Vendor: Fortinet

Exam Code: NSE7_FSN_AR-7.6

Exam Name: Fortinet NSE 7 - Secure Networking 7.6 Architect

Version: DEMO

QUESTION 1
Refer to the exhibit, which shows the output of a BGP debug command. What can you conclude about the router in this scenario?

```
# get router info bgp summary

VRF 0 BGP router identifier 0.0.0.117, local AS number 65117
BGP table version is 3
3 BGP AS-PATH entries
0 BGP community entries

Neighbor        V         AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.125.0.60     4      65060    1698    1756      103    0    0 03:02:49        1
10.127.0.75     4      65075    2206    2250      102    0    0 02:45:55        1
100.64.3.1      4      65501    101     115         0    0    0 never       Active

Total number of neighbors 3
```

A. The router 100.64.3.1 needs to update the local AS number in its BGP configuration in order to bring up the 8GP session with the local router.
B. An inbound route-map on local router is blocking the prefixes from neighbor 100.64.3.1.
C. All of the neighbors displayed are part of a single BGP configuration on the local router with the neighbor-range set to a value of 4.
D. The BGP session with peer 10.127.0.75 is up.

Answer: D
Explanation:
The BGP debug output shows session information for peers, including state details. According to official Fortinet BGP documentation, if the session state with a peer does not show "Idle," "Active," or "Connect," but instead shows "Established," "Up," or related counters (e.g., messages sent/received or uptime), it indicates the session is operational. In this scenario, the peer 10.127.0.75 is the only one showing a positive indication of a live, established session. Other options like neighbor-range configuration, AS mismatch, or route-maps blocking prefixes are not supported by evidence provided in a simple BGP session state debug, nor does the output show errors relating to local or remote AS issues.

The correct interpretation comes from Fortinet's BGP troubleshooting guide, which outlines how to read session status and neighbor states in debug and summary outputs.

QUESTION 2
Which two statements about an auxiliary session ate true? (Choose two.)

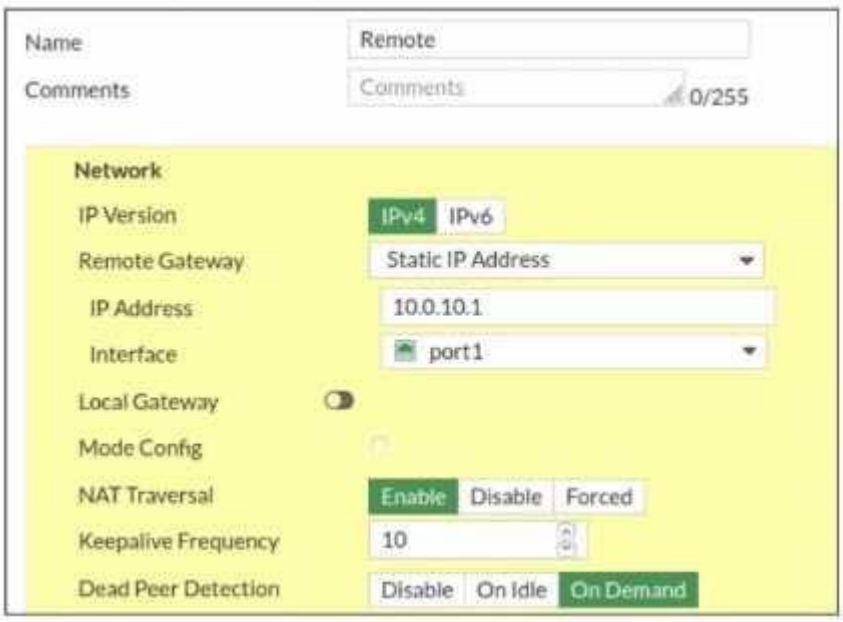
A. With the auxiliary session selling disabled, only auxiliary sessions are offloaded.
B. With the auxiliary session setting enabled, ECMP traffic is accelerated to the NP6 processor.
C. With the auxiliary session setting enabled, two sessions are created in case of routing change.
D. With the auxiliary session setting disabled, for each traffic path. FortiGate uses the same auxiliary session.

