

10.5 Deploy FortiGate in AWS

Learning Objectives

- Create a VPC, public and private subnet, internet gateway, route tables
- Create a FortiGate firewall in AWS through Marketplace
- Identify FortiGate subnets in AWS

Scenario: In this lab, we'll learn how to deploy FortiGate in AWS.

AWS Configuration

1. Create a VPC.

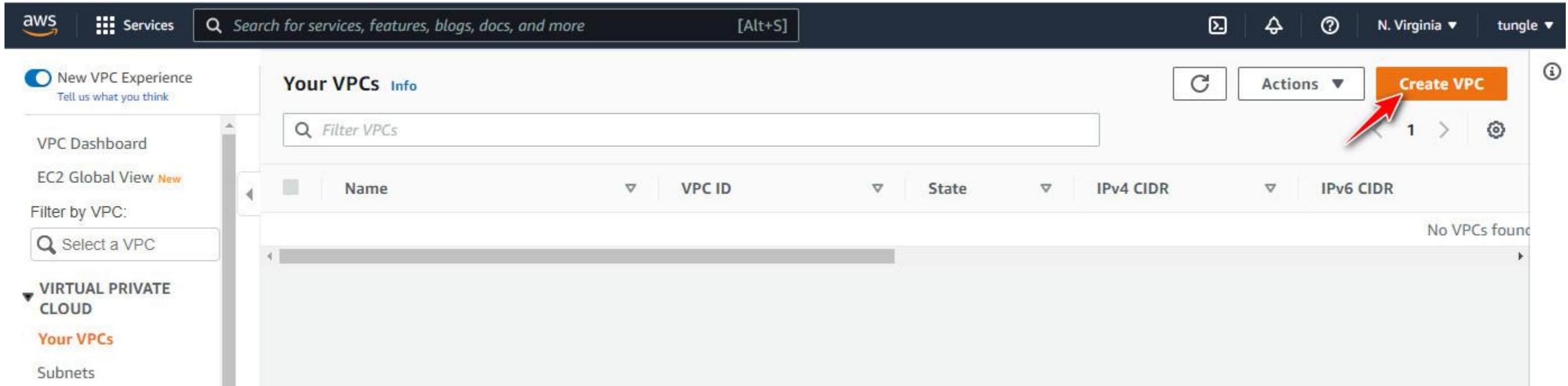


Figure 10.107: Create a VPC

A screenshot of the 'Create VPC' configuration page. It starts with a brief description: 'A VPC is an isolated portion of the AWS Cloud populated by AWS objects, such as Amazon EC2 instances.' Below this, there's a 'VPC settings' section. Under 'Resources to create', the 'VPC only' radio button is selected. There's a 'Name tag - optional' field containing 'AWS-VPC'. Under 'IPv4 CIDR block', the 'IPv4 CIDR manual input' radio button is selected, and the 'IPv4 CIDR' field contains '10.0.0.0/16'. Under 'IPv6 CIDR block', the 'No IPv6 CIDR block' radio button is selected. At the bottom, there's a 'Tenancy' dropdown set to 'Default'. A red arrow points to the 'Create VPC' button at the bottom right of the form.

Figure 10.108: Create a VPC named “AWS-VPC”

2. Create a subnet.

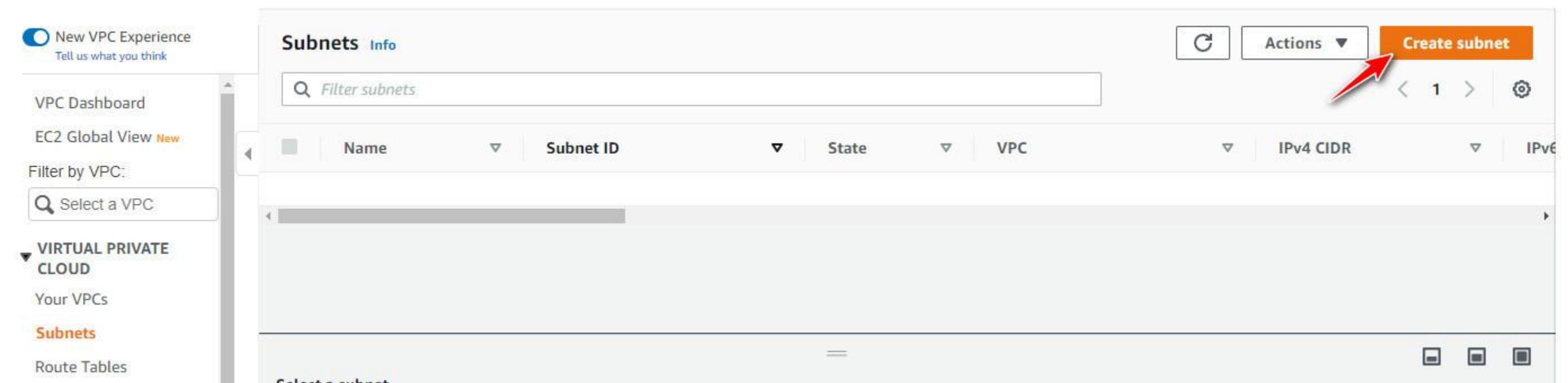


Figure 10.109: Create a subnet

VPC > Subnets > Create subnet

Create subnet Info

VPC

VPC ID
Create subnets in this VPC:
vpc-060a1e2007366fbf4 (AWS-VPC)

Associated VPC CIDRs
IPv4 CIDRs
10.0.0.0/16

Subnet settings
Specify the CIDR blocks and Availability Zone for the subnet.

Subnet 1 of 1

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

The name can be up to 256 characters long.

Availability Zone Info
Choose the zone in which your subnet will reside, or let Amazon choose one for you.
No preference

IPv4 CIDR block Info
Q 10.0.0.0/24

Figure 10.110: Create a public subnet under AWS-VPC

VPC > Subnets > Create subnet

Create subnet Info

VPC

VPC ID
Create subnets in this VPC:
vpc-060a1e2007366fbf4 (AWS-VPC)

Associated VPC CIDRs
IPv4 CIDRs
10.0.0.0/16

Subnet settings
Specify the CIDR blocks and Availability Zone for the subnet.

