Vendor: Fortinet

Exam Code: NSE7_PBC-7.2

Exam Name: Fortinet NSE 7 - Public Cloud Security 7.2

Version: DEMO

QUESTION 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:
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 security, 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.

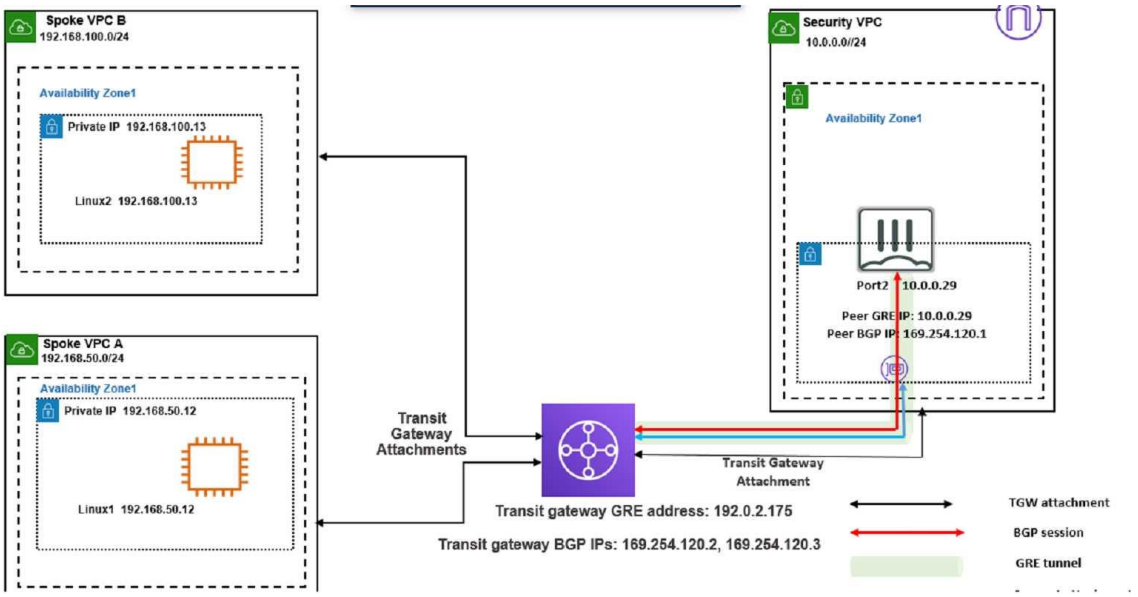
QUESTION 2
You need a solution to safeguard public cloud-hosted web applications from the OWASP Top 10 vulnerabilities. The solution must support the same region in which your applications reside, with minimum traffic cost.

Which solution meets the requirements?

A. Use FortiADC
B. Use FortiCNP
C. Use FortiWebCloud
D. Use FortiGate

Answer: C
Explanation:
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 attacks. FortiWebCloud also includes robust features such as API discovery and protection, bot mitigation, threat analytics, and advanced reporting. FortiWebCloud supports multiple regions across the world, and you can choose the region that is closest to your applications to minimize traffic cost.

QUESTION 3
Refer to the exhibit. You attempted to access the Linux1 EC2 instance directly from the internet using its public IP address in AWS.



