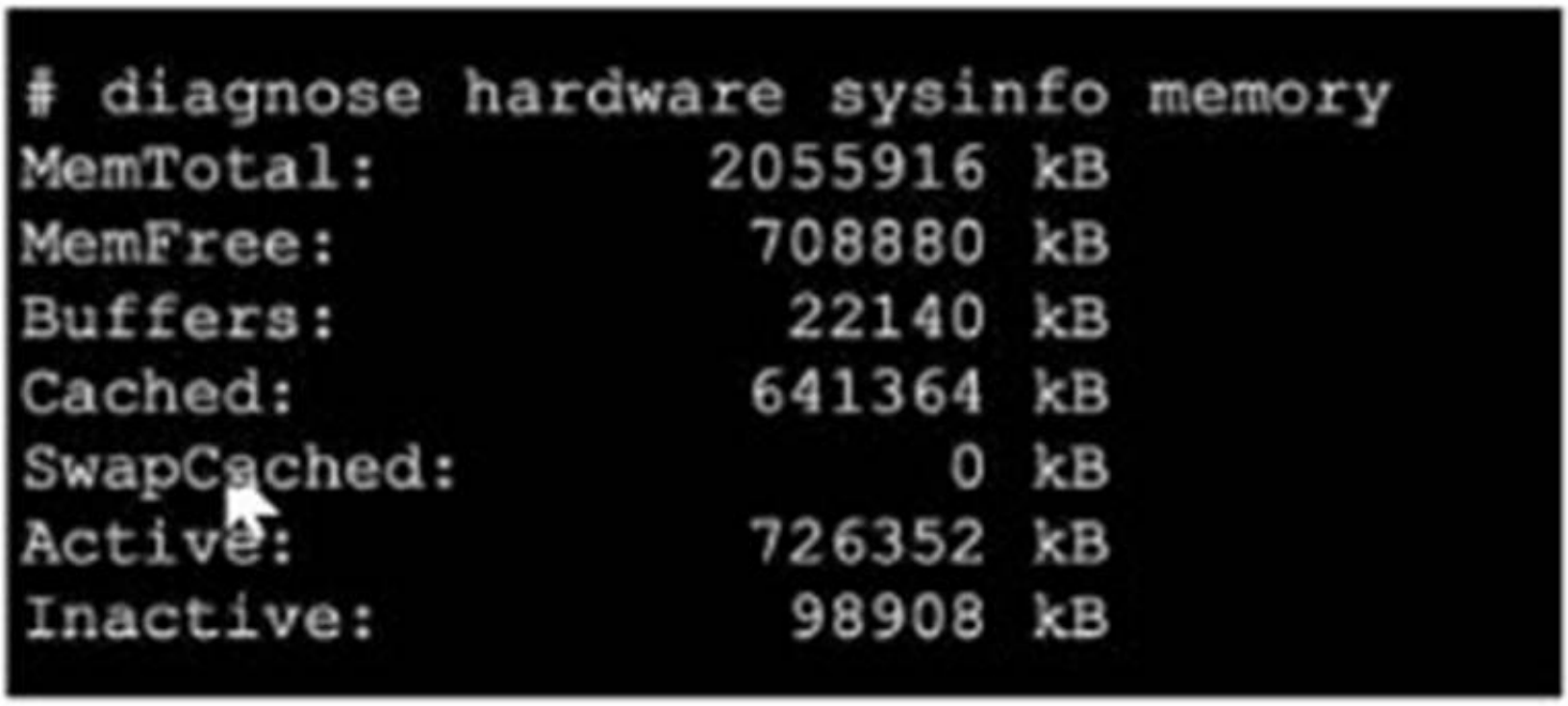
Fortinet

Exam Questions FCSS_NST_SE-7.6

FCSS - Network Security 7.6 Support Engineer

NEW QUESTION 1
Exhibit.