Subnet 1 of 1

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

The name can be up to 256 characters long.

Availability Zone Info
Choose the zone in which your subnet will reside, or let Amazon choose one for you.
No preference

IPv4 CIDR block Info
Q 10.0.1.0/24

Figure 10.111: Create a private subnet under AWS-VPC

3. Create an internet gateway.

New VPC Experience
Tell us what you think

Internet gateways Info

C Actions ▾ Create internet gateway

Filter internet gateways

Name	Internet gateway ID	State	VPC ID	Owner
No internet gateways found in this Region				

Select an internet gateway above

VIRTUAL PRIVATE CLOUD

- Your VPCs
- Subnets
- Route Tables
- Internet Gateways

Figure 10.112: Create an internet gateway

VPC > Internet gateways > Create internet gateway

Create internet gateway Info

An internet gateway is a virtual router that connects a VPC to the internet. To create a new internet gateway specify the name for the gateway below.

Internet gateway settings

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

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

Key	Value - optional
Q Name	Q AWS-IGW

Add new tag
You can add 49 more tags.

Create internet gateway

Figure 10.113: Create an internet gateway

Internet gateways (1/1) Info														
Actions ▾ Create internet gateway														
View details Attach to VPC Detach from VPC Manage tags Delete internet gateway														
<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>Name</th> <th>Internet gateway ID</th> <th>State</th> <th>VPC ID</th> </tr> </thead> <tbody> <tr> <td>AWS-IGW</td> <td>igw-0b81c8d93b9e4ea9f</td> <td>Detached</td> <td>-</td> </tr> </tbody> </table> <p style="margin-top: 10px;">igw-0b81c8d93b9e4ea9f / AWS-IGW</p> <p style="margin-top: 10px;"> Details Tags </p>	Name	Internet gateway ID	State	VPC ID	AWS-IGW	igw-0b81c8d93b9e4ea9f	Detached	-						
Name	Internet gateway ID	State	VPC ID											
AWS-IGW	igw-0b81c8d93b9e4ea9f	Detached	-											

Figure 10.114: Attach an internet gateway to VPC

VPC > Internet gateways > Attach to VPC (igw-0b81c8d93b9e4ea9f) [Info](#)

Attach to VPC (igw-0b81c8d93b9e4ea9f)

VPC

Attach an internet gateway to a VPC to enable the VPC to communicate with the internet. Specify the VPC to attach below.

Available VPCs

Attach the internet gateway to this VPC.

vpc-060a1e2007366fbf4

AWS Command Line Interface command

Cancel [Attach internet gateway](#)

Figure 10.115: Attach an internet gateway to VPC

4. Create a new Public RouteBy default, name of the “built-in route” is “-”. Rename it to Private Route.

Route tables (1/1) Info																		
Actions ▾ Create route table																		
View details Edit route table Delete route table																		
<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>Name</th> <th>Route table ID</th> <th>Explicit subnet associat...</th> <th>Edge associations</th> <th>Main</th> <th>VPC</th> </tr> </thead> <tbody> <tr> <td>Private Route</td> <td>rtb-087e78e7f2a174a94</td> <td>-</td> <td>-</td> <td>Yes</td> <td>vpc-060a1e2007366fbf4</td> </tr> </tbody> </table> <p style="margin-top: 10px;">rtb-087e78e7f2a174a94 / Private Route</p>	Name	Route table ID	Explicit subnet associat...	Edge associations	Main	VPC	Private Route	rtb-087e78e7f2a174a94	-	-	Yes	vpc-060a1e2007366fbf4						
Name	Route table ID	Explicit subnet associat...	Edge associations	Main	VPC													
Private Route	rtb-087e78e7f2a174a94	-	-	Yes	vpc-060a1e2007366fbf4													

Figure 10.116: Edit private route

Go to **Route tables > create route table**.

VPC > Route tables > Create route table

Create route table [Info](#)

A route table specifies how packets are forwarded between the subnets within your VPC, the internet, and your VPN connection.

Route table settings

Name - optional

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

Public Route

VPC

The VPC to use for this route table.

vpc-060a1e2007366fbf4 (AWS-VPC)

Tags

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

Key Value - optional

Name Public Route

Add new tag

You can add 49 more tags.

Cancel [Create route table](#)

Figure 10.117: Create a public route

The screenshot shows the AWS VPC Route Tables page. On the left, there's a navigation sidebar with options like VPC Dashboard, EC2 Global View, Filter by VPC, and a list of VPCs. The main area displays 'Route tables (1/2) Info' with a table:

Name	Route table ID	Explicit subnet associat...	Edge associations	Main	VPC
<input checked="" type="checkbox"/> Public Route	rtb-0121768a9204bc14a	-	-	No	vpc-060a1e2007366fbf4 A
<input type="checkbox"/> Private Route	rtb-087e78e7f2a174a94	-	-	Yes	vpc-060a1e2007366fbf4 A

Below the table, it says 'rtb-0121768a9204bc14a / Public Route'. There are tabs for Details, Routes (which is selected), Subnet associations, Edge associations, Route propagation, and Tags. Under the Routes tab, there's another table:

Destination	Target	Status	Propagated
10.0.0.0/16	local	<input checked="" type="checkbox"/> Active	No

With an 'Edit routes' button in the top right.

Figure 10.118: Edit routes on Public Route

The screenshot shows the 'Edit routes' dialog box. At the top, the path is VPC > Route tables > rtb-0121768a9204bc14a > Edit routes. The title is 'Edit routes'. Below it is a table:

Destination	Target	Status	Propagated
10.0.0.0/16	local	<input checked="" type="checkbox"/> Active	No
0.0.0.0/0	igw-	-	No

A dropdown menu shows 'igw-0b81c8d93b9e4ea9f (AWS-IGW)'. Buttons at the bottom include 'Add route', 'Cancel', 'Preview', and 'Save changes'.

