Lab Instructions

Site: Barracuda CloudGen WAF Training Portal
Course: API Security with Barracuda WAF - automated and simplified
Book: Lab Instructions
Printed by: aravindan a
Date: Monday, 24 May 2021, 1:28 AM

Table of contents

1. Lab Objective

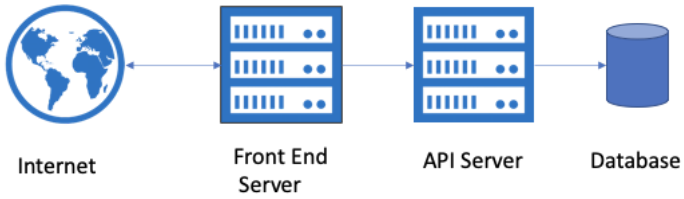
Objective

The objective of this hands on session is to deploy a Web Application called the PetStore and provide security at each layer.

About the Petstore Application

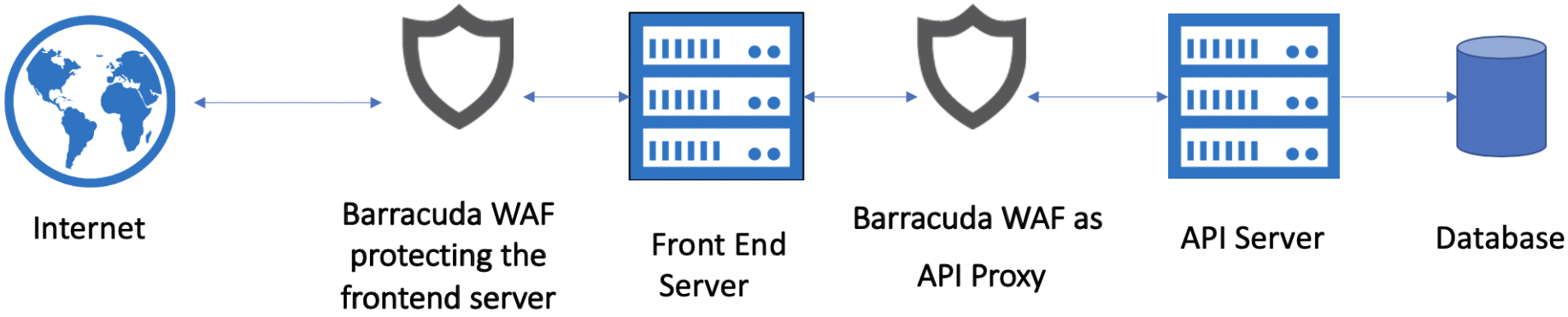
Pet Store comprises of a backend application i.e API Server and a Front End Server.

The Frontend Server communicates to the backend application through REST API. The frontend server stores and retrieves data from the database through APIs. Clients can connect to the application via the front end server.



Deploying security for the Pet Store application

We will use the Barracuda WAF Virtual Machine solution to deploy security for the front end and the API server of Pet Store. The intended deployment can be schematically represented as below:



This design provides the following benefits:

1. Defence in depth: Barracuda WAF will protect the Pet Store application from any malicious requests from the attackers.

2. The API server can be scaled up as per demand or migrated to a different network without too much of network / deployment changes.

3. If the Pet Store company wants to change the front end server to adopt a modern web application framework, it can be done wiithout changing the network design.

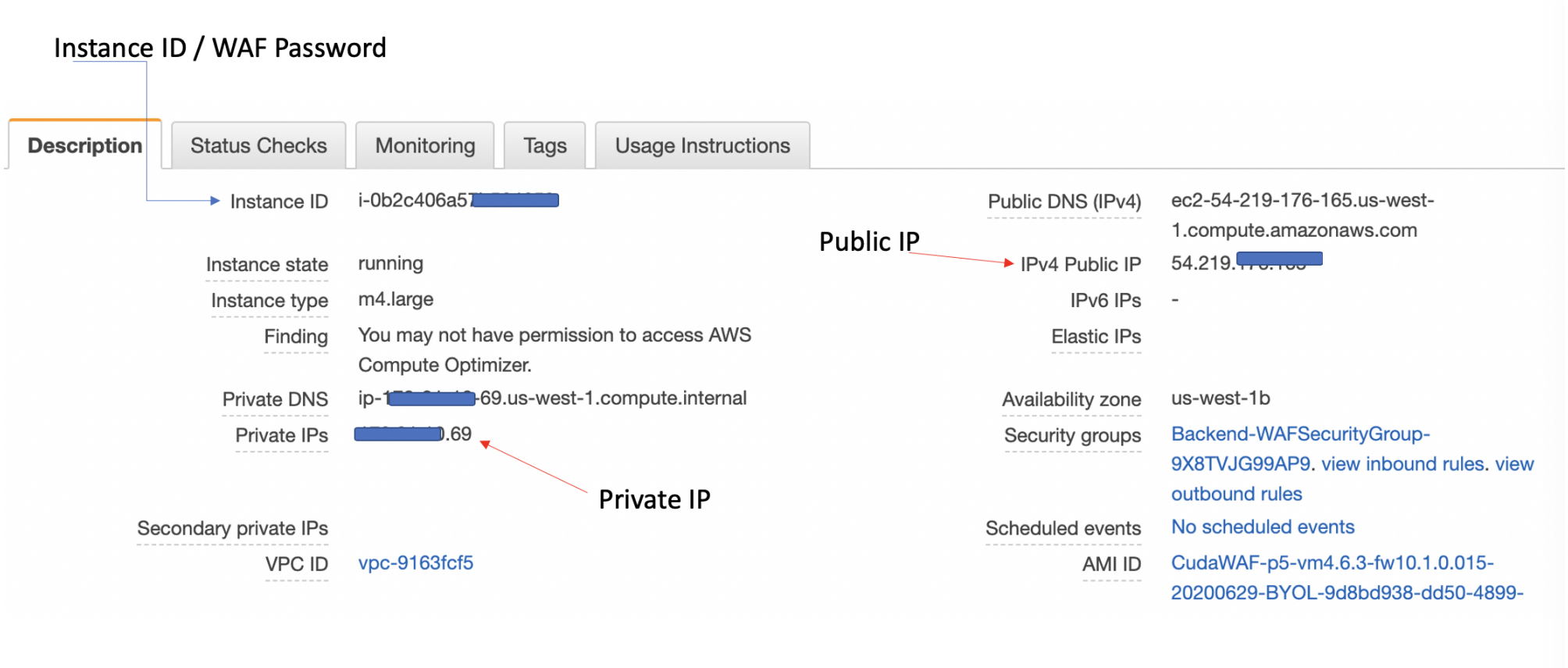
4.The Pet Store company can expose the API Server to another service provider to integrate their services, for example, to add order payment feature or to support auxillary services like pet care accessories.

2. Lab environment setup

The environment for the lab will have two resources auto created in the AWS Oregon Region:

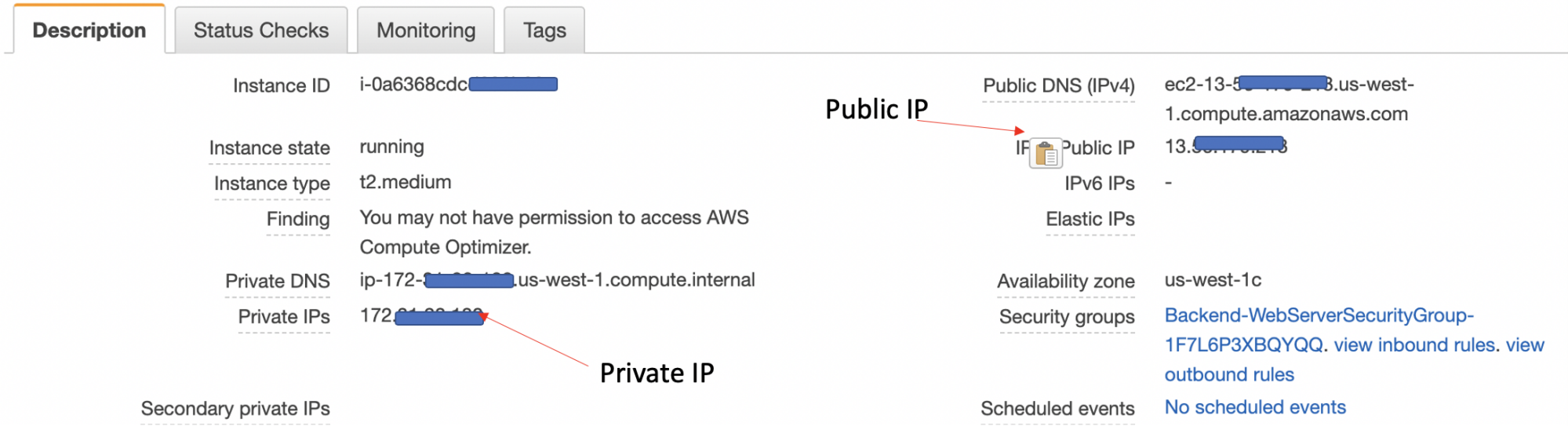
1. Barracuda WAF

Make a note of the AMI-ID (this is the password to login to the WAF), Public IP and Private IP of the Barracuda WAF.



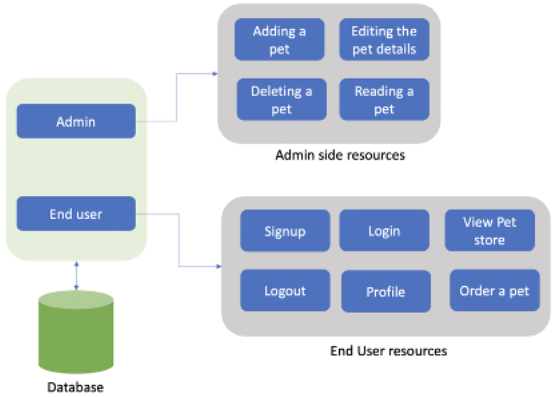
2. Backend API Server

Make a note of the public IP and the private IP of the Backend API Server


Description
Status Checks
Monitoring
Tags
Instance ID
i-0a6368cdc[redacted]
Instance state
running
Instance type
t2.medium
Finding
You may not have permission to access AWS Compute Optimizer.
Private DNS
ip-172-[redacted].us-west-1.compute.internal
Private IPs
172.[redacted]
Secondary private IPs
Public DNS (IPv4)
ec2-13-[redacted].us-west-1.compute.amazonaws.com
IPv4 Public IP
13.[redacted]
IPv6 IPs
-
Elastic IPs
Availability zone
us-west-1c
Security groups
Backend-WebServerSecurityGroup-1F7L6P3XBQYQQ. view inbound rules. view outbound rules
Scheduled events
No scheduled events
Public IP
Private IP

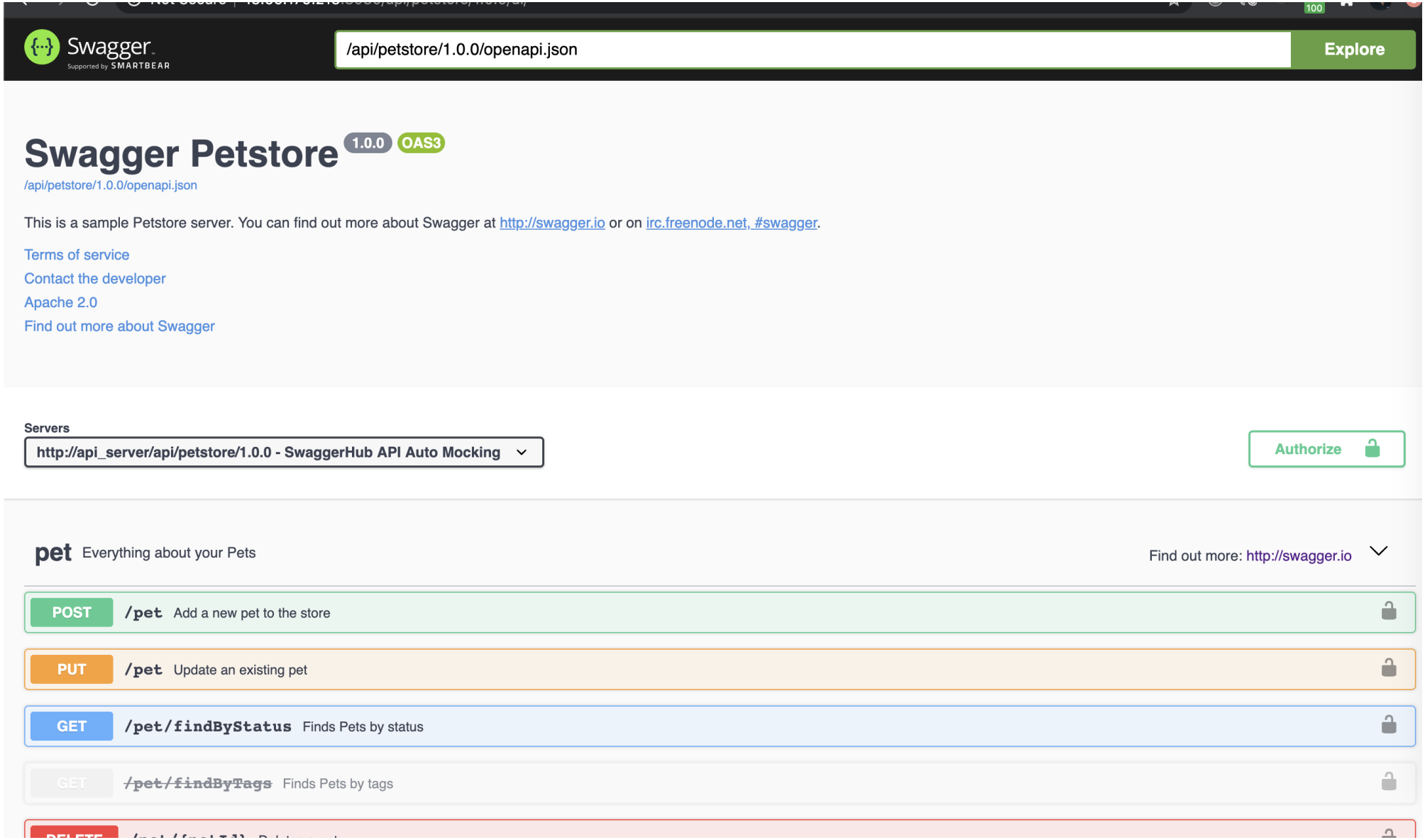
3. Familiarize with the Backend REST API

A schematic representation of the PetStore REST API is shown here:

