleteFirewallDomainList",
17        "route53resolver:ListFirewallDomainLists",
18        "route53resolver:ImportFirewallDomains"
19      ],
20      "Resource": "*"
21    }
22  ]
23 }
24
```

[+ Add new statement](#)

8. Click the **Next** button located on the bottom right of the page.



9. On the Review policy page, perform the following steps:
 - o Give the policy a **Name**.

Policy name

Enter a meaningful name to identify this policy.

Maximum 128 characters. Use alphanumeric and '+=, @-_' characters.

- (Optional) If desired, give the policy a **Description**.

Description - *optional*

Add a short explanation for this policy.

Maximum 1,000 characters. Use alphanumeric and '+,=, @, _' characters.

- (Optional) If desired, add tags via the **Add tag** button.

Add tags (Optional)

Tags are key-value pairs that you can add to AWS resources to help identify, organize, or search for resources.

No tags associated with the resource.

Add tag

- Click the **Create policy** button located on the bottom right of the page to confirm the creation of the Policy.

Cancel

Previous

Create policy

10. Now create a second policy to allow the Lambda script to interact with the S3 bucket. On the *Policies* page, click **Create Policy** located on the top right of the page.

The screenshot shows the AWS IAM console 'Policies' page. At the top right, there are three buttons: a refresh button, an 'Actions' dropdown menu, and a blue 'Create Policy' button. Below these is a pagination control showing page 1 of 48. The main content is a table with the following columns: 'Type', 'Used as', and 'Description'. The first row of the table shows a policy with ID 'a53cfae5a', Type 'Customer managed', and Used as 'Permissions policy (1)'. There is also a search bar on the left side of the table.

Type	Used as	Description
Customer managed	Permissions policy (1)	

11. On the *Create Policy* page, click the **JSON** button.



12. **Copy** the following JSON code:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::test"
    },
    {
      "Sid": "VisualEditor1",
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject"
      ],
      "Resource": "arn:aws:s3:::name_of_bucket/*"
    }
  ]
}
```

13. Replace all code in the JSON text box with the code copied from the previous step.

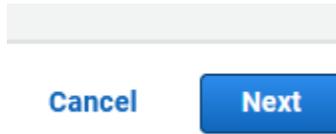
Policy editor

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Sid": "VisualEditor0",
6       "Effect": "Allow",
7       "Action": "s3:ListBucket",
8       "Resource": "arn:aws:s3:::test"
9     },
10    {
11      "Sid": "VisualEditor1",
12      "Effect": "Allow",
13      "Action": [
14        "s3:PutObject",
15        "s3:GetObject",
16        "s3>DeleteObject"
17      ],
18      "Resource": "arn:aws:s3:::name_of_bucket/*"
19    }
20  ]
21 }
22
```

14. On line 18, remove the text 'name_of_bucket', and **replace** it with the name of the bucket you created on [pages 50-51](#). Note, In the example screenshot the name of my bucket is 'r53-b1td-bucket', without quotations.

```
15     "s3:GetObject",
16     "s3>DeleteObject"
17   ],
18   "Resource": "arn:aws:s3:::r53-b1td-bucket/*"
19 }
20 ]
21 }
22
```

15. Click the **Next** button located on the bottom right of the page.



16. On the *Review policy* page, perform the following steps:

- Give the policy a **Name**.

Policy name

Enter a meaningful name to identify this policy.

Maximum 128 characters. Use alphanumeric and '+=, @-_' characters.

- (Optional) If desired, give the policy a **Description**.

Description - optional

Add a short explanation for this policy.

Maximum 1,000 characters. Use alphanumeric and '+=, @-_' characters.

- (Optional) If desired, add tags via the **Add tag** button.

Add tags (Optional)

Tags are key-value pairs that you can add to AWS resources to help identify, organize, or search for resources.

No tags associated with the resource.