Figure 10.119: Create a new default route to the internet gateway

The screenshot shows the 'rtb-0121768a9204bc14a / Public Route' details page. The path is VPC > Route tables > rtb-0121768a9204bc14a. It includes a message about using the Reachability Analyzer and a 'Run Reachability Analyzer' button. The 'Details' tab is selected, showing:

Route table ID: rtb-0121768a9204bc14a	Main: No	Explicit subnet associations: -	Edge associations: -
VPC: vpc-060a1e2007366fbf4 AWS-VPC	Owner ID: 590508865535		

Below the details are tabs for Routes, Subnet associations (selected), Edge associations, Route propagation, and Tags. Under Subnet associations, it says 'Explicit subnet associations (0)' with an 'Edit subnet associations' button.

Figure 10.120: Associate Public Subnet to Public Route

Edit subnet associations

Change which subnets are associated with this route table.

Available subnets (1/2)

Available subnets (1/2)					
<input type="text"/> Filter subnet associations					
Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID	
<input checked="" type="checkbox"/> Public Subnet	subnet-06ed7507849737ecf	10.0.0.0/24	-	Main (rtb-087e78e7f2a174a94 / Private Route)	
<input type="checkbox"/> Private Subnet	subnet-0936fd8c6f4984efe	10.0.1.0/24	-	Main (rtb-087e78e7f2a174a94 / Private Route)	

Selected subnets

subnet-06ed7507849737ecf / Public Subnet

[Cancel](#) [Save associations](#)

Figure 10.121: Associate Public Subnet to Public Route

5. Create Key Pair. Go to EC2 – Key Pairs > Create Key Pair.

EC2 > Key pairs > Create key pair

Create key pair [Info](#)

Key pair
A key pair, consisting of a private key and a public key, is a set of security credentials that you use to prove your identity when connecting to an instance.

Name The name can include up to 255 ASCII characters. It can't include leading or trailing spaces.

Key pair type [Info](#)
 RSA
 ED25519

Private key file format
 .pem
For use with OpenSSH
 .ppk
For use with PuTTY

Tags (Optional)
No tags associated with the resource.
[Add tag](#)
You can add up to 50 more tags.

[Cancel](#) [Create key pair](#)

Figure 10.122: Create a key pair

6. Create Instances. Go to EC2 – Instances > Launch instances.

New EC2 Experience [Tell us what you think](#)

EC2 Dashboard
EC2 Global View
Events
Tags
Limits
Instances
Instances [New](#)
Instance Types

Instances [Info](#)

[Launch instances](#)

No instances
You do not have any instances in this region
[Launch instances](#)

Figure 10.123: Launch a FortiGate instance

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 1: Choose an Amazon Machine Image (AMI)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. You can select an AMI provided by AWS, our user community, or AWS Marketplace; or you can select one of your own AMIs.

[Search by Systems Manager parameter](#)

Quick Start (0)
My AMIs (0)
AWS Marketplace (44)
Community AMIs (7)

Fortinet FortiGate Next-Generation Firewall
 ★★★★★ (19) | 7.2.0 Previous versions | By Fortinet Inc.
Starting from \$0.36/hr or from \$1,920.00/yr (up to 60% savings) for software + AWS usage fees
Linux/Unix, Other 7.2.0 | 64-bit (x86) Amazon Machine Image (AMI) | Updated: 4/30/22
Fortinet FortiGate allows mitigation of blind spots to improve policy compliance by implementing critical security controls within your AWS environment. FortiGate includes all of the security and networking services common to FortiGate physical appliances.

[Cancel and Exit](#) [Select](#)

Figure 10.124: Select Fortinet FortiGate Next-Generation Firewall

Fortinet FortiGate Next-Generation Firewall

Pricing Details

Instance Type	Software	EC2	Total
t2.small	\$0.36	\$0.023	\$0.383/hr
t3.small	\$0.88	\$0.021	\$0.901/hr
t3.xlarge	\$1.02	\$0.166	\$1.186/hr
c4.large	\$0.88	\$0.10	\$0.98/hr
c4.xlarge	\$1.02	\$0.199	\$1.219/hr
c4.2xlarge	\$2.35	\$0.398	\$2.748/hr
c4.4xlarge	\$3.29	\$0.796	\$4.086/hr
c4.8xlarge	\$4.10	\$1.591	\$5.691/hr
c5.large	\$0.88	\$0.085	\$0.965/hr
c5.xlarge	\$1.02	\$0.17	\$1.19/hr
c5.2xlarge	\$2.35	\$0.34	\$2.69/hr
c5.4xlarge	\$3.29	\$0.68	\$3.97/hr
c5.9xlarge	\$4.10	\$1.53	\$5.63/hr
c5.18xlarge	\$5.16	\$3.06	\$8.22/hr
c5d.large	\$0.88	\$0.096	\$0.976/hr
c5d.xlarge	\$1.02	\$0.192	\$1.212/hr
c5d.2xlarge	\$2.35	\$0.384	\$2.734/hr

Product Details

By Fortinet Inc.

Customer Rating ★★★★★ (19)

Latest Version 7.2.0

Base Operating System Linux/Unix, Other 7.2.0

Delivery Method 64-bit (x86) Amazon Machine Image (AMI)

License Agreement End User License Agreement

On Marketplace Since 11/7/14

Highlights

- FortiGate offers protection from a broad array of threats, with support for all of the security and networking services offered by the FortiOS operating

Cancel **Continue**

Figure 10.125: Accept FortiGate licence

Step 2: Choose an Instance Type

Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications, networking capacity, and give you the flexibility to choose the appropriate mix of resources for your applications. [Learn more](#) about instance types.