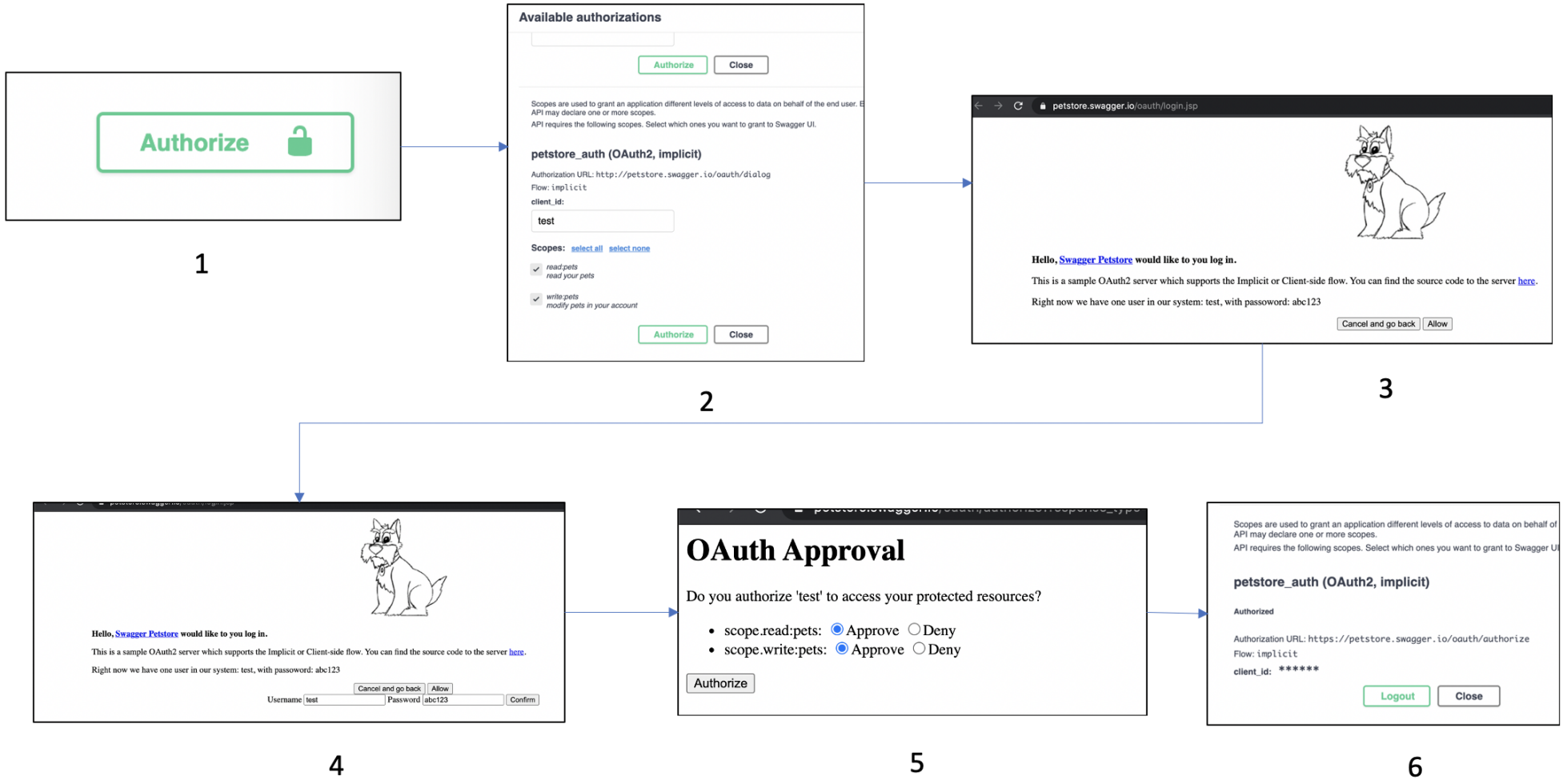


PetStore's API Documentation is available at the below address:

https://petstore.swagger.io/



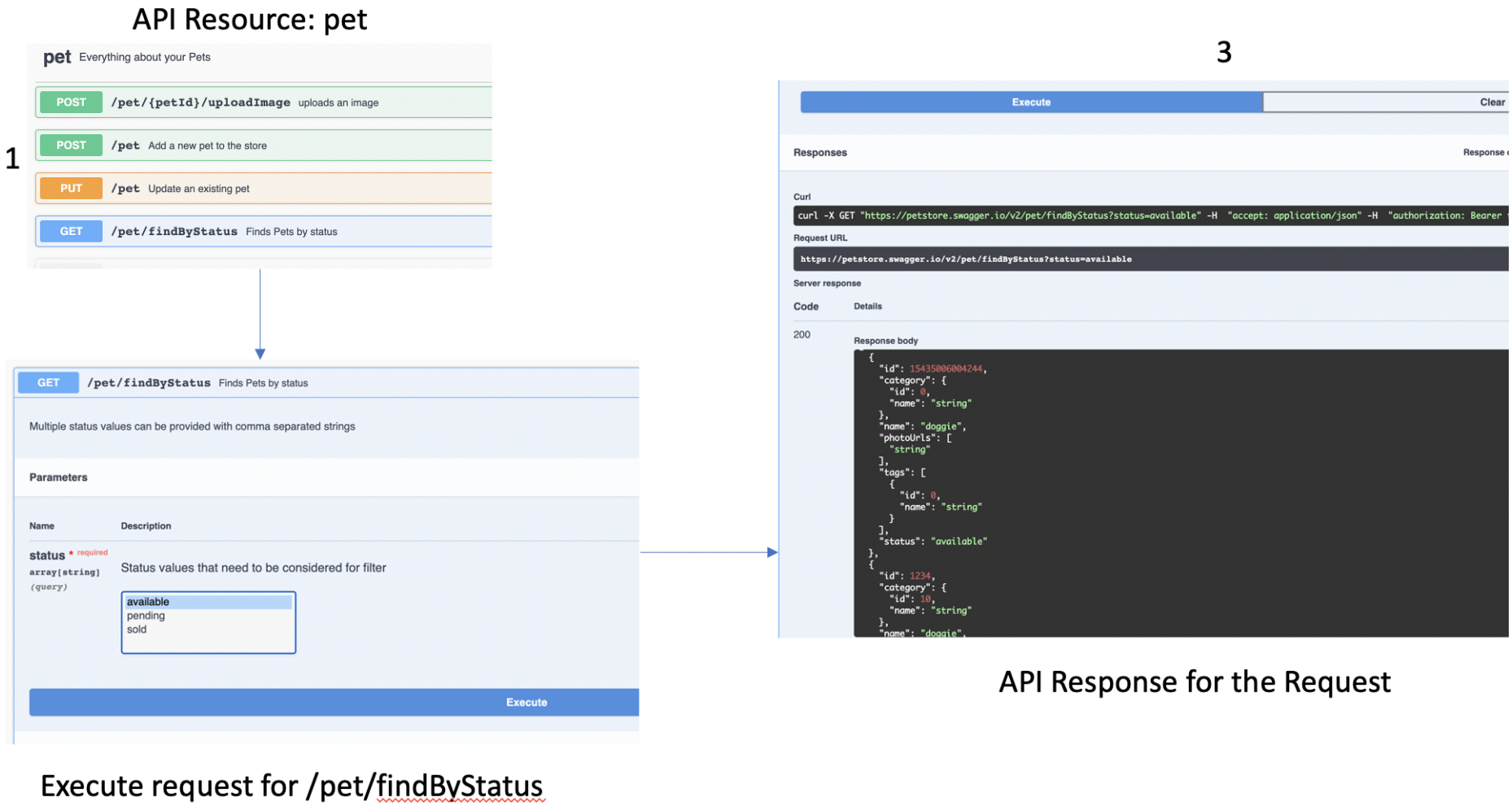
1. Authenticating as Admin



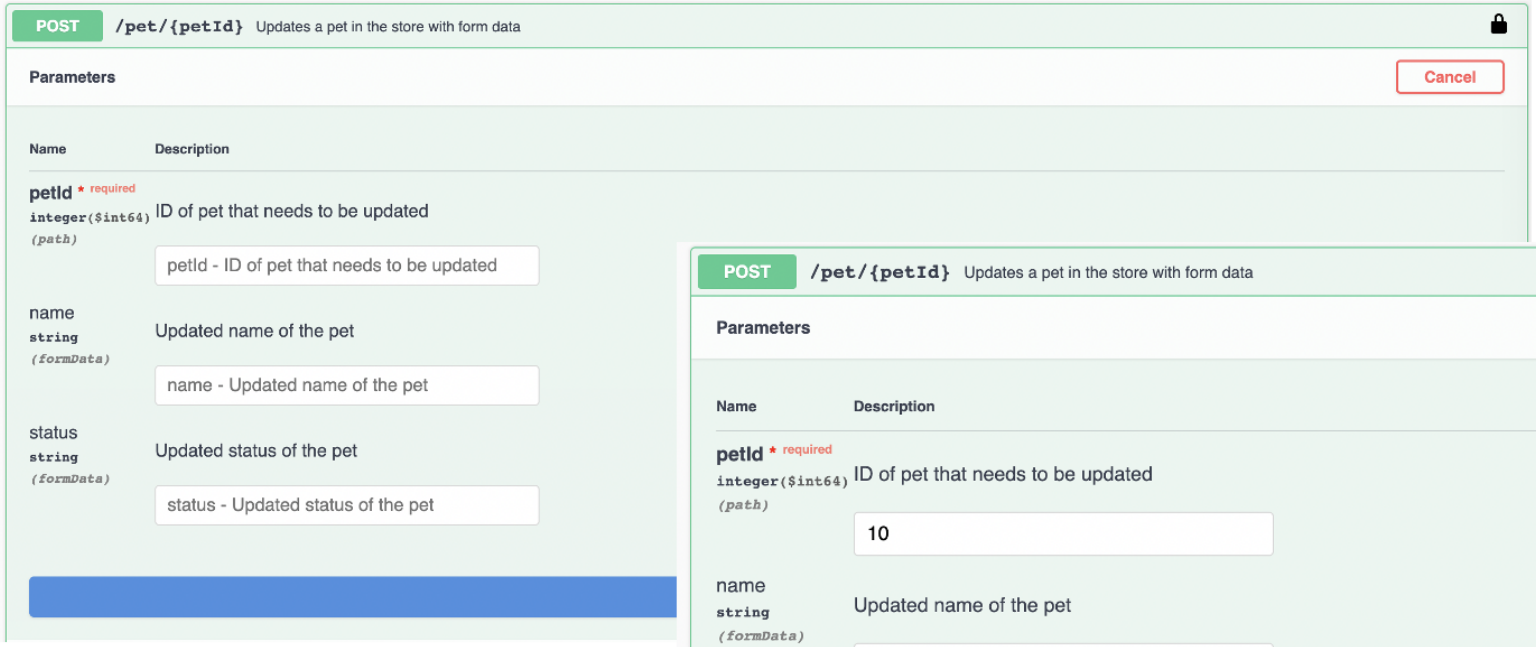
2. Creating, Updating, Reading and Deleting Resources (CRUD Operations)

Read : Getting Information about a resource

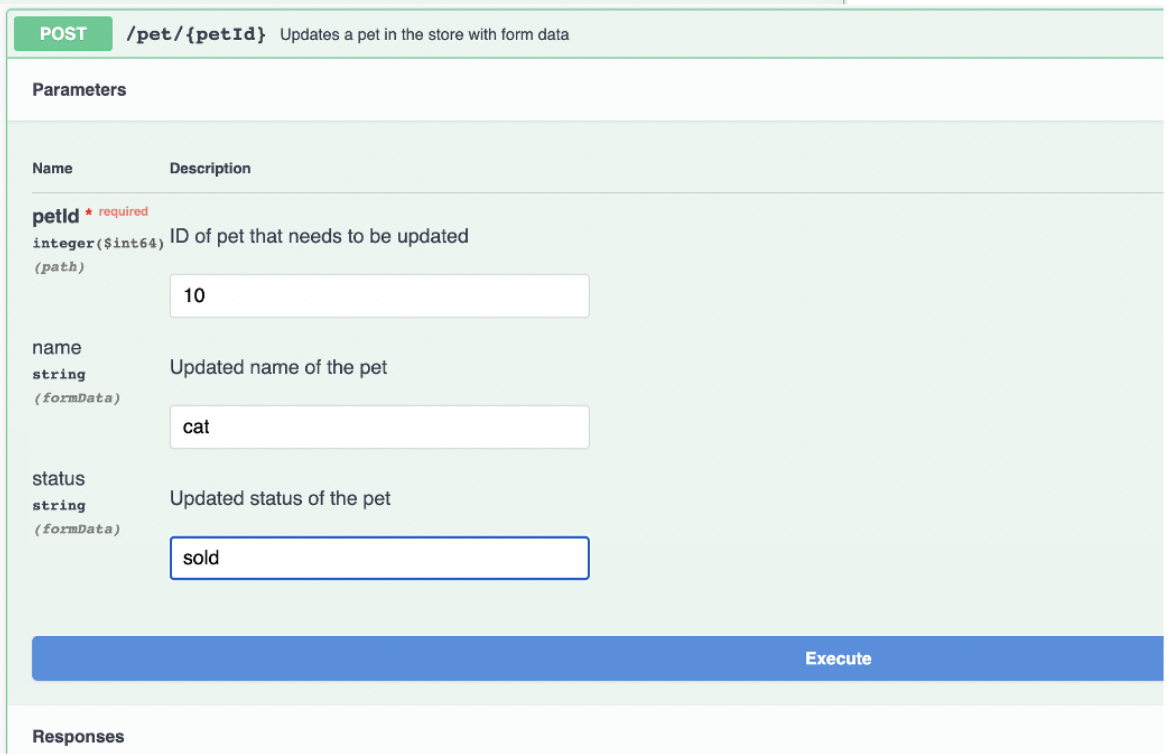
Uses the GET HTTP Method



Create:
Creating a resource: Uses the POST HTTP Method


POST
/pet/{petId}
Updates a pet in the store with form data
Parameters
Cancel
Name
Description
petId * required
integer($int64)
(path)
ID of pet that needs to be updated
petId - ID of pet that needs to be updated
name
string
(formData)
Updated name of the pet
name - Updated name of the pet
status
string
(formData)
Updated status of the pet
status - Updated status of the pet

1


POST
/pet/{petId}
Updates a pet in the store with form data
Parameters
Name
Description
petId * required
integer($int64)
(path)
ID of pet that needs to be updated
10
name
string
(formData)
Updated name of the pet
cat
status
string
(formData)
Updated status of the pet
sold
Execute
Responses

2

4. Access and configure the Barracuda WAF

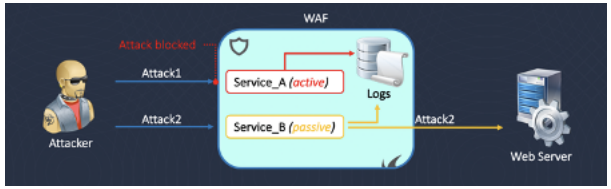
Introduction

The Barracuda Web Application Firewall blocks an ever-expanding list of sophisticated web-based intrusions and attacks that target applications hosted on web servers and in the cloud. The Barracuda Web Application Firewall scans all inbound web traffic to block attacks and inspects the HTTP responses from the configured back-end servers for Data Loss Prevention (DLP).

Security Policy Modes on the Barracuda WAF

Mode – The mode determines how the service responds to offending traffic. It can either be Active Mode or Passive Mode.

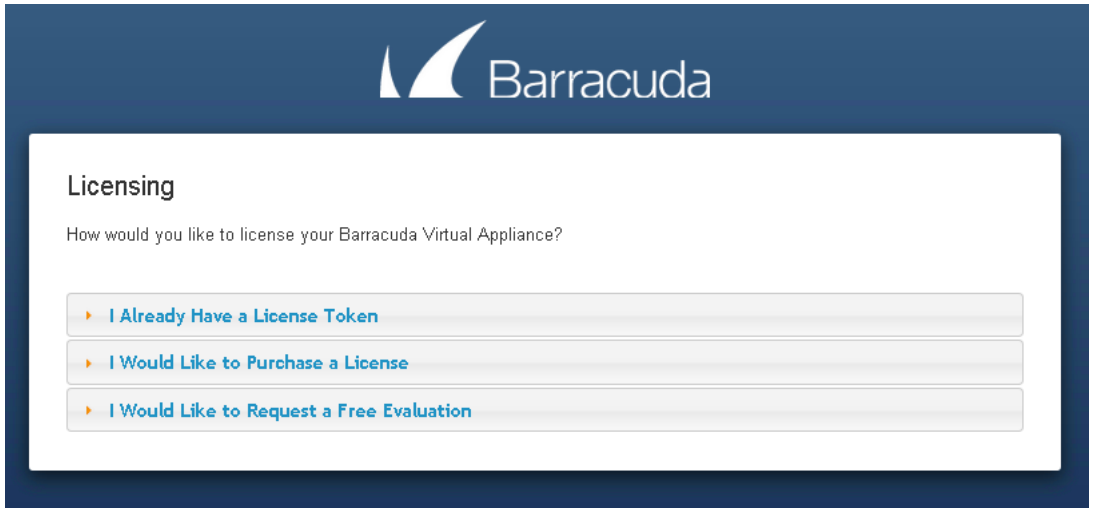
- *Passive* mode logs violating events but allows the request to pass through. This is the **default** mode.
- *Active* mode performs the action configured in association with the perceived threat.
  Note: *Passive* mode is recommended in the initial stages of deployment so that traffic to the service is not broken due to false positives. All traffic translation rules continue to work in both Active and Passive modes.



