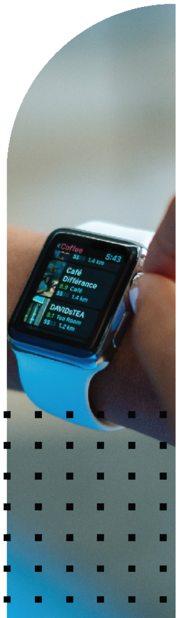
AWS Deployment Guide

FortNDR (BYOL) 7.0.0



FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO LIBRARY
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

FORTINET TRAINING INSTITUTE
https://training.fortinet.com

FORTIGUARD LABS
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

April 21, 2022
FortNDR (BYOL) 7.0.0 AWS Deployment Guide
00-700-794552-20220421

TABLE OF CONTENTS

Change Log

Date	Change Description
2019-05-25	Initial release.

Introduction

FortiNDR (formerly FortiAI) is the first Fortinet Network Detection and Response product from Fortinet. Apart from the Virtual Security Analyst^{TM} with malware detection technology based on neural networks, FortiNDR is built on FortiAI’s technology with extended and added features to detect Network Anomalies with auto and manual mitigation techniques. FortiNDR is renamed from FortiAI with additional Network Detection and Response functionality, with the original FortiAI malware analysis features.

FortiNDR is the next generation of Fortinet's malware detection technology, using Artificial Neural Networks (ANN) which can deliver sub-second malware detection and verdict. ANN is able to mimic human behavior using the Virtual Security Analyst (VSA)^{TM}, which is capable of the following:

- Detect encrypted attack (via JA3 hashes), look for presence of malicious web campaigns visited, weaker ciphers, vulnerable protocols, network and botnet-based attacks.
- Profile ML traffic and identify anomalies with user feedback mechanism.
- Detect malicious files in sub-seconds through neural network analysis including NFS file scan shares.
- Analyze malware scientifically by classifying malware based on its detected features, for example, ransomware, downloader, coinminer, and so on.
- Trace the origins of the attack, for example, worm infection.
- OutBreak search can use the similarity engine to search for malware outbreaks with hashes and similar variants in the network.
- Take advantage of Fortinet's Security Fabric with FortiGate(s) and other Fortinet Security Fabric solutions, along with 3rd party API calls, to quarantine infected hosts.

FortiNDR can operate in different modes:

Sniffer mode where it captures traffic on the network from SPAN port (or mirrored if deployed as VM), integrated mode with FortiGate devices and input from other Fortinet devices (See release notes for supported devices), with inline blocking with FortiOS (7.0.1 and higher) AV profiles.

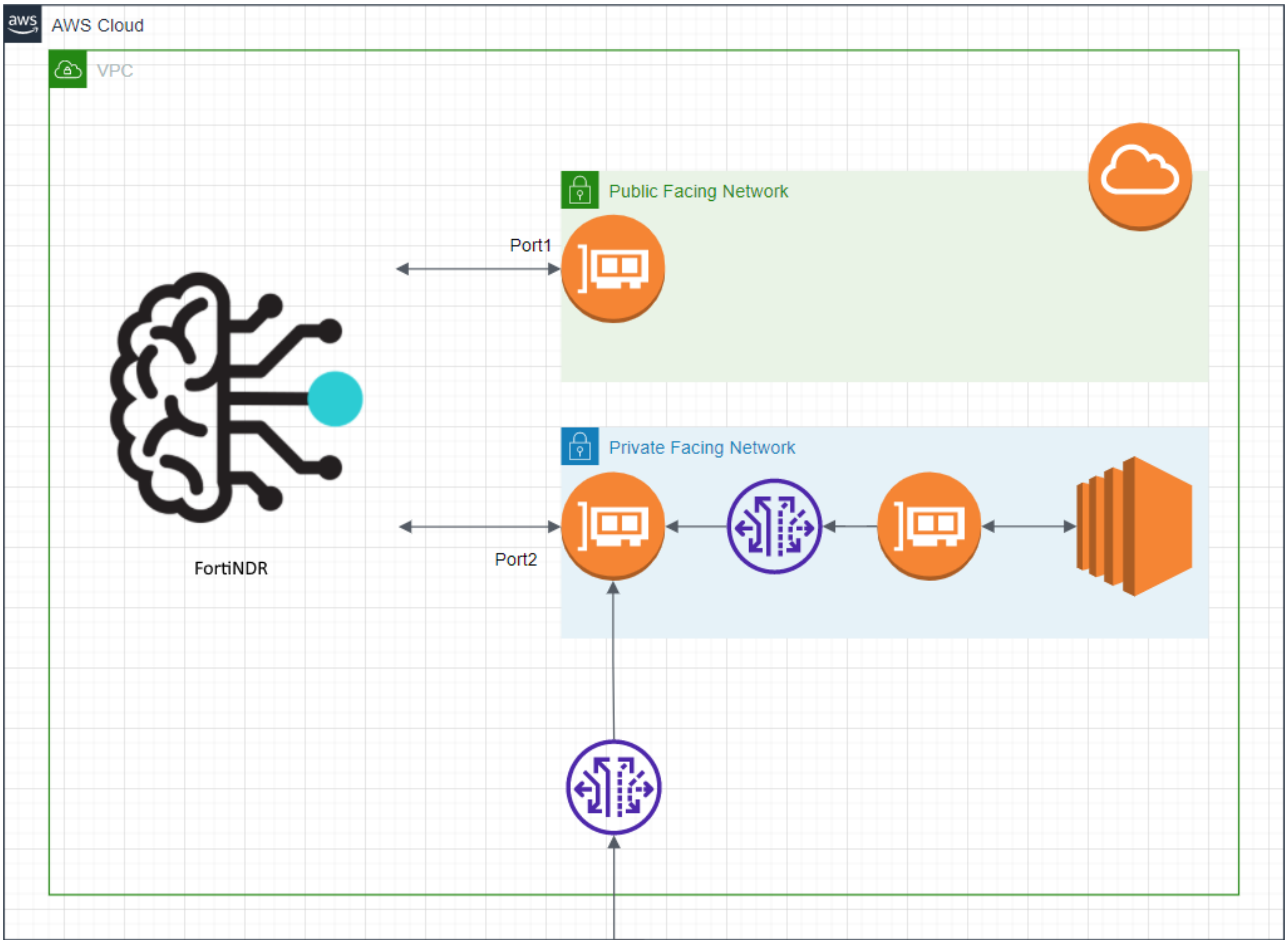
You can also configure FortiNDR as an ICAP server to serve ICAP clients such as FortiProxy and Squid. All modes can operate simultaneously.

