Fortinet NSE7_CDS_AR-7.6 NSE 7 Practice Questions

Shared by Lawrence on 17-08-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

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

Options:

A- You can use BGP over IPsec for maximum throughput.
B- You can combine it with IPsec to achieve higher bandwidth.
C- It eliminates the use of ECMP.
D- You can use GRE-based tunnel attachments.

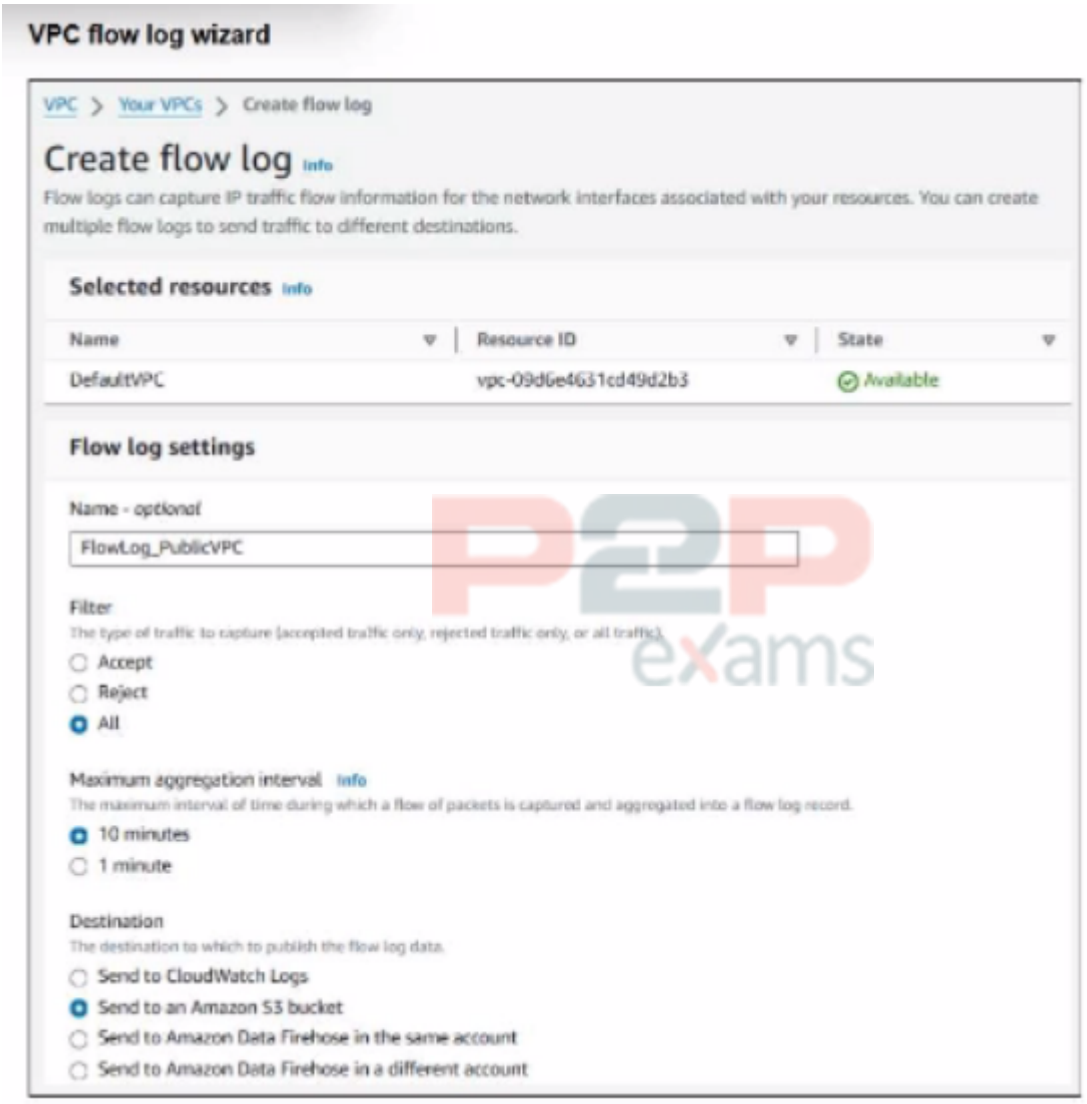
Answer:

D

Question 2

Question Type: MultipleChoice

Refer to the exhibit.



