Fortinet NSE4_FGT_AD-7.6 NSE 4: FortiOS Practice Questions

Shared by Joseph on 17-08-2026

For More Free Questions and Preparation Resources

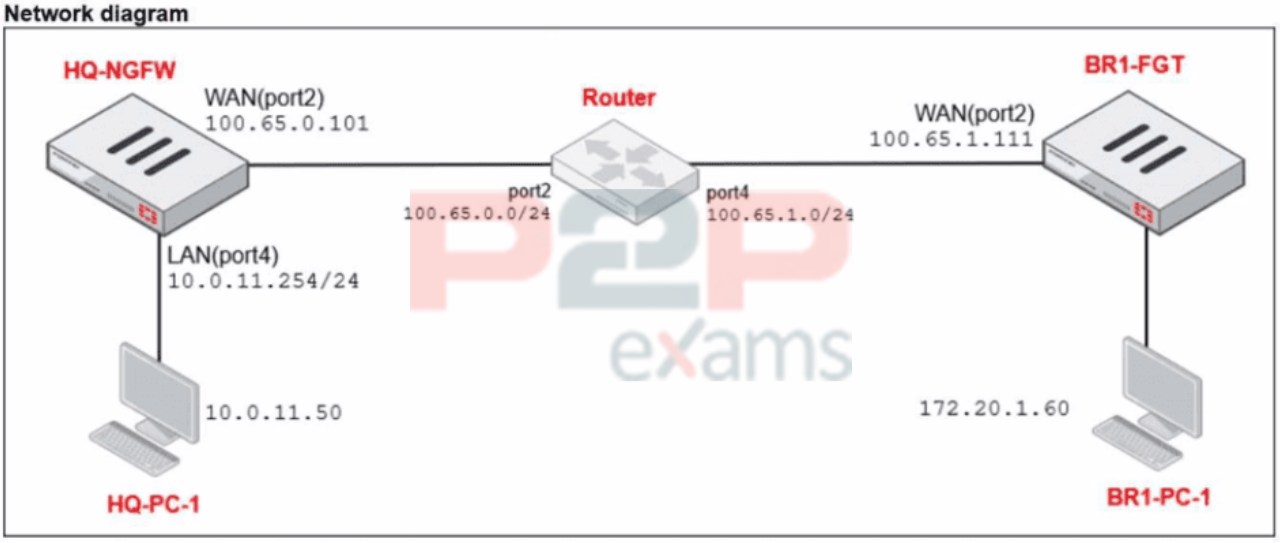
Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Refer to the exhibits.

Network diagram



NAT IP pool configuration

Name	External IP Range	Type	ARP Reply
SNAT-Pool	100.65.0.49 - 100.65.0.49	Overload	Enabled
SNAT-Remote	100.65.0.149 - 100.65.0.149	Overload	Enabled
SNAT-Remote1	100.65.0.99 - 100.65.0.99	Overload	Enabled

Firewall policies

Policy	Source	Destination	Schedule	Service	Action	IP Pool	NAT
LAN (port4) → WAN (port2) 3							
TCP traffic (2)	all	BR1-FGT	always	ALL_TCP	ACCEPT	SNAT-Pool	NAT
PING traffic (3)	all	all	always	PING	ACCEPT	SNAT-Remote1	NAT
IGMP traffic (4)	all	all	always	IGMP	ACCEPT	SNAT-Remote	NAT

The exhibits show a diagram of a FortiGate device connected to the network, as well as the IP pool configuration and firewall policy objects.

The WAN (port2) interface has the IP address

100.65.0.101/24.

The LAN (port4) interface has the IP address

10.0.11.254/24.

Which IP address will be used to source NAT (SNAT) the traffic, if the user on HQ-PC-1 (10.0.11.50) pings the IP address of BR-FGT (100.65.1.111)?

Options:

A- 100.65.0.101
B- 100.65.0.49
C- 100.65.0.149
D- 100.65.0.99

Answer:

D

Explanation:

From the exhibits, there are three relevant firewall policies from LAN (port4) to WAN (port2), each using a different IP pool for source NAT:

TCP traffic

Service: ALL_TCP

Destination: BR1-FGT

IP Pool: SNAT-Pool 100.65.0.49

PING traffic

Service: PING

Destination: all

IP Pool: SNAT-Remote1 100.65.0.99

IGMP traffic

Service: IGMP

Destination: all

IP Pool: SNAT-Remote 100.65.0.149

The user on HQ-PC-1 (10.0.11.50) is pinging BR1-FGT (100.65.1.111). In FortiOS, policy matching is based on (among other fields) source, destination, and service, and the first matching policy in top-down order is applied.