Key advantages of FortiNDR include the following:

- Detect network anomalies with different techniques where traditional security solutions might fail.
- Provide more context to attacks such as malware campaign name, web campaign devices and users participate in, intrusions and botnet attacks.
- Tracing and correlate source of malware events such as worm based detection.
- Manual and automatic mitigation (AKA Response) with Fortinet Security Fabric devices (such as FortiGate, FortiSwitch, FortiNAC), as well as 3rd Party solutions (via API calls).

Overview

FortiNDR-VM for AWS can be deployed as a virtual appliance in AWS (IaaS). This section shows you how to install and configure a single instance FortiNDR-VM in AWS to provide a threat monitoring/response security solution to protect your workloads in the AWS IaaS.



Instance support

Instance type	vCPU
R5.4xlarge	16
R5.8xlarge	32

Region support

The following regions are supported on BYOL deployments. See Order types.

Instance support may vary depending on the regions.

Region name	Region code
US East (N. Virginia)	us-east-1
US East (Ohio)	us-east-2
US West (N. California)	us-west-1
US West (Oregon)	us-west-2
Asia Pacific (Seoul)	ap-northeast-2
Asia Pacific (Singapore)	ap-southeast-1
Asia Pacific (Sydney)	ap-southeast-2
Asia Pacific (Tokyo)	ap-northeast-1
Canada (Central)	ca-central-1
EU (Frankfurt)	eu-central-1
EU (Ireland)	eu-west-1
EU (London)	eu-west-2
EU (Paris)	eu-west-3
AWS GovCloud (US-West)	us-gov-west-1

Opening ports in the security group:

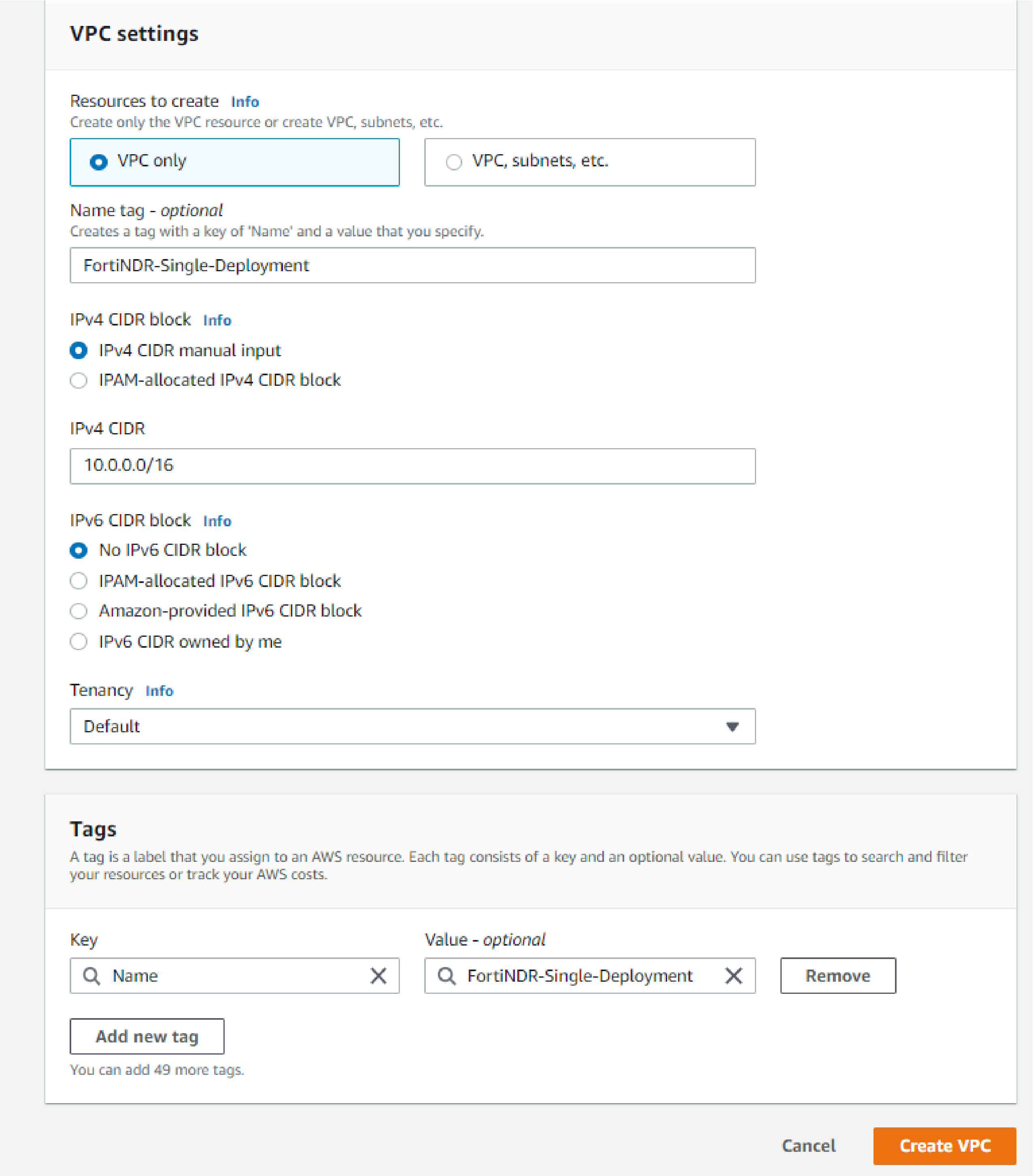
Port1 (Admin)	**Protocol/Ports**	**Purpose**
Incoming	TCP 22	SSH
	TCP 443	HTTPS
	TCP 514	OFTP
	TCP 1344/11344	ICAP
Outgoing	Any	
Port2 (Sniffer)	**Protocol/Ports**	**Purpose**
Incoming	Any	Traffic Mirroring to Sniffer
Outgoing	Any	

Creating a VPC and subnets:

To create a VPC and subnets:

1. Log in to the AWS Management Console.
2. Go to *Networking & Content Delivery* > *VPC*.

3. Go to *Virtual Private Cloud* > *Your VPCs*, then click *Create VPC*.



VPC settings

Resources to create Info
Create only the VPC resource or create VPC, subnets, etc.

● VPC only ○ VPC, subnets, etc.

Name tag - *optional*
Creates a tag with a key of 'Name' and a value that you specify.

FortiNDR-Single-Deployment

IPv4 CIDR block Info

● IPv4 CIDR manual input
○ IPAM-allocated IPv4 CIDR block

IPv4 CIDR

10.0.0.0/16

IPv6 CIDR block Info

● No IPv6 CIDR block
○ IPAM-allocated IPv6 CIDR block
○ Amazon-provided IPv6 CIDR block
○ IPv6 CIDR owned by me