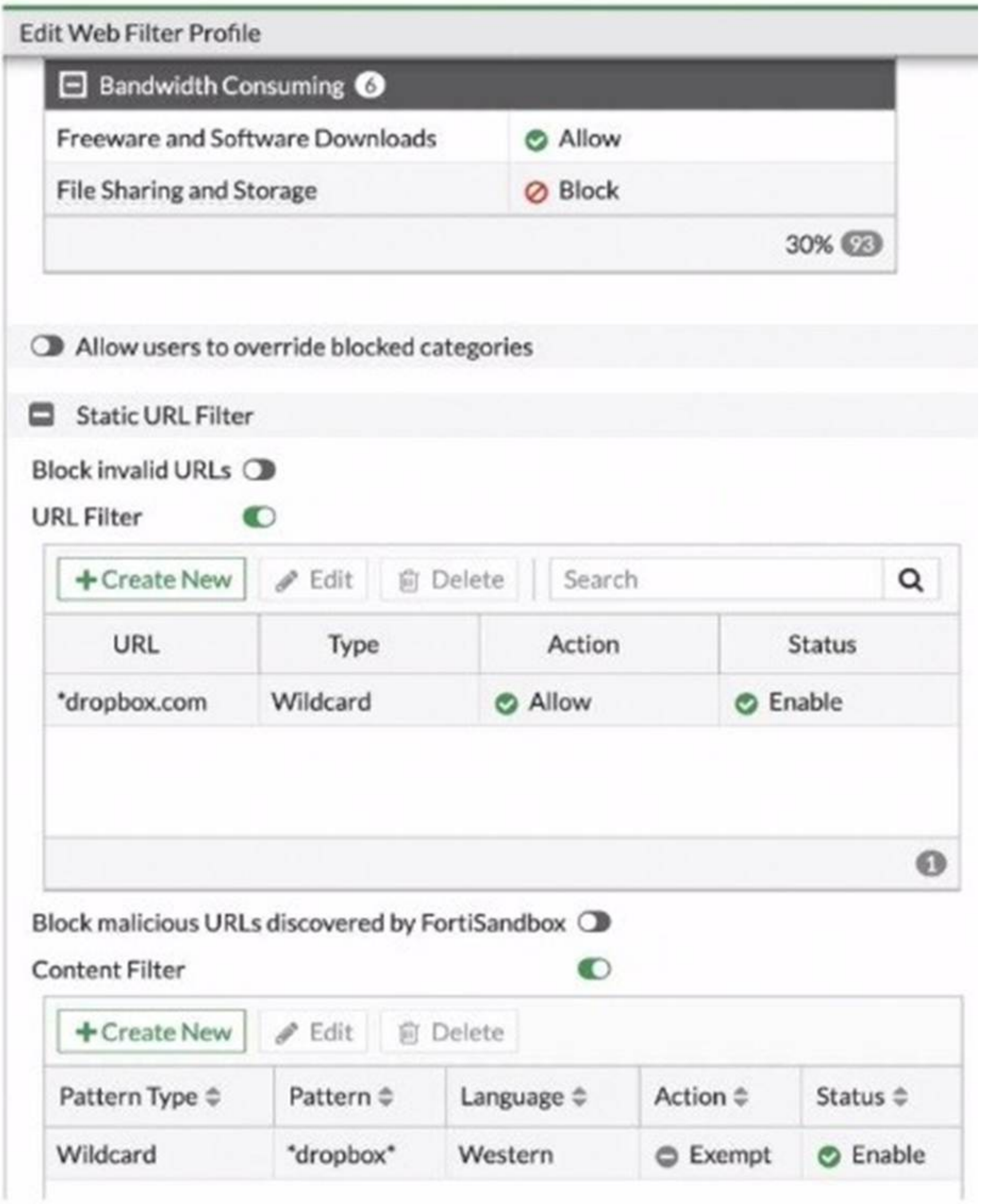


Refer to the exhibit, which shows a partial output of diagnose hardware aysinfo memory. Which two statements about the output are true? (Choose two.)

A. There are 98908 kB o! 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: AD

NEW QUESTION 2
Exhibit.



Refer to the exhibit, which shows a partial web fillet profile configuration.
Which action does FortiGate lake if a user attempts to access www. dropbox. com, which is categorized as File Sharing and Storage?

A. FortiGate allows the connection, based on the URL Filter configuration.
B. FortiGate blocks the connection as an invalid URL.
C. FortiGate exempts the connection, based on the Web Content Filter configuration.
D. FortiGate blocks the connection, based on the FortiGuard category based filter configuration.

Answer: D

NEW QUESTION 3
In which two slates is a given session categorized as ephemeral? (Choose two.)

A. A UDP session with only one packet received
B. A UOP session with packets sent and received
C. A TCP session waiting for the SYN ACK
D. A TCP session waiting for FIN ACK

Answer: AC

NEW QUESTION 4
Refer to the exhibits.

```
FGT-B # get router info routing-table all
Routing table for VRF=0
S*      0.0.0.0/0 [10/0] via 192.168.1.1, port1, [1/0]
C       10.23.23.0/24 is directly connected, port4
```

```
FGT-B # get router info ospf database brief
...
                AS External Link States

Link ID         ADV Router      Age  Seq#       CkSum Flag Route                Tag
8.8.8.8         0.0.0.112       1464 80000002 3106  0002 E2 8.8.8.8/32       0
```

An administrator Is expecting to receive advertised route 8.8.8.8/32 from FGT-A. On FGT-B, they confirm that the route is being advertised and received, however, the route is not being injected into the routing table. What is the most likely cause of this issue?

A. A batter route to the 8.8.8.8/32 network exists in the routing table.
B. FGT-B is configured with a prefix list denying the 8.8.8.8/32 network to be injected into the routing table.
C. The administrator has misconfigured redistribution of routes on FGT-A.
D. FGT-8 is configured with a distribution list denying the 8.8.8.8/32 network to be injected into the routing table.

Answer: B

NEW QUESTION 5
Consider the scenario where the server name indication (SNI) does not match either the common name (CN) or any of the subject alternative names (SAN) in the server certificate.
Which action will FortiGate take when using the default settings for SSL certificate inspection?

A. FortiGate uses the SNI from the user's web browser.
B. FortiGate closes the connection because this represents an invalid SSL/TLS configuration.
C. FortiGate uses the first entry listed in the SAN field in the server certificate.
D. FortiGate uses the CN information from the Subject field in the server certificate.

Answer: D

Explanation:
When FortiGate performs SSL certificate inspection with default settings, it checks if the Server Name Indication (SNI) matches either the Common Name (CN) or any Subject Alternative Name (SAN) in the server certificate. If there is no match, FortiGatedoes not block the connection; instead, it uses the CN value from the certificate's subject field to continue web filtering and categorization.
This behavior is described in the official Fortinet 7.6.4 Administration Guide:
"Check the SNI in the hello message with the CN or SAN field in the returned server certificate: Enable: If it is mismatched, use the CN in the server certificate."
This is the default (Enable) mode, which differs from the Strict mode that would block the mismatched connection.
By default, this policy ensures service continuity and prevents disruptions due to certificate mismatches, allowing FortiGate to log and inspect based on the CN even when the requested SNI does not match. It provides a balance between connection reliability and the accuracy of filtering by certificate identity, allowing security policies to remain functional without unnecessary blocks. This approach is recommended by Fortinet to maintain usability for end-users while still supporting granular inspection.
[References:, FortiGate 7.6.4 Administration Guide: Certificate Inspection?, SSL/SSH Inspection Profile Configuration,]

NEW QUESTION 6
Refer to the exhibit, which shows the partial output of a real-time OSPF debug.

