Prepare Smart for Success Free Fortinet NSE4_FGT_AD-7.6 Exam Questions and Answers

Ready to pass faster? Grab free and updated Fortinet NSE 4 - FortiOS 7.6 Administrator exam PDF questions now. Get authentic NSE4_FGT_AD-7.6 dumps packed with verified answers and secure your certification success with PrepBolt NSE4_FGT_AD-7.6 exam pdf questions and answers.

Thank you for Downloading NSE4_FGT_AD-7.6 exam PDF Demo

https://prepbolt.com/NSE4_FGT_AD-7.6.html

Question 1

Question Type: MultipleChoice

Refer to the exhibit.

Refer to the exhibit.

Packet trace output

Time	Message
Packet Trace #1 14	
06:39:29	vd-root:0 received a packet(proto=1, 10.0.11.50:3->100.65.0.254:2048) tun_id=0.0.0.0 from port4. type=8, code=0, id=3, seq=168.
06:39:29	allocate a new session-00000ec6
06:39:29	in-[port4], out-[]
06:39:29	len=0
06:39:29	result: skb_flags-02000000, vid-0, ret-no-match, act-accept, flag-00000000
06:39:29	find a route: flag=00000000 gw-0.0.0.0 via port2
06:39:29	in-[port4], out-[port2], skb_flags-02000000, vid-0, app_id: 0, url_cat_id: 0
06:39:29	gnum-100004, use addr/intf hash, len=1
06:39:29	checked gnum-100004 policy-0, ret-matched, act-accept
06:39:29	ret-matched
06:39:29	policy-0 is matched, act-drop
06:39:29	after iprope_captive_check(): is_captive-0, ret-matched, act-drop, idx-0
06:39:29	after iprope_captive_check(): is_captive-0, ret-matched, act-drop, idx-0
06:39:29	Denied by forward policy check (policy 0)

Why did the FortiGate device drop the packet?

Options:

A- It matched the default implicit firewall policy.
B- It failed the RPF check.
C- It matched an explicitly configured firewall policy with the action DENY.
D- It cannot reach the next-hop IP.

Answer:

A

Explanation:

''FortiGate looks for the matching firewall policy from top-to-bottom and, if a match is found, the traffic is processed based on the firewall policy. If no match is found, the traffic is dropped by the default

implicit deny firewall policy.''

Technical Deep Dive:

The debug flow output clearly points to the implicit deny:

ret-no-match

policy-0 is matched, act-drop

Denied by forward policy check (policy 0)

On FortiGate, policy 0 is the internal representation of the default implicit deny firewall policy. That means the packet did not match any user-defined forward firewall policy, so FortiGate dropped it automatically.

Why the other options are wrong:

B is wrong because an RPF failure would show a reverse-path-related drop reason, not Denied by forward policy check (policy 0).

C is wrong because the trace does not show a matched explicit policy ID with deny action; it shows policy 0, which is the implicit rule.

D is wrong because the trace actually shows a route lookup result: find a route: ... gw-0.0.0.0 via port2. So this is not a next-hop reachability failure.

In packet-flow troubleshooting, this pattern is one of the most important to recognize. If you see policy 0 in FortiGate debug flow, the first things to verify are:

diagnose debug flow filter addr <src_or_dst_ip>

diagnose debug flow show function-name enable

diagnose debug enable

Then review whether a firewall policy exists with the correct incoming interface, outgoing interface, source, destination, schedule, and service. If any one of those does not match, FortiGate falls through to policy 0 and drops the session.

Question 2

Question Type: MultipleChoice

Refer to the exhibit.

```
date=2025-09-03 time=09:09:57 id=7545895911432388608 itime="2025-09-03 09:10:02" euid=3 epid=3 dsteuid=3 dstepid=101
logflag=0 logver=706003401 type="utm" subtype="app-ctrl" level="warning" action="block" sessionid=510 policyid=1 srcip=
10.0.11.50 dstip=54.146.230.62 srcport=53398 dstport=80 proto=6 logid=1059028705 service="HTTP" eventtime=
1756915797391471958 incidentserialno=116391982 direction="outgoing" apprisk="elevated" appid=30220 srcintfrole="undefined"
dstintfrole="undefined" applist="default" appcat="Video/Audio" app="ABC.Com" hostname="abc.go.com" url="/favicon.ico"
eventtype="signature" srcintf="port4" dstintf="port2" msg="Video/Audio: ABC.Com" tz="-0700" policytype="policy"
srccountry="Reserved" dstcountry="United States" poluuid="b11ac58c-791b-51e7-4600-12f829a689d9" agent="Mozilla/5.0 (X11;
Ubuntu; Linux x86_64; rv:142.0) Gecko/20100101 Firefox/142.0" httpmethod="GET" referralurl="http://abc.go.com/"
devid="FGVM02TM24013423" vd="root" dtime="2025-09-03 09:09:57" itime_t=1756915802 devname="HQ-NGFW-1"
```

Which two ways can you view the log messages shown in the exhibit? (Choose two.)