Filter by: All instance families ▾ Current generation ▾ Show/Hide Columns

Currently selected: t2.small (- ECUs, 1 vCPUs, 2.5 GHz, -, 2 GiB memory, EBS only)

Note: The vendor recommends using a c6i.xlarge instance (or larger) for the best experience with this product.

	Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)
∅	t2	t2.nano	1	0.5	EBS only
∅	t2	t2.micro <small>Free tier eligible</small>	1	1	EBS only
<input checked="" type="checkbox"/>	t2	t2.small	1	2	EBS only
∅	t2	t2.medium	2	4	EBS only
∅	t2	t2.large	2	8	EBS only

Figure 10.126: Select FortiGate instance type

Step 3: Configure Instance Details

No default VPC found. Select another VPC, or [create a new default VPC](#).

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of lower costs, and more.

Number of instances	<input type="text" value="1"/>	Launch into Auto Scaling Group
Purchasing option	<input type="checkbox"/> Request Spot instances	
Network	vpc-060a1e2007366fbf4 AWS-VPC	<input type="button" value="Create new VPC"/>
Subnet	subnet-06ed7507849737ecf Public Subnet us-eas	<input type="button" value="Create new subnet"/>
Auto-assign Public IP	<input type="button" value="Enable"/>	
Hostname type	<input type="button" value="Use subnet setting (IP name)"/>	
DNS Hostname	<input checked="" type="checkbox"/> Enable IP name IPv4 (A record) DNS requests <input checked="" type="checkbox"/> Enable resource-based IPv4 (A record) DNS requests <input type="checkbox"/> Enable resource-based IPv6 (AAAA record) DNS requests	

Figure 10.127: Select Network is “AWS-VPC”, Subnet is “Public Subnet” and Auto-assign Public IP is “Enable”

Step 4: Add Storage

Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. [Learn more](#) about storage options in Amazon EC2.

Volume Type <i>i</i>	Device <i>i</i>	Snapshot <i>i</i>	Size (GiB) <i>i</i>	Volume Type <i>i</i>	IOPS <i>i</i>	Throughput (MB/s) <i>i</i>
Root	/dev/sda1	snap-0ba9f2da5ecf96965	2	General Purpose SSD (gp2)	100 / 3000	N/A
EBS	/dev/sdb	Search (case-insensit	30	General Purpose SSD (gp2)	100 / 3000	N/A
Add New Volume						

Figure 10.128: Leave the Add storage as the default

Step 5: Add Tags

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver.

A copy of a tag can be applied to volumes, instances or both.

Tags will be applied to all instances and volumes. [Learn more](#) about tagging your Amazon EC2 resources.

Key <small>(128 characters maximum)</small>	Value <small>(256 characters maximum)</small>	Instances <i>i</i>
Name	FG	<input checked="" type="checkbox"/>

Figure 10.129: Assign Tag with Key is Name and Value is FG

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 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 list of security groups.

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

Security group name: FortiGate Security Group

Description: FortiGate Security Group

Type <i>i</i>	Protocol <i>i</i>	Port Range <i>i</i>	Source <i>i</i>
SSH	TCP	22	Custom 0.0.0.0/0
HTTP	TCP	80	Custom 0.0.0.0/0
HTTPS	TCP	443	Custom 0.0.0.0/0
Custom TCP F	TCP	541	Custom 0.0.0.0/0
Custom TCP F	TCP	3000	Custom 0.0.0.0/0
Custom TCP F	TCP	8080	Custom 0.0.0.0/0
RDP	TCP	3389	Custom 0.0.0.0/0
All ICMP - IPv4	ICMP	0 - 65535	Custom 0.0.0.0/0

Add Rule

Figure 10.130: Change to FortiGate Security Group and add RDP and ICMP to the Security Group

Select an existing key pair or create a new key pair X

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance. Amazon EC2 supports ED25519 and RSA key pair types.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about removing existing key pairs from a public AMI.

Choose an existing key pair
Select a key pair
AWS-Lab | RSA
 I acknowledge that I have access to the corresponding private key file, and that without this file, I won't be able to log into my instance.

Launch Instances

Figure 10.131: Accept key pair and launch instances

The screenshot shows the AWS EC2 Instances page. On the left, there's a sidebar with various navigation options like EC2 Dashboard, EC2 Global View, Events, Tags, Limits, Instances, and Images. The main area displays a table titled 'Instances (1/1)'. The table has columns for Name, Instance ID, Instance state, Instance type, and Status check. One row is selected, showing 'FG' as the name, 'i-0ff098db861c07b53' as the Instance ID, 'Running' as the Instance state, 't2.small' as the Instance type, and 'Initializing' as the Status check. Below the table, a detailed view for 'Instance: i-0ff098db861c07b53 (FG)' is shown with tabs for Details, Security, Networking, Storage, Status checks, Monitoring, and Tags. The Details tab is active, showing Instance summary information including Instance ID, Public IPv4 address (3.239.117.237), Private IP DNS name (ip-10-0-0-22.ec2.internal), and other details.

Figure 10.132: FG instance has been launched successfully

The screenshot shows the AWS Network interfaces page. The sidebar includes options for Reserved Instances, Dedicated Hosts, Scheduled Instances, Capacity Reservations, Images, AMIs, Elastic Block Store, Volumes, Snapshots, Lifecycle Manager, Network & Security, Security Groups, Elastic IPs, Placement Groups, Key Pairs, Network Interfaces, and Load Balancing. The main area shows a table titled 'Network interfaces (1/1)'. A single row is selected, labeled 'FG Public Subnet' with Network interface ID 'eni-03b2e198495d21f54', Subnet ID 'subnet-06ed7507849737ecf', VPC ID 'vpc-060a1e2007366fb4', and Availability Zone 'us-east-1f'. Below the table, a detailed view for 'Network interface: eni-03b2e198495d21f54 (FG Public Subnet)' is displayed with tabs for Details, Flow logs, and Tags. The Details tab is active, showing a message about checking connectivity with Reachability Analyzer and a 'Run Reachability Analyzer' button. It also lists Network interface details such as Name ('FG Public Subnet'), Description ('Primary network interface'), Interface type ('Elastic network interface'), Security groups ('sg-09578bdb48a98e906 (FortiGate Security Group)'), and Availability Zone ('us-east-1f').

