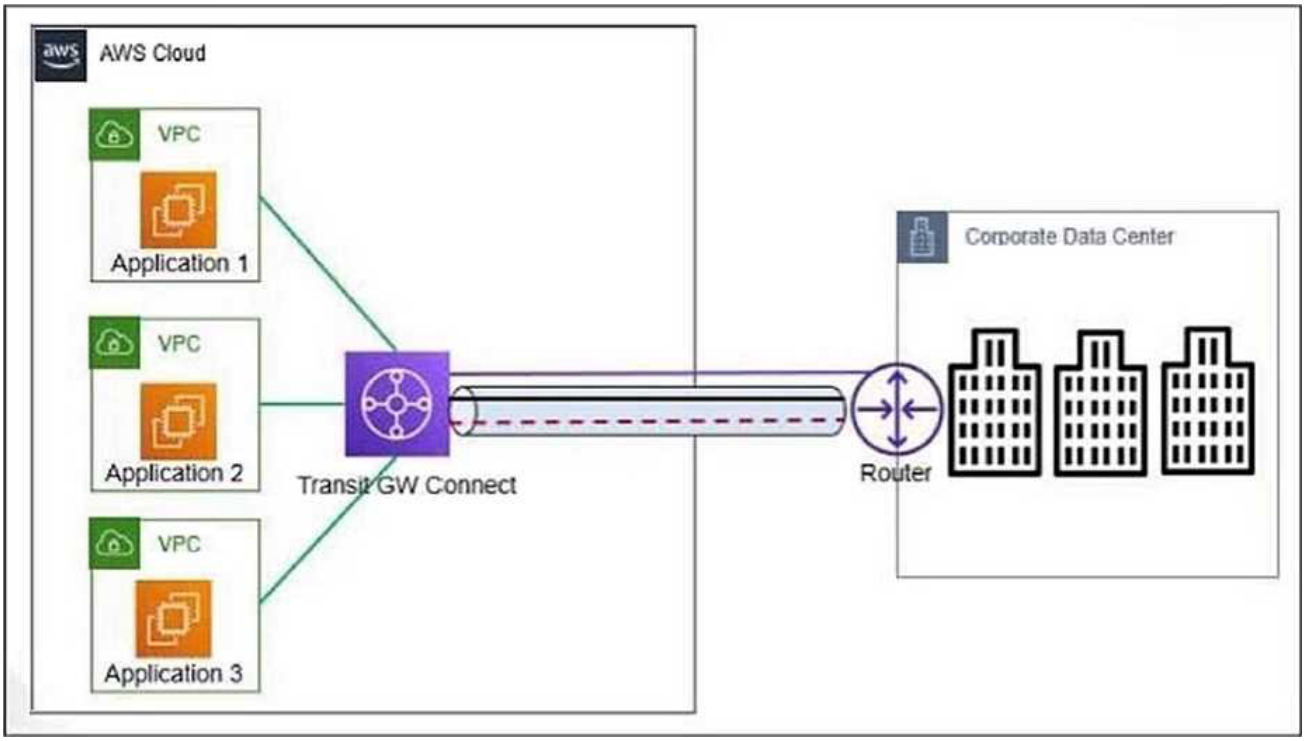
Exam : FCP_WCS_AD-7.4

Title : FCP - AWS Cloud Security 7.4 Administrator

Version : DEMO

1.Refer to the exhibit.



An organization deployed the application servers in the AWS VPC that connects to the corporate data center using Transit Gateway Connect. Demand for the applications has grown and the connection requires more bandwidth.

What is required to achieve higher bandwidth?

A. Use routable public IP addresses instead of private IP addresses for connectivity.

B. You cannot increase bandwidth the connection has a fixed limit.

C. No configuration change is required because GRE tunnels are scaled to provide higher bandwidth.

D. You add a Transit VPC between the organization's VPCs.

Answer: C

Explanation:

Understanding Transit Gateway Connect:

Transit Gateway Connect is a feature of AWS Transit Gateway that simplifies the integration of SD-WAN networks with AWS. It uses Generic Routing Encapsulation (GRE) tunnels to facilitate this connection.

GRE Tunnels and Bandwidth:

GRE tunnels can dynamically scale to meet increasing bandwidth demands. They allow multiple tunnels between the same endpoints, which can aggregate bandwidth without requiring additional configuration.

Scaling Bandwidth with GRE:

The GRE protocol used by Transit Gateway Connect can support high bandwidth requirements by spreading traffic across multiple tunnels. As demand grows, additional tunnels can be automatically used to handle the increased traffic load.

Comparison with Other Options:

Option A suggests using public IP addresses, which is not relevant to bandwidth scaling.

Option B is incorrect because bandwidth can be increased through GRE scaling.

Option D suggests adding a Transit VPC, which is unnecessary for increasing bandwidth when using Transit Gateway Connect.