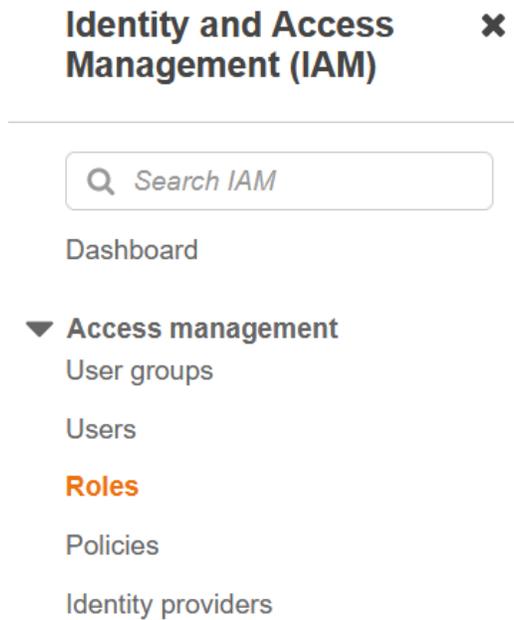
- Click the **Create policy** button located on the bottom right of the page to confirm the creation of the Policy.

Cancel

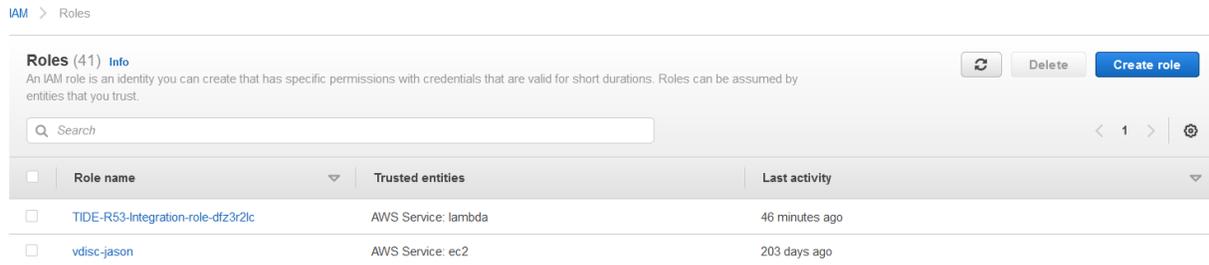
Previous

Create policy

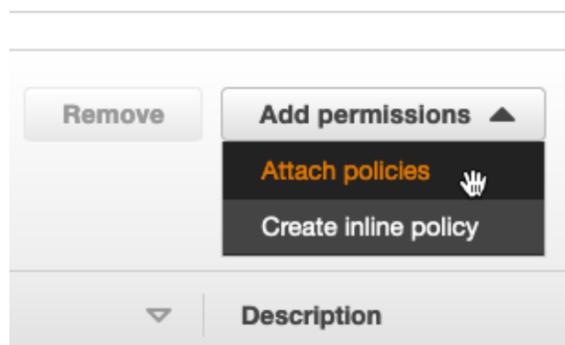
17. In the IAM navigation pane, click **Roles** located under the *Access management* header.



18. On the Roles page, locate and **click** the role that has been automatically created for your lambda function. *Note the role should contain the Lambda function's name in it. In the example screenshot, the Role name is Tide-R53-Integration-role-dfz32r2lc.*



19. On the role's *Summary* page, click the **Add permissions** button, then click the **Attach policies** button located in the list that is revealed.



20. Locate the two policies created earlier in this section. Click the **checkbox** associated with both Policies.



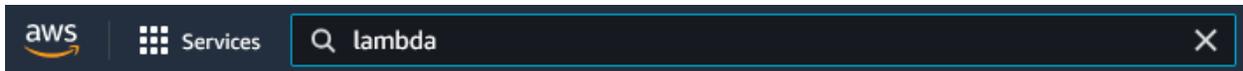
21. Click **Add permissions** to confirm the attaching of the two policies.



Test the Lambda Script

In order to test the lambda script, perform the following steps:

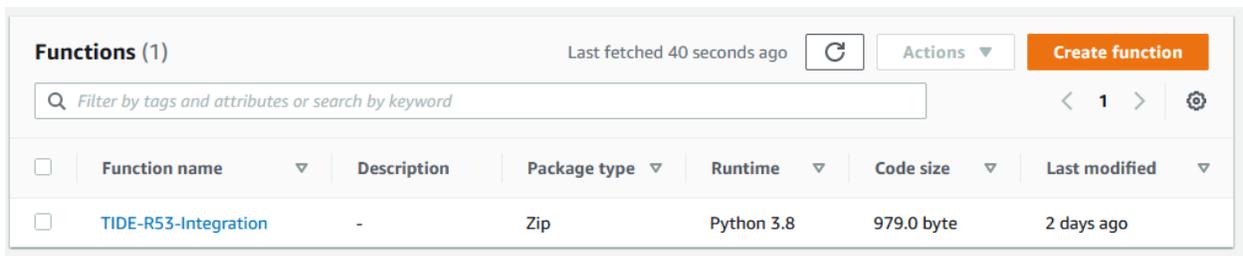
1. Input **Lambda** into the *search bar* located at the top of the AWS interface.



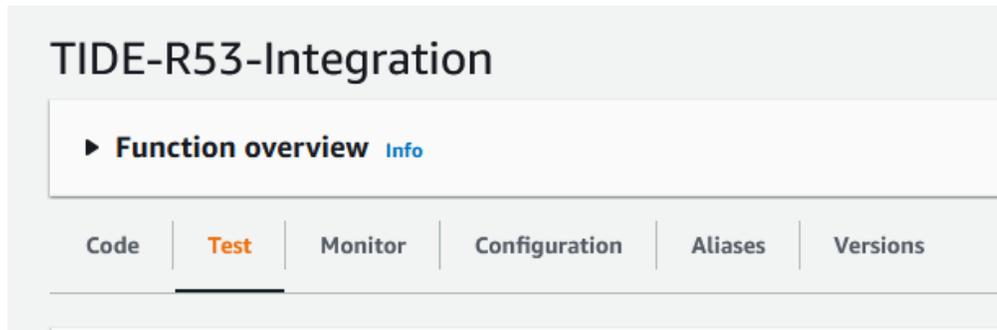
2. Locate and click on **Lambda** to navigate to the *Lambda* page.



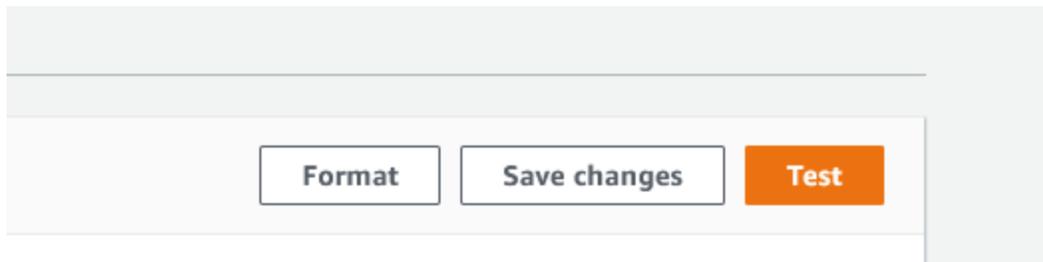
3. On the *Functions* page, locate and click the **Lambda function** you've just created.



- Click the **Test** tab located near the top of the function's page.



- Click the **Test** button located on the top left of the Test event panel.



- Above the Test event panel, the *Execution results* will show. Click the **Details** arrow to observe the details of the test.

Execution result: succeeded (logs)

▼ Details

The area below shows the result returned by your function execution. [Learn more](#) about returning results from your function.

```
{
  "statusCode": 200,
  "body": "Life is good"
}
```

Summary

Code SHA-256	Request ID
u3Djq2I7IaUTYvh0GeQahOdi77QQW8xfQXTJZ3px0Y=	59bb5fa3-8a75-4a42-86cd-c323a59a68d4
Init duration	Duration
358.34 ms	931.75 ms
Billed duration	Resources configured
932 ms	128 MB
Max memory used	
72 MB	

Log output

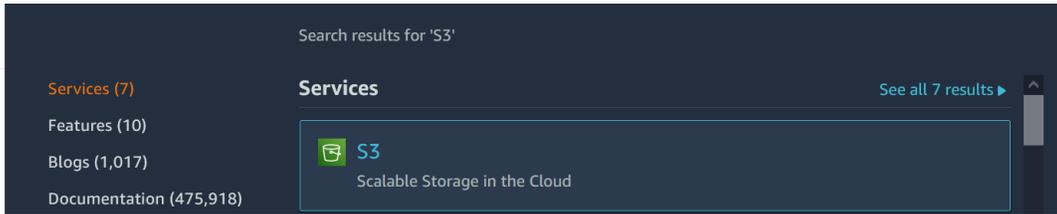
The section below shows the logging calls in your code. [Click here](#) to view the corresponding CloudWatch log group.

```
START RequestId: 59bb5fa3-8a75-4a42-86cd-c323a59a68d4 Version: $LATEST
s3://r53-bitd-bucket/MyIOCS.txt
INFO:botoecore.credentials:Found credentials in environment variables.