Answer: BC
Explanation:
Auxiliary sessions in Fortinet are designed to support ECMP (Equal Cost Multi-Path) and SD-WAN scenarios, allowing sessions to be handled efficiently when traffic needs to be dynamically distributed across multiple links. With the auxiliary session setting enabled, FortiGate creates additional session table entries for each possible path in ECMP or SD-WAN--meaning that if the

routing path changes (such as a link failover), a new session can be immediately activated and offloaded to the NP6 network processor for acceleration, ensuring minimal disruption. This greatly benefits high-throughput deployments.

Official documentation specifies that when auxiliary sessions are enabled, FortiGate doesn't just rely on dynamically creating new sessions after a routing event, it proactively creates sessions for all potential paths. This means that in the event of a route change, two sessions exist and the traffic is quickly re-routed and offloaded, maximizing performance and reliability. Without this feature, multiple paths cannot be efficiently offloaded, and routing changes trigger a single session update, reducing failover performance.

QUESTION 3
Refer to the exhibit, which contains a screenshot of some phase 1 settings.



The VPN is not up. To diagnose the issue, the administrator enters the following CLI commands on an SSH session on FortiGate:

```
diagnose vpn ike log-filter dst-addr4 10.0.10.1
diagnose debug application ike -1
```

However, the IKE real-time debug does not show any output. Why?

A. The administrator must also run the command diagnose debug enable.
B. The debug shows only error messages. If there is no output, then the phase 1 and phase 2 configurations match.
C. The log-filter setting is incorrect. The VPN traffic does not match this filter.
D. Replace diagnose debug application ike -1 with diagnose debug application ipsec -1.

Answer: A
Explanation:
To display debug output on FortiGate devices, you must always run both the application-specific

debug command and the global debug enable command. The command diagnose debug application ike -1 sets up the detail level for the IKE daemon debug, but it does not display any debug output on its own. As described in the FortiOS CLI debugging manuals, the command diagnose debug enable activates debug output on the console, making all previously set debugs visible. This is especially important for VPN troubleshooting--without the enable command, no output appears even if there is VPN traffic.

The correct diagnostic sequence is:

diagnose debug application ike -1

diagnose debug enable

This procedure is found in every FortiOS CLI debug tutorial and troubleshooting workflow.

QUESTION 4
Which two statements are true regarding heartbeat messages sent from an FSSO collector agent to FortiGate? (Choose two.)

A. The heartbeat messages can be seen using the command diagnose debug authd fsso list.
B. The heartbeat messages can be seen in the collector agent logs.
C. The heartbeat messages can be seen on FortiGate using the real-lime FSSO debug.
D. The heartbeat messages must be manually enabled on FortiGate.

Answer: BC
Explanation:
According to the official Fortinet documentation (Technical Tip: Useful FSSO Commands), heartbeat messages play a crucial role in communication between the FSSO Collector Agent and FortiGate. These messages are regularly sent from the Collector Agent to verify its status, maintain session awareness, and confirm connectivity between the authentication infrastructure and FortiGate appliances.

Option B is confirmed by Fortinet, as the collector agent logs on Windows or its management console will specifically note heartbeat events, connection status, and any issues maintaining contact with FortiGate units.

Option C is validated by both official CLI documentation and the technical tip linked. On FortiGate, heartbeat messages from the collector agent are visible using real-time debug tools such as diagnose debug application authd or FSSO-specific commands. These enable administrators to monitor live logon states, session status, and connection health directly from the FortiGate CLI. The debug stream shows heartbeats received and their effect on active logons, associating health monitoring with active sessions.

Heartbeat operation is fully automated once FSSO is set up--there is no requirement for manual enablement or configuration, aligning with Fortinet's philosophy of seamless integration and centralized management across the Security Fabric. This ensures that both FortiGate and the collector agent can quickly and reliably detect any miscommunication or outage, addressing authentication issues proactively.