Real-time OSPF debug output

```
OSPF: RECV[Hello]: From 0.0.0.112 via port2:192.168.37.114 (192.168.37.115 -> 224.0.0.5)
OSPF: ----------------------------------------------------
OSPF: Header
OSPF:   Version 2
OSPF:   Type 1 (Hello)
OSPF:   Packet Len 48
OSPF:   Router ID 0.0.0.112
OSPF:   Area ID 0.0.0.0
OSPF:   Checksum 0x2f85
OSPF:   AuType 0
OSPF: Hello
OSPF:   NetworkMask 255.255.255.0
OSPF:   HelloInterval 10
OSPF:   Options 0x2 (*|-|-|-|-|-|E|-)
OSPF:   RtrPriority 1
OSPF:   RtrDeadInterval 40
OSPF:   DRouter 192.168.37.114
OSPF:   BDRouter 192.168.37.115
OSPF:   # Neighbors 1
OSPF:     Neighbor 0.0.0.111
OSPF: ----------------------------------------------------
OSPF: RECV[Hello]: From 0.0.0.112 via port2:192.168.37.114: Authentication type mismatch
```

Why are the two FortiGate devices unable to form an adjacency?

A. The Hello packet is being sent from an OSPF router with ID 0.0.0.112.
B. The two FortiGate devices attempting adjacency are in area 0.0.0.0.
C. One FortiGate device is configured to require authentication, while the other is not.
D. The passwords on the FortiGate devices do not match.

Answer: C

NEW QUESTION 7
Refer to the exhibit, which contains the output of diagnose vpn tunnel list.

```
# diagnose vpn tunnel list
name=DialUp_0 ver=1 serial=4 10.200.1.1:4500->10.200.3.2:64916 tun_id=10.200.3.2 dst_mtu=1500 dpd-link=on remote_location=0.0.0.0 weight=1
bound_if=3 lgwy=static/1 tun=intf/0 mode=dial_inst/3 encap=none/896 options[0380]=rgwy-chg rport-chg frag-rfc  run_state=0 accept_traffic=1 overlay_id=0
parent=DialUp index=0
proxyid_num=1 child_num=0 refcnt=5 ilast=0 olast=0 ad=/0
stat: rxp=221 txp=0 rxb=35360 txb=0
dpd: mode=active on=1 idle=5000ms retry=3 count=0 seqno=70
natt: mode=silent draft=32 interval=10 remote_port=64916
proxyid=DialUp proto=0 sa=1 ref=2 serial=3 add-route
  dst: 0:0.0.0.0-255.255.255.255:0
  src: 0:10.0.10.10-10.0.10.10:0
  SA:  ref=3 options=82 type=00 soft=0 mtu=1422 expire=43065/0B replaywin=2048
       seqno=1 esn=0 replaywin_lastseq=00000079 itn=0 qat=0 hash_search_len=1
  life: type=01 bytes=0/0 timeout=43188/43200
  dec: spi=5ed4aafc esp=aes key=16 054852d43abb0e931641b4e8878dd9ce
       ah=sha1 key=20 082eafd018bf7d4d7b65d9c5b7448db5cc01f81d
  enc: spi=69d4231e esp=aes key=16 d5a23d09ab4128d094ac972f5511f9db
       ah=sha1 key=20 54eac30e29ce711d2ceaab9b5e179c20bb83605e
  dec:pkts/bytes=120/10080, enc:pkts/bytes=0/0
```

Which command will capture ESP traffic for the VPN named DialUp_0?

A. diagnose sniffer packet any 'ip proto 50'
B. diagnose sniffer packet any 'host 10.0.10.10'
C. diagnose sniffer packet any 'esp and host 10.200.3.2'
D. diagnose sniffer packet any 'port 4500'

Answer: D

NEW QUESTION 8
Refer to the exhibit, which shows the output of a policy route table entry.

```
id=2113929223 static_route=7 dscp_tag=0xff 0xff flags=0x0 tos=0x00 tos_mask=0x00 protocol=0 sport=0-0 iif=0 dport=1-65535 path(1) oif=3(port1) gwy=192.2.0.2
source wildcard(1): 0.0.0.0/0.0.0.0
destination wildcard(1): 0.0.0.0/0.0.0.0
internet service(1): Fortinet-FortiGuard(1245324,0,0,0)
hit_count=0 last_used=2022-02-23 06:39:07
```

Which type of policy route does the output show?

A. An ISDB route
B. A regular policy route
C. A regular policy route, which is associated with an active static route in the FIB
D. An SD-WAN rule

Answer: A

NEW QUESTION 9
The local OSPF router is unable to establish adjacency with a peer.
Which two things should the administrator do to troubleshoot the issue? (Choose two.)

A. Check whether TCP port 179 is blocked.
B. Check if there is an active static route to the peer.
C. Check whether both peers have an IP address within the same subnet.
D. Check if IP protocol 89 is blocked.

