Deployment Guide

Integrating BloxOne™ Threat Defense with AWS' Route 53

Table of Contents

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.

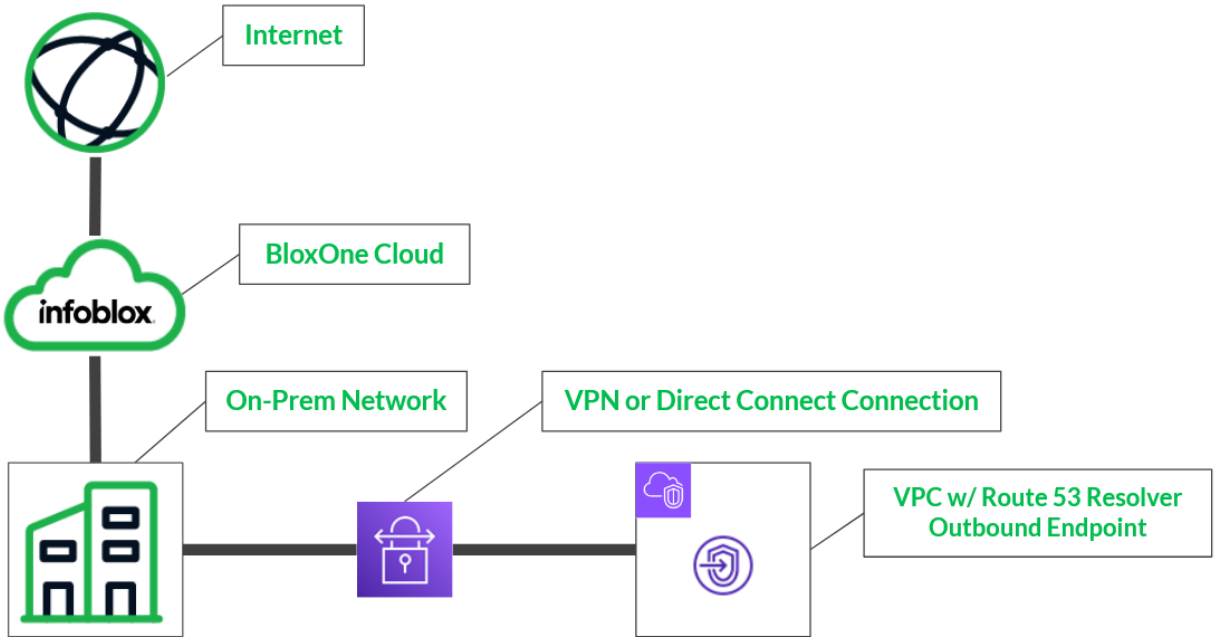
1. Create or identify VPC to use
    a. (Optional) Create a NAT Gateway
2. Locate the required IP for BloxOne from one of the following:
    a. VPN connection
    b. NAT rule
    c. AWS Direct Connect connection
3. Create a Route 53 Outbound Endpoint
4. Create a Route 53 Resolver rule
5. Create an External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

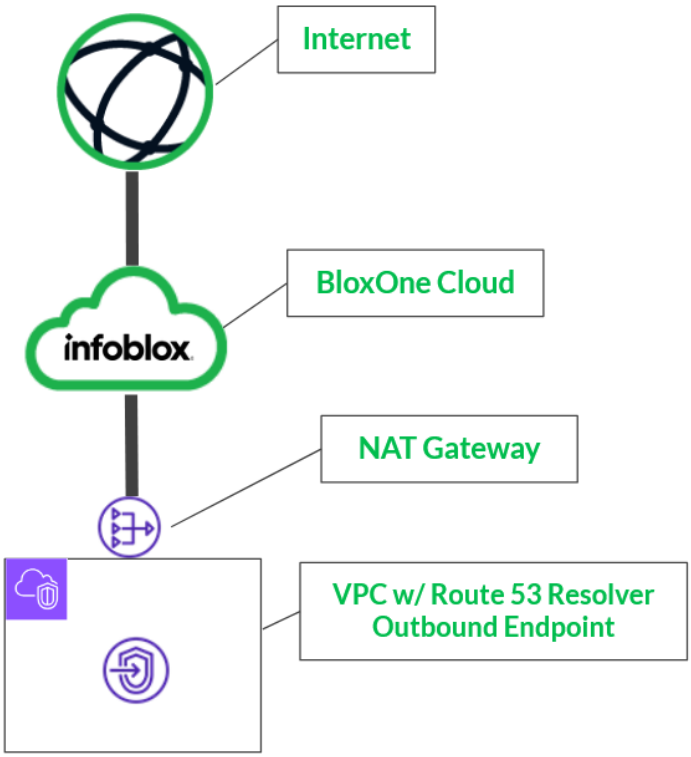


VPN or Direct Connect Connection External IP

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:

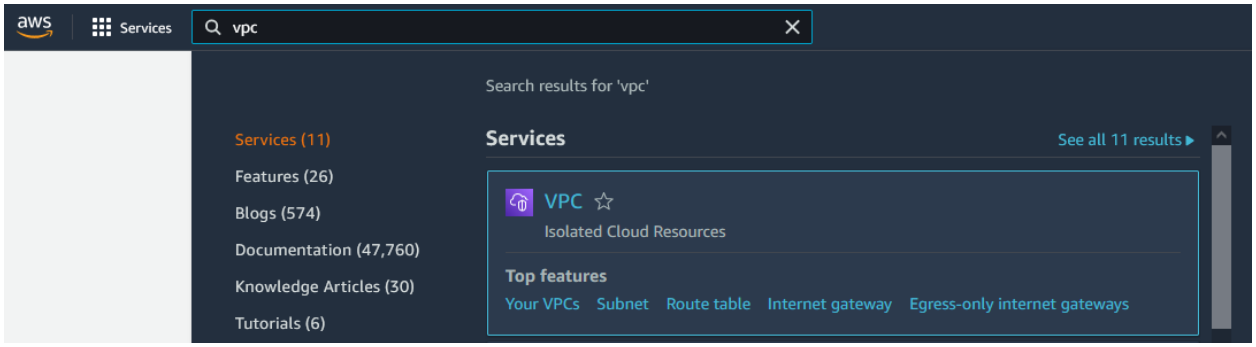


Create a VPC

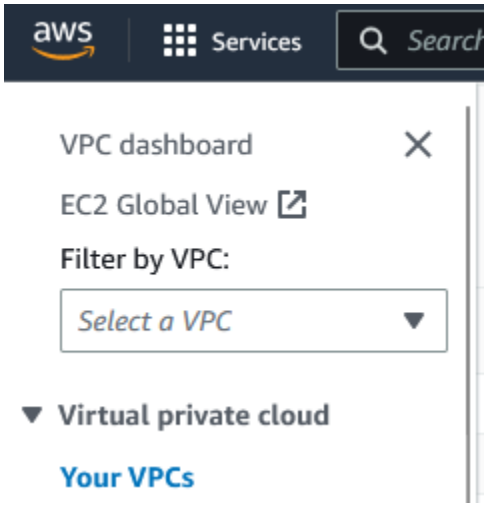
This is an optional step to configure a VPC, if you have already identified a VPC that you intend to use with this integration, please skip this step. In order to create a VPC, perform the following steps:

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

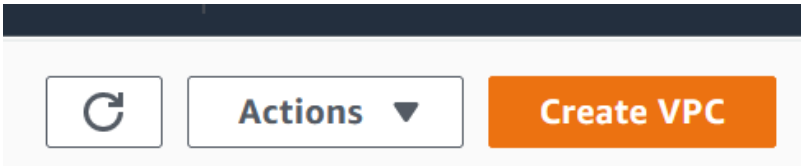
2. Click the text **VPC** in the list that is revealed.



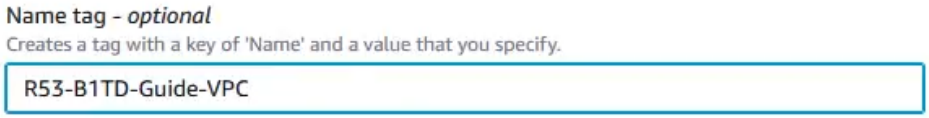
3. On the *VPC* page, click **Your VPCs** in the left navigation panel.



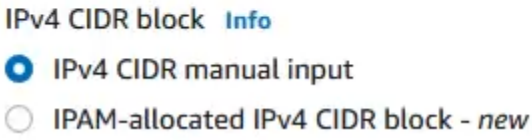
4. On the top right of the *Your VPCs* page, click the **Create VPC** button.



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

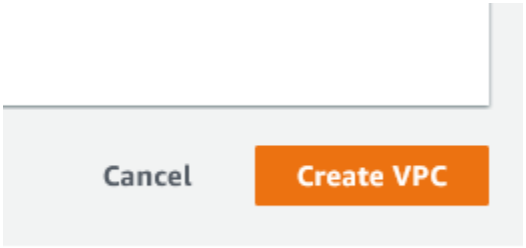


    - Under the *IPv4 CIDR block* header, click the I**Pv4 CIDR manual input** bubble.



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

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

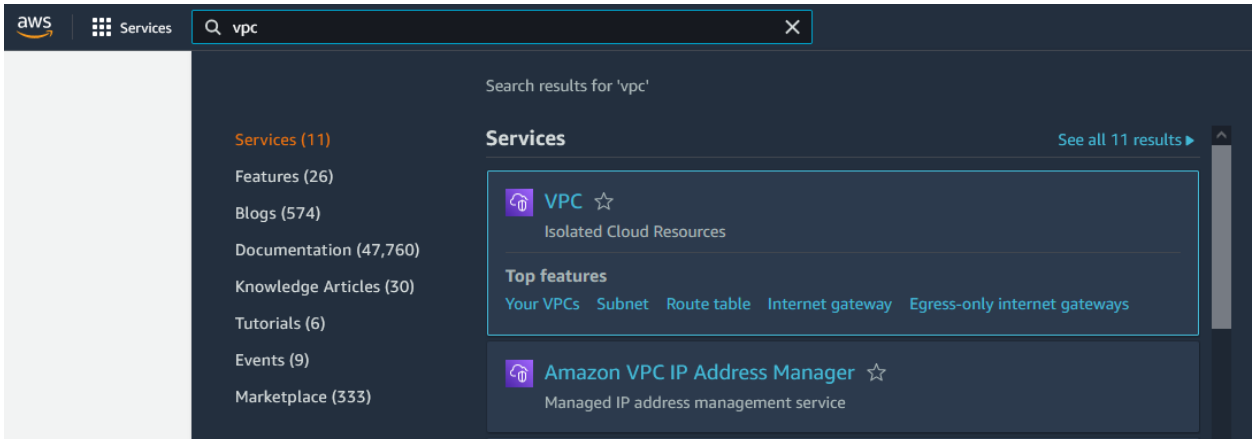


Configure Subnets

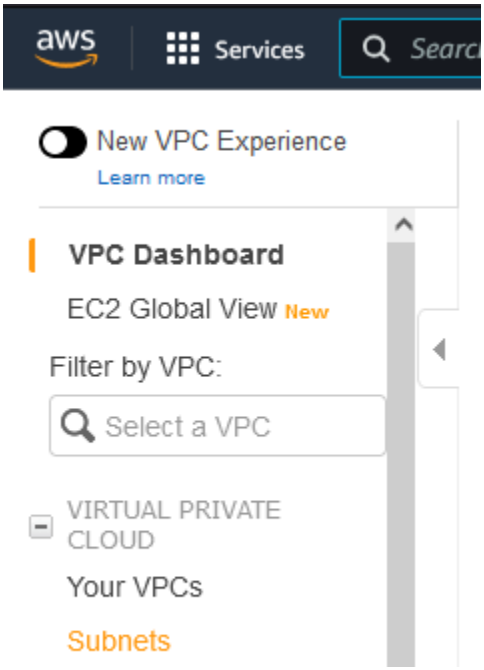
To configure a NAT gateway, you will need a Private and Public subnet. To create these subnets, perform the following steps:

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

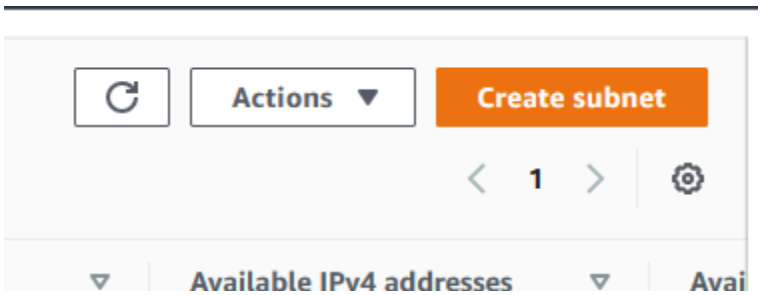
2. Click the text **VPC** in the list that is revealed.



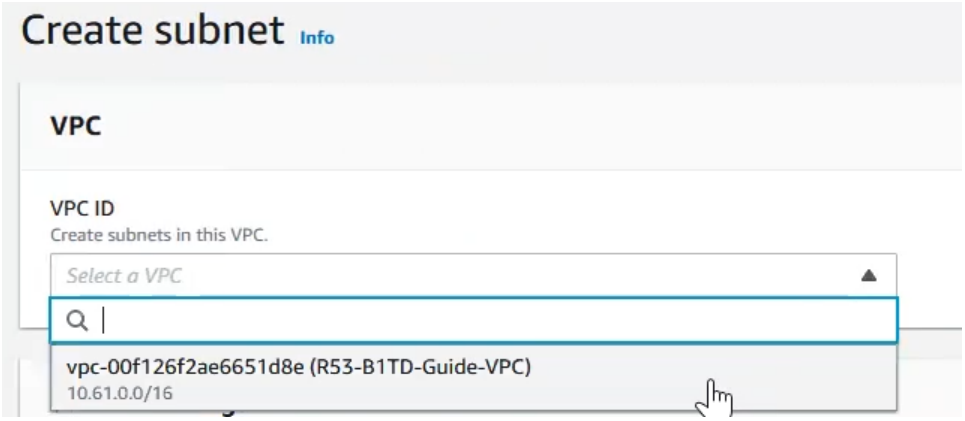
3. In the left navigation panel of the VPC page, click **Subnets**.



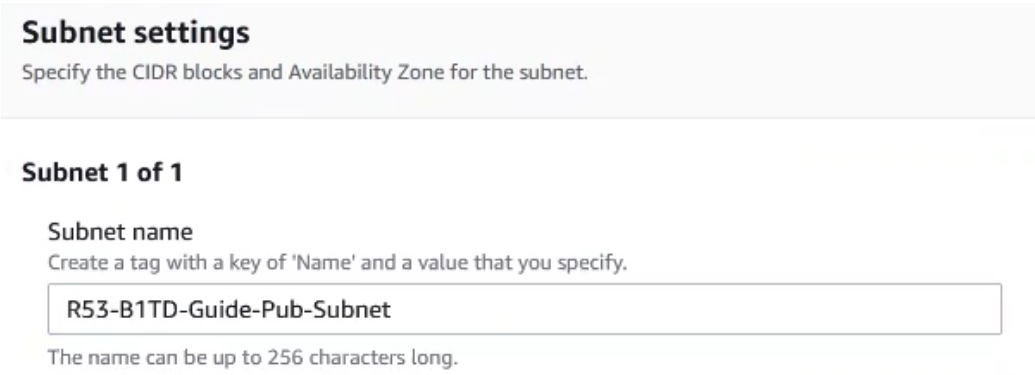
4. Click the **Create subnet** button located on the top right of the *Subnets* page. *Note that this will be a public subnet intended for external traffic via the NAT Gateway.*



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



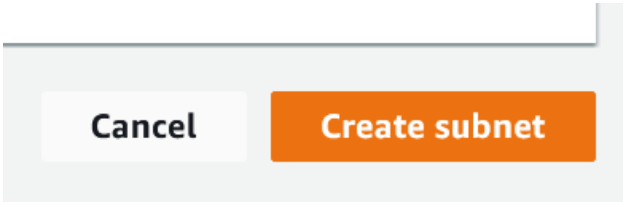
- In the Subnet settings panel that is revealed, input a **Subnet name.**



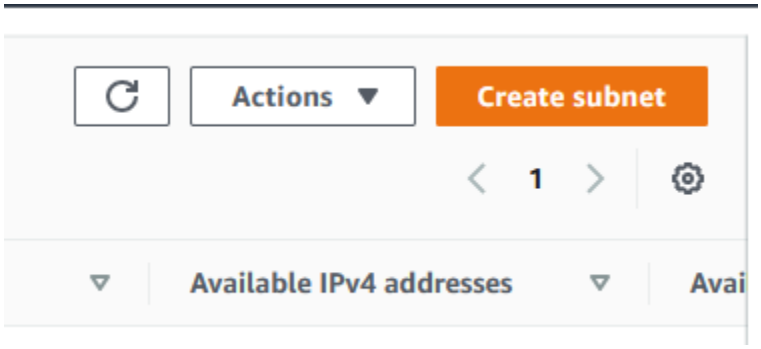
- Select an **Availability Zone** via the Availability Zone dropdown menu.

- 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.*

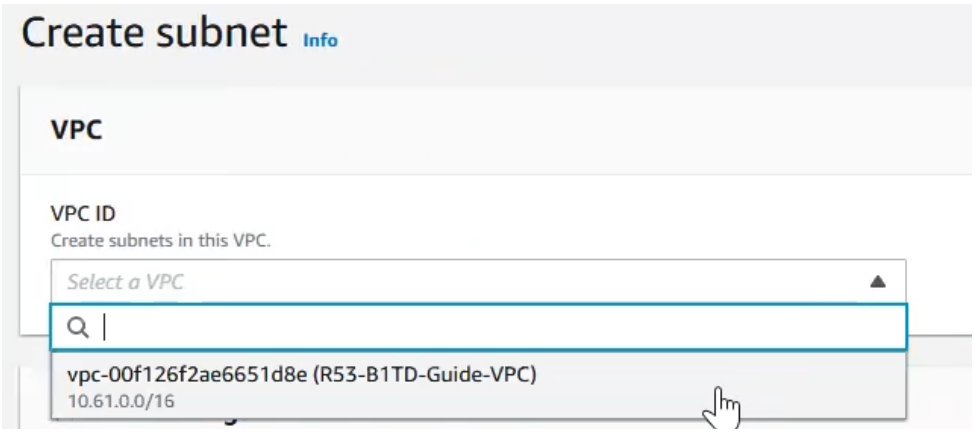
- Click **Create subnet** to confirm the creation of the subnet.



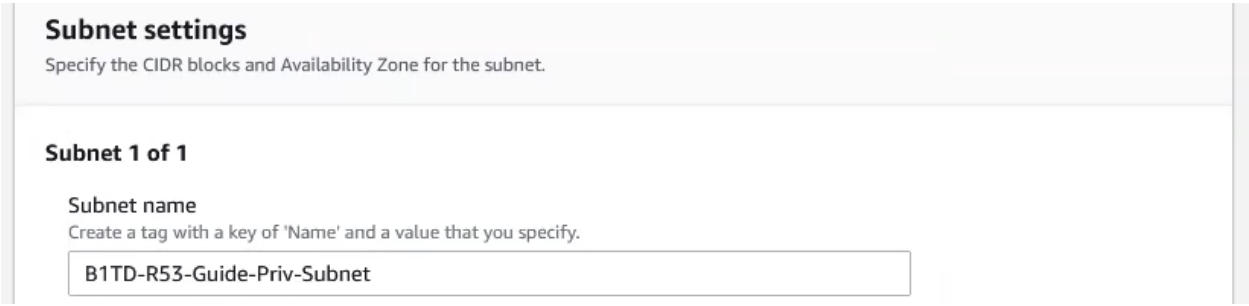
6. Click the **Create subnet** button located on the top right of the Subnets page. *Note that this will be a private subnet intended for internal traffic.*



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



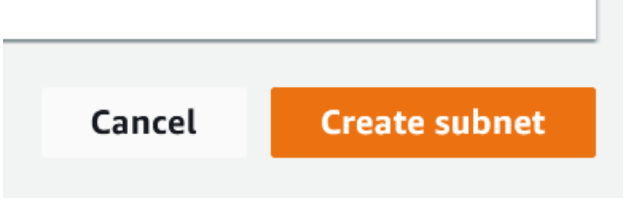
    - In the Subnet settings panel that is revealed, input a **Subnet name.**



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

    - 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.*

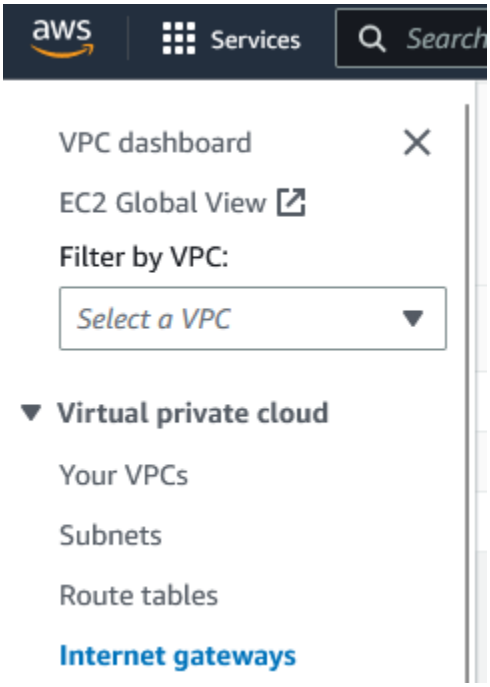
    - Click **Create subnet** to confirm the creation of the subnet.



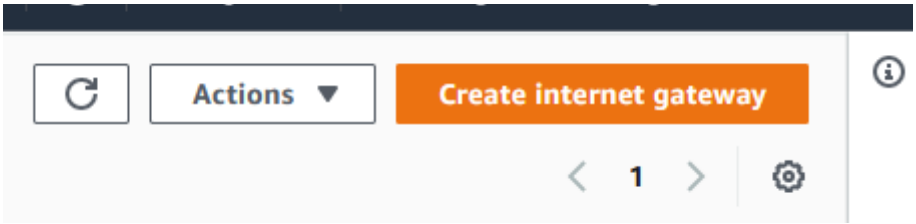
Create Internet Gateway

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:

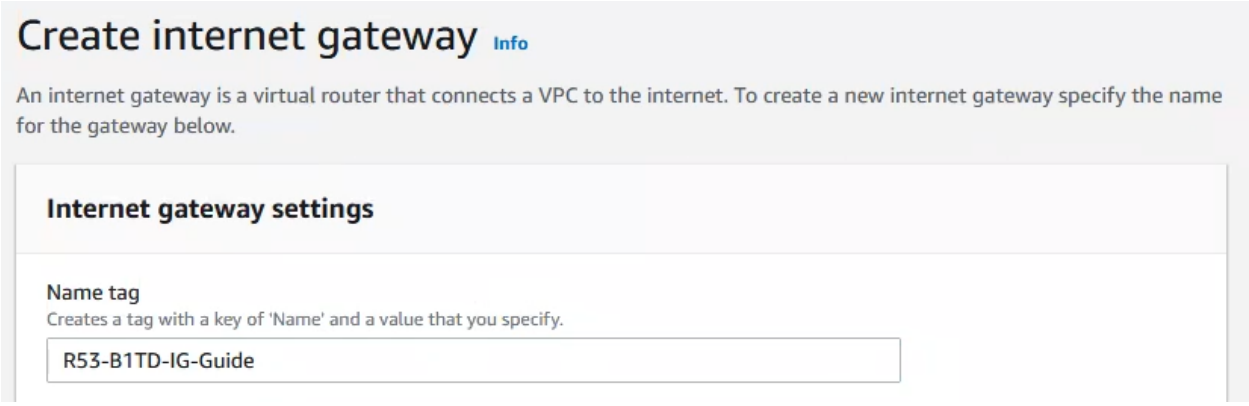
1. In the left navigation panel of the Subnets page, click **Internet Gateways**.



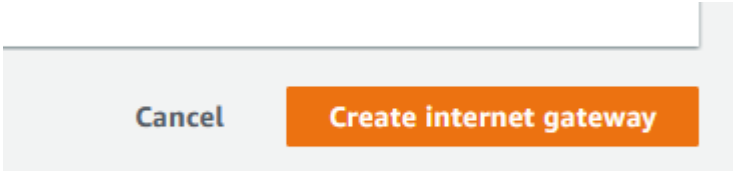
2. On the **Internet Gateways** page, click **Create internet gateway**.



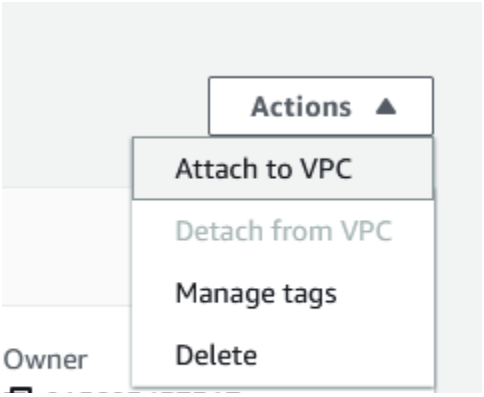
3. On the Create internet gateway page, input a **Name tag**.



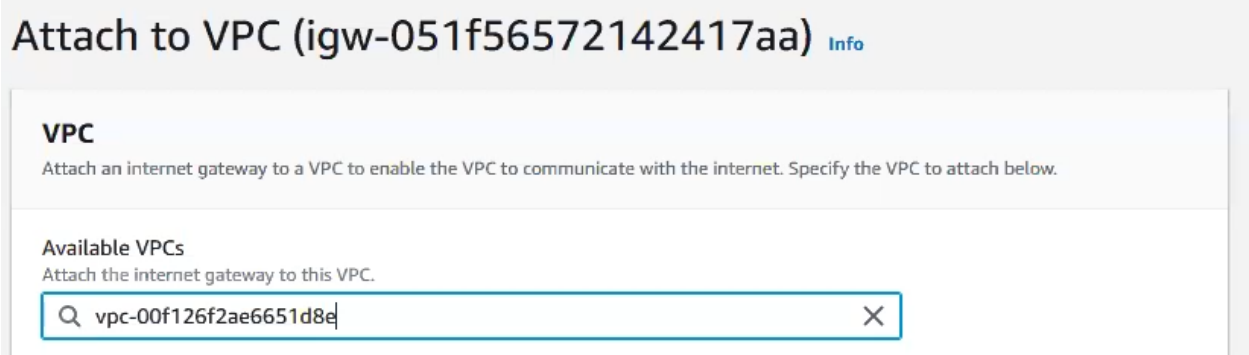
4. Click **Create internet gateway** to confirm the creation of the Internet Gateway.



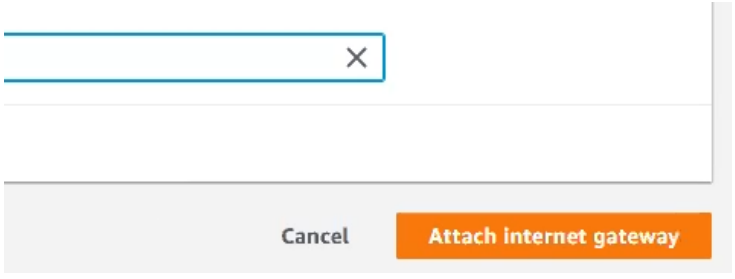
5. Once on the newly created Internet Gateway's page, click the **Actions** button. Then, click **Attach to VPC**.



