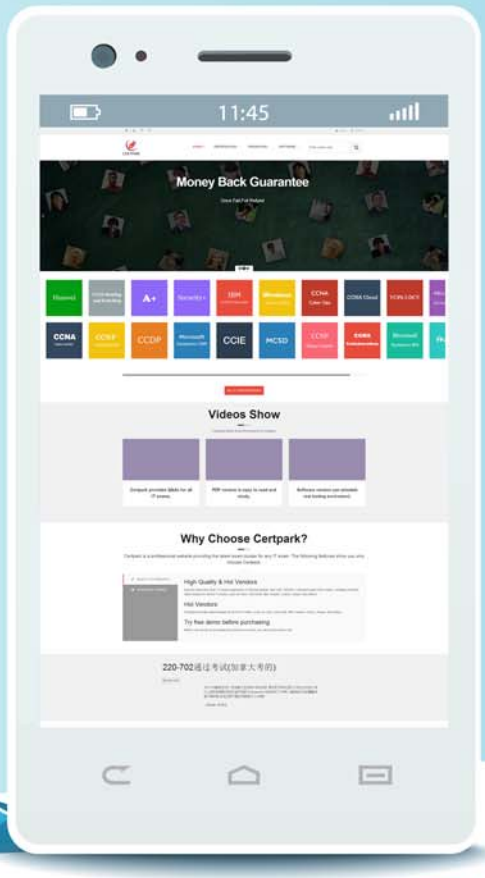
CERTPARK

QUESTION & ANSWER

CERTPARK.COM

Accurate Study Guides,
High Passing Rate!
provides update
free of charge
in one year!



https://www.certpark.com

Exam : **NSE7_PBC-7.2**

Title : Fortinet NSE 7 Public Cloud Security 7.2 (FCSS)