Reference: AWS Transit Gateway Documentation: AWS Transit Gateway
GRE Tunnels and AWS: AWS GRE Tunnels

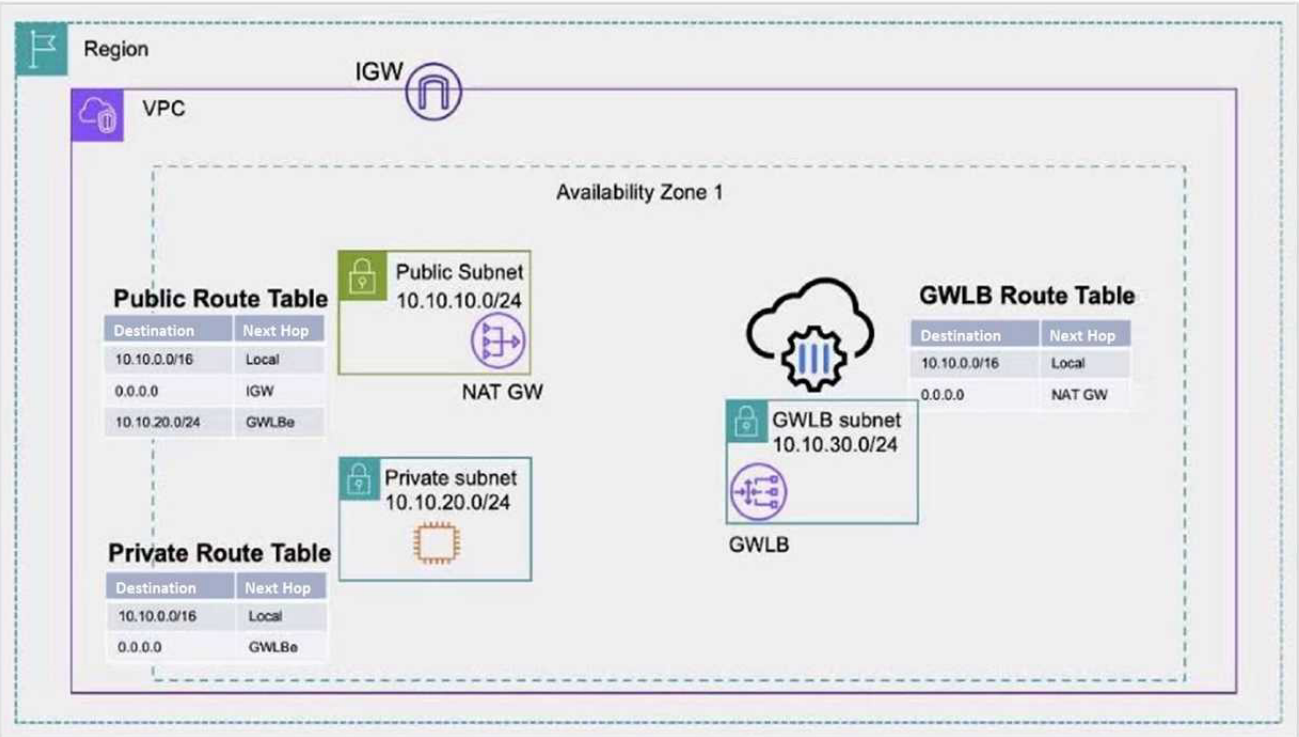
2.You want to deploy the Fortinet HA CloudFormation template to stage and bootstrap the FortiGate configuration in the same region in which you created your VPC, which is Ohio US-East-2.
Based on this information, which statement is correct?
A. You create an S3 bucket to stage and bootstrap FortiGate with an FGCP unicast configuration. The S3 bucket can be hosted in any region.
B. The Fortinet HA cloud formation template automatically creates an S3 bucket.
C. You create an S3 bucket to stage and bootstrap FortiGate with an FGCP unicast configuration. The S3 bucket needs to be hosted in the Ohio US-East-2 region.
D. You create a DynamoDB to stage and bootstrap FortiGate with an FGCP unicast configuration. It needs to be hosted in the Ohio US-East-2 region.
Answer: C
Explanation:
Understanding Fortinet HA CloudFormation Template:
The Fortinet High Availability (HA) CloudFormation template is used to automate the deployment and configuration of FortiGate instances in AWS.
Staging and Bootstrapping FortiGate:
Staging involves preparing the necessary configuration files and resources needed for deployment.
Bootstrapping is the process of automatically configuring FortiGate instances upon deployment.
S3 Bucket Requirement:
The configuration files required for staging and bootstrapping are typically stored in an S3 bucket.
Since the deployment is in the Ohio (US-East-2) region, it is recommended to host the S3 bucket in the same region to minimize latency and ensure regional compliance.
Comparison with Other Options:
Option A is incorrect because while an S3 bucket is required, it should be in the same region (US-East-2).
Option B is incorrect as the template does not automatically create the S3 bucket.
Option D is incorrect as DynamoDB is not used for staging and bootstrapping in this scenario.
Reference: Fortinet Documentation: FortiGate on AWS
AWS S3 Documentation: AWS S3

