Download Fortinet NSE4_FGT_AD-7.6 Exam Dumps Free

Shared by Sloan on 17-06-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

An administrator manages a FortiGate model that supports NTurbo

How does NTurbo acceleration enhance antivirus performance?

Options:

A- For flow-based inspection. NTurbo establishes a dedicated data path to redirect traffic between the IPS engine and FortiGate ingress and egress interfaces.
B- For flow-based inspection. NTurbo creates two inspection sessions on the FortiGate device.
C- For proxy-based inspection. NTurbo offloads traffic to the content processor.
D- For proxy-based inspection. NTurbo buffers the whole file and then sends it to the antivirus engine.

Answer:

A

Explanation:

According to the FortiOS 7.6 Administration Guide and Fortinet hardware acceleration (NTurbo) documentation, the correct answer is A.

What NTurbo Is (FortiOS 7.6 -- Verified)

NTurbo is a hardware-based acceleration feature available on specific FortiGate models. It is designed to improve antivirus and IPS performance when operating in flow-based inspection mode.

NTurbo works by creating a fast, optimized data path between:

FortiGate ingress interface

IPS/AV engine

FortiGate egress interface

This minimizes CPU involvement and reduces packet traversal overhead.

Why Option A Is Correct

A . For flow-based inspection, NTurbo establishes a dedicated data path to redirect traffic between the IPS engine and FortiGate ingress and egress interfaces.

This is exactly how NTurbo works, as documented:

NTurbo applies to flow-based inspection only

It accelerates IPS and antivirus scanning

It creates a dedicated fast path that bypasses unnecessary processing steps

This significantly improves throughput and lowers latency

This description matches Fortinet's official explanation of NTurbo.

Why the Other Options Are Incorrect

B . NTurbo creates two inspection sessions

Incorrect. NTurbo does not duplicate sessions; it optimizes the packet path.

C . NTurbo offloads traffic to the content processor (proxy-based)

Incorrect. NTurbo does not apply to proxy-based inspection and does not offload to content processors.

D . NTurbo buffers the whole file and then sends it to the antivirus engine

Incorrect. Buffering entire files is a proxy-based behavior, not NTurbo.

Question 2

Question Type: MultipleChoice

Which two components are part of the secure internet access (SIA) agent-based mode on FortiSASE? (Select two.)

Options:

A- FortiSASE Firewall-as-a-Service (FWaaS)
B- The proxy auto-configuration (PAC) file
C- VPN policies
D- FortiExtender

Answer:

A, C

Explanation:

In FortiSASE Secure Internet Access (SIA) agent-based mode, traffic steering and security enforcement rely on components integrated with the FortiClient agent.

Components used in SIA agent-based mode

A . FortiSASE Firewall-as-a-Service (FWaaS)

Correct.

FWaaS is a core security component of FortiSASE.

It enforces firewall policies, security inspection, and access control for agent-based users.

All user traffic tunneled by the agent is inspected by FWaaS.

C . VPN policies

Correct.

In agent-based mode, the FortiClient establishes a secure tunnel to FortiSASE.

VPN policies define:

Authentication

Access control

Traffic steering

These policies are fundamental to agent-based connectivity.

Why the other options are incorrect

B . Proxy auto-configuration (PAC) filePAC files are used in agentless or proxy-based modes, not agent-based SIA.

D . FortiExtenderFortiExtender is a WAN extension device and is unrelated to FortiSASE SIA agent-based architecture.

Question 3

Question Type: MultipleChoice

When configuring firewall policies Which option best is true regarding the policy ID? (Choose two.)

Options:

A- A firewall policy ID identifies the order of policy execution in firewall policies.
B- A policy ID cannot be modified once a policy is created.
C- You can create a policy in CLI with policy ID 0
D- It is mandatory to provide a policy ID while creating a firewall policy regardless of GUI or CLI.

Answer:

B, C

Explanation:

Comprehensive and Detailed 150 to 200 words of Explanation From Exact Extract of FortiOS 7.6 documents:

According to the FortiOS 7.6 Administration Guide, the firewall policy ID is a unique numerical identifier assigned to each policy for internal database tracking and management purposes. It is important to distinguish the policy ID from the policy sequence. While the FortiGate processes traffic based on a top-down approach (the sequence), the policy ID itself does not determine the order of execution (Statement A is incorrect).