Answer: CD

NEW QUESTION 10
Refer to the exhibit, which shows a partial output of the real-time LDAP debug.

```
# fnbamd_fsm.c[1274] handle_req-Rcvd auth req 6750221 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=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 6750221
fnbamd_ldap.c[275] get_all_dn-Found no DN
fnbamd_ldap.c[298] start_next_dn_bind-No more DN left
fnbamd_ldap.c[1603] fnbamd_ldap_get_result-Auth denied
fnbamd_auth.c[2074] fnbamd_auth_poll_ldap-Result for ldap svr 10.10.181.10 is denied
fnbamd_comm.c[116] fnbamd_comm_send_result-Sending result 1 for req 6750221
```

What two actions can the administrator take to resolve this issue? (Choose two.)

A. Ensure the user logs in using 'John Smith' not 'jsmith'.
B. Ensure the user is providing the correct user credentials.
C. Ensure the user is a member of at least one AD group to ensure step 4 of the LDAP authentication process is successful.
D. Ensure the account is active.

Answer: BD

NEW QUESTION 10
Exhibit.

```
session info: proto=6 proto_state=01 duration=157 expire=3559 timeout=3600 flags=00000000 socktype=0 sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
user=User1 state=log may_dirty authed f00 acct-ext
statistic(bytes/packets/allow_err): org=2137/14/1 reply=1663/12/1 tuples=2
tx speed(Bps/kbps): 1/0 rx speed(Bps/kbps): 1/0
orgin->sink: org pre->post, reply pre->post dev=5->3/3->5 gwy=10.1.0.254/10.1.10.1
hook=pre dir=org act=noop 10.1.10.1:34830->35.241.9.150:443(0.0.0.0:0)
hook=post dir=reply act=noop 35.241.9.150:443->10.1.10.1:34830(0.0.0.0:0)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=1 pol_uuid_idx=14735 auth_info=2 chk_client_info=0 vd=0
serial=0000352e tos=ff/ff app_list=0 app=0 url_cat=0
rpdb_link_id=00000000 ngfwid=n/anpu_state=0x000100
no_ofld_reason:  npu-flag-off
```

Refer to the exhibit, which shows the output of a session. Which two statements are true? (Choose Two.)

A. The TCP session has been successfully established.
B. The session was initiated from an authenticated user.
C. The session is being inspected using flow inspection.
D. The session is being offloaded.

Answer: AB

NEW QUESTION 14
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.
[References:, Fortinet FortiGate Handbook: Parallel Path Processing, Fortinet FortiOS Technical Documentation: Packet Flow and Path Selection,]

NEW QUESTION 18
Refer to the exhibit, which shows one way communication of the downstream FortiGate with the upstream FortiGate within a Security Fabric.

```
# diagnose sniffer packet any "tcp port 8013 or udp port 8014" 4
Using Original Sniffing Mode
interfaces=[any]
filters=[tcp port 8013 or udp port 8014]
47.220358 port1 in 192.168.1.112.11234 -> 192.168.1.111.8013: syn 1204417526
48.215338 port1 in 192.168.1.112.11234 -> 192.168.1.111.8013: syn 1204417526
50.218552 port1 in 192.168.1.112.11234 -> 192.168.1.111.8013: syn 1204417526
54.222117 port1 in 192.168.1.112.11234 -> 192.168.1.111.8013: syn 1204417526
```

What three actions must you take to ensure successful communication? (Choose three.)
A. You must authorize the downstream FortiGate on the root FortiGate.
B. FortiGate must not be in NAT mode.
C. Ensure TCP port 8013 is not blocked along the way.
D. You must enable Security Fabric/Fortitelemetry on the receiving interface of the upstream FortiGate.
E. Ensure the port for Neighbor Discovery has been changed.
A.

Answer: ACD

NEW QUESTION 23
Which exchange lakes care of DoS protection in IKEv2?

A. Create_CHILD_SA
B. IKE_Auth
C. IKE_Req_INIT
D. IKE_SA_NIT

Answer: C

Explanation:
TheIKE_SA_INITexchange in IKEv2 is responsible for DoS protection measures. During IKE_SA_INIT, before authentication and further exchange, the responder can use cookie challenges (per RFC 7296 and Fortinet VPN documentation). If a DoS attack is suspected (many requests from the same source), the responder replies with a cookie. Only after the initiator returns the correct cookie does the exchange proceed, protecting the responder from state exhaustion and certain forms of DoS traffic at the handshake stage.
FortiOS VPN Manual: IKEv2 Exchange Process and DoS Protections
IKEv2 RFC 7296: Description of IKE_SA_INIT and DoS Cookie Mechanism

NEW QUESTION 28
Refer to the exhibit, which shows a session entry.

```
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
```

Which statement about this session is true?

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, thehook=post

dir=org act=snatshows 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.
FortiOS Administration Guide: Session Table, NAT, and Route Interaction
Fortinet Technical Note: Diagnose sys session list, Direction and NAT Analysis

NEW QUESTION 31
Refer to the exhibit, which shows the output of the command get router info bgp neighbors 100.64.2.254 advertised-routes.

```
# get router info bgp neighbors 100.64.2.254 advertised-routes

VRF 0 BGP table version is 3, local router ID is 172.16.1.254
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network              Next Hop      Metric LocPrf   Weight RouteTag Path

*> 10.20.30.40/24    100.64.2.1           xxx       0        0          100 i <-/->

Total number of prefixes 1
```

What can you conclude from the output?

A. The BGP state of the two BGP participants is OpenConfirm.
B. The router ID of the neighbor is 100.64.2.254.
C. The BGP neighbor is advertising the 10.20.30.40/24 network to the local router.
D. The local router is advertising the 10.20.30.40/24 network to its BGP neighbor.

Answer: D

NEW QUESTION 33
Refer to the exhibit, which shows the output of a BGP debug command.

```
# 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
```

What can you conclude about the router in this scenario?
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.