An experienced AWS administrator is creating a new virtual public cloud (VPC) flow log with the settings shown in the exhibit.

What is the purpose of this configuration?

Options:

A- To maximize the number of logs saved
B- To monitor logs in real time
C- To retain logs for a long term
D- To troubleshoot a log flow issue

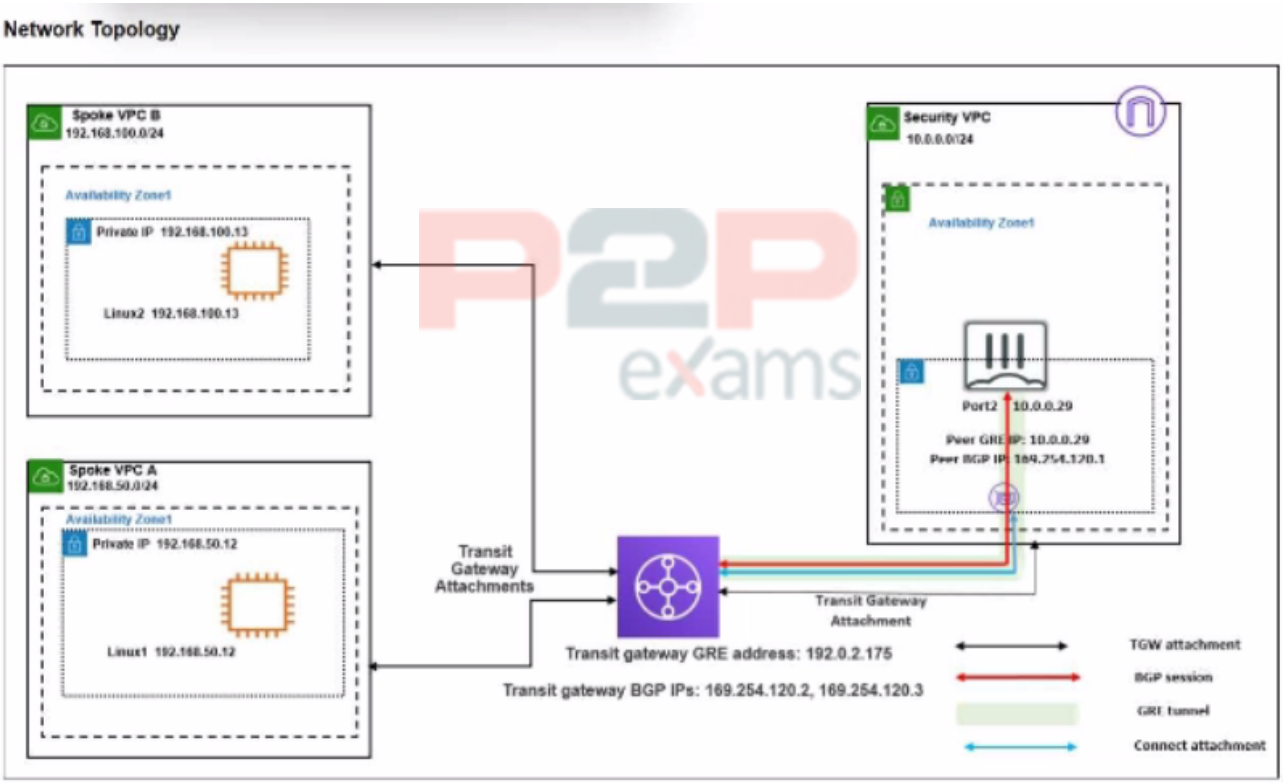
Answer:

C

Question 3

Question Type: MultipleChoice

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?

Options:

A- There is no connection between VPC A and VPC B.
B- There is no internet gateway attached to the Spoke VPC A.
C- The Transit Gateway BGP IP address is incorrect.
D- There is no elastic IP address attached to FortiGate in the Security VPC.

Answer:

B

Explanation:

The Fortinet documentation states: 'An IGW in AWS is a VPC component that allows

communication between instances in your VPC and the internet... AWS users with less experience may face connectivity issues if they create a new VPC, add EC2 instances to it, but forget that they need an IGW for internet connectivity.'

Question 4

Question Type: MultipleChoice

An administrator is relying on an Azure Bicep linter to find possible issues in Bicep files.

Which problem can the administrator expect to find?