Getting Familiar with the Barracuda WAF

To connect to your Barracuda WAF : http://<publicIP of the Barracuda WAF>:8000/

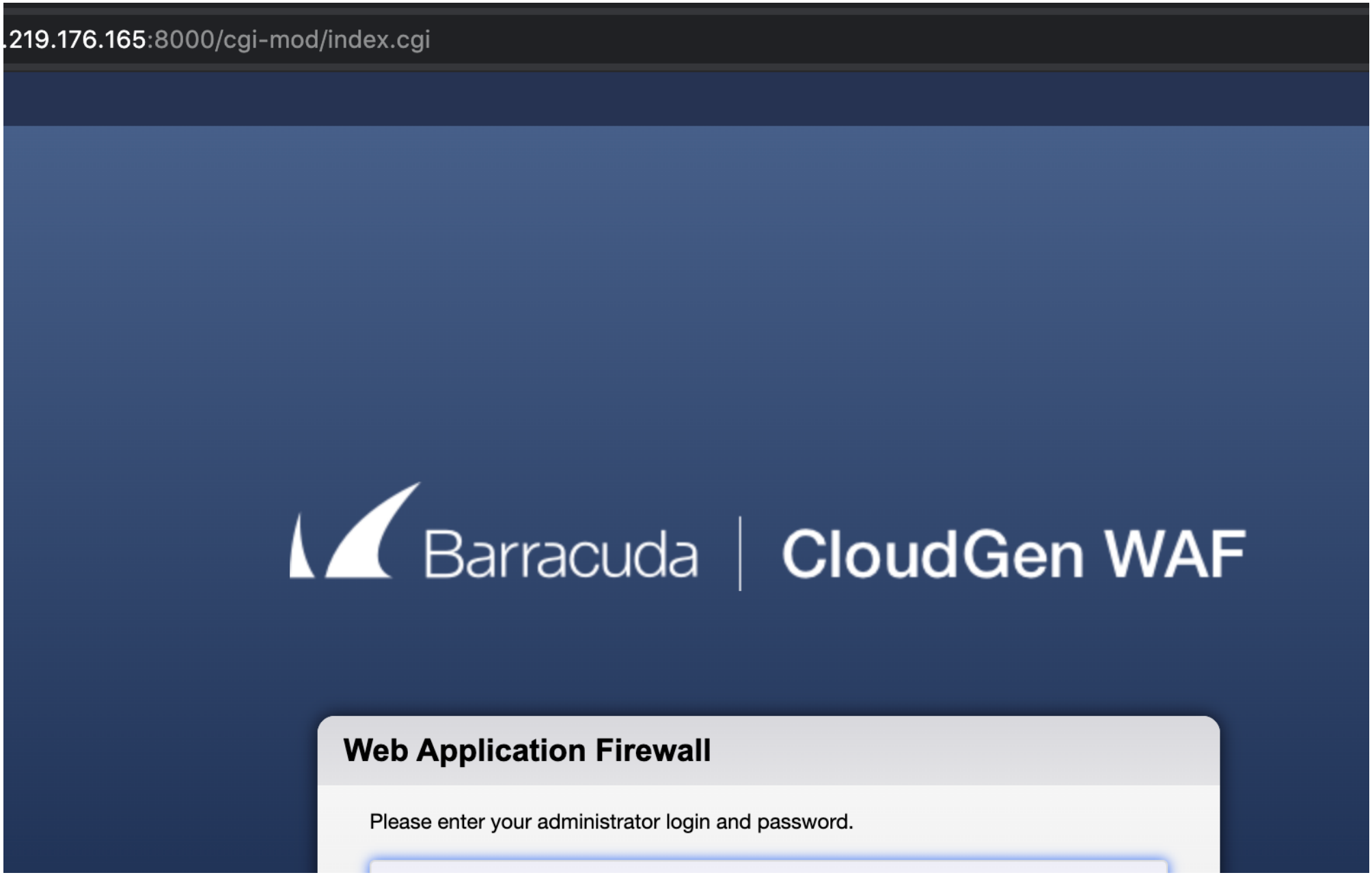
After the boot process is complete, the **Licensing** page displays with the following options:

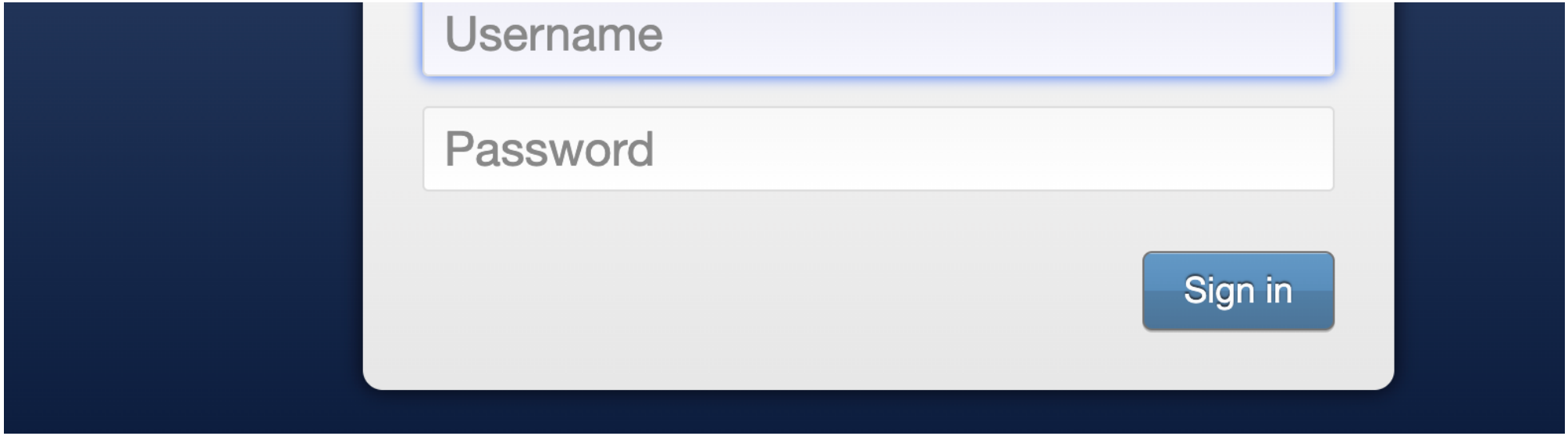


From the 3 options, choose the last i.e. "I would like to request a free Evaluation".

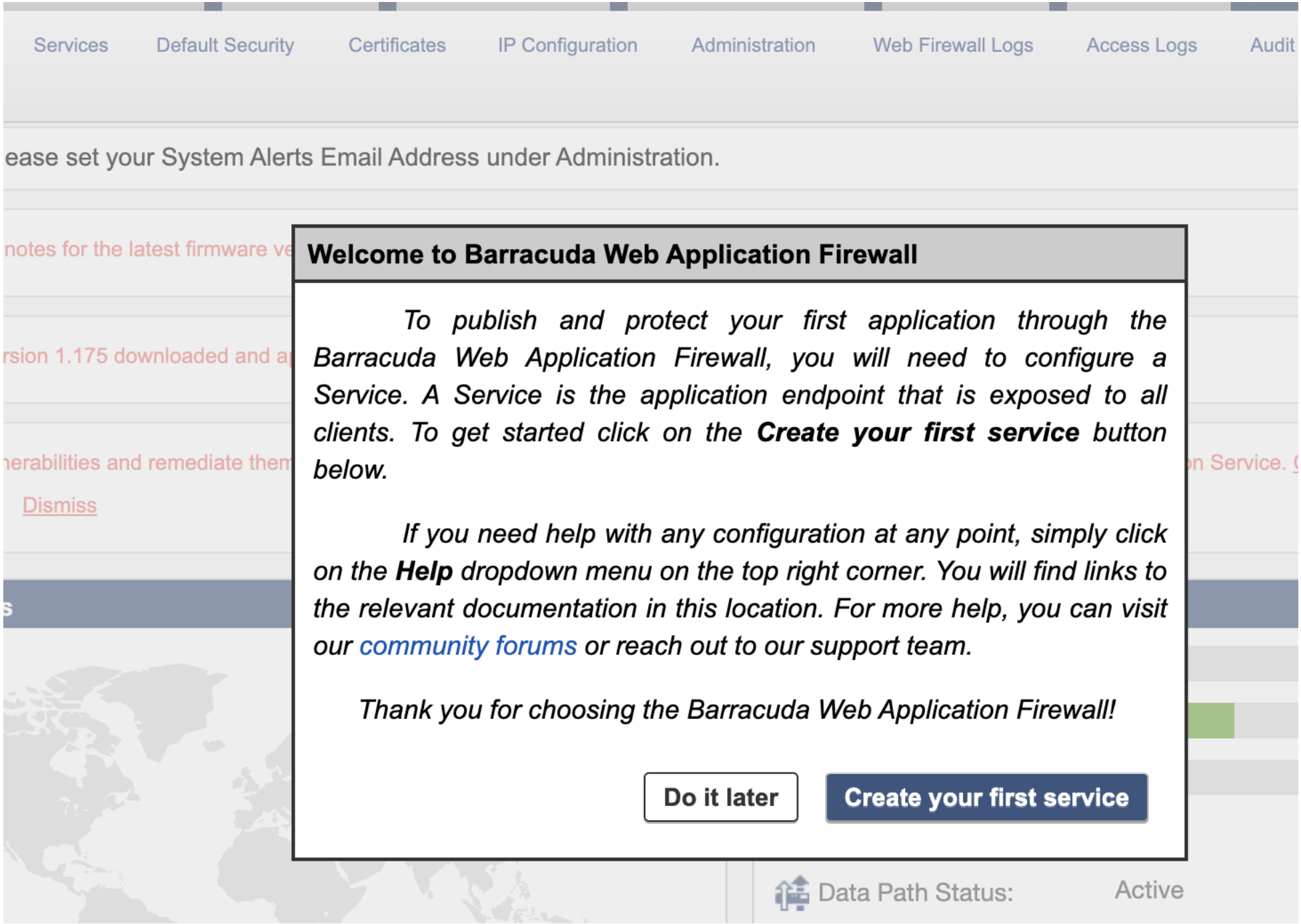
Use this option to get 30 days free evaluation of the Barracuda CloudGen WAF. Provide the required information in the form, accept the terms and conditions, and click **Evaluate**.

The Barracuda CloudGen WAF connects to the Barracuda Update Server to get the required information based on your license, and then reboots automatically. Allow a few minutes for the reboot process. Once the instance is provisioned, you are redirected to the login page.

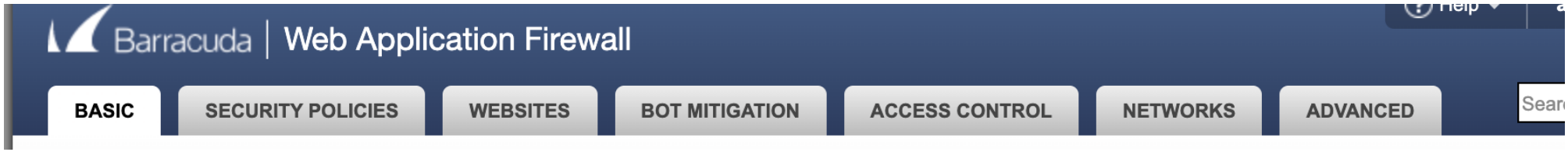




Username : admin
Password: AMI ID of the Barracuda WAF VM instance (you can get the id from the AWS Console)


Services
Default Security
Certificates
IP Configuration
Administration
Web Firewall Logs
Access Logs
Audit
ease set your System Alerts Email Address under Administration.
notes for the latest firmware ve
rsion 1.175 downloaded and ap
nerabilities and remediate them
Dismiss
on Service.
Welcome to Barracuda Web Application Firewall
To publish and protect your first application through the Barracuda Web Application Firewall, you will need to configure a Service. A Service is the application endpoint that is exposed to all clients. To get started click on the Create your first service button below.
If you need help with any configuration at any point, simply click on the Help dropdown menu on the top right corner. You will find links to the relevant documentation in this location. For more help, you can visit our community forums or reach out to our support team.
Thank you for choosing the Barracuda Web Application Firewall!
Do it later
Create your first service
Data Path Status:
Active

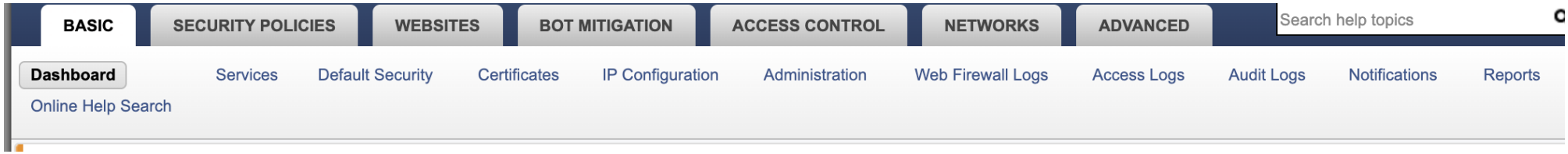
Parent Tabs on the GUI:



Each of the parent tabs has its set of child tabs :

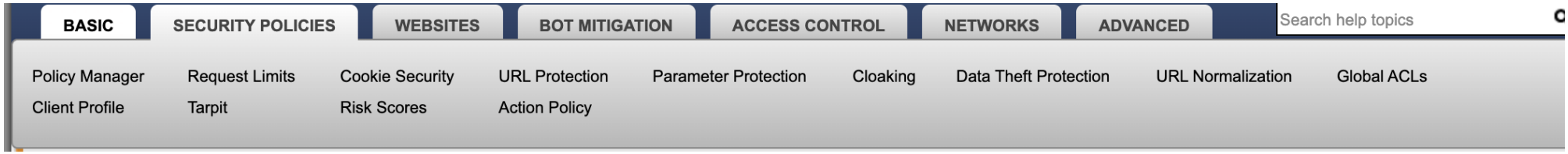
Basic Tab:

Provides the necessary options/features to get started with the product. Covers basic system administration, reporting and logging.



Security Policies Tab

A collection of 9 sub-policies which make up the global security layer for the virtual service. If no other configuration is enabled, the security policy will still guard the application from external threats.

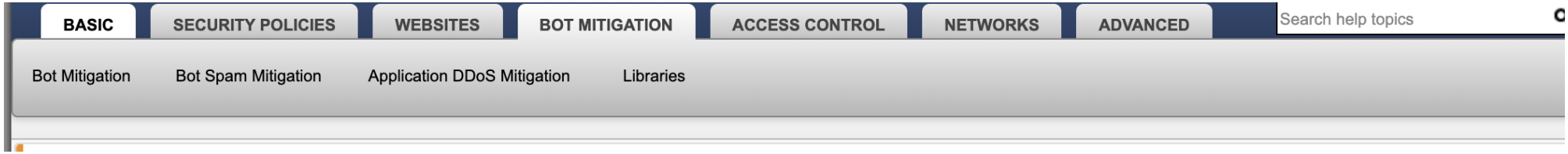


WebSites Tab

Covers the advanced security options. The features work in relation to the security policy but cover specific parts of the application in more detail. URLs, Parameters, Headers can be secured with a lot more granular control here. Application DDoS, IP Reputation, Anti Virus checks, Session tracking checks etc are enabled here.

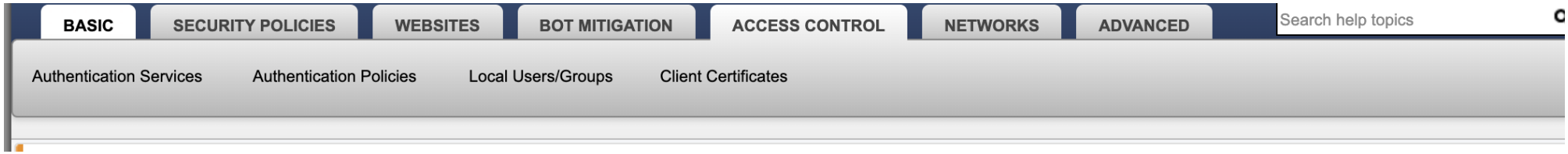
Bot Mitigation Tab

Advanced Bot Management features can be configured here. Features include credential stuffing protection, referer header/comment/form spamming protection, web scraping protection, bot allow/deny settings.



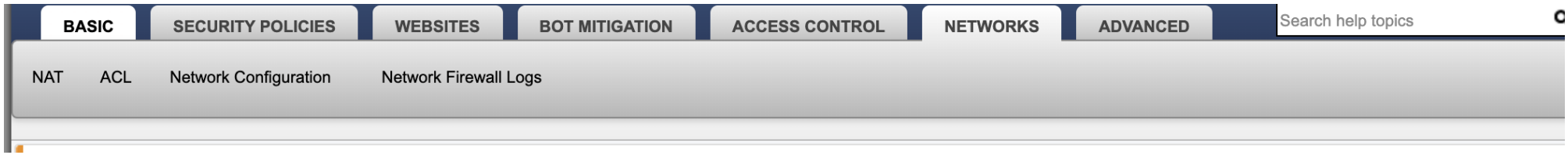
Access Control Tab

Authentication and Authorization features can be enabled for pre-authentication requirements. Integration is available for protocols like LDAP, RADIUS, SAMLv2, OpenID Connect and Kerberos.



Networks Tab

Covers the system networking options



Advanced Tab

Covers more granular system administration tasks like Backup/Restore, High Availability, Troubleshooting, Role Based Access Control.

5. Protecting the API-Part 1: Configure the Virtual Service

The first step to protecting the Backend API is to create a virtual service on the Barracuda WAF to process and validate the request connections.

