
Deploy and Secure an Internet Facing Application with the Barracuda Web Application Firewall in Amazon Web Services

<https://campus.barracuda.com/doc/70586316/>

In this lab, you will deploy an unsecure web application into Amazon Web Services (AWS), and then secure the application using the Barracuda Web Application Firewall. To create the environment, you will deploy a Virtual Private Cloud, Internet Gateway and NAT Gateway to provide for the virtual networking. Then a Barracuda Web Application Firewall and an Ubuntu server with Apache, PHP, MySQL and the Damn Vulnerable Web Application (DVWA), installed.

DVWA is a PHP/MySQL web application that is vulnerable attack. Its main goals are to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and aid teachers/students to teach/learn web application security in a class room environment. More information can be found on the DVWA [site](#).

Once this infrastructure is built you create an Elastic Load Balancer in AWS that will direct traffic from the Internet to the Barracuda Web Application Firewall (both management and web). Next you will configure a Barracuda Web Application Firewall (WAF) to provide the service of the Damn Vulnerable Web Application (DVWA). After this is created you will connect to the DVWA web application and run the attacks to see how they are logged in the Barracuda Web Application Firewall.

These detailed step-by-step instructions will guide you through the lab.

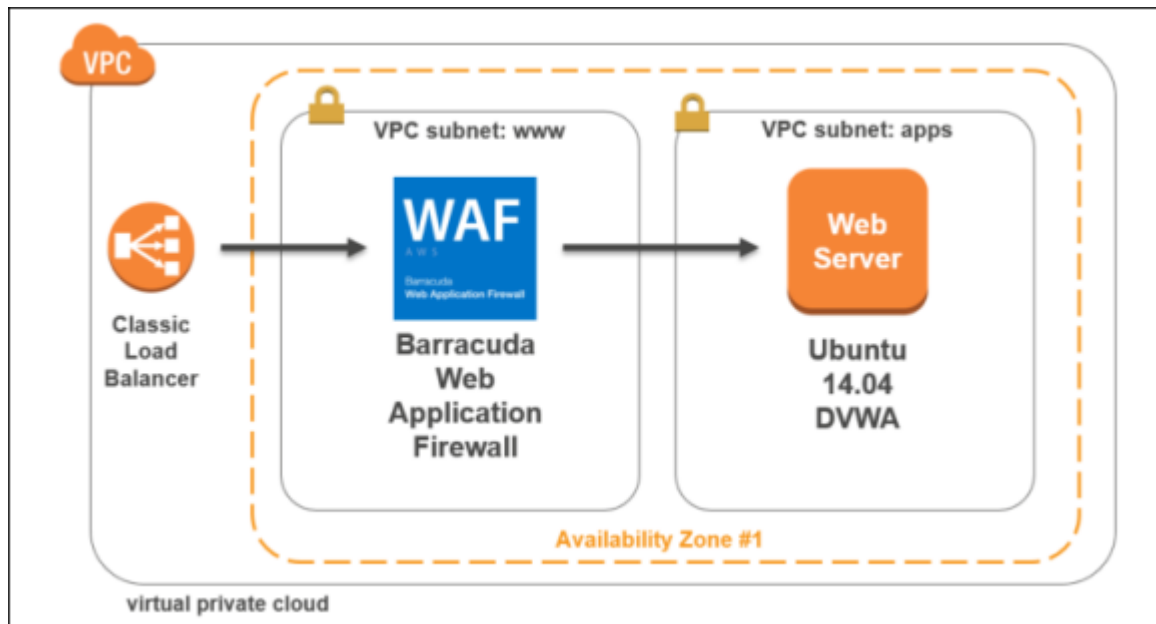
Scenarios

- Deploy and configure an AWS Virtual Private Cloud.
- Provision and configure the Barracuda Web Application Firewall.
- Deploy and configure the DVWA application.
- Simulate attacks on the site using the DVWA application and capture the attacks being launched, configure policies and run reports from the WAF.

Requirements

- Amazon Web Services subscription
- Valid contact details to complete the Barracuda Web Application Firewall trial registration

The following is a diagram of the deployment that will be completed at the end of this hands-on lab.

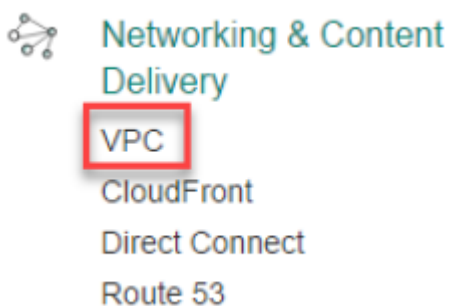


Exercise 1: Environment Setup

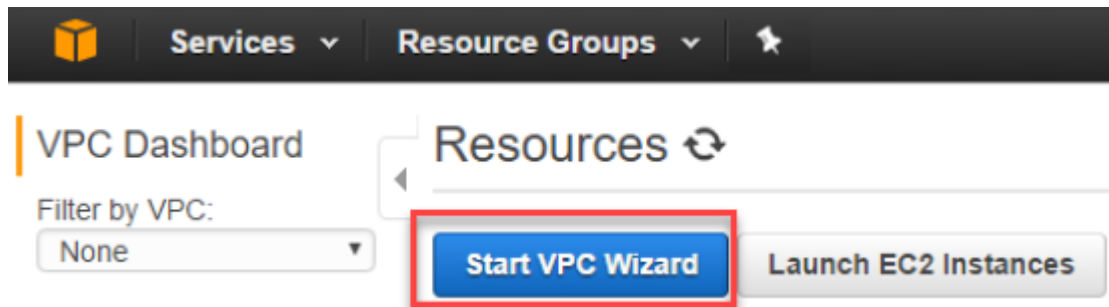
In this exercise, you will use an AWS Console to implement the infrastructure that will be leveraged for the rest of the exercises. This includes creating the Virtual Private Cloud (VPC), provisioning the Barracuda Web Application Firewall, the Elastic Load Balancer (ELB), and the Ubuntu server which will host the DVWA application.

Task 1: Create the Networking Infrastructure using an AWS Console

1. Go to the AWS portal <https://console.aws.amazon.com/>. After entering your credentials, the AWS Dashboard will display.
2. Click through **Console > Networking & Content Delivery > VPC**.

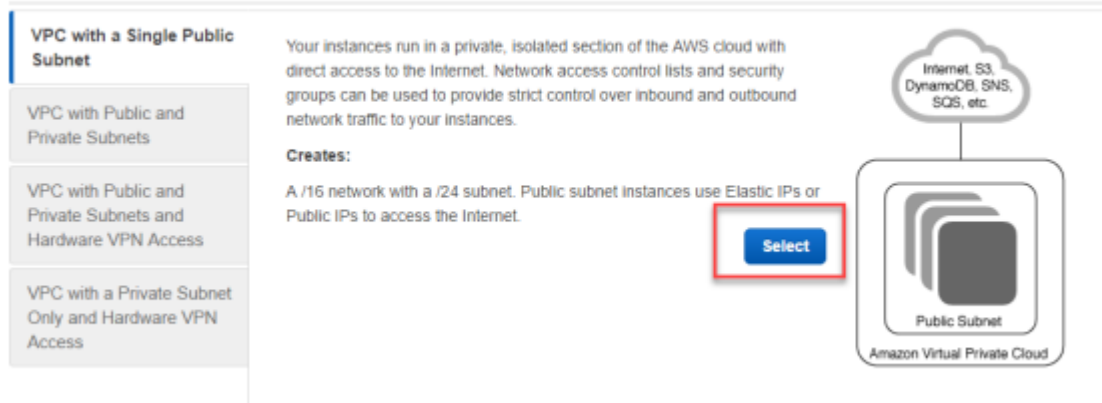


3. Next, click **Start VPC Wizard**.

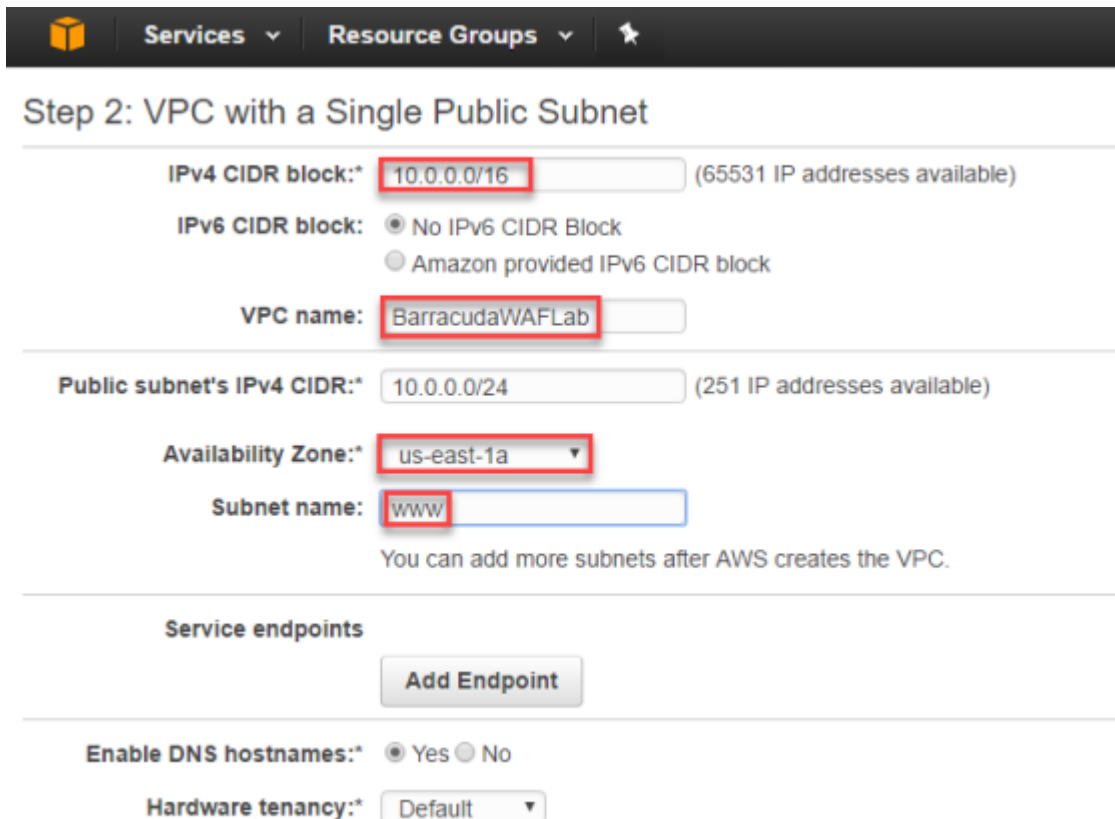


4. On **Step 1: Select a VPC Configuration**, click **Select**.

Step 1: Select a VPC Configuration



5. Complete the **Step 2: VPC with a Single Public Subnet** screen using the following details and then click **Create VPC**.
- **IPv4 CIDR block** - 10.0.0.0/16
 - **VPC name** - BarracudaWAFLab
 - **Availability Zone** - us-east-1a
 - **Subnet name** - www



Step 2: VPC with a Single Public Subnet

IPv4 CIDR block:* 10.0.0.0/16 (65531 IP addresses available)

IPv6 CIDR block: ☒ No IPv6 CIDR Block
☐ Amazon provided IPv6 CIDR block

VPC name: BarracudaWAFLab

Public subnet's IPv4 CIDR:* 10.0.0.0/24 (251 IP addresses available)

Availability Zone:* us-east-1a

Subnet name: www

You can add more subnets after AWS creates the VPC.

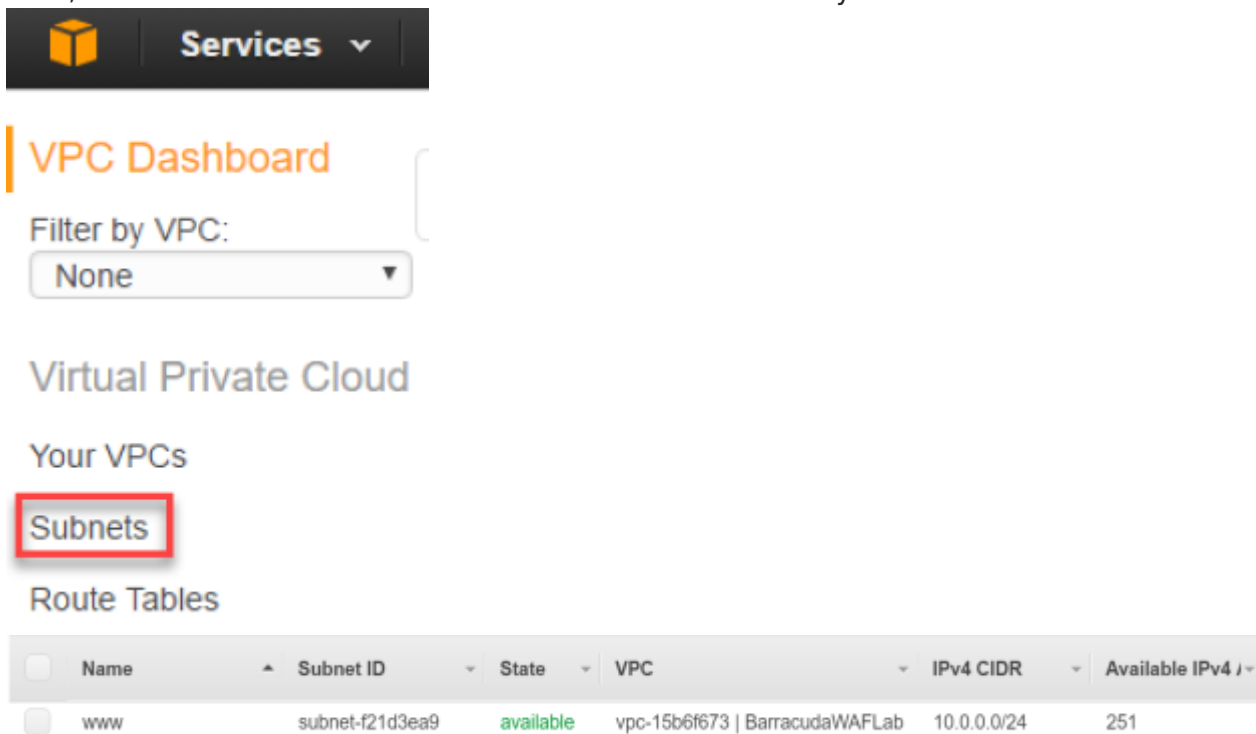
Service endpoints

[Add Endpoint](#)