Figure 10.133: Change default interface name to FG Public Subnet

7. Add a new private subnet interface.

The screenshot shows the 'Create network interface' wizard. The first step, 'Details', is active. It asks for a descriptive name ('Description - optional') and a subnet ('The subnet in which to create the network interface'). The 'Description' field contains 'FG Private Subnet'. The 'Subnet' dropdown shows two options: 'Public Subnet' (selected) and 'Private Subnet'. The 'Private Subnet' option is highlighted with a red box. Other settings include 'Elastic Fabric Adapter' (disabled) and 'Advanced settings' (collapsed). The URL at the top is 'EC2 > Network interfaces > Create network interface'.

Figure 10.134: Create FG Private Subnet

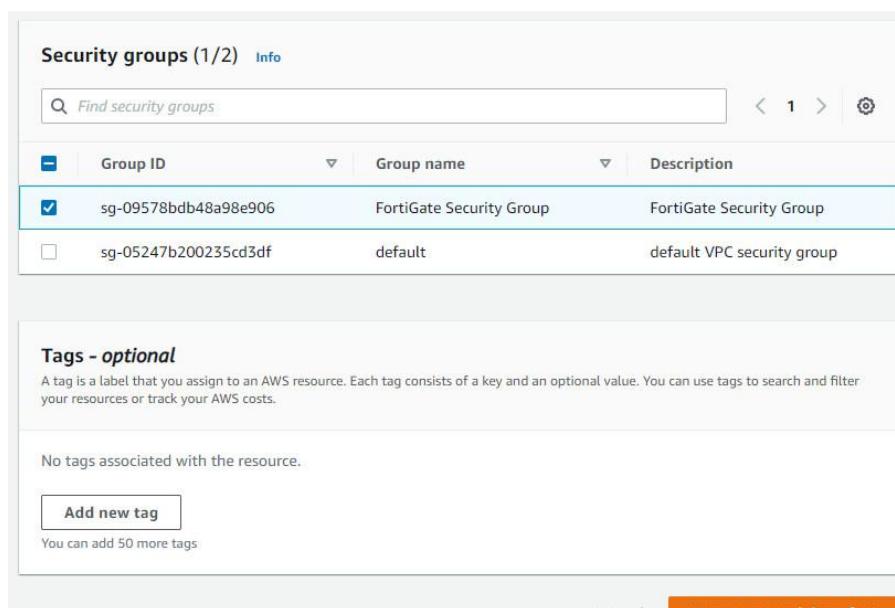


Figure 10.135: Create FG Private Subnet

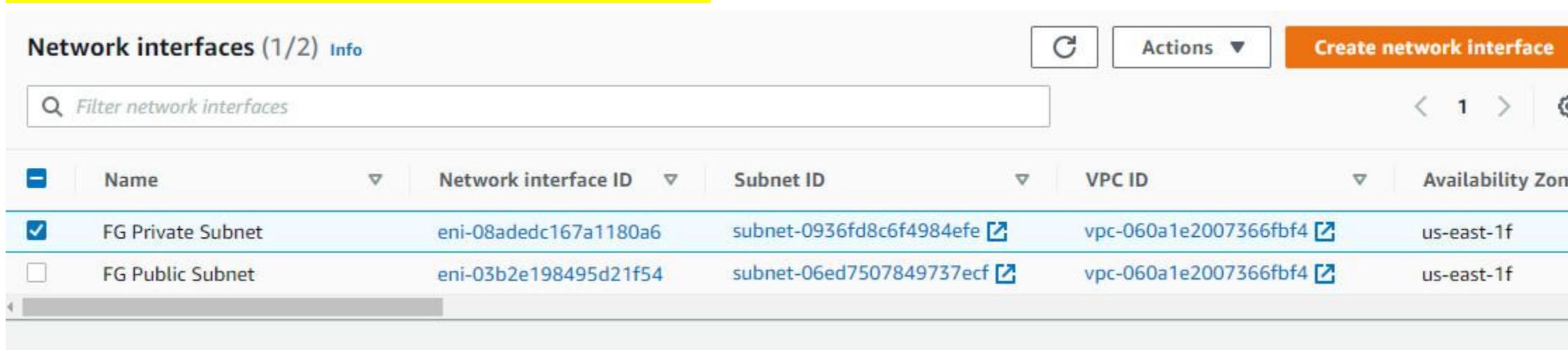


Figure 10.136: Change to FG Private Subnet

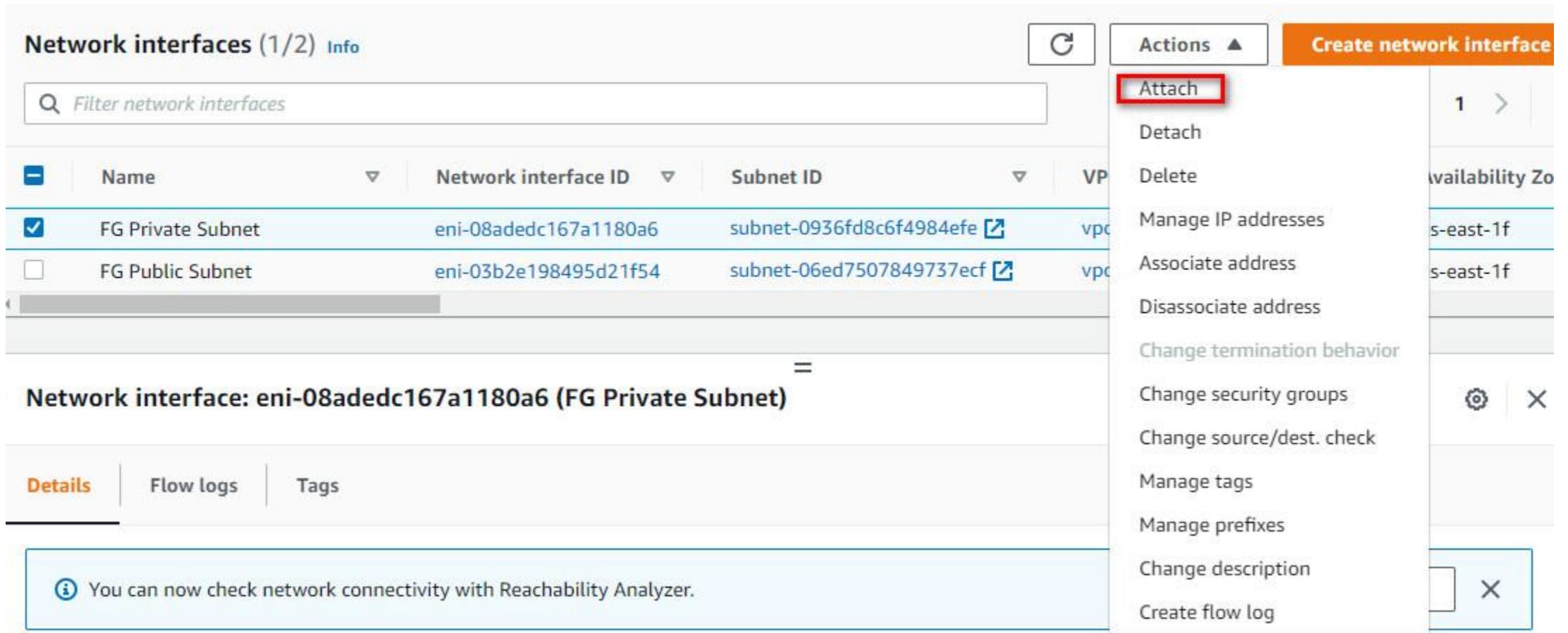


Figure 10.137: Attach the FG Private Subnet to FG

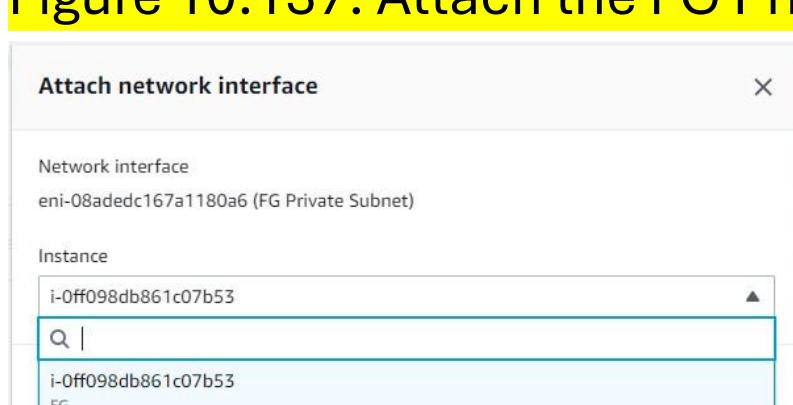


Figure 10.138: Attach the FG Private Subnet to FG

8. Disable Source and Destination check on both FG Private and Public Subnet.

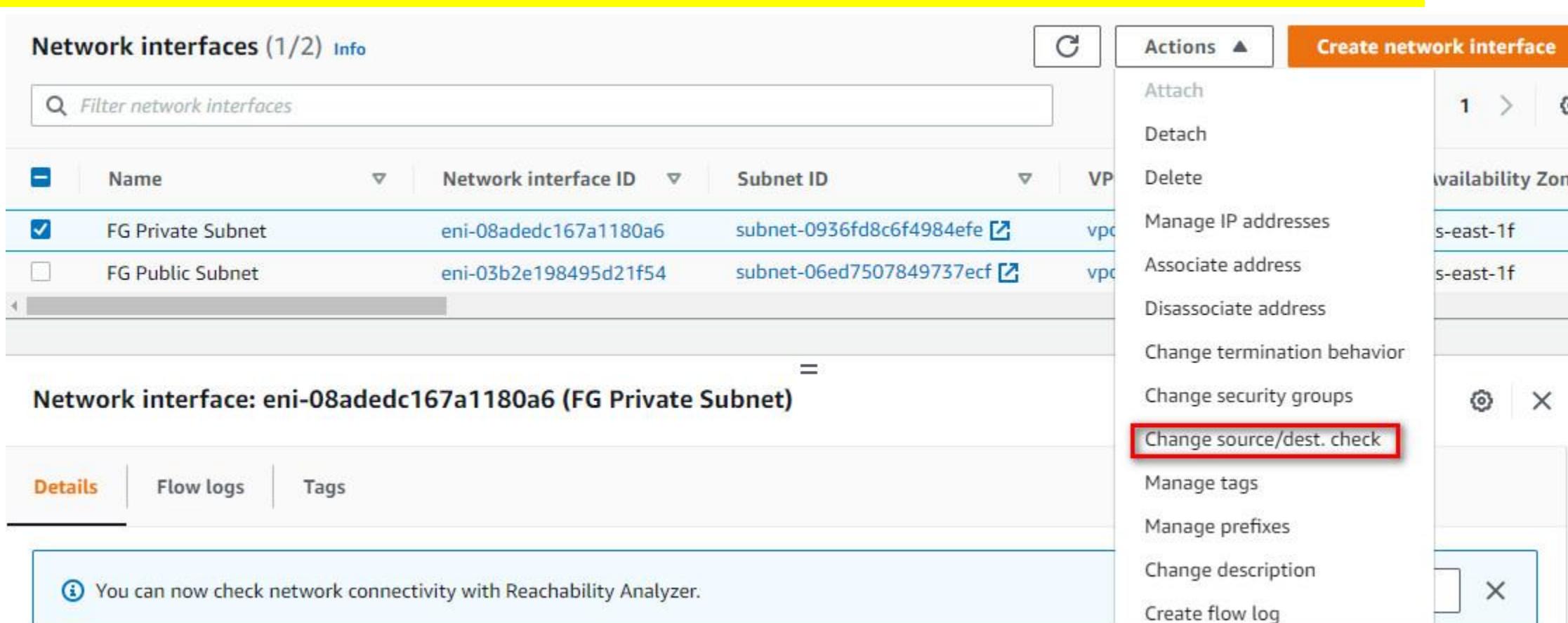


Figure 10.139: Disable source/destination check on FG Private Subnet

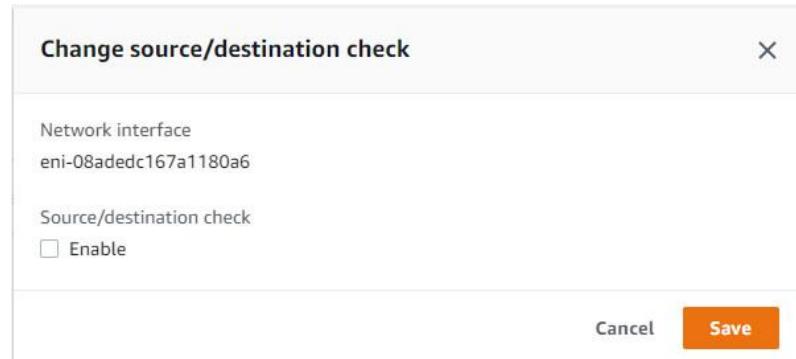


Figure 10.140: Disable source/destination check on FG Private Subnet

Figure 10.141: Disable source/destination check on FG Public Subnet

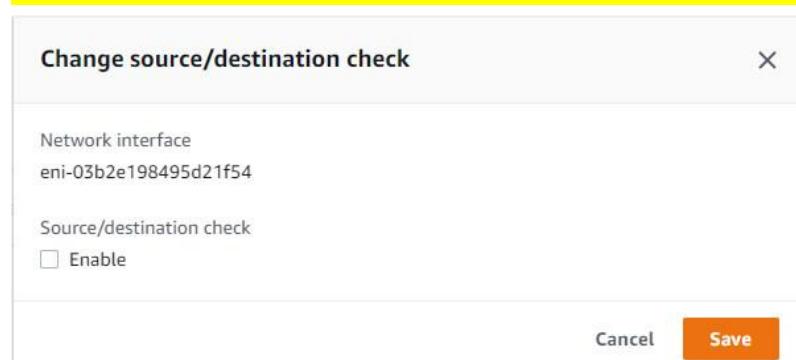