Tenancy Info

Default ▾

Tags

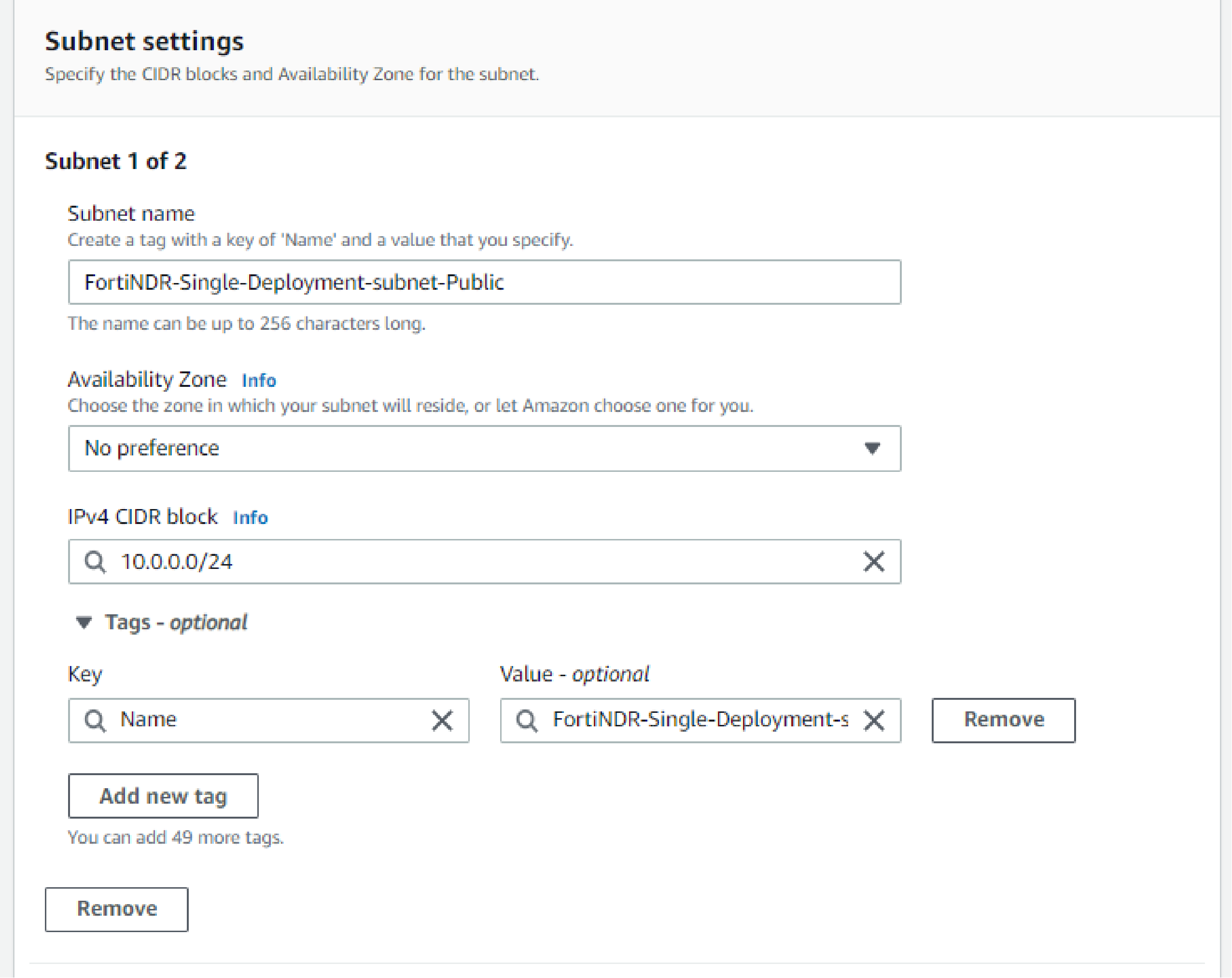
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key	Value - *optional*	
Name	FortiNDR-Single-Deployment	Remove

You can add 49 more tags.

4. Select VPCs, subnet, etc.
5. In the *Name tag* field, set the VPC name.
6. In the *CIDR block* field, specify an IPv4 address range for your VPC.
7. In the *Tenancy* field, select Default.

8. Select *Yes* and click Create Subnet.



Subnet settings

Specify the CIDR blocks and Availability Zone for the subnet.

Subnet 1 of 2

Subnet name
Create a tag with a key of 'Name' and a value that you specify.
FortiNDR-Single-Deployment-subnet-Public
The name can be up to 256 characters long.

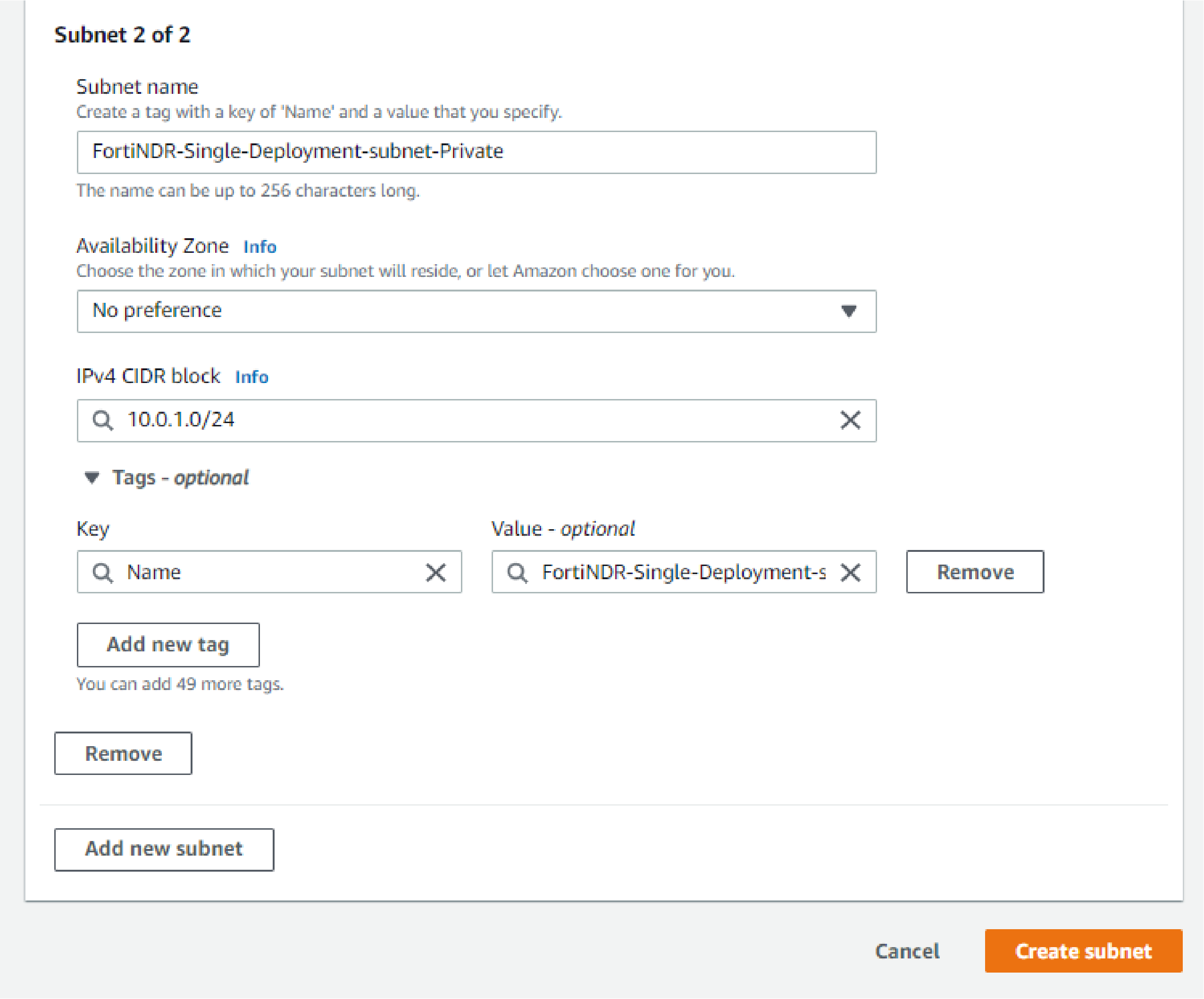
Availability Zone Info
Choose the zone in which your subnet will reside, or let Amazon choose one for you.
No preference