In FortiOS, once a policy is committed to the configuration, the policy ID cannot be modified (Statement B). If an administrator needs to change a policy ID, they must either delete and recreate the policy or use the clone command in the CLI to copy the settings to a new ID.

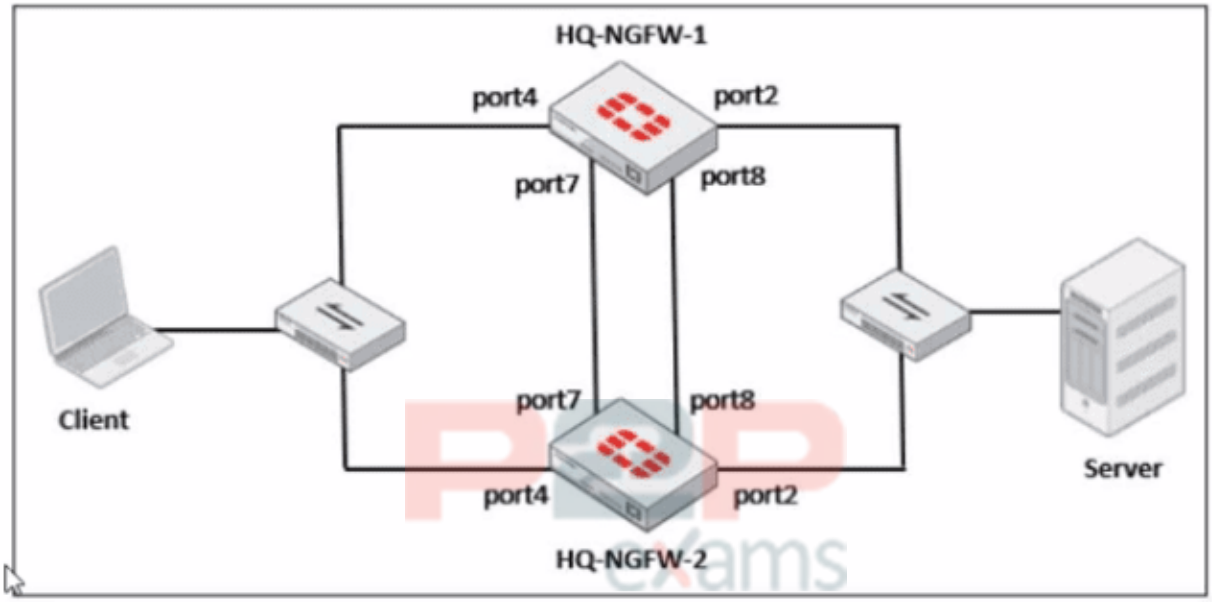
Furthermore, the CLI provides a specific shortcut for policy creation: you can create a policy with ID 0 (Statement C). When the command edit 0 is used within the config firewall policy context, the FortiOS kernel automatically assigns the next available integer as the policy ID. This is a standard practice for efficient configuration via the command line. Statement D is incorrect because, while every policy must have an ID, the GUI automatically generates this value without requiring the user to manually provide or even see it during the initial creation process.

Question 4

Question Type: MultipleChoice

Refer to the exhibits.

FortiGate HA cluster topology



Current HA status

```
HQ-NGFW-1 # get system ha status
 ...
Configuration Status:
    FGVM02TM24013423(updated 0 seconds ago): in-sync
    FGVM02TM24013423 chksum dump: e1 60 2e 42 b8 c1 c6 df 11 34 0c 21 80 79 a4 9f
    FGVM02TM24013501(updated 4 seconds ago): in-sync
    FGVM02TM24013501 chksum dump: e1 60 2e 42 b8 c1 c6 df 11 34 0c 21 80 79 a4 9f
 ...
number of member: 2
HQ-NGFW-1       , FGVM02TM24013423, HA cluster index = 1
HQ-NGFW-2       , FGVM02TM24013501, HA cluster index = 0
number of vcluster: 1
vcluster 1: work 169.254.0.2
Primary: FGVM02TM24013423, HA operating index = 0
Secondary: FGVM02TM24013501, HA operating index = 1
```