Enable DNS hostnames:* ☒ Yes ☐ No

Hardware tenancy:* Default

6. Next, click **Subnets** and review the subnet that was created by the wizard.



VPC Dashboard

Filter by VPC: None

Virtual Private Cloud

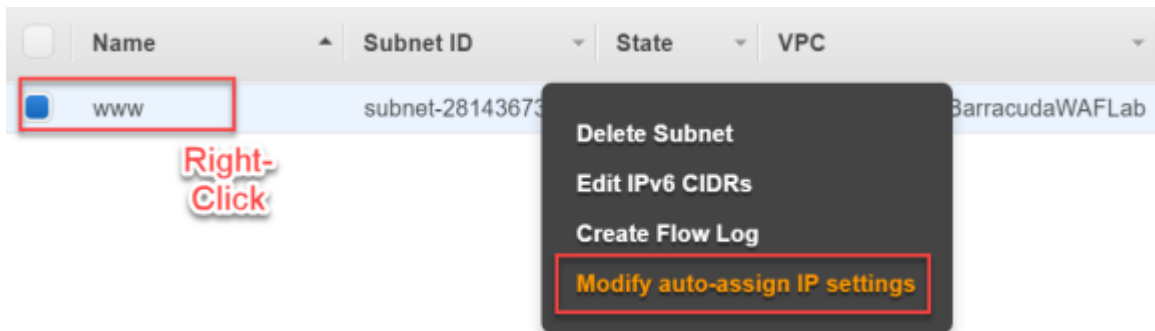
Your VPCs

Subnets

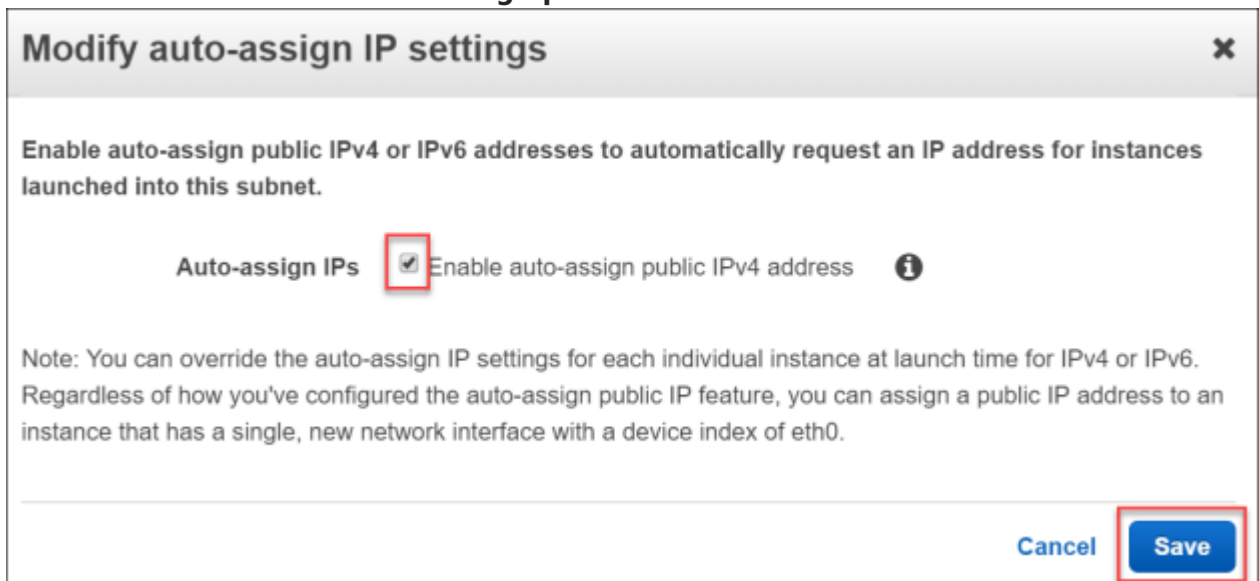
Route Tables

Name	Subnet ID	State	VPC	IPv4 CIDR	Available IPv4
www	subnet-f21d3ea9	available	vpc-15b6f673 BarracudaWAFLab	10.0.0.0/24	251

7. Right click on the subnet, and then click **Modify auto-assign IP settings**. The **Modify auto-assign IP settings** screen opens.



8. Check the box for **Enable auto-assign public IPv4 address** and then click **Save**.



Modify auto-assign IP settings

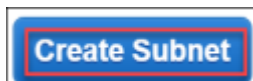
Enable auto-assign public IPv4 or IPv6 addresses to automatically request an IP address for instances launched into this subnet.

Auto-assign IPs ☒ Enable auto-assign public IPv4 address

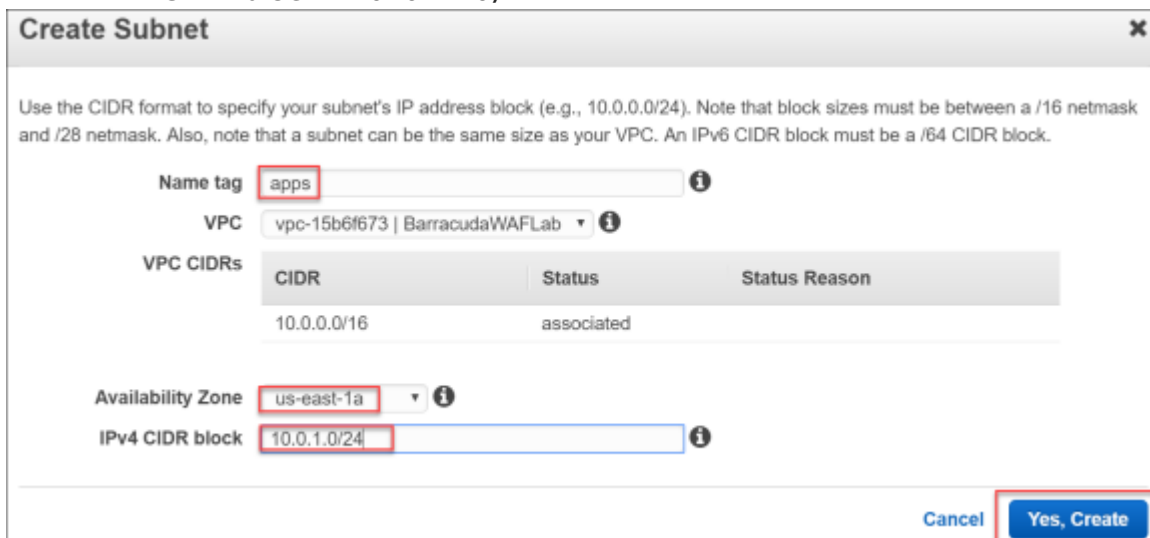
Note: You can override the auto-assign IP settings for each individual instance at launch time for IPv4 or IPv6. Regardless of how you've configured the auto-assign public IP feature, you can assign a public IP address to an instance that has a single, new network interface with a device index of eth0.

Cancel Save

9. From the **Subnet** screen, click **Create Subnet** to create a new subnet.



10. Complete the **Create Subnet** screen using the following details, then click **Yes Create**:
- **Name tag** - apps
 - **Availability Zone** - us-east-1a
 - **IPv4 CIDR block** - 10.0.1.0/24



Create Subnet

Use the CIDR format to specify your subnet's IP address block (e.g., 10.0.0.0/24). Note that block sizes must be between a /16 netmask and /28 netmask. Also, note that a subnet can be the same size as your VPC. An IPv6 CIDR block must be a /64 CIDR block.

Name tag

VPC

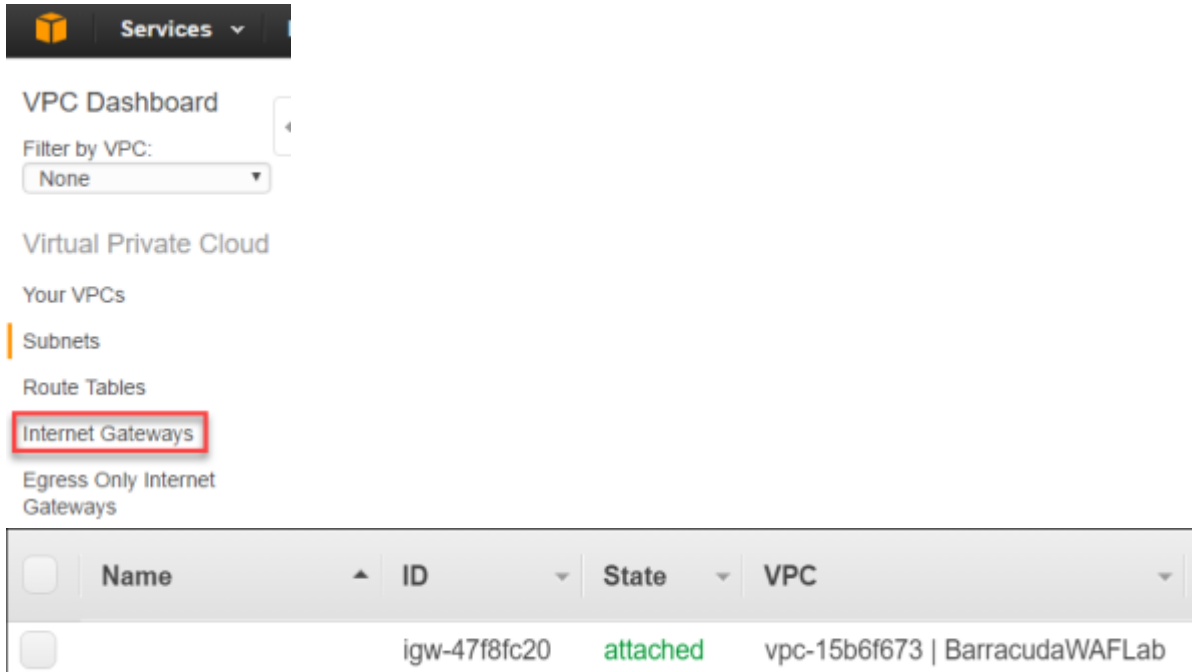
VPC CIDRs	CIDR	Status	Status Reason
	10.0.0.0/16	associated	

Availability Zone

IPv4 CIDR block

Cancel Yes, Create

11. On the **Subnets** page, review both the **www** and **apps** subnets.
12. From the **VPC Dashboard**, click **Internet Gateways** and review how this was created by the wizard. Make sure that the **State** shows **attached**.



VPC Dashboard

Filter by VPC: None

Virtual Private Cloud

Your VPCs

Subnets

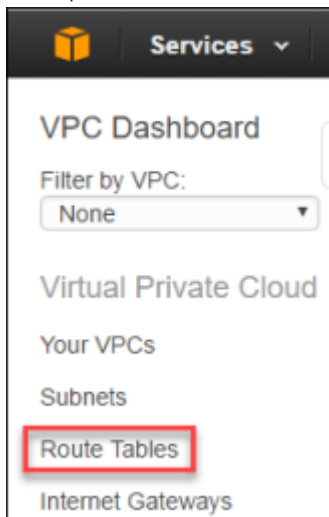
Route Tables

Internet Gateways

Egress Only Internet Gateways

<input type="checkbox"/>	Name	ID	State	VPC
<input type="checkbox"/>		igw-47f8fc20	attached	vpc-15b6f673 BarracudaWAFLab

13. Next, click **Route Tables** to review how the routing has been configured.



VPC Dashboard

Filter by VPC: None

Virtual Private Cloud

Your VPCs

Subnets

Route Tables

Internet Gateways

14. Notice that the **www** subnet has been configured to associate the Internet bound route 0.0.0.0/0 to the **Internet Gateway**.

rtb-43d2463a

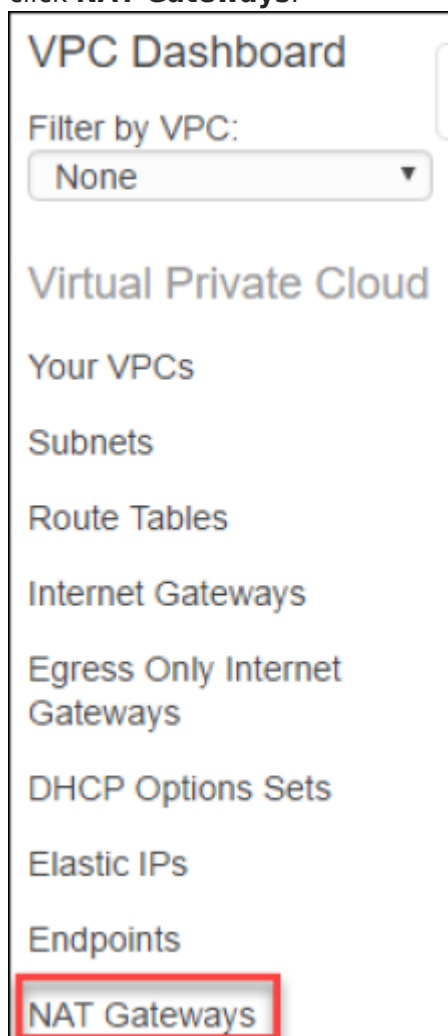
Summary Routes Subnet Associations Route Propagation Tags

Edit

View: All rules ▼

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No
0.0.0.0/0	igw-47f8fc20	Active	No

15. From the AWS console, click **VPC** under the **Networking and Content Delivery**, then click **NAT Gateways**.



16. Click **Create a NAT Gateway**.

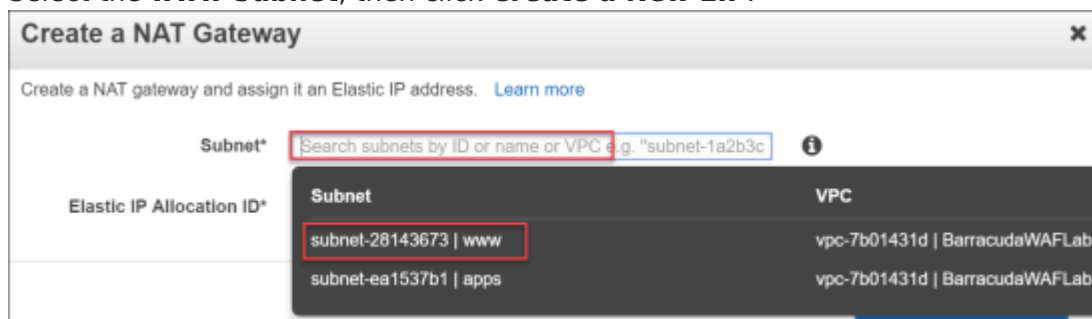
You do not have any NAT gateways in this region.