A.

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.
FortiOS BGP Debugging Guide: Session State Interpretation
BGP CLI Reference: Neighbor Status Fields

NEW QUESTION 38
Refer to the exhibit.

```
**** SP Login Dump ****<lasso:Login
xmlns:lasso="http://www.entrouvert.org/namespaces/lasso/0.0"
xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
LoginDumpVersion="2"><lasso:Request><samlp:AuthnRequest
ID="_EEC718A47FB37B472B205B11153ED409" Version="2.0" IssueInstant="2024-02-
21T00:58:44Z" Destination="https://10.1.10.2/saml-idp/nst/login/"
SignType="0" SignMethod="0" ForceAuthn="false" IsPassive="false"
ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
AssertionConsumerServiceURL="https://10.1.10.254:1003/remote/saml/login/"><sa
ml:Issuer>https://10.1.10.254:1003/remote/saml/metadata/</saml:Issuer><samlp:
NameIDPolicy Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified"
AllowCreate="true"/></samlp:AuthnRequest></lasso:Request><lasso:RemoteProvide
rID>http://10.1.10.2/samlidp/nst/metadata/</lasso:RemoteProviderID><lasso:Msg
Url>https://10.1.10.2/saml-
idp/nst/login/?SAMLRequest=jZJfT8IwFMW%2FytL3OW5sAZtBwhhEEtQF0AdfTN0u0GRr22%2
Fnn29vGWIwUeJLk97eX%2B85p01Q1FXDJ63dqxW8tIDWe68rhbw7GJHWKK4FSuRK1IDcFnw9uVnys
Md4Y7TVha7IGXKZEIhgrNSKeItsRJ5ms%4</lasso:HttpRequestMethod><lasso:RequestID>
_EEC718A47FB37B472B205B11153ED409</lasso:RequestID></lasso:Login>
```

The exhibit shows the output from using the command diagnose debug application samld -1 to diagnose a SAML connection.
Based on this output, what can you conclude?
A. Active Directory is used for authentication.
B. The authentication request is for an SSL VPN connection.
C. The IdP IP address is 10.1.10.254.
D. The IdP IP address is 10.1.10.2.

A.

Answer: D

NEW QUESTION 39
In IKEv2, which exchange establishes the first CHILD_SA?

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

Answer: A

Explanation:
According to RFC 7296 (IKEv2) and Fortinet's official documentation, theIKE_SA_INIT exchangeis responsible for negotiating cryptographic parameters, performing the initial Diffie-Hellman exchange, and implementing the cookie challenge mechanism for DoS protection. When the responder suspects a DoS attack (such as mass requests by the same source), it includes a cookie in the IKE_SA_INIT response. The initiator must return the cookie in its next request to prove that it truly exists at the IP address it claims, thereby mitigating resource exhaustion attacks.
This two-step exchange ensures the responder only allocates resources after successful proof of address, aligning with best security practices. Fortinet documentation confirms that this process occurs strictly in the IKE_SA_INIT phase, not in subsequent IKE_Auth or CHILD_SA exchanges.
[References:, RFC 7296: IKEv2, Section 2.6, ??Denial of Service Protection??, Fortinet FortiOS VPN Handbook: IKEv2 Exchange Process and DoS Protection Mechanism, , ,]

NEW QUESTION 42
Refer to the exhibit, which shows the output of the command get router info ospf neighbor.

```
# get router info ospf neighbor

OSPF process 0, VRF 0:
Neighbor ID     Pri   State           Dead Time   Address         Interface
0.0.0.12          1   Full/DROther    02:14:39    10.10.2.1       wan1
0.0.0.15          1   Full/BDR        04:26:37    10.10.3.2       wan2
0.0.0.18         c1   Full/ -         05:04:36    172.16.1.2      ToHub
```

To what extent does FortiGate operate when looking at its OSPF neighbors? (Choose two.)

A. The local FortiGate has at least one interface that participates in a broadcast network.

B. The local FortiGate has at least one interface that participates in a point-to-point network.
C. The local FortiGate is the DR.
D. Neighbor 0.0.0.18 is the designated router (DR).

Answer: AB

Explanation:
The command on this slide shows a summary of the statuses of all the OSPF neighbors. For each neighbor, it displays the adjacency state and if it is a DR, a BDR, or neither (DROther) Pagina 362 Enterprise_Firewall_7.2_Study. - Point-to-point networks contain only two peers, one at each end of a point-to-point link - Broadcast networks (multi-access) support more than two attached routers. They also support sending messages to multiple recipients (broadcasting). Pagina 365 Enterprise_Firewall_7.2_Study. In any multi-access network there is one DR and one BDR. Pagina 439 Network_Security_Support_Engineer_7.4_Study FULL/- This represents a point-to-point network

NEW QUESTION 47
Refer to the exhibit, which shows a partial output of the fssod daemon real-time debug command.

```
# diagnose debug application fssod -1
# diagnose debug enable
[fsso_svr.c:save_result:579] event_id=4768, logon=bobby, domain=FSSO workstation=, ip=10.124.2.90 port=49215, time=1372061722
```

What two conclusions can you draw from the output? (Choose two.)

A. The workstation with IP 10.124.2.90 will be polled frequently using TCP port 445 to see if the user is still logged on.
B. The logon event can be seen on the collector agent installed on Windows.
C. FSSO is using DC agent mode to detect logon events.
D. FSSO is using agentless polling mode to detect logon events.