Because the traffic is ICMP echo (ping), it matches the policy named PING traffic (service PING, destination all). That policy explicitly uses Use Dynamic IP Pool with SNAT-Remote1, which is configured with external IP 100.65.0.99.

Therefore, the source NAT IP used for this ping is 100.65.0.99.

Question 2

Question Type: MultipleChoice

A new administrator is configuring FSSO authentication on FortiGate using DC Agent Mode. Which step is not part of the expected process?

Options:

A- The DC agent sends login event data directly to FortiGate.
B- FortiGate determines user identity based on the IP address in the FSSO list.
C- The collector agent forwards login event data to FortiGate.
D- The user logs into the windows domain.

Answer:

A

Question 3

Question Type: MultipleChoice

You have configured an application control profile, set peer-to-peer traffic to Block under the Categories tab. and applied it to the firewall policy. However, your peer-to-peer traffic on known ports is passing through the FortiGate without being blocked.

What FortiGate settings should you check to resolve this issue?

Options:

A- FortiGuard category ratings
B- Network Protocol Enforcement
C- Replacement Messages for UDP-based Applications
D- Application and Filter Overrides

Answer:

B

Explanation:

When the Application sensor receives traffic on that port, the protocol decoder will try to determine if the received data matches the HTTPS traffic In this case it will not match because it is P2P traffic, so this will class as violation and blocked The protocol decoder also try to determine what type of traffic it is, and even if it could not figure out it is P2P traffic, it still count as a violation because even though it does not know what it is, it knows for fact it is not HTTPS

Question 4

Question Type: MultipleChoice

An administrator wants to form an HA cluster using the FGCP protocol.

Which two requirements must the administrator ensure both members fulfill? (Choose two.)

Options:

A- They must have the same hard drive configuration.
B- They must have the same number of configured VDOMs.
C- They must have the heartbeat interfaces in the same subnet
D- They must have the same HA group ID.

Answer:

B, D

Explanation:

According to the FortiOS 7.6 High Availability (HA) Administration Guide and FGCP (FortiGate Clustering Protocol) requirements, the correct answers are B and D.

FGCP HA Cluster Mandatory Requirements (FortiOS 7.6)

When forming an HA cluster using FGCP, FortiGate devices must meet several strict compatibility and configuration requirements. Among the options given, the following two are mandatory:

B. They must have the same number of configured VDOMs

In FortiOS HA, all cluster members must have the same VDOM configuration.

This includes:

Same number of VDOMs

Same VDOM names

This is required so configuration synchronization can occur correctly between members.

If VDOM counts differ, HA formation will fail.

This is explicitly required and documented.

D. They must have the same HA group ID

The HA group ID uniquely identifies an HA cluster on the network.

All FortiGate units intended to join the same cluster must share the same HA group ID.

If the group IDs differ, devices will not recognize each other as cluster peers.

This is a fundamental FGCP requirement.

Why the Other Options Are Incorrect

A. They must have the same hard drive configuration

Hard drive presence or size does not have to match for FGCP HA to function.

Disk differences may affect logging behavior, but they do not prevent HA cluster formation.

Therefore, this is not a required condition.

C. They must have the heartbeat interfaces in the same subnet

Heartbeat interfaces must be:

Directly connected

In the same Layer 2 broadcast domain

They do not require IP addressing or being in the same IP subnet.

In many deployments, heartbeat interfaces have no IP addresses at all.

Therefore, ''same subnet'' is not a documented requirement.

Question 5

Question Type: MultipleChoice

A network administrator is reviewing firewall policies in both Interface Pair View and By Sequence View. The policies appear in a different order in each view. Why is the policy order different in these two views?

Options:

A- By Sequence View groups policies based on rule priority, while Interface Pair View always follows the order of traffic logs.
B- The firewall dynamically reorders policies in Interface Pair View based on recent traffic patterns, but By Sequence View remains static.
C- Interface Pair View sorts policies based on matching interfaces, while By Sequence View shows the actual processing order of rules.
D- Policies in Interface Pair View are prioritized by security levels, while By Sequence View strictly follows the administrator's manual ordering.

Answer:

C

Explanation:

In FortiOS 7.6, firewall policies can be displayed in multiple views to help administrators understand and manage rules more effectively. The difference in ordering between Interface Pair View and By Sequence View is intentional and documented.