New FortiGate HA configuration

```
HQ-NGFW-1
# config system ha
      set group-id 5
      set group-name "Fortinet"
      set mode a-p
      set password *
      set hbdev "port7" 50 "port8" 60
      set session-pick enable
      set override disable
      set priority 90
      set monitor "port3"


HQ-NGFW-2
# config system ha
      set group-id 5
      set group-name "Fortinet"
      set mode a-p
      set password *
      set hbdev "port7" 50 "port8" 60
      set session-pick enable
      set override enable
      set priority 110
      set monitor "port3"
```

Based on the current HA status, an administrator updates the override and priority parameters on HQ-NGFW-1 and HQ-NGFW-2 as shown in the exhibits.

What would be the expected outcome in the HA cluster?

Options:

A- HQ-NGFW-2 will take over as the primary because it has the override enable setting and higher priority than HQ-NGFW-1.
B- HQ-NGFW-1 will remain the primary because HQ-NGFW-2 has lower priority
C- The HA cluster will become out of sync because the override setting must match on all HA members.
D- HQ-NGFW-1 will synchronize the override disable setting with HQ-NGFW-2.

Answer:

A

Explanation:

From the current HA status, HQ-NGFW-1 is the primary and HQ-NGFW-2 is the secondary.

The administrator then changes these HA parameters:

HQ-NGFW-1: set override disable, set priority 90

HQ-NGFW-2: set override enable, set priority 110

In FGCP (A-P mode), the override (preemption) feature controls whether a higher-priority unit is allowed to take over the primary role.

When override is enabled, the cluster will prefer (and can re-elect) the unit with the highest device priority to become primary (preempting a lower-priority primary when conditions trigger re-election behavior as defined by FGCP).

Here, HQ-NGFW-2 has:

override enabled

higher priority (110) than HQ-NGFW-1 (90)

Therefore, the expected result is that HQ-NGFW-2 becomes the primary.

Why the other options are incorrect:

B is incorrect because it claims HQ-NGFW-2 has lower priority (it is higher: 110 > 90).

C is incorrect because a mismatch in the override setting is not what causes the ''configuration out of sync'' condition shown in get system ha status (that is about synchronized configuration databases, not a requirement that override values must match to remain in-sync).

D is incorrect because HA settings like override/priority are not synchronized in the way regular configuration objects are; they are device-level HA parameters.

Question 5

Question Type: MultipleChoice

Refer to the exhibits.

HA configuration

```
HQ-NGFW-1 # config system ha

HQ-NGFW-1 (ha) # show
config system ha
    set group-id 5
    set group-name "Training"
    set mode a-p
    set password ENC a4fbyqY4iPexFmAnZgzDY
    set hbdev "port7" 0
    set session-pickup enable
    set override disable
    set priority 200
    set monitor "port1"
    set memory-based-failover enable
    set memory-failover-threshold 70
    set memory-failover-monitor-period 50
    set memory-failover-sample-rate 10
    set memory-failover-flip-timeout 60
end
```

HQ-NGFW-1 System Performance output

```
HQ-NGFW-1 # get system performance status
CPU states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU0 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU1 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
Memory: 2042076k total, 1837868k used (90%), 104146k free (5.1%), 100062k freeable (4.9%)
Average network usage: 19/2 kbps in 1 minute, 19/4 kbps in 10 minutes, 19/3 kbps in 30 minutes
Maximal network usage: 36/18 kbps in 1 minute, 58/86 kbps in 10 minutes, 58/87  kbps in 30 minutes
Average sessions: 21 sessions in 1 minute, 22 sessions  in 10 minutes, 21 sessions in 30 minutes
Maximal sessions: 22 sessions in 1 minute, 28 sessions  in 10 minutes, 28 sessions in 30 minutes
Average session setup rate: 0 sessions per second in last 1 minute, 0 sessions per second in last 10 minutes
Maximal session setup rate: 0 sessions per second in last 1 minute, 1 sessions per second in last 10 minutes
Average NPU sessions: 0 sessions in last 1 minute, 0 sessions in last 10 minutes, 0 sessions in last 30 minutes
Maximal NPU sessions: 0 sessions in last 1 minute, 0 sessions in last 10 minutes, 0 sessions in last 30 minutes
Virus caught: 0 total in 1 minute
IPS attacks blocked: 0 total in 1 minute
Uptime: 10 days, 22 hours, 50 minutes
```