Getting Started with the Virtual Service

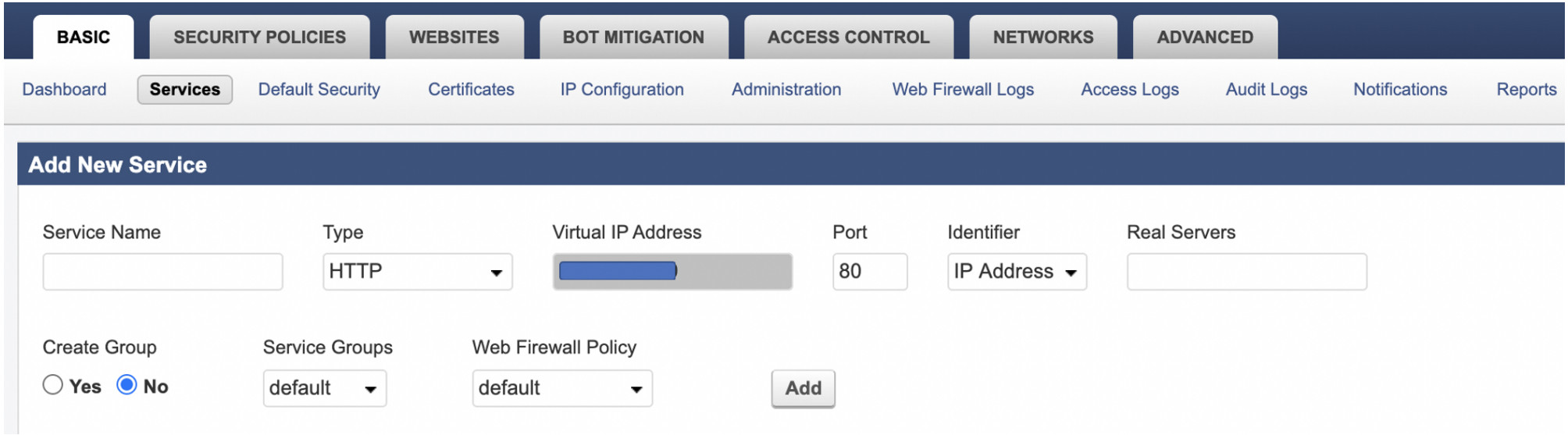
You can configure the Barracuda Web Application Firewall to secure web servers from incoming traffic threats. To do this, create a service to receive the incoming traffic type (for example: an HTTP service can receive HTTP data), and then associate security settings with that service to address the security risks of that traffic type. The service also receives responses from the servers and applies security before returning responses to the client.

The Barracuda Web Application Firewall acts as a server for the client connection on the front end, and the service acts as a client to the real servers on the back end. The Barracuda Web Application Firewall fulfills each of these roles using the service and its associated configuration settings.

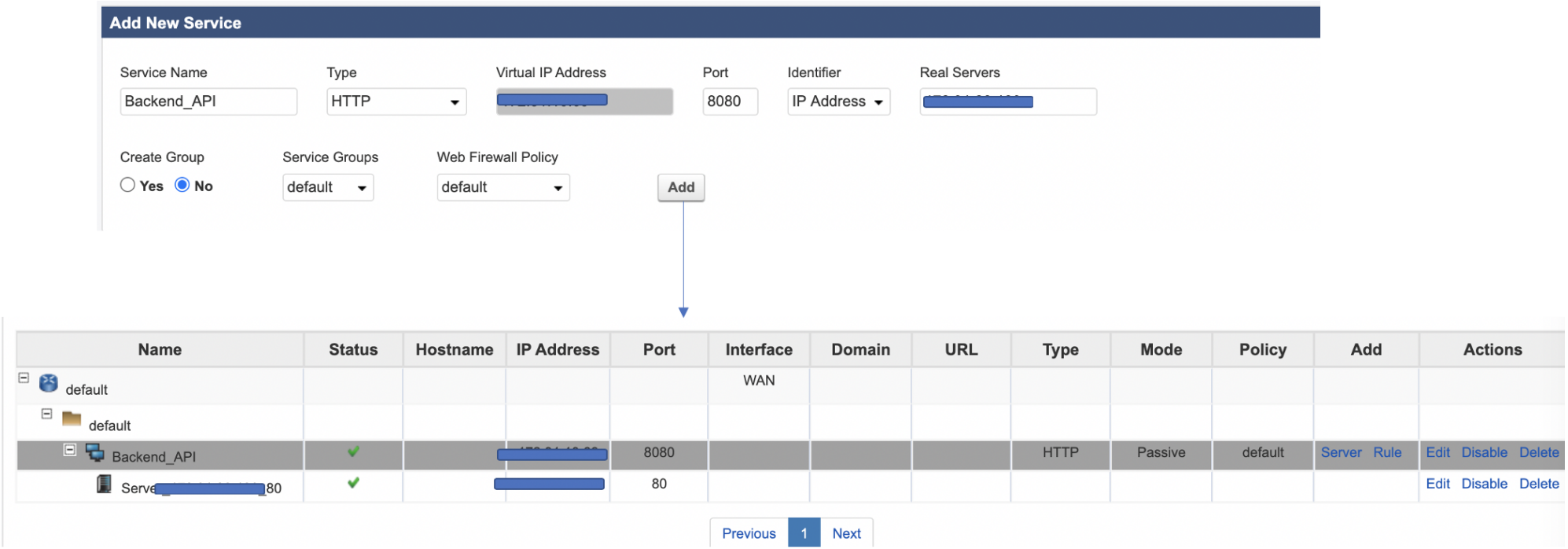
A service is configured with a Virtual IP (VIP) address and a TCP port. Traffic arriving at the designated VIP and port is validated, subjected to security checks configured for the service, and then passed to one of the real servers associated with that service.

To configure a Service

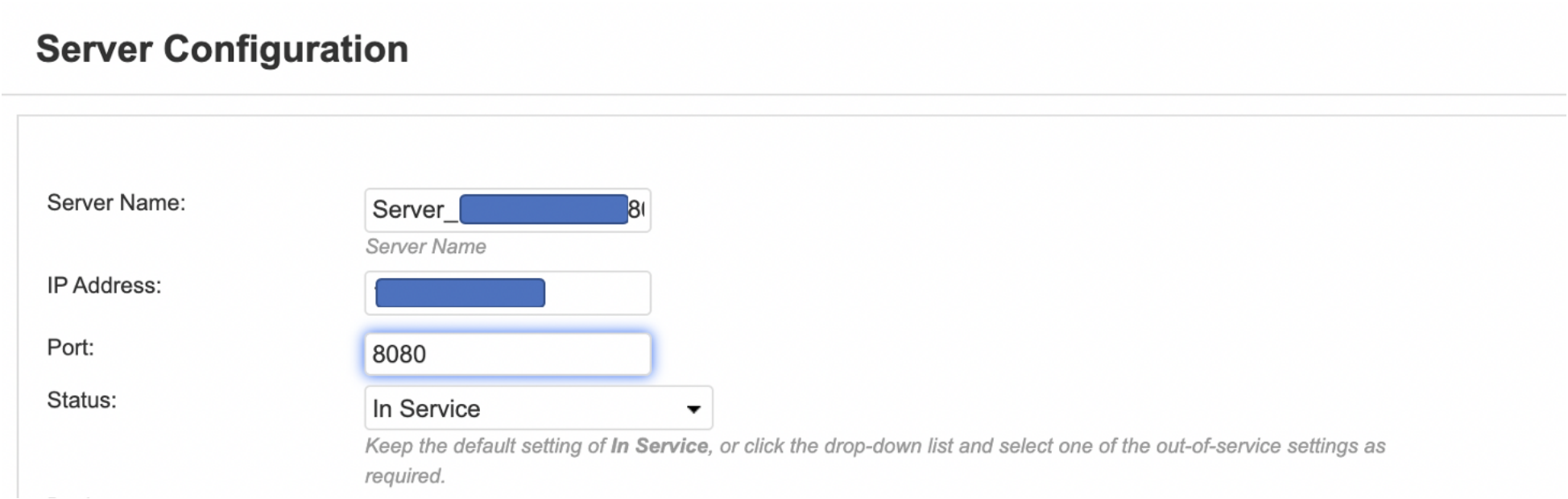
1. Go to Basic->Services Page

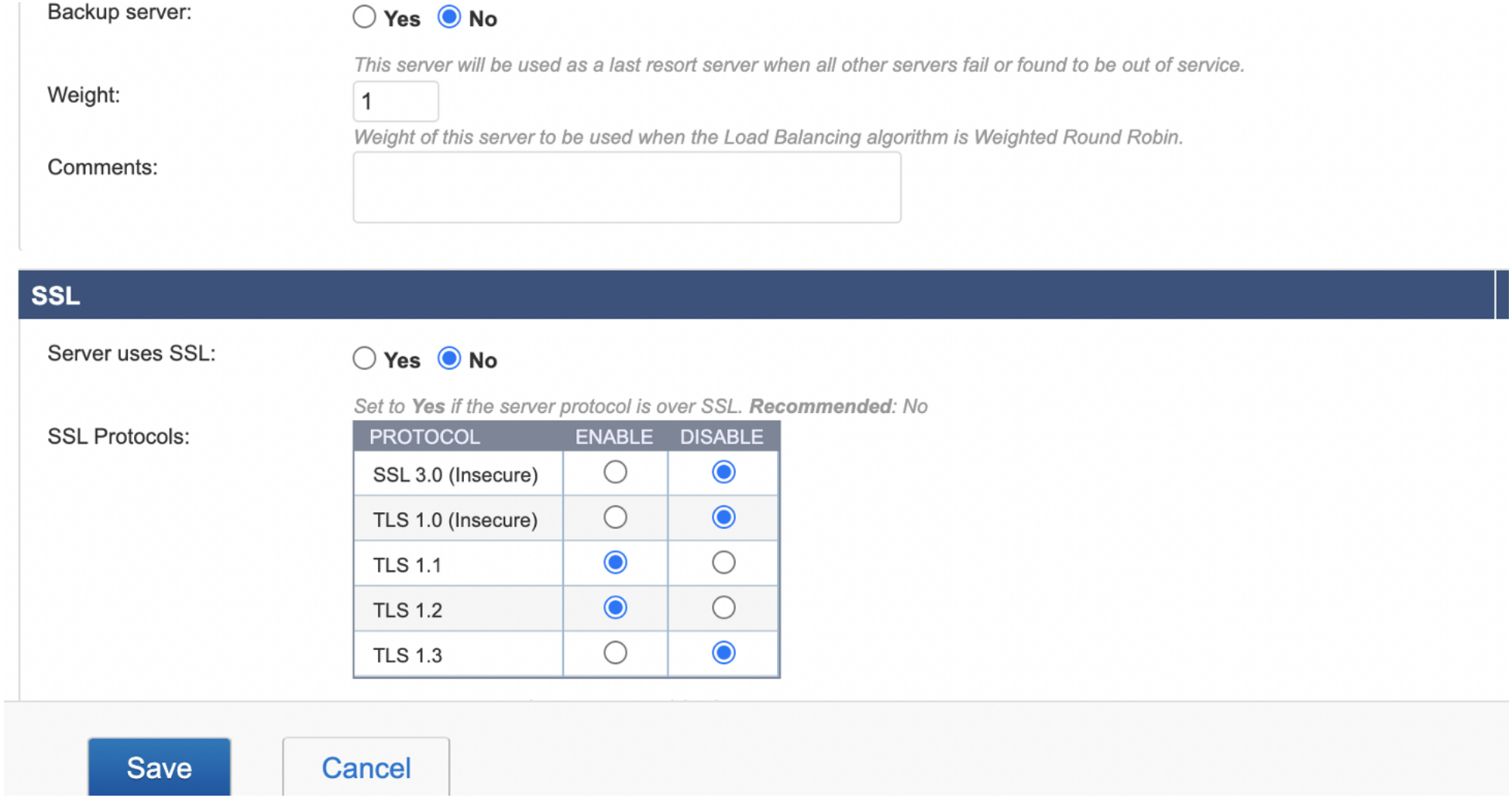


2.
Service Name : Backend_API
Service Type: HTTP
Virtual IP Address: Leave as is
Port: 8080
Identifier: IP Address
Real Servers: <Private IP of the Backend API Server>



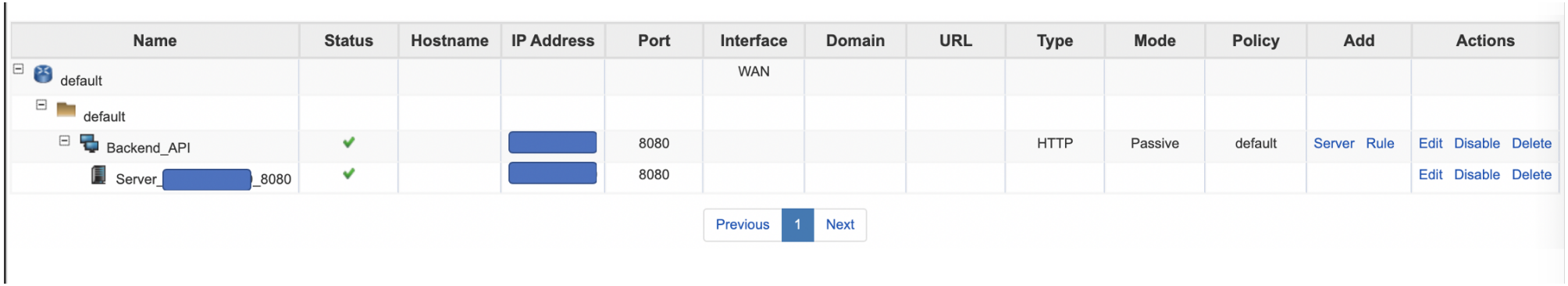
3. As seen above the port number for the server is 80, which is incorrect. Click edit for the server entry and change to 8080





4. Final Configuration

The port number for both service and server should be 8080



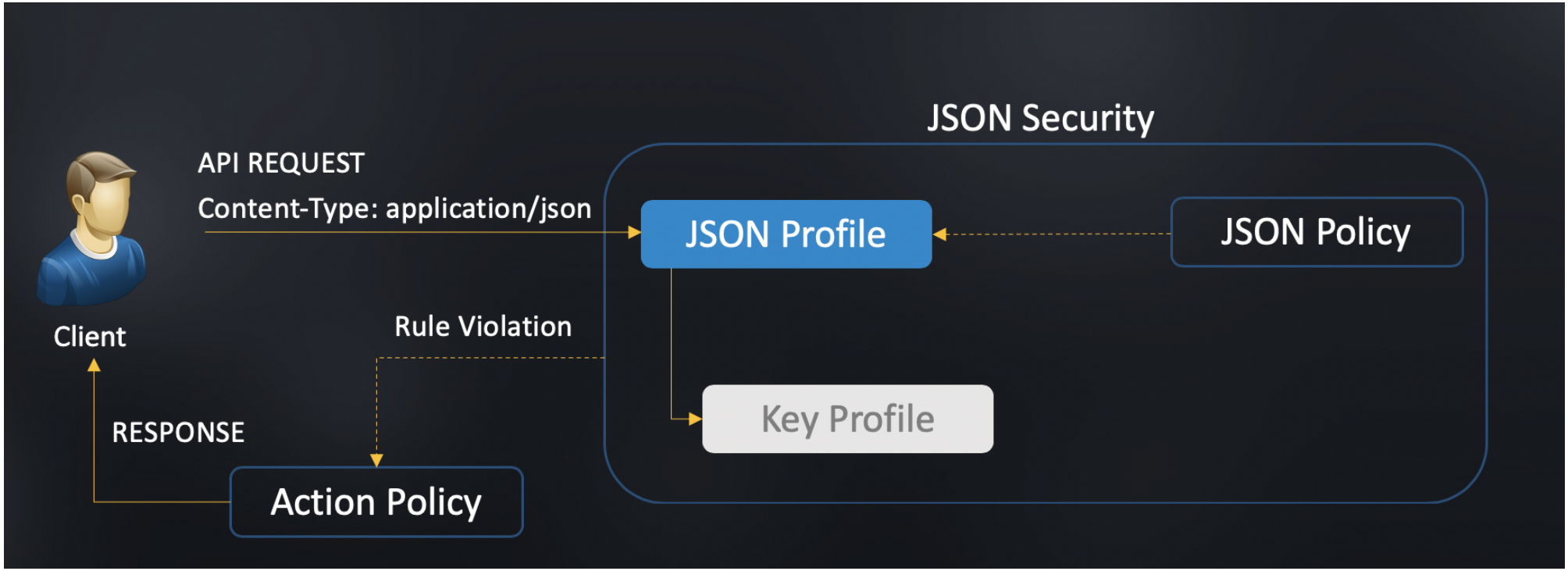
To access the API Server visit, http://<waf_publicIP>:8080/api/petstore/1.0.0/ui

Introduction to API Security on Barracuda WAF

The following are the security capabilities offered by the Barracuda WAF for APIs:

- Quota Management/Traffic Throttling
- Content Inspection
- Content Validation
- Automated Attack / Bot Detection
- Transport Layer Security
- Signature Validation
- Third Party identity provider (IdP)
- Integration with access management
- XML / SOAP Security
- SIEM Integration

Request processing workflow on the Barracuda WAF for API requests



1. Client sends a request with the Content-Type header whose value is "application/json"

2. WAF processes the request, identifies that the request is for an API from the Content-Type header.

3. The request is sent to the JSON Security module. The JSON Security module provides JSON profiles and JSON Key profiles to create API Key/Value specific rules. The Barracuda WAF uses this module in addition to features like protocol security, rate limiting, SSL encryption amongst a suite of other features to effectively safeguard an API.

