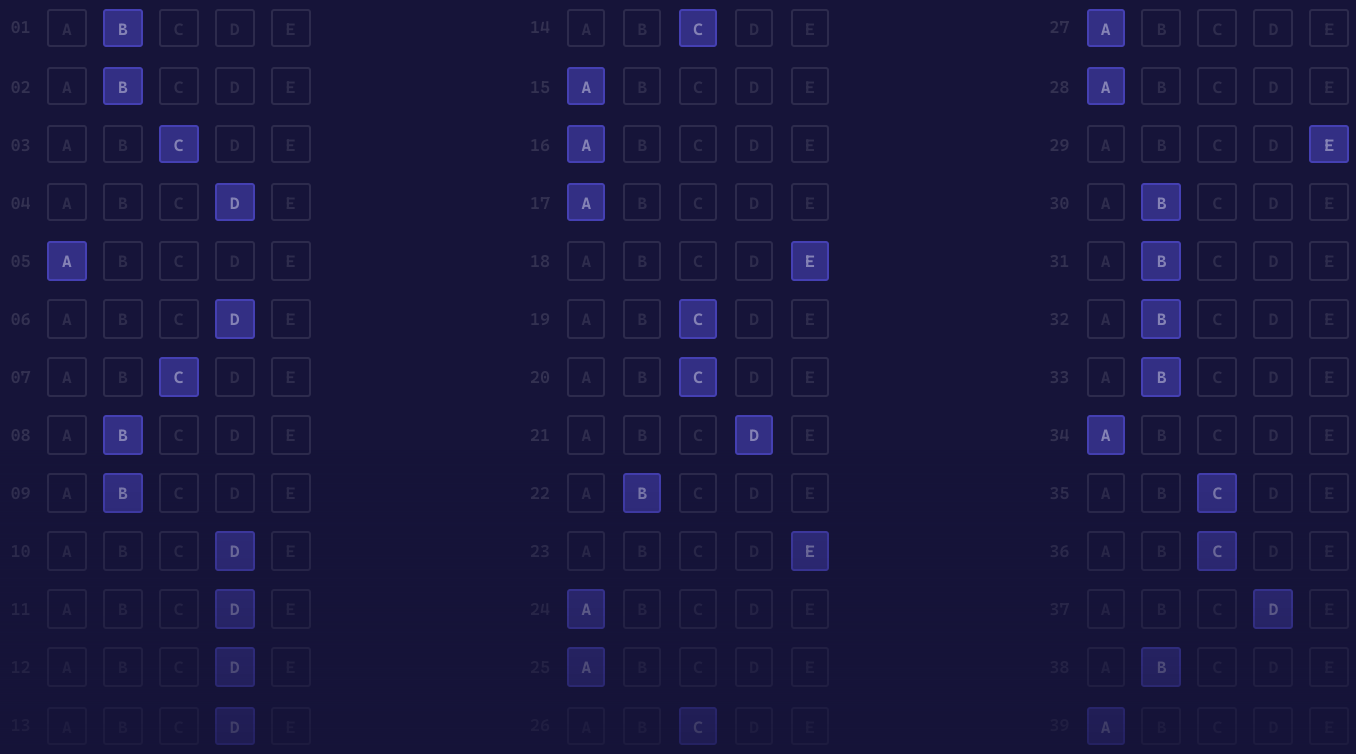
MOMETRIX
SMARTER PREP. BETTER RESULTS.



PRACTICE QUESTIONS

Fortinet

NSE7_FSN_AR-7.6

Fortinet NSE 7 - Secure Networking 7.6 Architect

EDITION	QUESTIONS	ISSUED
Demo	9	August 12, 2026

WEB www.mometrix.net

SUPPORT support@mometrix.net

Before you begin

What this is

9 practice questions for Fortinet `NSE7_FSN_AR-7.6`, each with its answer key and an explanation. Answer a question before you read its key — the explanation is worth more once you have committed.