Choose the Create NAT gateway button to create your first NAT gateway.

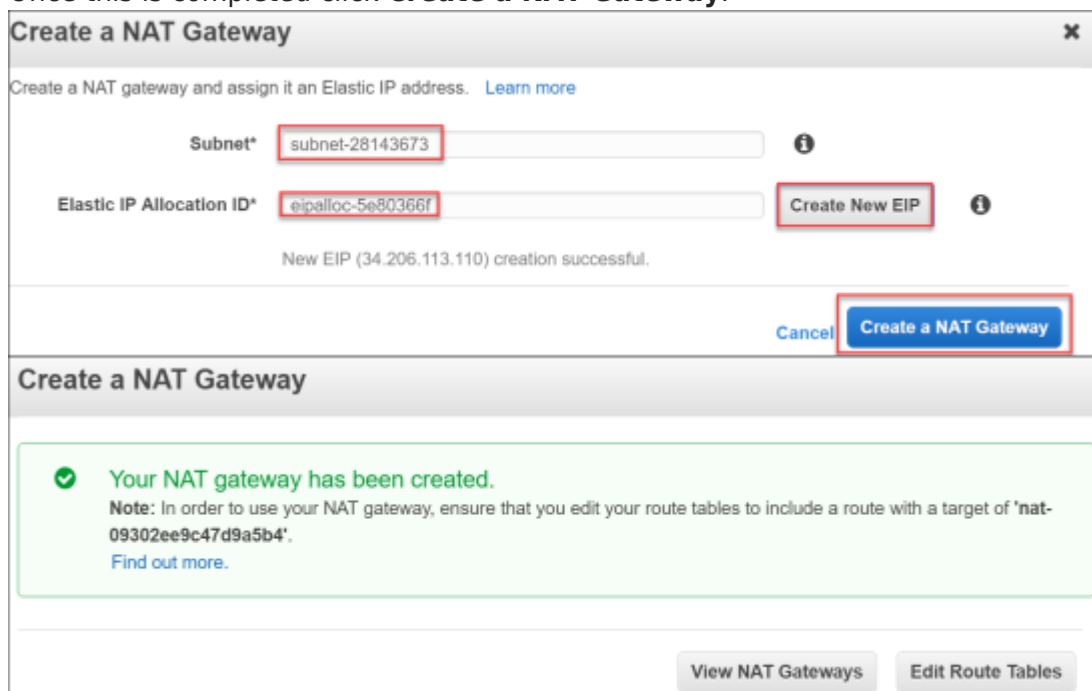
Create a NAT Gateway

The **Create a NAT Gateway** window opens.

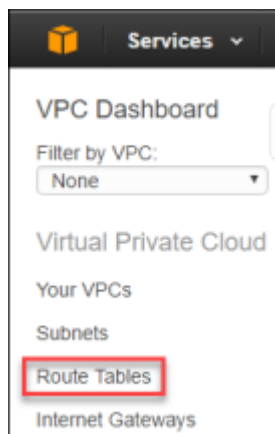
17. Select the **www Subnet**, then click **Create a New EIP**.



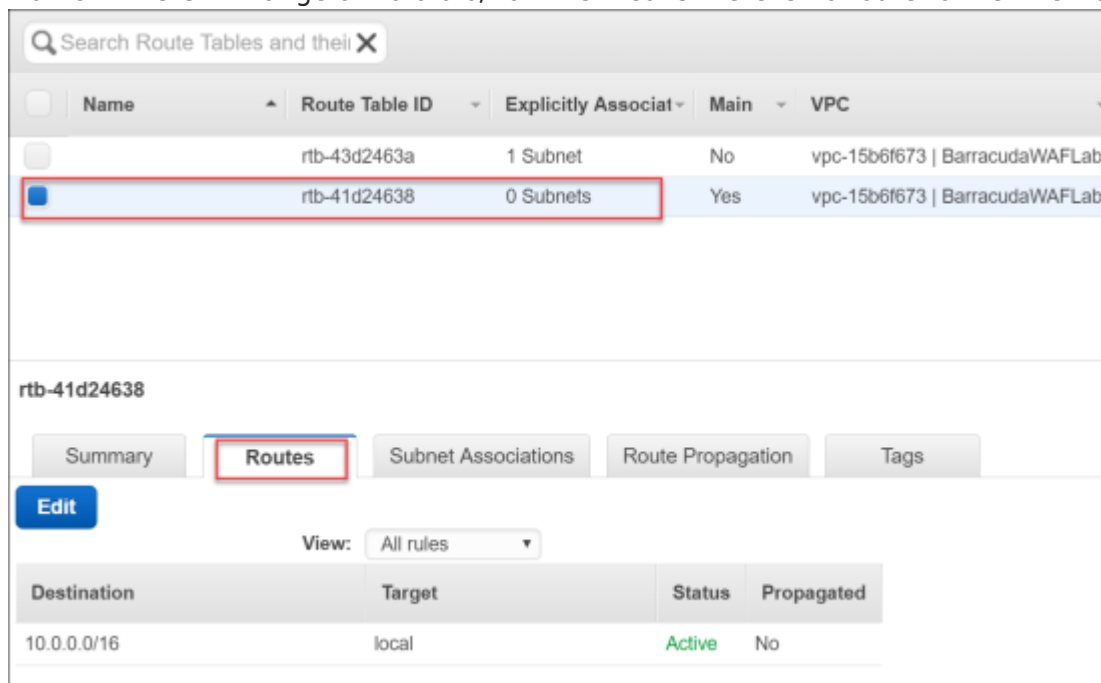
18. Once this is completed click **Create a NAT Gateway**.



19. Next, click **Route Tables** to review how the routing has been configured.



20. Locate the second route table that was created, but currently has 0 subnets associated.
21. Click this **Route Table** and select **Routes**. Notice how currently this is only a route for local traffic in the CIDR range of 10.0.0.0/16. This means there is no route to the Internet.



22. Click **Edit**, to make changes to the route table:
 1. Click **Add Another Route**.
 2. As the **Destination**, select **0.0.0.0/0**.
 3. As the **Target**, select the NAT gateway.
 4. Click **Save**.

rtb-41d24638

Summary Routes Subnet Associations Route Propagation Tags

Cancel Save

View: All rules

Destination	Target	Status	Propagated	Remove
10.0.0.0/16	local	Active	No	
0.0.0.0/0	nat-09302ee9c47d9a5b4		No	

Add another route

23. Click the **Subnet Associations** tab, and select **Edit**.

Summary Routes Subnet Associations

Edit

Subnet	IPv4 CIDR	IPv6 CIDR
You do not have any subnet associations.		
The following subnets have not been explicitly associated with any route tables and are therefore associated with the main route table:		
Subnet	IPv4 CIDR	IPv6 CIDR
subnet-ea1537b1 apps	10.0.1.0/24	-

24. Now, check the box for the **apps** subnet to associate this route table with the **apps** subnet.

Summary Routes Subnet Associations Route Propagation

Cancel Save

Associate	Subnet	IPv4 CIDR	IPv6 CIDR	Current Route Table
<input type="checkbox"/>	subnet-28143673 www	10.0.0.0/24	-	rtb-204fd859
<input checked="" type="checkbox"/>	subnet-ea1537b1 apps	10.0.1.0/24	-	Main

Now the private servers on the **apps** subnet will use the NAT gateway for their Internet bound traffic.

Task 2: Provision the Barracuda WAF using the AWS Marketplace

1. Sign-in to the AWS Console.
2. On the right-hand side of the console under AWS Marketplace, click the **Learn more** link.

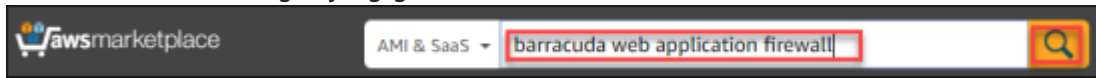
AWS Marketplace

Discover, procure, and deploy popular software products that run on AWS

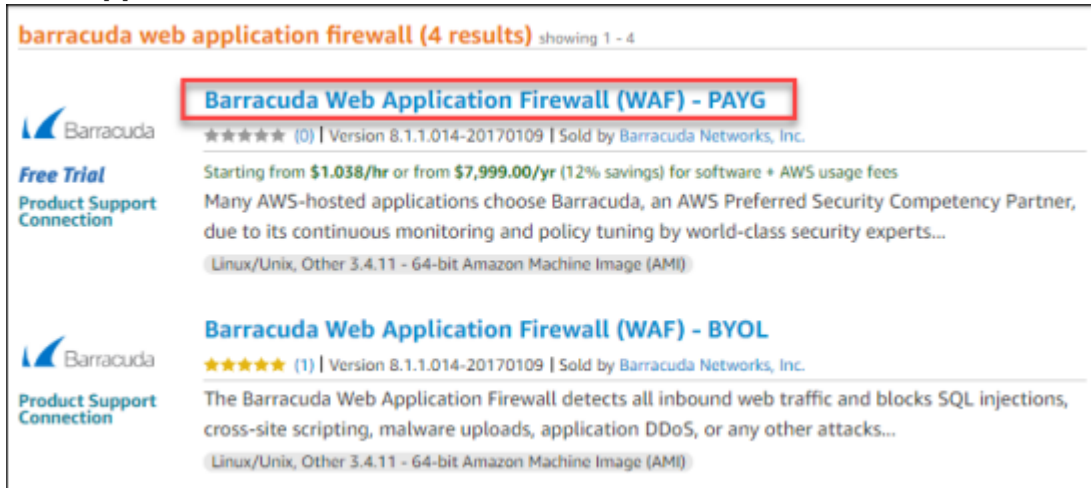
[Learn more](#)

3. In the **AWS Marketplace** search box, type Barracuda Web Application Firewall and

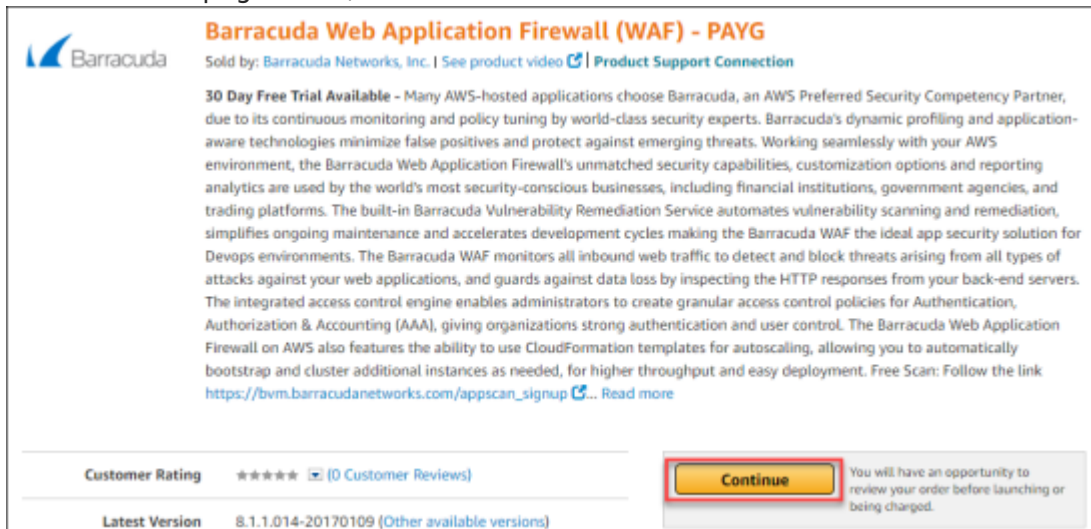
then click on the magnifying glass.



4. Several Barracuda Networks products will be returned by this search. Choose the **Barracuda Web Application Firewall (WAF) - PAYG**.

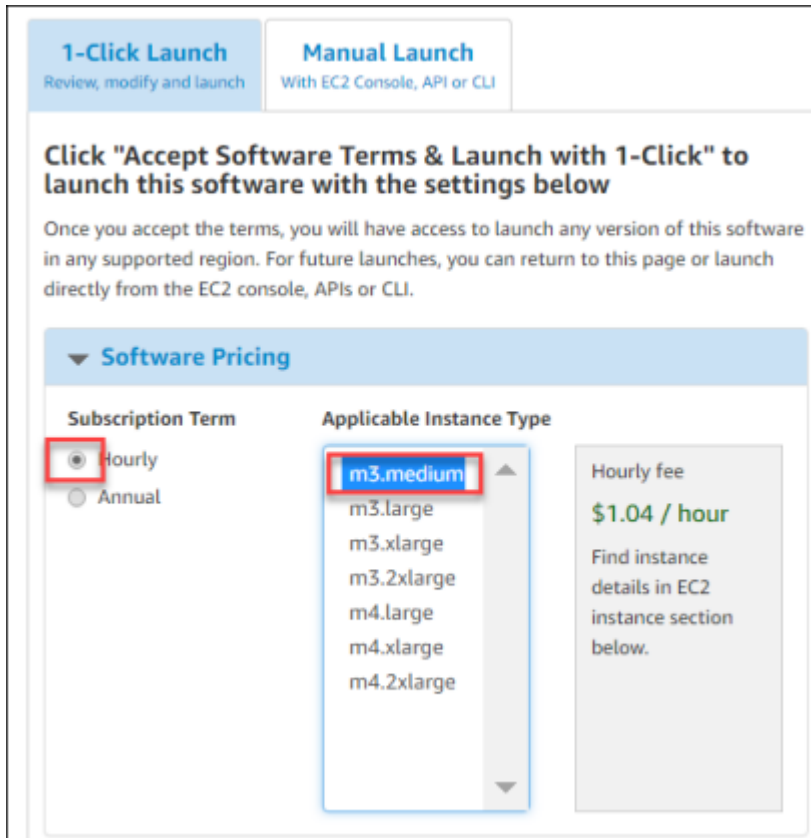


5. Once the WAF page loads, click **Continue**.



6. Complete the Launch wizard using the following settings:

- **Type - 1-Click Launch**
- **Software Pricing - Hourly / m3. medium**



1-Click Launch
Review, modify and launch

Manual Launch
With EC2 Console, API or CLI

Click "Accept Software Terms & Launch with 1-Click" to launch this software with the settings below

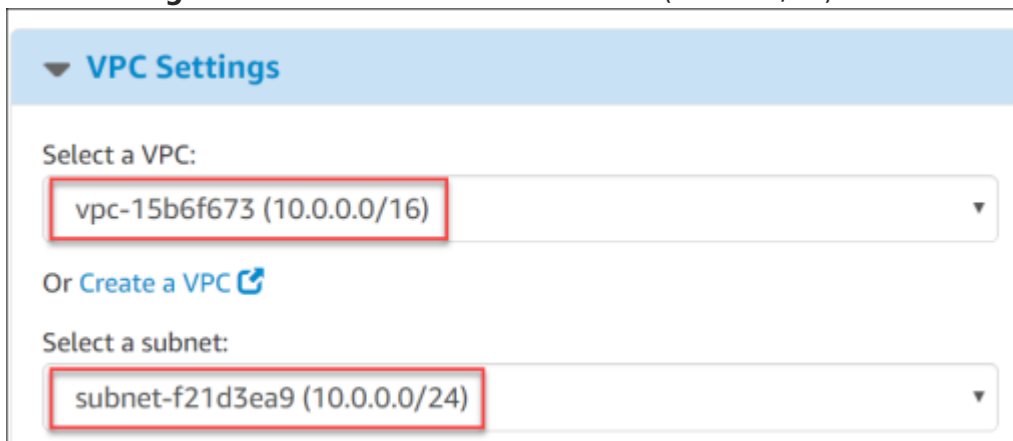
Once you accept the terms, you will have access to launch any version of this software in any supported region. For future launches, you can return to this page or launch directly from the EC2 console, APIs or CLI.