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



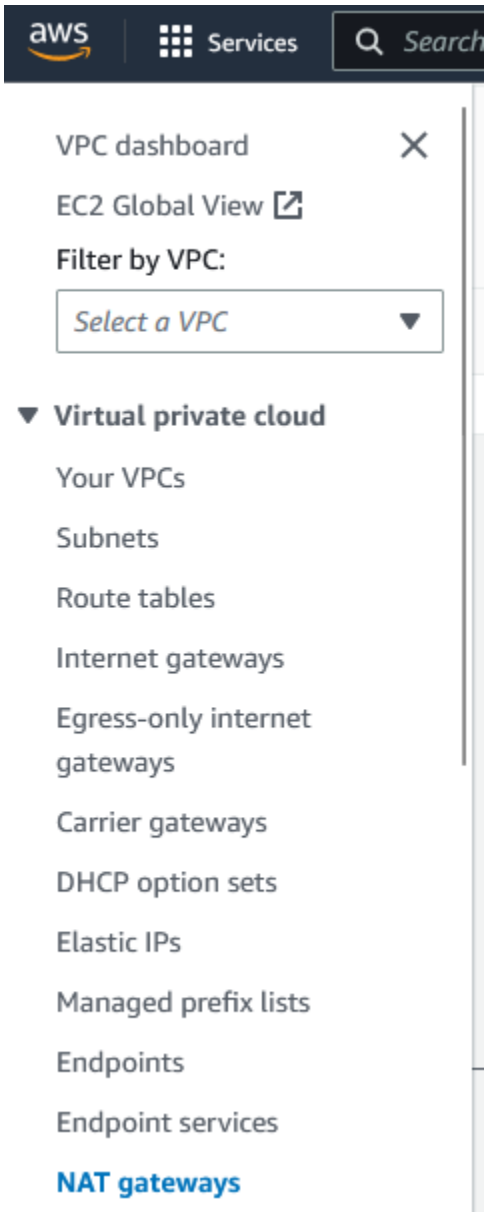
7. Click the **Attach internet gateway** button to confirm the operation.



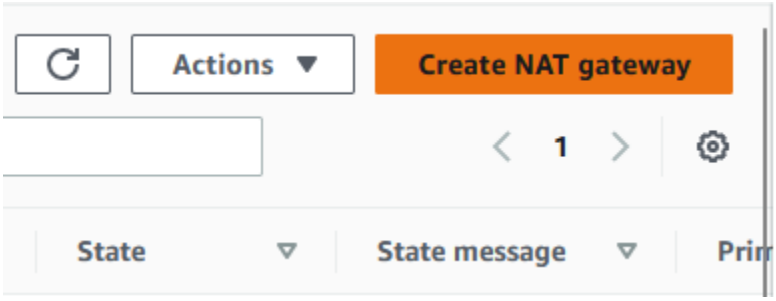
Create a NAT Gateway

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

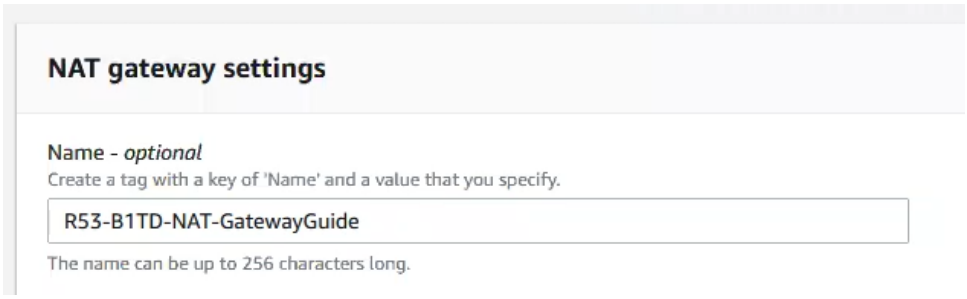
1. In the left navigation panel of the Internet Gateways page, click **NAT Gateways**.



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

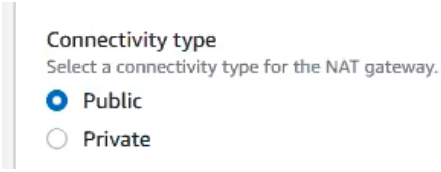


3. On the NAT gateway settings page perform the following steps:
    - Input a **Name**.



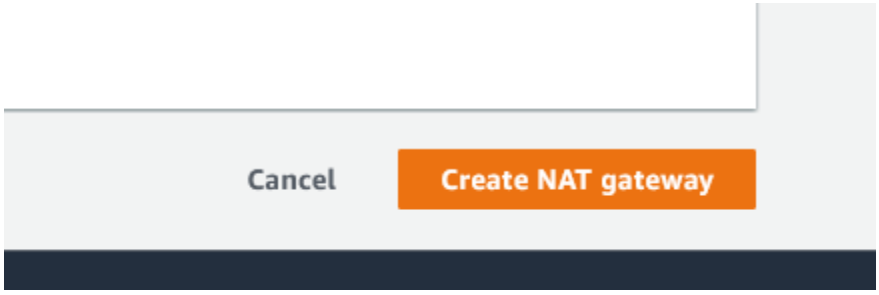
    - Select the **Public subnet** that was created earlier in this guide via the **Subnet** dropdown.

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

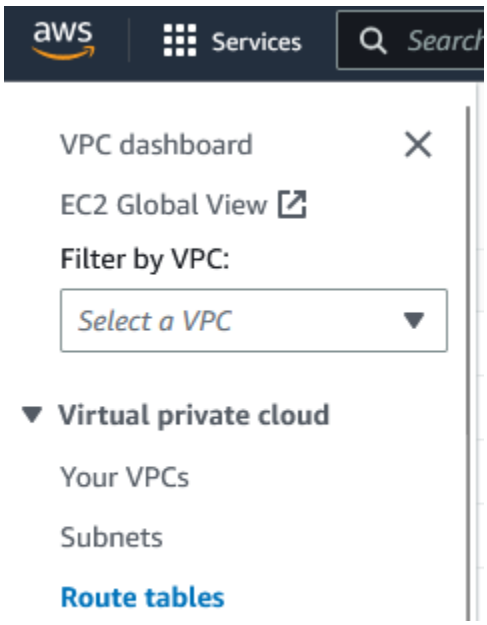


    - Select an existing Elastic IP via the **Elastic IP allocation ID dropdown** or allocate a new Elastic IP via the **Allocate Elastic IP** button.

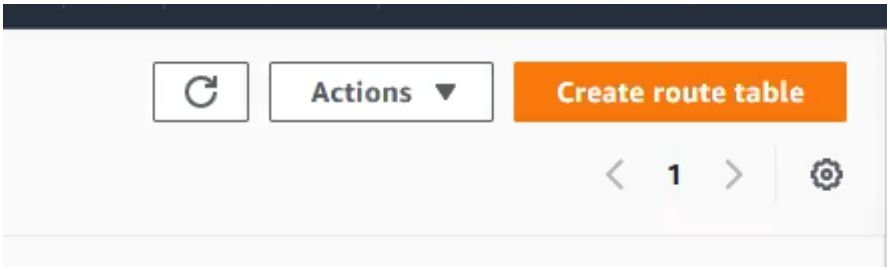
- Click **Create NAT gateway** to confirm the creation of the NAT gateway.



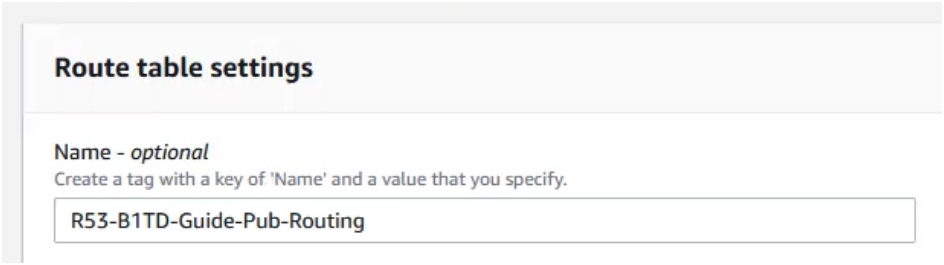
4. In the left navigation panel of the Nat Gateways page, click **Route Tables**.



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**.



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

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

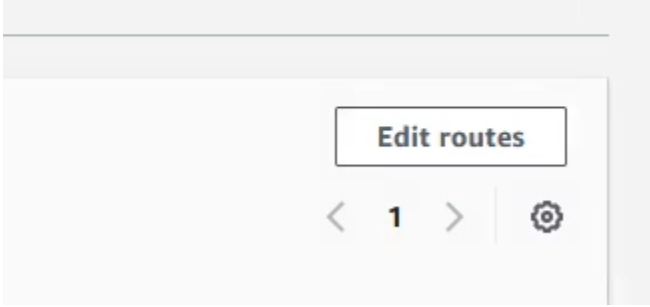
9. In the newly created *Route table*, click the **Subnet associations** tab located near the bottom of the page.

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

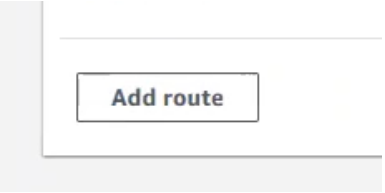
11. In the **Available subnets** panel, select the public subnet that was created earlier in this guide.

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.



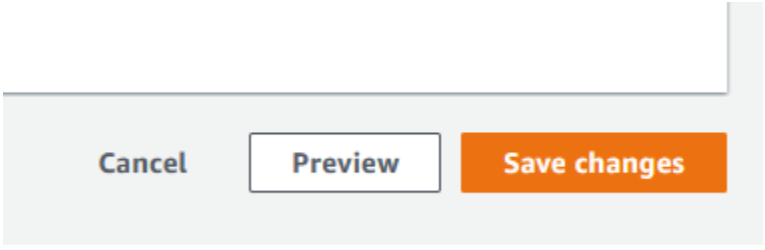
14. On the Edit routes page, click the **Add route** button.



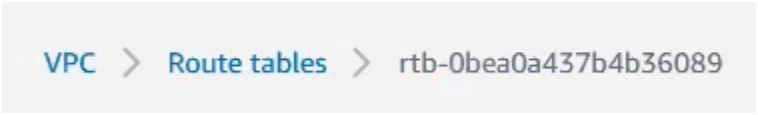
15. In the new route's *Destination* textbox, input the wildcard address **0.0.0.0/0**.

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

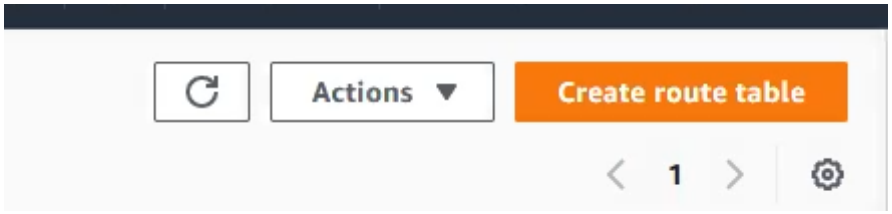
17. Click the **Save changes** button to confirm the changes to the routing table.



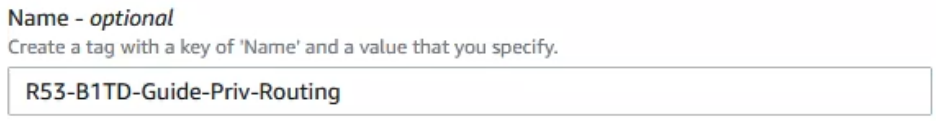
18. On the top of the *Route table's* page, click **Route tables** to return to the Route tables page.



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.*



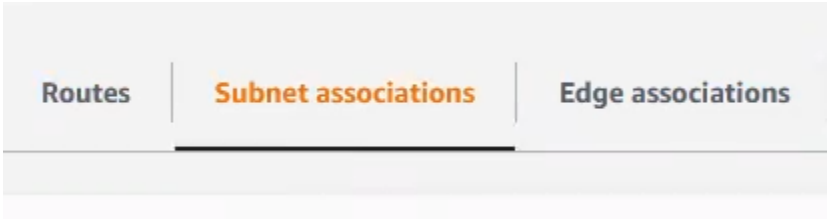
20. On the Create Route table page, give the Route table a **Name**.



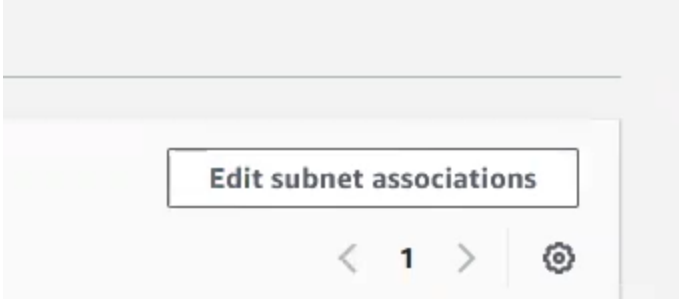
21. Then, assign the VPC that you created the subnets in on *pages 6-8*.

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

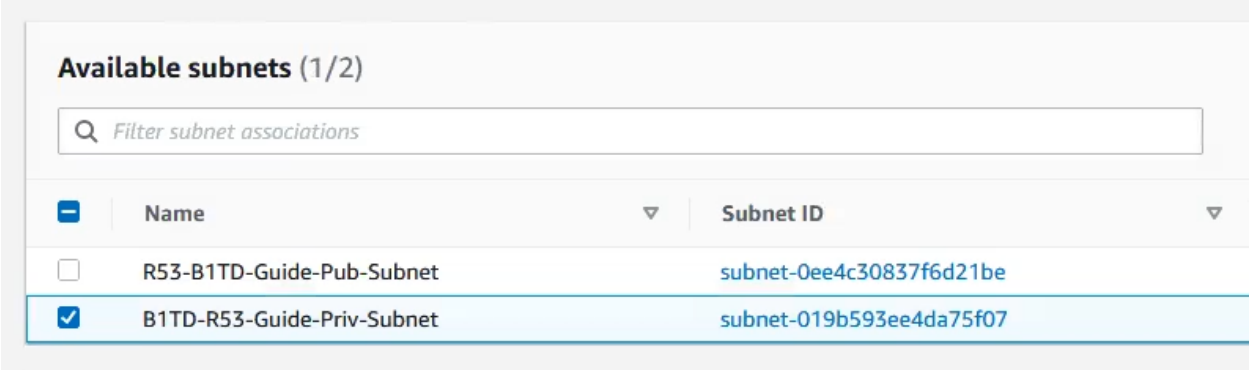
23. In the newly created *Route table*, click the **Subnet associations** tab located near the bottom of the page.



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

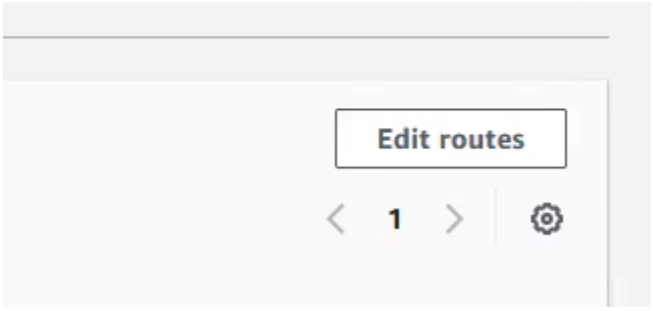


25. In the **Available subnets** panel, select the private subnet that was created earlier in the guide.

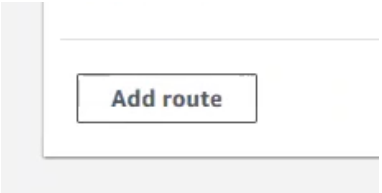


26. Click **Save association** to confirm the subnet association.

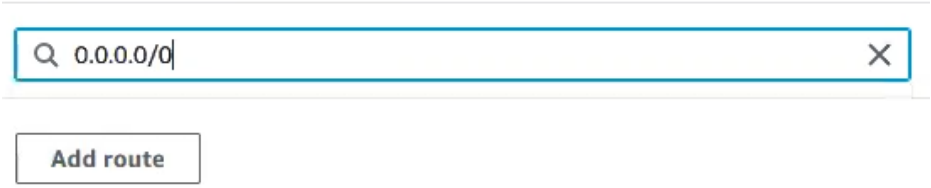
27. On the Route table's primary page, click **Edit routes** located in the Routes panel.



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

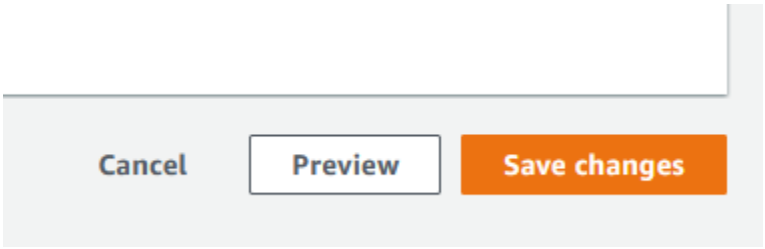


29. In the new route's *Destination* textbox, input the wildcard address **0.0.0.0/0**.

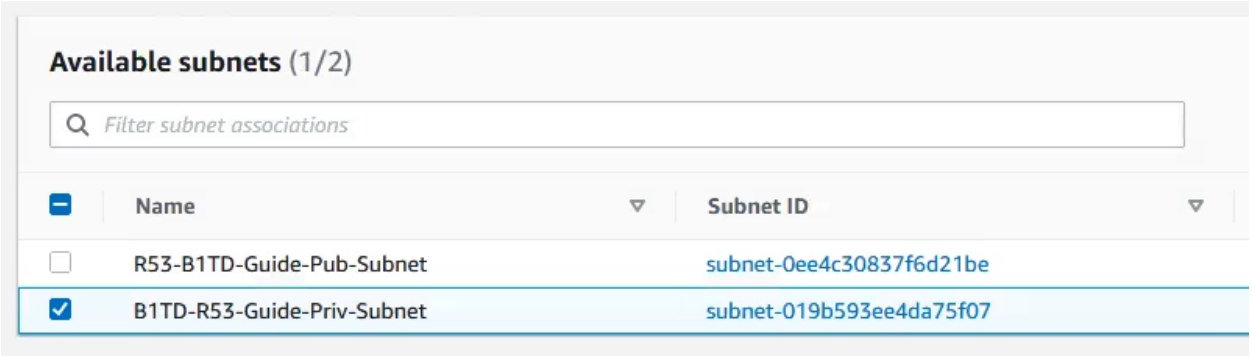


30. In the new route's *Target* textbox, input the ID of the **NAT Gateway** that was created earlier in this guide.

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



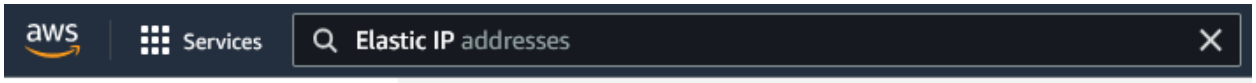
32. In the **Available subnets** panel, select the private subnet that was created on *pages 10-11*.



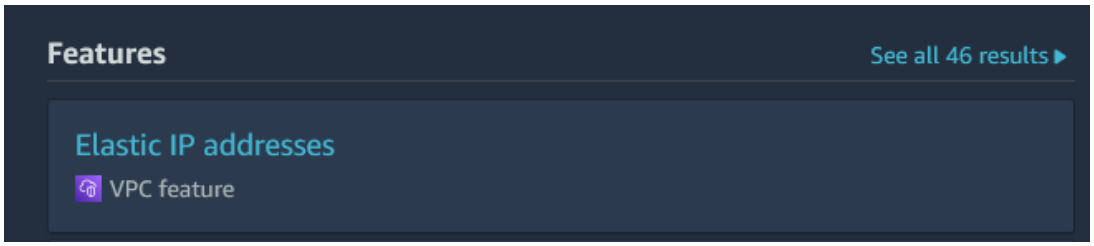
Acquire the public IP from the NAT Gateway

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

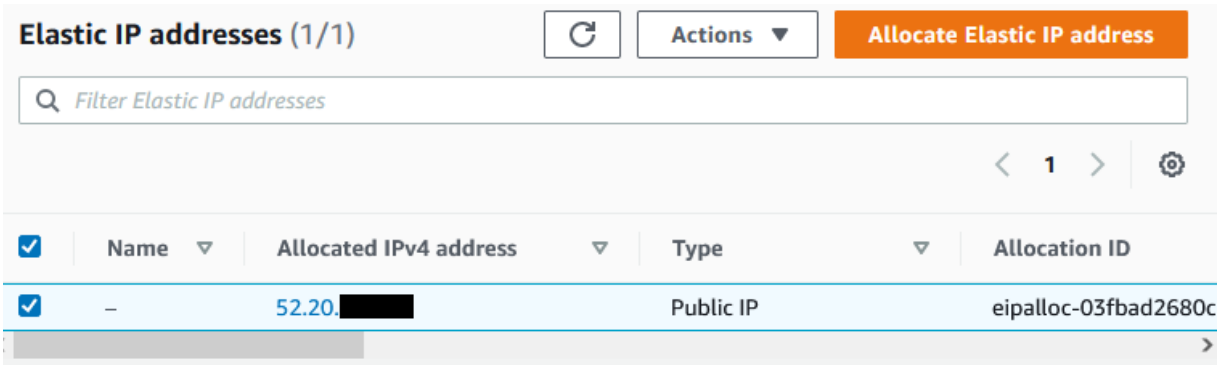
1. In the *AWS Management Console*, input **Elastic IP** into the search bar.



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



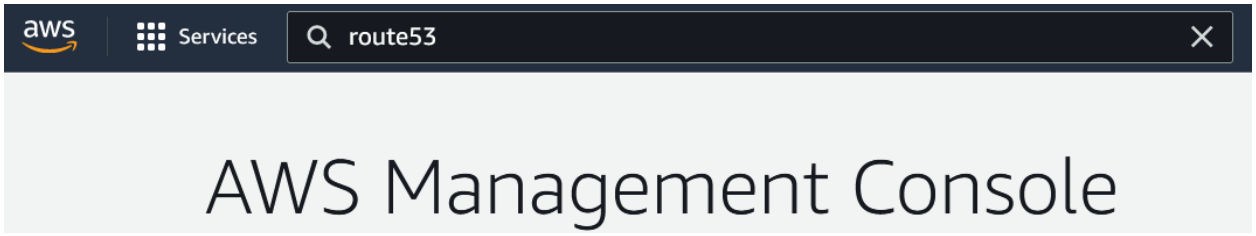
3. Once on the Elastic IP addresses page, locate the Elastic IP of the NAT Gateway you've configured for your VPC. Copy and **save** this IP to another location for use later. *Note: the IP will be located in the **Allocated IPv4 address** column.*



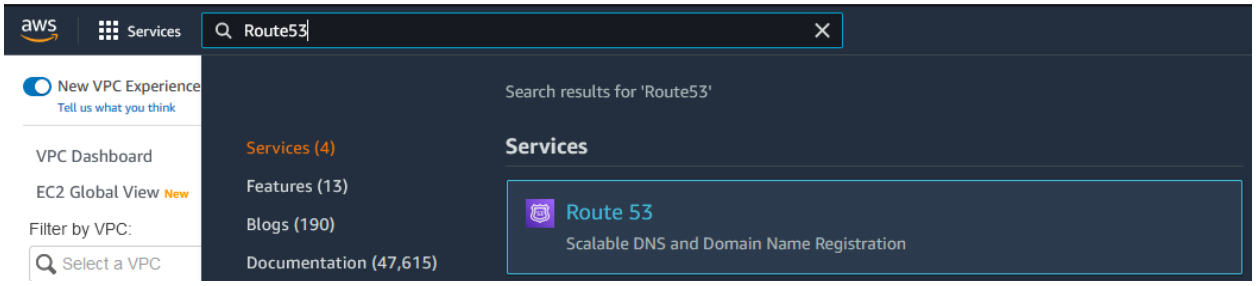
Create a Route53 Outbound Endpoint

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:

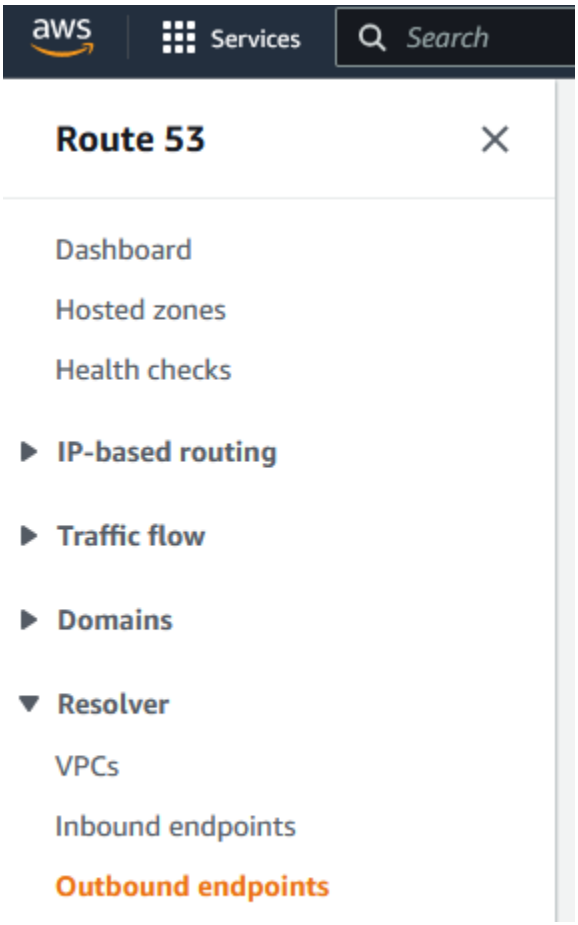
1. Log in to your AWS account. Once logged in, input **Route53** into the *search bar* located at the top of the AWS interface.



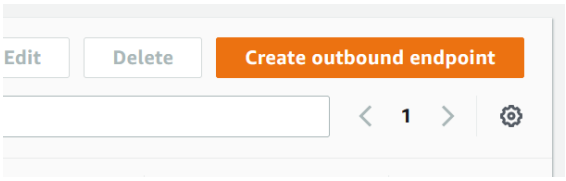
2. Click the text **Route 53** in the list that is revealed.



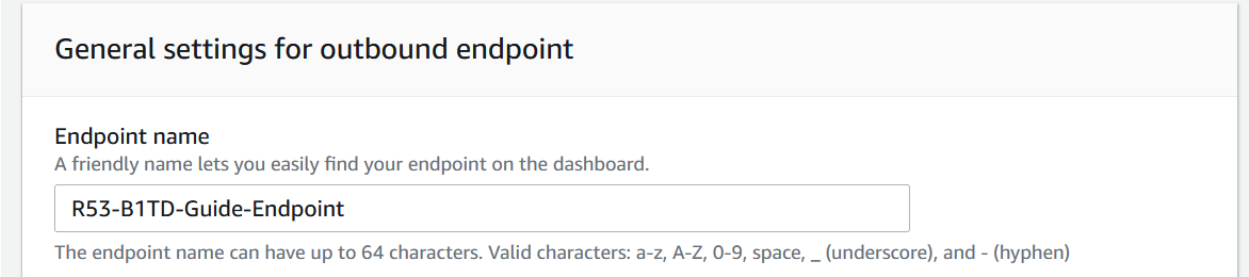
3. In the *Route 53 navigation pane*, click **Outbound endpoints** located under the *Resolver* header.