Answer: AD

Explanation:
https://community.fortinet.com/t5/FortiGate/Troubleshooting-Tip-How-to-troubleshoot-FSSO-agentless-polling/ta-p/214349
From the snippet we can see that FortiGate (via the fssod daemon) is directly detecting the user logon rather than relying on a separate ??collector?? or ??DC agent.?? This indicates agentless polling—FortiGate polls the DC??s event logs over TCP 445 to discover logons. So: - FSSO is using agentless polling mode to detect logon events - In agentless mode, FortiGate will periodically poll the same IP (the DC) on port 445 to see if the user is still logged on

NEW QUESTION 51
Which authentication option can you not configure under config user radius on FortiOS?

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

Answer: D

NEW QUESTION 53
Refer to the exhibit showing a debug output.

```
# diagnose debug application authd 8256
# diagnose debug enable
....
[fsae_server_init_spec:116]: num 1, idx 0, 127.0.0.1:8000 disconnect_server_only
[FSSO]: disconnecting_event_error[Local FSSO Agent]: error occurred in read: Connection refused
....
```

An administrator deployed FSSO in DC Agent Mode but FSSO is failing on FortiGate. Pinging FortiGate from where the collector agent is deployed is successful. The administrator then produces the debug output shown in the exhibit.
What could be causing this error message?

A. The TCP port 445 is blocked between FortiGate and collector agent.
B. The collector agent preshared password is mismatched.
C. The FortiGate cannot resolve the active directory server name.
D. The FortiGate and the collector agent are using different TCP ports.

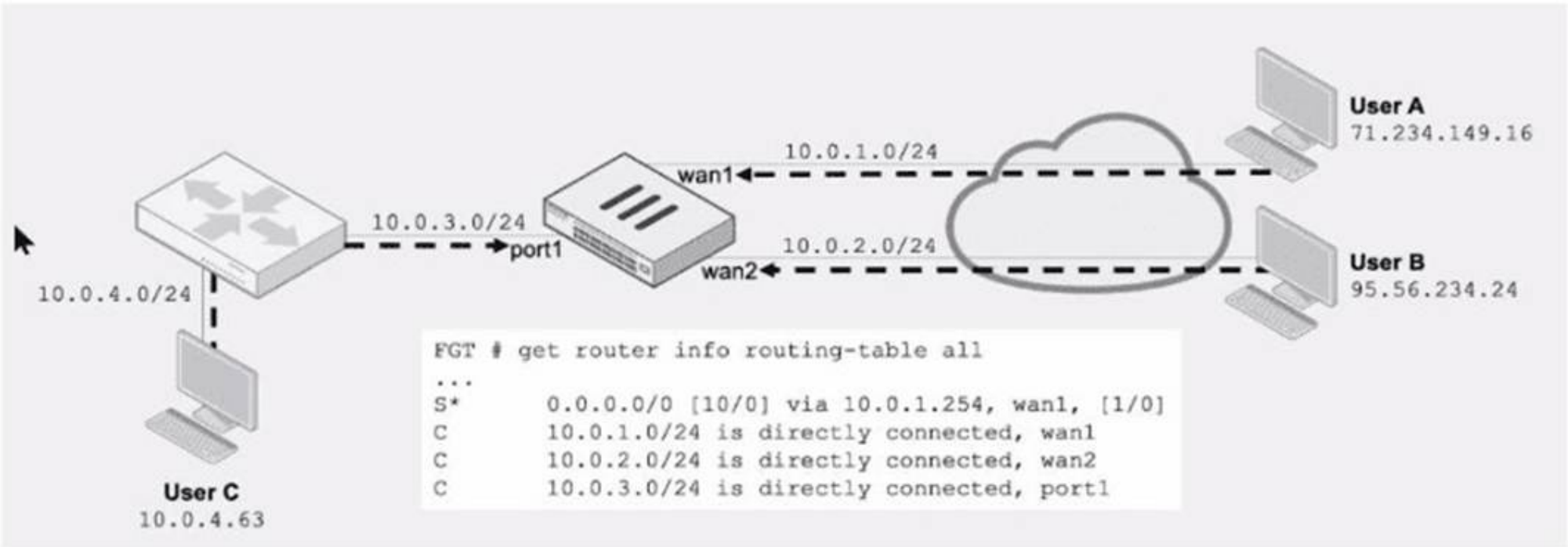
Answer: D

NEW QUESTION 55
Which statement about IKEv2 is true?

A. Both IKEv1 and IKEv2 share the feature of asymmetric authentication.
B. IKEv1 and IKEv2 have enough of the header format in common that both versions can run over the same UDP port.
C. IKEv1 and IKEv2 use same TCP port but run on different UDP ports.
D. IKEv1 and IKEv2 share the concept of phase1 and phase2.

Answer: B

NEW QUESTION 56
Refer to the exhibit.



Assuming a default configuration, which three statements are true? (Choose three.)

A. Strict RPF is enabled by default.
B. User B: Fai
C. There is no route to 95.56.234.24 using wan2 in the routing table.
D. User A: Pas
E. The default static route through wan1 passes the RPF check regardless of the source IP address.
F. User B: Pas
G. FortiGate will use asymmetric routing using wan1 to reply to traffic for 95.56.234.24.
H. User C: Fai
I. There is no route to 10.0.4.63 using port1 in the touting table.