HQ-NGFW-2 System Performance output

```
HQ-NGFW-2 # get system performance status
CPU states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU0 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU1 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
Memory: 2042076k total, 993836k used (48.7%), 690352k free (33.8%), 357888k freeable (17.5%)
Average network usage: 26/18 kbps in 1 minute, 25/18 kbps in 10 minutes, 24/18 kbps in 30 minutes
Maximal network usage: 91/27 kbps in 1 minute, 92/27 kbps in 10 minutes, 92/32  kbps in 30 minutes
Average sessions: 9 sessions in 1 minute, 9 sessions    in 10 minutes, 9 sessions in 30 minutes
Maximal sessions: 11 sessions in 1 minute, 11 sessions  in 10 minutes, 13 sessions in 30 minutes
Average session setup rate: 0 sessions per second in last 1 minute, 0 sessions per second in last 10 minutes
Maximal session setup rate: 0 sessions per second in last 1 minute, 1 sessions per second in last 10 minutes
Average NPU sessions: 0 sessions in last 1 minute, 0 sessions in last 10 minutes, 0 sessions in last 30 minutes
Maximal NPU sessions: 0 sessions in last 1 minute, 0 sessions in last 10 minutes, 0 sessions in last 30 minutes
Virus caught: 0 total in 1 minute
IPS attacks blocked: 0 total in 1 minute
Uptime: 10 days, 10 hours, 50 minutes
```

An administrator has observed the performance status outputs on an HA cluster for 55 seconds.

Which FortiGate is the primary?

Options:

A- HQ-NGFW-1 with the parameter memory-failover-flip-timeout setting
B- HQ-NGFW-2 with the parameter priority setting
C- HQ-NGFW-1 with the parameter override setting
D- HQ-NGFW-2 with the parameter memory-failover-threshold setting

Answer:

D

Explanation:

From the HA configuration shown for HQ-NGFW-1:

set memory-based-failover enable

set memory-failover-threshold 70

set memory-failover-monitor-period 50

set memory-failover-sample-rate 10

set memory-failover-flip-timeout 60

set override disable

set priority 200

From the performance status outputs:

HQ-NGFW-1 memory used is 90% (well above the configured threshold of 70%)

HQ-NGFW-2 memory used is about 48.7% (well below the threshold)

What happens in FortiOS 7.6 with memory-based failover

When memory-based failover is enabled, FortiGate monitors memory utilization. If the unit's memory usage stays above the configured memory-failover-threshold for the configured memory-failover-monitor-period, the cluster triggers a failover away from the unit under memory pressure.

Threshold = 70%

HQ-NGFW-1 is at 90%, so it violates the threshold.

Monitor period = 50 seconds.