{"Id": "r53vnr-fd1-879a580ca13641a3",
 "Name": "R53-BITD-GUIDE-Domain-List",
 "ResponseMetadata": {"HTTPHeaders": {"connection": "keep-alive",
 "content-length": "148",
 "content-type": "application/x-amz-json-1.1",
 "date": "Mon, 10 Jan 2022 20:56:06 GMT",
 "x-amzn-requestid": "feedd4e6-5e54-4399-9506-2e1d4c028b5e"},
 "HTTPStatusCode": 200,
```

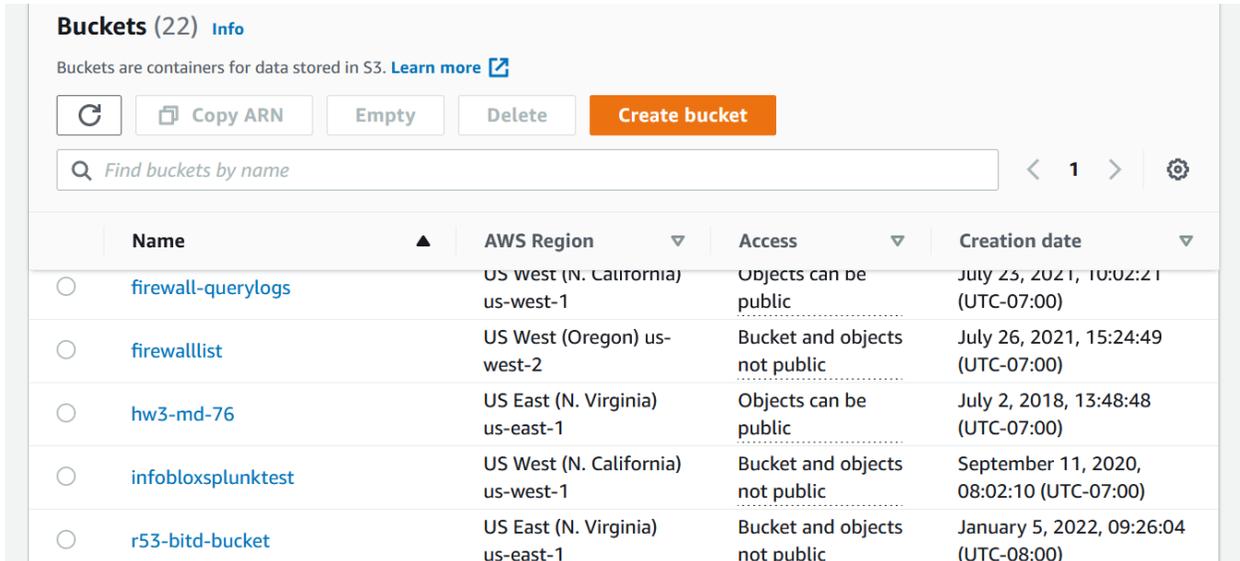
- Navigate to the simple text file that holds the IOCs before they are added to the AWS R53 DNSFW domain list. Input **S3** into the *search bar* located at the top of the AWS interface.