Answer: BDE

NEW QUESTION 60
Refer to the exhibit, which shows the output o! the BGP database.

```
router info bgp network
0 BGP table version is 3, local router ID is 1.1.1.1
tus codes: s suppressed, d damped, h history, * valid, > best, i - internal,
           S Stale
gin codes: i - IGP, e - EGP, ? - incomplete

Network          Next Hop            Metric     LocPrf Weight RouteTag Path
0.0.0.0/0        100.64.2.254    0              100        0         0 ? <-/->
                 100.64.2.1                              32768     0 ? <-/1>
1.2.2.1/32       100.64.2.1                              32768     0 ? <-/1>
3.8.8.8/32       100.64.2.254    0              100        0         0 ? <-/1>
10.20.30.0/24    172.16.54.115   0              100        0         0 i <-/1>

al number of prefixes 4
```

Which two statements are correct? (Choose two.)

A. The advertised prefix of 10.20.30.0'24 was configured using the network command.
B. The first four prefixes are being advertised using a legacy route advertisement.
C. The advertised prefix of 10.20.30.0'24 is being advertised through the redistribution of another routing protocol.
D. The output shows all prefixes advertised by all neighbors as well as the local router.

Answer: AD

NEW QUESTION 62
Refer to the exhibit, which shows partial outputs from two routing debug commands.

```
FortiGate # get router info kernel
tab=254 vf=0 scope=0 type=1 proto=11 prio=0 0.0.0.0/0.0.0.0/0->0.0.0.0/0 pref=0.0.0.0 qwy=100.64.1.254 dev=3 (port1)
tab=254 vf=0 scope=0 type=1 proto=11 prio=10 0.0.0.0/0.0.0.0/0->0.0.0.0/0 pref=0.0.0.0 gwy=100.64.2.254 dev=6 (port2)
tab=254 vf=0 scope=253 type=1 proto=2 prio=0 0.0.0.0/0.0.0.0/0->10.1.0.0/24 pref=10.1.0.254 gwy=0.0.0.0 dev=9 (port3)

FortiGate # get router info routing-table all

Routing table for VRF=0
S*          0.0.0.0/0 [10/0] via 100.64.1.254, port1
                             [10/0] via 100.64.2.254, port2, [10/0]
C           10.1.0.0/24 is directly connected, port3
S           10.1.10.0/24 [10/0] via 10.1.0.1, port3
C           100.64.1.0/24 is directly connected, port1
C           100.64.2.0/24 is directly connected, port2
```

Which change must an administrator make on FortiGate to route web traffic from internal users to the internet, using ECMP?

A. Set snat-route-change to enable.
B. Set the priority of the static default route using port2 to 1.
C. Set preserve-session-route to enable.
D. Set the priority of the static default route using port1 to 10.

Answer: D

NEW QUESTION 65
Refer to the exhibit, which shows a partial output of a real-time LDAP debug.

```
# 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
```

What two conclusions can you draw from the output? (Choose two.)

A. The user was found in the LDAP tree, whose root is TAC.ottawa.fortinet.com.
B. FortiOS performs a bind to the LDAP server using the user's credentials.
C. FortiOS collects the user group information.
D. FortiOS is performing the second step (Search Request) in the LDAP authentication process.

Answer: AD

NEW QUESTION 70
What are two functions of automation stitches? (Choose two.)

A. You can configure automation stitches on any FortiGate device in a Security Fabric environment.
B. You can configure automation stitches to execute actions sequentially by taking parameters from previous actions as input for the current action.
C. You can set an automation stitch configured to execute actions in parallel to insert a specific delay between actions.
D. You can create automation stitches to run diagnostic commands and attach the results to an email message when CPU or memory usage exceeds specified thresholds.

Answer: BD

NEW QUESTION 71
Exhibit.

```
# diagnose automation test HAFailOver
automation test failed(1). stitch:HAFailOver
```

Refer to the exhibit, which shows the output of diagnose automation test. What can you observe from the output? (Choose two.)

A. The automation stitch test is not being logged.
B. The automation stitch test failed but the HA failover was successful.
C. An HA failover occurred.
D. The test was unsuccessful.

Answer: AD

NEW QUESTION 72
Exhibit.