QUESTION 5
Refer to the exhibit, which shows a truncated output of a real-time LDAP debug. What two conclusions can you draw from the output? (Choose two.)

```
# diagnose debug application fnbamd -1
# diagnose debug enable
   fnbamd_fsm.c[1274] handle_req-Rcvd auth req 8781845 for jsmith in Lab opt=27 prot=0
   fnbamd_ldap.c[637] resolve_ldap_FQDN-Resolved address 10.10.181.10, result 10.10.181.10
   fnbamd_ldap.c[232] start_search_dn-base:'DC=TAC,DC=ottawa,DC=fortinet,DC=com' filter:sAMAccountName=jsmith
   fnbamd_ldap.c[1351] fnbamd_ldap_get_result-Going to SEARCH state
   fnbamd_fsm.c[1833] poll_ldap_servers-Continue pending for req 8781845
   fnbamd_ldap.c[266] get_all_dn-Found DN 1:CN=John Smith,CN=Users,DC=TAC,DC=ottawa,DC=fortinet,DC=com
```

A. The name of the configured LDAP server is Lab.
B. The user is authenticating using CN=John Smith.
C. FortiOS is able to locate the user in step 3 (Bind Request) of the LDAP authentication process.
D. FortiOS is performing the second step (Search Request) in the LDAP authentication process.

Answer: AD
Explanation:
The exhibit shows these key lines:

handle_req-Rcvd auth req ... for jsmith in Lab

start_search_dn-base:'DC=TAC,DC=ottawa,DC=fortinet,DC=com' filter:sAMAccountName=jsmith

get_all_dn-Found DN 1:CN=John Smith,CN=Users,DC=TAC,DC=ottawa,DC=fortinet,DC=com

The study guide explicitly shows the same LDAP real-time debug pattern and says the request line includes the LDAP server object name:

handle_req-Rcvd auth req ... for jsmith in Lab ...

That supports A: Lab is the configured LDAP server name being used for this authentication request.

For the LDAP flow stage, the study guide states:

"An fnbamd_ldap_build_dn_search_req-base message indicates that FortiGate is performing step two: searching for the user in the LDAP tree." It also says that if the LDAP server finds the user, the output shows the user's full DN.

That matches the exhibit's start_search_dn-base ... filter:sAMAccountName=jsmith and Found DN ... CN=John Smith... lines, so D is correct.

QUESTION 6
Refer to the exhibit, which shows a session entry. Which statement about this session is true?

```
session_info: proto=1 proto_state=00 duration=1 expire=59 timeout=0 flags=00000000
sockflag=00000000 sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=log may_dirty none
statistic (bytes/packets/allow_err): org=168/2/1 reply=168/2/1 tuples=2
tx speed (Bps/kbps) : 97/0 rx speed (Bps/kbps) : 97/0
orgin->sink: org pre->post, reply pre->post dev=9->3/3->9 gwy=10.200.1.254/10.1.0.1
hook=post dir=org act=snat 10.1.10.10:40602->10.200.5.1:8 (10.200.1.1:60430)
hook=pre dir=reply act=dnat 10.200.5.1:60430->10.200.1.1:0(10.1.10.10:40602)
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=0
serial=0002a5c9 tos=ff/ff app_list=0 app=0 url_cat=0
dd_type=0 dd_mode=0
```

A. Return traffic to the initiator is sent to 10.1.0.1.
B. Return traffic to the initiator is sent lo 10.200.1.254.
C. It is an ICMP session from 10.1.10.10 to 10.200.1.1.
D. It is an ICMP session from 10.1.10.1 to 10.200.5.1.

Answer: B
Explanation:
The session output reveals a session with proto=1 (ICMP) and the origin and reply directions show address and NAT translations. Specifically, the hook=post dir=org act=snat shows that source NAT is performed for outgoing packets, where the source 10.1.10.10:40602 is translated to 10.200.5.1:8 (likely ICMP id 8, not a TCP/UDP port). The reply direction, hook=pre dir=reply act=dnat, indicates destination NAT for incoming packets: packets incoming for 10.200.5.1:60430 are destination-NATed to 10.1.10.10:40602. The gateway (gwy) is listed as 10.200.1.254/10.1.0.1, which for outgoing traffic means that return traffic is directed to the gateway (10.200.1.254), per the NAT policy. This is confirmed by the FortiOS Session Table Guide, which explains that the returned ICMP reply will be routed out to this NAT gateway. The session statistics and logical flow (SNAT out, matching DNAT in) reinforce that reply traffic to the initiator traverses via 10.200.1.254.

QUESTION 7
Which statement about parallel path processing is correct (PPP)?