IPv4 CIDR block Info
10.0.0.0/24

▼ Tags - *optional*

Key	Value - *optional*
Name	FortiNDR-Single-Deployment-s

You can add 49 more tags.



Subnet 2 of 2

Subnet name
Create a tag with a key of 'Name' and a value that you specify.
FortiNDR-Single-Deployment-subnet-Private
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
10.0.1.0/24

Tags - *optional*

Key: Name
Value - *optional*: FortiNDR-Single-Deployment-s

You can add 49 more tags.

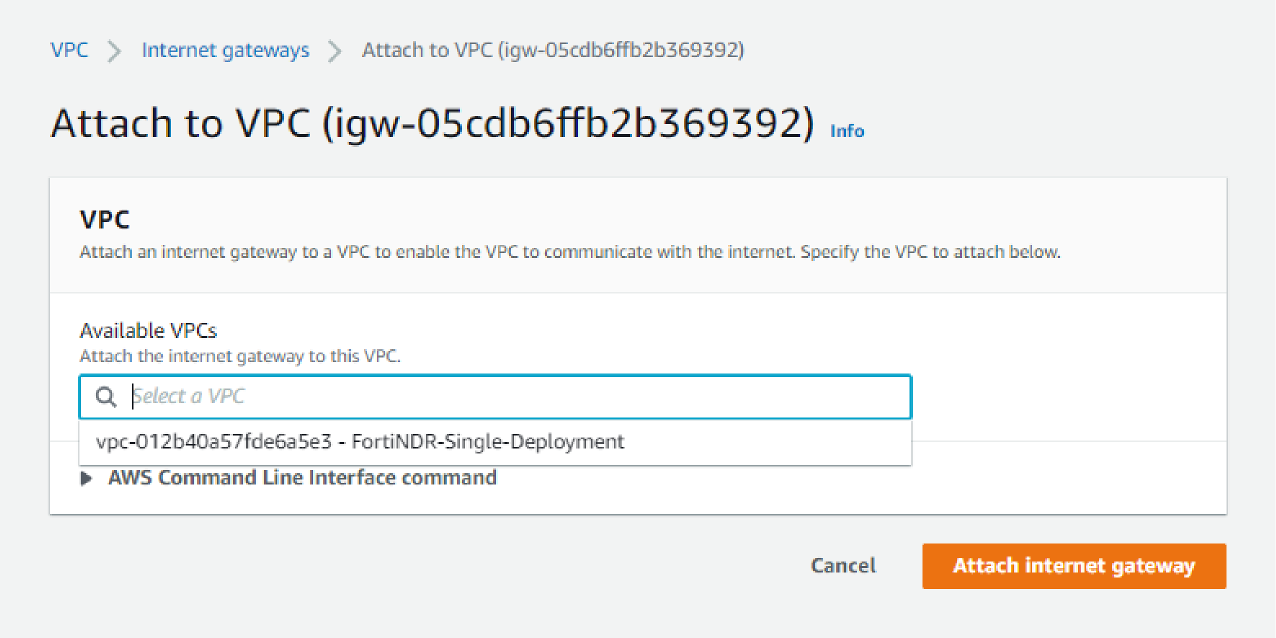
9. In the Virtual Private Cloud menu, select Subnets, then select Create Subnet. Create a public subnet (in this example, Subnet1) and a private subnet (Subnet2), as shown in this example. Both subnets belong to the VPC that you created.