3.An organization has the requirement to connect a data VPC to the on-premises infrastructure of a branch office in a hybrid cloud environment. The connectivity needs the higher bandwidth but the organization does not want to use multiple connections between sites.
Which AWS solution meets the requirement?
A. Transit VPC with IPSec
B. Internet Gateway
C. Transit Gateway multicast
D. Transit Gateway Connect
Answer: D
Explanation:
Understanding the Requirement:

The organization needs to connect a data VPC to the on-premises infrastructure with high bandwidth. The solution should avoid multiple connections between sites.
Transit Gateway Connect:
Transit Gateway Connect is designed to integrate with SD-WAN networks and provides scalable bandwidth using GRE tunnels.
It simplifies hybrid cloud connectivity by allowing high bandwidth connections without the need for multiple physical connections.
Benefits of Transit Gateway Connect:
Supports scalable bandwidth through GRE tunnels.
Facilitates seamless integration with on-premises and cloud environments. Reduces complexity by avoiding the need for multiple VPN connections. Comparison with Other Options:
Option A (Transit VPC with IPSec) is not preferred due to complexity and potential limitations in bandwidth scalability.
Option B (Internet Gateway) is not suitable for private, high-bandwidth connections.
Option C (Transit Gateway multicast) does not address the requirement for high bandwidth in a hybrid cloud setup.
Reference: AWS Transit Gateway Documentation: AWS Transit Gateway Connect
Hybrid Cloud Connectivity: AWS Hybrid Cloud

4.Refer to the exhibit.

FortiGate CNF deployment



Traffic is initiated from the EC2 instance and is destined for the internet.
Which traffic flow is correct?
A. EC2 instance > NAT GW > IGW > internet
B. There is no route to the internet in the Private Route Table. The traffic does not reach the internet.
C. EC2 instance > GWLBe > NAT GW > IGW > internet

D. EC2 instance > GWLBe > internet
Answer: C
Explanation:
Understanding the Architecture:
The architecture includes an EC2 instance in a private subnet, a Gateway Load Balancer Endpoint (GWLBe), a NAT Gateway (NAT GW), and an Internet Gateway (IGW). Route Tables and Routing:
The private route table for the subnet containing the EC2 instance has a route pointing to the GWLBe for internet-bound traffic.
The public route table for the subnet containing the NAT Gateway has routes to the IGW.
Traffic Flow Analysis:
Traffic initiated from the EC2 instance destined for the internet will first be routed to the GWLBe as per the private route table.
The GWLBe will forward the traffic to the NAT Gateway.
The NAT Gateway will then route the traffic to the IGW, which finally sends the traffic to the internet.
Comparison with Other Options:
Option A suggests direct routing to the NAT GW from the EC2 instance, which is incorrect. Option B incorrectly states there is no route to the internet in the private route table. Option D suggests direct routing from GWLBe to the internet, which is not the case.
Reference: AWS Documentation on Route Tables: AWS Route Tables
Gateway Load Balancer Overview: AWS Gateway Load Balancer

5.A customer has implemented GWLB between the partner and application VPCs. FortiGate appliances are deployed in the partner VPC with multiple AZs to inspect traffic transparently.
Which two things will happen to application traffic based on the GWLB deployment? (Choose two.)
A. Inbound and outbound traffic will go to multiple devices, which will perform load balancing.
B. Inbound and outbound traffic will go to the same device, which will perform stateful processing.
C. The content of the original traffic exchanged between the GWLB and FortiGate will be preserved.
D. The original traffic exchanged between the GWLB and FortiGate will be hashed for data integrity.
Answer: A, B
Explanation:
Understanding Gateway Load Balancer (GWLB):
GWLB is designed to distribute traffic across multiple appliances for both inbound and outbound traffic, providing scalability and high availability.
Traffic Load Balancing:
GWLB can send traffic to multiple FortiGate appliances for load balancing purposes, ensuring efficient use of resources (Option A).
Stateful Processing:
For stateful processing, GWLB ensures that traffic flows (both inbound and outbound) for a given connection are directed to the same FortiGate appliance. This maintains session integrity (Option B).
Preservation and Hashing of Traffic:
Options C and D are incorrect as they suggest incorrect behavior regarding traffic content preservation and hashing for data integrity, which are not primary functions of GWLB.
Reference: AWS Gateway Load Balancer Documentation: AWS Gateway Load Balancer
FortiGate Integration with GWLB: Fortinet Documentation