Fast2Test
FIRST TEST, FIRST PASS!

# Fast2Test



We're not the only ones **happy** about Fast2test Practice Materials ...

**62316+** customers in 100+ countries use Fast2test Self Test Engine. Meet our customers.

https://www.fast2test.com

Everything you need to prepare, learn & pass your certification exam easily.

**Exam** : **FCP_WCS_AD-7.4**

**Title** : FCP - AWS Cloud Security 7.4 Administrator

**Vendor** : Fortinet

**Version** : DEMO

**NO.1** An organization has created a VPC with two subnets and deployed a FortiGate-VM (VM04/c4.xlarge) in AWS.
The EC2 instance is initially configured with two Elastic Network Interfaces (ENIs). The primary ENI is configured on the public subnet, and the secondary ENI is configured on the private subnet. To provide internet access for the FortiGate-VM, they now want to associate an EIP to its primary ENI, but the assignment is failing.
Which action would allow the EIP assignment to be successful?
**A.** Create and attach an internet gateway to the VPC, and then assign the EIP to the primary ENI of the FortiGate VM.
**B.** Shut down the FortiGate VM, if it is running, assign the EIP to the primary ENI, and then power it on.
**C.** Create and attach a public routing table to the public subnet, associate the public subnet with the primary ENI of the FortiGate VM, and then assign the EIP to the primary ENI.
**D.** Create and associate a public subnet with the primary ENI of the FortiGate VM, and then assign the EIP to the primary ENI.
***Answer:*** A
Explanation:
Internet Gateway Requirement:
For an Elastic IP (EIP) to be assigned to an instance's primary ENI, the VPC must have an Internet Gateway (IGW) attached. The IGW enables the VPC to communicate with the internet, allowing the EIP to function properly (Option C).
Process of Assigning EIP:
Once the Internet Gateway is attached to the VPC, the EIP can be successfully assigned to the primary ENI of the FortiGate VM, providing it with internet access.
Other Options Analysis:
Option A is incorrect because the primary ENI is already in a public subnet.
Option B is not necessary and may not solve the issue without an attached Internet Gateway.
Option D is partially correct about the routing table but does not address the primary issue of needing an Internet Gateway.
Reference:
AWS Elastic IP Documentation: Elastic IP
AWS Internet Gateway: Internet Gateway

**NO.2** An administrator has been asked to deploy an active-passive (A-P) FortiGate cluster in the AWS cloud across two availability zones.
In addition to enhanced redundancy, which other major difference is there compared to deploying A-P high availability in the same availability zone?
**A.** Secondary IP address configuration is used.
**B.** The FortiGate devices act as a single, logical instance.
**C.** IP addressing and subnetting are not shared.
**D.** The number of subnets required is less.
***Answer:*** C
Explanation:
Enhanced Redundancy:
Deploying an active-passive (A-P) FortiGate cluster across two availability zones (AZs) provides

enhanced redundancy by ensuring that if one AZ fails, the other can take over, maintaining high availability and uptime.
IP Addressing and Subnetting:
One of the major differences when deploying across different AZs compared to the same AZ is that IP addressing and subnetting are not shared between the instances. Each AZ operates independently with its own set of subnets and IP addresses, which must be managed separately (Option D).
Other Options Analysis:
Option A is incorrect because the FortiGate devices in an A-P setup do not act as a single logical instance; they operate in a failover setup.
Option B is incorrect because secondary IP address configuration is used in both single AZ and multi-AZ deployments.
Option C is incorrect because the number of subnets required is typically more when deploying across multiple AZs for redundancy.
Reference:
FortiGate HA Configuration Guide: FortiGate HA
AWS Availability Zones: AWS AZ

**NO.3** You are troubleshooting network connectivity issues between two VMs deployed in AWS. One VM is a FortiGate located on subnet "LAN" that is part of the VPC "Encryption". The other VM is a Windows server located on the subnet "servers" which is also in the "Encryption" VPC. You are unable to ping the Windows server from FortiGate.
What are two reasons for this? (Choose two.)
**A.** By default, AWS does not allow ICMP traffic between subnets.
**B.** The default AWS Network Access Control List (NACL) does not allow this traffic.
**C.** The firewall in the Windows VM is blocking the traffic.
**D.** Add an inbound allow ICMP rule in the security group attached to the windows server.
***Answer:*** C,D
Explanation:
Windows Firewall Blocking Traffic:
The firewall on the Windows VM might be configured to block incoming ICMP traffic (ping requests). By default, Windows Firewall is set to block ICMP traffic, which could be a reason for the connectivity issue (Option A).
Security Group Configuration:
AWS Security Groups act as virtual firewalls for instances. If there is no rule allowing ICMP traffic in the security group attached to the Windows server, the ping requests from FortiGate will be blocked. An inbound allow ICMP rule must be added to the security group to permit this traffic (Option D).
Other Options Analysis:
Option B is incorrect because the default AWS Network Access Control List (NACL) allows all inbound and outbound traffic.
Option C is incorrect as AWS does allow ICMP traffic between subnets if properly configured with Security Groups and NACLs.
Reference:
AWS Security Groups: AWS Security Groups
Windows Firewall Configuration: Windows Firewall

**NO.4** An organization has created a VPC with two subnets and deployed a FortiGate-VM

(VM04/c4.xlarge) in AWS.
The EC2 instance is initially configured with two Elastic Network Interfaces (ENIs). The primary ENI is configured on the public subnet, and the secondary ENI is configured on the private subnet. To provide internet access for the FortiGate-VM, they now want to associate an EIP to its primary ENI, but the assignment is failing.
Which action would allow the EIP assignment to be successful?

**A.** Create and associate a public subnet with the primary ENI of the FortiGate VM, and then assign the EIP to the primary ENI.

**B.** Create and attach a public routing table to the public subnet, associate the public subnet with the primary ENI of the FortiGate VM, and then assign the EIP to the primary ENI.

**C.** Create and attach an internet gateway to the VPC, and then assign the EIP to the primary ENI of the FortiGate VM.

**D.** Shut down the FortiGate VM, if it is running, assign the EIP to the primary ENI, and then power it on.

***Answer:*** C