Attaching the new VPC Internet gateway

If you are using the default VPC, the Internet gateway should already exist.

To attach the new VPC Internet gateway:

1. In the *Virtual Private Cloud* menu, select *Internet Gateways*, then select *Create Internet Gateway*.
2. In the *Name tag* field, set the Internet gateway name, then click *Yes, Create*.
3. Select the Internet gateway, then select *Attach to VPC*.
4. Select the VPC that you created and click *Yes, Attach*. The Internet gateway state changes from detached to attached.



VPC > Internet gateways > Attach to VPC (igw-05cdb6ffb2b369392)

Attach to VPC (igw-05cdb6ffb2b369392) Info

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.

Select a VPC

vpc-012b40a57fde6a5e3 - FortiNDR-Single-Deployment

▶ AWS Command Line Interface command

Subscribing to the FortiNDR

To subscribe to the FortiNDR:

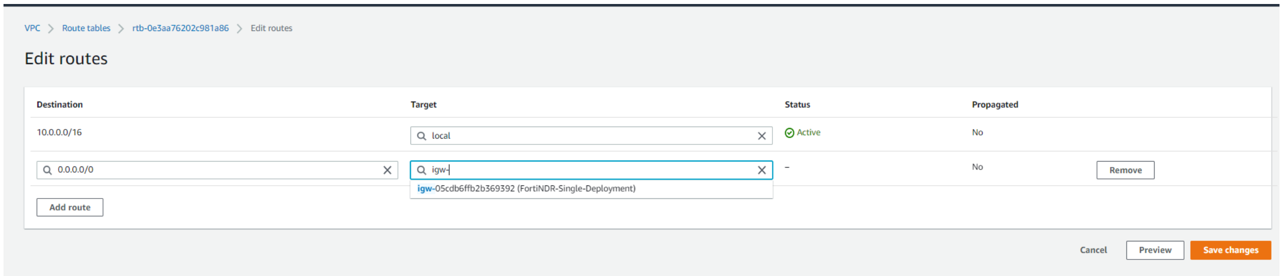
1. Go to the AWS Marketplace and search for *Fortinet FortiNDR-VM-BYOL*. Click *Continue*.
2. Click *Manual Launch*.
3. Click *Launch with EC2 Console* beside the region you want to launch.
4. Select an instance type, then click *Next: Configure Instance Details*.
5. Configure instance details:
   a. In the *Network* field, select the VPC that you created.
   b. In the *Subnet* field, select the public subnet.
   c. In the *Network interfaces* section, you will see the entry for *eth0* that was created for the public subnet. Click *Add Device* to add another network interface (in this example, eth1), and select the private subnet. It is recommended that you assign static IP addresses.
   d. When you have two network interfaces, an EIP is not assigned automatically. You must manually assign one later. Click *Review and Launch*, then click *Launch*.
6. Select an existing key pair or create a new key pair. Select the acknowledgment checkbox. Click *Launch Instances*.
7. To easily identify the instance, set a name for it in the *Name* field.
   a. When registered FortiNDR AWS-BYOL license on https://support.fortinet.com/welcome/#/, please ensure management ip is set to 0.0.0.0 to incorporate with DHCP mode in VPC.
8. Configure an EIP:
   a. In the *Network & Security* menu, select *Elastic IPs*, then select an IP that is available for you to use or create one.
   b. Go to *Actions* > *Associate Address*. If you do not have an address that is available to use, create one.
   c. In the *Resource type* section, select *Network Interface*.
   d. In the *Network interface* field, select the interface ID of the network interface that you created for the public subnet (in this example, eth0).
   e. In the *Private IP* field, select the IP address that belongs to the public subnet. To find these values, go to the *EC2 Management Console*, select *Instances*, and select the interface in the Network interfaces section in the lower pane of the page (Interface ID and Private IP Address fields).
   f. Select *Associate*. A message is displayed indicating the address association was successful.

> 1. If the Internet Gateway is not associated with a VPC, the elastic IP assignment will fail.

Creating routing tables and associate subnets

To configure the public subnet's routing table:

1. Go to *Networking & Content Delivery* > *VPC* in the AWS management console.
2. In the *VPC* Dashboard, click *Your VPCs*, and click the VPC you created.
3. In the *Summary* tab in the lower pane, select the route table ID located in the *Route table* field. To easily identify the route table, set a name for it in the *Name* field.
4. In the *Routes* tab, click *Edit*, then click *Add another route*.
5. In the *Destination* field, type `0.0.0.0/0`.
6. In the *Target* field, type *igw* and select the Internet Gateway from the auto-complete suggestions.
7. Click *Save*. The default route on the public interface in this VPC is now the Internet Gateway.