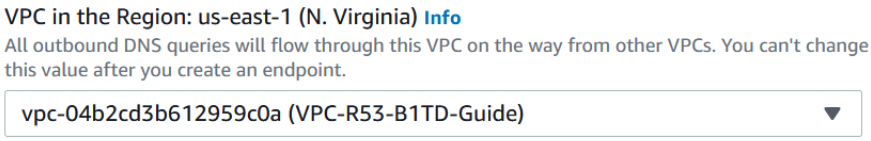
4. On the *Outbound endpoints* page, click **Create outbound endpoint**.



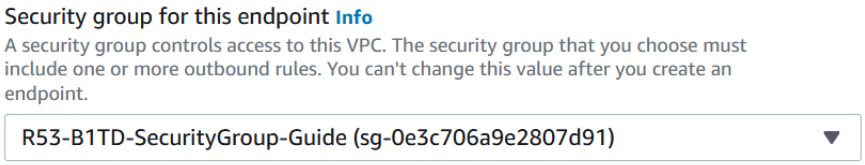
5. On the *Create outbound endpoint* page, input the following data:
    - Give the Outbound Endpoint a **Name**.



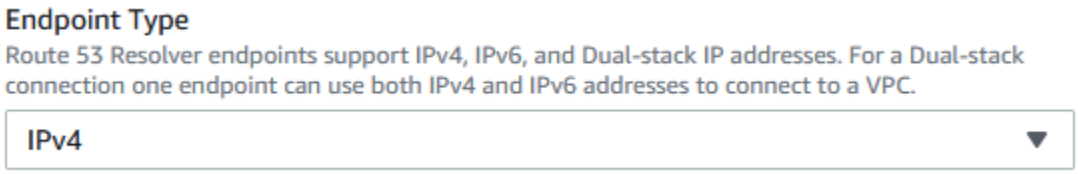
    - Select the **VPC** you would like to associate with the Outbound Endpoint via the dropdown.



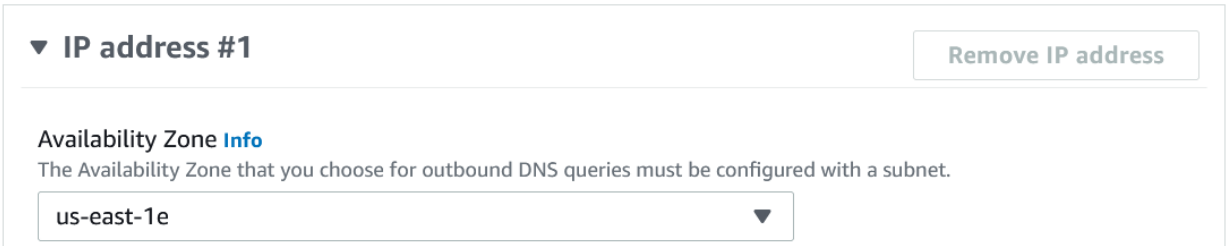
    - Select the **Security group** you would like to associate with this Outbound Endpoint by using the dropdown.



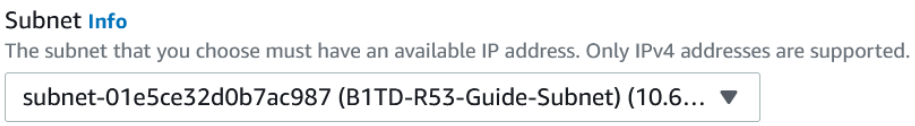
    - Select **IPv4** as the Endpoint Type via the dropdown.



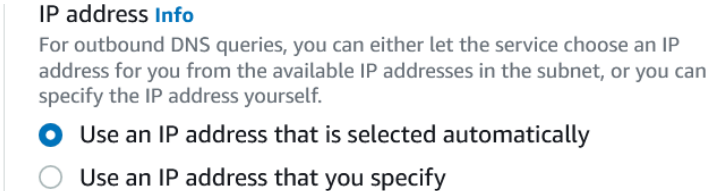
    - Under the *IP address #1* header, select the **Availability Zone** you would like to use for this Outbound Endpoint. *Note that this is the IP clients will send DNS requests to, any additional IP addresses entered will act as redundant to the first one to improve availability.*



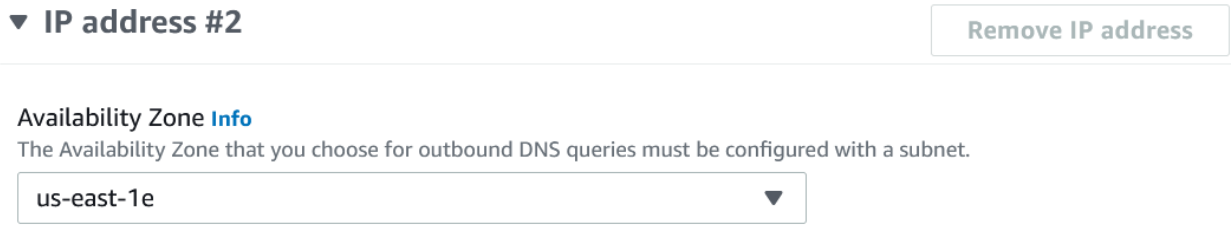
- Select the private **Subnet** associated with the Availability zone.



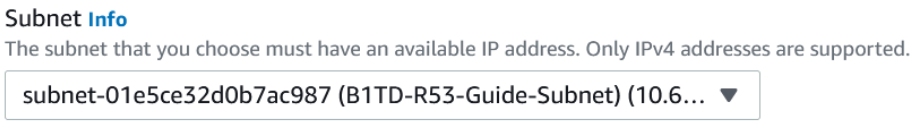
- Choose an **IP address** for the Outbound Endpoint. You may choose to allow AWS to choose one automatically, or input one manually.



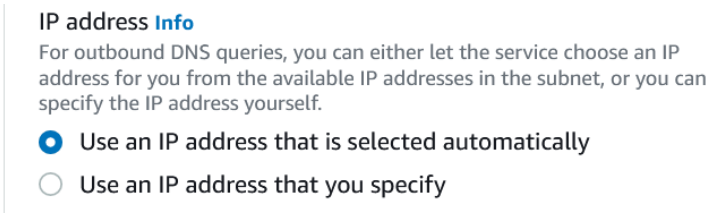
- Under the *IP address #2* header, select the **Availability Zone** you would like to use for this Outbound Endpoint. *Note that this is the IP clients will send DNS requests to.*



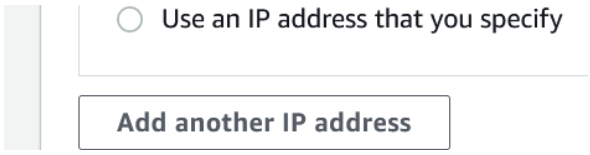
- Select the private **Subnet** associated with the Availability zone.



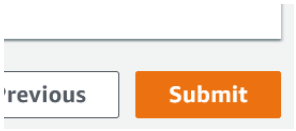
- Choose an **IP address** for the Outbound Endpoint. You may choose to allow AWS to choose one automatically, or input one manually.



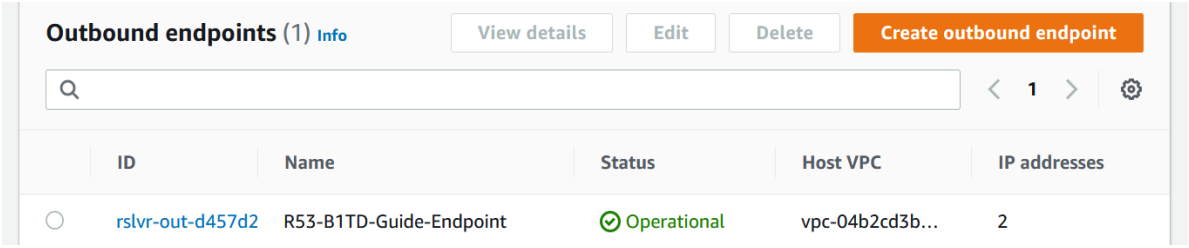
- (Optional) If desired, input additional IP addresses via the **Add another IP address** button.



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



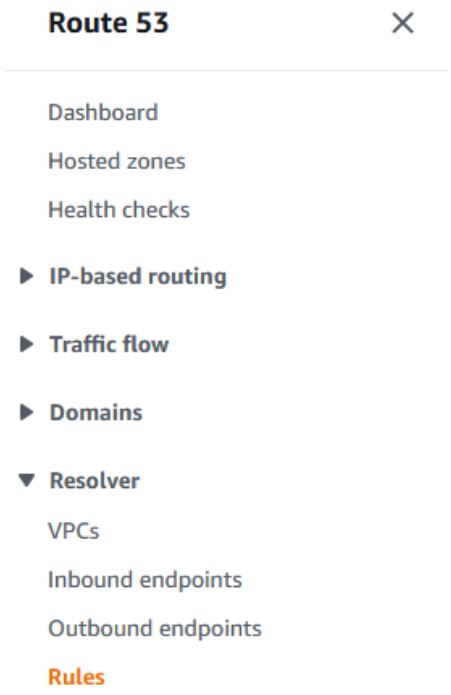
- If the creation of the Outbound Endpoint was successful, you will now see the newly created outbound endpoint on the Outbound endpoints page.



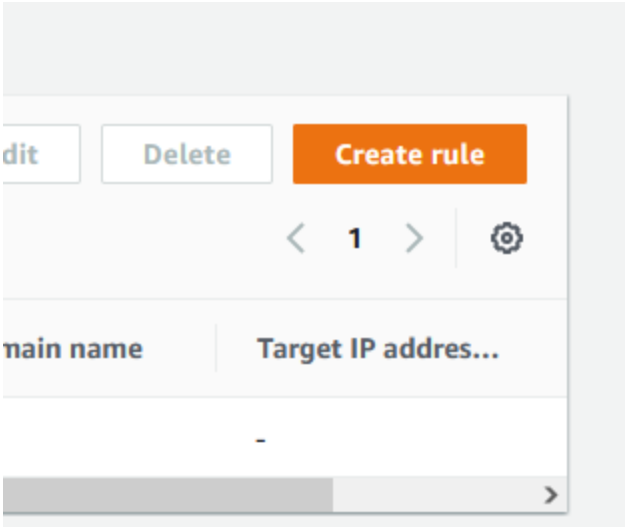
Create a Route53 Resolver Rule

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:

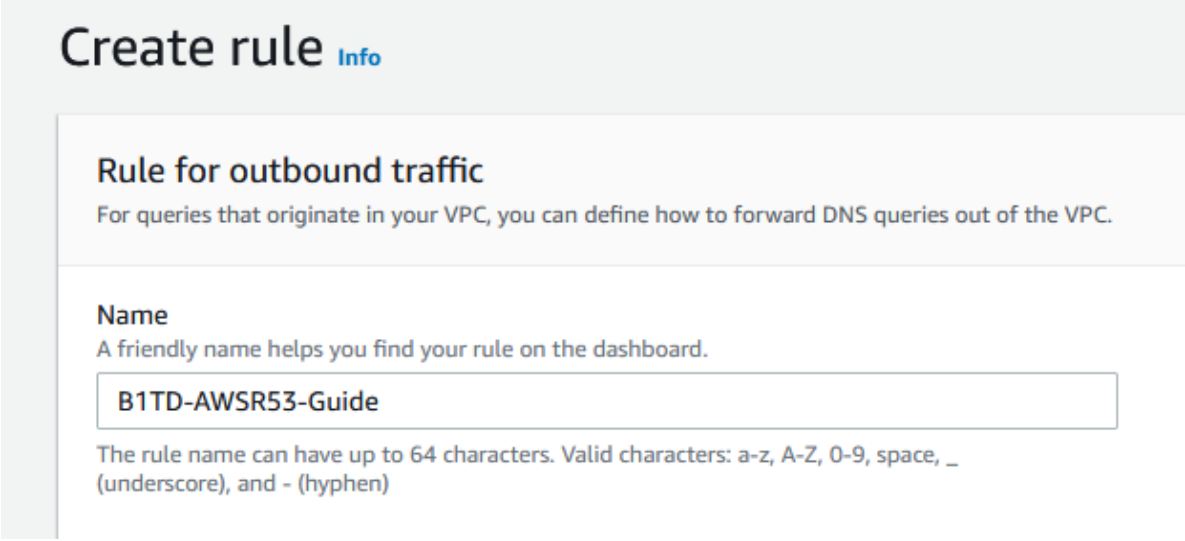
1. In the *Route 53 navigation panel*, click **Rules** located under the *Resolver* header.



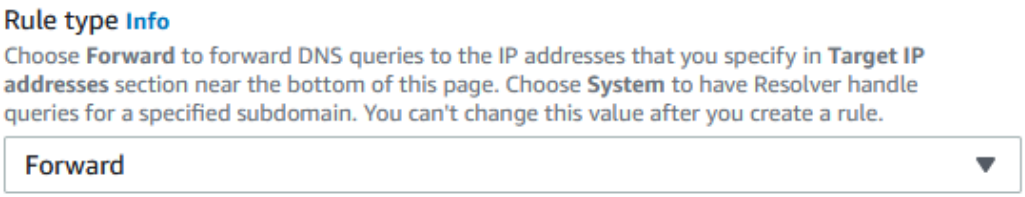
2. On the *Rules* page, click **Create rule**.



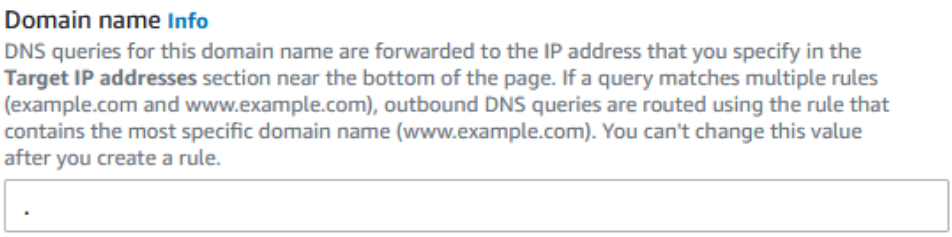
3. Configure the new **rule**:
    - Give the rule a **Name.**



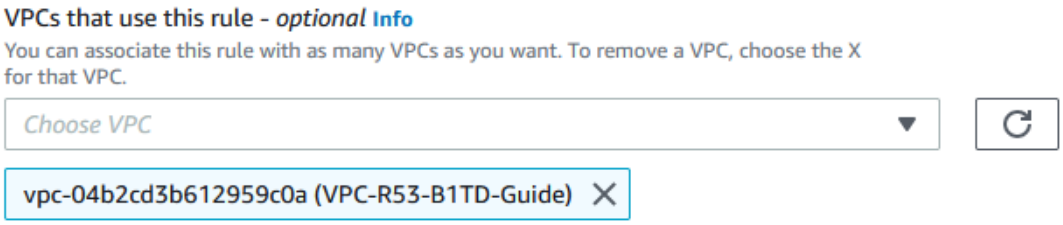
    - Set the *Rule type* as **Forward.**



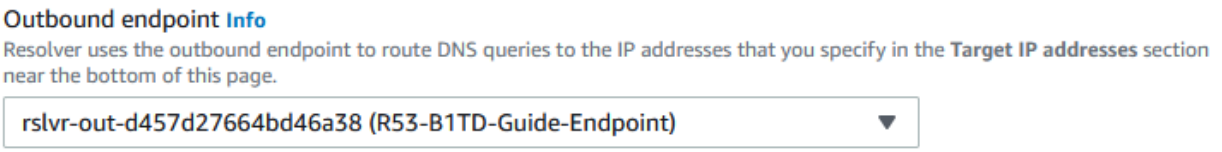
- In the *Domain name* text field input the character '**.**' without quotations.



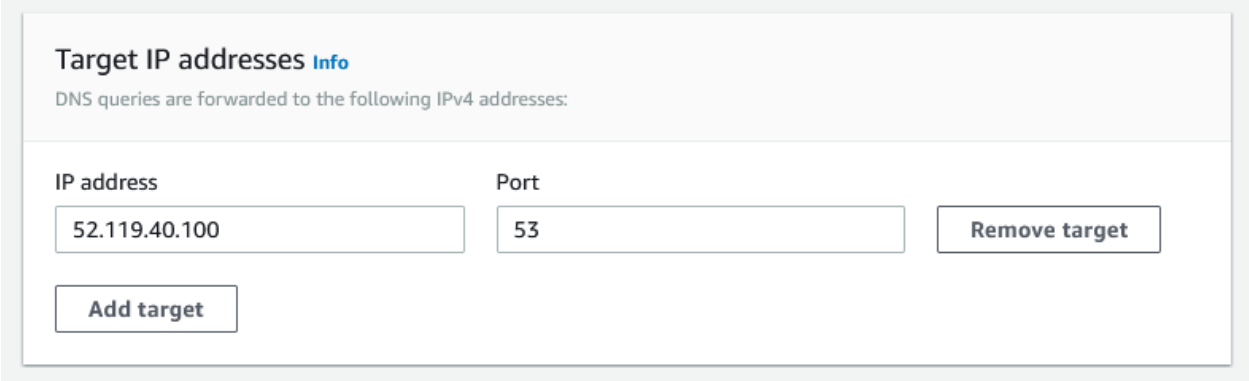
- Select any **VPC**(s) that you would like this rule to apply to via the dropdown menu located under the *VPCs that use this rule* header.



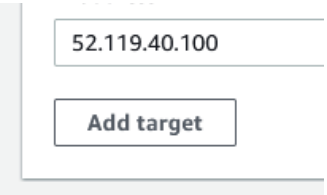
- Select the **Outbound endpoint** that was created earlier via the dropdown menu.



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

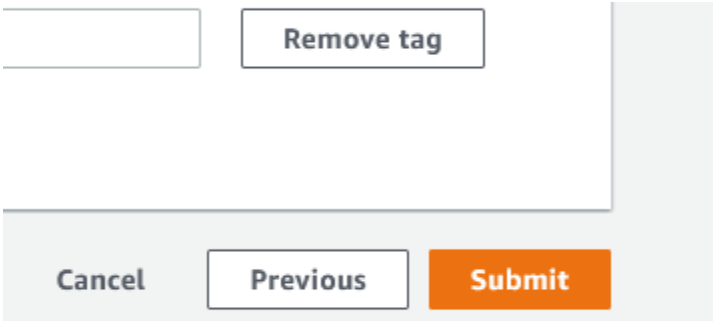


- Click **Add target** to input another IP address.

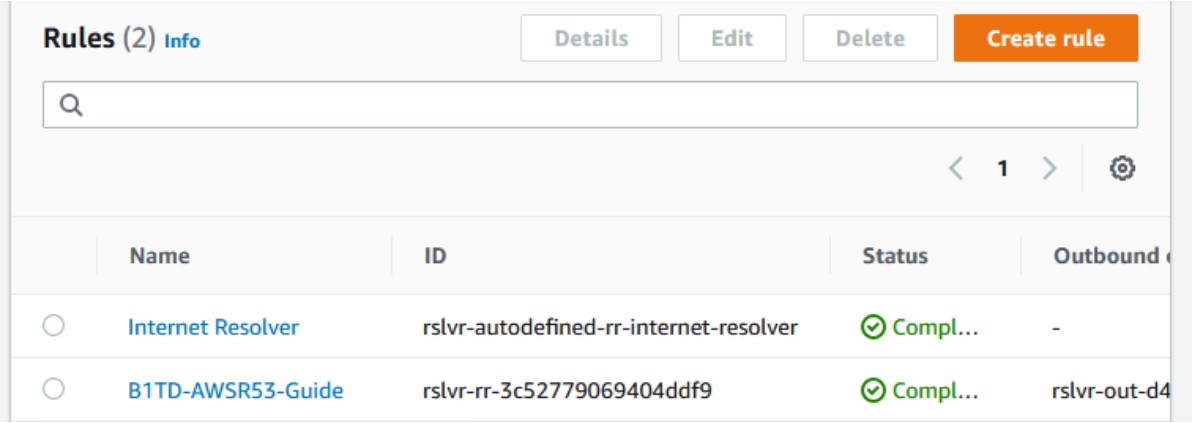


- In the second Target IP addresses field input the IP **103.80.5.100**. Additionally, input **53** in the *Port* text field

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



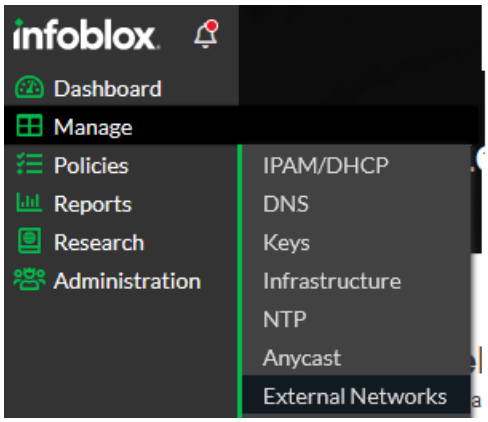
- If the creation of the rule was successful, you will now see the new rule in the list of *Rules*.



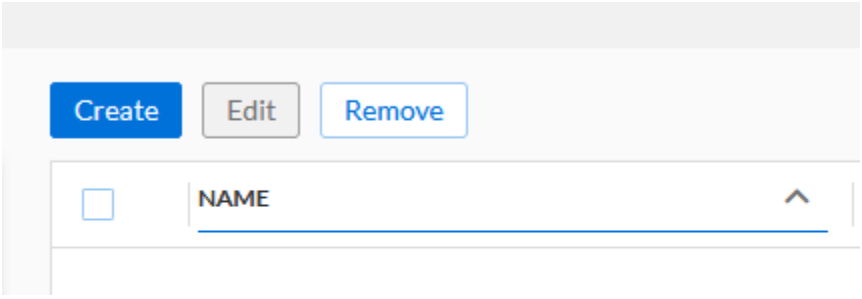
Add an External Network to BloxOne

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

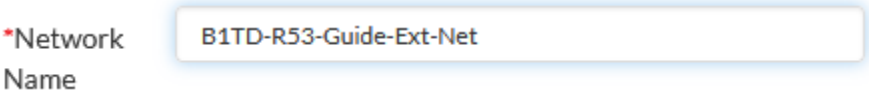
1. Log in to the Infoblox CSP. Once logged in, navigate to the External Networks page. Highlight Manage, then click on **External Networks** in the list that is revealed.



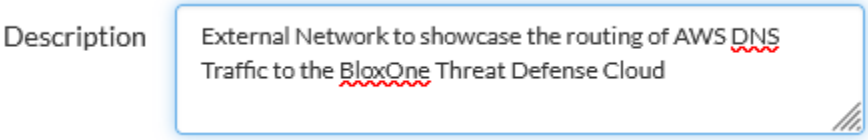
2. Create a new External Network. Click **Create** located on the top left of the External Networks page.



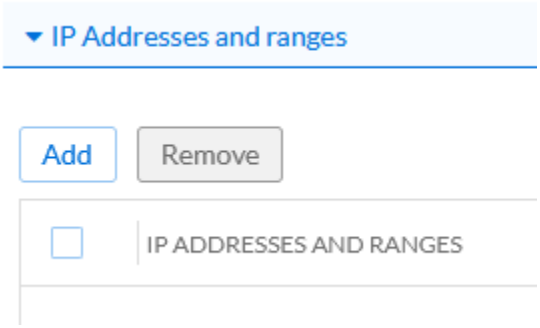
3. In the *Add New Network Panel* that is revealed, input the following:
    - Give the new External Network a **Name**.



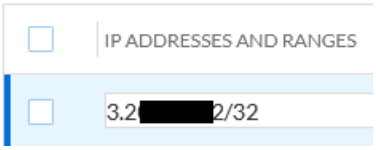
    - (Optional) If desired, input a **Description**.



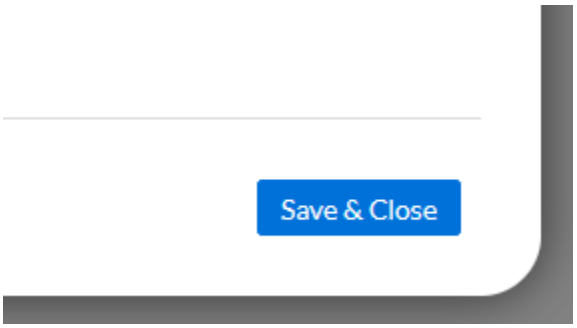
- Click the **Add** button located in the *IP Addresses and ranges* section.



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



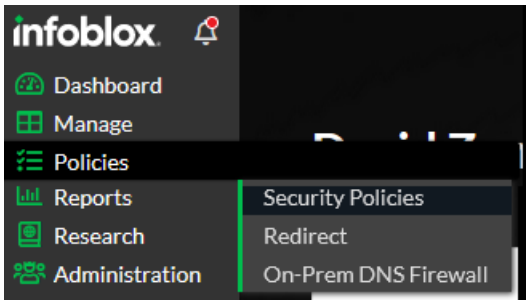
- Click **Save & Close** to confirm the creation of the new External Network.



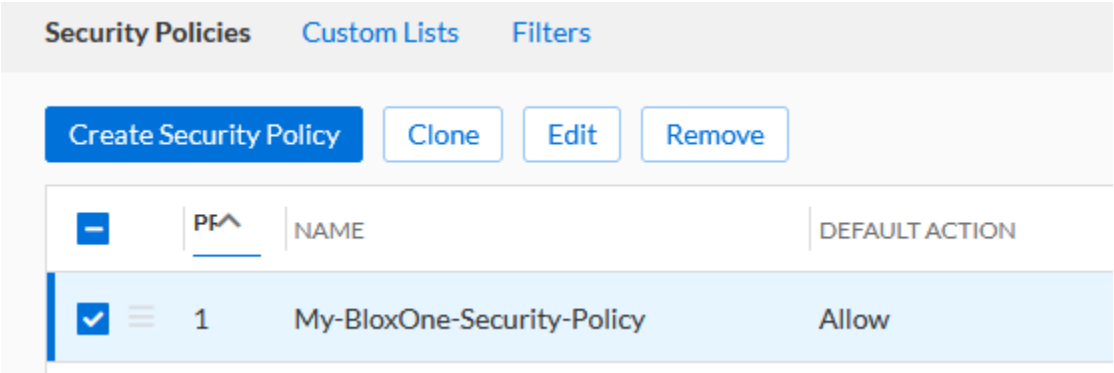
Add the External Network to a Security Policy

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

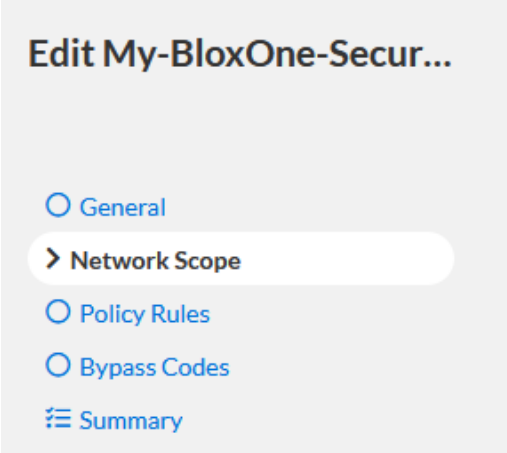
1. In the Infoblox CSP, Navigate to the Security Policy page. Highlight Policies, then click on **Security Policy** in the list that is revealed.