Software Pricing

Subscription Term	Applicable Instance Type	Hourly fee
<input checked="" type="radio"/> Hourly	m3.medium	\$1.04 / hour
<input type="radio"/> Annual	m3.large	
	m3.xlarge	
	m3.2xlarge	
	m4.large	
	m4.xlarge	
	m4.2xlarge	

Find instance details in EC2 instance section below.

- **Version** – accept the latest version.
- **Region** – **US East (N. Virginia)**
- **EC2 Instance Type** – **m3.medium**
- **VPC Settings** – Select the VPC and www subnet (10.0.0.0/24).



VPC Settings

Select a VPC:

vpc-15b6f673 (10.0.0.0/16)

Or [Create a VPC](#)

Select a subnet:

subnet-f21d3ea9 (10.0.0.0/24)

- **Security Group** – Select **Create new based on seller settings**.

▼ Security Group

A security group acts as a firewall that controls the traffic allowed to reach one or more instances. [Learn more about Security Groups.](#)

You can create a new security group based on seller-recommended settings or choose one of your existing groups.

Create new based on seller settings ▼

! A new security group will be generated by AWS Marketplace. It is based on recommended settings for Barracuda Web Application Firewall (WAF) - PAYG version 8.1.1.014-20170109 provided by Barracuda Networks, Inc..

Connection Method	Protocol	Port Range	Source (IP or Group)
	tcp	8000 - 8000	Anywhere ▼ 0.0.0.0/0
HTTPS*	tcp	8443 - 8443	Anywhere ▼ 0.0.0.0/0
HTTP	tcp	80 - 80	Anywhere ▼ 0.0.0.0/0

- **Key Pair** - Select or **Create a New Key**

7. After verifying the selections, click **Launch with 1-click**.

Price for your Selections:

\$1.10 / hour
\$0.07 m3.medium EC2 Instance usage fees +
\$1.04 hourly software fee
Additional taxes may apply.

\$0.10 per GB-month of provisioned storage
EBS General Purpose (SSD) volumes

Launch with 1-click

You will be subscribed to this software and agree that your use of this software is subject to the pricing terms and the seller's [End User License Agreement \(EULA\)](#) and your use of AWS services is subject to the [AWS Customer Agreement](#).

8. Next on the **AWS Marketplace Product Support Connection** screen, click **Share your contact details**.

AWS Marketplace Product Support Connection

You can register for support with this software's vendor by clicking the button below, which will open a new browser tab. Sharing your contact details is not required, but offering this information to the vendor will make it easier for you to obtain support for this product. We recommend you enter this information now, but you can do so from the right column of this page or the [Your Software](#) page at any time.

[Share your contact details](#) [Skip this step](#)

9. Complete the **Barracuda Networks Support Form** and click **Register & Close**.

Add contact 1 of 5 for Barracuda Web Application Firewall (WAF) - PAYG

Please list the contact details for a person you would like to have as a support contact for this subscription. While you are not required to register a contact for support, if you choose to do so vendors will need the information in the fields marked with an asterisk.

First Name *	<input type="text"/>	Last Name *	<input type="text"/>
Job Title	<input type="text"/>	Organization *	<input type="text"/>
Email *	<input type="text"/>	Phone *	<input type="text"/>
Zip Code	<input type="text"/>	Country	<input type="text"/>

☐ I agree that by submitting this form I am granting permission to share the contact information listed above with Barracuda Networks, Inc.
[Click Here](#) to learn more about how Amazon processes the provided information and how it can be shared with vendors for product support purposes.

[Cancel](#) [Register & Add Another Contact](#) [Register & Close](#)

10. After completing the registration, the following page will appear from which the WAF was launched:

✓ Thank you for subscribing to Barracuda Web Application Firewall (WAF) - PAYG

An instance of this software will be deployed on EC2 soon after your subscription completes.
You can check the status of this instance on [EC2 Console](#). You can also view all instances on [Your Software](#) page.
Software and AWS hourly usage fees apply when the instance is running and will appear on your monthly bill.

Next Steps:

- You will receive an email once your subscription completes.
- Once you are subscribed, an instance of this software will be deployed on EC2.
- The software will be ready in a few minutes.

Software Installation Details

Product	Barracuda Web Application Firewall (WAF) - PAYG
Version	8.1.1.014-20170109
Region	us-east-1
EC2 Instance Type	m3.medium
VPC	vpc-26357040
Subnet	subnet-4134131a
Security Group	Create new security group based on seller settings
Key Pair	AWSKEY

AWS Marketplace Product Support Connection

You can register for support with software vendors by providing contact information. Sharing your contact details is not required, but offering this information to the vendor will make it easier for you to obtain support for this product. We recommend you enter this information now, but you can do so from the [Your Software](#) page at any time.

[Share your contact details](#)

Related Links

- [AWS Management Console](#)
- [Your Software](#)
- [Continue shopping on AWS Marketplace](#)

Service Catalog

[Click here](#) for instructions to deploy Marketplace products in [AWS Service Catalog](#).

11. Click on the EC2 Console link in the green message about the deployment of the Barracuda

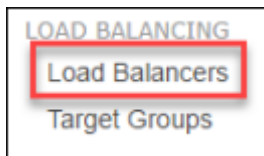
Web Application Firewall. Once it is deployed the instance will show it is **Running**.

<input type="checkbox"/>	Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks
<input type="checkbox"/>		i-001be783834af5661	m3.medium	us-east-1a	running	2/2 checks ...

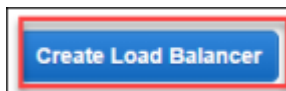
Don't continue on to the next step until the Barracuda WAF instance is in the running state as in the screen shot above.

Task 3: Provision the Elastic Load Balancer

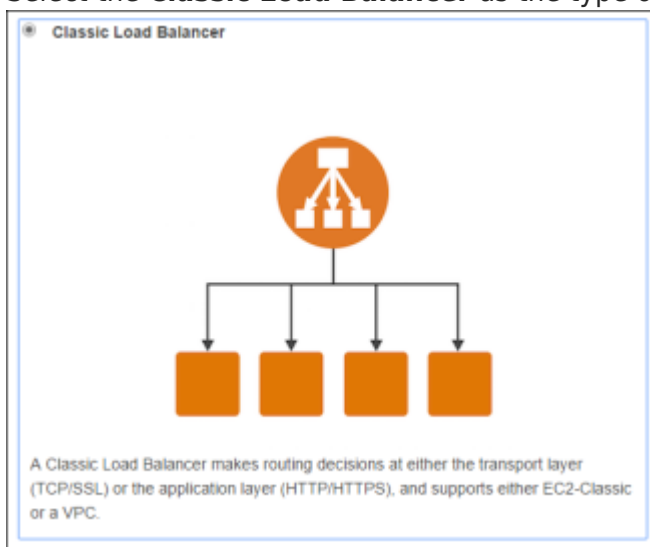
1. In the AWS Console, click on **Load Balancers**.



2. Select **Create Load Balancer**.



3. Select the **Classic Load Balancer** as the type of Elastic Load Balancer, and click **Continue**.



4. In **Step 1: Define Load Balancer**, complete the screen using these inputs.
 - **Load Balancer Name** – BarracudaWAF-ELB
 - **Create LB Inside** – Select the VPC that you created for this lab.
 - **Subnet** – Select the **www** subnet.

Step 1: Define Load Balancer

Create an internal load balancer: ☐ (what's this?)

Enable advanced VPC configuration: ☒

Listener Configuration:

Load Balancer Protocol	Load Balancer Port	Instance Protocol	Instance Port
HTTP	80	HTTP	80
HTTP	8000	HTTP	8000

Add

Select Subnets

You will need to select a Subnet for each Availability Zone where you wish traffic to be routed by your load balancer. If you have instances in only one Availability Zone, please select at least two Subnets in different Availability Zones to provide higher availability for your load balancer.

VPC vpc-26357040 (10.0.0.0/16) | BarracudaWAFLab

Please select at least two Subnets in different Availability Zones to provide higher availability for your load balancer.

Actions	Availability Zone	Subnet ID	Subnet CIDR	Name
<input checked="" type="radio"/>	us-east-1a	subnet-4134131a	10.0.0.0/24	www

5. Click **Next: Assign Security Groups**.

Next: Assign Security Groups

6. Deselect the default security group, and select the new **Barracuda Web Application (WAF)** security group that was created by the AWS Marketplace deployment of the device.

Step 2: Assign Security Groups

You have selected the option of having your Elastic Load Balancer inside of a VPC. You must assign one or more security groups to this load balancer. This can be changed at any time.

Assign a security group:

☐ Create a **new** security group

☒ Select an **existing** security group

Security	Name
<input checked="" type="checkbox"/>	sg-f3302b8f Barracuda Web Application Firewall (WAF) - PAYG-8.1.1
<input type="checkbox"/>	sg-0a786376 default

7. Click **Next: Configure Security Settings**.

Next: Configure Security Settings

8. Click **Next: Configure Health Check**.

Next: Configure Health Check

9. Complete the **Step 4: Configure Health Check** screen, using the following settings:

- **Ping Protocol** – TCP
- **Ping Port** – 8000
- **Advanced Details** – Accept defaults.

Step 4: Configure Health Check
Your load balancer will automatically perform health checks on your health check, it is automatically removed from the load balancer. Cu

Ping Protocol

Ping Port

Advanced Details

Response Timeout	<input type="text" value="5"/>	seconds
Interval	<input type="text" value="30"/>	seconds
Unhealthy threshold	<input type="text" value="2"/>	
Healthy threshold	<input type="text" value="10"/>	

10. Click **Next: Add EC2 Instances**.

Next: Add EC2 Instances

11. On the **Step 5: Add EC2 Instances** screen, click on the instance.

Step 5: Add EC2 Instances
The table below lists all your running EC2 Instances. Check the boxes in the Select column to add those instan

VPC vpc-26357040 (10.0.0.0/16) | BarracudaWAFLab

<input type="checkbox"/>	Instance	Name	State	Security groups
<input checked="" type="checkbox"/>	i-001be783...		running	Barracuda Web Application Firew..

12. Click **Next: Add Tags**.

Next: Add Tags

13. Click **Review and Create**.

Review and Create

14. Review **Step 7: Review** and compare to the ensure that everything is configured properly.

Step 7: Review
Please review the load balancer details before continuing

▼ Define Load Balancer [Edit load balancer definition](#)

Load Balancer name: BarracudaWAF-ELB
Scheme: internet-facing
Port Configuration: 80 (HTTP) forwarding to 80 (HTTP)
8000 (HTTP) forwarding to 8000 (HTTP)

▼ Configure Health Check [Edit health check](#)

Ping Target: TCP:8000
Timeout: 5 seconds
Interval: 30 seconds
Unhealthy threshold: 2
Healthy threshold: 10

▼ Add EC2 Instances [Edit instances](#)

Cross-Zone Load Balancing: Enabled
Connection Draining: Enabled, 300 seconds
Instances: i-068104bc019b7c6a5

▼ VPC Information [Edit subnets](#)

VPC: vpc-26357040 (BarracudaWAFLab)
Subnets: subnet-4134131a (www)

▼ Security groups [Edit security groups](#)

[Cancel](#) [Previous](#) [Create](#)

15. You should then get a message that the **BarracudaWAF-ELB** was successfully created:

Load Balancer Creation Status

✓ **Successfully created load balancer**
Load balancer **BarracudaWAF-ELB** was successfully created.
Note: It may take a few minutes for your instances to become active in the new load balancer.

[Close](#)

16. In the AWS Console, click the **Load Balancers** link.

LOAD BALANCING

Load Balancers

Target Groups

17. On the **BarracudaWAF-ELB** load balancer that you created, on the **Description** tab, locate the DNS name of the load balancer and copy it to a text file. You will use this to connect to later in the lab.

Load balancer: **BarracudaWAF-ELB**

Description Instances Health Check Listeners Monitoring Tags

Basic Configuration

Name: BarracudaWAF-ELB

* DNS name: **BarracudaWAF-ELB-1474027757.us-east-1.elb.amazonaws.com**

Scheme: internet-facing

Availability Zones: subnet-28143673 - us-east-1a

barracudalab - Notepad

File Edit Format View Help

BarracudaWAF-ELB-1474027757.us-east-1.elb.amazonaws.com

18. Next, click the **Instances** tab. You may notice that the WAF has yet to be put into service by the ELB. Wait until you see that the **Status** change to **InService**. You need to hit the refresh button to see the updates.