VPC > Route tables > rtb-0e3aa76202c981a86 > Edit routes

Edit routes

Destination	Target	Status	Propagated	
10.0.0.0/16	local	Active	No	
0.0.0.0/0	igw- igw-05cdb6ffb2b369392 (FortiNDR-Single-Deployment)	-	No	Remove

8. In the *Subnet Associations* tab, click *Edit*, and select the public subnet to associate it with this routing table.
9. Click *Save*.
10. Select the network interface in private subnet, click the *Actions* dropdown list.
11. Click *Change Source/Dest*.
12. Click *Disabled*.
13. Click*Save*.

Connecting to the FortiNDR-VM

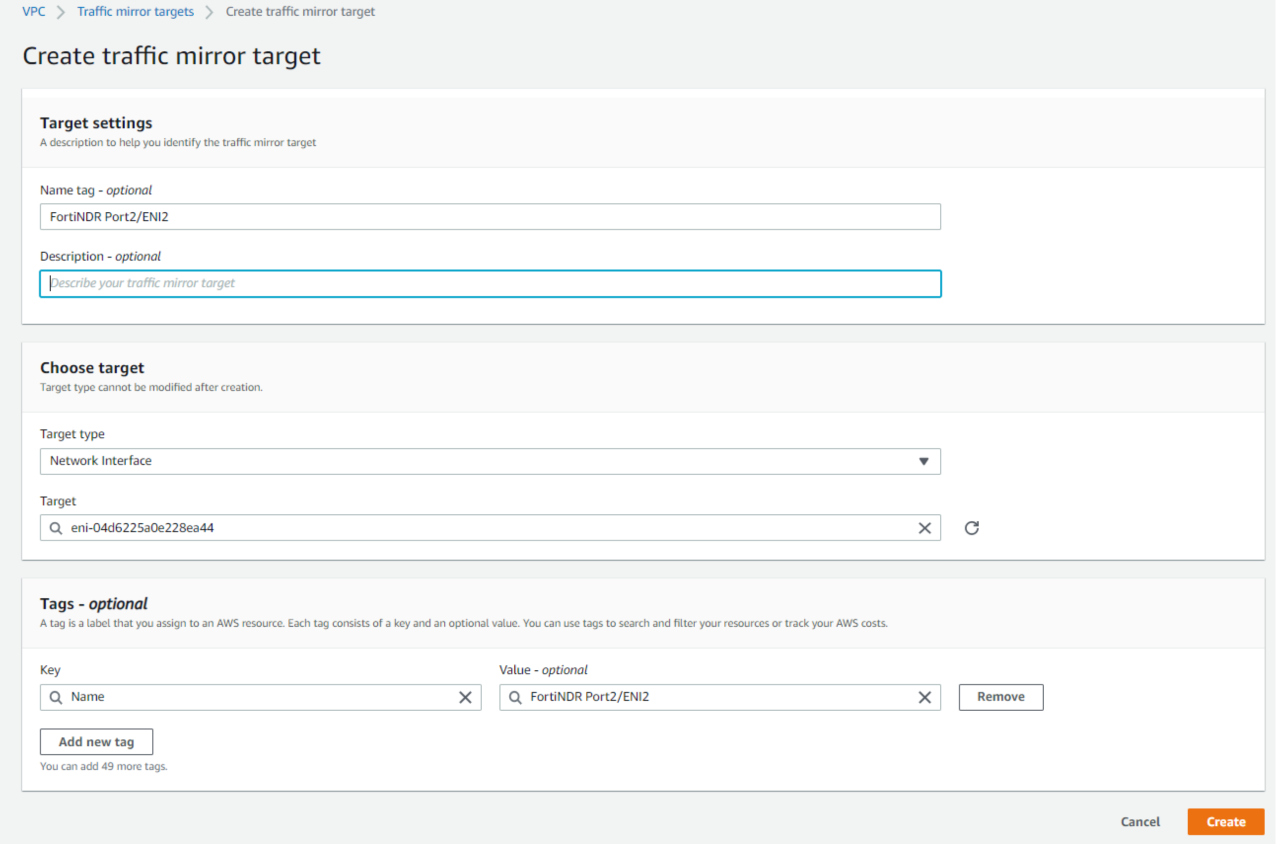
To connect to the FortiNDR-VM, you need your login credentials and its public DNS address.

The default username is *admin* and the default password is the instance ID.

1. You can find the public DNS address in the EC2 management console. Click *Instances* and locate the *Public DNS (IPv4)* field in the lower pane. If you do not see the DNS address, you may need to enable DNS host assignment on your VPC. In this case, go back to the VPC management console, click *Your VPCs*, and select your VPC. Select
2. Open an HTTPS session using the public DNS address of the FortiNDR-VM in your browser (https://). You will see a certificate error message from your browser, which is normal because the default FortiNDR certificate is self-signed and isn't recognized by browsers. Proceed past this error. You can upload a publicly signed certificate at a later time to avoid this error. Log in to the FortiNDR-VM with your username and password (the login credentials mentioned above).
3. If you are using a BYOL license, upload your license (.lic) file to activate the FortiNDR-VM. The FortiNDR-VM will automatically restart. After it restarts, log in again. You will now see the FortiNDR-VM dashboard. Depending on your license type, the information in the license widget on the dashboard may vary.
4. Go to *Network > Interfaces*, and edit the interfaces, if required. If the IP address or subnet mask is missing for port 1 or port 2, configure these values.