If something looks wrong

Send us three things and we will check it:

- the exam code, `NSE7_FSN_AR-7.6`
- the question number
- the email address on your order

Write to **support@mometrix.net**. We reply within one business day.

Licence

QUESTION 1 SINGLE CHOICE

Which IKE version does FortiGate use by default when configuring an ADVPN spoke that establishes a shortcut tunnel between spokes?

A IKEv1 only

B IKEv2 only

C Both IKEv1 and IKEv2 are supported, but IKEv1 is the default.

D The IKE version is configurable per shortcut tunnel and defaults to the same version used for the spoke-to-hub tunnel.

ANSWER B

WHY FortiGate ADVPN uses IKEv2 for shortcut tunnels. While spoke-to-hub tunnels can use IKEv1 or IKEv2, ADVPN shortcut negotiations require IKEv2 because of its built-in support for informational exchanges required for shortcut establishment. Option D is not fully correct; the IKE version for ADVPN shortcuts is not independently configurable per shortcut and must be IKEv2 if ADVPN is enabled.

QUESTION 2 SINGLE CHOICE

An architect must ensure that real-time voice traffic uses the lowest-latency path, while bulk backup traffic uses the least-cost path. Which SD-WAN rule action should be used to evaluate both voice and backup traffic in a single rule?

A Best Quality

B Load Balancing

C Manual

D Automatic

ANSWER C

WHY In FortiGate SD-WAN, the 'Manual' rule action allows the administrator to explicitly set a strategy (e.g., 'lowest latency' or 'best quality') per application or application group. 'Best Quality' is a strategy, not a rule action. 'Load Balancing' distributes traffic across members but does not select per-app strategy. 'Automatic' uses only a single assigned strategy for the whole rule. With 'Manual', the architect can create multiple match-and-apply entries: one for real-time voice using the lowest-latency strategy, and another for backup traffic using the least-cost strategy, all within one SD-WAN rule.

QUESTION 3 SINGLE CHOICE

When using a FortiGate as the root of a Security Fabric, which of the following is a prerequisite for downstream FortiGates to join the Fabric automatically?

A All downstream devices must be managed by the same FortiManager.

B The root FortiGate must have an Authorization Key configured and the downstream devices must use the same key during initial setup.

C All FortiGates must be in NAT mode and have identical firmware versions.

D The downstream FortiGates must be connected to the root FortiGate's management interface.

ANSWER B

WHY For automatic Security Fabric join, the root FortiGate configures a Fabric authorization key (under Security Fabric > Settings). Downstream FortiGates that have just been factory reset and configured with the same key will automatically discover and join the Fabric over any reachable interface. Option A is not required; FortiManager is optional. Option C is partially true (NAT mode required), but identical firmware is not mandatory (minor version differences may be tolerated). Option D is incorrect; the connection can be over any physical/logical interface that is routable.

QUESTION 4 MULTIPLE CHOICE

In a FortiGate Cluster Protocol (FGCP) active-passive HA pair, which two actions will cause a failover to the passive unit? (Choose two.)

A An administrator disables the active unit's HA heartbeat interface.

B A power failure occurs on the active unit.

C The active unit receives a higher-priority BGP route than the passive unit.

D The active unit's CPU utilization exceeds 80% for 10 seconds.

ANSWER A · B

WHY FGCP handles failover when a unit's heartbeat link(s) fail (option A) or when the active unit becomes completely unreachable (option B). Option C is irrelevant because BGP route selection does not trigger FGCP failover. Option D is not a default FGCP trigger; while custom monitoring scripts can cause failover based on CPU, it is not a built-in mechanism.

QUESTION 5 SINGLE CHOICE

An architect configures route redistribution from OSPF into BGP on a FortiGate. By default, what is the MED (multi-exit discriminator) assigned to the redistributed OSPF routes?

A 0

B 1

C The OSPF metric of the route

D The BGP next-hop cost

ANSWER C

WHY When FortiGate redistributes OSPF routes into BGP, by default the MED is set to the OSPF metric value. This is documented behavior to allow OSPF metric to influence BGP path selection when routes are received by another AS. Options A and B are incorrect default values. Option D is not used.

QUESTION 6 SINGLE CHOICE

In a FortiGate ZTNA access proxy configuration, which type of resource is directly associated with a ZTNA application and includes the actual server that hosts the application?

A ZTNA rule

B ZTNA server

C ZTNA application

D ZTNA proxy

ANSWER B

WHY A ZTNA server object defines the application server's IP address and port. Multiple ZTNA applications can reference the same ZTNA server. The ZTNA application is the configuration that specifies the virtual host, certificate, and access rule, but it does not hold the server IP directly. A ZTNA rule is a policy that controls access. A ZTNA proxy is not a configuration object.

QUESTION 7 SINGLE CHOICE

A FortiGate administrator wants to inspect FTP traffic using a deep inspection profile that includes SSL inspection and application control. Which type of firewall policy configuration is required for the FortiGate to properly decrypt and inspect FTP over SSL (FTPS) using explicit FTPS mode?

A. A policy allowing port 990 without SSL inspection, because FTPS uses an implicit SSL connection on port 990.

B. A policy with SSL/SSH inspection enabled, and the FTPS protocol must be added to the SSL inspection exceptions list.

C. A policy with SSL/SSH inspection enabled and no exceptions for FTPS.

D. A policy using a NAT mode, because FTPS cannot be inspected in transparent mode.

ANSWER B

WHY FTPS (explicit mode on port 21, or implicit on port 990) uses SSL/TLS. For the FortiGate to intercept the SSL handshake, SSL inspection must be enabled. However, FTPS uses the CONNECT method (for port 990) or AUTH TLS on port 21. To avoid breaking SSL inspection, the FTPS protocol must be added to the SSL inspection exceptions list, which allows the FortiGate to act as a man-in-the-middle without attempting to convert the connection to HTTP. Option A would not allow inspection. Option C would cause inspection errors. Option D is unrelated to inspection.

QUESTION 8 MULTIPLE CHOICE

An architect enables central NAT on a FortiGate and creates central SNAT policies. Which two statements correctly describe the behavior of central SNAT policies? (Choose two.)

A Central SNAT policies are evaluated before any firewall policy lookups.

B If no central SNAT policy matches, the source IP of the original packet is used unchanged.

C Central SNAT policies can be configured to use the IP address of the outgoing interface as the translated source.

D Central SNAT policies require that the corresponding firewall policy has NAT enabled.

ANSWER B · C

WHY Option B is correct: When central NAT is enabled, if no SNAT policy matches the traffic, no source translation occurs. Option C is correct: You can set 'source address' to 'outgoing-interface' to use the egress interface IP. Option A is false: Central SNAT policies are evaluated after the firewall policy lookup (during the forward path). Option D is false: When central NAT is enabled, the NAT settings on the firewall policy are ignored; central SNAT policies control translation independently.

QUESTION 9 SINGLE CHOICE

Exhibit.

EXHIBIT

```
config system auto-trigger
  edit 1
    set event-type config-change
    set action execute-cli-script
    set cli-script "execute backup config scp <remote_ip> <remote_path> <user>
<password>"
  next
end
```

A FortiGate administrator creates an automation stitch that triggers on a 'configuration change' event. Which action type can be used to save the current configuration file to a remote server using SFTP?

A **Execute CLI Script**

B Run a Google Cloud Function

C Send a webhook

D Execute a FortiGate CLI command with redirect to a file

ANSWER **A**

WHY The 'Execute CLI Script' action in an automation stitch can contain a sequence of FortiGate CLI commands. This can include commands like 'execute backup config tftp' or 'execute backup config ftp' (or SCP/SFTP commands with appropriate settings). There is no built-in SFTP client action, but you can use the CLI script to run 'execute backup config scp' or similar. Option B is cloud-specific, not suited for local config backup. Option C sends an HTTP request; may trigger a backup externally but does not directly save the config. Option D is not a valid action type.