4. If the request is valid, its sent to the backend server for further processing. If there is a rules violation, the request is blocked and a suitable JSON response is sent to the client by the WAF.

Since, the creation of JSON profiles and JSON key profiles can be a lengthy process, Barracuda WAF provides a way to automate this using the OpenAPI Specification File.

Proceed to the next section to use the API Spec file to create the rules on the WAF.

6. Protecting the API-Part 2: Import the swagger file and create the rules on the WAF

OpenAPI Specification

The OpenAPI Specification (OAS) defines a standard, language-agnostic interface to RESTful APIs which allows both humans and computers to discover and understand the capabilities of the service without access to source code, documentation, or through network traffic inspection. When properly defined, a consumer can understand and interact with the remote service with a minimal amount of implementation logic.

An OpenAPI definition can then be used by documentation generation tools to display the API, code generation tools to generate servers and clients in various programming languages, testing tools, and many other use cases.

[Source: https://swagger.io/specification/]

Importing the OpenAPI Specification File into Barracuda WAF

OpenAPI File Import

Barracuda WAF parses through the swagger specs and extracts the data which can be used to configure API Security rules.

WAF Rules affected: JSON Profile, URL Profiles, Header ACLs

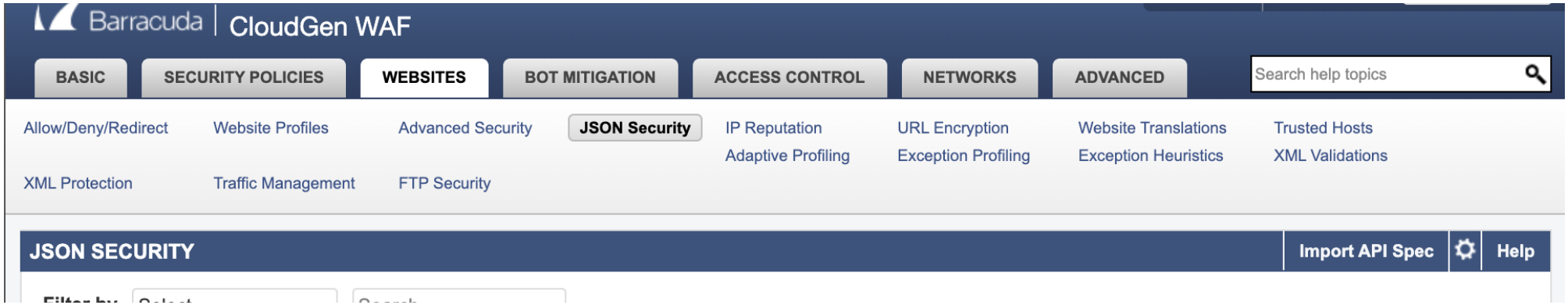
Request form	Path/ Form data/ Body	Query	Headers
WAF Rules	JSON Profile, key Profiles	URL Profile, param Profile	Header ACLs

- Enables brute force protection rules for rate limiting
- Optionally enables Access Control

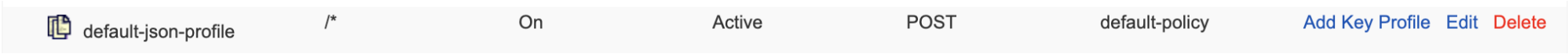
Getting Started

1. Download the OpenAPI Specification File for PetStore from here: https://raw.githubusercontent.com/aravindan-acct/awsdevdays_sep2020/master/petStore_req_check.yaml

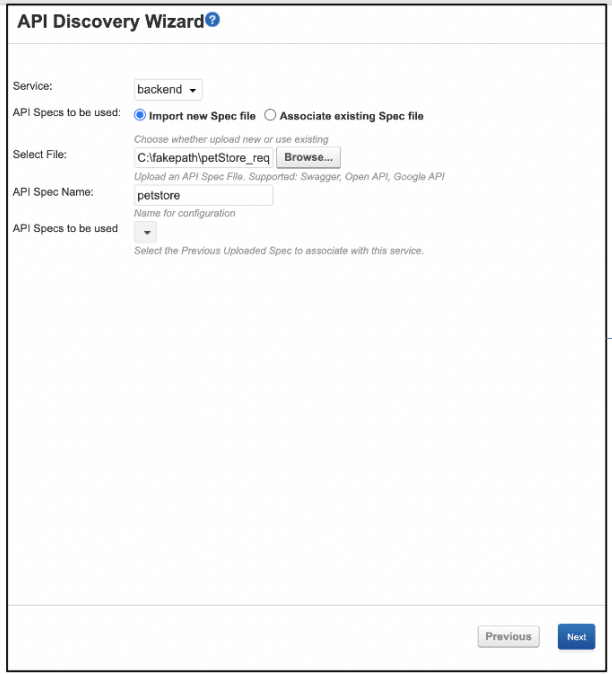
2. Login to your WAF appliance as 'admin'
3. Go to WebSites -> JSON Security

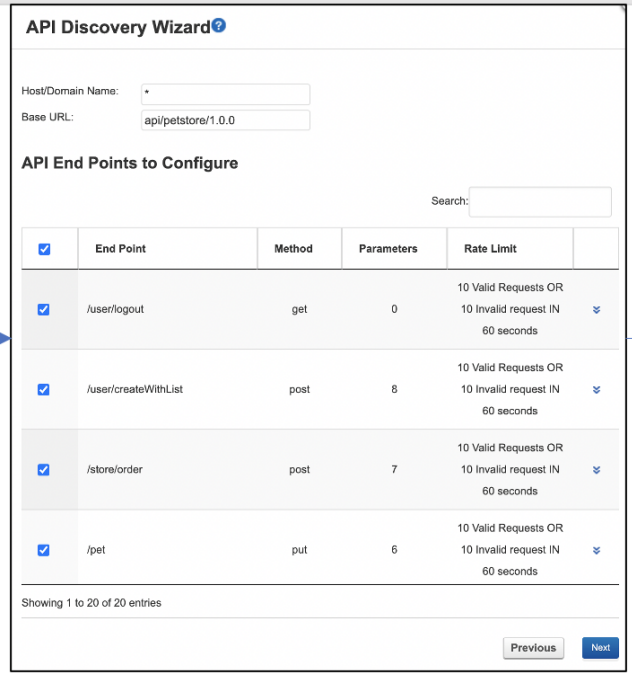


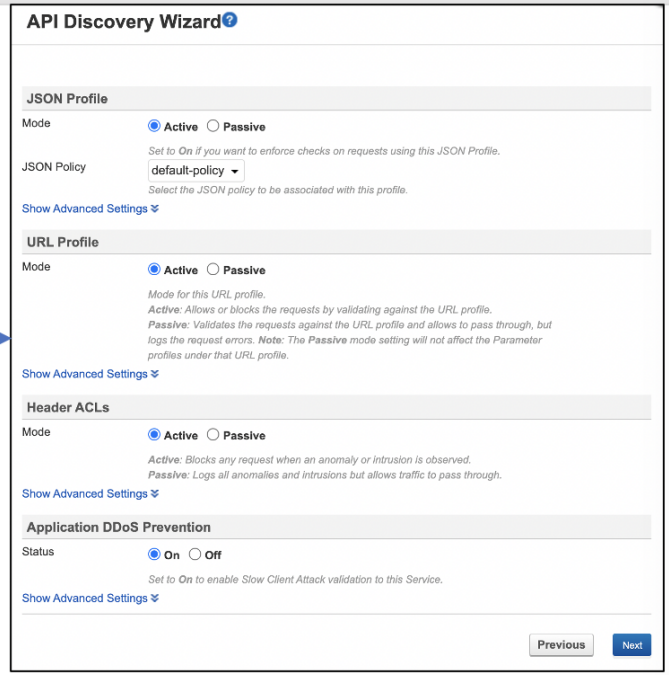
4. Delete the existing default json profile with the name "default-json-profile". Click on Delete to remove the rule.

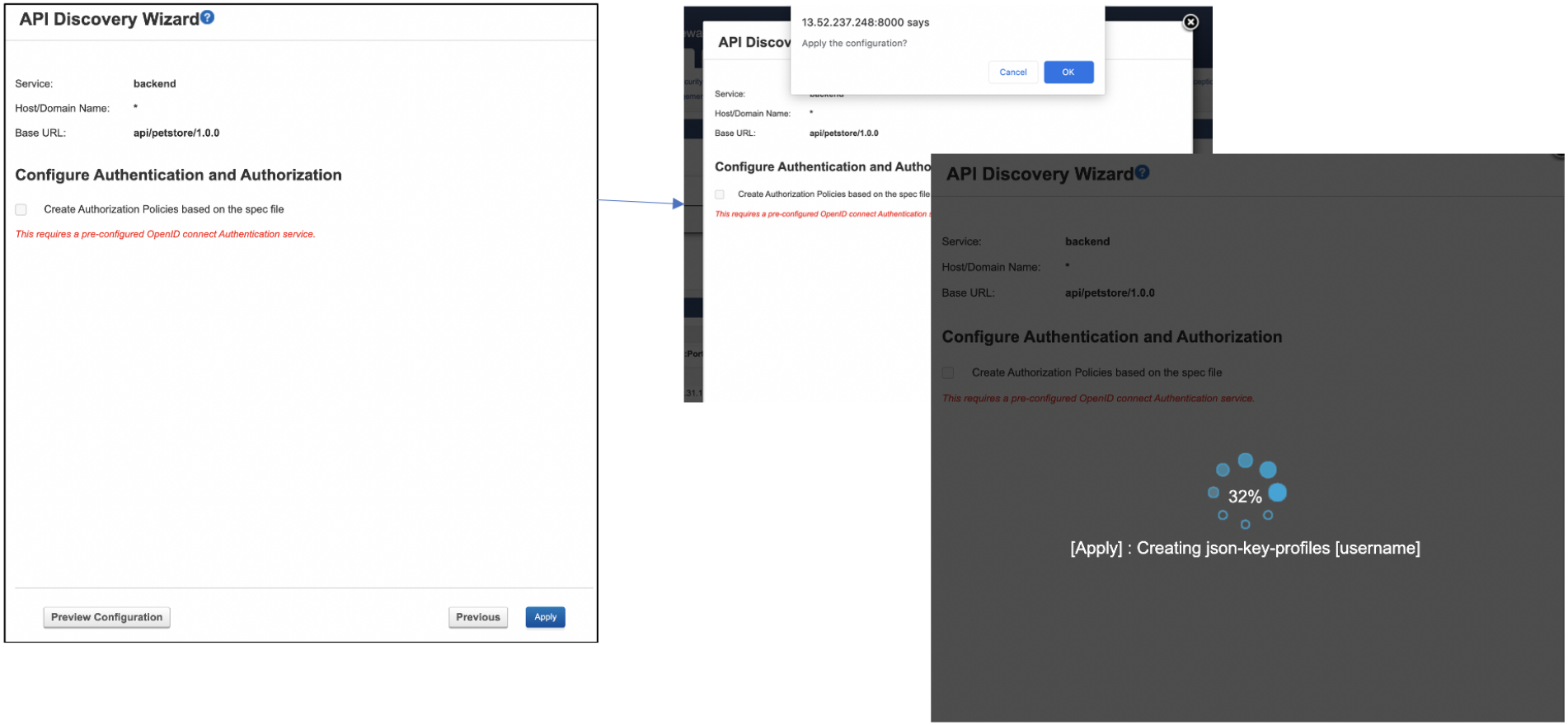


5. Import the OpenAPI Specification file by clicking on Import API Spec and follow the Wizard in to complete the configuration


API Discovery Wizard
Service:
backend
API Specs to be used:
Import new Spec file
Associate existing Spec file
Choose whether upload new or use existing
Select File:
C:\fakepath\petStore_req
Browse...
Upload an API Spec File. Supported: Swagger, Open API, Google API
API Spec Name:
petstore
Name for configuration
API Specs to be used
Select the Previous Uploaded Spec to associate with this service.
Previous
Next


API Discovery Wizard
Host/Domain Name:
*
Base URL:
api/petstore/1.0.0
API End Points to Configure
Search:
End Point
Method
Parameters
Rate Limit
/user/logout
get
0
10 Valid Requests OR
10 Invalid request IN
60 seconds
/user/createWithList
post
8
10 Valid Requests OR
10 Invalid request IN
60 seconds
/store/order
post
7
10 Valid Requests OR
10 Invalid request IN
60 seconds
/pet
put
6
10 Valid Requests OR
10 Invalid request IN
60 seconds
Showing 1 to 20 of 20 entries
Previous
Next


API Discovery Wizard
JSON Profile
Mode
Active
Passive
Set to On if you want to enforce checks on requests using this JSON Profile.
JSON Policy
default-policy
Select the JSON policy to be associated with this profile.
Show Advanced Settings
URL Profile
Mode
Active
Passive
Mode for this URL profile.
Active: Allows or blocks the requests by validating against the URL profile.
Passive: Validates the requests against the URL profile and allows to pass through, but logs the request errors. Note: The Passive mode setting will not affect the Parameter profiles under that URL profile.
Show Advanced Settings
Header ACLs
Mode
Active
Passive
Active: Blocks any request when an anomaly or intrusion is observed.
Passive: Logs all anomalies and intrusions but allows traffic to pass through.
Show Advanced Settings
Application DDoS Prevention
Status
On
Off
Set to On to enable Slow Client Attack validation to this Service.
Show Advanced Settings
Previous
Next


API Discovery Wizard
Service: backend
Host/Domain Name: *
Base URL: api/petstore/1.0.0
Configure Authentication and Authorization
Create Authorization Policies based on the spec file
This requires a pre-configured OpenID connect Authentication service.
Preview Configuration
Previous
Apply
13.52.237.248:8000 says
Apply the configuration?
Cancel
OK
32%
[Apply] : Creating json-key-profiles [username]

API Spec Name	Type	Import Time	Associated Services	Host/Domain Name	Base URL	Actions
petstore	openapi_3.0.0	2020-08-17 23:20:41	backend	*	api/petstore/1.0.0	Select

Showing 1 to 1 of 1 entries

Previous 1 Next

JSON SECURITY Help

Filter by Select Search

Service	IP:Port/URI	Status	Mode	Methods	Policy/Validation	Actions
default						
backend	172.31.13.240:8080					Add JSON Profile
default-json-profile	/*	On	Active	POST	default-policy	Add Key Profile Edit Delete
restApi-user-createWithList	/api/petstore/1.0.0/u…	On	Active	POST	default-policy	Add Key Profile Edit Delete
id		On			Number	Edit Delete
username		On			String	Edit Delete
firstName		On			String	Edit Delete
lastName		On			String	Edit Delete
email		On			String	Edit Delete
password		On			String	Edit Delete
phone		On			String	Edit Delete
userStatus		On			Number	Edit Delete
restApi-user-createWithArra	/api/petstore/1.0.0/u…	On	Active	POST	default-policy	Add Key Profile Edit Delete
id		On			Number	Edit Delete
username		On			String	Edit Delete
firstName		On			String	Edit Delete

This import operation results in the rules getting configured on the Barracuda WAF for the Backend API Server