Load balancer: **BarracudaWAF-ELB**

Description **Instances** Health Check Listeners Monitoring Tags

Connection Draining: Enabled, 300 seconds (Edit)

Edit Instances

Instance ID	Name	Availability Zone	Status
i-068104bc019b7c6a5		us-east-1a	OutOfService ⓘ

Instance registration is still in progress.

Load balancer: **BarracudaWAF-ELB**

Description **Instances** Health Check Listeners Monitoring Tags

Connection Draining: Enabled, 300 seconds (Edit)

Edit Instances

Instance ID	Name	Availability Zone	Status
i-068104bc019b7c6a5		us-east-1a	InService ⓘ

19. Click the **Instance ID** number which will break up details about the BarracudaWAF instance.

Instance ID

i-068104bc019b7c6a5

20. On the **Description** tab, locate the IPv4 Public IP for the WAF and take note of the address.

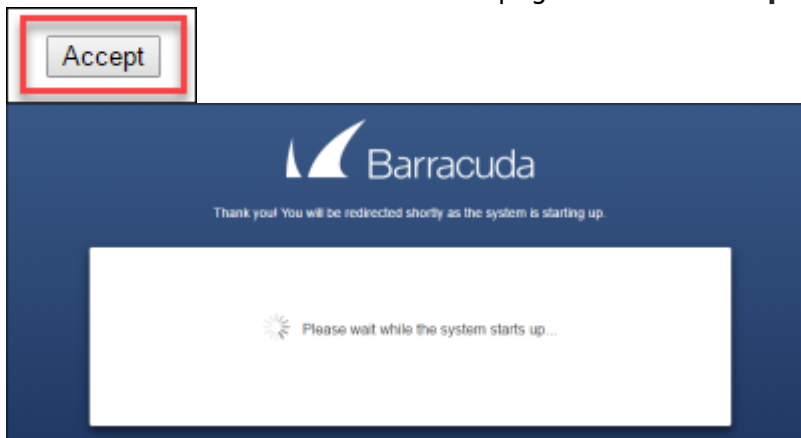
IPv4 Public IP 54.88.67.91

21. Open a new tab on your web browser and point it to **PUBLIC IP address on the management port of 8000**. This will bring you to the home page of the WAF where there will be a licensing agreement displayed.

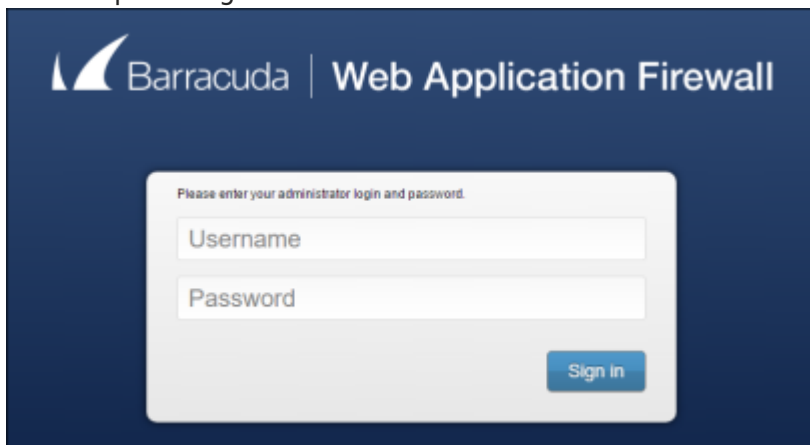


If the VM has just booted there may be a note that the VM is provisioning. This is normal and takes a few minutes to complete.

22. Scroll down to the bottom of the webpage and click **Accept**.



23. Once the system starts the login page will appear. Once this page has loaded move on to the next step leaving the tab here.

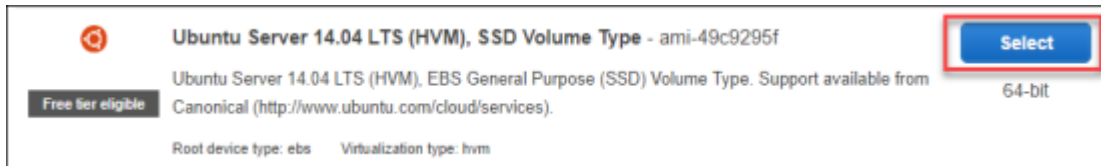


Task 4: Provision Ubuntu Server with the DVWA Application

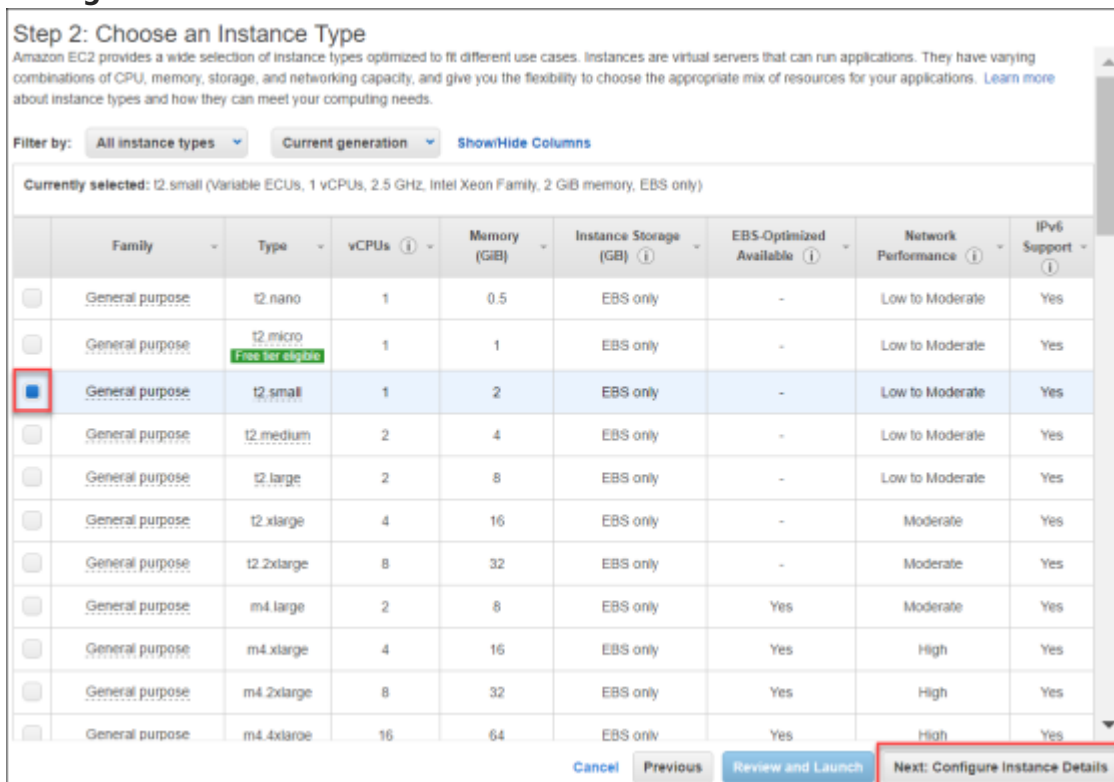
1. From the AWS console click **Instances**, then click **Launch Instance**.



2. Scroll down and select the **Ubuntu Server 14.04 LTS (HVM)** AMI to deploy as your Web Server for the DVWA.





3. At **Step 2: Choose an Instance Type**, select **t2.small** size for the VM. Then click **Next: Configure Instance Details**.




4. On **Step 3: Configure Instance Details**, complete the screen using these details wherever details are not provided leave the defaults, move on to the next step **without** clicking **Next**.
 - **Subnet** – apps
 - **Primary IP** – 10.0.1.50

Step 3: Configure Instance Details

Network ⓘ vpc-15b6f673 | BarracudaWAFLab  [Create new VPC](#)

Subnet ⓘ subnet-941c3fcf | apps | us-east-1a  [Create new subnet](#)
250 IP Addresses available

Auto-assign Public IP ⓘ Use subnet setting (Disable)

IAM role ⓘ None  [Create new IAM role](#)


Shutdown behavior ⓘ Stop

Enable termination protection ⓘ ☐ Protect against accidental termination

Monitoring ⓘ ☐ Enable CloudWatch detailed monitoring
[Additional charges apply.](#)

Tenancy ⓘ Shared - Run a shared hardware instance
[Additional charges will apply for dedicated tenancy.](#)

▼ **Network interfaces** ⓘ

Device	Network Interface	Subnet	Primary IP	Secondary IP addresses
eth0	New network interface ▼	subnet-941c3fcf (▼)	10.0.1.50 	Add IP

5. Again, on **Step 3: Configure Instance Details**, scroll down and click the **Advanced Details** tab. Copy this script text into the **User Data** box:

- `#!/bin/bash`
- `wget https://opsgilityweb.blob.core.windows.net/20170304-barracudawaf/dvwa.sh`
- `bash dvwa.sh`

Make sure that when pasting from the work document you could get spacing issues.
The script is only 3 lines, so check the spacing or the VM won't provision properly.

6. Click **Next: Add Storage**.

Next: Add Storage

7. On the **Step 4: Add Storage** screen, accept the defaults and click **Next: Add Tags**.

Next: Add Tags

8. On the **Step 5: Add Tags** screen, accept the defaults and click **Next: Configure Security Groups**.

Next: Configure Security Group

9. On **Step 6: Configure Security Group**, name it DVWA, click **Add Rule**, and add a rule for **HTTP Port 80**.

Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. [Learn more](#) about Amazon EC2 security groups.

Assign a security group: ☒ Create a new security group
☐ Select an existing security group

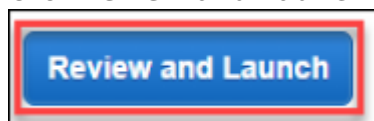
Security group name:

Description:

Type	Protocol	Port Range	Source
SSH	TCP	22	Custom 0.0.0.0/0
HTTP	TCP	80	Custom 0.0.0.0, ::0

[Add Rule](#)

10. Click **Review and Launch**.



11. On **Step 7: Review Instance Launch**, click **Launch**.

Step 7: Review Instance Launch

Please review your instance launch details. You can go back to edit changes for each section. Click **Launch** to assign a key pair to your instance and complete the launch process.

Improve your instances' security. Your security group, DVWA, is open to the world.

Your instances may be accessible from any IP address. We recommend that you update your security group rules to allow access from known IP addresses only. You can also open additional ports in your security group to facilitate access to the application or service you're running, e.g., HTTP (80) for web servers. [Edit security groups](#)

Your instance configuration is not eligible for the free usage tier

To launch an instance that's eligible for the free usage tier, check your AMI selection, instance type, configuration options, or storage devices. [Learn more about free usage tier eligibility and usage restrictions.](#)

[Don't show me this again](#)

AMI Details [Edit AMI](#)

Ubuntu Server 14.04 LTS (HVM), SSD Volume Type - ami-49c9295f

Free tier eligible: Ubuntu Server 14.04 LTS (HVM), EBS General Purpose (SSD) Volume Type. Support available from Canonical (<http://www.ubuntu.com/cloud/services>).
Root Device Type: ebs Virtualization type: hvm

Instance Type [Edit instance type](#)

Instance Type	ECUs	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance
t2.small	Variable	1	2	EBS only	-	Low to Moderate

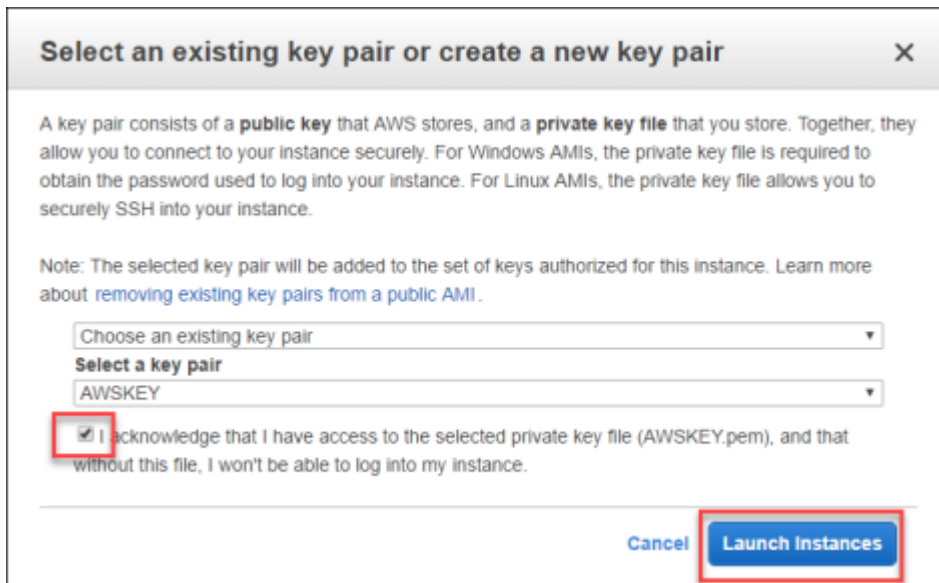
Security Groups [Edit security groups](#)

Security group name: DVWA
Description: This rule is used by the Damn Vulnerable Web Application (DVWA) http://http://www.dvwa.co.uk/

Type	Protocol	Port Range	Source
------	----------	------------	--------

[Cancel](#) [Previous](#) [Launch](#)

12. Select your AWS key pair, and click **Launch Instances**.



13. After a few minutes (maybe 10), check back on the EC2 Console and now both the WAF and the DVWA server should show as **running**. You can add names to the instances to make it easier to identify the VMs. The T2.small is the DVWA and the M3.Medium is the WAF.

<input type="checkbox"/>	DVWA	i-0069c029edfaf3e82	t2.small	us-east-1a	● running	✓ 2/2 checks ...
<input checked="" type="checkbox"/>	BarracudaWAF	i-054e125e897bf1f04	m3.medium	us-east-1a	● running	✓ 2/2 checks ...