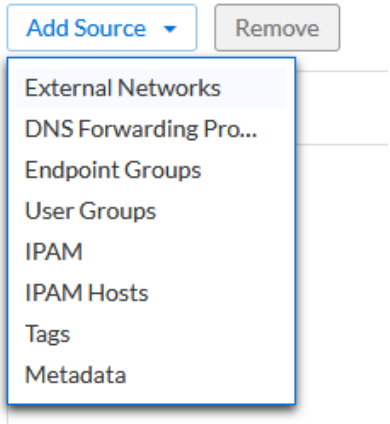
2. Once on the Security Policies page, locate the security policy that you would like to add your AWS VPC to. Click the **checkbox** associated with the Security Policy. Then, click **Edit**.



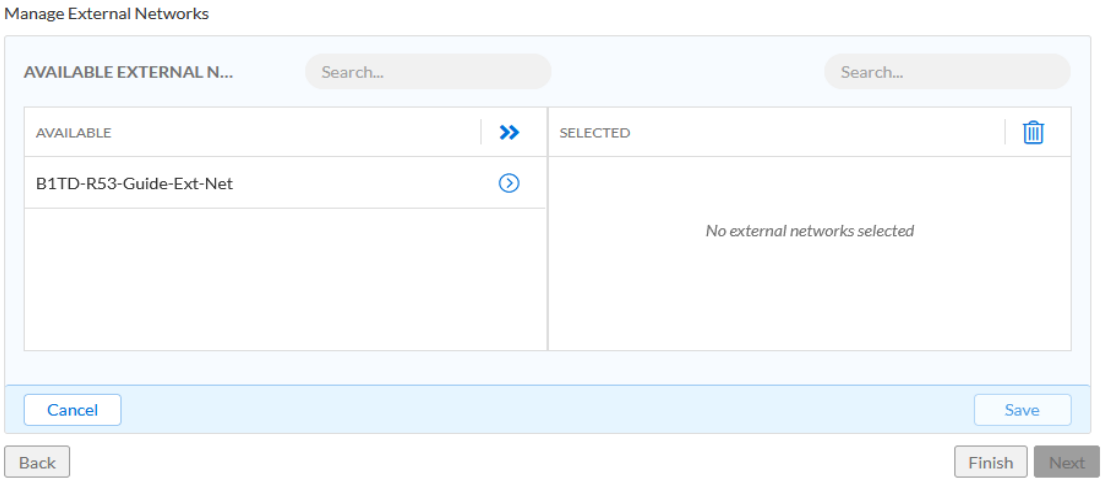
3. On the panel that is revealed, click **Network Scope** in the left navigation panel.



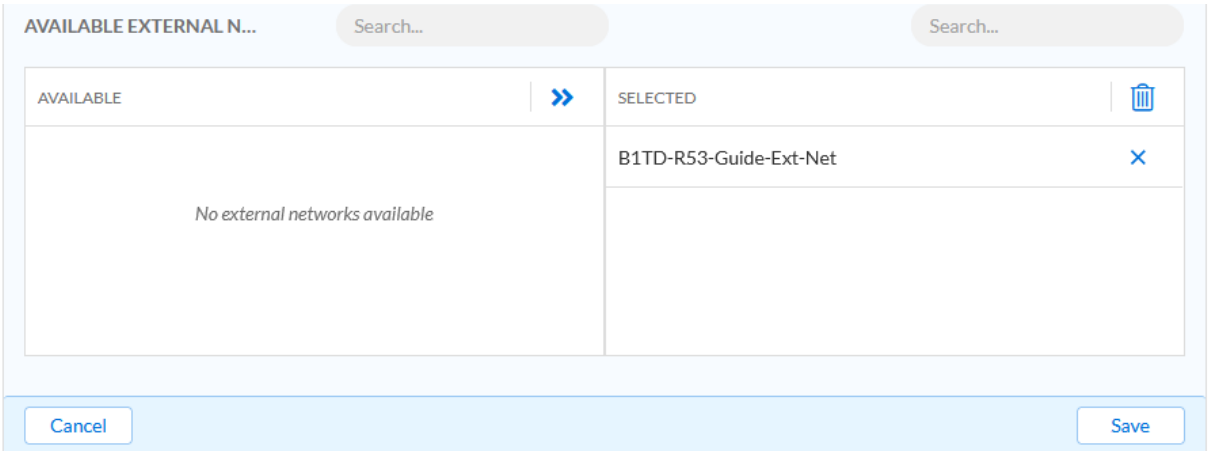
4. On the *Network Scope* page, click **Add Source**. Then, click **External Networks** in the list that is revealed.



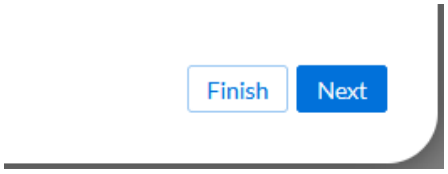
5. In the Available External Networks panel of the Security Policy, click the **arrow** associated with the External network that you've created in the previous section.



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



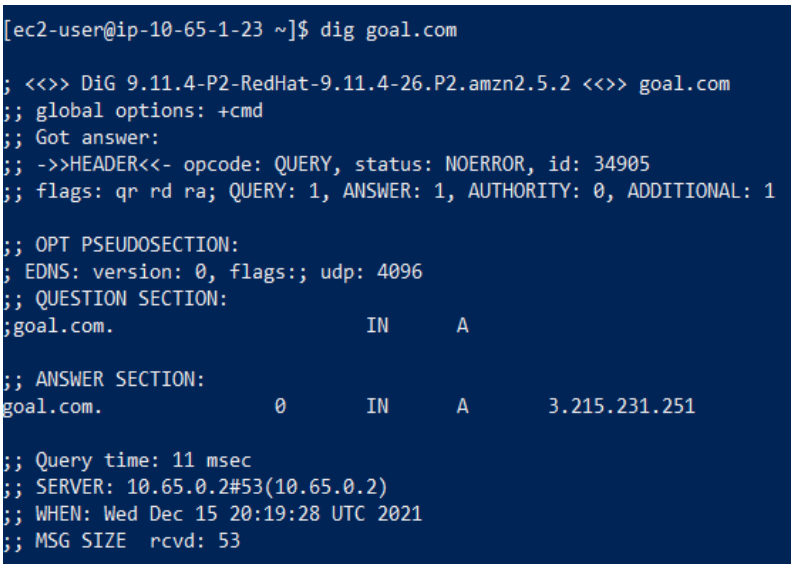
7. Finally, click **Finish**, then **Save & Close** to confirm the changes to your Security Policy.



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.
    - 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.



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.

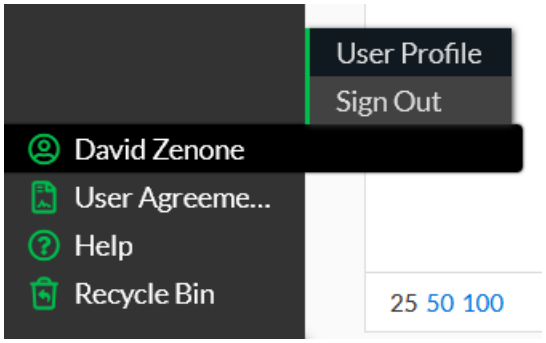
Workflow

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.

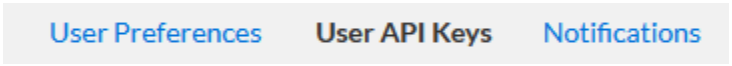
Acquire a TIDE API Key

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:

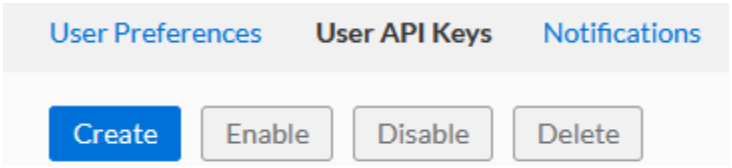
1. Log into the Infoblox CSP. Once logged in, highlight your **username** located in the bottom left of the navigation panel, then click on **User Profile** in the list that is revealed.



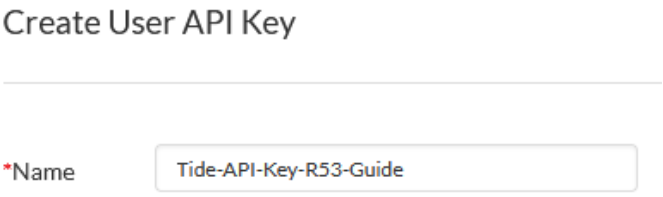
2. On the *User Profile* page, click the **User API Keys** tab located at the top of the page.



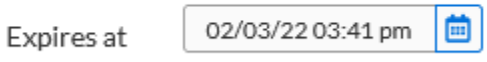
3. Click the **Create** button to begin creating an API key.



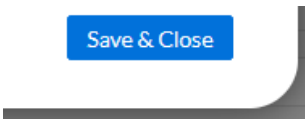
4. On the Create Service API Key panel that is revealed. Give the API Key a **Name**.



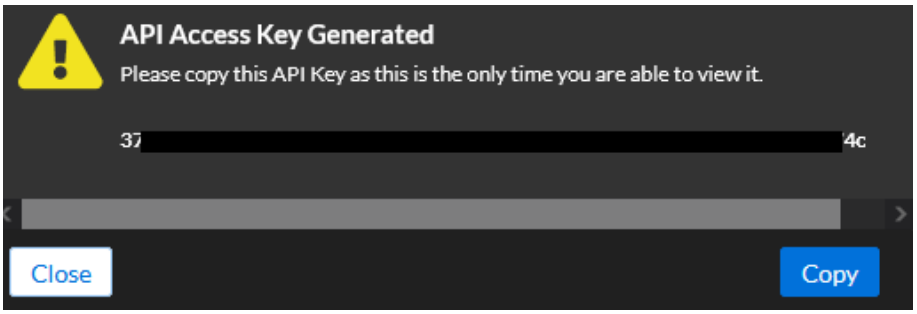
5. (Optional) Change the API Keys expiration date by changing the **Expires at** field.



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



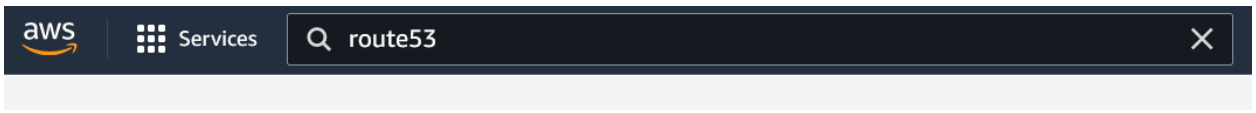
7. After clicking Save & Close, a *dialog box* will appear. **Copy** the API key from this dialog box and save it to a text file for use later. *Please note that once you close this dialog box, the API key will no longer be accessible.*



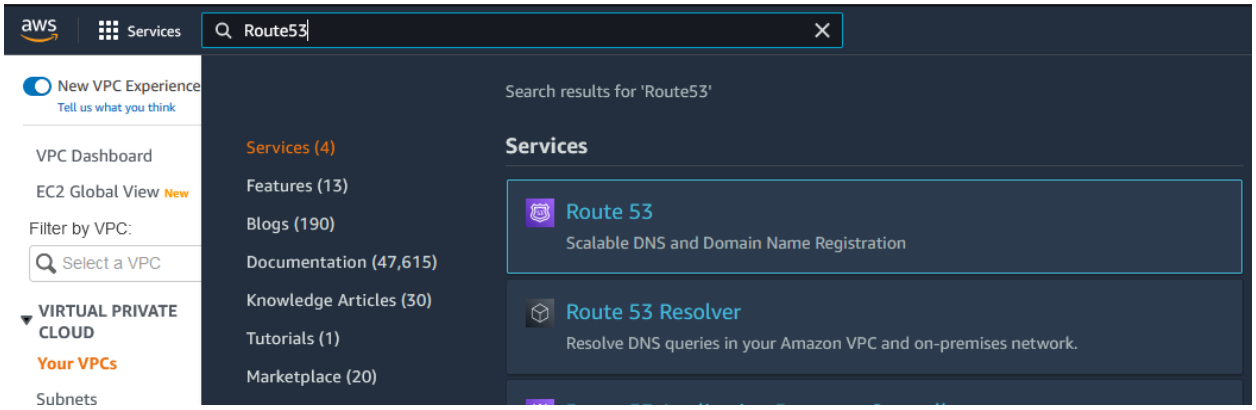
Create an AWS Route 53 DNS Firewall domain list

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:

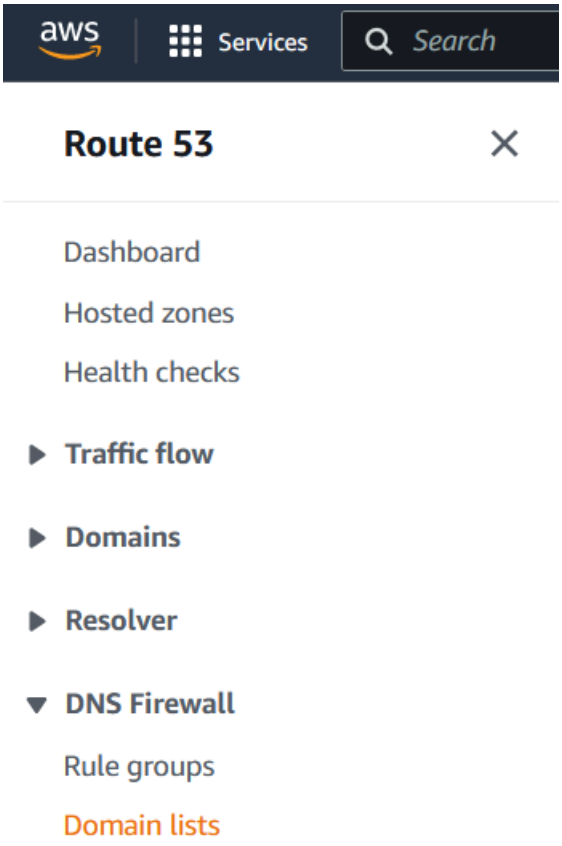
1. Log in to your AWS account. Once logged in, input **Route53** into the *search bar* located at the top of the AWS interface.



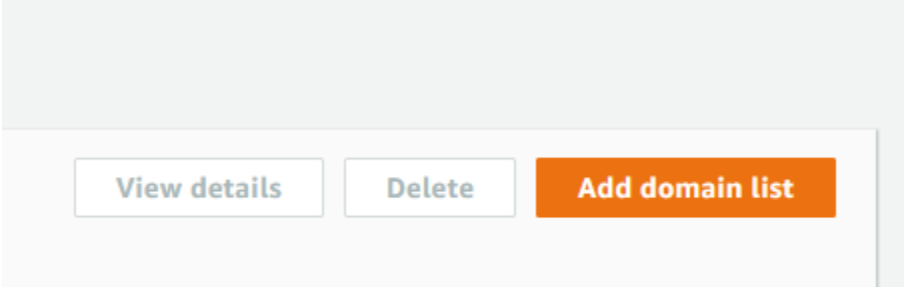
2. Click the text **Route 53** in the list that is revealed.



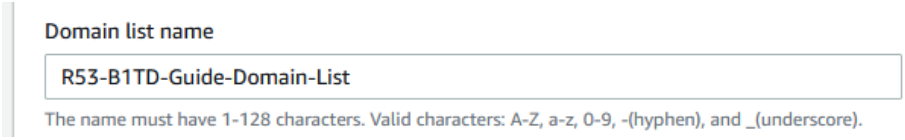
3. In the *Route 53 navigation pane*, click **Domain List** located under the *DNS Firewall* header.



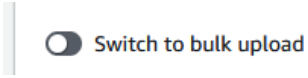
4. On the *Domain Lists* page, in the *Owned domain lists* panel click **Add domain list**.



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

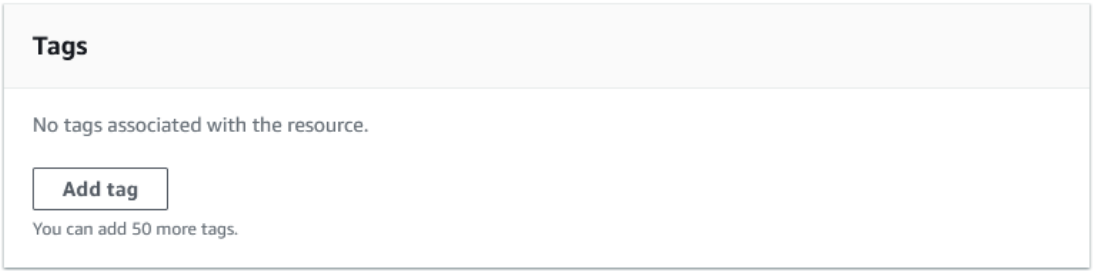


- (Optional) If desired, you may input a bulk list of domains to the domain list via the **Switch to bulk upload** toggle switch and an *S3 bucket*.

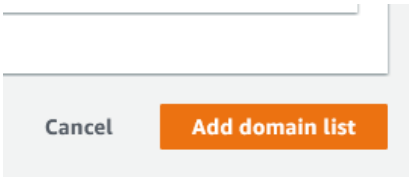


- Input one or more domains in the **Enter one domain per line** text box. *Note, you may only input one domain per line*

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



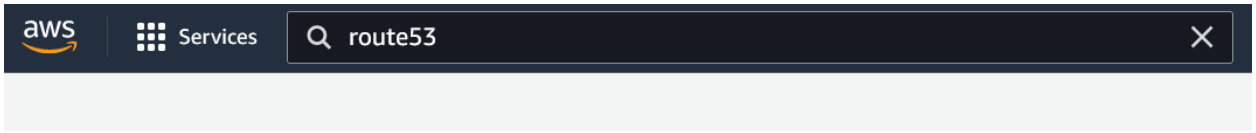
- Click the **Add domain list** button to confirm the creation of the domain list



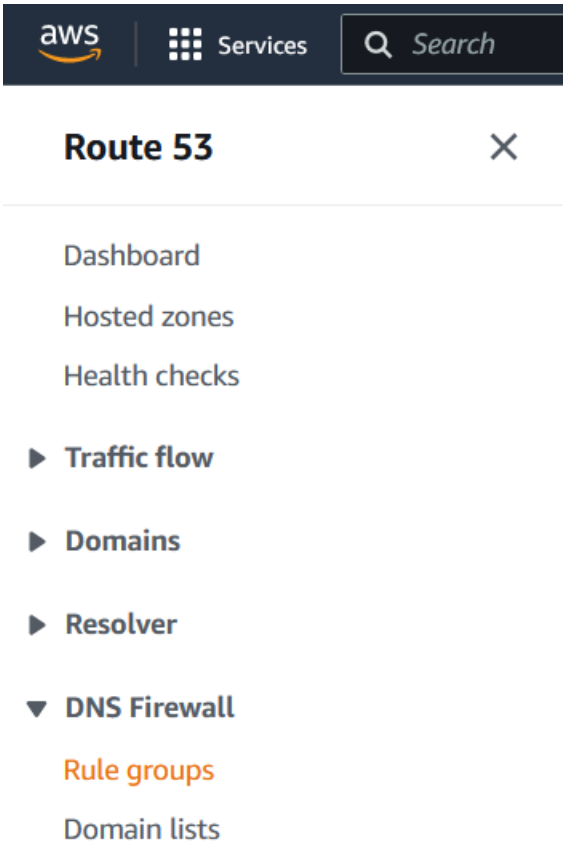
Create an AWS Route 53 DNS Firewall Rule Group and Associated Rule

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:

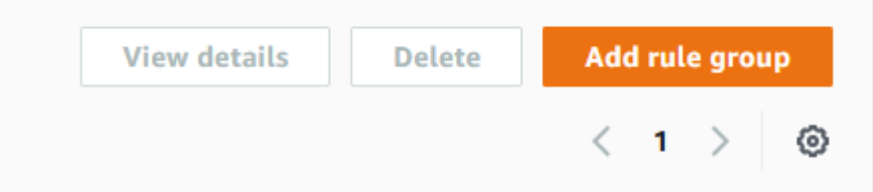
1. On the AWS Interface, input **Route53** into the *search bar* located at the top of the page.



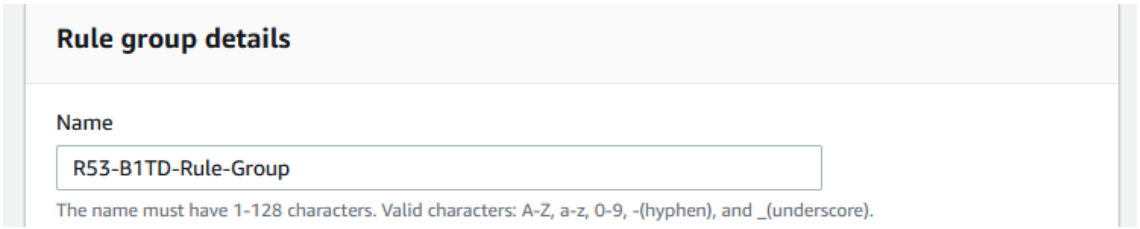
2. In the *Route 53 navigation pane*, click **Rule groups** located under the *DNS Firewall* header.



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

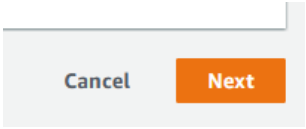


4. On the Add rule group page perform the following steps:
    - In the Rule group details panel, give the rule group a **Name.**

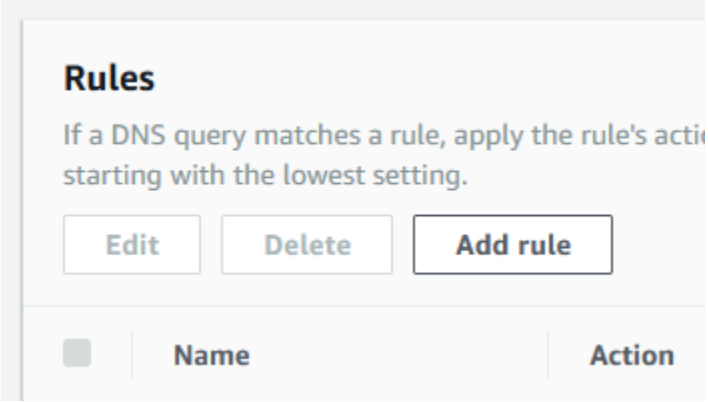


    - (Optional) If desired, give the Rule group a **Description.**

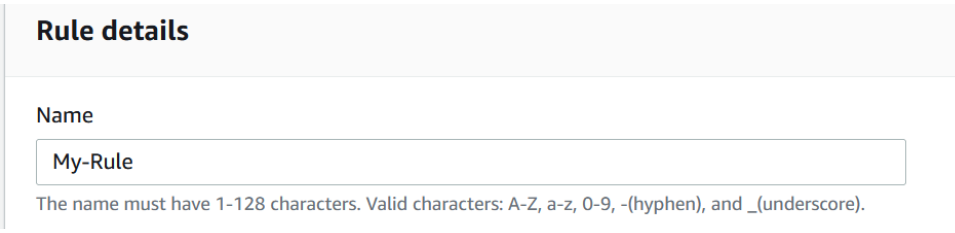
    - Click **Next**



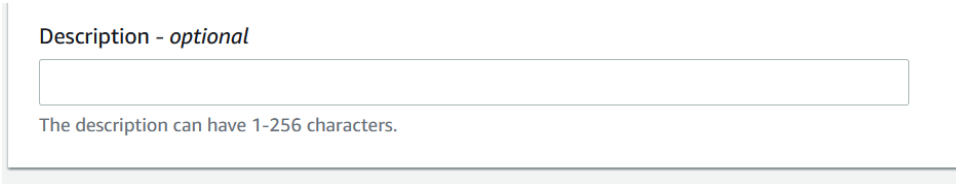
    - Click the **Add Rule** button located near the top of the *Rules* panel to begin adding a rule.



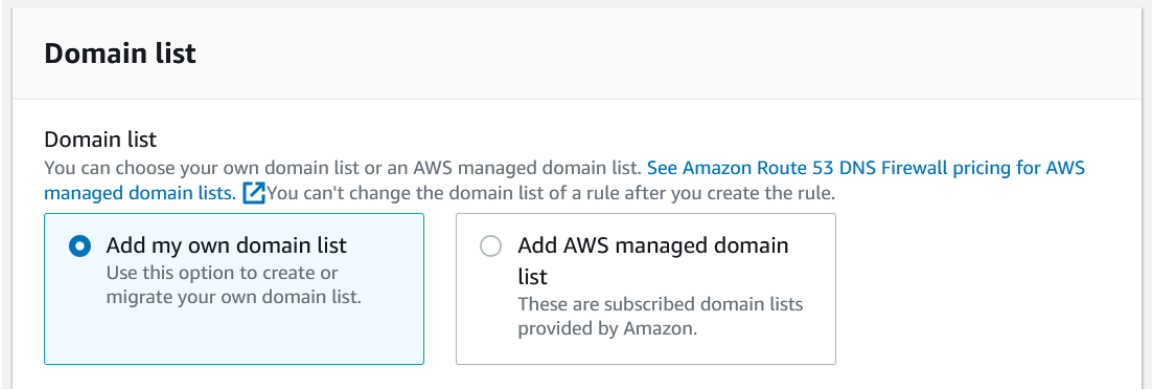
    - Give the rule a **Name**.



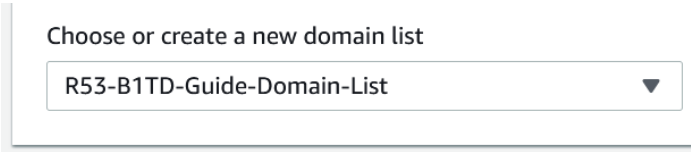
- (Optional) If desired, give the rule a **Description**.