Options:

A- The resources to be deployed exceed the quota for a region.
B- Some resources are missing dependsOn statements.
C- There are output statements that contain passwords.
D- One or more modules are not using runtime values as parameters.

Answer:

B

Question 5

Question Type: MultipleChoice

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 infrastructures? (Select two.)

Options:

A- FortiGate NGFW can inspect north-south container traffic with label aware policies.
B- FortiGate NGFW and FortiWeb can be used to secure container traffic.
C- FortiGate NGFW can connect to the worker nodes and protect the containers.
D- FortiGate NGFW can be placed between each application container for north-south traffic inspection.

Answer:

A, B

Question 6

Question Type: MultipleChoice

A customer would like to use FortiGate fabric integration with FortiCNP. When adding a FortiGate VM to FortiCNP, which three mandatory configuration steps must you follow on FortiGate? (Select three answers)

Options:

A- Enable pre-shared key on both sides.
B- Import the FortiGate certificate into FortiCNP.
C- Configure FortiGate to send logs to FortiCNP.
D- Create an IPS sensor and a firewall policy.
E- Create an SSL/SSH inspection profile.

Answer:

C, D, E

Explanation:

Comprehensive and Detailed Explanation From FortiOS 7.6, FortiWeb 7.4 Exact Extract study guide:

According to the FortiCNP 24.x Administration Guide and the FortiOS 7.6 Security Fabric Integration documentation, integrating a FortiGate-VM with FortiCNP requires specific local configurations on the FortiGate to ensure the cloud security platform can ingest and analyze traffic data.

Configuring Logging (Option C): Before adding the FortiGate VM to FortiCNP, the administrator must Enable Send Logs on the FortiGate. This allows the FortiGate to forward the necessary security telemetry and traffic logs to the FortiCNP cloud endpoint for threat correlation and risk analysis.

Policy and Inspection Setup (Option D): The integration relies on the FortiGate's ability to identify and block threats at the network layer. Specifically, the administrator must Create a FortiGate IPS Sensor and Create a FortiGate Firewall Policy. The IPS sensor detects malicious patterns, while the firewall policy dictates which traffic is subjected to this inspection.

Deep Packet Inspection (Option E): To provide visibility into encrypted traffic---which is critical

for identifying threats hidden in HTTPS flows---the administrator must Create an SSL/SSH Inspection Profile on the FortiGate. Without this profile, FortiCNP would lose significant visibility into potential attack vectors utilizing encrypted channels.

Why other options are incorrect:

Option A: While pre-shared keys are used in VPN and some Fabric setups, they are not listed as one of the specific mandatory steps for the initial FortiGate-to-FortiCNP fabric integration workflow.

Option B: While certificate exchange is part of the overall trust relationship, the primary 'mandatory configuration steps on FortiGate' defined in the official setup guide focus on the logging and security profile components required to generate the data FortiCNP needs.

Question 7

Question Type: MultipleChoice

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

Options:

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

Answer:

B

Explanation:

According to the FortiOS 7.6 AWS Administration Guide and the Fortinet Public Cloud Security 7.4 training materials regarding centralized security inspection:

Multiple Route Tables (Option B): A single AWS Transit Gateway is designed to support multiple TGW route tables. By default, there is a soft limit of 20 route tables per Transit Gateway, which allows administrators to implement sophisticated network segmentation and granular routing policies. In a FortiGate-centric 'Security Hub' or 'Transit VPC' architecture, multiple route tables are used to separate 'Spoke' traffic from 'Security' traffic, ensuring all inter-VPC traffic is forced through the FortiGate-VM for inspection.

Associations and Propagations: * Association: Each individual TGW attachment (VPC, VPN, or Direct Connect) can be associated with exactly one TGW route table at any given time. This table dictates where packets coming from that attachment will be sent. Because of this 1:1 relationship, Option C is incorrect.

Propagation: An attachment can propagate its routes to one or many TGW route tables. This flexibility allows a VPC's prefix to be known in multiple routing domains, meaning that association and propagation do not need to occur in the same table, making Option A incorrect.

Default Route Table Management: When creating an AWS Transit Gateway, the options for 'Default route table association' and 'Default route table propagation' are enabled by default, but they can be disabled during or after creation. Disabling these is a security best practice when deploying FortiGate-VMs to prevent the TGW from automatically creating a 'full-mesh' connectivity that bypasses the firewall, making Option D incorrect.

Question 8

Question Type: MultipleChoice

Refer to the exhibit.