Figure 10.142: Disable source/destination check on FG Public Subnet

9. Edit private route table.

Figure 10.143: Edit Private Route

Edit routes

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No
0.0.0.0/0	-	No	<button>Remove</button>

Add route

Target dropdown options (highlighted 'Network Interface'): Carrier Gateway, Core Network, Egress Only Internet Gateway, Gateway Load Balancer Endpoint, Instance, Internet Gateway, local, NAT Gateway, Network Interface, Outpost Local Gateway, Peering Connection, Transit Gateway, Virtual Private Gateway.

Buttons: Cancel, Preview, Save changes

Figure 10.144: Add a default route and select Network Interface

Destination	Target	Status
10.0.0.0/16	local	Active
0.0.0.0/0	eni-05bze198495d21f54 (FG Public Subnet)	-

Add route

Figure 10.145: Add a default route to target FG Private Subnet

10. Verify Public and Private IP address of FG.

Instances (1/1) Info		C	Connect	Instance state ▾	Actions ▾	Launch instances
<input checked="" type="checkbox"/>	Name	Instance ID	Instance state	Instance type	Status check	
<input checked="" type="checkbox"/>	FG	i-Off098db861c07b53	Running	t2.small	2/2 checks passed	

Instance: i-Off098db861c07b53 (FG)

Details	Security	Networking	Storage	Status checks	Monitoring	Tags												
Instance summary Info <table border="1"> <tr> <td>Instance ID i-Off098db861c07b53 (FG)</td> <td>Public IPv4 address 3.239.117.237 open address</td> <td>Private IPv4 addresses 10.0.0.22 10.0.1.147</td> </tr> <tr> <td>IPv6 address -</td> <td>Instance state Running</td> <td>Public