Why the policy order is different

Interface Pair View

Groups firewall policies based on the incoming (From) and outgoing (To) interfaces.

Policies are organized under interface pairs such as:

LAN WAN

WAN LAN

Within each interface pair, policies may appear reordered compared to the global list.

This view is designed for readability and troubleshooting, not to show execution order.

By Sequence View

Displays firewall policies in their actual evaluation (processing) order.

This is the top-down order FortiGate uses when matching traffic.

It reflects the real rule sequence that determines which policy is hit first.

Why option C is correct

C . Interface Pair View sorts policies based on matching interfaces, while By Sequence View shows the actual processing order of rules.

This statement exactly matches FortiOS behavior as documented in the FortiOS 7.6 Firewall Policy Views section of the Administrator Guide.

Why the other options are incorrect

A: Interface Pair View does not follow traffic logs, and By Sequence View is not based on ''rule priority'' grouping.

B: FortiGate does not dynamically reorder policies based on traffic patterns.

D: Security levels do not affect policy ordering in Interface Pair View.

Question 6

Question Type: MultipleChoice

An administrator has configured a dialup IPsec VPN on FortiGate with add-route enabled. However, the static route is not showing in the routing table. Which two statements about this scenario are correct? (Choose two.)

Options:

A- The administrator must use a policy route instead of a static route for add-route to work properly.
B- The administrator must ensure phase 2 is successfully established
C- The administrator must define the remote network correctly in the phase 2 selectors.
D- The administrator must enable a dynamic routing protocol on the dialup interface.

Answer:

B, C

Explanation:

With a dialup IPsec VPN on FortiGate, when add-route is enabled, FortiGate will only install the corresponding route when it has enough negotiated information from the tunnel. In FortiOS 7.6, that means the route is tied to the Phase 2 (Quick Mode) selectors and is created dynamically when the IPsec SA is actually up.

B . The administrator must ensure phase 2 is successfully established

This is required. FortiGate does not install the add-route route just because Phase 1 exists or because the configuration is present. The route is added when the tunnel is effectively usable, which requires Phase 2 (IPsec SA) to be up. If Phase 2 is not established, there is no active SA and FortiGate will not inject the related route into the routing table.

So, if the static route is not showing, one correct explanation is that Phase 2 is not up.

C . The administrator must define the remote network correctly in the phase 2 selectors

This is also required. For dialup tunnels, FortiGate derives what route to add from the remote subnet(s) defined in the Phase 2 selector (proxy ID). If the remote network in Phase 2 is missing, incorrect, or too broad/too narrow in a way that prevents negotiation, the tunnel either won't come up (so no route), or the route that would be installed won't match what the administrator expects.

So, another correct explanation is that the Phase 2 remote network is not correctly defined, preventing the correct route from being created.

Why the other options are incorrect

A . Policy route instead of a static route

Add-route does not require policy routes. It is specifically a feature that injects a route (route-table entry) associated with the IPsec tunnel/SA and the Phase 2 selector networks.

D . Enable a dynamic routing protocol

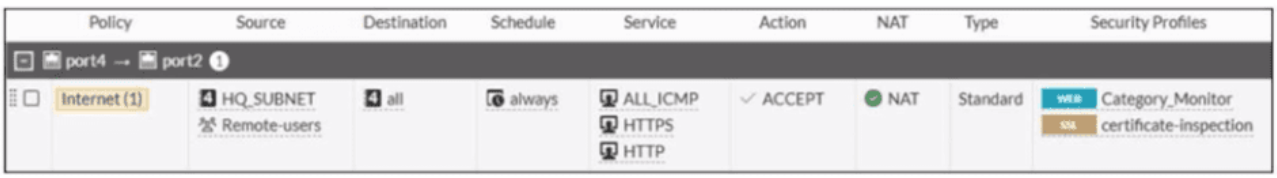
Dynamic routing protocols (OSPF/BGP/RIP) are not required for add-route. Add-route is independent of dynamic routing and works by installing routes locally based on the negotiated selectors.

Question 7

Question Type: MultipleChoice

Refer to the exhibit

A firewall policy to enable active authentication is shown.



When attempting to access an external website using an active authentication method, the user is not presented with a login prompt. What is the most likely reason for this situation?

Options:

A- No matching user account exists for this user.
B- The Remote-users group must be set up correctly in the FSSO configuration.
C- The Remote-users group is not added to the Destination
D- The Service DNS is required in the firewall policy.