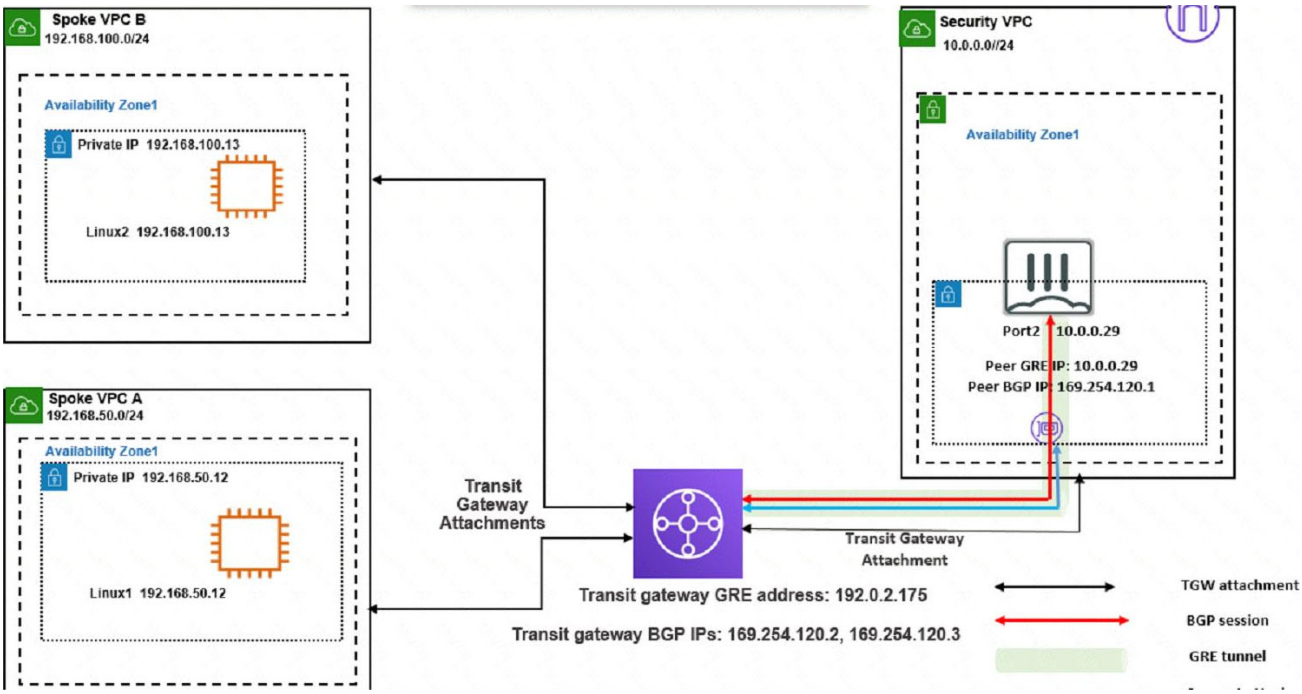
Version : DEMO

1.A Network security administrator is searching for a solution to secure traffic going in and out of the container infrastructure.
In which two ways can Fortinet container security help secure container infrastructure? (Choose two.)
A. FortiGate NGFW can be placed between each application container for north-south traffic inspection
B. FortiGate NGFW can connect to the worker node and protects the container-
C. FortiGate NGFW can inspect north-south container traffic with label aware policies
D. FortiGate NGFW and FortiSandbox can be used to secure container traffic
Answer: CD
Explanation:
The correct answer is C and D. FortiGate NGFW can inspect north-south container traffic with label aware policies and FortiGate NGFW and FortiSandbox can be used to secure container traffic. According to the Fortinet documentation for container security1, FortiGate NGFW can provide the following benefits for securing container infrastructure:
It can inspect north-south traffic between containers and external networks using label aware policies, which allow for dynamic policy enforcement based on Kubernetes labels and metadata. It can integrate with FortiSandbox to provide advanced threat protection for container traffic, by sending suspicious files or URLs to a cloud-based sandbox for analysis and detection.
It can leverage FortiGuard Security Services to provide real-time threat intelligence and updates for container traffic, such as antivirus, web filtering, IPS, and application control. The other options are incorrect because:
FortiGate NGFW cannot be placed between each application container for north-south traffic inspection, as this would create unnecessary complexity and overhead. Instead, FortiGate NGFW can be deployed at the edge of the container network or as a sidecar proxy to inspect traffic at the ingress and egress points.
FortiGate NGFW cannot connect to the worker node and protect the container, as this would not provide sufficient visibility and control over the container traffic. Instead, FortiGate NGFW can leverage the native Kubernetes APIs and services to monitor and secure the container traffic.
1: Fortinet Documentation Library - Container Security

2.You need a solution to safeguard public cloud-hosted web applications from the OWASP Top 10 vulnerabilities. The solution must support the same region in which your applications reside, with minimum traffic cost
Which solution meets the requirements?
A. Use FortiADC
B. Use FortiCNP
C. Use FortiWebCloud
D. Use FortiGate
Answer: C
Explanation:
The correct answer is C. Use FortiWebCloud.
FortiWebCloud is a SaaS cloud-based web application firewall (WAF) that protects public cloud hosted web applications from the OWASP Top 10, zero day threats, and other application layer attacks1. FortiWebCloud also includes robust features such as API discovery and protection, bot mitigation, threat analytics, and advanced reporting2. FortiWebCloud supports multiple regions across the world, and you

can choose the region that is closest to your applications to minimize traffic cost3.
The other options are incorrect because:
FortiADC is an application delivery controller that provides load balancing, acceleration, and security for web applications. It is not a dedicated WAF solution and does not offer the same level of protection as FortiWebCloud4.
FortiCNP is a cloud-native platform that provides security and visibility for containerized applications. It is not a WAF solution and does not protect web applications from the OWASP Top 10 vulnerabilities5.
FortiGate is a next-generation firewall (NGFW) that provides network security and threat prevention. It is not a WAF solution and does not offer the same level of protection as FortiWebCloud for web applications. It also requires additional configuration and management to deploy in the public cloud6.
1: Overview | FortiWeb Cloud 23.3.0 - Fortinet Documentation 2: Web Application Firewall (WAF) & API Protection | Fortinet 3: [FortiWeb Cloud WAF-as-a-Service | Fortinet] 4: [Application Delivery Controller (ADC) | Fortinet] 5: [Fortinet Cloud Native Platform | Fortinet] 6: [FortiGate Next-Generation Firewall (NGFW) | Fortinet]

