KaozhengPro

IT認證考試題庫

專業平臺

考證寶提供最新考古題與模擬試題
協助您高效通過認證考試

www.kaozhengpro.com

Exam : **NSE7_FSN_AR-7.6**

Title : Fortinet NSE 7 - Secure Networking 7.6 Architect

Version : DEMO

1.An architect is deploying a high-traffic volume data center and opts to use the FortiGate Session Life Support Protocol (FGSP) to synchronize sessions between two standalone FortiGate devices. Due to asymmetric routing, traffic enters the network through one device and exits through the other.
Which statement accurately describes a critical requirement or limitation of FGSP in this specific environment?
A. IPsec VPN tunnels are automatically fully synchronized by default, ensuring seamless failover without requiring any re-negotiation.
B. FGSP includes built-in configuration synchronization, meaning administrators only need to manage policies on the primary node.
C. Both FortiGate devices must be configured with identical routing tables and security policies to process the asymmetric traffic correctly.
D. A dedicated hardware heartbeat interface is mandatory to elect the primary and secondary roles before synchronization can begin.
Answer: C
Explanation:
➪ Core Concept: FGSP standalone synchronization and asymmetric traffic handling.
➪ Analysis: Unlike FGCP (which operates as a strict cluster with a master/slave dynamic and automatic configuration sync), FGSP synchronizes sessions between standalone devices. Because the devices are standalone, configuration is *not* automatically synced. For symmetric or asymmetric traffic to be allowed and processed correctly across both peers, the underlying routing tables, firewall policies, and inspection profiles must perfectly match on both units.
Option A is incorrect because IPsec synchronization has specific requirements and limitations in FGSP.
Option B is incorrect as configuration sync must be handled via FortiManager or manual replication.
Option D describes FGCP, not FGSP.
➪ CLI /Reference: config system standalone-cluster and config system session-sync.

2.An enterprise is implementing the Fortinet Security Fabric to enhance its incident response capabilities. The architect wants to configure an Automation Stitch that automatically quarantines an endpoint at the switch port level when a high-severity Indicator of Compromise (IoC) is detected.
Which of the following is a mandatory prerequisite for this specific IoC trigger to function?
A. FortiAnalyzer must be actively integrated into the Security Fabric to provide the threat database and trigger the IoC event.
B. The upstream core router must support dynamic BGP routing in order to actively isolate the infected subnet via route maps.
C. A third-party webhook API must be deployed locally to interpret the telemetry data before passing it to the FortiSwitch.
D. A FortiGate active-active (FGCP) cluster is required at the edge to ensure the Automation Stitch avoids false positive detections.
Answer: A
Explanation:
➪ Core Concept: Automation Stitches and Security Fabric IoC detection.
➪ Analysis: In the Fortinet Security Fabric, FortiGate heavily relies on FortiAnalyzer to collect, analyze, and detect Indicators of Compromise (IoCs) based on threat intelligence. The Automation Stitch trigger for an IoC event specifically requires FortiAnalyzer to be part of the Fabric to identify the compromised

host and fire the trigger to the root FortiGate.
Options B and C are technically irrelevant to the native Automation Stitch mechanics.
Option D is incorrect; clustering is an availability feature, not a prerequisite for IoC detection logic.
⇨ CLI /Reference: Security Fabric GUI -> Automation -> Trigger: FortiAnalyzer Event (IoC).