Answer:

D

Explanation:

Based on the exhibit and FortiOS 7.6 Active Authentication (captive portal) behavior, the most likely reason the user is not presented with a login prompt is that DNS is missing from the firewall policy.

What the exhibit shows

The firewall policy configured for active authentication includes:

Source: HQ_SUBNET and Remote-users

Destination: all

Services:

HTTP

HTTPS

ALL_ICMP

Security Profiles: Web filter and SSL inspection enabled

Authentication: Active (user group referenced)

DNS is not included as a service in the policy.

Why DNS is required for active authentication

In FortiOS 7.6, active authentication (captive portal) works as follows:

The user attempts to access a website using a URL (for example, www.example.com).

The client must first perform a DNS lookup to resolve the domain name.

FortiGate intercepts the initial HTTP/HTTPS request and redirects the user to the authentication portal.

If DNS traffic is blocked or not allowed:

The hostname cannot be resolved.

The HTTP/HTTPS request never properly occurs.

FortiGate has nothing to intercept, so the login prompt is never triggered.

This is explicitly documented in the FortiOS 7.6 Authentication and Captive Portal requirements, which state that DNS must be permitted for captive portal--based authentication to function correctly.

Why the other options are incorrect

A . No matching user account exists for this user

Incorrect.

If the user account did not exist, the login page would still appear, but authentication would fail after credentials are entered.

B . The Remote-users group must be set up correctly in the FSSO configuration

Incorrect.

This policy is using active authentication, not FSSO.

FSSO configuration is irrelevant for active authentication login prompts.

C . The Remote-users group is not added to the Destination

Incorrect.

User groups are applied in the Source field for authentication-based policies.

Destination does not accept user groups.

Question 8

Question Type: MultipleChoice

Refer to the exhibit.

Destination	Gateway IP	Interface	Status
0.0.0.0/0	100.65.0.254	port2	Enabled
10.10.10.0/24	100.66.0.254	port3	Enabled
10.0.13.0/24	10.0.13.125	port6	Enabled

Based on the routing table shown in the exhibit, which two statements are true? (Select two.)

Options:

A- A packet with the source IP address 10.0.13.10 arriving on port2 is allowed if strict RPF is disabled.
B- A packet with the source IP address 10.100.110.10 arriving on port2 is allowed if strict RPF is enabled.
C- A packet with the source IP address 10.100.110.10 arriving on port3 is allowed if strict RPF is disabled.
D- A packet with the source IP address 10.10.10.10 arriving on port2 is allowed if strict RPF is enabled.

Answer:

A, C

Question 9

Question Type: MultipleChoice

A network administrator has enabled full SSL inspection and web filtering on FortiGate. When visiting any HTTPS websites, the browser reports certificate warning errors. When visiting HTTP websites, the browser does not report errors.

What is the reason for the certificate warning errors?

Options:

A- The option invalid SSL certificates is set to allow on the SSL/SSH inspection profile.
B- The matching firewall policy is set to proxy inspection mode.
C- The browser does not trust the certificate used by FortiGate for SSL inspection.
D- The certificate used by FortiGate for SSL inspection does not contain the required certificate extensions.

Answer:

C

Explanation:

With full SSL inspection, FortiGate performs a man-in-the-middle process: it decrypts the HTTPS session, inspects it, then re-encrypts it. To do this, FortiGate presents a substitute certificate to the client, signed by the CA certificate configured in the SSL/SSH inspection profile (for example, Fortinet_CA_SSL or a custom enterprise CA).

Browsers will show certificate warning errors when the issuing CA is not trusted by the client device/browser trust store. This only happens for HTTPS because certificates are used in TLS; HTTP has no certificate exchange, so no warning appears.

Why the other options are incorrect:

A: Allowing invalid server certificates affects whether FortiGate blocks/permits connections to sites with bad certs; it does not fix the client warning about FortiGate's substituted cert.

B: Proxy vs flow inspection mode does not inherently cause certificate warnings; the warning is about trust of the signing CA.

D: Missing extensions is not the typical reason across ''any HTTPS website''; the standard reason is the client does not trust the FortiGate inspection CA

Question 10

Question Type: MultipleChoice

FortiGate is operating in NAT mode and has two physical interfaces connected to the LAN and DMZ networks respectively. Which two statements about the requirements of connected physical interfaces on FortiGate are true? (Choose two.)