Summary:

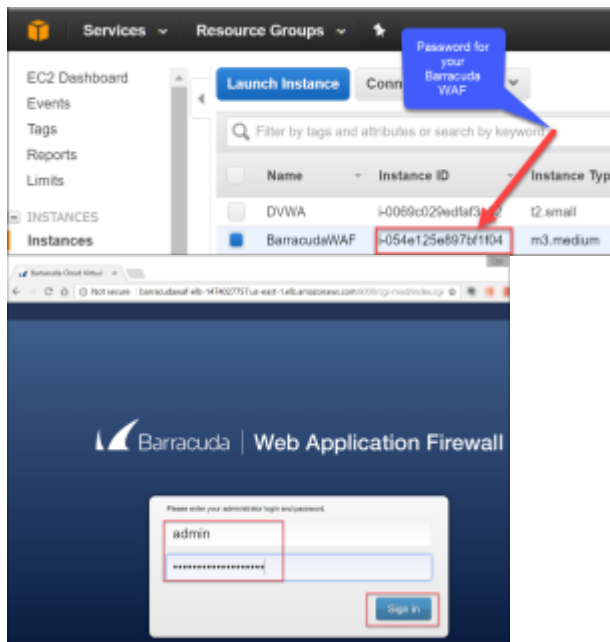
In this exercise, the AWS Console was used to implement the infrastructure that will be leveraged for the rest of the exercises. This included creating the Virtual Private Cloud (VPC), provisioning the Barracuda WAF, the Elastic Load Balancer (ELB), and the Ubuntu server.

Exercise 2: Configure the Barracuda WAF Virtual Appliance and the DVWA Application

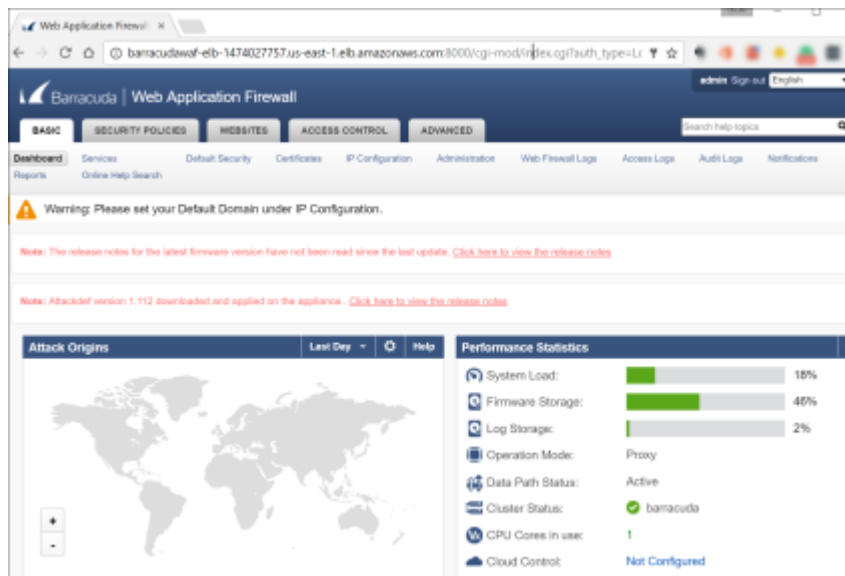
In this exercise, the Barracuda WAF Appliance and the DVWA Services will be configured. First the WAF will be configured to connect to the DVWA. Once this is completed then a connection to DVWA server will be made and the configuration will be completed. After this is finished the end to end setup will be complete allowing for simulated attacks in the next exercise.

Task 1: Configure the WAF Appliance

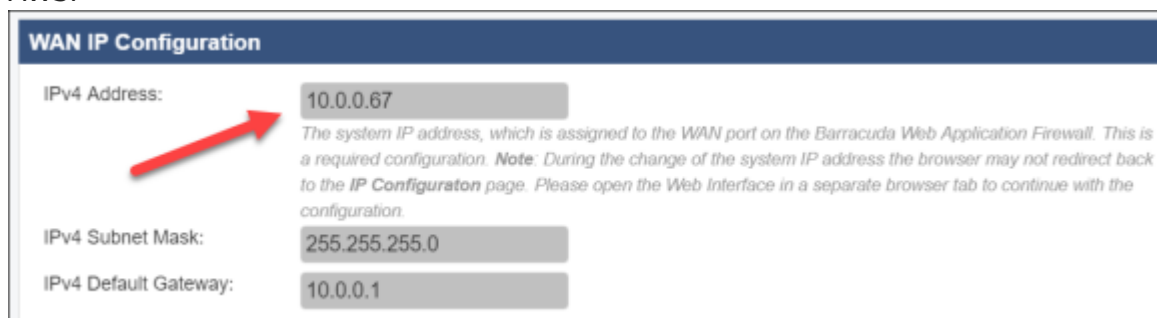
1. Move back to the tab that contained the login page or if this has been closed open it backup and connect to the WAF.
2. Use the following login information:
 - **Username** - admin
 - **Password** - Instance ID of your Barracuda WAF Instance in Amazon Web Services.



- Once logged in, you will be directed to the **Dashboard** page of the Barracuda Web Application Firewall.



- Go to **BASIC > IP Configuration**.
- Review the networking configuration and **take note of the IP address** assigned to the WAF by AWS.



- Update the **Default Host Name** barracudawaf which is the name you gave the VM when you

provisioned in the AWS Portal.



Domain Configuration

Default Host Name:
Used in reports and notifications.

Default Domain:
The default domain for the system. Example: mydomain.com

The Host Name is used in reporting, and is displayed in alerts, notifications and messages sent by the Barracuda Web Application Firewall.

7. Click **Save**.



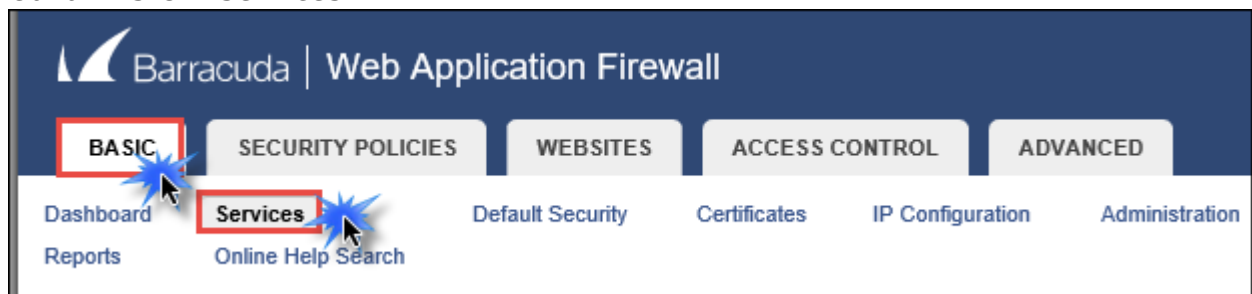
An error will be displayed about a Default Domain not configured. For this lab, this can be ignored. In production, the domain should be matched to that of the certificates being used for the SSL configuration.

Task 2: Create a Web Service to Publish the DVWA Application

1. Log into the Barracuda Networks device.

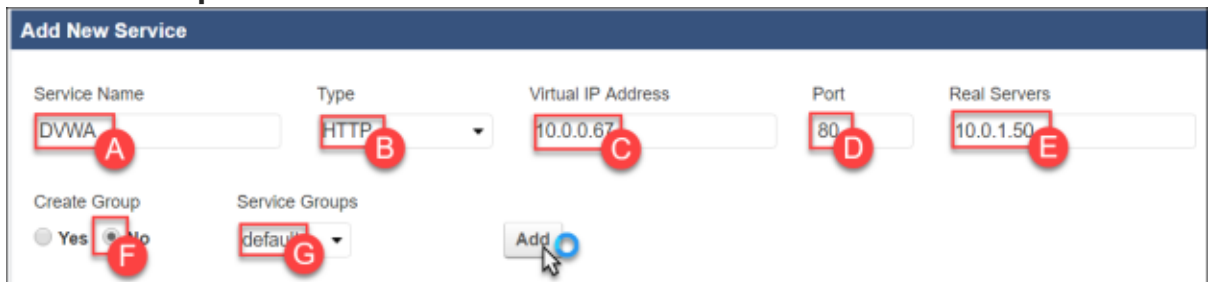
- **User** - admin
- **Password** - [InstanceID]

2. Go to **BASIC > Services**.



3. Go to **ADD NEW SERVICE**, update the fields, and then click **Add**.

- **Service Name** - DVWA
- **Type** - HTTP
- **Virtual IP Address** - IP address assigned to the WAF by AWS.
- **Port** - 80
- **Real Servers** - 10.0.1.50 (This is the address you assigned to the DVWA Server)
- **Create Group** - No
- **Service Groups** - default



Add New Service

Service Name: (A)

Type: (B)

Virtual IP Address: (C)

Port: (D)

Real Servers: (E)

Create Group: ☐ Yes ☒ No (F)

Service Groups: (G)

4. After about 15 seconds the firewall will update and the **Services** pane will now look like below:

Services											
Filter		Service Name ▾	Search		Search						
Name	Status	Hostname	IP Address	Port	Interface	Domain	URL	Type	Mode	Policy	Add
default											
default											
DVWA	✓		10.0.0.67	80	WAN			HTTP	Passive	default	Server Rule
Server_10.0.1.50	✓		10.0.1.50	80							

5. Open a new tab on the web browser and point it at the DNS name of the Elastic Load Balancer. This should be in the text file that you saved, or can be found on the ELB in the AWS Console. The DVWA server should load with the traffic flowing through the ELB and if the DVWA folder is on the server then it is installed.

If for some reason this webpage doesn't load make sure that you have entered the correct IP address for the barracudawaf and the DVWA web server. Another troubleshooting step if the DVWA is not coming up is to review the NAT Gateway configuration. The NAT Gateway must be deployed into the www subnet and the routing table for the apps subnet must point 0.0.0.0/0 to the NAT Gateway instance.

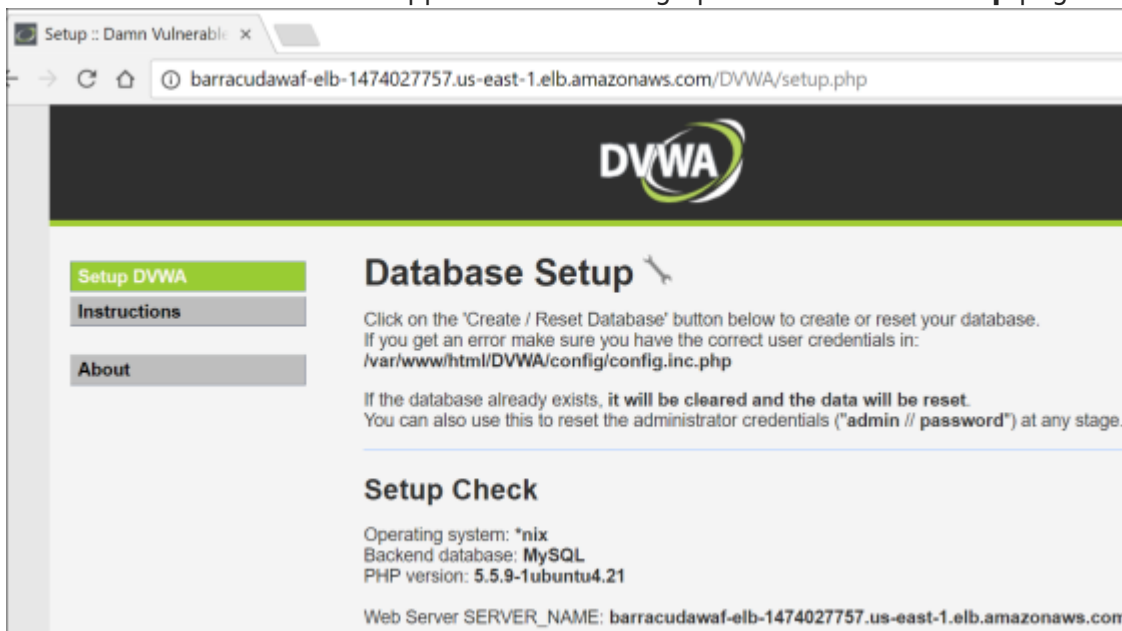


Task 3: Configure the Damn Vulnerable Web App

- From the connection to the DVWA server through the ELB, click the **DVWA** link to attach to DVWA and complete its configuration.



2. This will load the DVWA web application and bring up the **Database Setup** page.



3. Scroll down and click **Create / Reset Database**. You will briefly see an update that the database was created and then be redirected to a login page.

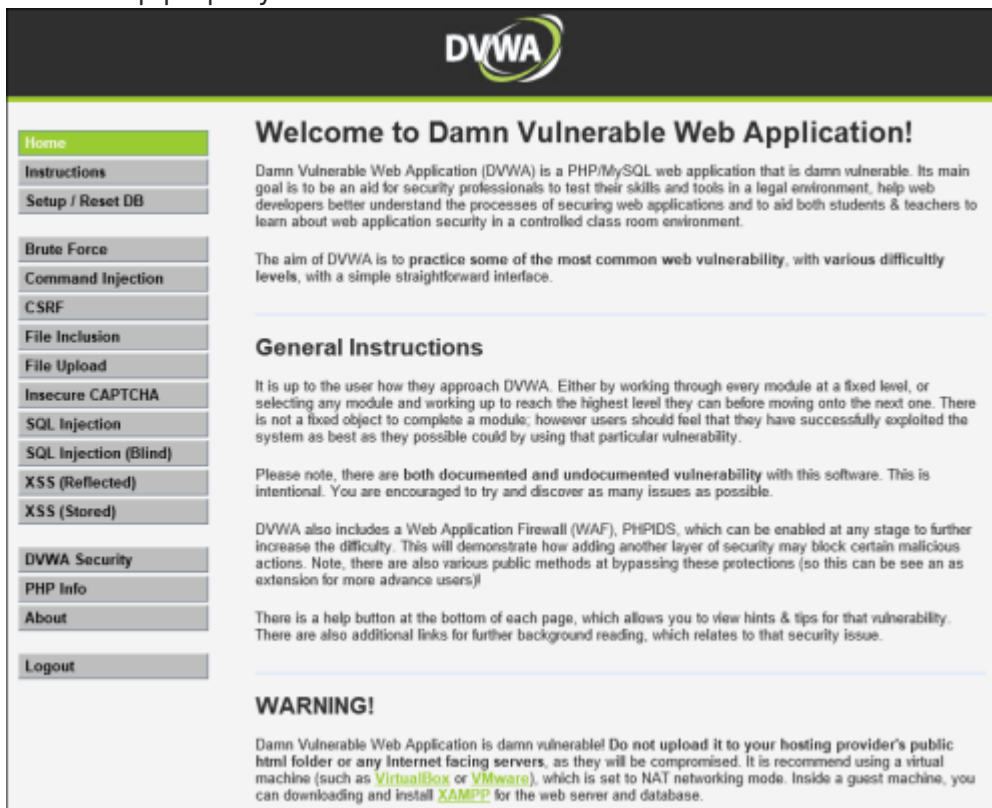


4. Once at the login page use the following login information to test the application.
- **Username** - admin
 - **Password** - password



The image shows the login page of the Damn Vulnerable Web Application (DVWA). It features the DVWA logo at the top. Below the logo, there are two input fields: 'Username' with the text 'admin' and 'Password' with masked characters. A 'Login' button is positioned below the password field.