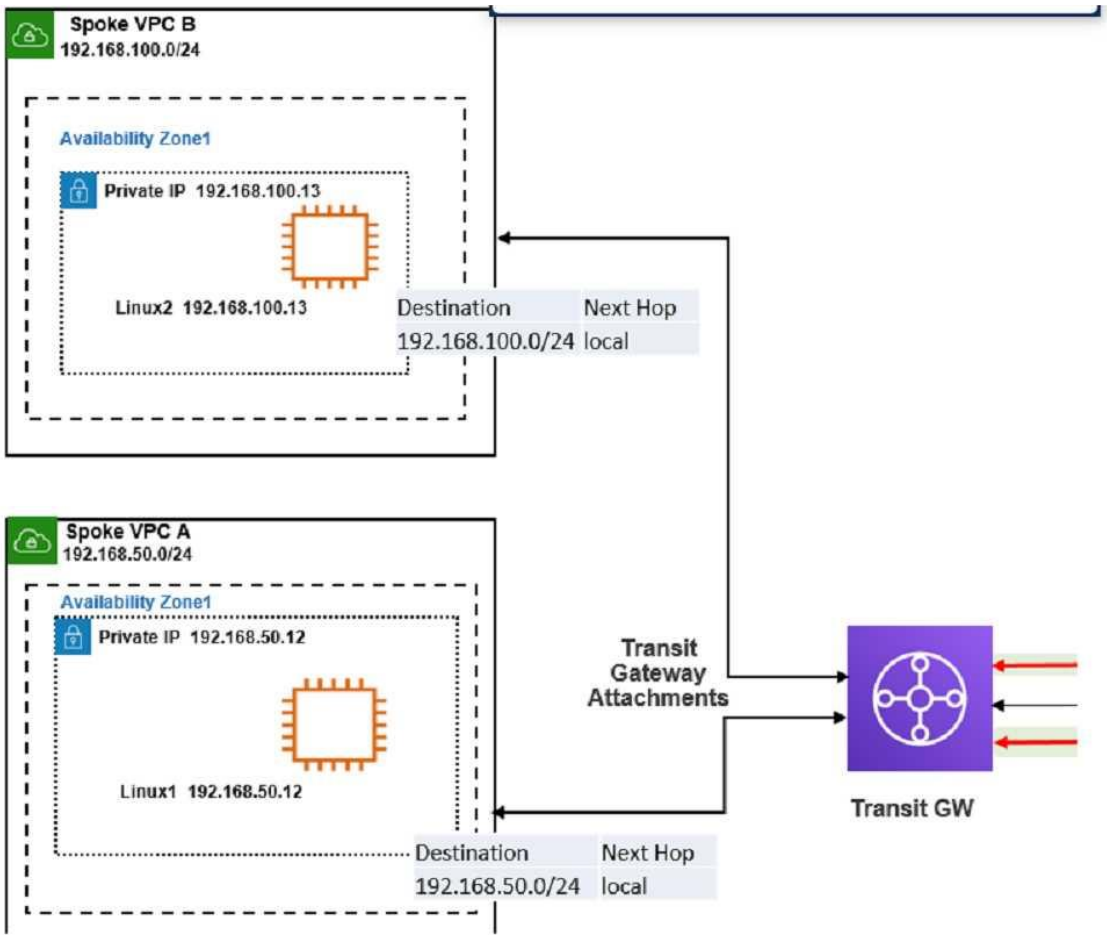
However, your connection is not successful.

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.

QUESTION 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.

QUESTION 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:
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.

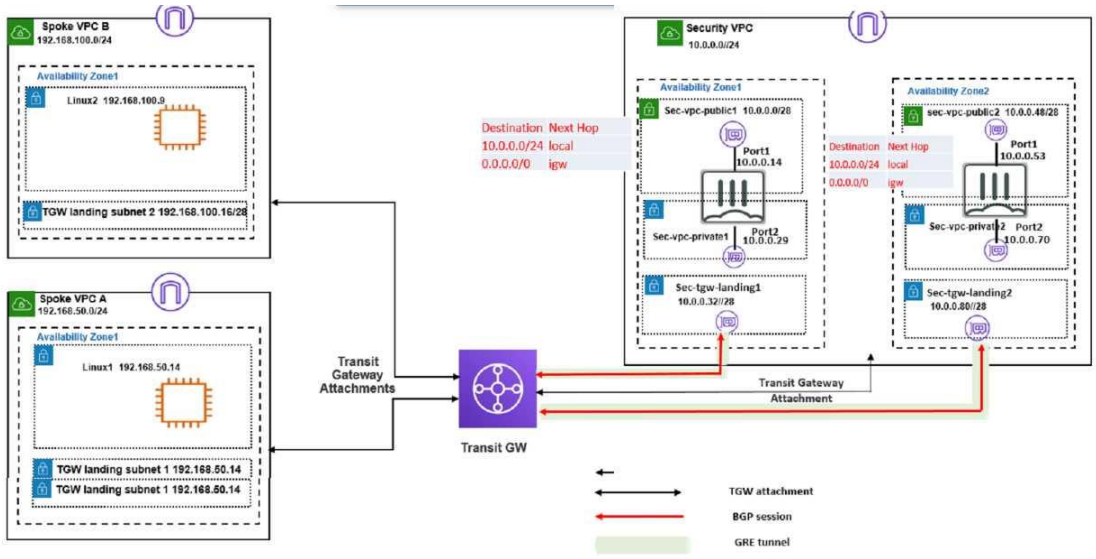
QUESTION 6
You have created a TGW route table to route traffic from your spoke VPC to the security VPC where two FortiGate devices are inspecting traffic. Your spoke VPC CIDR block is already propagated to the Transit Gateway (TGW) route table.

Which type of attachment should you use to advertise routes through BGP from the spoke VPC to the security VPC?

