Free Questions for NSE7_PBC-7.2 by certsinside

Shared by Mcpherson on 09-08-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

You are adding a new spoke to the existing transit VPC environment using the AWS Cloud Formation template. Which two components must you use for this deployment? (Choose two.)

Options:

A- The OSPF AS value used for the hub.

B- The Amazon CloudWatch tag value.

C- The BGPASN value used for the transit VPC.

D- The tag value of the spoke

Answer:

C, D

Explanation:

When using an AWS CloudFormation template to add a new spoke to an existing transit VPC environment, the necessary components are:

The BGPASN value used for the transit VPC (Option C): BGP Autonomous System Number (ASN) is required for setting up BGP routing between the transit VPC and the new spoke. This number uniquely identifies the system in BGP routing and is crucial for correct routing and avoiding routing conflicts.

The tag value of the spoke (Option D): Tags in AWS are used to identify and manage resources. The tag value assigned to a spoke VPC helps in organizing, managing, and locating the VPC within the larger AWS environment. Tags are essential for automation scripts and policies that depend on specific identifiers to apply configurations or rules.

Question 2

Question Type: **MultipleChoice**

Which two Amazon Web Services (AWS) features do you use for the transit virtual private cloud (VPC) automation process to add new spoke N/PCs? (Choose two)

Options:

A- Amazon S3 bucket

B- AWS Security Hub

C- AWS Transit Gateway

D- Amazon CloudWatch

Answer:

C, D

Explanation:

For automating the process of adding new spoke VPCs in a transit VPC architecture within Amazon Web Services (AWS), the two relevant features are:

AWS Transit Gateway (Option C): This service is crucial for managing connectivity between VPCs and other networks without routing traffic through the public internet. It acts as a hub that controls how traffic is routed among all the connected networks, which simplifies network management and minimizes latency.

Amazon CloudWatch (Option D): CloudWatch provides monitoring and observability services that are essential for managing the health and performance of the AWS infrastructure, including Transit Gateways. It allows administrators to set alarms and react to changes in AWS resources, which is vital for the dynamic addition and integration of new spoke VPCs into the transit VPC architecture.

Question 3

Question Type: MultipleChoice

In an SD-WAN TGW Connect topology, which three initial steps are mandatory when routing traffic from a spoke VPC to a security VPC through a Transit Gateway? (Choose three.)

Options:

A- From the spoke VPC internal routing table, point 0.0.0.0/0 traffic to the TGW

B- From the security VPC TGW subnet routing table: point 0.0.0.0/0 traffic to the FortiGate internal port

C- From the security VPC TGW subnet routing table: point 0.0.0.0/0 traffic to the TGW

D- From the security VPC FortiGate internal subnet routing table, point 0.0.0.0/0 traffic to the TGW

E- From both spoke VPCs and the security VPC, point 0.0.0.0/0 traffic to the Internet Gateway

Answer:

A, B, D

Explanation:

Spoke VPC Routing:The 0.0.0.0/0 (default) route in the spoke VPC must point to the Transit Gateway attachment for traffic to reach other VPCs or external destinations.

Security VPC Routing:Traffic from the security VPC needs to pass through the FortiGate for inspection and security controls. Therefore, the 0.0.0.0/0 route in the security VPC's TGW subnet routing table must point to the FortiGate's internal port.

FortiGate Routing:The FortiGate's internal subnet must have its 0.0.0.0/0 route configured to point to the Transit Gateway attachment, allowing traffic to be returned to other VPCs or reach the internet.

In an SD-WAN TGW Connect topology, when routing traffic from a spoke VPC to a security VPC through a Transit Gateway, the mandatory initial steps include:

From the spoke VPC internal routing table, point 0.0.0.0/0 traffic to the TGW (Option A): This step is crucial for ensuring that all traffic from the spoke VPC destined for external networks is directed through the Transit Gateway, allowing for centralized management and security inspection.

From the security VPC TGW subnet routing table: point 0.0.0.0/0 traffic to the FortiGate internal port (Option B): Routing all traffic from the TGW subnet in the security VPC to the FortiGate's internal port ensures that traffic is subjected to the necessary security policies and inspections provided by the FortiGate appliance before it proceeds to other destinations or returns to the spoke VPCs.

From the security VPC FortiGate internal subnet routing table, point 0.0.0.0/0 traffic to the TGW (Option D): This configuration ensures that traffic returning from the security processes handled by the FortiGate is routed back through the Transit Gateway, maintaining the integrity of the secure transit path and ensuring proper routing back to the originating spoke or onward to the internet.

Question 4

Question Type: MultipleChoice

Which two statements are true about Transit Gateway Connect peers in anlPv4 BGP configuration'? (Choose two.)