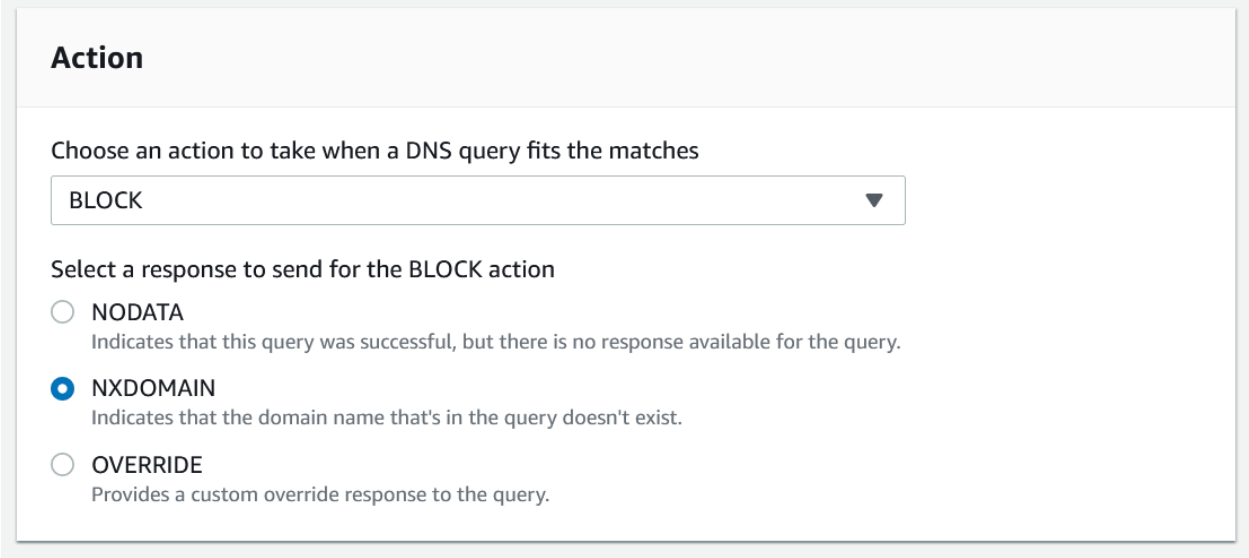
- In the *Domain list* panel, select **Add my own domain list**.



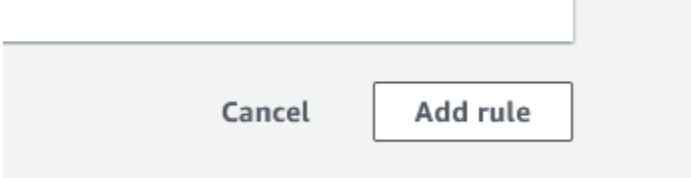
- In the *Choose or create a new domain list* drop-down menu, select the **domain list** you intend to add TIDE feeds to.



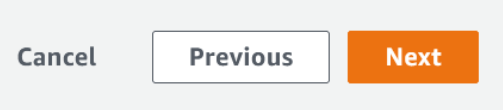
- In the Action panel, select the action that will be taken when this rule is triggered by selecting the **action** in the *Choose an action to take when a DNS query fits the matches* drop-down, and the associated bubbles.



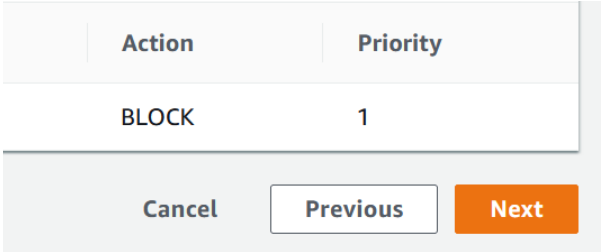
- Click the **Add rule** button to confirm the creation of the rule.



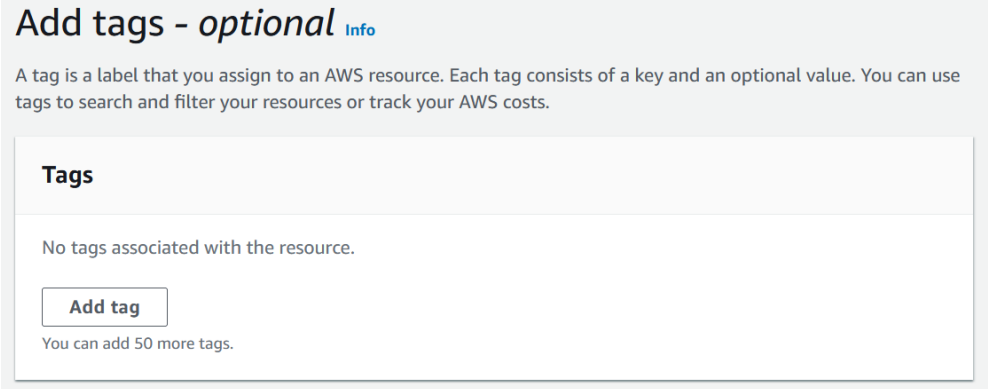
- Click **Next**.



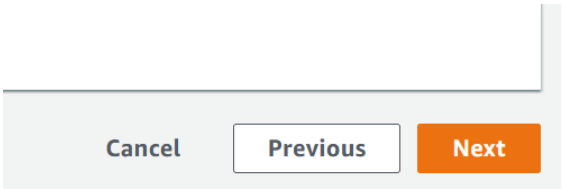
- Click **Next**.



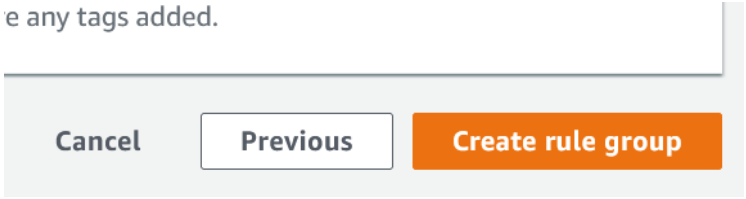
- (Optional) If desired, add Tags to the rule group via the **Add tag** button.



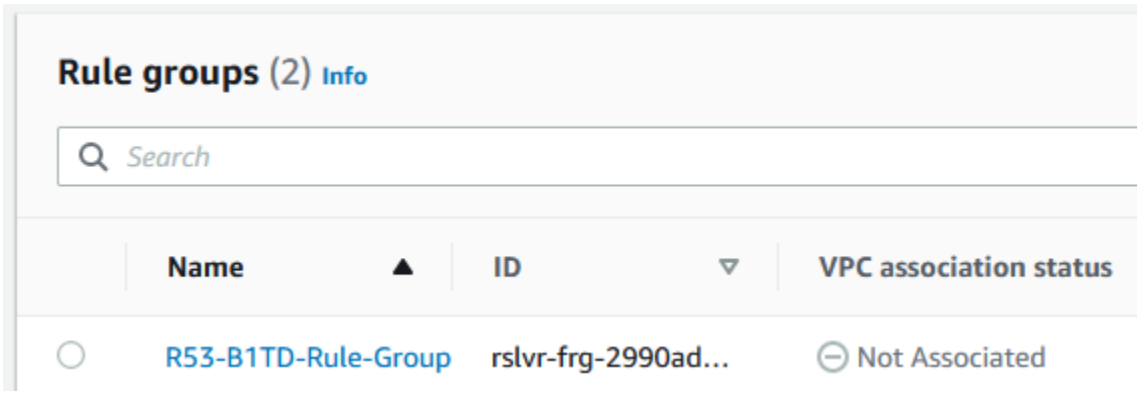
- Click **Next**



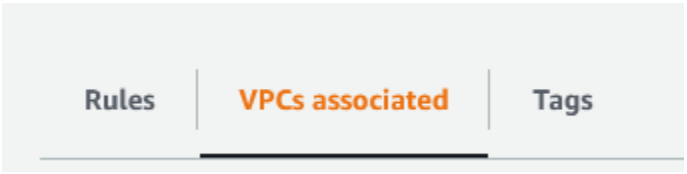
- Review the rule groups settings, then click **Create rule group** to confirm the creation of the rule group.



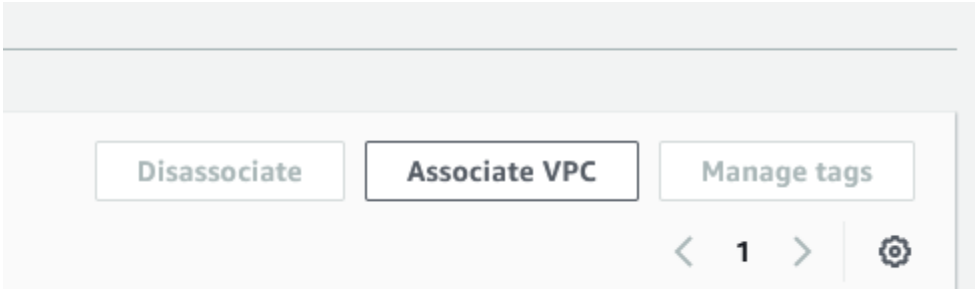
5. This *Rule group* must be associated with a VPC in order to take action on domains contained in your domain list. In order to associate the rule group to a VPC click the rule group you've just created by clicking the **rule group** located in the rule group panel.



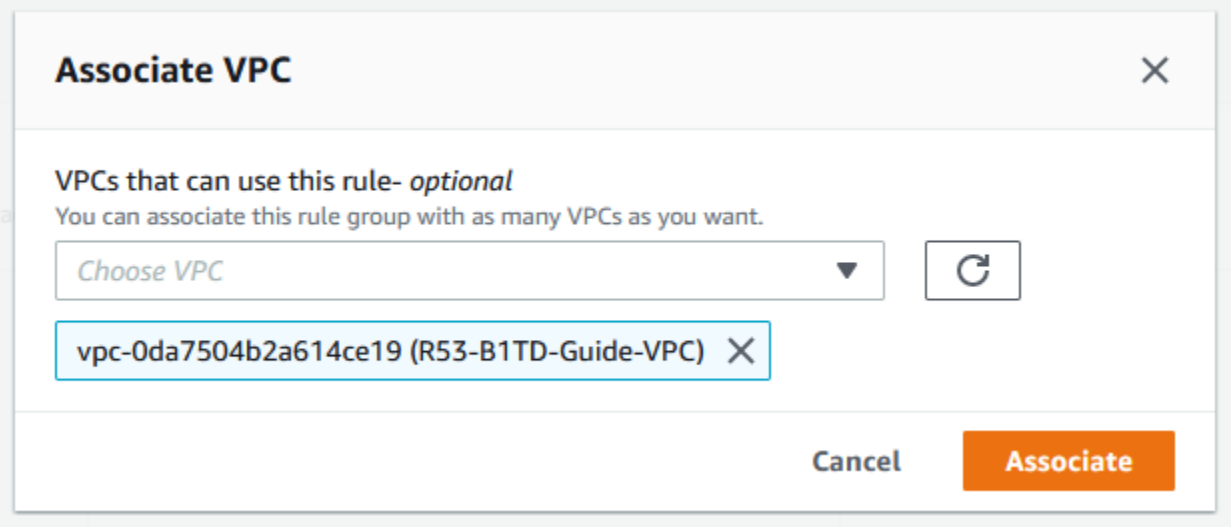
6. Near the bottom of the *rule group's* page, click the **VPCs Association** tab.



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



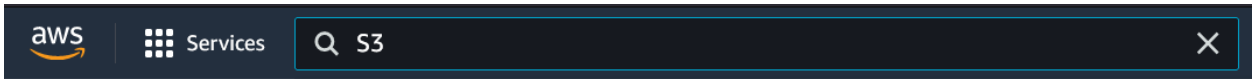
8. In the *Associate VPC* panel **select** a VPC via the Choose *VPC drop-down*, then Click **Associate**.



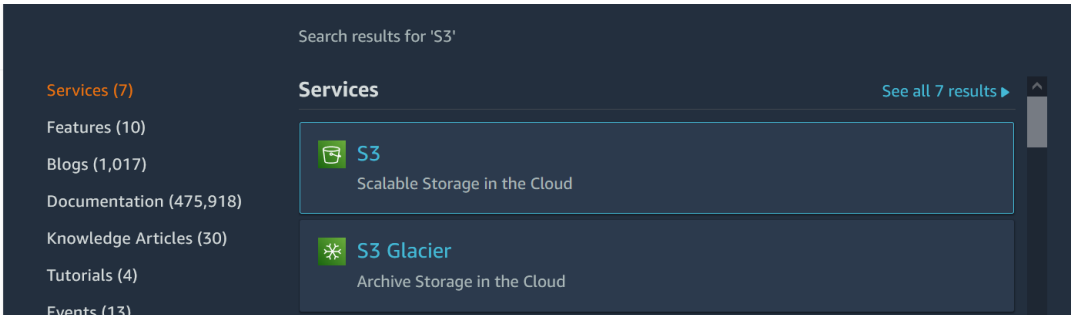
Create an S3 Bucket and File

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:

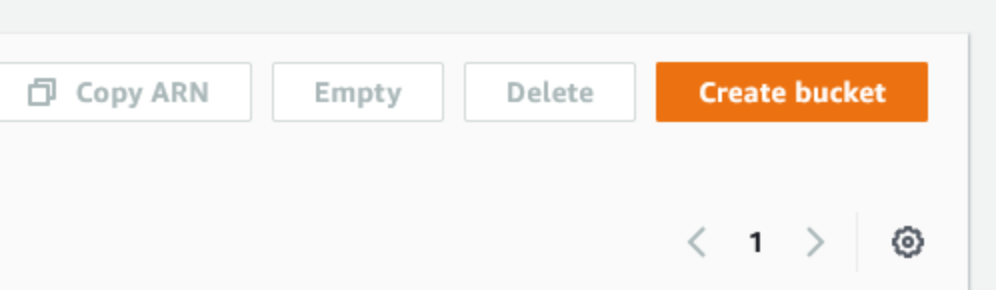
1. Input **S3** into the *search bar* located at the top of the AWS interface.



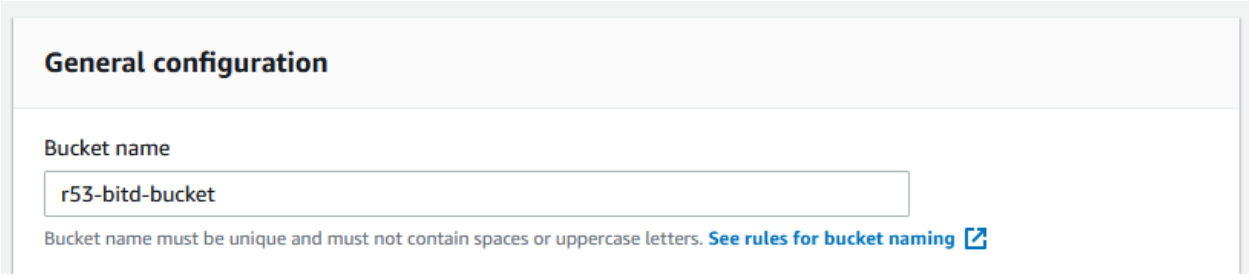
2. Locate and click on **S3** to navigate to the *Amazon S3* page.



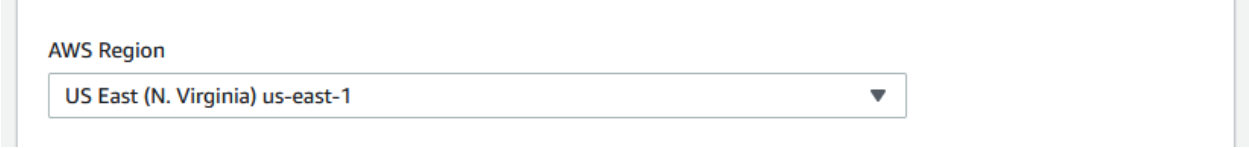
3. On the *S3 Amazon* page, click **Create bucket**.



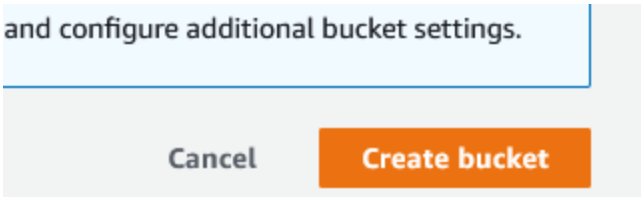
4. On the *Create bucket* page perform the following steps:
    - Give the bucket a **name**. *Note: save this name to a text file for use later in this guide*



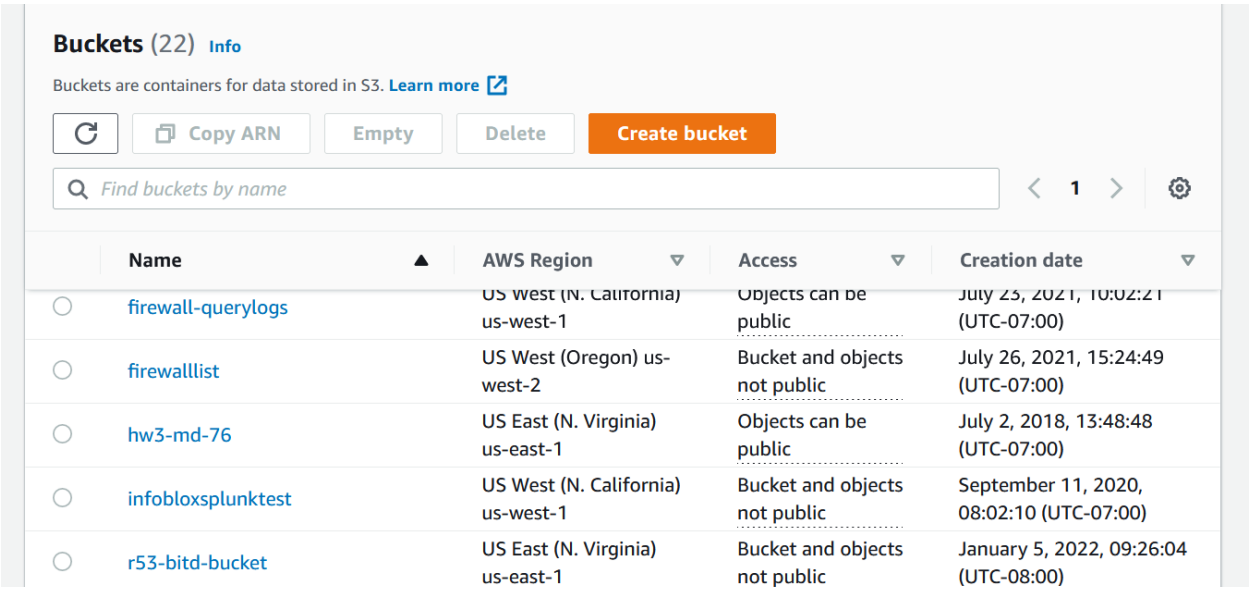
    - Select the **AWS region** you intend to use via the AWS Region drop-down.



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

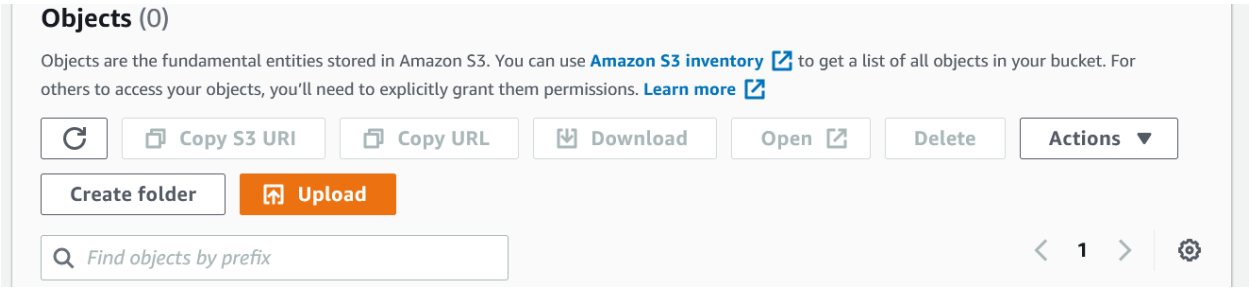


5. On the *Buckets* page, scroll down to the Buckets panel. Locate and click on the **S3 bucket** you've just created.

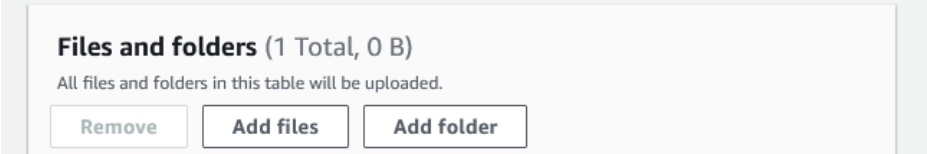


6. On your desktop, create a simple **text file** with no content.

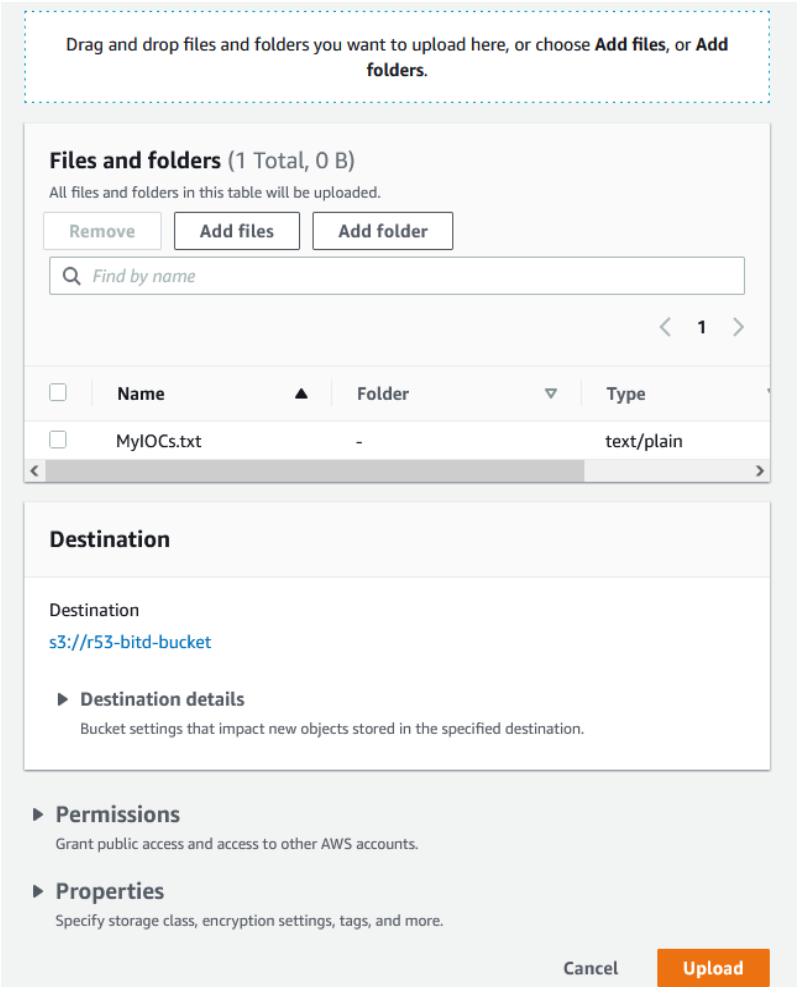
7. In the *Objects* panel of Bucket's page click **Upload**.



8. 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.



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.*



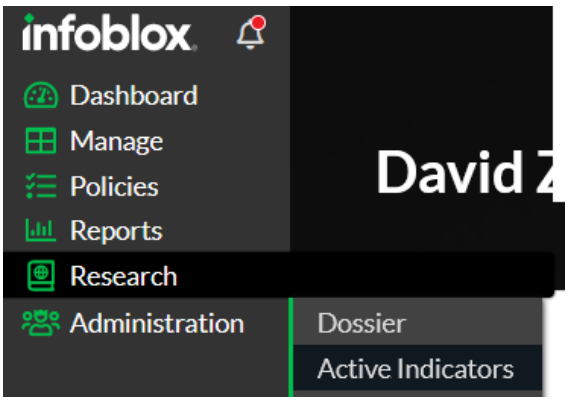
Acquire Information for a Lambda function

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:

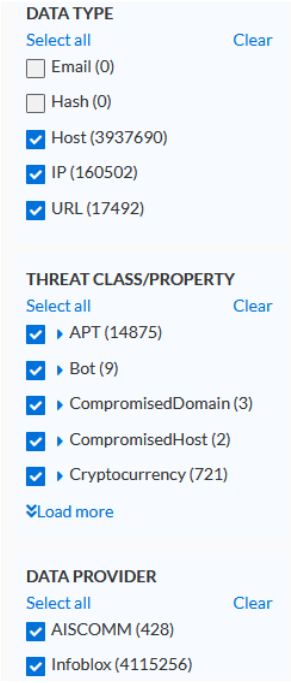
Acquire a TIDE API Call URL

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:

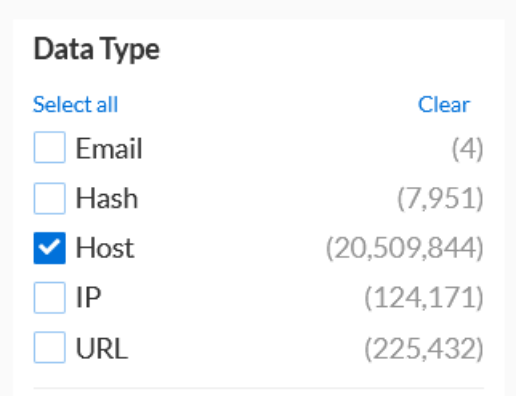
1. Log into the Infoblox CSP. Once logged in, highlight *Research* located in the bottom left of the navigation panel, then click on **Active Indicators** in the list that is revealed.



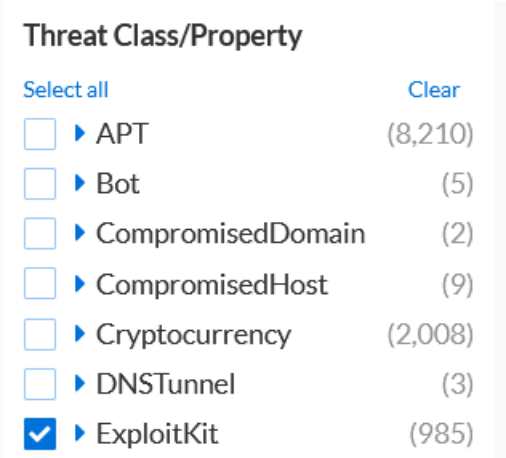
2. Here you can see the list of *Active indicators*. Due to the quantity of data, it is suggested to filter the API call. Click **Clear** for each section, until all sections are unchecked.



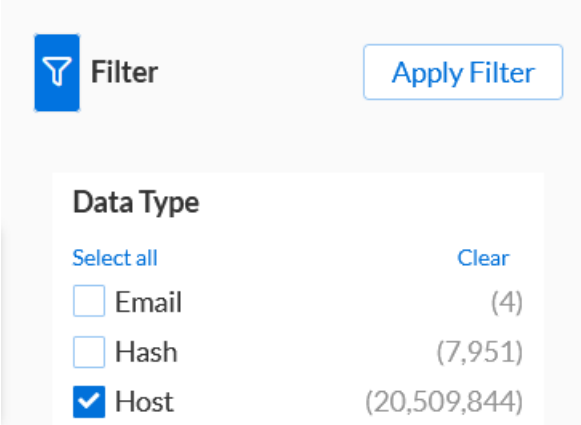
3. Under the *DATA TYPE* header, click the **checkbox** associated with the **Host** data type.



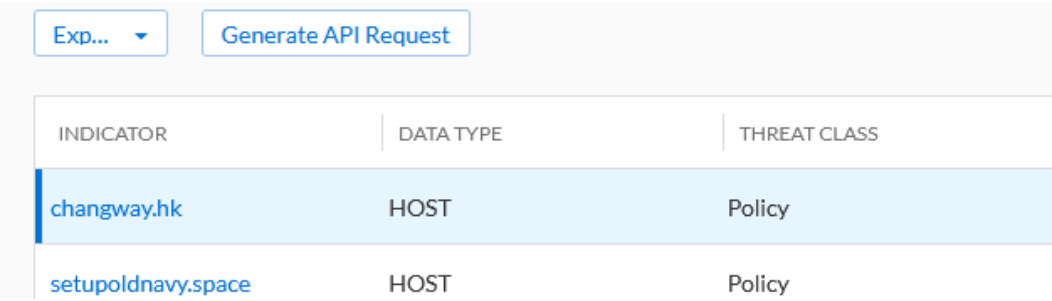
4. Under the *THREAT CLASS/PROPERTY* header, click the **checkboxes** associated with the **Threat Class / Properties** you would like to add to your AWS Route 53 Domain Firewall list. *Note that it is suggested to only select one threat class/property per lambda function as duplicates may occur for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



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

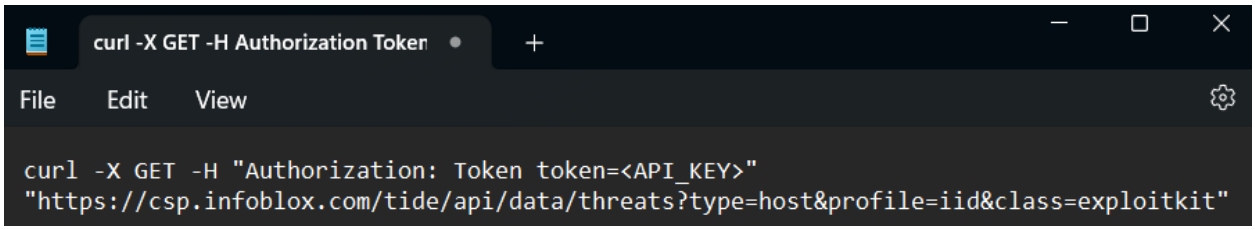


6. At the top of the *Active Indicators* page, click **Generate API request**. *Note this will create a simple API call for the IOC defined, this API call can be modified further with additional parameters.*

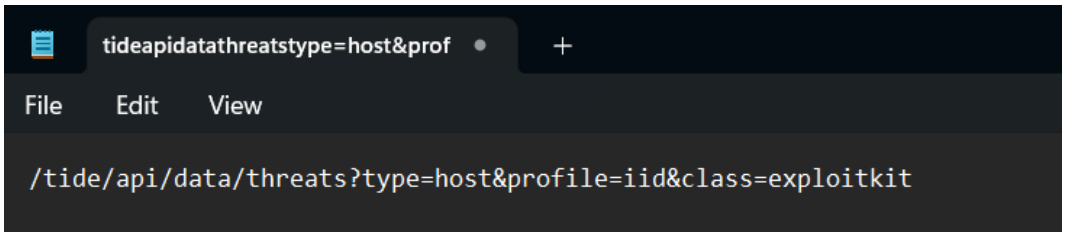


7. **Copy** the API call in the dialog box that has been revealed.

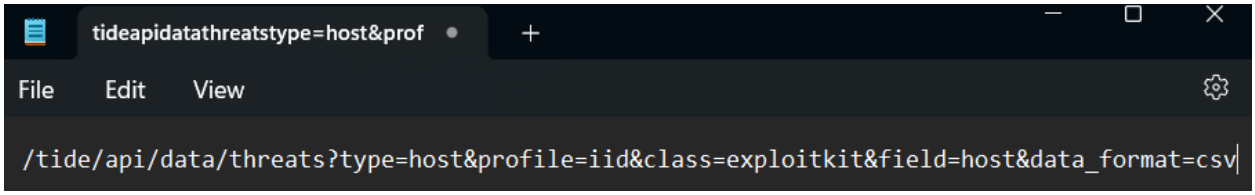
8. **Paste** the API call to a text editor of your choice.



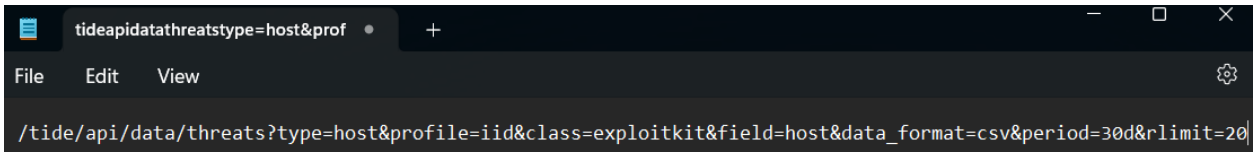
9. Modify the API call by **deleting** all text until */tide/*. Additionally, keep all following text except for the closing quotation mark.



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.*



11. (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*.

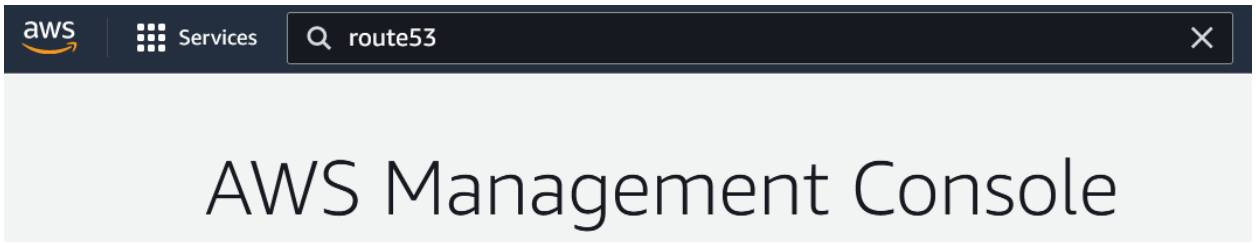


12. **Save** this API call for use later.

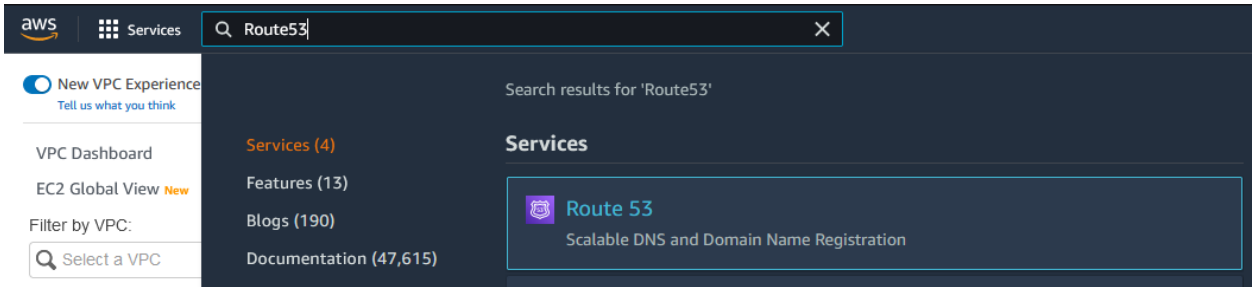
Acquire an AWS Route 53 DNS Firewall domain list ID

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

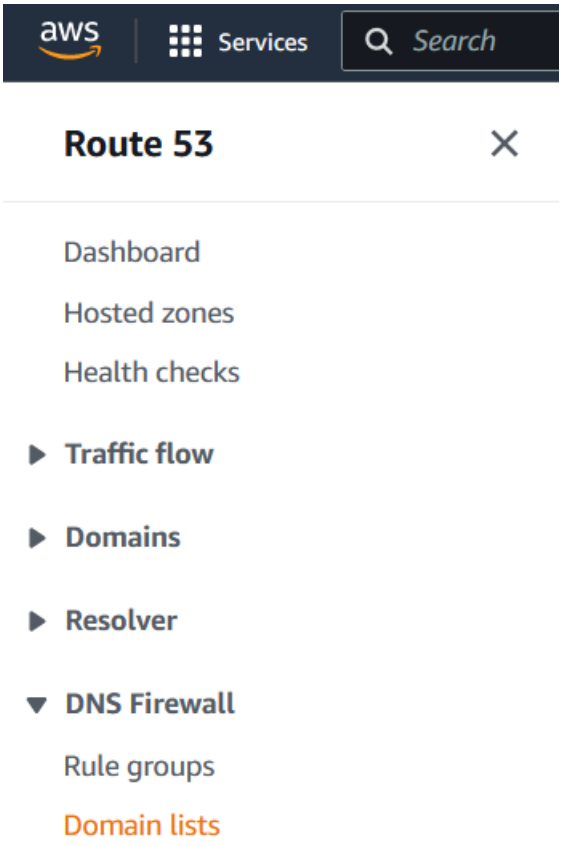
1. Log in to your AWS account. Once logged in, input **Route53** into the *search bar* located at the top of the AWS interface.



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 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.*

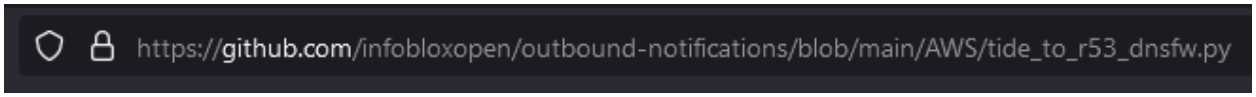
Create a Lambda function

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.

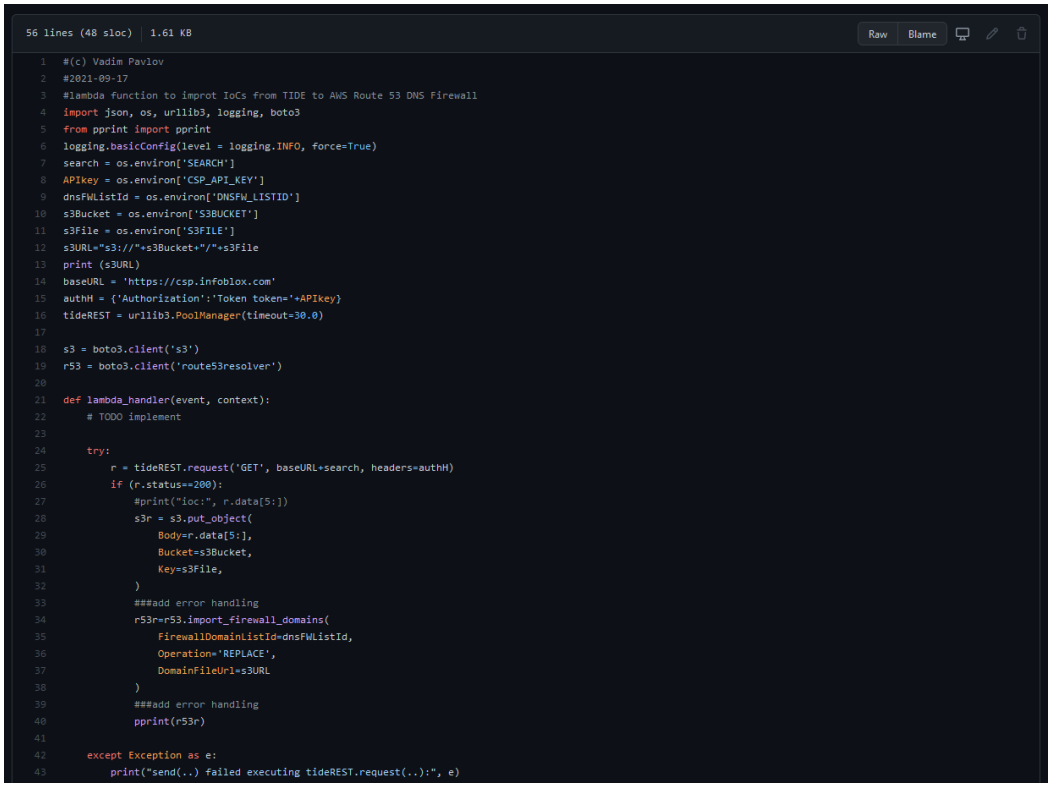
Please note that the script replaces any existing domains in the domain list it is interacting with. If desired, you may alter the script to append instead of replace.

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.

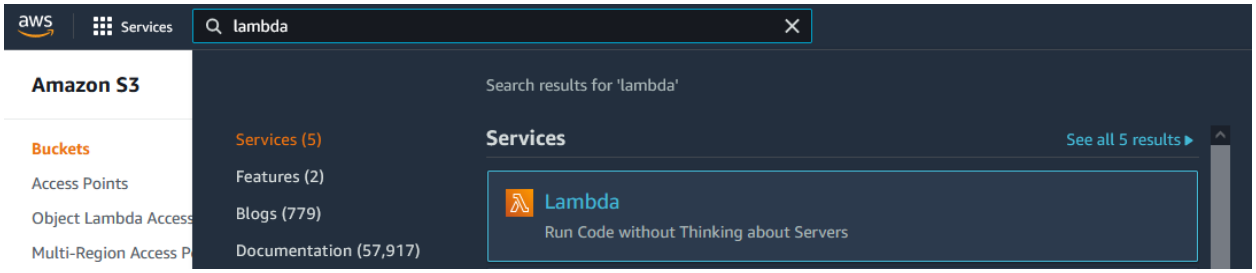


2. **Copy** the Python script and **save** it to a text file.

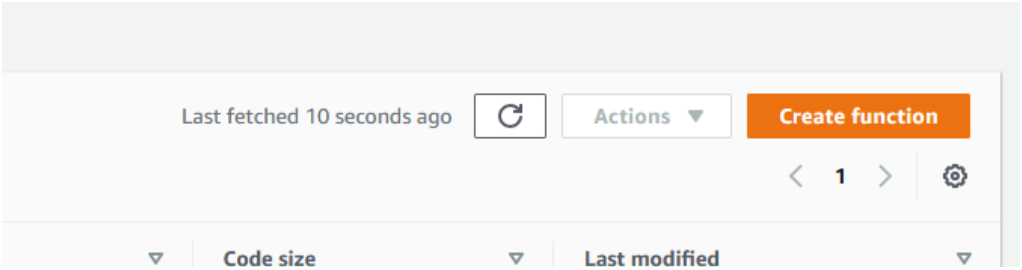


1. Back in the AWS console, input **Lambda** into the *search bar* located at the top of the AWS interface.

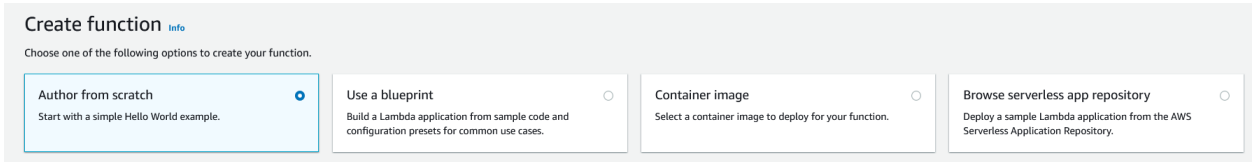
2. Locate and click on **Lambda** to navigate to the *Lambda* page.



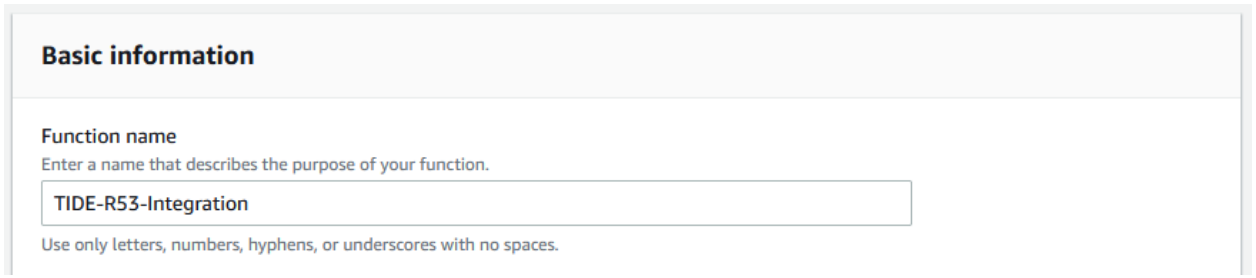
3. On the *AWS Lambda functions* page, click **Create function**.



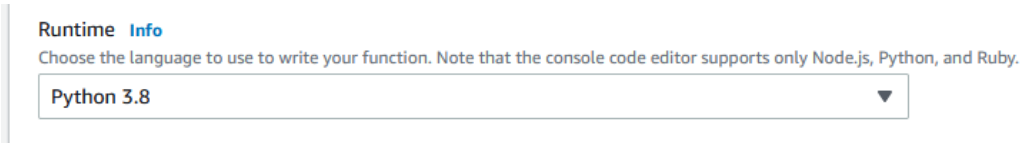
4. On the *Create function* page, configure the following settings:
    - Click the **Author from scratch** bubble.



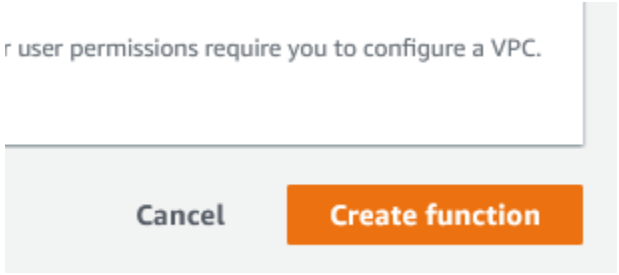
    - Give the Function a **name**.



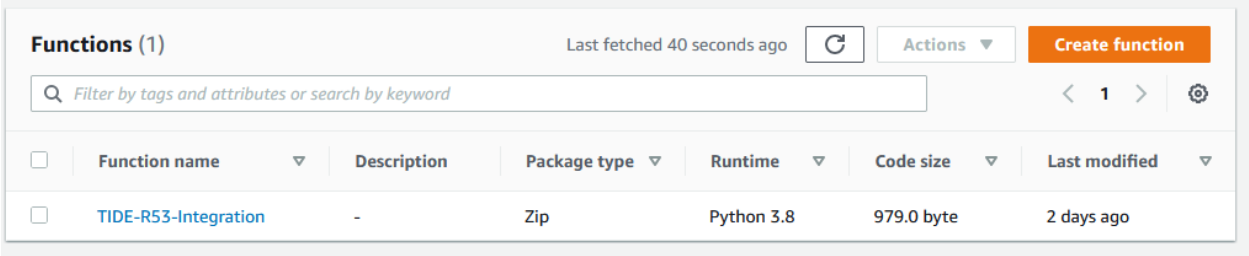
5. Select **Python 3.8** via the *Runtime* drop-down menu.



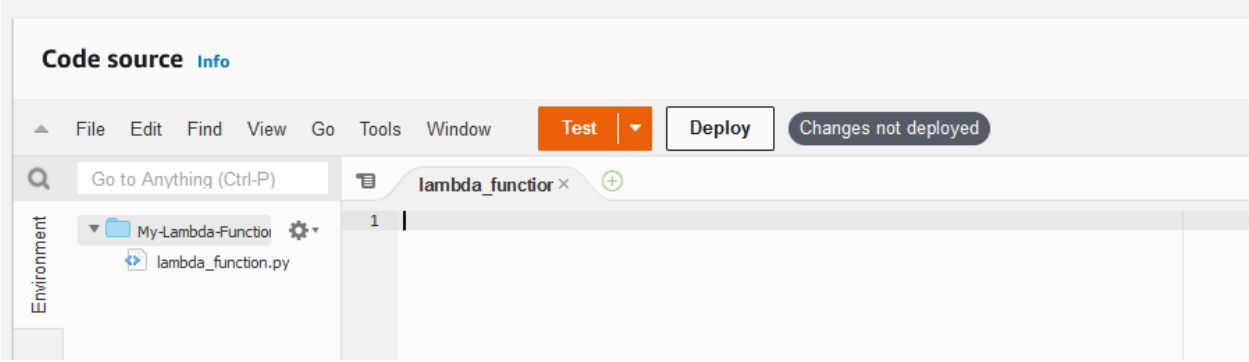
6. Keep all other settings as their default and click **Create function**.



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

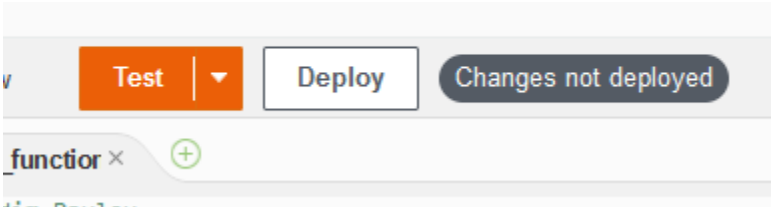


8. Once on the Lambda function's page, **delete** all text located in the code editor.

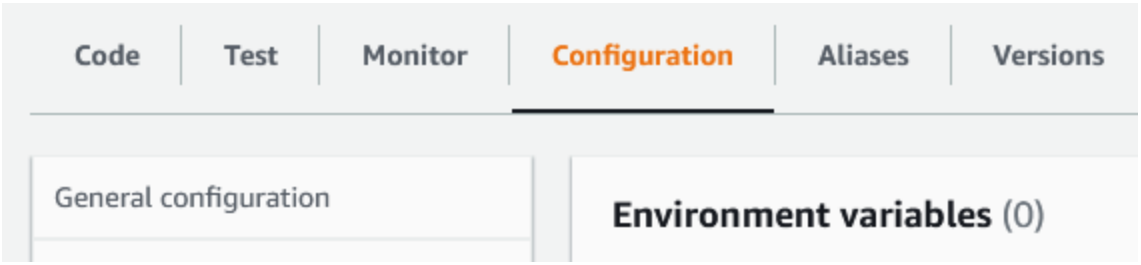


9. **Paste** the code acquired previously in this section on page 36.

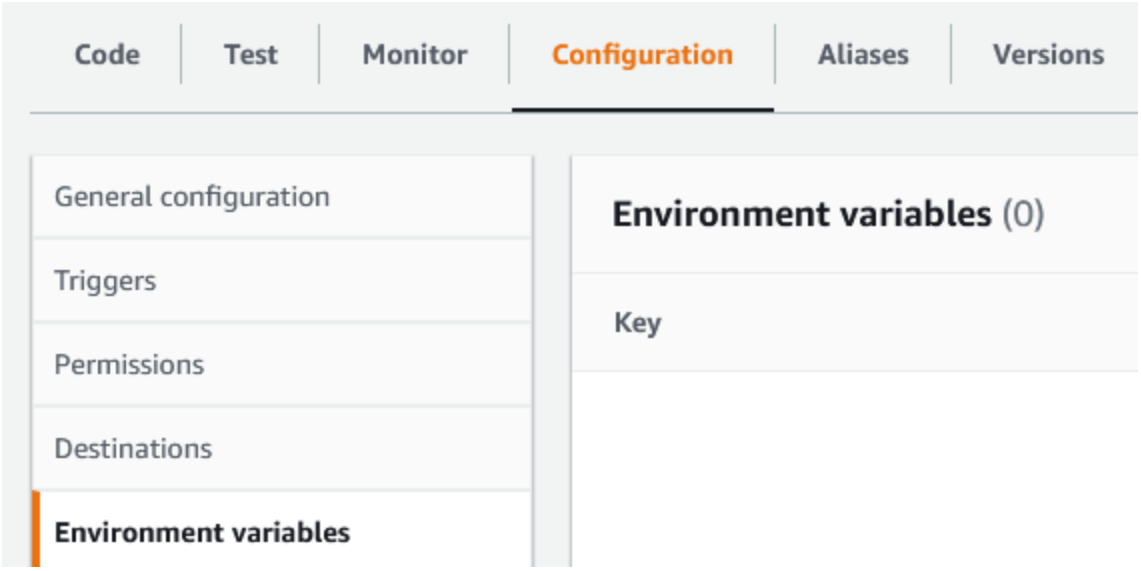
10. To deploy the code, click the **Deploy** button located above the code editor.



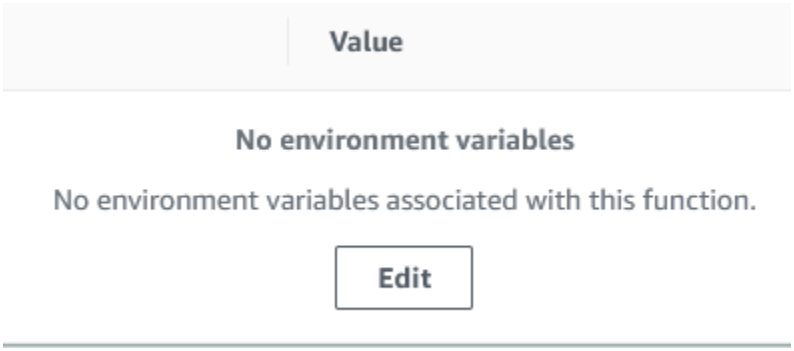
11. On the Lambda function's page, click the **Configuration** tab.



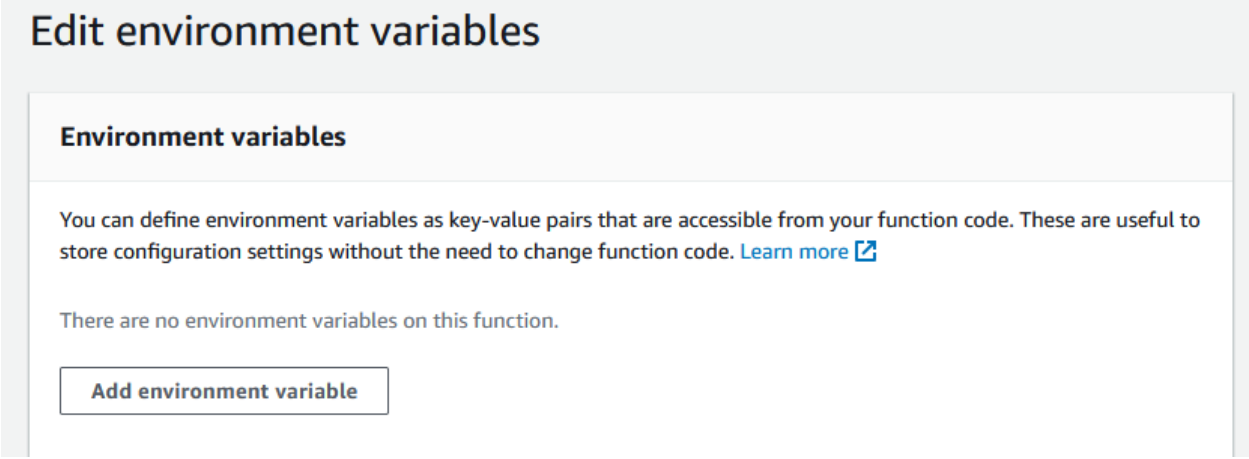
12. On the *Configuration* page, click **Environment variables** in the navigation panel.



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

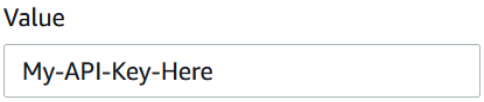


14. On the Edit environment variables page, click **Add environment variable**.



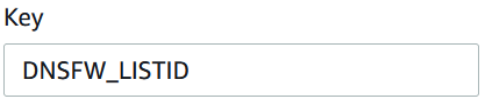
15. In the first *Environment Variable*, input **CSP_API_KEY** in the **Key** text field.