This will bring you to the home page of the DVWA page. This means that the application has been setup properly.



The image shows the home page of the Damn Vulnerable Web Application (DVWA). It features a sidebar with a menu of options: Home, Instructions, Setup / Reset DB, Brute Force, Command Injection, CSRF, File Inclusion, File Upload, Insecure CAPTCHA, SQL Injection, SQL Injection (Blind), XSS (Reflected), XSS (Stored), DVWA Security, PHP Info, About, and Logout. The main content area has a header 'Welcome to Damn Vulnerable Web Application!' followed by a paragraph about DVWA's purpose. Below this is a section titled 'General Instructions' with two paragraphs of text. At the bottom, there is a 'WARNING!' section with a paragraph of text.

5. Click **Logout**.



Summary:

In this exercise, the Barracuda WAF appliance and the DVWA services were configured. The WAF was configured to connect to the DVWA, and then the DVWA application configuration was completed. This completed the necessary steps to allow for an end to end setup allowing for simulated attacks in

the next exercise.

Exercise 3: Simulate Attacks and Secure the Environment using the WAF

In this exercise, attacks will be simulated against a website using the DVWA application. Using the tools of the WAF, fixes will be applied to avoid these attacks in the future.

Task 1: Command Injection Attack

1. Open a new tab on your local web browser and navigate to the public IP address of the ELB. The example here is at <http://BarracudaWAF-ELB-1474027757.us-east-1.elb.amazonaws.com/DVWA> (DVWA is case sensitive). This will load the DVWA application as published via the Barracuda Web Application Firewall.

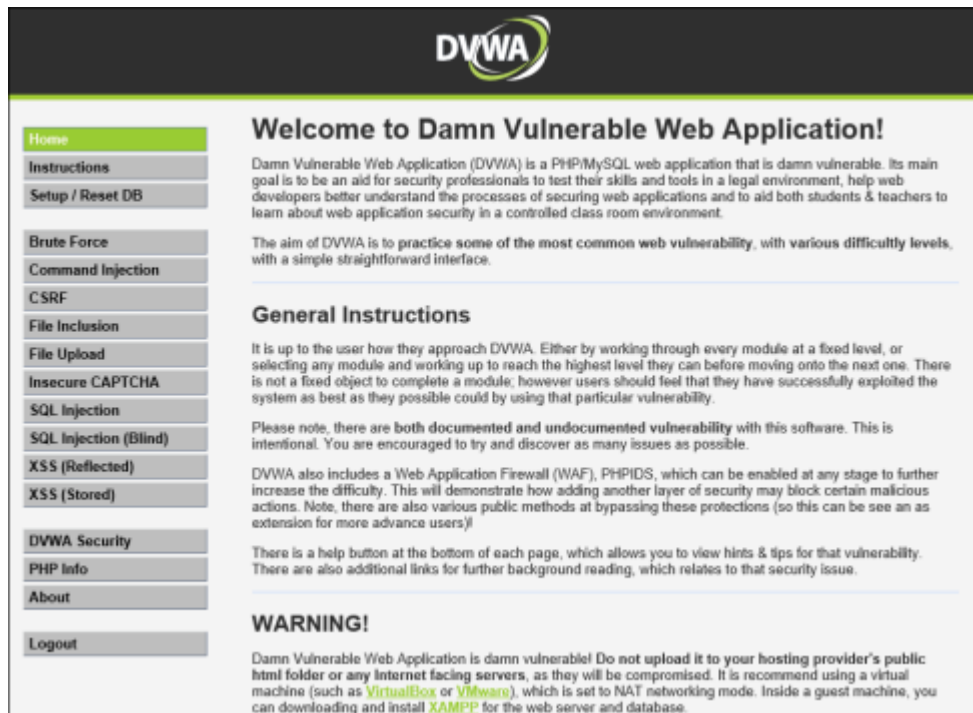
If the address to the ELB is entered into the browser, then simply click the DVWA folder to load the application.

2. The login page of the DVWA website will appear. Use these credentials:
 - **Username** - admin
 - **Password** - password

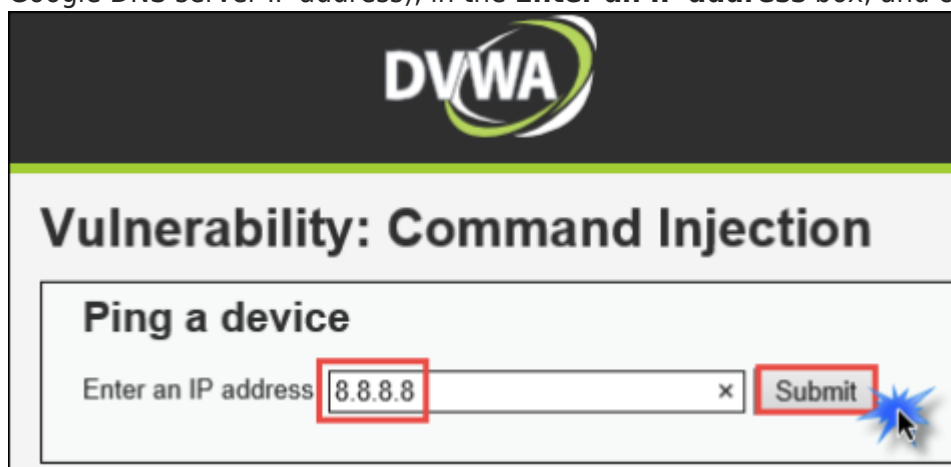


The screenshot shows the DVWA login page. At the top is the DVWA logo. Below it are two input fields: 'Username' with the text 'admin' and 'Password' with masked characters. A 'Login' button is at the bottom right of the form.

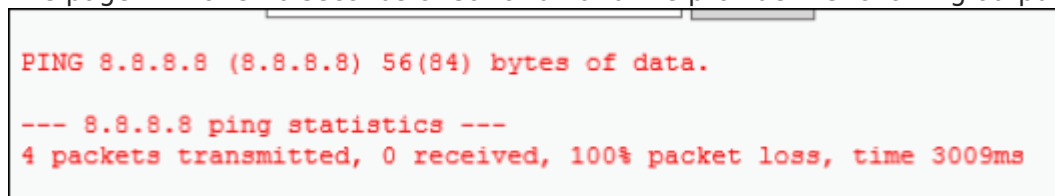
3. The home page for DVWA will appear in the browser window.



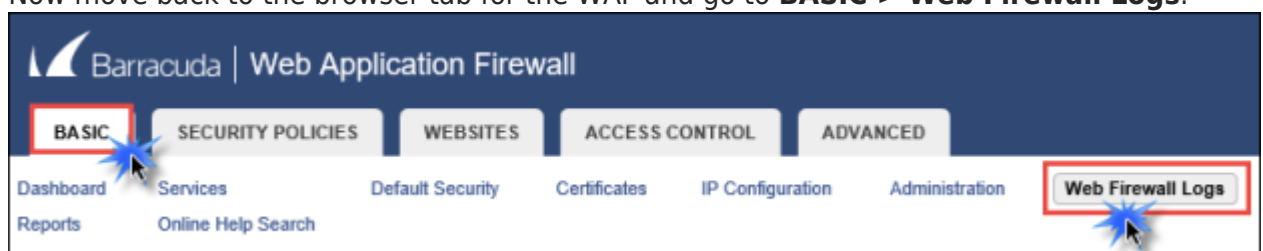
4. Once on the home page click on the **Command Injection** link. Next, type 8.8.8.8 (this is the Google DNS server IP address), in the **Enter an IP address** box, and click **Submit**.



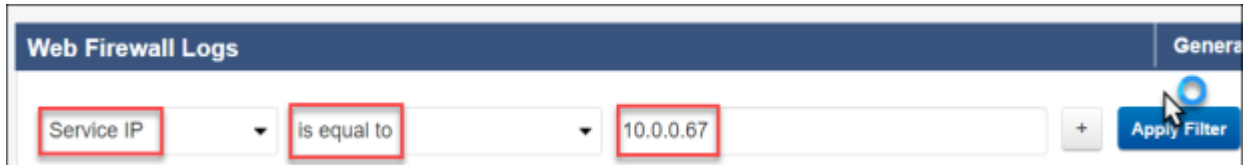
The page will take 10 seconds or so to run and the provide the following output.



5. Now move back to the browser tab for the WAF and go to **BASIC > Web Firewall Logs**.



6. On the **Web Firewall Logs** page, update the filter with the following details, and then click **Apply Filter**.
- **Service IP**
 - **is equal to**
 - IP address of the WAF

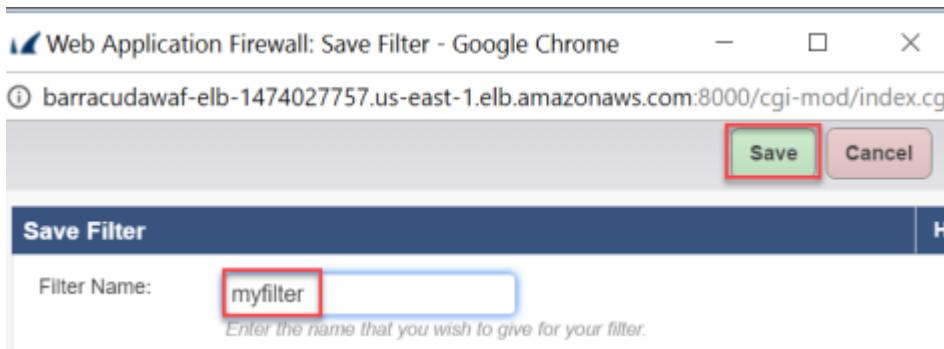


The screenshot shows the 'Web Firewall Logs' page with a filter configuration. The 'Service IP' dropdown is selected, the operator is 'is equal to', and the value is '10.0.0.67'. The 'Apply Filter' button is highlighted with a red circle and a mouse cursor.

7. Notice how the WAF has alerted at the attack.
 Highlighting the red arrow will show the severity alert.

Time	Event Details	Client Details	Attack Details	Actions
↑ LOGGED	URL: /DVWA/vulnerabilities/exe			
Severity: ALERT	Service IP:Port: 10.0.0.67:80	Client IP: 10.0.0.217	Attack Name: Python PHP Attack in URL	Fix Details
ID: 15aa6cd28fd-f9ecddc6	Service Name: dvwa	Country: ? Z1	Attack Detail: type="python-php-attacks-medium security-policy"	
	Protocol: HTTP	Method: POST	Rule: security-policy	
↑ LOGGED	URL: /DVWA/vulnerabilities/exe			
Time: 19:25:47.645	Service IP:Port: 10.0.0.67:80	Client IP: 10.0.0.217	Attack Name: Cookie Tampered	Fix Details
Date: 2017-03-06	Service Name: dvwa	Country: ? Z1	Attack Detail: Cookie="currentPage" Reason="global"	
ID: 15aa6cd28fd-f9ecddc6	Protocol: HTTP	Method: POST	Rule: global	
↑ LOGGED	URL: /DVWA/vulnerabilities/exe			
Time: 19:25:47.645	Service IP:Port: 10.0.0.67:80	Client IP: 10.0.0.217	Attack Name: Cookie Tampered	Fix Details
Date: 2017-03-06	Service Name: dvwa	Country: ? Z1	Attack Detail: Cookie="PHPSESSID" Reason="global"	
ID: 15aa6cd28fd-f9ecddc6	Protocol: HTTP	Method: POST	Rule: global	
↑ LOGGED	URL: /DVWA/vulnerabilities/exe			
Time: 19:06:18.407	Service IP:Port: 10.0.0.67:80	Client IP: 10.0.0.217	Attack Name: OS Command Injection in URL	Fix Details
Date: 2017-03-06	Service Name: dvwa	Country: ? Z1	Attack Detail: type="os-command-injection" path="security-policy"	
ID: 15aa6bb51a7-f9ecddc6	Protocol: HTTP	Method: POST	Rule: security-policy	

8. Click **Save Filter**, this will open a new window. Type **myfilter** into the **Filter Name** box, and then click **Save**.

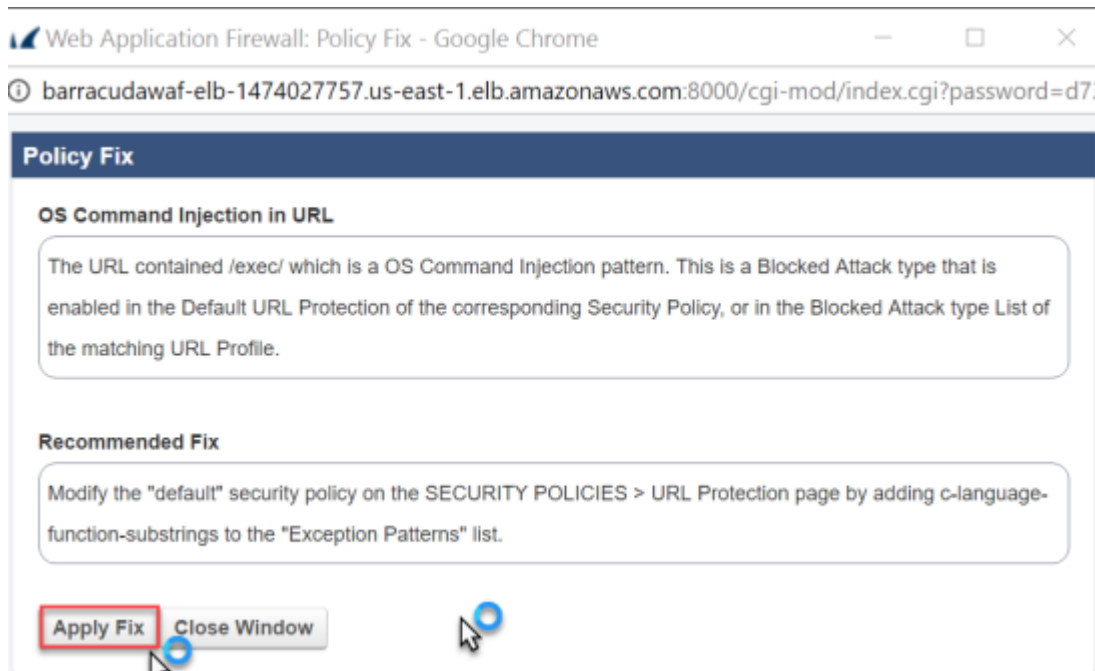


The screenshot shows the 'Web Application Firewall: Save Filter - Google Chrome' window. The URL is 'barracudawaf-elb-1474027757.us-east-1.elb.amazonaws.com:8000/cgi-mod/index.cg'. The 'Save Filter' dialog box is open, showing a 'Filter Name' field with 'myfilter' entered. The 'Save' button is highlighted with a red box.