7. Deploy the front end application

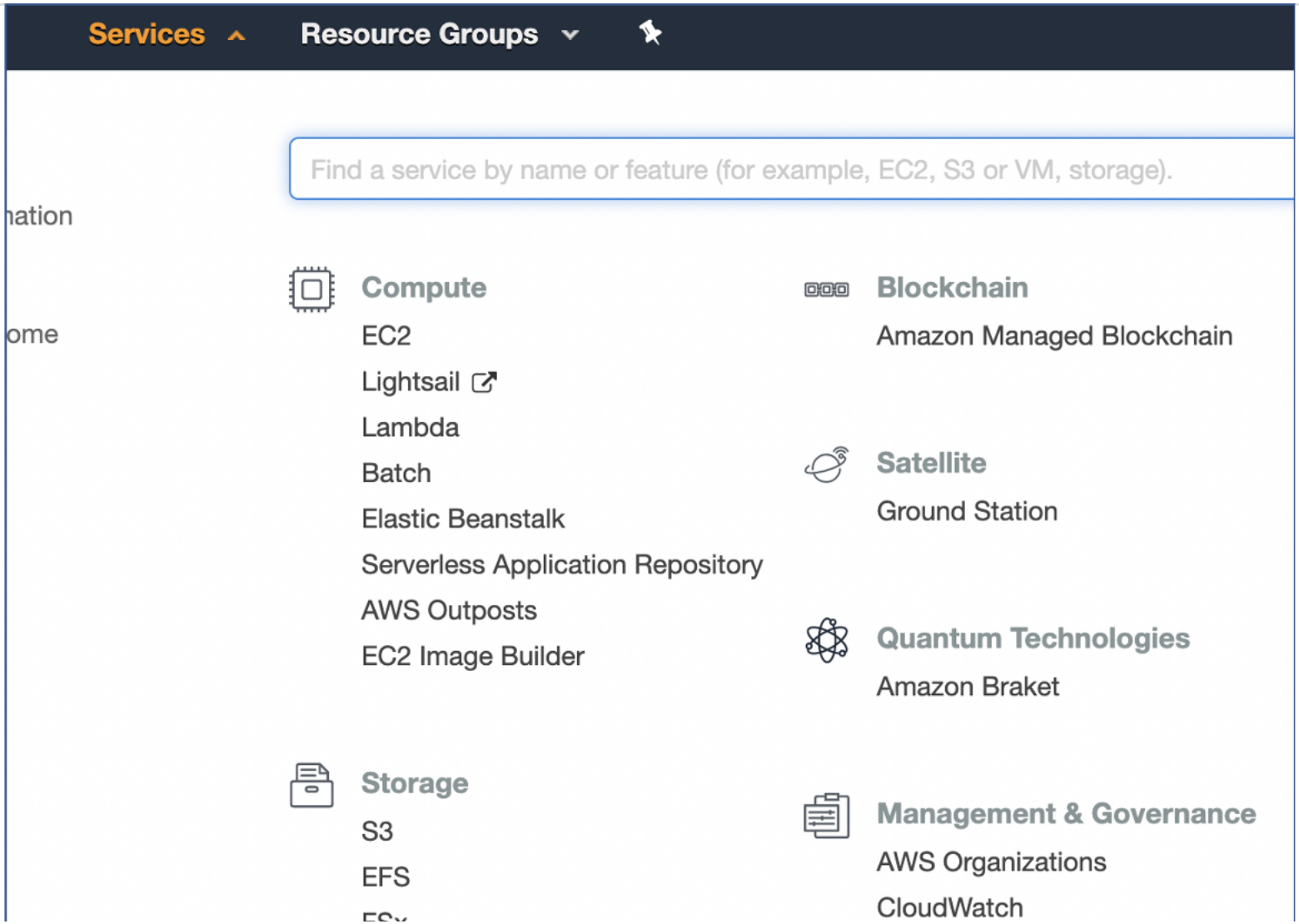
Frontend Application Deployment

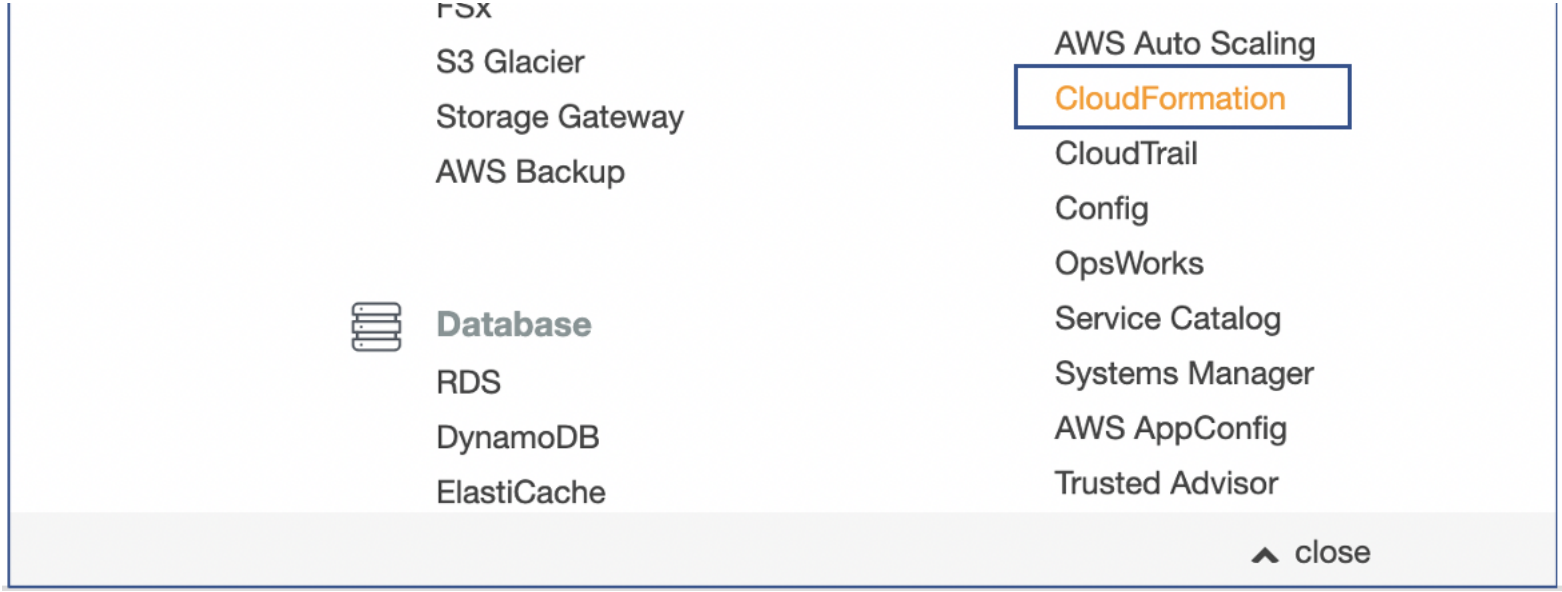
To deploy the Front end Application, please use the Cloud Formation Template from the following link:

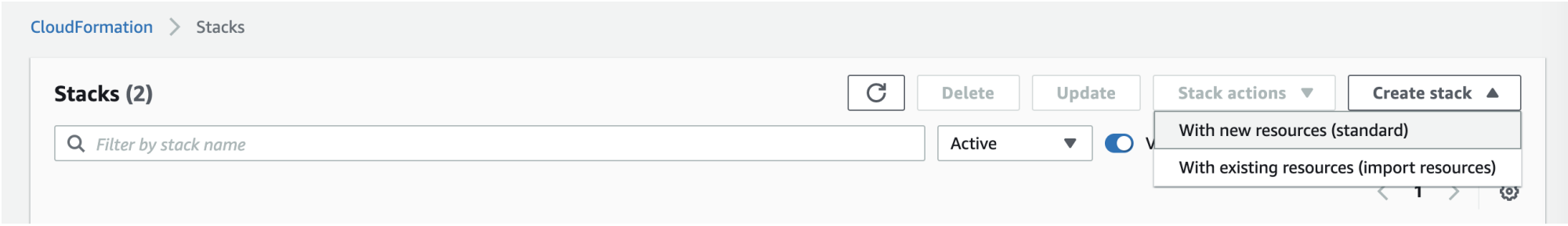
https://raw.githubusercontent.com/aravindan-acct/awsdevdays_sep2020/master/frontend_app_template.yaml

To get started with the CFT deployment, please follow the instructions below:

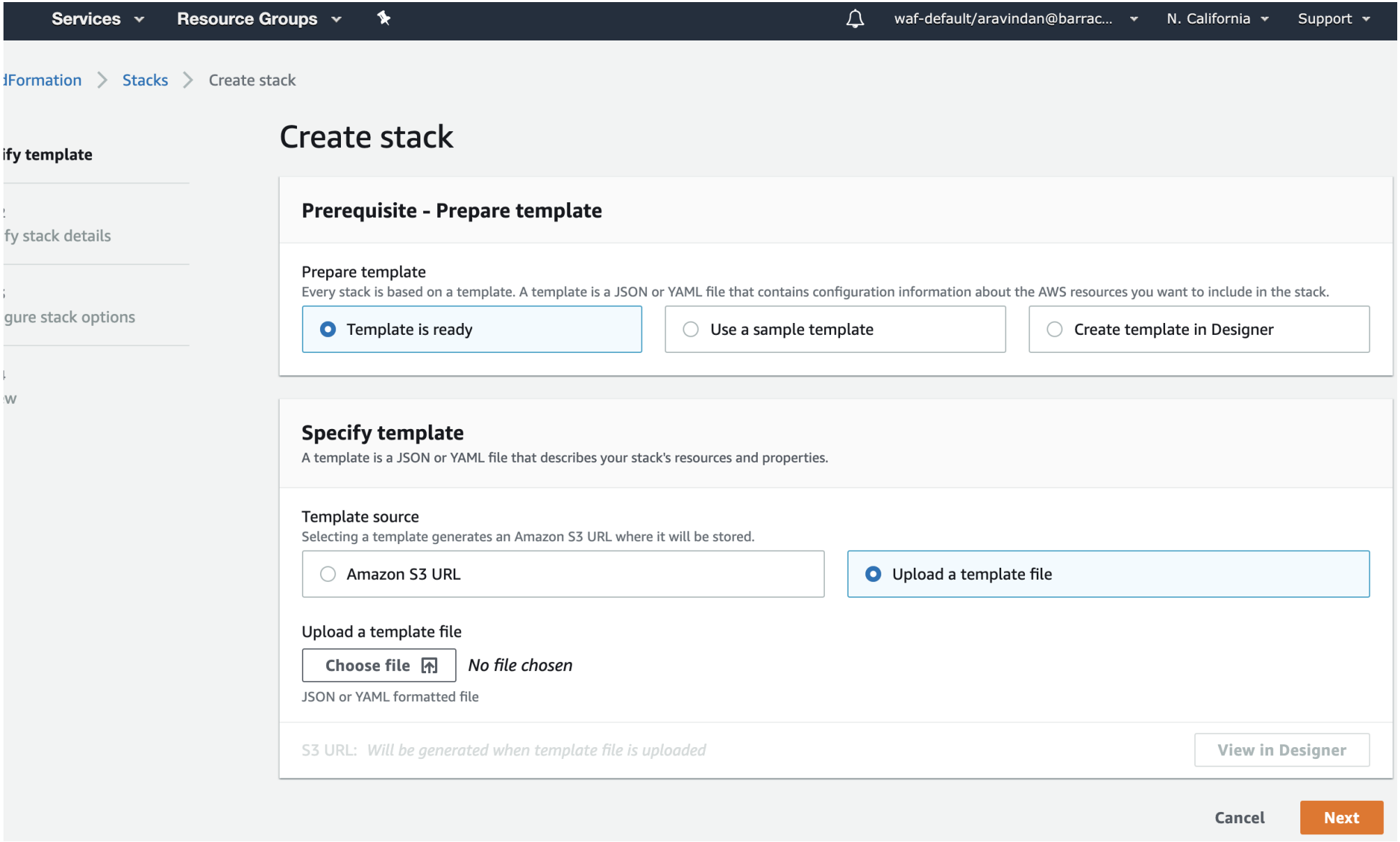
1. Go to the Cloud Formation console

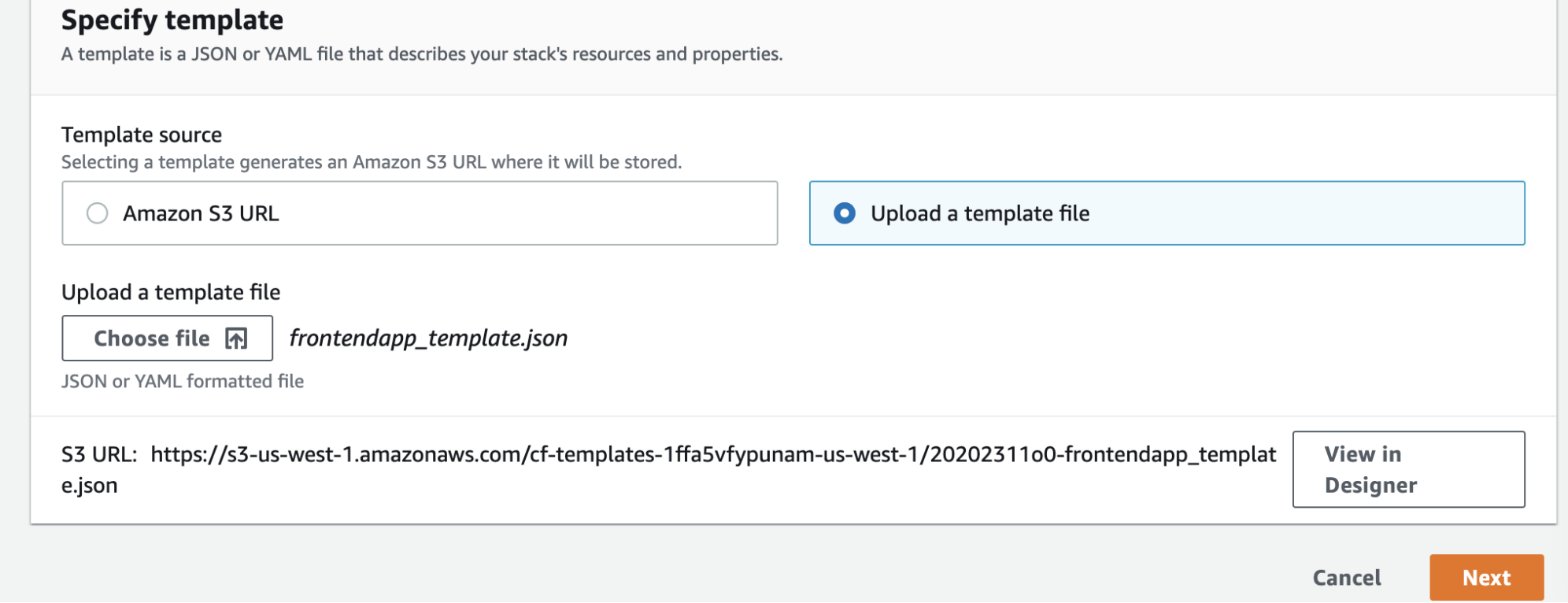






2. Select "Upload a template file" and select the file downloaded from the link above:

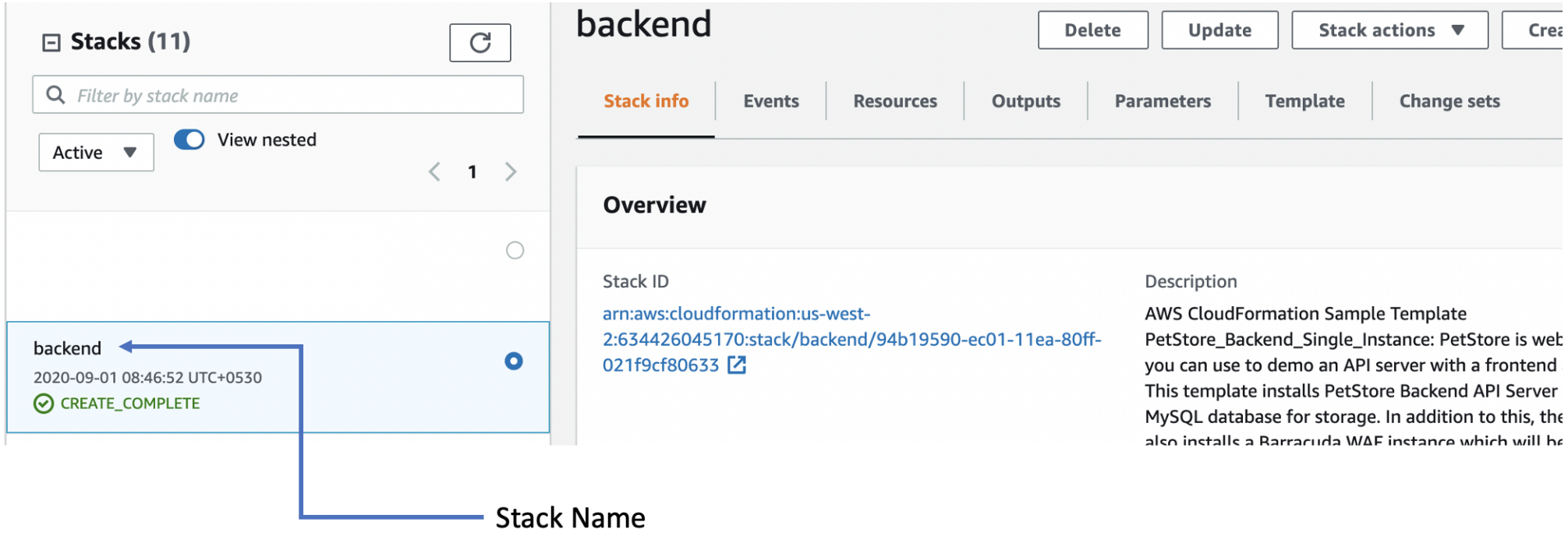

Services
Resource Groups
waf-default/aravindan@barrac...
N. California
Support
dFormation
Stacks
Create stack
ify template
fy stack details
gure stack options
w
Create stack
Prerequisite - Prepare template
Prepare template
Every stack is based on a template. A template is a JSON or YAML file that contains configuration information about the AWS resources you want to include in the stack.
Template is ready
Use a sample template
Create template in Designer
Specify template
A template is a JSON or YAML file that describes your stack's resources and properties.
Template source
Selecting a template generates an Amazon S3 URL where it will be stored.
Amazon S3 URL
Upload a template file
Upload a template file
Choose file
No file chosen
JSON or YAML formatted file
S3 URL: Will be generated when template file is uploaded
View in Designer
Cancel
Next