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

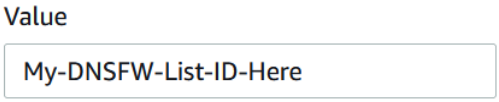


17. Click **Add environment variable** to add an additional environment variable.

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



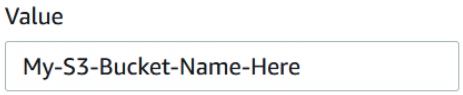
19. Input the **AWS Route 53 DNS Firewall domain list ID** that was acquired on *page 49* in the **Value** text field.



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

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

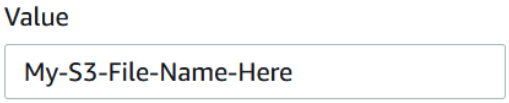
22. Input the **S3 Bucket name** that was created on *page 43* in the **Value** text field.



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

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

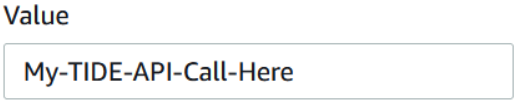
25. Input the **S3 file name** that was created on *page 45* in the **Value** text field.



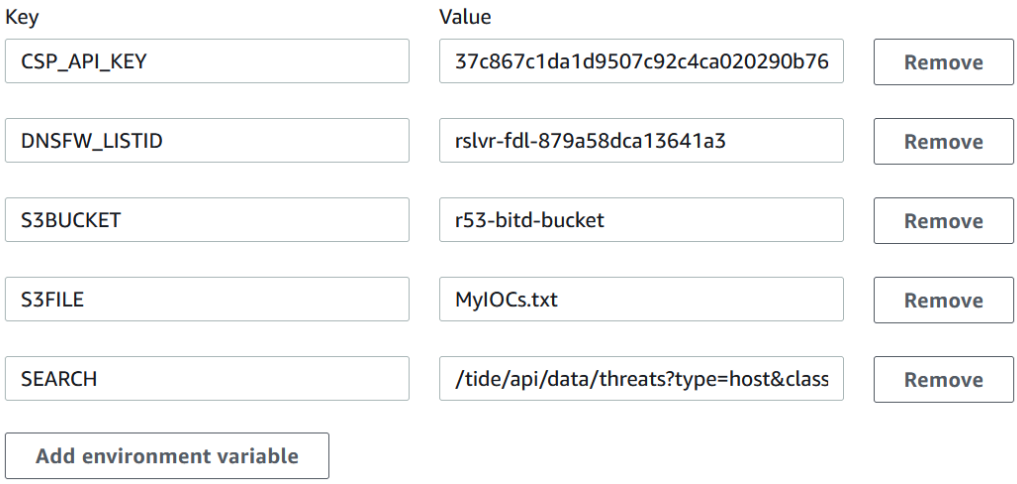
26. Click **Add environment variable** to add an additional environment variable.

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

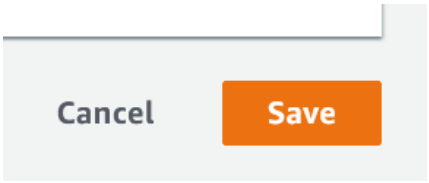
28. Input the **TIDE API call** that was created on *pages 46-48* in the **Value** text field.



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



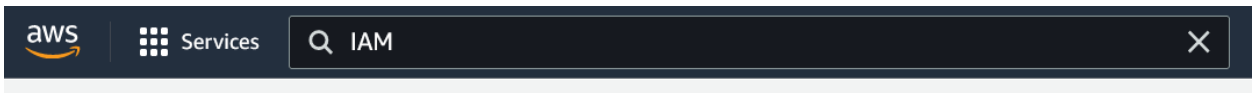
29. Click **Save** to confirm the addition of the newly created environment variables.



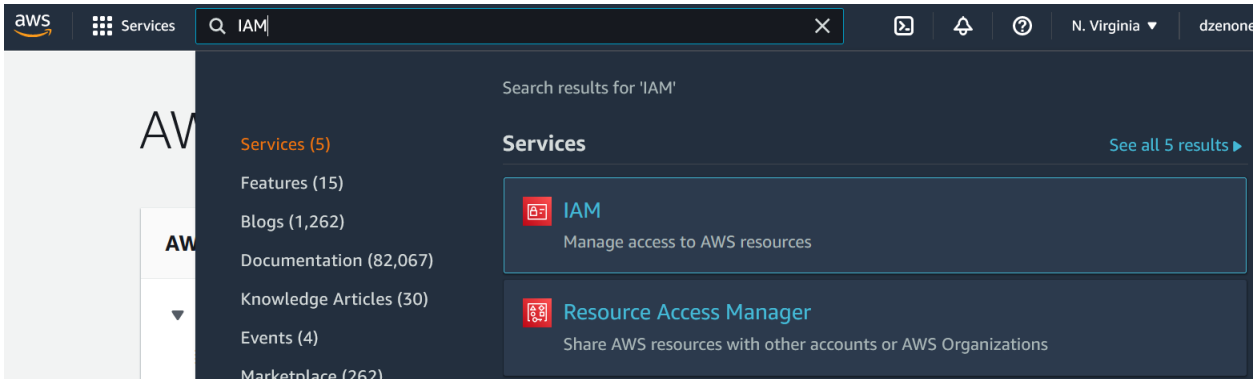
Create IAM Policies

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:

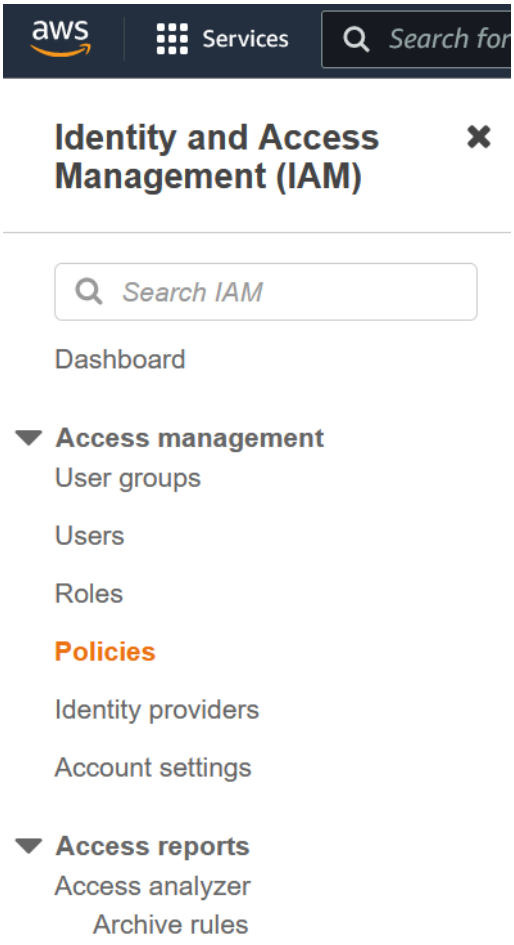
1. Input **IAM** into the *search bar* located at the top of the AWS interface.



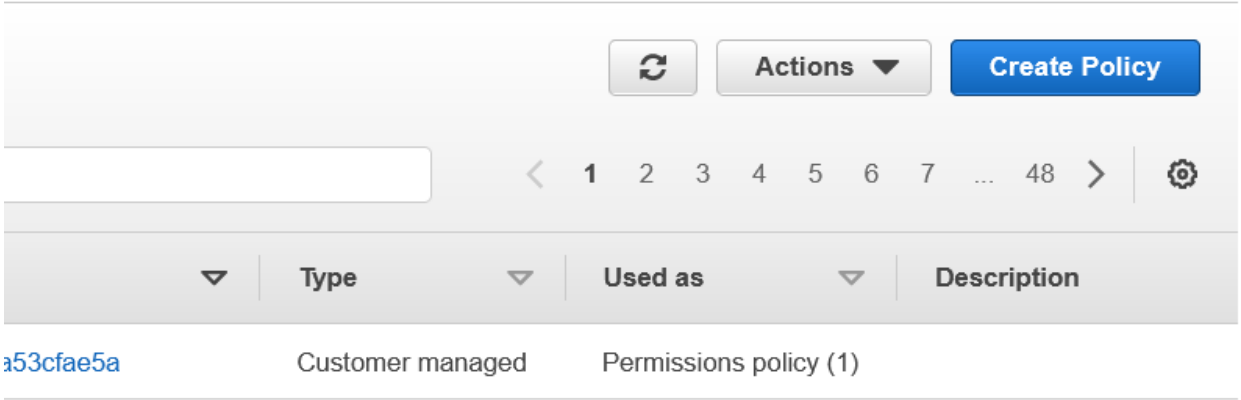
2. Locate and click on **IAM** to navigate to the *IAM* page.



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.



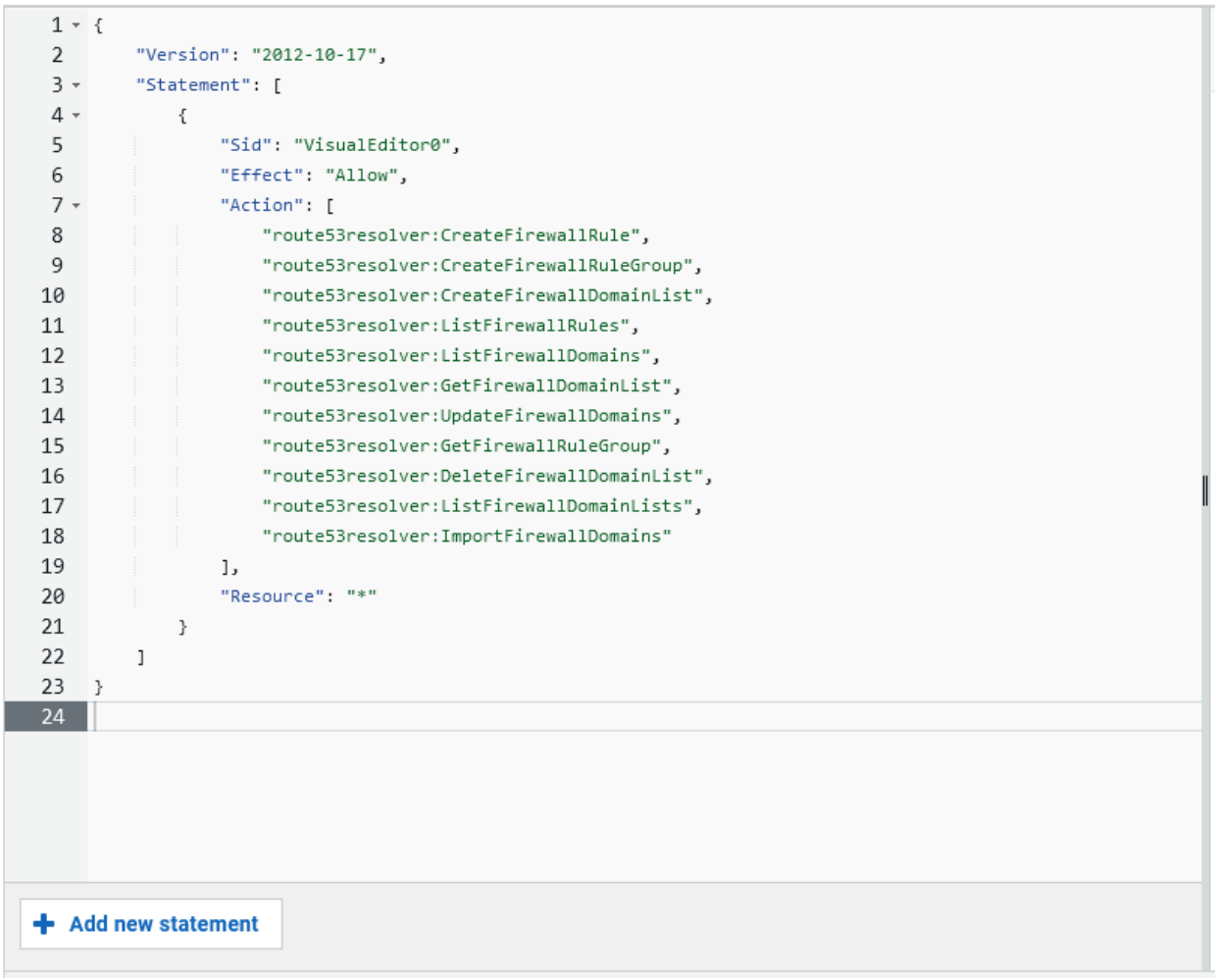
5. On the *Create Policy* page, click the **JSON** button.