Options:

A- By right clicking the implicit deny policy
B- Using the FortiGate CLI command diagnose log test
C- By filtering by policy universally unique identifier (UUID) and application name in the log entry
D- In the Forward Traffic section

Answer:

C, D

Explanation:

The exhibit shows a FortiGate UTM application control log with fields such as:

type='utm'

subtype='app-ctrl'

action='block'

policyid=1

appid=30220

appcat='Video/Audio'

service='HTTP'

apprisk='elevated'

This is a forward traffic security log, generated by Application Control applied to a firewall policy.

Why the correct answers are C and D

C . By filtering by policy universally unique identifier (UUID) and application name in the log entry

Correct.

FortiOS logs can be viewed and filtered in:

Log & Report Forward Traffic

Administrators can filter logs using fields such as:

Policy ID / Policy UUID

Application name (app)

Application ID (appid)

The log entry clearly includes application-related fields, making filtering by policy and application a valid and documented way to view these logs.

D . In the Forward Traffic section

Correct.

The log is a UTM Application Control log for traffic passing through a firewall policy.

Such logs are displayed under:

Log & Report Forward Traffic

This is the standard and correct location to view application control, web filter, IPS, and other security profile logs related to user traffic.

Why the other options are incorrect

A . By right clicking the implicit deny policy

Incorrect.

Implicit deny policies do not generate UTM forward traffic logs like the one shown.

Application control logs are generated only by explicit firewall policies with security profiles enabled.

B . Using the FortiGate CLI command diagnose log test

Incorrect.

diagnose log test is used to test log connectivity and log settings, not to view historical log entries.

It does not display traffic or UTM logs.

Question 3

Question Type: MultipleChoice

What are two characteristics of HA cluster heartbeat IP addresses in a FortiGate device? (Choose two.)

Options:

A- Heartbeat IP addresses are used to distinguish between cluster members.
B- The heartbeat interface of the primary device in the cluster is always assigned IP address 169.254.0.1.
C- A change in the heartbeat IP address happens when a FortiGate device joins or leaves the cluster.
D- Heartbeat interfaces have virtual IP addresses that are manually assigned.

Answer:

A, C

Explanation:

In FortiOS 7.6, HA cluster heartbeat IP addresses are automatically managed by FortiGate and play a critical role in cluster communication and synchronization.

Correct statements

A . Heartbeat IP addresses are used to distinguish between cluster members.

Correct

FortiGate assigns unique heartbeat IP addresses (link-local addresses in the 169.254.0.0/16 range) to each HA member.

These addresses are used for:

Cluster member identification

Health checks

Synchronization traffic

This allows FortiGate units to uniquely identify and communicate with each other inside the HA cluster.

C . A change in the heartbeat IP address happens when a FortiGate device joins or leaves the cluster.

Correct

Heartbeat IPs are dynamically assigned.

When:

A new FortiGate joins the cluster, or

A member leaves or fails,

FortiGate may reassign heartbeat IP addresses to maintain unique identification among members.

This behavior is documented in the FortiOS HA operation and troubleshooting guides.

Why the other options are incorrect

B . The heartbeat interface of the primary device is always assigned IP address 169.254.0.1.

Incorrect

There is no fixed or guaranteed heartbeat IP (such as 169.254.0.1) for the primary unit.

Heartbeat IP assignment is dynamic, not role-based.

D . Heartbeat interfaces have virtual IP addresses that are manually assigned.

Incorrect

Heartbeat IP addresses are:

Automatically assigned

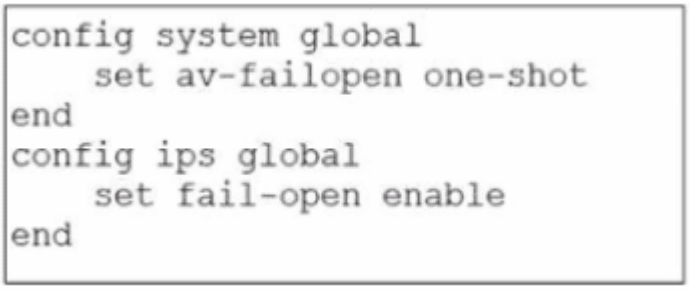
Link-local

Administrators do not manually configure heartbeat IP addresses.