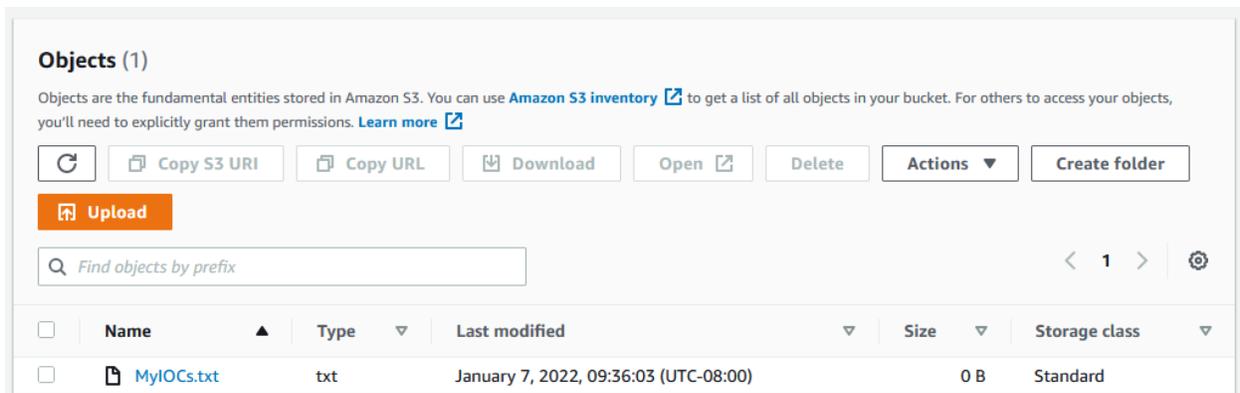
8. Locate and click on **S3** to navigate to the *Amazon S3* page.



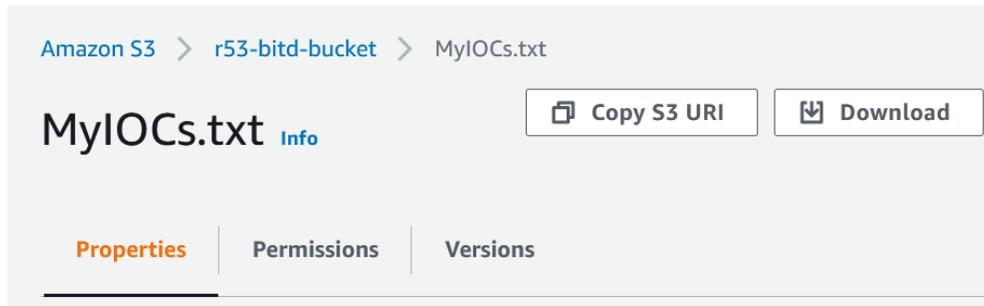
9. On the *Buckets* page, scroll down to the Buckets panel. Locate and click on the **S3 bucket** that is being used with this integration.



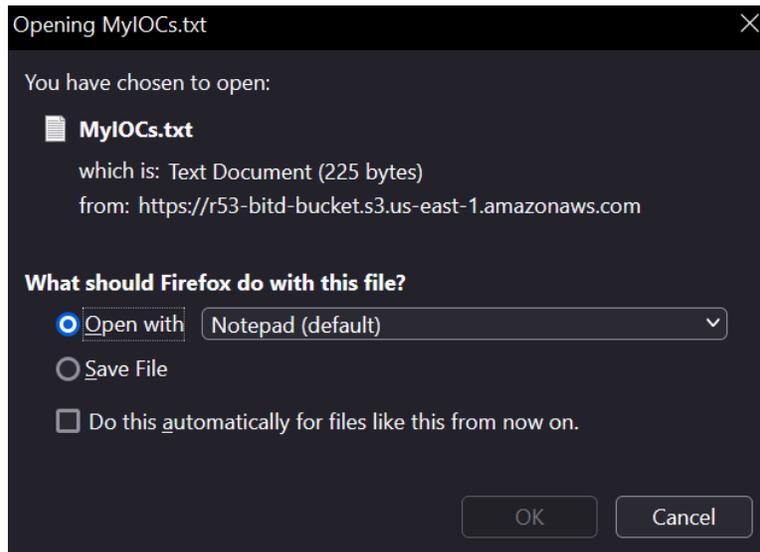
10. In the Objects panel, locate and **click** the simple text file that was created for this integration. *Note, in the example screenshot, the file's name is MyIOCs.txt.*



11. On the text file's page, click the **Download** button located near the top of the page.



12. **Save, or Open** the file in the prompt that is revealed.



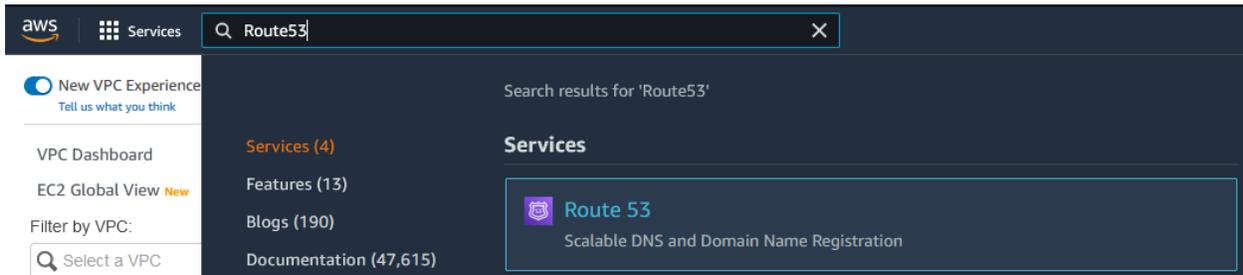
- o Observe the contents of the text file. As mentioned earlier in the guide, IOCs should be one per line.