A. PPP chooses from a group of parallel options lo identity the optimal path tor processing a packet.
B. Only FortiGate hardware configurations affect the path that a packet takes.
C. PPP does not apply to packets that are part of an already established session.
D. Software configuration has no impact on PPP.

Answer: A
Explanation:
Parallel Path Processing (PPP) in FortiOS refers to the system's ability to evaluate and select among multiple processing paths--often involving dedicated network processors, content processors, or CPU-based workflows--to optimally process packets. The official documentation highlights that the PPP engine dynamically selects which hardware or software path to use for each session based on session characteristics, policy configuration, and traffic type. This dynamic selection results in optimal throughput and resource utilization.

The document specifies that PPP assesses several processing paths in parallel, using decision logic to determine whether a session should be offloaded to specialist hardware (like NP6, CP9, etc.) or stay in the CPU path, ensuring that each packet is handled by the most efficient available

method under current load and policy. Hardware and software configurations both influence this outcome, but it is the PPP engine's decision-making that defines the optimal path per session.

QUESTION 8
In IKEv2, which exchange establishes the first CHILD_SA?

A. IKE_SA_INIT
B. INFORMATIONAL
C. CREATE_CHILD_SA
D. IKE_AUTH

Answer: D
Explanation:
The study guide explicitly states:

"IKE_Auth exchange:

Performs the mutual authentication of two IKE endpoints.

Configures settings like IP/mask, DNS, and so on.

Sets up the piggyback of a child SA. Negotiates IP flow and security settings for the IPsec SA."

It also says:

"By default, a piggyback child (IPsec) SA is negotiated along with the IKEv2 SA during IKE_AUTH. If additional IPsec SAs are needed ... they are negotiated during subsequent CREATE_CHILD_SA exchanges."

QUESTION 9
Which authentication option can you not configure under config user radius on FortiOS?

A. mschap
B. pap
C. mschap2
D. eap

Answer: D
Explanation:
According to the official Fortinet administration guide for FortiOS 7.6.4 under the section "Configuring a RADIUS server," the supported RADIUS authentication methods you can configure via the CLI with config user radius are:

pap

chap

mschap

mschapv2

auto

The relevant CLI syntax is set auth-type {auto | ms_chap_v2 | ms_chap | chap | pap} . You can confirm this directly in the configuration table and from real CLI sessions.

EAP (Extensible Authentication Protocol) is NOT an authentication option you can directly set under config user radius. EAP methods (such as EAP-TLS, EAP-PEAP, EAP-TTLS) are negotiated between the RADIUS client and server but are not configurable as an explicit auth-type option in FortiOS. EAP authentication is typically used automatically by features like 802.1X, not through the user radius object authentication-type setting, and always requires proper backend workings between supplicant and RADIUS server

QUESTION 10
Refer to the exhibit, which shows a partial output of diagnose hardware aysinfo memory. Which two statements about the output are true? (Choose two.)

A. There are 98908 kB of memory that will never be used.
B. The user space has 708880 kB of physical memory that is not used by the system.
C. The I/O cache, which has 641364 kB of memory allocated to it.
D. The value indicated next to the inactive heading represents the currently unused cache page.

Answer: BD
Explanation:
The partial output from diagnose hardware sysinfo memory provides details on system RAM allocation. According to Fortinet's technical documentation for memory troubleshooting and Linux memory management (which FortiOS is based on):

MemFree is the portion of physical memory not currently allocated to any running process or kernel function. Thus, 708880 kB is available and can be immediately used by user-space programs or system operations.

Inactive refers to pages in the memory cache that were previously in use for I/O or file system buffering but are now not actively referenced. These pages are retained in memory for quick access if needed again, but can be reclaimed for other memory operations if demand increases. The value 98908 kB here represents currently unused cache pages (inactive pages), ready for repurposing or deletion if the system requires more RAM.

Cached represents the total amount of system memory allocated to cache, which includes both active and inactive cache pages. It does not, by itself, represent I/O cache exclusively, nor does "inactive" mean memory "will never be used" as the kernel can re-purpose inactive pages on demand.

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.lead2pass.com/all-products.html

10% Discount Coupon Code: **ASTR14**