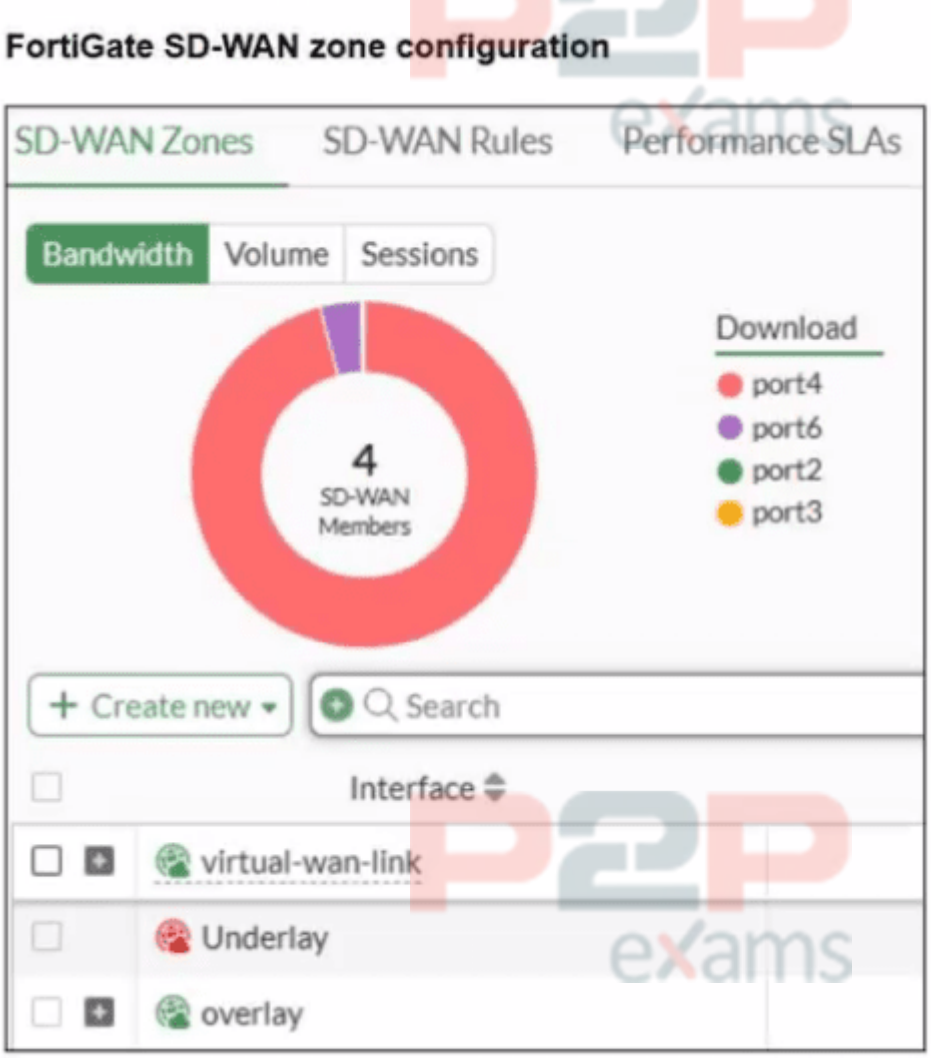
The administrator observed for 55 seconds, which is longer than 50 seconds, so the condition is met for long enough to trigger failover.

The memory-failover-flip-timeout 60 is used to prevent rapid back-and-forth role changes (flapping) after a failover decision; it does not prevent the initial failover from occurring once the threshold breach persists for the monitor period.

Question 6

Question Type: MultipleChoice

Refer to the exhibit.



An SD-WAN zone configuration on the FortiGate GUI is shown. Based on the exhibit, which statement is true?

Options:

A- The Underlay zone contains no member.

B- The virtual-wan-link and overlay zones can be deleted
C- The Underlay zone is the zone by default.
D- port2 and port3 are not assigned to a zone.

Answer:

A

Explanation:

According to the FortiOS 7.6 Administrator Guide and the specific behavior of the SD-WAN GUI, here is the technical breakdown:

SD-WAN Zone Hierarchy and UI Elements: In the FortiGate GUI, SD-WAN zones that contain member interfaces are displayed with a plus (+) icon next to the checkbox. This icon allows administrators to expand the zone and view the specific physical or logical interfaces assigned to it.

Analysis of the 'Underlay' Zone: In the provided exhibit, the virtual-wan-link and overlay zones both feature the plus (+) expansion icon, indicating they have active members. The Underlay zone, however, lacks this icon and displays a red status icon. This is the visual indicator in FortiOS that the zone is currently empty and contains no member interfaces.

Mandatory Zone Membership: In FortiOS 7.x, every SD-WAN member interface must be assigned to a zone. It is not possible for an interface to be an 'SD-WAN member' (as shown in the legend with port2 and port3) without being assigned to a zone. Since port2 and port3 are listed in the legend, they are indeed assigned to one of the other expanded zones (likely virtual-wan-link or overlay), making Option D incorrect.

Default Zone Behavior: While FortiOS 7.6 often creates default zones like virtual-wan-link, underlay, and overlay during certain configuration wizards or by default in newer versions, they are distinct entities. There is no single 'default' zone that acts as a global catch-all in the way Option C suggests.

Immutability of System Zones: While certain system-defined zones have restrictions, the primary focus of this specific exhibit is the current membership state, which clearly shows the Underlay zone is empty.