Question 4

Question Type: MultipleChoice

Refer to the exhibit.



```
config system global
    set av-failopen one-shot
end
config ips global
    set fail-open enable
end
```

Based on this partial configuration, what are the two possible outcomes when FortiGate enters conserve mode? (Choose two.)

Options:

A- FortiGate drops new sessions requiring inspection.
B- Administrators must restart FortiGate to allow new sessions.
C- Administrators cannot change the configuration.
D- FortiGate skips quarantine actions.

Answer:

C, D

Question 5

Question Type: MultipleChoice

You have configured an application control profile, set peer-o-peer traffic to Block under the Categories tab, and applied it to the firewall policy. However, you 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- Replacement Messages for UDP-based Applications
B- Network Protocol Enforcement
C- Application and Filter Overrides
D- FortiGuard category ratings

Answer:

C

Explanation:

''After the IPS engine examines the traffic stream for a signature match, FortiGate scans packets for matches, in this order, for the application control profile:

1. Application and filter overrides...''

''Because application overrides are applied first in the scan, these two applications are allowed and generate logs.''

''The priority in which application and filter overrides are placed takes precedence.''

Technical Deep Dive:

The correct answer is C. Application and Filter Overrides.

If you already set the P2P category to Block, but some peer-to-peer traffic is still being allowed, the first thing to check is whether there is an application override or filter override that matches that traffic before the category action is applied. FortiGate processes Application and Filter Overrides before Categories, so any matching override set to Allow or Monitor will effectively bypass the category block.

Why the others are wrong:

A only affects user-facing block-page behavior for HTTP/HTTPS applications, not whether P2P is blocked.

B is for enforcing expected services on expected ports and for blocking applications on non-default ports. It is not the first place to look when a category block is being bypassed.

D concerns web categorization, not application-control category enforcement.

Operationally, this is a classic troubleshooting sequence: first inspect the override table, then the category action, then logs under Application Control to see which signature and action actually matched.

Question 6

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 answers)

Options:

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

Answer:

A, D

Explanation:

''To successfully form an HA cluster, you must ensure that the members have the same:

* Model: hardware model or VM model

* Firmware version

* Licensing: includes the FortiGuard license, virtual domain (VDOM) license, FortiClient license, and so on

* Hard drive configuration: the same number and size of drives and partitions

* Operating mode: the operating mode---NAT mode or transparent mode---of the management VDOM.''

''From a configuration and setup point of view, you must ensure that the HA settings on each member have the same group ID, group name, password, and heartbeat interface settings. Try to place all heartbeat interfaces in the same broadcast domain, or for two-member clusters, connect them directly.''

Technical Deep Dive:

The correct answers are A and D.

A is correct because FGCP cluster formation requires matching HA parameters, and group ID is explicitly one of them. If the group ID differs, the units will not consider each other part of the same cluster during HA discovery and election.

D is correct because FortiGate HA expects hardware parity in critical platform characteristics, including hard drive configuration. If disk layout differs, the members do not satisfy the HA formation prerequisites.

B is incorrect because the study guide does not require heartbeat interfaces to be in the same IP subnet. The requirement is that heartbeat links be in the same broadcast domain, or directly connected in a two-node design. In practice, heartbeat links are Layer 2 adjacency links; IP subnet matching is not the stated requirement.

C is incorrect because the guide does not say both units must start with the same number of configured VDOMs. What must match is the licensing level and the operating mode of the management VDOM. After cluster formation, the primary synchronizes its configuration to the secondary.

A practical verification set before forming FGCP HA is:

get system status

show system ha

diagnose sys ha status

Operationally, FGCP then uses the heartbeat links for member discovery, health monitoring, election, and config/session synchronization. On supported hardware, session forwarding and HA processing can still benefit from FortiGate's ASIC-assisted architecture, but HA state, config sync, and election logic remain control-plane functions handled by FortiOS.

Thank You for trying NSE4_FGT_AD-7.6 PDF Demo

To try our NSE4_FGT_AD-7.6 practice exam software visit link below

https://prepbolt.com/NSE4_FGT_AD-7.6.html

Start Your NSE4_FGT_AD-7.6 Preparation

Use Coupon “SAVE50” for extra 50% discount on the purchase of Practice Test Software. Test your NSE4_FGT_AD-7.6 preparation with actual exam questions.