IPv4 DNS -</td> </tr> <tr> <td>Hostname type IP name: ip-10-0-0-22.ec2.internal</td> <td>Private IP DNS name (IPv4 only) ip-10-0-0-22.ec2.internal</td> <td>Answer private resource DNS name IPv4 (A)</td> </tr> <tr> <td>Instance type t2.small</td> <td>Elastic IP addresses -</td> <td>Auto-assigned IP address 3.239.117.237 [Public IP]</td> </tr> </table>							Instance ID i-Off098db861c07b53 (FG)	Public IPv4 address 3.239.117.237 open address	Private IPv4 addresses 10.0.0.22 10.0.1.147	IPv6 address -	Instance state Running	Public IPv4 DNS -	Hostname type IP name: ip-10-0-0-22.ec2.internal	Private IP DNS name (IPv4 only) ip-10-0-0-22.ec2.internal	Answer private resource DNS name IPv4 (A)	Instance type t2.small	Elastic IP addresses -	Auto-assigned IP address 3.239.117.237 [Public IP]
Instance ID i-Off098db861c07b53 (FG)	Public IPv4 address 3.239.117.237 open address	Private IPv4 addresses 10.0.0.22 10.0.1.147																
IPv6 address -	Instance state Running	Public IPv4 DNS -																
Hostname type IP name: ip-10-0-0-22.ec2.internal	Private IP DNS name (IPv4 only) ip-10-0-0-22.ec2.internal	Answer private resource DNS name IPv4 (A)																
Instance type t2.small	Elastic IP addresses -	Auto-assigned IP address 3.239.117.237 [Public IP]																

Figure 10.146: Verify public and private IP address of FG

11. Accessing FortiGate on AWS.

Type the IP address in the browser. You should be able to see the FortiGate credentials page. Enter your username and password to login to the firewall.