9. Find the last logged with the attack name **OS Command Injection in URL**, and click **Fix**.

Time	Event Details	Client Details	Attack Details	Actions
↑ LOGGED	URL: /DVWA/vulnerabilities/exe			
Time: 19:06:18.407	Service IP:Port: 10.0.0.67:80	Client IP: 10.0.0.217	Attack Name: OS Command Injection in URL	Fix Details
Date: 2017-03-06	Service Name: dvwa	Country: ? Z1	Attack Detail: type="os-command-injection" path="security-policy"	
ID: 15aa6bb51a7-f9ecddc6	Protocol: HTTP	Method: POST	Rule: security-policy	

10. This will open a **Policy Fix** window. Read the details and then click **Apply Fix**.



The window will update showing that the policy has been updated.

11. Click **Close Window**.



12. Move back to the DVWA application and again launch the command injection attack by entering 8.8.8.8 in the **Ping a Device** tool.
13. Once this is completed move back to the WAF tab and click **Apply Filter**. Notice that you no longer see the Attack Name **OS Command Injection in URL**, in the logs.
14. Go to **Basic > Dashboard**.



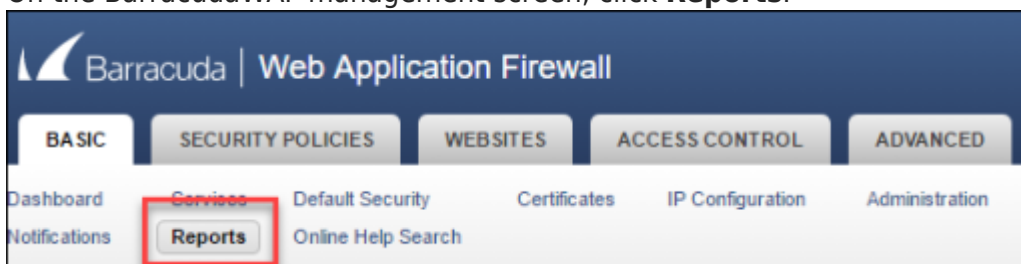
15. Once at the **Dashboard**, scroll down to the **Attacks** graphs. Change the time to **Last Hour**. It should then resemble the following showing attacks that you have made against the site.
- You may have to change the time from **Last Day** to **Last Hour** to see the results.



16. Move back to the DVWA application in your browser. Click through some of the other attacks. Once this is completed move on to the next task.

Task 2: Using Reporting

1. On the BarracudaWAF management screen, click **Reports**.



2. In **Report Options** section, change the **Time Frame** to **Today**.

Report Options

Time Frame

Today

3. Scroll down to the **Security** section, select the checkbox next to **Attacks by Category**, and then click **Show Report**.

Security

☒ Attacks by Category

Show Report

4. The report window will load showing the different attacks. Take the time to review the report.



5. In the drill down section, click on the different areas to better understand the information behind the report. Select **Clients** or **Time**.



6. Close the report by hitting the **X** at the top of the window.
7. Locate the **Top Attacked URLs** in the **Security** section, select the checkbox, and then click **Show Report**.

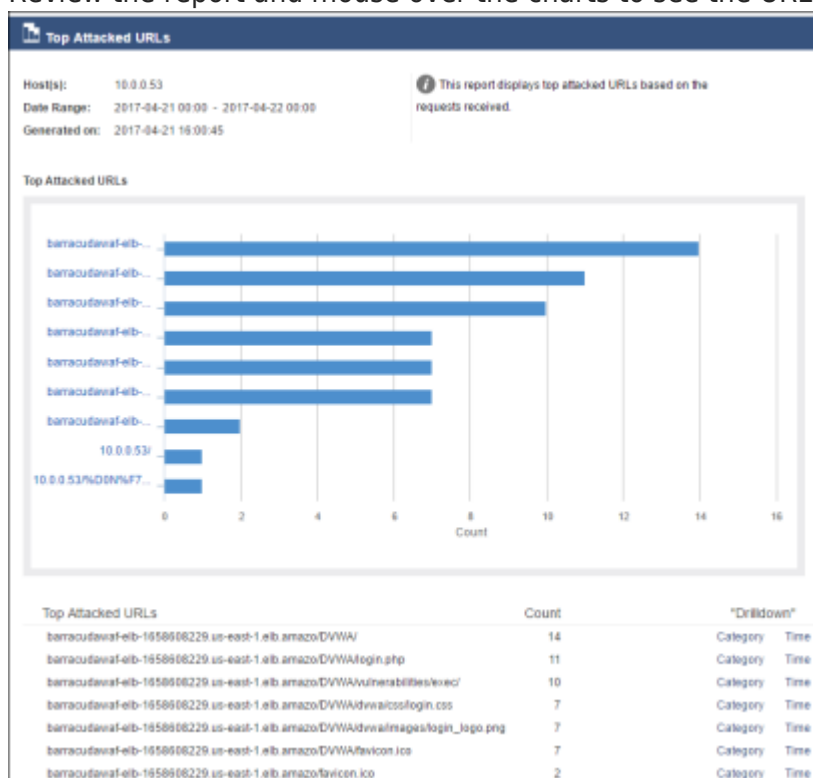
Security

☐ Attacks by Category
☐ Attacks By Services
☐ Attack by Hour
☐ Attack by Day
☐ Top Attacking Clients
☐ Top Attacked Domains
☒ **Top Attacked URLs**

[Show Report](#)
[Show Report](#)
[Show Report](#)
[Show Report](#)
[Show Report](#)
[Show Report](#)

[Show Report](#)

8. Review the report and mouse over the charts to see the URLs.



Figures

1. worddav8ff9fb17da705b0ef2a20c131f8e9f19.png
2. worddavfc437f774a01573bedf0f2893e11e4d5.png
3. worddavef956a67c35bf222190858f39cdc7c99.png
4. worddavf3e0620c66c3b3404f1db222a1b0ae8a.png
5. worddavc3882903a899cd3ad4695a5a8a9418d7.png
6. worddav0ee9b48178251895c53a8b3ba32bcc7.png
7. worddavc6973ffb21d925fc33817897ed135680.png
8. worddav38490ab292a8ecf4c9488642034df800.png
9. worddav74a33011f21a721717c3b1a5549b79ab.png
10. worddav466ee782638a0e11d4245e95e07f0267.png
11. worddave0dc9f82b83eb199d8c637f8a8907da4.png
12. worddav56be5cfe1ca9af6ca41cd10ca73ec16b.png
13. worddav7b733c09535ad20966652462f3dea4c4.png
14. worddav53be39c2c01954dc36b34adc64d991dd.png
15. worddavid5e033d00901e2466facf74cb0da7845.png
16. worddav17eae58f122d14e789d9177da436b119.png
17. worddavid3e4ae226e330d5510be22682e54353c.png
18. worddava72156f7881ad224db891558193b4958.png
19. worddav9c62d25dcfe1006122e4e6d4127d0ee0.png
20. worddavfa5b3001366ba64a43e47959f15b440a.png
21. worddavfabb225af2887635303226347311b06f.png
22. worddavfda046b87d9435dd1d85a2178973487b.png
23. worddav86cfaa03094bd67249a73727daa2a66a.png
24. worddav4a4166fe965f49c8582ba1b3d0a2b053.png
25. worddav345ae2557ce23d9d82b548b42acc7e67.png
26. worddave1115815535e08269ca9562e00d17287.png
27. worddav4c94ba01377cc2bb0db8fa84470e821b.png
28. worddavf33bd941cb6dd8c2b3610fcc17ab9fef.png
29. worddav115bf6fbce5b3ffc6b45210ab945b993.png
30. worddavc8a73c0a6dc2ecc61871dd8e05d8094c.png
31. worddav0e79554be9acac8d0ab0137c92109d2b.png
32. worddavn574a53d521fcd02c5015370cbe52ba0.png
33. worddav1f562f6082f27918d96a1d1f45eb7314.png
34. worddav35ea34227343c70c5b22625024a4731b.png
35. worddav1048f46a178d51364417112dba4e669d.png
36. worddav4a0e31f4a5866d565a8eb87a5745b9cc.png
37. worddav89f42efb2cae6be3a263c6b51aea462c.png
38. worddav4392991937196367767da9f49a443bff.png
39. worddav8df663f652f3bfeca7b570c2f986f700.png
40. worddavbc637f5f6a985a19cc63781930934b0b.png
41. worddav9b90af958b67e203396d3444c5aa4fff.png
42. worddav7730b0256018f225a6019dc8605ba55f.png
43. worddav01fa4165b21322ddd42b96a5c2fc753a.png
44. worddav4281c00b7838301a78bfd3678157e36.png

45. worddav82676a9ba0f69f767432784d47dc1045.png
46. worddav094d8acd10cb9b8b15e7984f0ee4c041.png
47. worddav98d03457add444c37a8ac95c98d13bbf.png
48. worddavf6d26255034c21c973d34e9baf6b1354.png
49. worddav32673b37633831396fddd414dc952297.png
50. worddavaf0bb9d34375cec271fc430c365fc1ff.png
51. worddavn83a866e248926edb54b1437a48b2ecb.png
52. worddavcadb6f8f2fd8c41a0c23670638c25304.png
53. worddave0545191485f739a556fea4796b2177f.png
54. worddav0898892df695aa5fcf36cddc7aedd90c.png
55. worddav6fe33f1c26e691b59c4508d1a8da1f2e.png
56. worddavn46c0a86d50b64cba4c6be5b876535b4.png
57. worddavn0af9570dfcd46596a813cce5c0fc7cf.png
58. worddav642ca406a92acdb346cac9a16a7f74b5.png
59. worddav98f426dc282320b7fabee4a1ea8da8e.png
60. worddav89be6be278341951bd0791494b7ff5fe.png
61. worddav05e68e3b0dd60999efe8dd8251687017.png
62. worddavaa0caddef66d8abe0ae54b85df7b48ad.png
63. worddav419bdf9043d5439fa5a21744120aa244.png
64. worddav885b786336765591e4465fbbd7fd91bc.png
65. worddav08a6886573bd374304417b01fbc102e3.png
66. worddav4913b582a649bacae834e5e086f9e803.png
67. worddav249294e44f173b816f8861878a4e3fcd.png
68. worddav6c5ac430913a6943276fb59a93225409.png
69. worddav22e9e2eb906f90274d538cac9fb5c038.png
70. worddav4824df566c365f0a584399595df772e3.png
71. worddavn5dcab64c5e6be0916622eefc27886fc.png
72. worddav320a041b0c3f6e7977a598e46e90901b.png
73. worddavfd35f03d3d1af7ff873d57a95db9a0e6.png
74. worddava5acfe5b2d2476e45470525cd25bcb79.png
75. worddav06665c890f0295af9f3d707fe2c6e26d.png
76. worddav38260db66bc34a5a461ac93dd377e7b1.png
77. worddav02648564b5f306943cdf8170da8892b4.png
78. worddavfd4f36a2306f13e48bcb1d455910dd31.png
79. worddav0d32601525cfd1556f10cf2ddcd1d296.png
80. worddav2f329f45a10cb4d2eb37431565d077d1.png
81. worddav3d026e7bd5b2a2eff2542c6e24546069.png
82. worddav596254fe45cd52f0c7af1ea3f87ac7ab.png
83. worddav55bfab4ad0fad9ee83bf1ca1f4a31236.png
84. worddavn7fc9dd81930eac922a2c2c6e2f07961.png
85. worddav32ffefc46f79badba2c563f19f523b69.png
86. worddavn11cdc19d121485728690174ad4c995e.png
87. worddavnbb197e3763a53d0f93fc66dcf28e5b1.png
88. worddavnbb6d6f8611b9bf79b92099486ce8f23c.png
89. worddav1650ad5358e6ced0ab2893cf6c81d454.png
90. worddav794fdceff6675b7800424d37c1ab8cdf.png

91. worddav49dfcd05d8d2830c87de165113c2abcb.png
92. worddav0f9e84fd32993e5c93b04b6c806d5319.png
93. worddavea5dff0af68581ab9634877d9ea475e8.png
94. worddav91253f722774901ecfa23ec001c58b3c.png
95. worddav0392b84bb5f701533713ad1aab7799a4.png
96. worddav42908e8e7d181f14eed7cd5c9f69f5b7.png
97. worddav3be06025b5514404be4af4e1ecb3e66d.png
98. worddav3822110428382fd73ed91c7bf807ec1f.png
99. worddavic9202fd38692192ed4c899ec80da6e05.png
100. worddave754f06d15b095549f11bf81495a1a58.png
101. worddavd0501c5d3bc56d4fd41c47956f1c2de3.png
102. worddav12437c9e962b3caec91aa8a0be9189b9.png
103. worddav4e5e7652bda57232826d4dce40ffbc68.png
104. worddavefea08350a1456428358916e1cfac607.png
105. worddav305c54e6b6181349ff7062c3ccede8ec.png
106. worddavd338e13fc1aa154ad8c6c10f7a924500.png
107. worddav91359f09ff26f5da9976f83b0c81f147.png
108. worddavff7204555747ef5343b535d579ad2fe5.png
109. worddav4544c714e6ed6b34446e733ae26d40b4.png
110. worddava57cdb947303c8fad7e8d0a36c3e640a.png
111. worddav602857c687ba53880235e957fa84a42f.png

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.