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": "*"
    }
    ]
}
```

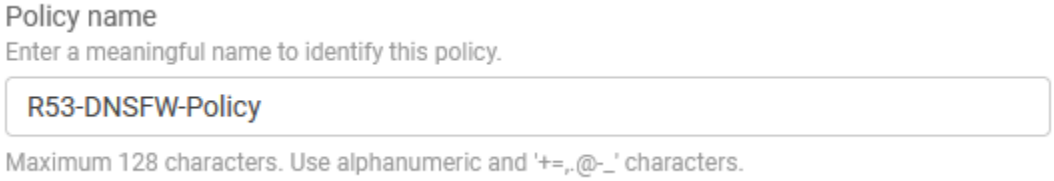
7. **Replace** all code in the JSON text box with the code copied from the previous step.

Policy editor

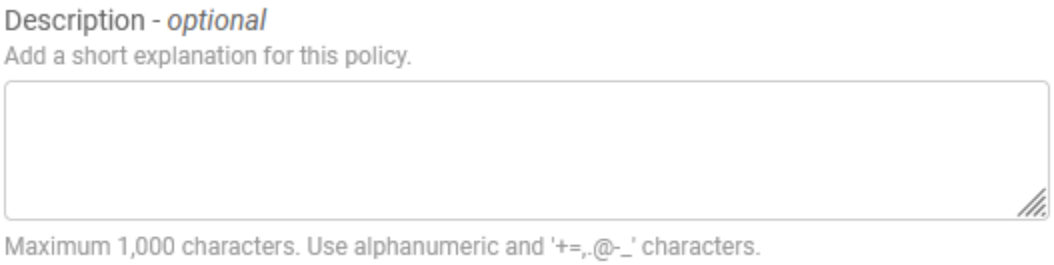


8. Click the **Next** button located on the bottom right of the page.

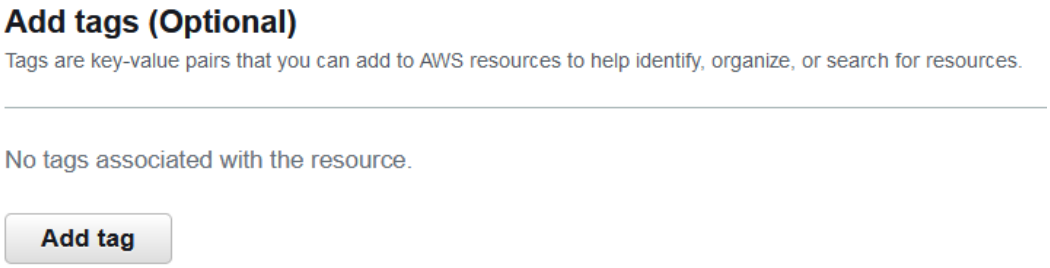
9. On the Review policy page, perform the following steps:
    - Give the policy a **Name.**



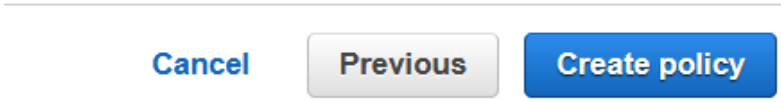
- (Optional) If desired, give the policy a **Description.**



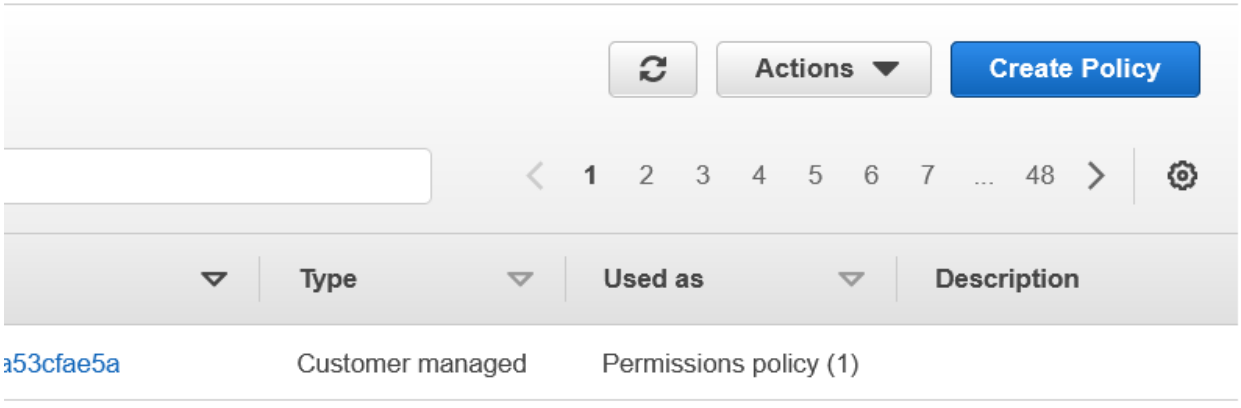
- (Optional) If desired, add tags via the **Add tag** button.



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



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

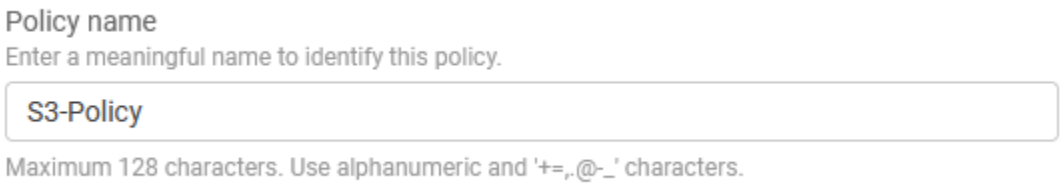
```
1  {
2      "Version": "2012-10-17",
3      "Statement": [
4          {
5              "Sid": "VisualEditor0",
6              "Effect": "Allow",
7              "Action": "s3:ListBucket",
8              "Resource": "arn:aws:s3:::test"
9          },
10         {
11             "Sid": "VisualEditor1",
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
```

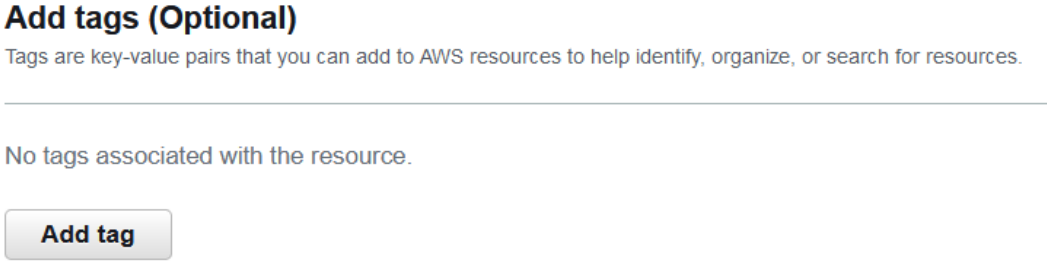
15. Click the **Next** button located on the bottom right of the page.

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

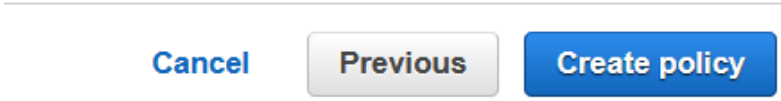


    - (Optional) If desired, give the policy a **Description.**

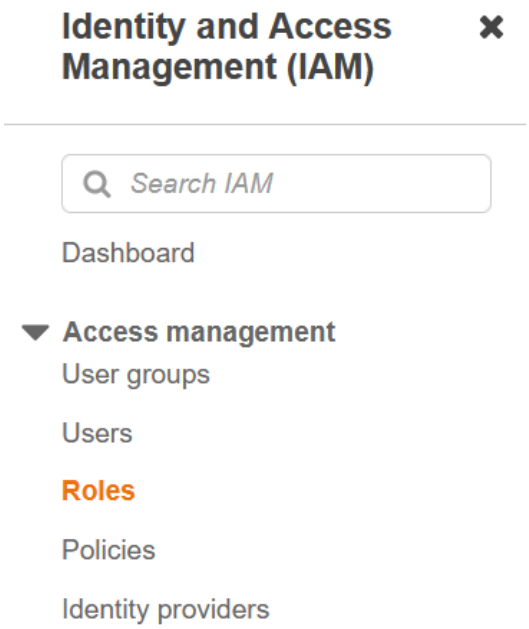
    - (Optional) If desired, add tags via the **Add tag** button.



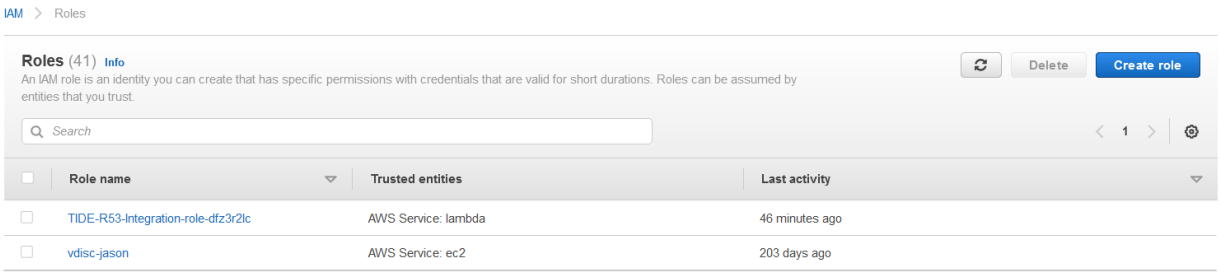
    - Click the **Create policy** button located on the bottom right of the page to confirm the creation of the Policy.



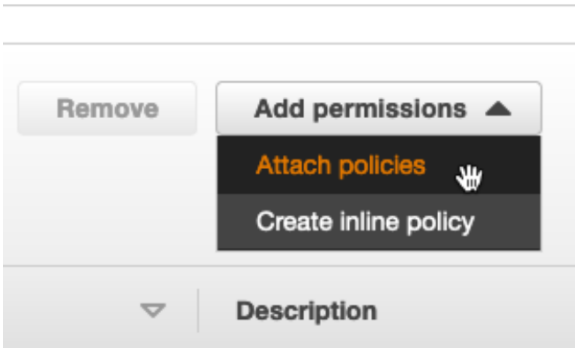
17. In the *IAM navigation pane*, click **Roles** located under the *Access management* header.



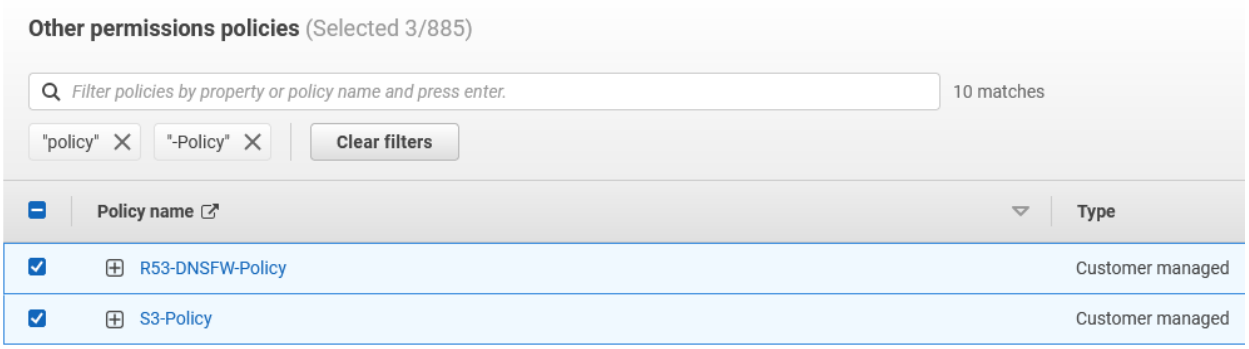
18. On the Roles page, locate and **click** the role that has been automatically created for your lambda function. *Note the role should contain the Lambda function's name in it. In the example screenshot, the Role name is Tide-R53-Integration-role-dfz32r2lc.*



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.



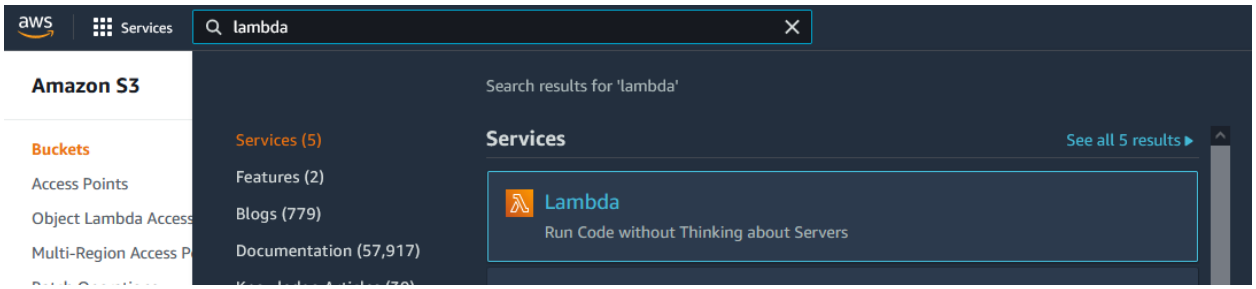
21. Click **Add permissions** to confirm the attaching of the two policies.

Test the Lambda Script

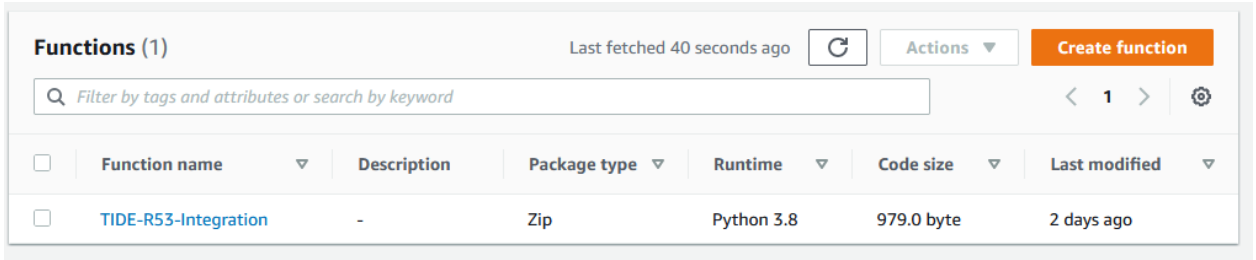
In order to test the lambda script, perform the following steps:

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

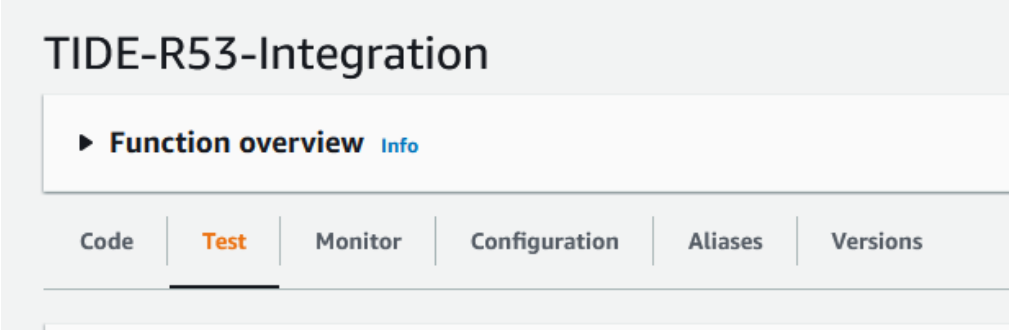
2. Locate and click on **Lambda** to navigate to the *Lambda* page.



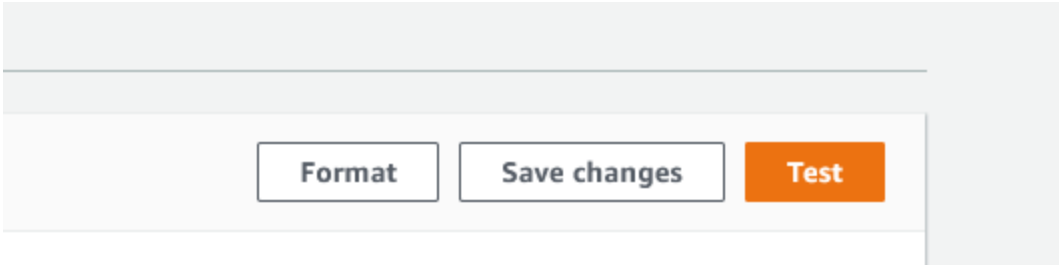
3. On the *Functions* page, locate and click the **Lambda function** you've just created.



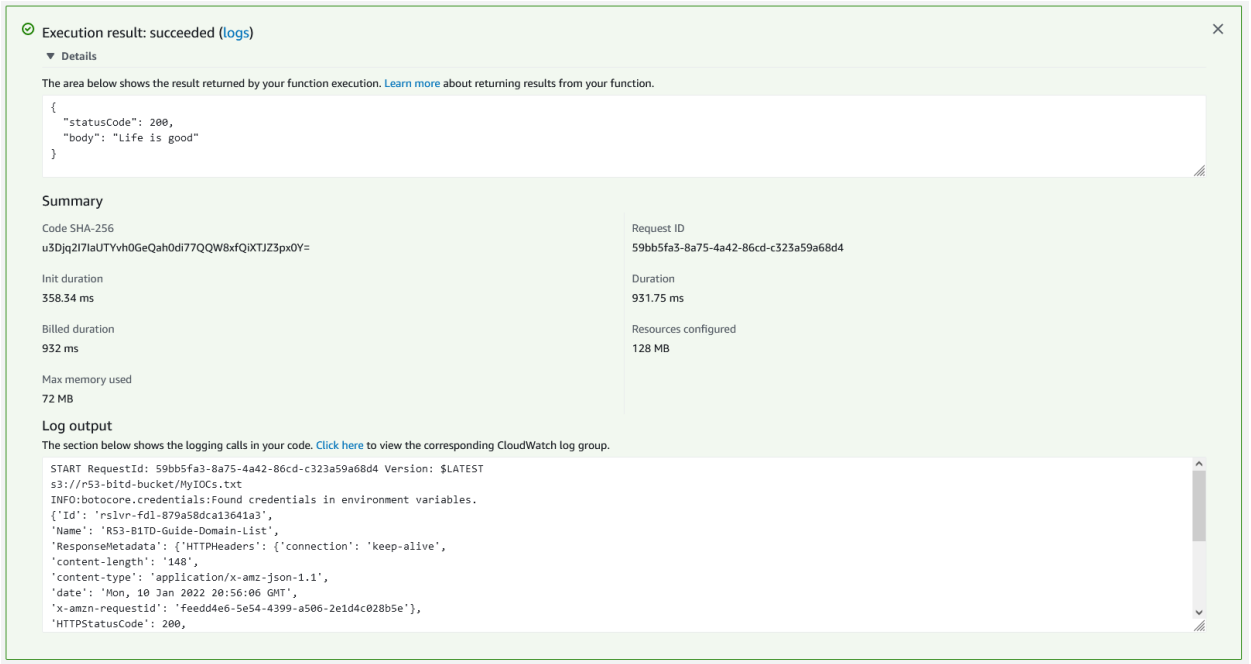
4. Click the **Test** tab located near the top of the function's page.



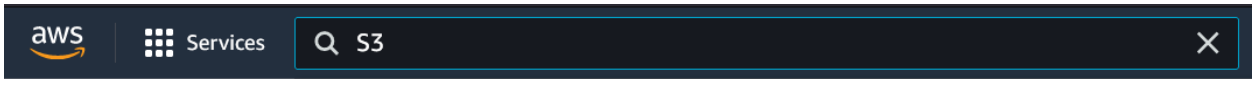
5. Click the **Test** button located on the top left of the Test event panel.



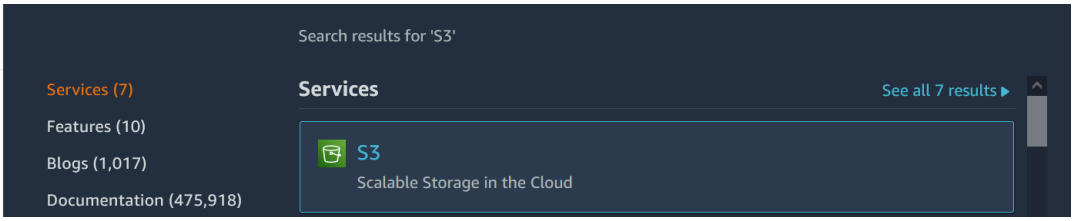
6. Above the Test event panel, the *Execution results* will show. Click the **Details** arrow to observe the details of the test.



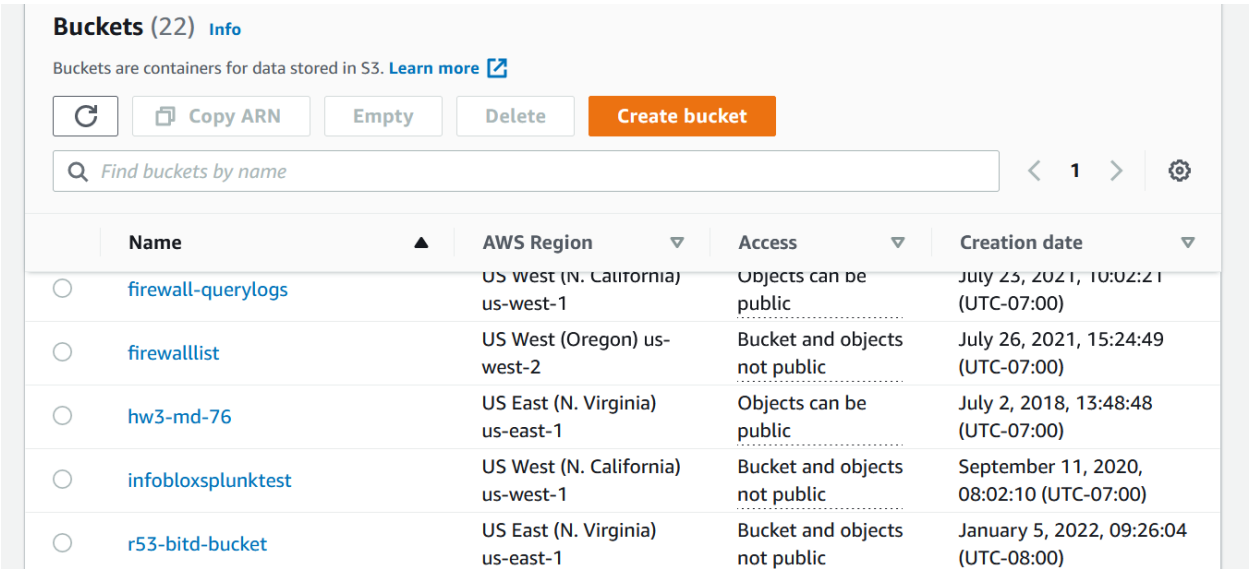
7. Navigate to the simple text file that holds the IOCs before they are added to the AWS R53 DNSFW domain list. Input **S3** into the *search bar* located at the top of the AWS interface.



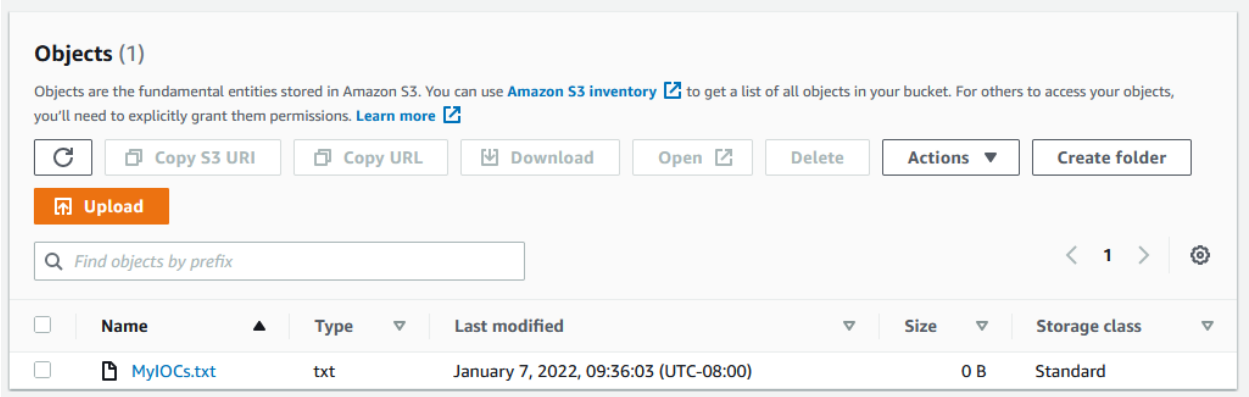
8. Locate and click on **S3** to navigate to the *Amazon S3* page.



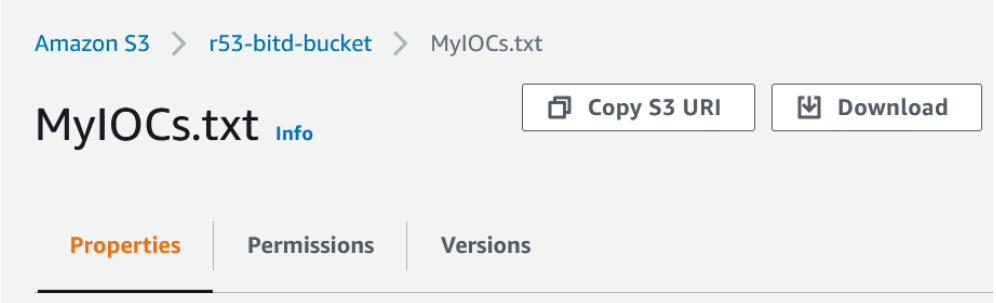
9. On the *Buckets* page, scroll down to the Buckets panel. Locate and click on the **S3 bucket** that is being used with this integration.



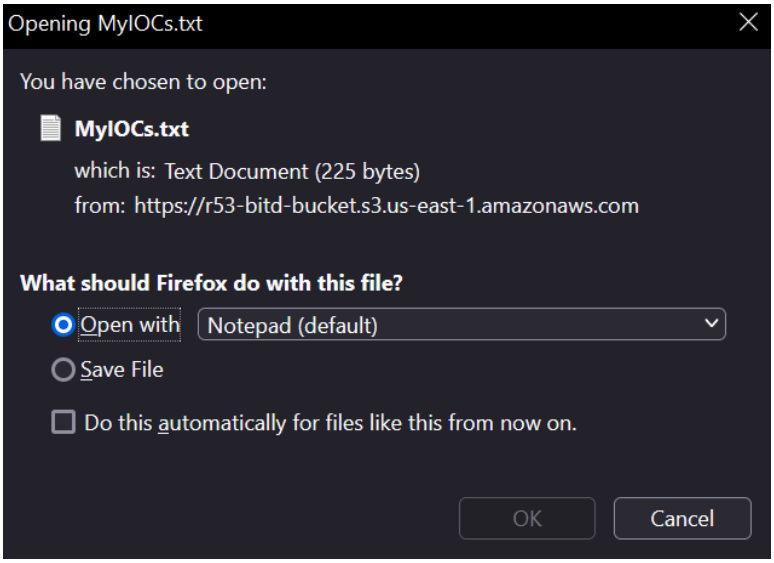
10. In the Objects panel, locate and **click** the simple text file that was created for this integration. *Note, in the example screenshot, the file's name is MyIOCs.txt.*



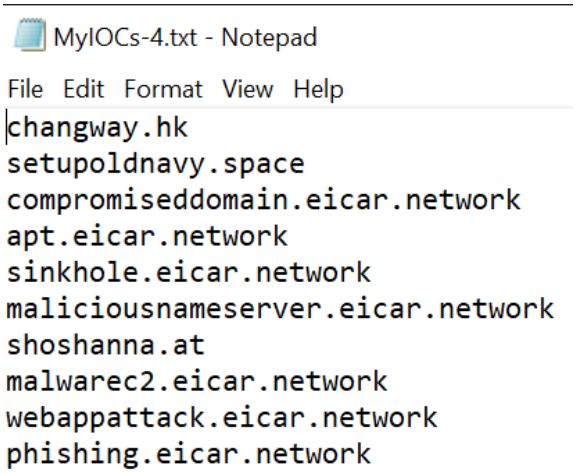
11. On the text file's page, click the **Download** button located near the top of the page.



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

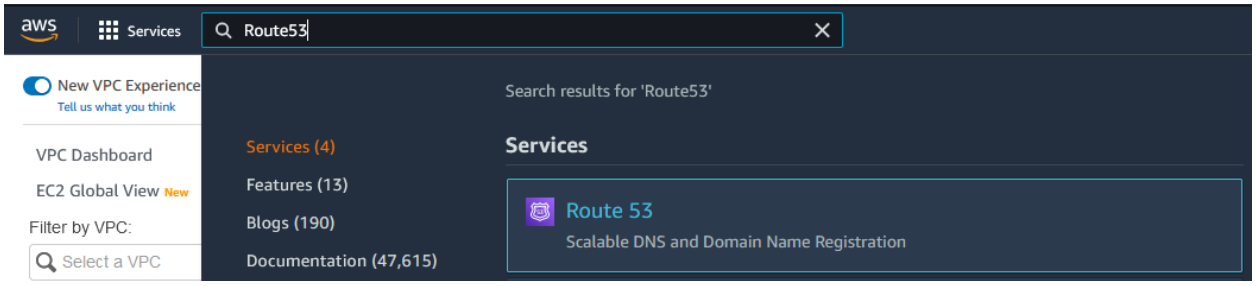


- Observe the contents of the text file. As mentioned earlier in the guide, IOCs should be one per line.

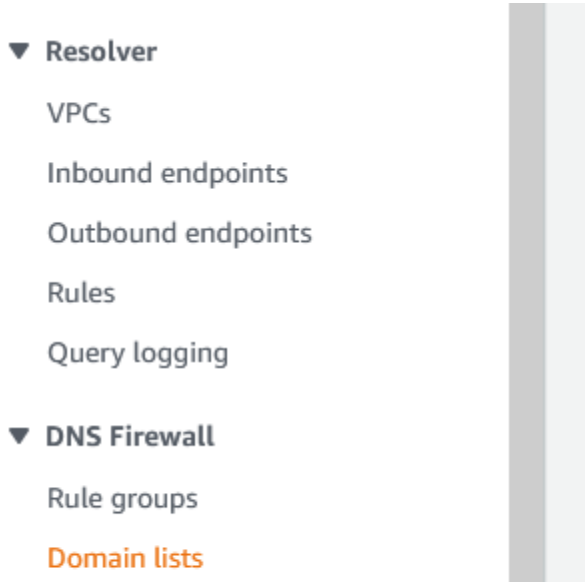


13. To observe the IOCs added to your AWS Route 53 DNS Firewall domain list via the test, navigate to the Route 53 page. input **Route53** into the *search bar* located at the top of the AWS interface.

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

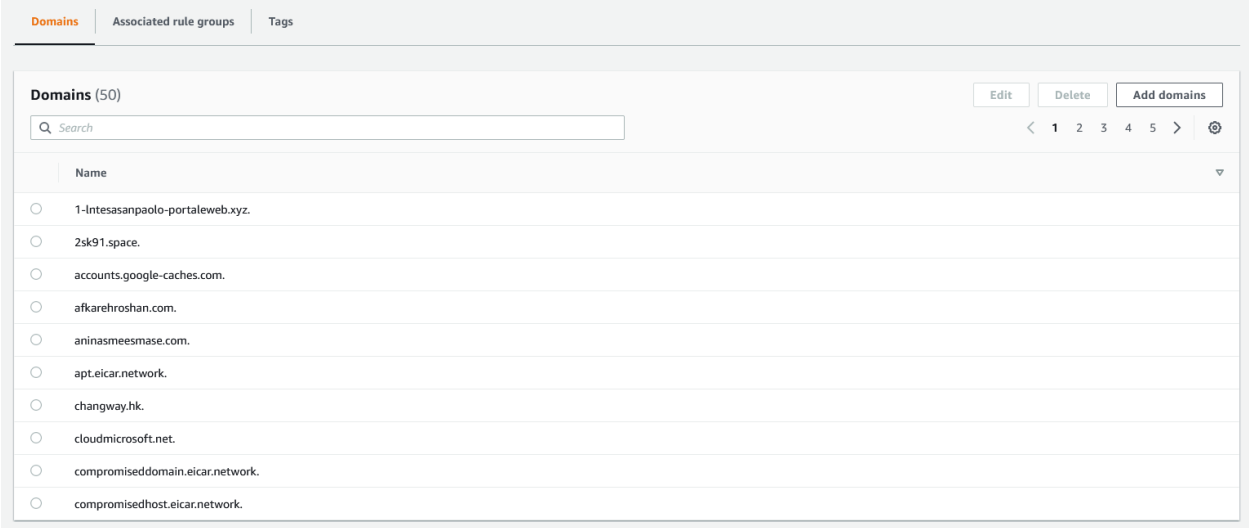


15. In the *Route 53 navigation pane*, click **Domain List** located under the *DNS Firewall* header.



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.

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

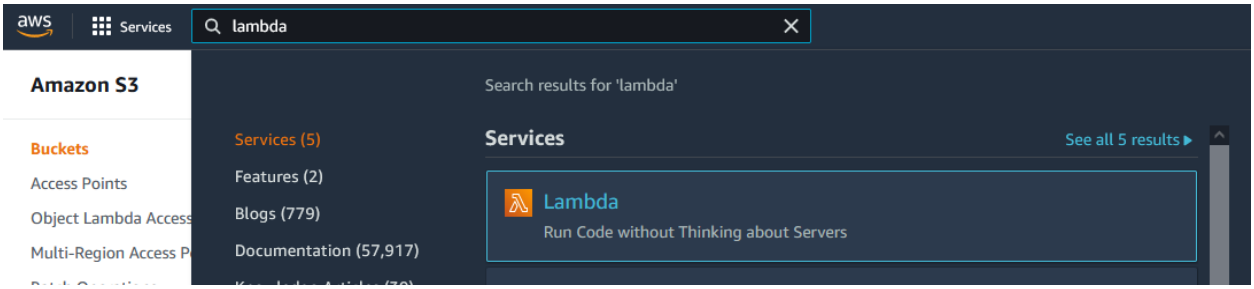


Automate the script execution via EventBridge

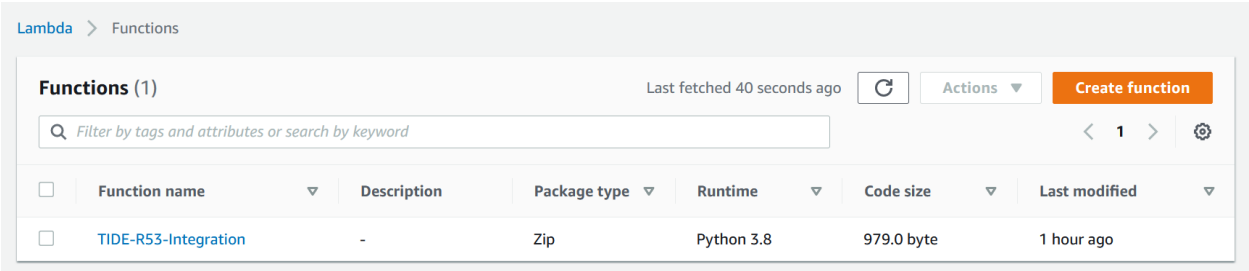
To automate the importing of IOCs from Infoblox an EventBridge can be used. This allows for the ingestion of IOCs from Infoblox via the Python script to occur on a schedule. To configure an Amazon EventBridge, perform the following steps:

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

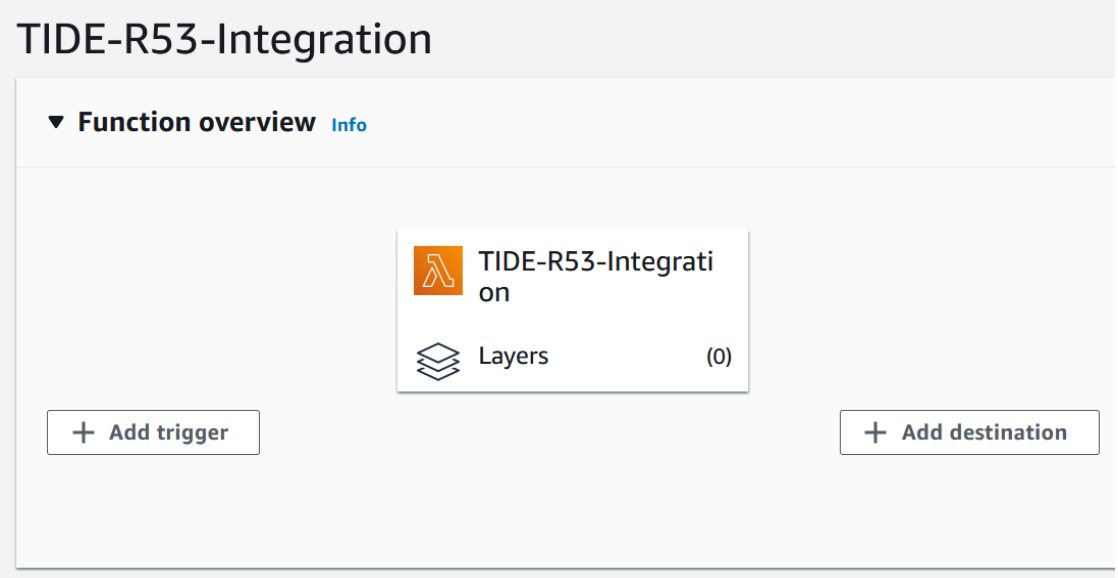
2. Locate and click on **Lambda** to navigate to the *Lambda* page.



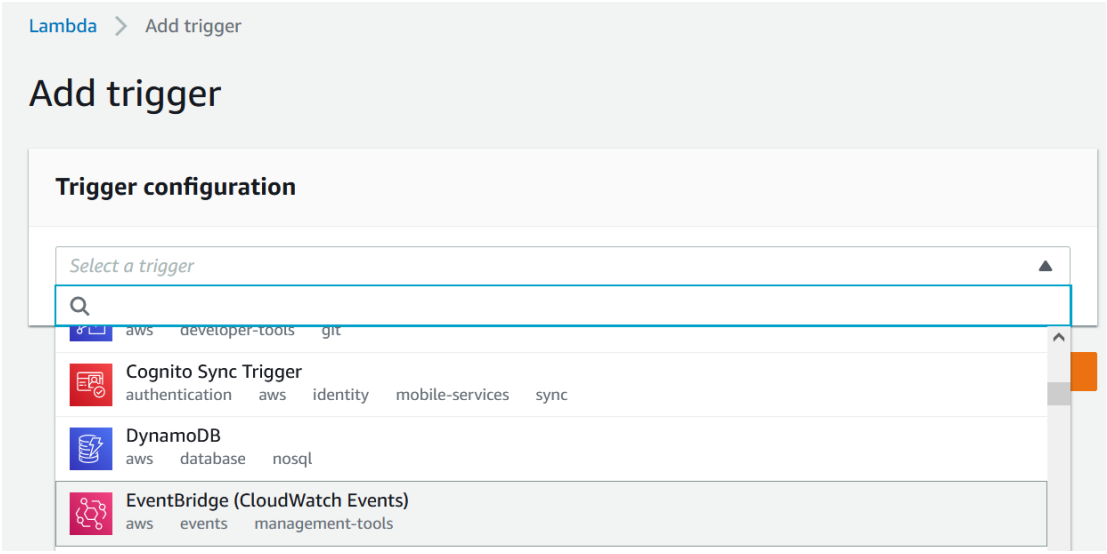
3. Locate and **click** the Lambda function that was created in the previous section.



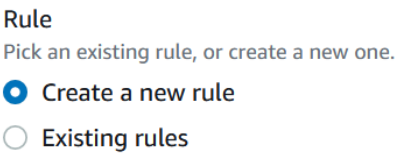
4. In the *Function overview* panel of the function's page, click the **Add trigger** button



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



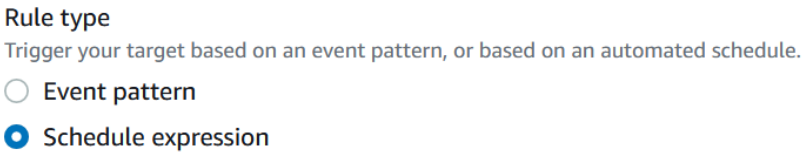
    - Under the Rule header, click the **Create a new rule** bubble.



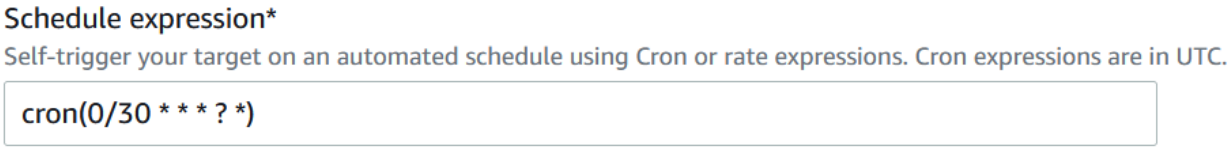
- Give the Rule a **name.**

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

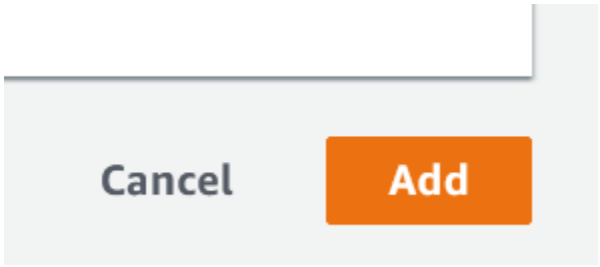
- Under the Rule type header, click the **Schedule expression** bubble.



- 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*.



- 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