Which FortiCNP policy type generated the finding shown in the exhibit? (Choose one answer)

Options:

A- This finding was generated by a data scan policy.
B- This finding was generated by a threat detection policy.
C- This finding was generated by a risk management policy.
D- This finding was generated by a file collection policy.

Answer:

B

Explanation:

Comprehensive and Detailed Explanation From FortiOS 7.6, FortiWeb 7.4 Exact Extract study guide:

Based on the FortiCNP 22.4/24.4 Administration Guide and the Fortinet Cloud Security Study Guide, findings in FortiCNP are categorized by the specific policy type that triggered the alert.

Threat Detection Policy (Option B): This policy category is designed to monitor and alert on anomalous User Activity and Network threats. Specifically, 'Suspicious Location' is a predefined threat detection rule that triggers when a user performs an action (such as a Download File as seen in the exhibit) from a geographic location or IP address that is not on the organization's allow list or deviates from established behavioral baselines. The exhibit explicitly shows the 'Activity Type' as 'Download File' and the 'Policy Name' as 'Suspicious Location,' both of which fall under the Threat Detection > User Activity policy tab.

Policy Hierarchy and Finding Types:

Threat Detection: Includes User Activity (Suspicious Location, Suspicious Time, Suspicious Movement) and Network findings.

Data Scan Policy (Option A): These policies are used for content-level inspection, such as searching for Malware or Data Loss Prevention (DLP) patterns like credit card numbers within files.

Risk Management Policy (Option C): These policies focus on Cloud Security Posture Management (CSPM), alerting on misconfigurations such as unencrypted buckets or disabled logging (e.g., CloudTrail).

File Collection (Option D): While 'File Collection' is a configuration object used to define a group of files for monitoring, it is not the policy type that generates a behavioral alert like 'Suspicious Location'.

Question 9

Question Type: MultipleChoice

You have deployed a FortiGate HA cluster in Azure using a gateway load balancer for traffic inspection. However, traffic is not being routed correctly through the firewalls.

What can be the cause of the issue?

Options:

A- The FortiNet VMs have IP forwarding disabled, which is required for traffic inspection.
B- The health probes for the gateway load balancer are failing, which causes traffic to bypass the HA cluster.
C- The gateway load balancer is not associated with the correct network security group (NSG) rules, which allow traffic to pass through.
D- The protected VMs are in a different Azure subscription, which prevents the gateway load balancer from forwarding traffic.

Answer:

A

Explanation:

According to the FortiOS 7.6 Azure Administration Guide and the Cloud Security 7.4 Public Cloud Study Guide, the integration of FortiGate-VMs with an Azure Gateway Load Balancer (GWLB) requires specific network configurations to ensure packet transit:

IP Forwarding Requirement (Option A): By default, Azure Network Interfaces (NICs) drop any traffic that does not originate from or is not destined for the IP address assigned to that NIC. For a FortiGate to act as a 'bump-in-the-wire' or transparent inspector, it must receive traffic destined for other IPs and forward it. This requires the IP Forwarding setting to be explicitly enabled on the FortiGate's network interfaces within the Azure portal. If this is disabled, the Azure fabric will discard the traffic being steered through the FortiGate HA cluster by the GWLB.

VXLAN Encapsulation: The Azure GWLB uses VXLAN to encapsulate traffic (adding a VXLAN header with a specific VNI) before sending it to the FortiGate. The FortiGate must terminate this VXLAN tunnel. While the VXLAN configuration is crucial, the underlying infrastructure check for IP Forwarding is the most common cause of traffic being blocked at the NIC level before the FortiOS stack can process the packet.

Why other options are incorrect:

Option B: If health probes fail, the GWLB will typically stop sending traffic to that specific instance. While this affects the HA cluster's availability, the question states traffic is not being routed correctly through the firewalls (implying an active flow issue), and the primary mechanism for allowing a VM to process third-party traffic in Azure is IP Forwarding.

Option C: NSGs are typically applied to the NIC or Subnet. While incorrect NSG rules can block traffic, 'IP Forwarding' is a specific requirement for the FortiGate to function as a network appliance (NVA) regardless of the NSG state.

Option D: Azure GWLB supports cross-subscription and cross-tenant chaining. The consumer (protected VMs) and the provider (FortiGate HA cluster) do not need to be in the same subscription, provided the GWLB endpoint is correctly mapped.