```
MyIOCs-4.txt - Notepad
File Edit Format View Help
changway.hk
setupoldnavy.space
compromiseddomain.eicar.network
apt.eicar.network
sinkhole.eicar.network
maliciousnameserver.eicar.network
shoshanna.at
malwarec2.eicar.network
webappattack.eicar.network
phishing.eicar.network
```

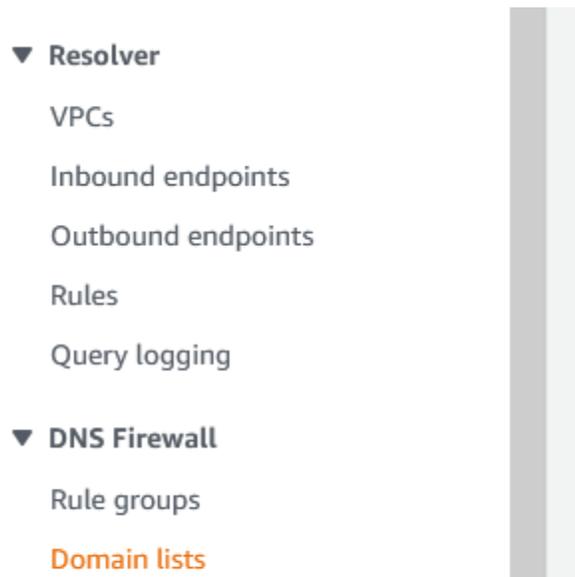
13. To observe the IOCs added to your AWS Route 53 DNS Firewall domain list via the test, navigate to the Route 53 page. input **Route53** into the *search bar* located at the top of the AWS interface.



14. Click the text **Route 53** in the list that is revealed.



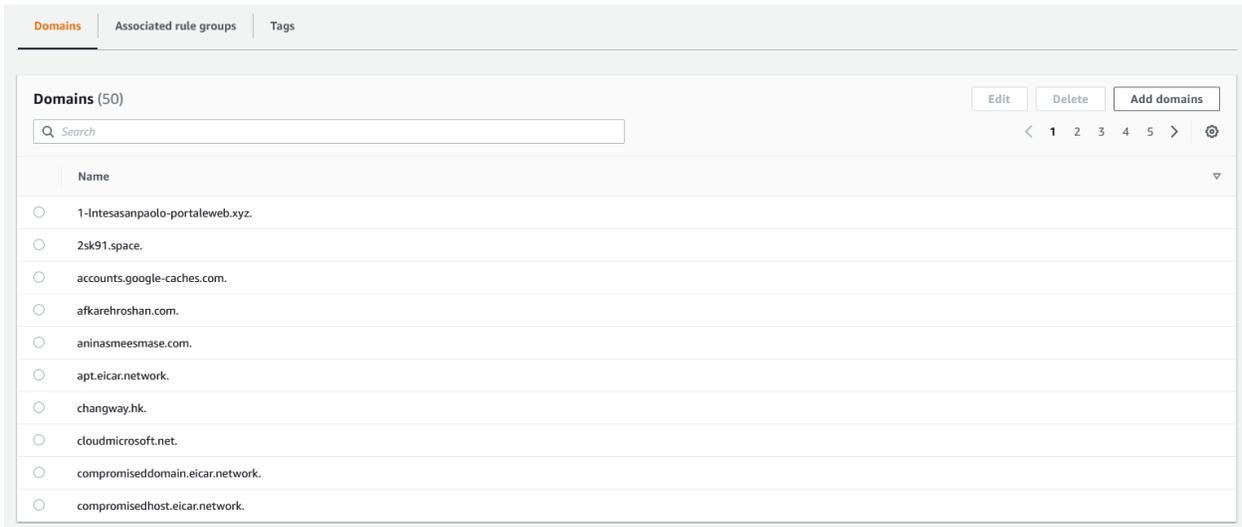
15. In the *Route 53 navigation pane*, click **Domain List** located under the *DNS Firewall* header.



16. On the *Domain Lists* page, in the *Owned domain lists* panel locate and click on the Domain list you added in the previous section.