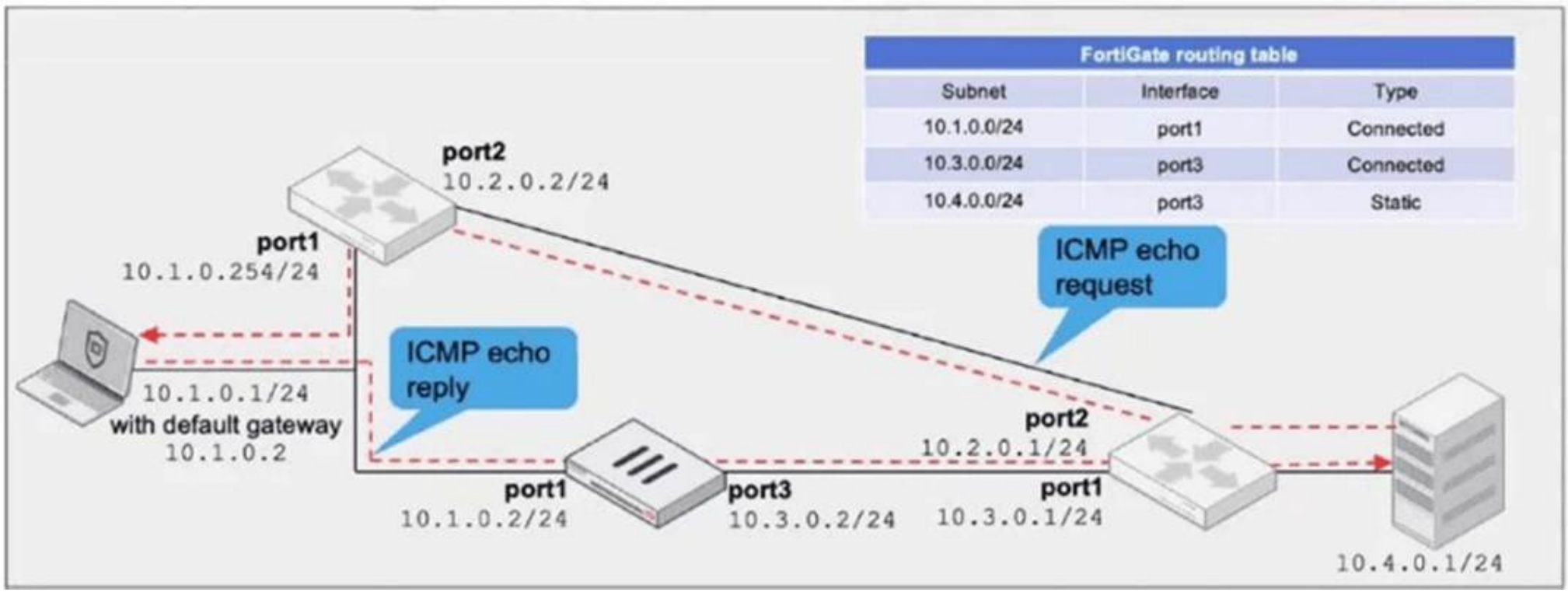
```
ike 0: comes 10.0.0.2:500->10.0.0.1:500,ifindex=7.
ike 0: IKEv1 exchange=Aggressive id=a2fbd6bb6394401a/06b89c022d4df682 1em=426
ike 0: Remotesite:3: initiator: aggressive mode get 1st response.
ike 0: Remotesite:3: VID DD AFCAD71368A1F1C96B8696FC77570100
ike 0: Remotesite:3: DPD negotiated                  FC77570100
ike 0: Remotesite:3: VID FORTIGATE 8299031757A3608
ike 0: Remotesite:3: peer is Fortifate/Fartios, (v2C6A621DE00000000
ike 0: Remotesite:3: VID FRAGMENTATION 4048B7D56EB0 bo)
ike 0: Remotesite:3: VID FRAGMENTATION 4048B7D56EBCE88525E7DE7F00D6C2D3
ike 0: Remotesite:3: received peer identifier FQDNCE88525E7DE7F00D6C2D3C0000000
ike 0: Remotesite:3: negotiation result              'remote"
ike 0: Remotesite:3: proposal id =1:
ike 0: Remotesite:3:       protocol id = ISAKMP:
ike 0: Remotesite:3:           trans id = KEY IKE.
ike 0: Remotesite:3:           encapsulation = IKE/
ike 0: Remotesite:3:               type=OAKLEY _ENCnone
ike 0: Remotesite:3:               type=OAKLEY HASHRYPT _ALG, val=AES CBC, key-len=128
ike 0: Remotesite:3:           type=AUTH METHOD, va ALG, val=SHA.
ike 0: Remotesite:3:           type=OAKLEY _GROUP, l=PRESHARED KEY.
ike 0: Remotesite:3: ISAKMP SA lifetime=86400        val=MODP1024.
ike 0: Remotesite:3: NAT-T unavailable
ike 0: Remotesite:3: ISAKMP SA a2fbd6bb6394401a/06
ike 0: Remotesite:3: ISAKMP SA a2fbd6bb6394401a/06b89c022d4df682 key 16:39915120ED73E520787C801DE3678916
ike 0: Remotesite:3: PSK authentication succeeded
ike 0: Remotesite:3: authentication OK
ike 0: Remotesite:3: add INITIAL-CONTACT
ike 0: Remotesite:3: enc A2FBD6BB6394401A06B89C022D4DF68208100401000000000000000500B000018882A07809026CA8B2
ike 0: Remotesite:3: out A2FBD6BB6394401A06B89C022D4DF68208100401000000000000000SC64D5CBA90B873F150CB8B5CCZA
ike 0: Remotesite:3: sent IKE msg (agg i2send): 10.0.0.1:500->10.0.0.2:500, len=140, id=a2fbd6bb6394401a/
ike 0: Remotesite:3: established IKE SA a2fbd6bb6394401a/06689c022d4df682
```

Refer to the exhibit, which contains partial output from an IKE real-time debug. Which two statements about this debug output are correct? (Choose two.)

A. Perfect Forward Secrecy (PFS) is enabled in the configuration.
B. The local gateway IP address is 10.0.0.1.
C. It shows a phase 2 negotiation.
D. The initiator provided remote as its IPsec peer ID.

Answer: CD

NEW QUESTION 73
Refer to the exhibit, which a network topology and a partial routing table.



FortiGate has already been configured with a firewall policy that allows all ICMP traffic to flow from port1 to port3.
Which changes must the administrator perform to ensure the server at 10.4.0.1/24 receives the echo reply from the laptop at 10.1.0.1/24?

A. Enable asymmetric routing under config system settings.
B. Change the configuration from strict RPF check mode to feasible RPF check mode.
C. A firewall policy that allows all ICMP traffic from port3 to port1.
D. Modify the default gateway on the laptop from 10.1.0.2 to 10.2.0.2.

Answer: A

NEW QUESTION 78
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

FCSS_NST_SE-7.6 Practice Exam Features:

* FCSS_NST_SE-7.6 Questions and Answers Updated Frequently

* FCSS_NST_SE-7.6 Practice Questions Verified by Expert Senior Certified Staff

* FCSS_NST_SE-7.6 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* FCSS_NST_SE-7.6 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year