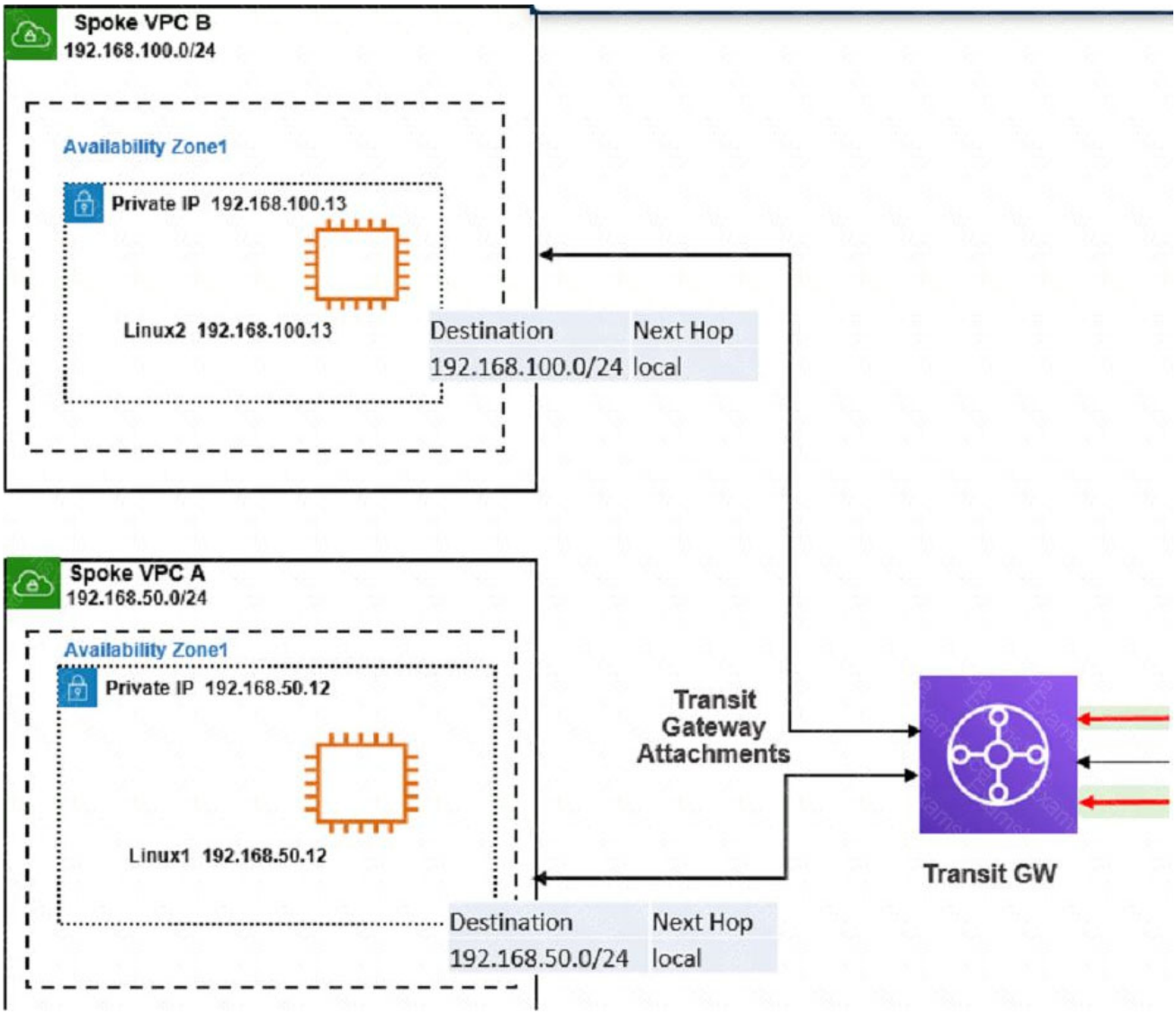
3.Refer to the exhibit



You attempted to access the Linux1 EC2 instance directly from the internet using its public IP address in AWS.
However, your connection is not successful.
Given the network topology, what can be the issue?
A. There is no connection between VPC A and VPC B.
B. There is no elastic IP address attached to FortiGate in the Security VPC.
C. The Transit Gateway BGP IP address is incorrect.
D. There is no internet gateway attached to the Spoke VPC A.
Answer: D
Explanation:
This is because the Linux1 EC2 instance is not accessible directly from the internet using its public IP