- o In the *Domains* panel observe the newly added domains



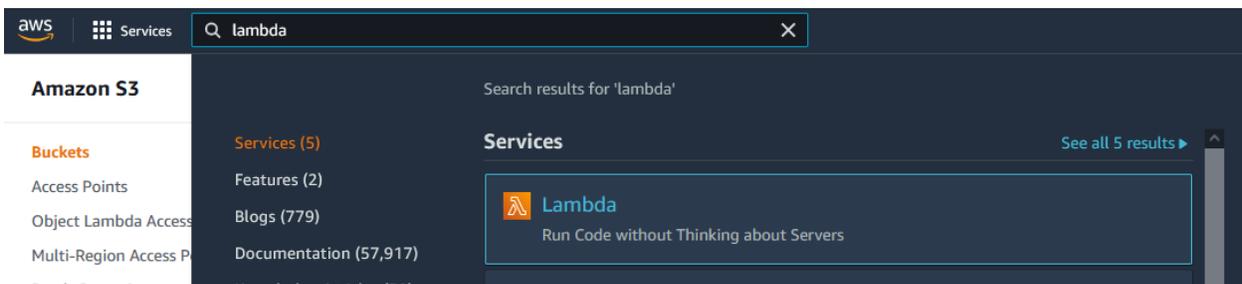
Automate the script execution via EventBridge

To automate the importing of IOCs from Infoblox an EventBridge can be used. This allows for the ingestion of IOCs from Infoblox via the Python script to occur on a schedule. To configure an Amazon EventBridge, perform the following steps:

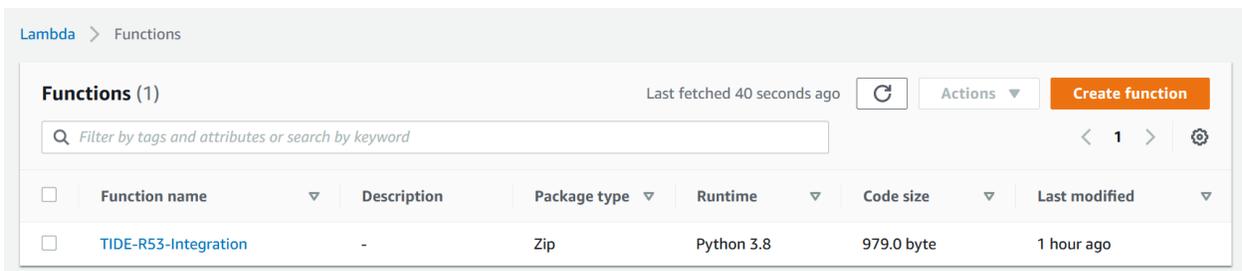
1. Input **Lambda** into the *search bar* located at the top of the AWS interface.