Options:

A- The inside CIDR blocks are used for BGP peering

B- You cannot use IPv6 addresses

C- You must specify a /29CIDR block from the 169.254.0.0/16 range

D- You must configure the second address from the IPv4 range on the device as the BGP IP address

Answer:

A, C

Explanation:

For Transit Gateway Connect peers in an IPv4 BGP configuration, the correct statements are:

The inside CIDR blocks are used for BGP peering (Option A): In a BGP configuration for Transit Gateway Connect, the inside CIDR blocks, typically within the 169.254.0.0/16 range, are designated for the BGP peering connections. These blocks are reserved for internal network protocols and are commonly used in AWS for automatic IP address assignment within managed networking services.

You must specify a /29 CIDR block from the 169.254.0.0/16 range (Option C): It is a requirement to specify a /29 CIDR block within the 169.254.0.0/16 range for setting up the network interfaces that facilitate BGP peering. This specific range allows for the necessary number of IP addresses to establish BGP sessions effectively between the transit gateway and on-premises or other virtual appliances.

Question 5

Question Type: **MultipleChoice**

What kind of underlying mechanism does Transit Gateway Connect use to send traffic from the virtual private cloud (VPC) to the transit gateway?

Options:

A- A BGP attachment

B- A GRE attachment

C- A transport attachment

D- Transit Gateway Connect attachment

Answer:

D

Explanation:

Transit Gateway Connect Specificity:AWS Transit Gateway Connect is a specific feature designed to streamline the integration of SD-WAN appliances and third-party virtual appliances into your Transit Gateway.expand_moreIt utilizes a specialized attachment type.exclamation

BGP's Role:While Transit Gateway Connect attachments leverage BGP for dynamic routing, BGP itself is a routing protocol and not the core connectivity mechanism in this context.

GRE Tunneling:GRE is a tunneling protocol commonly used with Transit Gateway Connect attachments to encapsulate traffic.

Question 6

Question Type: **MultipleChoice**

An administrator is looking for a solution that can provide insight into users and data stored in major SaaS applications in the multicloud environment Which product should the administrator deploy to have secure access to SaaS applications?

Options:

A- FortiProxy

B- FortiSandbox

C- ForliCASB

D- FortiWeb

Answer:

C

Explanation:

For administrators seeking to gain insights into user activities and data within major SaaS applications across multicloud environments, deploying FortiCASB (Cloud Access Security Broker) is the most effective solution (Option C).

Role of FortiCASB: FortiCASB is specifically designed to provide security visibility, compliance, data security, and threat protection for cloud-based services. It acts as a mediator between users and cloud service providers, offering deep visibility into the operations and data handled by SaaS applications.

Capabilities of FortiCASB: This product enables administrators to monitor and control the access and usage of SaaS applications. It helps in assessing security configurations, tracking user activities, and evaluating data movement across the cloud services. By doing so, it assists organizations in enforcing security policies, detecting anomalous behaviors, and ensuring compliance with regulatory standards.

Integration and Functionality: FortiCASB integrates seamlessly with major SaaS platforms, providing a centralized management interface that allows for comprehensive analysis and real-time protection measures. This integration ensures that organizations can maintain control over their data across various cloud services, enhancing the overall security posture in a multicloud environment.

Question 7

Question Type: **MultipleChoice**

What is the main advantage of using SD-WAN Transit Gateway Connect over traditional SD-WAN?

Options:

A- It eliminates the use of ECMP

B- You can use GRE-based tunnel attachments

C- You can combine it with IPsec to achieve higher bandwidth

D- You can use BGP over IPsec for maximum throughput

Answer:

B

Explanation:

Simplified and Scalable Connectivity:Transit Gateway Connect allows you to establish GRE tunnels to your SD-WAN appliances natively within the AWS network. This eliminates the complexity of managing individual IPsec VPN connections, especially as your cloud presence grows.

Potential for Enhanced Performance:GRE offers lower overhead compared to IPsec, which can result in higher throughput for bandwidth-intensive SD-WAN applications.

Flexibility:While IPsec is supported for scenarios requiring strong encryption, the focus on GRE highlights the performance and scalability benefits that are often prioritized when integrating SD-WAN with AWS.

Dynamic Routing:The integration with BGP further streamlines network management by automating route updates and distribution.

Addressing the IPsec Consideration:

It's important to acknowledge that SD-WAN Transit Gateway Connect does support IPsec. If your question is specifically framed within the context of Fortinet's FCSS 7.2 materials and they emphasize the hybrid usage of GRE and IPsec, then a modified answer might be appropriate: