FortiGate NSE 4 — 25 Free Sample Questions

FortiOS 7.6 Administrator (NSE 4 / FCP) · 5 domains · every answer cited
fortigateprep.com

This is a free sample of the full 350-question bank. Each answer is explained — why it's right and why the others are wrong — and cited to the exact page in the official FortiOS 7.6 documentation.

Domain 1 — Deployment & System Configuration

D1-Q1 · A — Perform initial configuration

Where are the protocols that administrators may use to reach a FortiGate (HTTPS, SSH, PING, etc.) controlled?

A) In the firewall policy table
B) In the DoS policy
C) Globally, in System > Settings only
D) Per interface, in the interface's Administrative Access settings

✓ Answer: D

Administrative access is set per interface (Network > Interfaces > Administrative Access), where you enable the allowed protocols for IPv4/IPv6. This restricts management access to chosen interfaces and protocols. A, B, and C are not where per-interface admin access is configured.

Ref: Interface settings (doc 574723)

D1-Q76 · C — Configure an FGCP HA cluster

Two identical FortiGates (same model, firmware, and number of connected monitored interfaces) form an FGCP cluster with default settings. The unit configured with the higher HA priority does NOT become the primary. Why, and what change would make priority decide?

A) The cluster always picks the unit with the lower serial number first
B) By default HA override is disabled, so uptime is evaluated before priority; enabling override makes the higher-priority unit become primary
C) Priority only applies in active-active mode
D) Priority is ignored unless Central NAT is enabled

✓ Answer: B

The configurations that impact primary selection are priority, monitored interfaces (`monitor`), and `override`. With override disabled (the default), uptime is considered before priority — so a unit with longer uptime can remain primary even if the other has a higher priority. Enabling override makes priority take precedence, so the higher-priority unit is selected as primary. A, C, and D are incorrect (serial number is only the final tiebreaker; priority applies in both HA modes).

Ref: HA primary unit selection criteria (doc 996846)

D1-Q19 · A — Perform initial configuration

On a factory-default FortiGate, what are the default administrator credentials, and what controls what an administrator can do?

A) There is no default account
B) Username admin with password "admin"; no profiles exist
C) Username admin with no password; an administrator profile defines permissions
D) Username root with password "fortinet"; permissions are fixed

✓ Answer: C

A factory-default FortiGate has an administrator account with username admin and no password; an administrator profile defines what each admin can see and do. A, B, and D are incorrect.

Ref: System (doc 617430)

D1-Q36 · B — Implement the Fortinet Security Fabric

Which of the following is a valid automation stitch trigger?

A) A VLAN tag
B) A static route
C) An IP pool
D) A specific log event or a failed login attempt

✓ Answer: D

A trigger is the condition or event that activates a stitch — for example, a specific log or a failed login attempt (other triggers include events such as a security rating notification or conserve mode). A, B, and C are not triggers.

Ref: Automation stitches (doc 139441)

D1-Q59 · D — Diagnose resource and connectivity problems

In the CLI, how can an administrator narrow the session list to sessions from a specific source IP (10.11.101.112)?

A) `config firewall policy`
B) `get system status`
C) `diagnose sys session filter src 10.11.101.112` (then list the sessions)
D) `execute ping 10.11.101.112`

✓ Answer: C

A session filter limits the displayed sessions; `diagnose sys session filter src ` filters by source address (separate lines can add more filters such as `dst`). B pings, B shows status, A edits policies.

Ref: Using a session table (doc 562859)

Domain 2 — Firewall Policies & Authentication

Q7 · B — Configure SNAT and DNAT options in firewall policies

Which object performs destination NAT so external users can reach an internal server?

A) Static route
B) Virtual IP (VIP)
C) Address group
D) IP Pool

✓ Answer: B

A VIP maps an external address (and optionally port) to an internal server and is used as the destination in a firewall policy. IP Pools handle source NAT; address groups just collect addresses; static routes direct but don't translate.

Ref: Static virtual IPs (doc 510402)

Q15 · D — Deploy and configure FSSO

An organization wants FSSO but will not install an agent on each domain controller. Which approach fits?

A) DC Agent mode
B) Captive portal mode
C) IPsec mode
D) Polling mode — the Collector Agent (or FortiGate) polls the DC security event logs

✓ Answer: D

Polling mode reads logon events from the DCs' security event logs without a per-DC agent; the docs state DC Agent mode requires an agent installed on every domain controller. Captive portal is active authentication, not transparent FSSO; "IPsec mode" is not an FSSO mode.

Ref: FSSO polling connector agent installation (doc 503764)

Q16 · A — Configure firewall policies

In policy-based NGFW mode, how are applications and URL categories handled compared to profile-based mode?

A) They are not supported at all
B) They can only be configured through the CLI
C) They require a separate antivirus profile on every policy
D) They can be used directly in security policies, without web filter or application control profiles

✓ Answer: D

Profile-based (traditional) mode applies security profiles to a policy; policy-based NGFW mode lets you reference applications and URL categories directly in security policies without web filter/application control profiles. A and C are false; B is wrong — both modes are GUI-configurable.

Ref: NGFW policy (doc 243446)

Q34 · A — Configure firewall policies

In current FortiOS, how are ISDB objects referenced within firewall policies?

A) By interface
B) By name
C) By MAC address
D) By their numeric ID only

✓ Answer: B

ISDB objects are now referenced in policies by name rather than by numeric ID. D reflects older behavior; A and C are unrelated.

Ref: Allow creation of ISDB objects with regional information (doc 336471)

Q50 · B — Configure SNAT and DNAT options in firewall policies

Which VIP type distributes incoming connections across multiple internal real servers?

A) Static NAT VIP
B) Server load balance VIP (type server-load-balance)
C) One-to-One IP pool
D) FQDN address object

✓ Answer: B

A server load balance VIP (type server-load-balance) forwards incoming connections to a set of configured real servers. A is a single 1:1 mapping; C is a source-NAT pool; D is an address object.

Ref: Virtual server load balance (doc 713497)

Q69 · C — Configure firewall authentication methods

An organization wants users authenticated by the digital certificate they present. What must a PKI user definition specify?

A) A DoS anomaly threshold
B) A static route to the CA
C) An IP pool and a VIP
D) The CA certificate used to validate the user's certificate, and the certificate field/value to match

✓ Answer: D

A PKI user is identified by a digital certificate; the definition specifies which CA certificate validates the user's certificate and which certificate field/value FortiOS checks. A, B, and C are unrelated.

Ref: Configuring a PKI user (doc 776666)

Domain 3 — Content Inspection

D3-Q31 · A — Inspect encrypted traffic with certificates (SSL inspection)

Using certificate inspection only, what can the FortiGate see about an HTTPS request?

A) Only the certificate/domain information (e.g., the hostname) — not the full URL path or decrypted content

B) Only the source MAC address

C) The full decrypted payload

D) Nothing at all

✓ Answer: A

Certificate inspection examines the certificate/handshake (such as the hostname) but does not decrypt the session, so it cannot see the full URL path or content. Deep inspection is required to inspect content. B, C, and D are incorrect.

Ref: Configuring an SSL/SSH inspection profile (doc 709167)

D3-Q37 · B — Identify inspection modes & configure web filtering

A policy has both a DNS filter and a web filter applied. Which takes precedence?

A) The web filter always overrides the DNS filter

B) The DNS filter takes precedence

C) They cannot be applied to the same policy

D) Whichever was created last

✓ Answer: B

When both a DNS filter and a web filter are configured on the same firewall policy, the DNS filter takes precedence. A, C, and D are incorrect.

Ref: DNS filter (doc 605868)

D3-Q47 · D — Configure antivirus scanning modes

What does Content Disarm and Reconstruction (CDR) do?

A) Blocks all document downloads

B) Encrypts all documents

C) Compresses files to save bandwidth

D) Sanitizes supported documents (e.g., Microsoft Office, PDF) by removing active content such as macros, hyperlinks, embedded media, and JavaScript, while preserving the readable content

✓ Answer: D

CDR sanitizes documents by stripping active content (hyperlinks, macros, embedded media, JavaScript, etc.) — "disarm" — while keeping the textual content intact — "reconstruction." A, B, and C are incorrect.

Ref: Content disarm and reconstruction (doc 788313)

D3-Q54 · E — Configure IPS (intrusion prevention)

How does the FortiGate detect a compromised internal host communicating with a known botnet command-and-control server?

A) Only the antivirus engine can detect this

B) DHCP detects it

C) The IPS engine scans outgoing connections to botnet sites; accessing a botnet IP generates an IPS log

D) The routing table blocks it automatically

✓ Answer: C

The IPS engine scans outgoing connections against known botnet sites; when a host reaches a botnet IP, an IPS log (subtype ips, eventtype botnet) is generated. A, B, and D are incorrect.

Ref: IPS with botnet C&C; IP blocking (doc 668865)

D3-Q43 · C — Configure application control

What characterizes NGFW policy-based mode (versus profile-based mode) for application control and web filtering?

A) It disables application control entirely

B) It only works in transparent mode

C) Applications and URL categories are used directly in security policies without requiring application control or web filter profiles, and Central NAT is always enabled

D) You must always create profiles first

✓ Answer: C

In NGFW policy-based mode, applications and URL categories are referenced directly in security policies (no separate profiles required), and Central NAT is always enabled. Profile-based mode is the traditional model of building profiles and applying them to policies. A, B, and D are incorrect.

Ref: NGFW policy (doc 243446)

Domain 4 — Routing

D4-Q1 · A — Configure and route packets using static routes

How does the FortiGate decide which route to install when several routes match a destination?

A) The route with the highest administrative distance wins

B) Most specific (longest prefix) wins; if tied, lowest administrative distance; if still tied, cost and priority decide; if still equal, ECMP distributes traffic

C) Routes are chosen at random

D) The newest route always wins

✓ Answer: B

The routing table keeps the best routes: the most specific route always takes precedence; on a tie the lower administrative distance is injected; if AD is equal, cost and priority decide; if those are equal too, FortiGate uses ECMP. A, C, and D are incorrect.

Ref: Routing concepts (doc 139692)

D4-Q11 · A — Configure and route packets using static routes

A policy route and a regular static route both match a flow. Which is used, and why?

A) Whichever has more specific subnet

B) The static route, because it has lower AD

C) The policy route — ECMP/route lookup is considered after policy routing, so any matching policy route takes precedence

D) Both are used simultaneously

✓ **Answer: C**

Policy routes are evaluated before the routing table; ECMP (and normal route lookup) is considered after policy routing, so a matching policy route takes precedence over the regular route. A, B, and D are incorrect.

Ref: Equal cost multi-path (doc 25967)

D4-Q20 · B — Configure SD-WAN to load-balance traffic across multiple WAN links

An SD-WAN member has two health checks configured. What happens to its routes if only one health check fails?

A) The routes are removed immediately

B) Nothing is removed — all configured health checks must fail before the link's routes are removed from the SD-WAN load-balancing group

C) The member is deleted

D) The FortiGate reboots

✓ **Answer: B**

When a member has multiple health checks, all of them must fail before that link's routes are removed from the SD-WAN link load-balancing group (and traffic reroutes); routes are reestablished when the link recovers. A, C, and D are incorrect.

Ref: Link health monitor (doc 580649)

D4-Q27 · B — Configure SD-WAN to load-balance traffic across multiple WAN links

Using the Lowest Cost (SLA) strategy, how is the member chosen?

A) Among the links that meet the SLA target, the one with the lowest cost is chosen; if costs tie, the interface preference order decides (lowest possible cost is 0)

B) The link with the most sessions is chosen

C) A random link that meets the SLA is chosen

D) The most expensive link is chosen

✓ **Answer: A**

Lowest Cost (SLA) selects the lowest-cost link that satisfies the SLA target; the lowest possible cost is 0, and if multiple eligible links share the same cost, the interface preference order is used. B, C, and D are incorrect.

Ref: Lowest cost (SLA) strategy (doc 342836)

Domain 5 — VPN

D5-Q1 · A — Configure SSL VPNs for secure access to the private network

What major remote-access change occurred in FortiOS 7.6.3?

A) All VPNs now require FortiAuthenticator

B) IPsec VPN was removed in favor of SSL VPN

C) VPNs can no longer use certificates

D) SSL VPN tunnel mode was removed and replaced by IPsec VPN, which can be configured to use TCP port 443

✓ Answer: D

Starting in FortiOS 7.6.3 (and continuing in 7.6.6), SSL VPN tunnel mode is removed from the GUI and CLI for all models and replaced by IPsec VPN, which can be configured to use TCP port 443. (SSL VPN web mode remains, renamed Agentless VPN.) A, B, and C are incorrect.

Ref: SSL VPN tunnel mode replaced with IPsec VPN (doc 173430)

D5-Q14 · B — Implement a meshed or partially redundant IPsec VPN

What is the purpose of IPsec phase 1 (IKE)?

A) To secure a tunnel with one bidirectional IKE security association (SA) used to negotiate the phase 2 parameters

B) To encrypt user data directly

C) To replace the routing table

D) To assign IP addresses to LAN hosts

✓ Answer: A

Phase 1 establishes a bidirectional IKE SA between the peers (initiator and responder) that is then used to negotiate phase 2; the data-protecting SAs are created in phase 2. B, C, and D are incorrect.

Ref: Phase 1 configuration (doc 790613)

D5-Q39 · B — Implement a meshed or partially redundant IPsec VPN

What does enabling Perfect Forward Secrecy (PFS) on phase 2 do?

A) It removes the need for a proposal

B) It disables rekeying

C) It forces a fresh Diffie-Hellman exchange at each rekey (when keylife expires), so new keys aren't derived from previous keying material

D) It turns off encryption between rekeys

✓ Answer: C

PFS forces a new Diffie-Hellman exchange whenever the phase 2 keylife expires, generating independent keys each time so compromise of one key doesn't expose past/future sessions. A, B, and D are incorrect.

Ref: Phase 2 configuration (doc 604285)

D5-Q27 · B — Implement a meshed or partially redundant IPsec VPN

What does ADVPN add to a hub-and-spoke VPN?

A) Removal of all encryption

B) Mandatory web-mode portals

C) A second hub requirement

D) Dynamic on-demand spoke-to-spoke shortcut tunnels, so traffic between spokes doesn't have to permanently hairpin through the hub

✓ Answer: D

ADVPN (Auto-Discovery VPN) lets spokes build dynamic shortcut tunnels directly to each other on demand, avoiding constant hairpinning through the hub while keeping the hub for control. A, B, and C are incorrect.

Ref: IPsec VPN wizard hub-and-spoke ADVPN support (doc 853412)

D5-Q47 · B — Implement a meshed or partially redundant IPsec VPN

What does the phase 1 monitor option do for VPN redundancy, and how does failback behave?

A) It load-balances both tunnels equally at all times

B) It deletes the primary tunnel

C) It designates a tunnel as the backup for a specified primary phase 1; the backup activates when the primary fails (via DPD), and traffic stays on the backup even after the primary recovers (until the backup fails)

D) It forces immediate failback to the primary

✓ Answer: C

The `monitor` option ties a backup phase 1 to a primary; with DPD, the backup comes up when the primary fails. By default traffic continues on the replacement tunnel even after the original recovers, until the replacement itself fails. A, B, and D are incorrect.

Ref: Manual redundant VPN configuration (doc 432685)