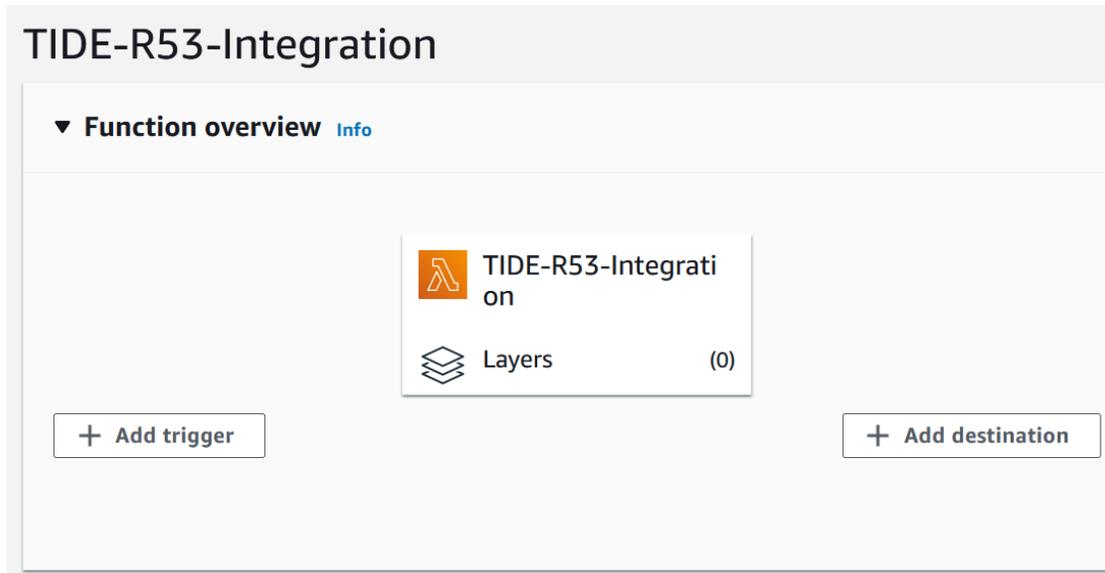
2. Locate and click on **Lambda** to navigate to the *Lambda* page.



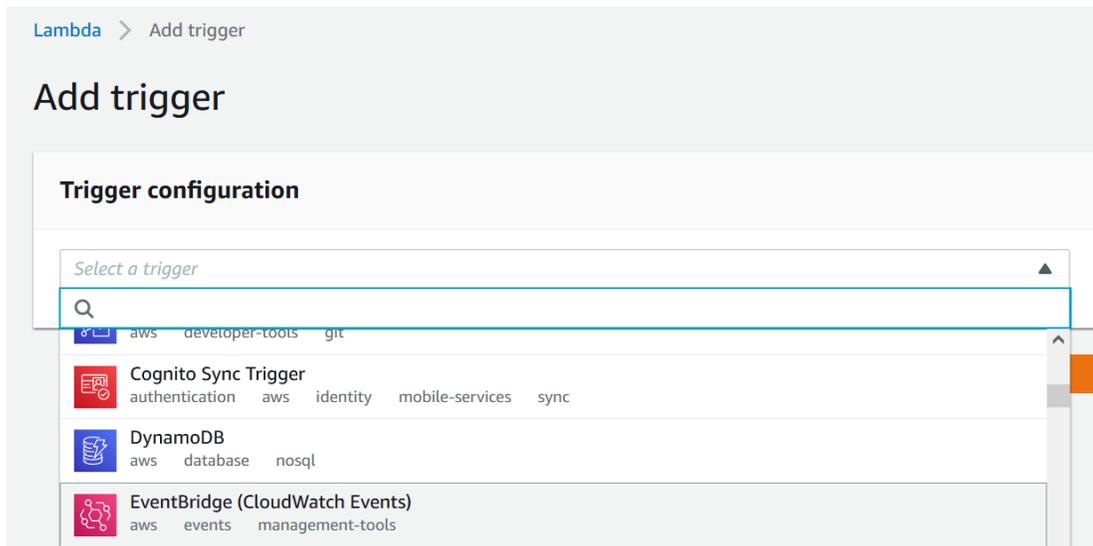
3. Locate and **click** the Lambda function that was created in the previous section.



4. In the *Function overview* panel of the function's page, click the **Add trigger** button



5. On the **Add trigger** page, perform the following steps:
 - Select **EventBridge** from the Select a trigger drop-down menu located in the Trigger configuration panel



- Under the Rule header, click the **Create a new rule** bubble.

Rule

Pick an existing rule, or create a new one.

- Create a new rule
- Existing rules

- Give the Rule a **name**.

Rule name*

Enter a name to uniquely identify your rule.

TIDE-Sync

- (Optional) If desired, give the rule a **description**.

Rule description

Provide an optional description for your rule.

- Under the Rule type header, click the **Schedule expression** bubble.

Rule type

Trigger your target based on an event pattern, or based on an automated schedule.

- Event pattern
- Schedule expression

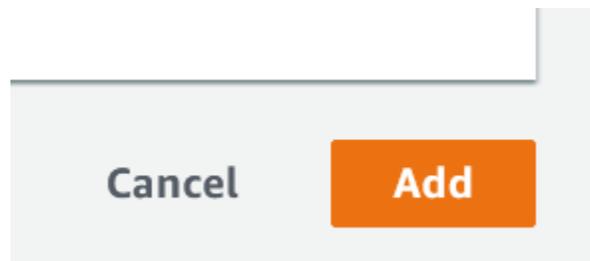
- In the Schedule expression text panel, input a **Cron** or **Rate** expression. *Note, for more information about the accepted input types, see the AWS documentation [here](#).*

Schedule expression*

Self-trigger your target on an automated schedule using Cron or rate expressions. Cron expressions are in UTC.

cron(0/30 * * * ? *)

- Click **Add** to confirm the addition of the trigger.





Infoblox unites networking and security to deliver unmatched performance and protection. Trusted by Fortune 100 companies and emerging innovators, we provide real-time visibility and control over who and what connects to your network, so your organization runs faster and stops threats earlier.

Corporate Headquarters
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054
+1.408.986.4000
www.infoblox.com