Configuring Traffic Mirroring Target/Filter/Session:

1. Go to *VPC* > *Traffic mirror targets* and click *Create traffic mirror target*.
2. Under *Choose target* > *target*, select the secondary network interface of FortiNDR in private subnet.



Create traffic mirror target

Target settings
A description to help you identify the traffic mirror target

Name tag - *optional*
FortiNDR Port2/ENI2

Description - *optional*
Describe your traffic mirror target

Choose target
Target type cannot be modified after creation.

Target type
Network Interface

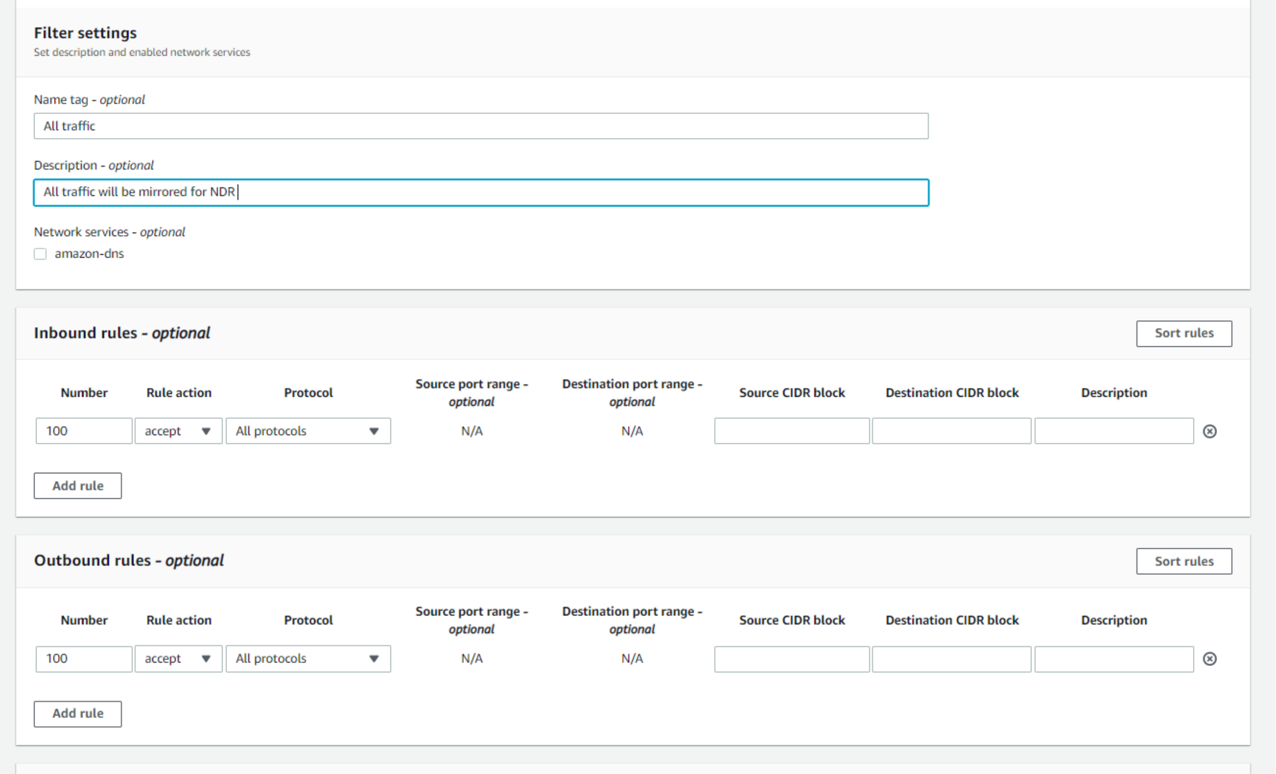
Target
eni-04d6225a0e228ea44

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*
Name	FortiNDR Port2/ENI2

3. In the *VPC/ Traffic Mirror Filter*, select *Create traffic mirror filter*.

4. Configure inbound/outbound traffic filter for NDR. E.G All traffic will be mirrored as illustrated in following figure.



Filter settings

Set description and enabled network services

Name tag - *optional*

All traffic

Description - *optional*

All traffic will be mirrored for NDR

Network services - *optional*

□ amazon-dns

Inbound rules - *optional*

Number	Rule action	Protocol	Source port range - *optional*	Destination port range - *optional*	Source CIDR block	Destination CIDR block	Description
100	accept	All protocols	N/A	N/A			

Outbound rules - *optional*

Number	Rule action	Protocol	Source port range - *optional*	Destination port range - *optional*	Source CIDR block	Destination CIDR block	Description
100	accept	All protocols	N/A	N/A			

5. In the *VPC/ Traffic Mirror Session*, click *Create traffic mirror session*.
6. Select designated network interface for mirror source.
7. Select the previously created mirror target and mirror filter. Configure *Session Number*, *VNI* and *Packet Length* as required.

FORTINET®

www.fortinet.com