3.A company is deploying SD-WAN Direct Internet Access (DIA) to offload internet-bound SaaS traffic from their costly MPLS links. The architecture requires that if the latency of the primary DIA link exceeds 40ms, the SaaS traffic must automatically fail over to a secondary backup broadband link.
Which SD-WAN component is specifically responsible for enforcing this failover condition?
A. A dynamically adjusted SD-WAN static route with a higher priority metric.
B. A Performance SLA configured in conjunction with an SD-WAN rule.
C. A BGP neighbor group configured with an aggressive hold-time route map.
D. A standard firewall policy with the action set to traffic-shaping enforcement.
Answer: B
Explanation:
⇨ Core Concept: SD-WAN Direct Internet Access (DIA) best practices and use cases.
⇨ Analysis: The core of Fortinet SD-WAN's dynamic path selection is the integration of Performance SLAs (Health Checks) with SD-WAN rules (Services). The Performance SLA actively monitors the latency, jitter, and packet loss of the links. The SD-WAN rule utilizes this telemetry to steer traffic based on the defined strategy (e.g., Maximum Bandwidth, Lowest Cost (SLA), or Best Quality).
Option A is incorrect because static routes do not monitor real-time latency.
Option C is a routing protocol feature, not native SD-WAN traffic steering.
Option D manages bandwidth allocation, not link failover.
⇨ CLI /Reference: config system sdwan -> config health-check (SLA) and config service (SD-WAN Rule).

4.Examine the following CLI output for a branch office SD-WAN configuration:

```
config system sdwan
    set load-balance-mode measured-volume-based
    config members
        edit 1
            set interface "port1"
            set volume-ratio 70
        next
        edit 2
            set interface "port2"
            set volume-ratio 30
        next
    end
end
```

Based on this configuration, how will the FortiGate distribute traffic across the SD-WAN members?
A. It calculates the real-time bandwidth utilization on both interfaces and dynamically adjusts the ratio to maintain equilibrium.
B. It requires an active Performance SLA integrated with FortiAnalyzer to distribute traffic according to

the configured volume ratios.
C. It allocates the first 70 concurrent sessions to port1 and the subsequent 30 sessions to port2 sequentially.
D. It tracks the amount of traffic in bytes and distributes new sessions so the total volume matches the 70:30 ratio.
Answer: D
Explanation:
➪ Core Concept: SD-WAN traffic distribution and load balancing modes.
➪ Analysis: The measured-volume-based load balancing mode does not balance based on the sheer *number* of sessions (which would be session-based or weight-based), but rather on the actual data volume (bytes) transferred. The FortiGate continuously tracks the traffic volume on the interfaces and attempts to assign new sessions to the interfaces in a way that keeps the overall byte distribution at the specified 70:30 ratio.
Option C describes a session-based approach.
Option A describes a bandwidth-utilization approach (spillover or similar dynamic algorithms).
Option B is a distractor.
➪ CLI /Reference: config system sdwan -> set load-balance-mode measured-volume-based.

5.An architect is designing a highly available enterprise network using FortiGate Clustering Protocol (FGCP) in an Active-Passive setup. The cluster spans two distinct data centers (Stretched HA) interconnected via a Layer 2 link.
What happens to the virtual MAC addresses immediately after a failover event occurs?
A. The virtual MAC addresses are permanently stripped, and the cluster reverts to the physical MAC addresses of the active interfaces.
B. The virtual MAC is mathematically tied to the management IP and requires an external SDN controller to migrate traffic seamlessly.
C. The new primary unit sends gratuitous ARP packets to prompt the connected Layer 2 switches to update their MAC forwarding tables.
D. Both data centers will briefly generate conflicting virtual MACs, requiring manual intervention on the core routers to clear the ARP cache.
Answer: C
Explanation:
➪ Core Concept: FGCP virtual MAC addresses and Layer 2 failover mechanisms.
➪ Analysis: In an FGCP HA cluster, the interfaces share virtual MAC (vMAC) addresses. When a failover occurs, the newly elected primary unit assumes the active role and retains the same vMACs. To ensure downstream and upstream Layer 2 switches know that the vMAC has moved to a new physical port (on the new primary unit), the FortiGate sends Gratuitous ARP (GARP) packets. This forces the switches to immediately update their MAC address tables, ensuring seamless traffic continuation without manual intervention.
➪ CLI /Reference: diagnose sys ha dump-by vcluster and understanding of standard FGCP GARP behavior.