A. Connect attachment
B. VPC attachment
C. Route attachment
D. GRE attachment

Answer: B
Explanation:
A VPC attachment is the type of attachment that allows you to connect a VPC to a TGW and advertise routes through BGP. A VPC attachment creates a VPN connection between the VPC and the TGW, and enables dynamic routing with BGP. A connect attachment is used to connect a VPN or Direct Connect gateway to a TGW. A route attachment is not a valid type of attachment for TGW. A GRE attachment is used to connect a FortiGate device to a TGW using GRE tunnels.

QUESTION 7
Refer to the exhibit. A customer has deployed an environment in Amazon Web Services (AWS) and is now trying to send outbound traffic from the Linux1 and Linux2 instances to the internet through the security VPC (virtual private cloud). The FortiGate policies are configured to allow all outbound traffic; however, the traffic is not reaching the FortiGate internal interface. Assume there are no issues with the Transit Gateway (TGW) configuration.



Which two settings must the customer add to correct the issue? (Choose two.)

A. Both landing subnets in the spoke VPCs must have a 0.0.0.0/0 traffic route to the Internet Gateway (IOW).
B. Both landing subnets in the spoke VPCs must have a 0.0.0.0/0 traffic route to the TGW
C. Both landing subnets in the security VPC must have a 0.0.0.0/0 traffic route to the FortiGate port2.
D. The four landing subnets in all the VPCs must have a 0.0.0.0/0 traffic route to the TGW

Answer: BC
Explanation:
The correct answer is B and C. Both landing subnets in the spoke VPCs must have a 0.0.0.0/0 traffic route to the TGW. Both landing subnets in the security VPC must have a 0.0.0.0/0 traffic route to the FortiGate port2.
According to the AWS documentation for Transit Gateway, a transit gateway is a network transit hub that connects VPCs and on-premises networks. To send outbound traffic from the Linux instances to the internet through the security VPC, you need to do the following steps:
In the main subnet routing table in the spoke VPCs, 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. In the main subnet routing table in the security VPC, add a new route with destination 0.0.0.0/0, next hop FortiGate port2. This route directs all traffic from the TGW to the FortiGate internal interface, where it can be inspected and allowed by the FortiGate policies.

QUESTION 8
Which two Amazon Web Services (AWS) features support east-west traffic inspection within the AWS cloud by the FortiGate VM? (Choose two.)

A. A NAT gateway with an EIP
B. A transit gateway with an attachment
C. An Internet gateway with an EIP
D. A transit VPC

Answer: BD

Explanation:
A transit gateway with an attachment and a transit VPC support east- west traffic inspection within the AWS cloud by the FortiGate VM. According to the Fortinet documentation for Public Cloud Security, a transit gateway is a network transit hub that connects VPCs and on-premises networks. A transit gateway attachment is a resource that connects a VPC or VPN to a transit gateway. By using a transit gateway with an attachment, you can route traffic from your spoke VPCs to your security VPC, where the FortiGate VM can inspect the traffic.
A transit VPC is a VPC that serves as a global network transit center for connecting multiple VPCs, remote networks, and virtual private networks (VPNs). By using a transit VPC, you can deploy the FortiGate VM as a virtual appliance that provides network security and threat prevention for your VPCs.

QUESTION 9
Which statement about Transit Gateway (TGW) in Amazon Web Services (AWS) is true?

A. TGW can have multiple TGW route tables.
B. Both the TGW attachment and propagation must be in the same TGW route table
C. A TGW attachment can be associated with multiple TGW route tables.
D. The TGW default route table cannot be disabled.

Answer: A
Explanation:
A transit gateway is a network transit hub that connects VPCs and on-premises networks. A transit gateway route table is a set of rules that determines how traffic is routed among the attachments to the transit gateway. A transit gateway can have multiple route tables, and you can associate different attachments with different route tables. This allows you to control how traffic is routed between your VPCs and VPNs based on your network design and security requirements.

QUESTION 10
You are adding more spoke VPCs to an existing hub and spoke topology. Your goal is to finish this task in the minimum amount of time without making errors.

Which Amazon AWS services must you subscribe to accomplish your goal?

A. GuardDuty, CloudWatch
B. WAF, DynamoDB
C. Inspector, S3
D. CloudWatch, S3

Answer: D
Explanation:
According to the GitHub repository for the Fortinet aws-lambda-tgw script, this function requires the following AWS services:
CloudWatch: A monitoring and observability service that collects and processes events from various AWS resources, including Transit Gateway attachments and route tables.
S3: A scalable object storage service that can store the configuration files and logs generated by the Lambda function.

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.lead2pass.com/all-products.html

10% Discount Coupon Code: **ASTR14**