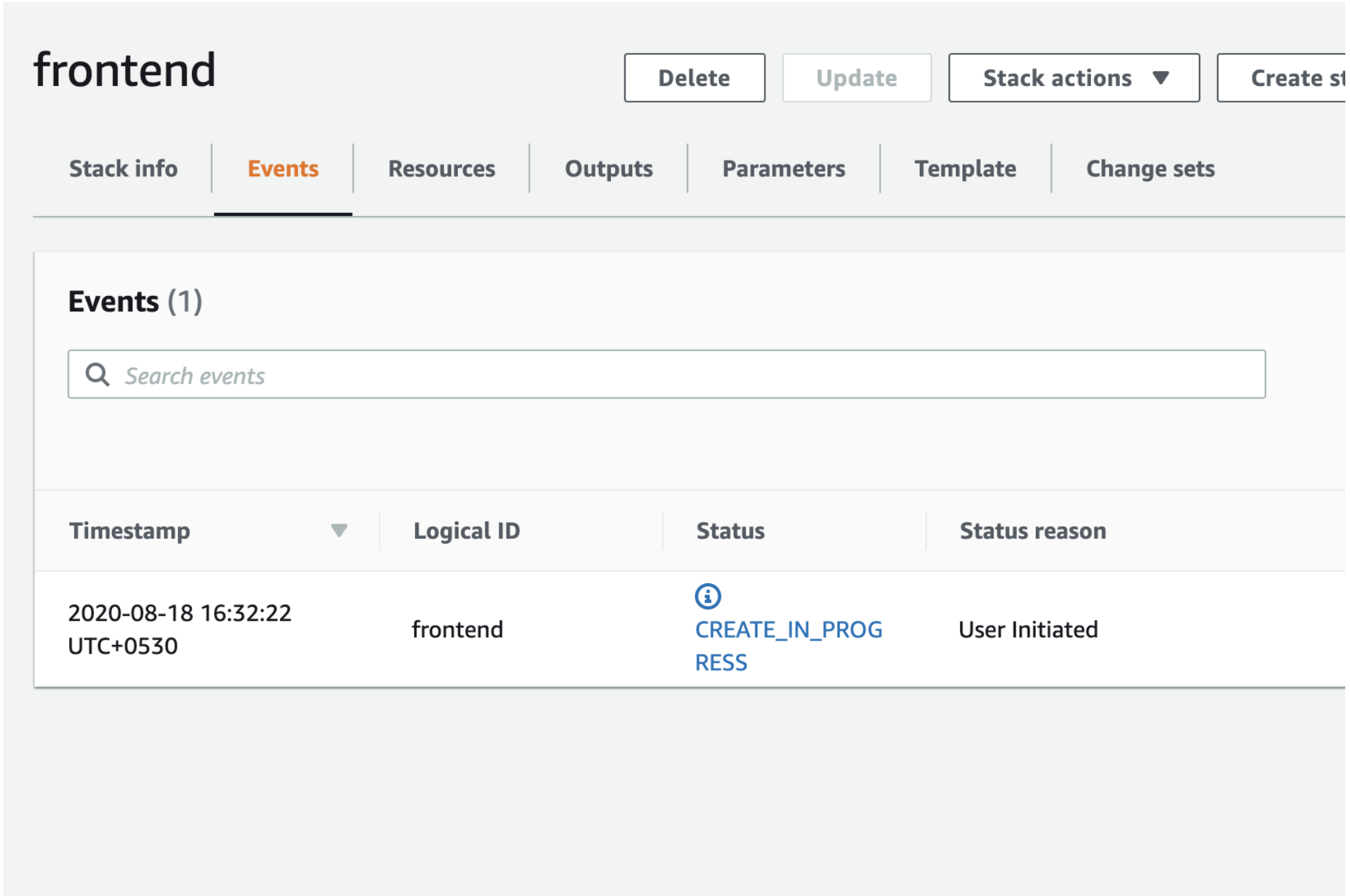
3. Configure the launch parameters:

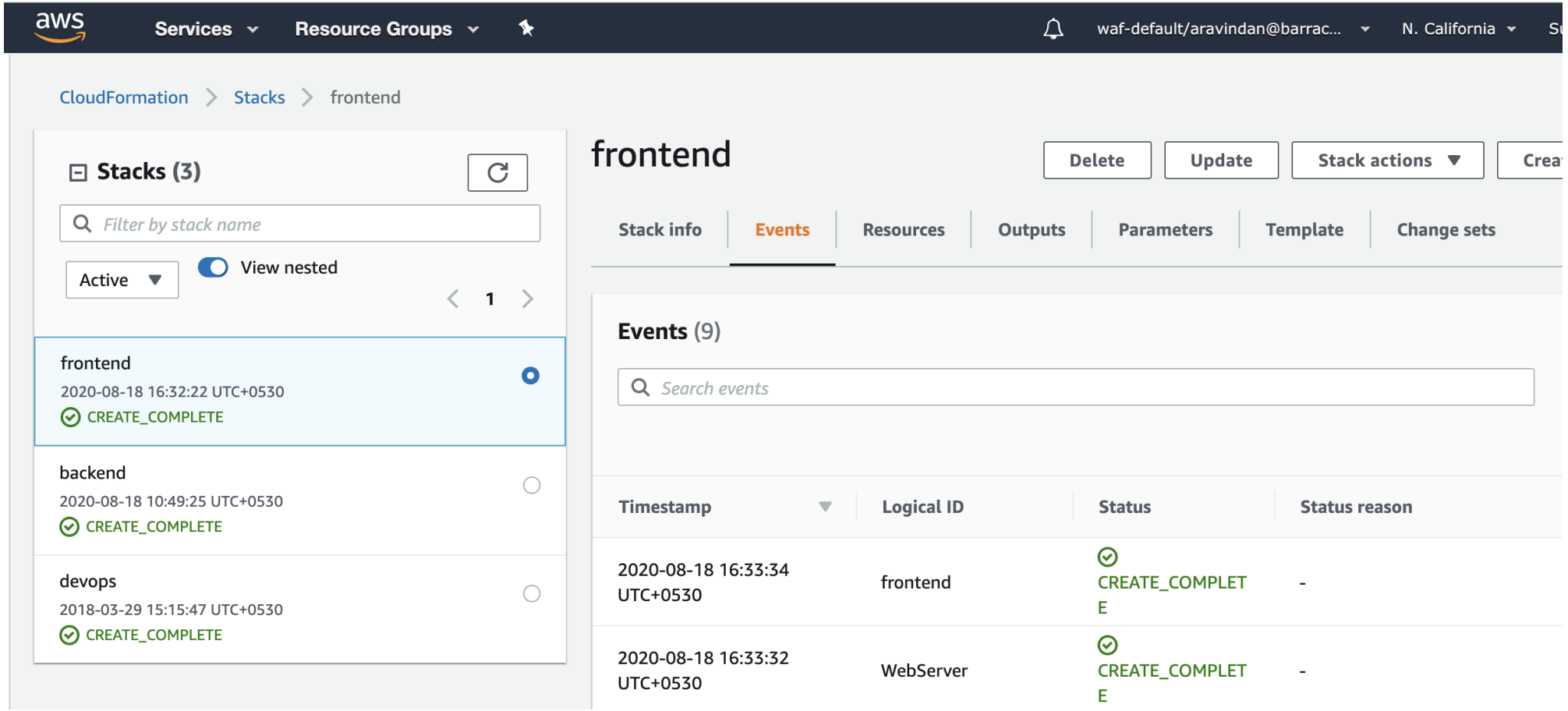
- WAF Password: **WAF admin password is the Instance ID of the Barracuda WAF**. This can be copied from the AWS EC2 instances page.

- StackID: **This is the name of the stack which was used to launch the api and the waf in the lab**. Please note this stack would have been auto-created. This stack name can be seen from the CloudFormation service page on the AWS Console. For example, see the following screenshot of a stack created with the name "backend". In your environment, the name will be different, so please use the name seen in your lab account.



Please proceed with "Next" without any other changes in CFT creation steps in the screen i.e. Step 3 and Step 4 in the AWS console.


frontend
Delete
Update
Stack actions
Create st
Stack info
Events
Resources
Outputs
Parameters
Template
Change sets
Events (1)
Search events
Timestamp
Logical ID
Status
Status reason
2020-08-18 16:32:22 UTC+0530
frontend
CREATE_IN_PROGRESS
User Initiated



To access the Front End application visit: https://<WAF Public IP>/

The CFT creates the front end application VM as well as configures the virtual service on the WAF. Confirm that the virtual service is created on the WAF by logging into the WAF GUI. The service should be created with the name as "frontend_svc" on port 443.
The following changes are made to the Barracuda WAF configuration by the script:
1. Creates a self signed certificate called "petstore"
2. Creates a HTTPS virtual service on port 443 and binds the self signed certificate
3. TLS 1.3 is disabled since we are using a self signed certificate
4. Authentication is enabled for the frontend service
5. A local user is created for the admin portal
6. A response rewrite rule is created to handle redirects

For reference, the script can be found here:
https://raw.githubusercontent.com/aravindan-acct/frontend_UI_app/master/waf_configuration.py

The API documentation for the Barracuda WAF is available here: https://campus.barracuda.com/product/webapplicationfirewall/api#/

If successfully deployed, you should be able get to the home page for the frontend app by visiting **https://<PublicIP of WAF>/** :

8. Petstore Frontend App User Manual

Getting Started with the application

The application provides two types of logins - admin login and end user login

Administrator login

The admin login allows the administrator of Petstore to **add/remove/edit the pets**

To access the admin portal go to : https://<WAF publicIP>/admin

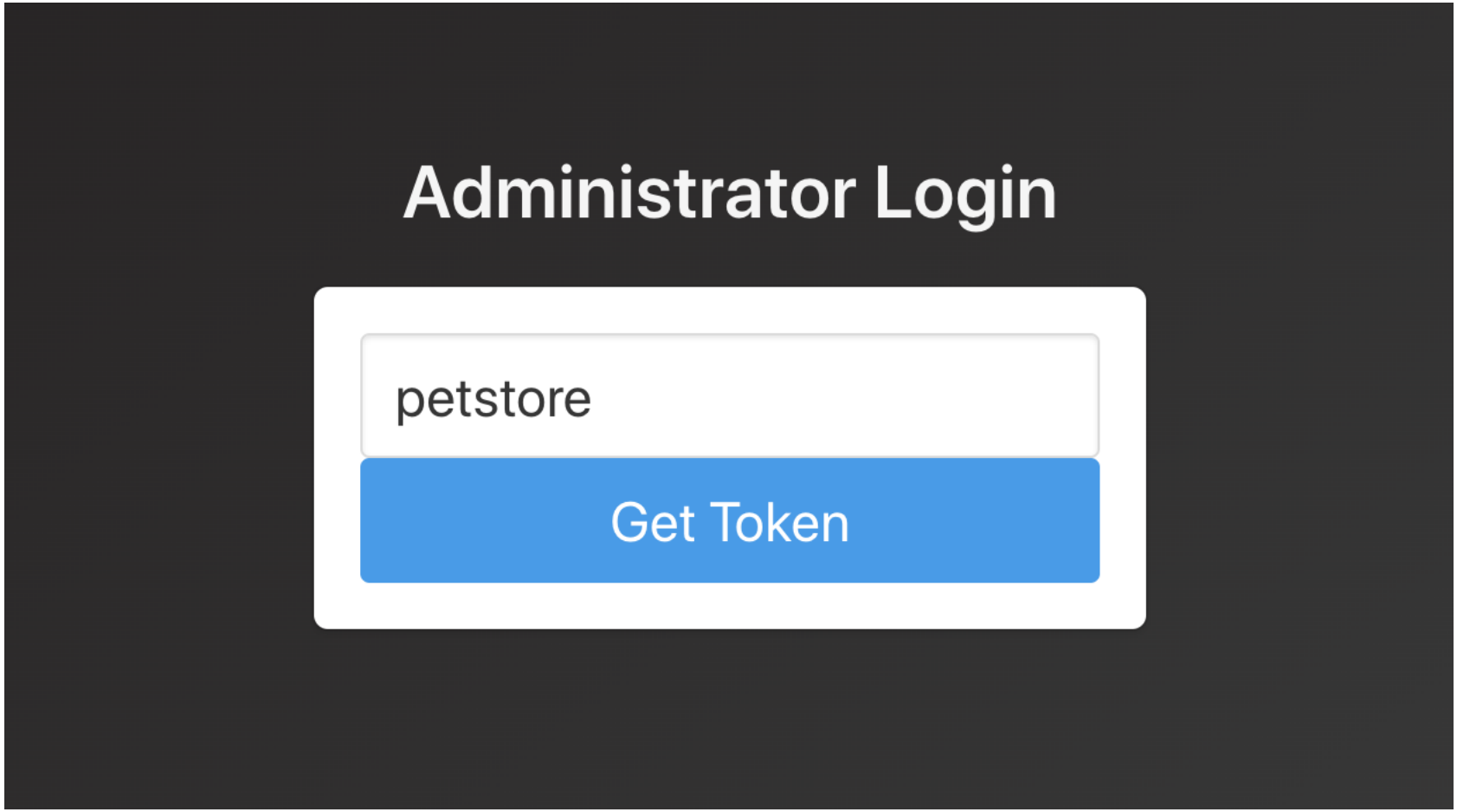
The credentials for the login page are

Username: administrator

Password: administrator

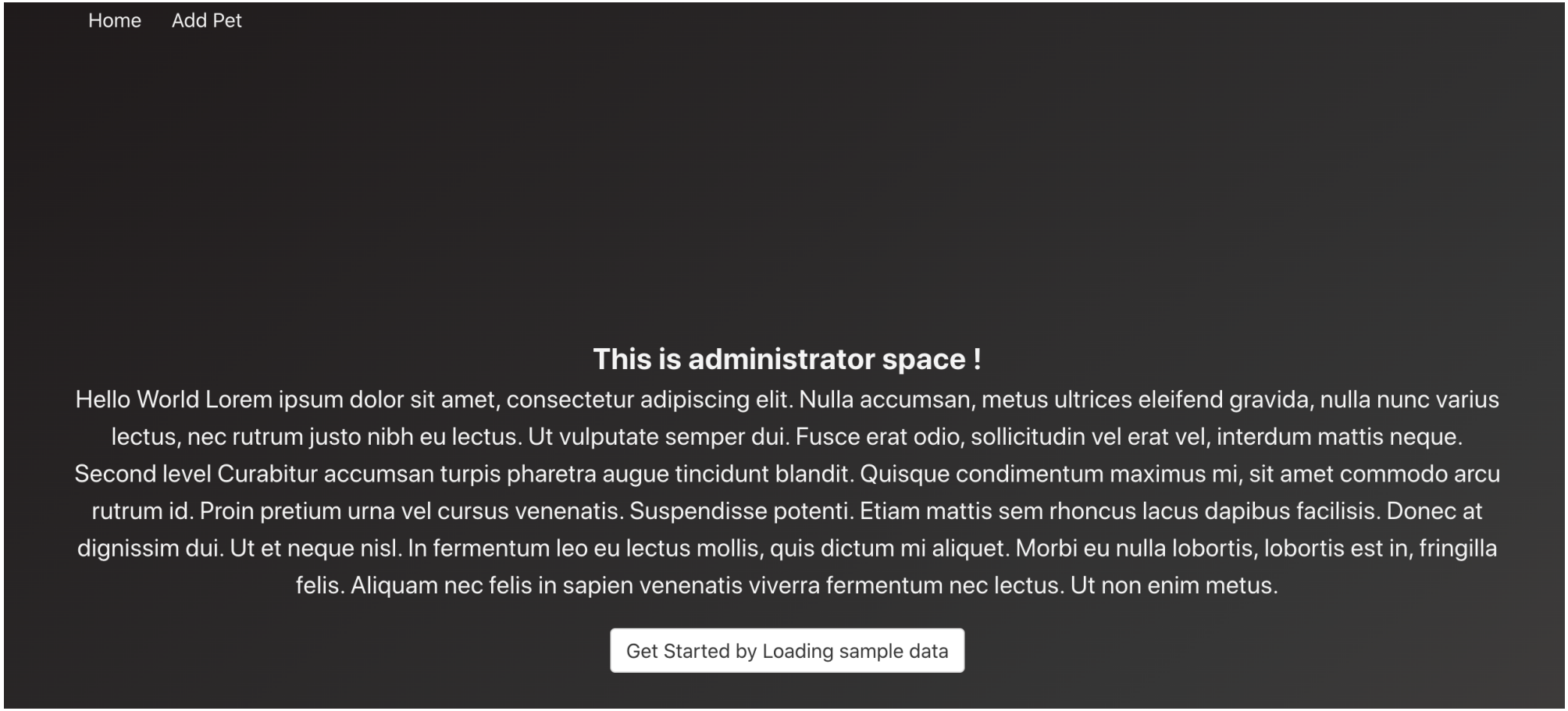
Note: Please note that the above credentials are created on the Barracuda WAF during the deployment of the frontend app

Oauth Token: Implicit grant flow OAUTH authentication is enabled for the /admin URL. Type a string, for example, "petstore" and click on Get Token to login to the admin portal.