Options:

A- Both interfaces must have DHCP enabled and interfaces set to LAN and DMZ roles assigned.
B- Both interfaces must have the interface role assigned.
C- Both interfaces must have directly connected routes on the routing table.
D- Both interfaces must have IP addresses assigned.

Answer:

C, D

Explanation:

In FortiOS 7.6, when a FortiGate is operating in NAT mode, physical interfaces that participate in traffic forwarding (such as LAN and DMZ) must meet certain fundamental requirements.

Correct statements

D . Both interfaces must have IP addresses assigned.

Correct

In NAT mode, FortiGate operates as a Layer-3 device.

Every interface that forwards traffic must have an IP address.

Without an IP address:

The interface cannot participate in routing

Firewall policies cannot be applied correctly

This is a mandatory requirement.

C . Both interfaces must have directly connected routes on the routing table.

Correct

When an IP address is assigned to an interface, FortiGate automatically installs a connected route for that subnet in the routing table.

These connected routes are required so FortiGate:

Knows how to reach the locally attached networks

Can forward traffic between LAN and DMZ

While administrators do not manually create these routes, their presence is required for correct operation.

Why the other options are incorrect

A . Both interfaces must have DHCP enabled and roles assigned.

Incorrect

DHCP is optional; interfaces can use static IPs.

Interface roles (LAN, DMZ, WAN) are administrative/GUI aids, not functional requirements.

B . Both interfaces must have the interface role assigned.

Incorrect

Interface roles affect GUI grouping and some default behavior.

They are not required for NAT mode operation or traffic forwarding.

Question 11

Question Type: MultipleChoice

What is the main FortiGate election process when the HA override setting is enabled? (Choose one answer)

Options:

A- Connected monitored ports > Priority > HA uptime > FortiGate serial number
B- Connected monitored ports > Priority > System uptime > FortiGate serial number
C- Connected monitored ports > HA uptime > Priority > FortiGate serial number
D- Connected monitored ports > System uptime > Priority > FortiGate serial number

Answer:

A

Explanation:

According to the FortiOS 7.6 Study Guide and technical documentation regarding High Availability (HA), the FortiGate Clustering Protocol (FGCP) uses a specific set of rules to elect the primary unit in a cluster. By default, the election order follows: Connected Monitored Ports > HA Uptime > Priority > Serial Number.

However, when the HA override setting is enabled, the election logic is modified to prioritize the administrator-defined priority value over the uptime of the cluster members. In this specific configuration, the election process follows this sequence:

Connected monitored ports: The unit with the most functioning monitored interfaces is preferred.

Priority: The unit with the highest manually configured priority value (e.g., 255) is selected next.

HA uptime: If monitored ports and priority are equal, the unit that has been up in the HA cluster the longest is chosen.

FortiGate serial number: As a final tie-breaker, the unit with the higher serial number is

elected.1

Question 12

Question Type: MultipleChoice

An administrator wants to configure dead peer detection (DPD) on IPsec VPN for detecting dead tunnels. The requirement is that FortiGate sends DPD probes only when there is no inbound traffic.

Which DPD mode on FortiGate meets this requirement?

Options:

A- On Demand
B- Enabled
C- On Idle
D- Usabled

Answer:

A

Explanation:

Based on the FortiOS 7.6 Infrastructure and IPsec VPN documentation, Dead Peer Detection (DPD) can be configured in three primary modes: On Demand, On Idle, and Disabled.

On Demand (Default Mode): This mode is specifically designed to minimize unnecessary traffic. In this mode, FortiGate sends DPD probes only when there is no inbound traffic but the FortiGate is attempting to send outbound traffic. Because network communication is typically bidirectional, the absence of inbound traffic while outbound traffic is being sent is a primary indicator of a potentially dead tunnel. This matches the specific requirement described in the question.

On Idle: In this mode, DPD probes are sent if no traffic (neither inbound nor outbound) has been observed in the tunnel for a specific period. It verifies the tunnel status even when the connection is completely idle.

Enabled: In older versions or specific CLI contexts, 'Enabled' may refer to periodic DPD, but in the current FortiOS 7.x/7.6 GUI and CLI terminology for Phase 1 settings, the active modes are defined as on-demand or on-idle.

Disabled: In this mode, the FortiGate does not send DPD probes but will still respond to DPD probes sent by the remote peer.

The requirement that the administrator wants probes sent only when there is no inbound traffic (usually implying the FortiGate is sending but not receiving) is the fundamental definition of the On Demand mechanism in the Fortinet curriculum.