Your connection is not private

Attackers might be trying to steal your information from 3.239.117.237 (for example, passwords, messages, or credit cards). [Learn more](#)

NET::ERR_CERT_AUTHORITY_INVALID

To get Chrome's highest level of security, [turn on enhanced protection](#)

Advanced

Back to safety

Figure 10.147: Access FortiGate

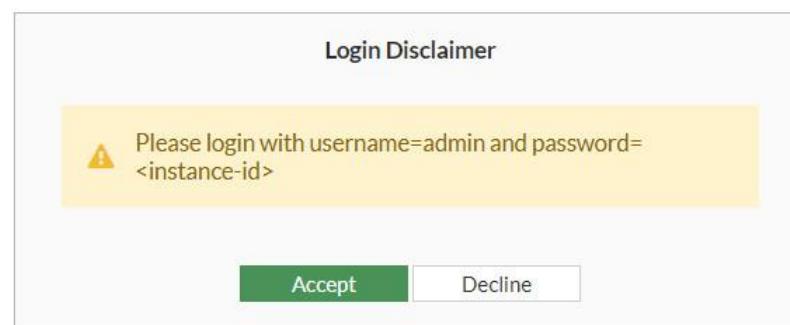


Figure 10.148: Access FortiGate

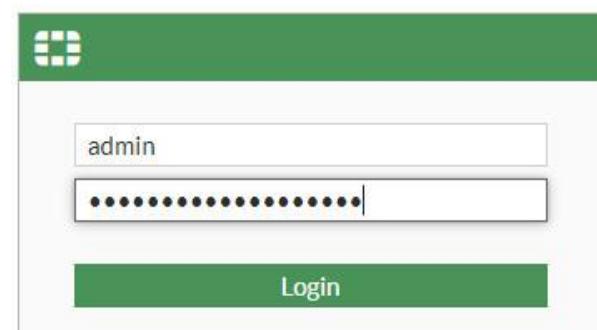


Figure 10.149: Username is admin and password is instance ID of FortiGate

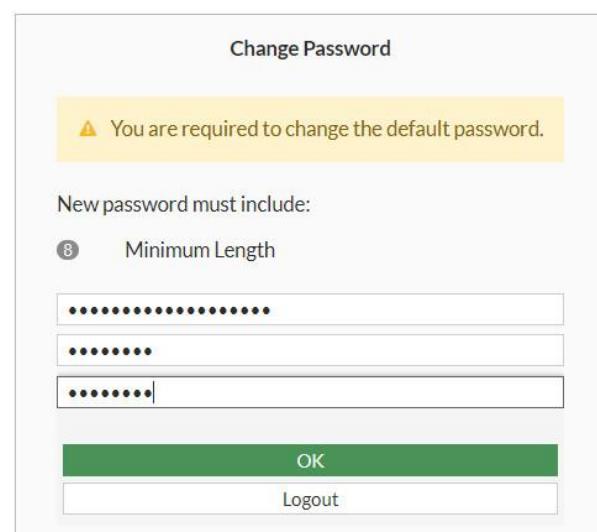


Figure 10.150: Change password

Figure 10.151: FortiGate dashboard

You should set port1 and port2 as DHCP client to receive an IP address from External and LAN subnet. Port1 is belong to External subnet or the internet and port2 is belong to the LAN.

Table 10.5: Port1 and Port2 description

Subnet	Description
Port1	External subnet used to connect the FortiGate-VM to the internet.
Port2	LAN subnet used to deploy services.

Figure 10.152: Change port2 to DHCP Client

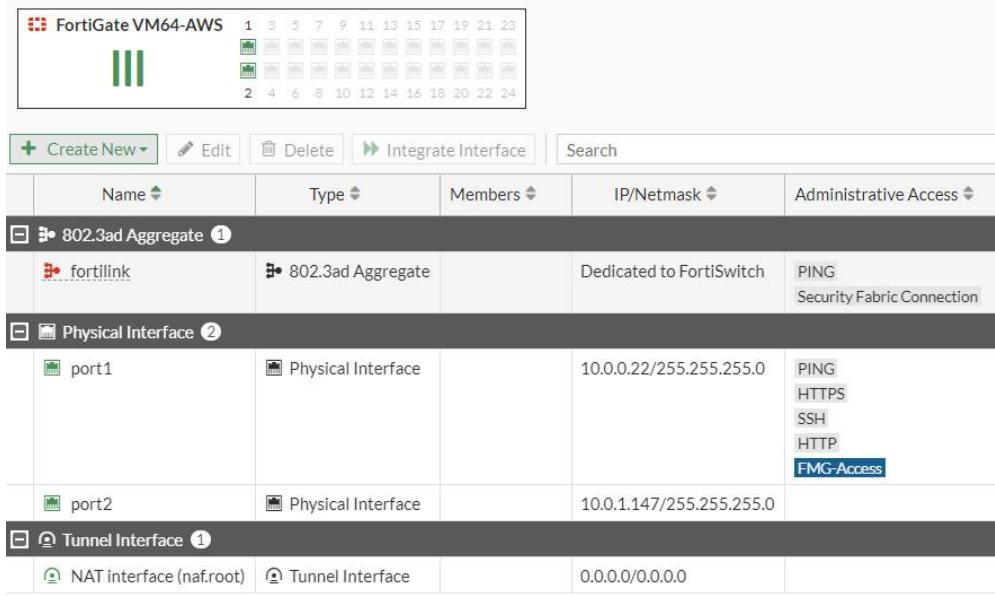


Figure 10.153: FortiGate interfaces