Loading sample data

Once you are logged in to the admin portal, load the sample data by clicking on the option "Get Started by Loading Sample Data" in the landing page:



Other Admin options:

Once the sample data is loaded, the administrator can add/remove/edit the data.

End User login

- The end user login allows Petstore clients to **signup to the portal and access the store inventory and complete an order.**

Note:
There is no end user configured by default. Complete the user registration page and signup to login to the application

Security Concerns / Vulnerabilities in PetStore

The frontend application has a few security concerns:

1. **The site is not SSL enabled**

This is overcome by enforcing SSL on the virtual service created on the Barracuda WAF. The certificate is a self signed certificate which can be easily replaced with a 3rd party certificate if required.

2. **The admin portal is open and needs to be protected**

This is overcome by enforcing form based authentication on the Barracuda WAF. Unauthorized access to the /admin portal can be prevented using this step.

Note: Both the above security concerns are handled during the application provisioning phase i.e. as part of the deployment of the Cloud Formation Template in Chapter 7.

9. Check the logs and fine tune the WAF settings

Barracuda WAF provides lots of features around logging and reporting.

Events related to HTTP traffic, actions of the Barracuda Web Application Firewall, and user actions are captured in logs. These log messages enable a system administrator to do the following:

- Obtain information about the Barracuda Web Application Firewall traffic and performance.
- Analyze logs for suspicious activity.
- Troubleshoot problems.

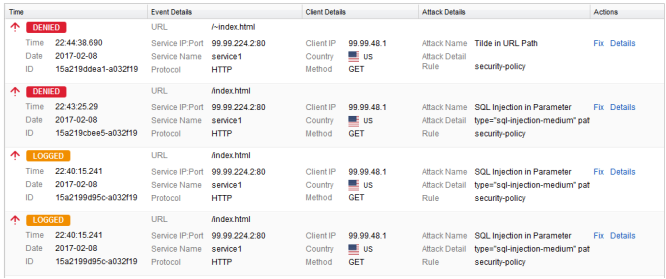
The following types of logs are available in the Barracuda Web Application Firewall:

- Web Firewall logs
- Access logs
- Audit logs
- System logs
- Network Firewall logs

Each log in **Web Firewall Logs**, **System Logs**, and **Network Firewall Logs** is associated with a log level that indicates the severity of the log. An administrator can configure the severity level based on the error messages/information that needs to be recorded in the logs. You can export the logs in .csv format and save the file to your desktop using **Generate CSV File** and **Download CSV File** options.

You can use the Web Firewall Logs to evaluate rule violations and, when warranted, to create exceptions to the rule violated. Exceptions can apply globally if they modify the security policy, which affects all services using that policy. Or, you can apply an exception locally that only applies to a specific website or URL.

Once logged in to the unit, select **Web Firewall Logs** from the **BASIC** tab to search for a log entry believed to be a false positive. These log entries are in red and have an action of DENY (active mode) or LOG (passive mode).



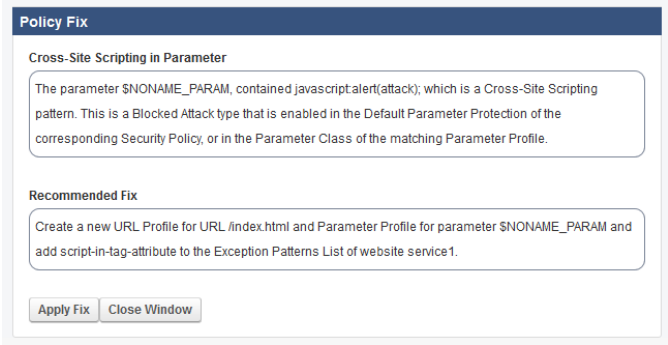
Scroll over to the right of the selected log and click **Fix**. A **Policy Fix** window appears.

The fix recommended by the Barracuda Web Application Firewall may be localized or global, depending upon which rule was violated. Accepting a recommendation can have the following impact:

1. **Web site profile (localized) modification:** As the most fine-grained security, changes impact only a given URL or parameter.
2. **Security Policy (global) modification:** As a policy shared by multiple applications, changes impact all applications using the security policy.

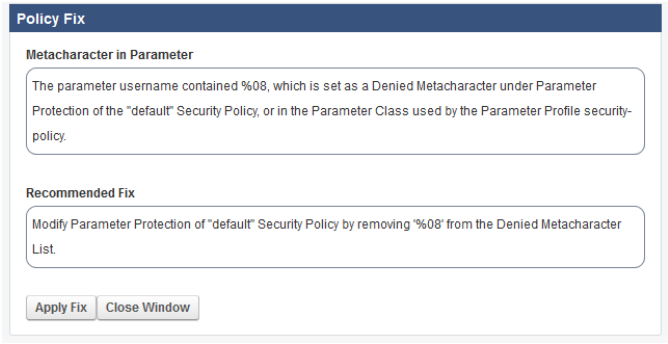
Examples of Fixes Suggested by the Barracuda Web Application Firewall

Example 1: Recommendation to Configure a Fine-Grained Rule.



Following the recommendation to create a URL profile for /modules.php creates an exception only for that particular page.

Example 2: Recommendation to Change the Configuration in Security Policy.

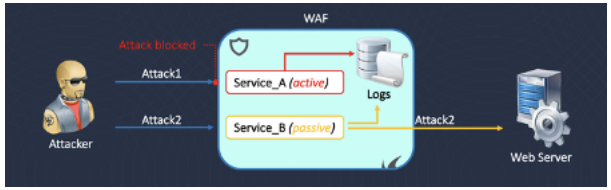


The suggested change to the Parameter Protection sub-policy of the default Security Policy would allow the meta-character (%08) in any parameter for any application using this security policy. To avoid an exception that applies globally, you can add an exception that only applies to the URL or parameter noted in the log.

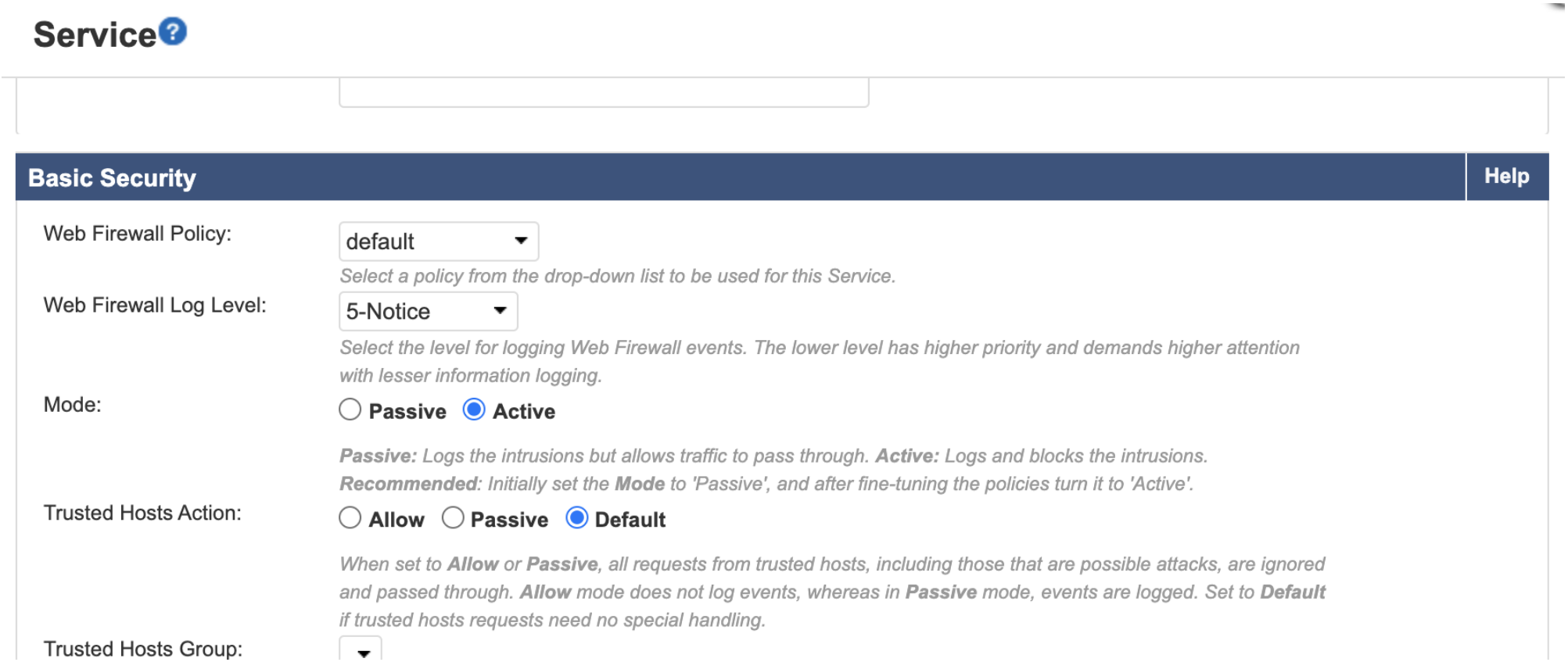
10. Change the Security Policy Mode

Now that the rules have been setup and the web firewall logs have been analysed, we can be sure that there will be no false positives, and so, the security policy mode can be changed to Active.

In Active mode, any requests that match rules on the Barracuda WAF will be blocked and a response will be sent back to the client.



To change the mode of the security policy, go to Basic -> Services and edit the service configuration and change the mode to "Active":

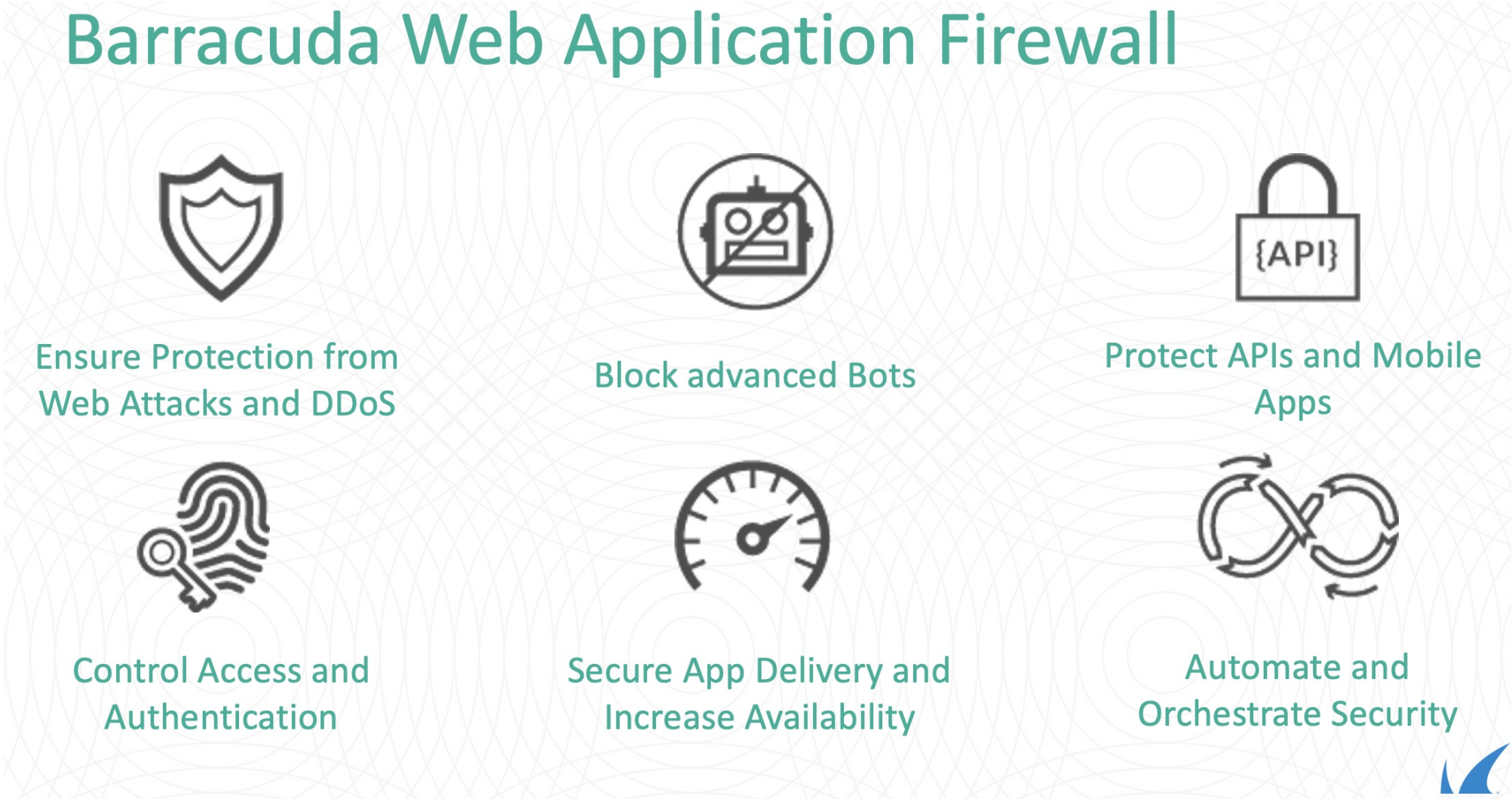


Barracuda WAF has over 215 categories of attack rules for which a request may be blocked. Each rule category has an event ID which is logged in the Web Firewall Logs.

Based on the attack group, a response action is triggered. These response actions are configured in action policies page under the security policy.

11. Conclusion and Next Steps

Summary



Ensure Protection from Web Attacks and DDoS

The Barracuda Web Application Firewall protects applications, APIs, and mobile app backends against a variety of attacks including the OWASP Top 10, zero-day threats, data leakage, and application-layer denial of service (DoS) attacks. By combining both positive signature-based policies with robust anomaly detection capabilities, Barracuda WAF can defeat today's most sophisticated attacks targeting your web applications.

Barracuda Active DDoS Prevention—an add-on service for the Barracuda Web Application Firewall—filters out volumetric DDoS attacks before they ever reach your network and harm your apps. It also protects against sophisticated application DDoS attacks without the administrative and resource overhead of traditional solutions, to eliminate service outages while keeping costs manageable for organizations of all sizes.

Additional References

1. **https://www.barracuda.com/cap**
2. **https://campus.barracuda.com/**
3. **https://www.barracuda.com/demos**
4. **https://www.barracuda.com/products/webapplicationfirewall**
5. **https://campus.barracuda.com/product/webapplicationfirewall/api#/**

Next Steps

Want to know more about WAF and WAF-as-a-Service?

- We can talk to your teams about Application Security
- We can help your teams with your evaluations and PoC's

Congratulations !! You have successfully deployed the Petstore in AWS and secured it using the Barracuda Web Application Firewall !