address in AWS.
An internet gateway is a horizontally scaled, redundant, and highly available VPC component that allows communication between instances in your VPC and the internet. Without an internet gateway, the Linux1 EC2 instance cannot receive or send traffic to or from the internet, even if it has a public IP address assigned to it.
To fix this issue, you need to attach an internet gateway to the Spoke VPC A and configure a route table that directs internet-bound traffic to the internet gateway. You also need to ensure that the Linux1 EC2 instance has a security group that allows inbound and outbound traffic on the desired ports.
: [Internet Gateways - Amazon Virtual Private Cloud] : [Attach an Internet Gateway to Your VPC - Amazon Virtual Private Cloud] : [Security Groups for Your VPC - Amazon Virtual Private Cloud]

4.Refer to the exhibit



The exhibit shows a customer deployment of two Linux instances and their main routing table in Amazon Web Services (AWS). The customer also created a Transit Gateway (TGW) and two attachments
Which two steps are required to route traffic from Linux instances to the TGWQ (Choose two.)
A. In the TGW route table, add route propagation to 192.168.0 0/16
B. In the main subnet routing table in VPC A and B, add a new route with destination 0_0.0.0/0, next hop

Internet gateway (IGW).
C. In the TGW route table, associate two attachments.
D. In the main subnet routing table in VPC A and B, add a new route with destination 0_0.0.0/0, next hop TGW.
Answer: CD
Explanation:
According to the AWS documentation for Transit Gateway, a Transit Gateway is a network transit hub that connects VPCs and on-premises networks.
To route traffic from Linux instances to the TGW, you need to do the following steps:
In the TGW route table, associate two attachments. An attachment is a resource that connects a VPC or VPN to a Transit Gateway. By associating the attachments to the TGW route table, you enable the TGW to route traffic between the VPCs and the VPN.
In the main subnet routing table in VPC A and B, add a new route with destination 0_0.0.0/0, next hop TGW. This route directs all traffic from the Linux instances to the TGW, which can then forward it to the appropriate destination based on the TGW route table. The other options are incorrect because:
In the TGW route table, adding route propagation to 192.168.0 0/16 is not necessary, as this is already the default route for the TGW. Route propagation allows you to automatically propagate routes from your VPC or VPN to your TGW route table.
In the main subnet routing table in VPC A and B, adding a new route with destination 0_0.0.0/0, next hop Internet gateway (IGW) is not correct, as this would bypass the TGW and send all traffic directly to the internet. An IGW is a VPC component that enables communication between instances in your VPC and the internet.
: [Transit Gateways - Amazon Virtual Private Cloud]

5.Which two attachments are necessary to connect a transit gateway to an existing VPC with BGP? (Choose two)
A. A transport attachment
B. A BGP attachment
C. A connect attachment
D. A GRE attachment
Answer: AC
Explanation:
The correct answer is A and C. A transport attachment and a connect attachment are necessary to connect a transit gateway to an existing VPC with BGP.
According to the AWS documentation for Transit Gateway, a transit gateway is a network transit hub that connects VPCs and on-premises networks. To connect a transit gateway to an existing VPC with BGP, you need to do the following steps:
Create a transport attachment. A transport attachment is a resource that connects a VPC or VPN to a transit gateway. You can specify the BGP options for the transport attachment, such as the autonomous system number (ASN) and the BGP peer IP address.
Create a connect attachment. A connect attachment is a resource that enables you to use your own appliance to provide network services for traffic that flows through the transit gateway. You can use a connect attachment to route traffic between the transport attachment and your appliance using GRE tunnels and BGP.

The other options are incorrect because:
A BGP attachment is not a valid type of attachment for a transit gateway. BGP is a protocol that enables dynamic routing between the transit gateway and the VPC or VPN.
A GRE attachment is not a valid type of attachment for a transit gateway. GRE is a protocol that encapsulates packets for tunneling purposes. GRE tunnels are established between the connect attachment and your appliance.
: [Transit Gateways - Amazon Virtual Private Cloud] : [Transit Gateway Connect - Amazon Virtual Private Cloud]