



Fortinet

Exam Questions FCSS_NST_SE-7.6

FCSS - Network Security 7.6 Support Engineer

About ExamBible

Your Partner of IT Exam

Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1

What are two reasons you might see iprobe_in_check() check failed, drop when using the debug flow? (Choose two.)

- A. Packet was dropped because of policy route misconfiguration.
- B. Packet was dropped because of traffic shaping.
- C. Trusted host list misconfiguration.
- D. VIP or IP pool misconfiguration.

Answer: CD

NEW QUESTION 2

Exhibit.

```
config system fortiguard
  set protocol udp
  set port 8888
  set load-balance-servers1
  set auto-join-forticloud enable
  set update-server-location any
  set sandbox-region ''
  set fortiguard-anycast disable
  set antispam-force-off disable
  set antispam-cache enable
  set antispam-cache-ttl 1800
  set antispam-cache-mpercent2
  set antispam-timeout 7
  set webfilter-force-off enable
  set webfilter-cache enable
  set webfilter-cache-ttl 3600
  set webfilter-timeout 15
  set sdns-server-ip "208.91.112.220"
  set sdns-server-port 53
  unset sdns-options
  set source-ip 0.0.0.0
  set source-id6 ::
  set proxv-server-ip 0.0.0.0
  set proxy-server-port 0
  set proxy-username
  set ddns-server-ip 0.0.0.0
  set dons-server-port 443
end
```

Refer to the exhibit, which shows a FortiGate configuration.

An administrator is troubleshooting a web filter issue on FortiGate. The administrator has configured a web filter profile and applied it to a policy; however the web filter is not inspecting any traffic that is passing through the policy.

What must the administrator do to fix the issue?

- A. Disable webfilter-force-off.
- B. Increase webfilter-timeout.
- C. Enable fortiguard-anycast.
- D. Change protocol to TCP.

Answer: A

NEW QUESTION 3

Refer to the exhibit, which shows a truncated output of a real-time LDAP debug.

```
# diagnose debug application fnbamd -l
# 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 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: BD

NEW QUESTION 4

Web filter profile

Edit Web Filter Profile

Bandwidth Consuming 6

Freeware and Software Downloads	☒ Allow
File Sharing and Storage	☐ Block

30% 93

☐ Allow users to override blocked categories

Static URL Filter

Block invalid URLs ☐

URL Filter ☒

[+ Create New](#)
 [Edit](#)
 [Delete](#)

[Q](#)

URL	Type	Action	Status
*dropbox.com	Wildcard	☒ Allow	☒ Enable

1

Block malicious URLs discovered by FortiSandbox ☐

Content Filter ☒

[+ Create New](#)
 [Edit](#)
 [Delete](#)

Pattern Type ⇅	Pattern ⇅	Language ⇅	Action ⇅	Status ⇅
Wildcard	*dropbox*	Western	☐ Exempt	☒ Enable

A. FortiGate blocks the connection as an invalid URL.
B. Based on the URL Filter configuration, FortiGate allows the connection.
C. FortiGate blocks the connection, based on the FortiGuard category-based filter configuration.
D. Based on the Web Content filter configuration, access to www.dropbox.com would be exempted.

NEW QUESTION 5

Your Partner of IT Exam

- 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, FortiGate does 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

Which three common FortiGate-to-collector-agent connectivity issues can you identify using the FSSO real-time debug? (Choose three.)

- A. Log is full on the collector agent.
- B. Inability to reach IP address of the collector agent.
- C. Refused connectio
- D. Potential mismatch of TCP port.
- E. Mismatched pre-shared password.
- F. Incompatible collector agent software version.

Answer: BCD

NEW QUESTION 7

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 8

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 9

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 10

Refer to the exhibit, which shows the output of a debug command.

```
FGT # get router info ospf interface port4
port4 is up, line protocol is up
Internet Address 172.20.121.236/24, Area 0.0.0.0, MTU 1500
Process ID 0, VRF 0, Router ID 0.0.0.4, Network Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State DROther, Priority 1

Designated Router (ID) 172.20.140.2, Interface Address 172.20.121.2

Backup Designated Router (ID) 0.0.0.1, Interface Address 172.20.121.239
Timer intervals configured, Hello 10.000, Dead 40, Wait 40, Retransmit 5

Hello due in 00:00:05
Neighbor Count is 4, Adjacent neighbor count is 2
Crypt Sequence Number is 411
Hello received 106 sent 27, DD received 6 sent 3
LS-Req received 2 sent 2, LS-Upd received 7 sent 17
LS-Ack received 4 sent 3, Discarded 1
```

Which two statements about the output are true? (Choose two.)

- A. The interlace is part of the OSPF backbone area.
- B. There are a total of five OSPF routers attached to the vorz4 network segment
- C. One of the neighbors has a router ID of 0.0.0.4.
- D. In the network connected to port4, two OSPF routers are down.

Answer: AB

Explanation:

FortiOS Admin Guide: OSPF, Debug Outputs

NEW QUESTION 10

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 12

Which exchange takes care of DoS protection in IKEv2?

- A. Create_CHILD_SA
- B. IKE_Auth
- C. IKE_Req_INIT
- D. IKE_SA_INIT

Answer: C

Explanation:

The IKE_SA_INIT exchange 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 15

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 20

Which two statements about Security Fabric communications are true? (Choose two.)

- A. FortiTelemetry and Neighbor Discovery both operate using TCP.
- B. The default port for Neighbor Discovery can be modified.
- C. FortiTelemetry must be manually enabled on the FortiGate interface.
- D. By default, the downstream FortiGate establishes a connection with the upstream FortiGate using TCP port 8013.

A.

Answer: CD

Explanation:

FortiTelemetry is a critical part of Security Fabric communications and requires explicit configuration for each participating FortiGate interface. The administrative access setting 'fabric' (corresponding to FortiTelemetry) must be manually enabled per interface on both upstream and downstream devices. This is performed in the GUI under Administrative Access or via the CLI using the commandset allowaccess fabricfor the relevant network interface. Without this step, FortiTelemetry communications will not occur on that interface.

Additionally, the default communication between downstream and upstream FortiGate units in the Security Fabric is over TCP port 8013. This port is well-documented as the standard for Security Fabric and FortiTelemetry connections, and must be open and permitted across the network path for connectivity and status enforcement between units. The downstream FortiGate initiates the connection to the upstream via this port unless otherwise configured. This has also been documented as a PCI-relevant port, showing its default usage.

Other options:

Neighbor Discovery in FortiOS uses IPv6 ND protocol, not TCP.

FortiTelemetry port (8013) can be modified, but the interface Administrative Access for the Security Fabric must be manually enabled; Neighbor Discovery port modification is not documented as a supported change for FortiGate.

FortiGate/FortiOS Administration Guide: Enabling FortiTelemetry (fabric) on interfaces

Fortinet Technical Tip: FortiTelemetry uses TCP port 8013 by default

PCI compliance documentation on port 8013 usage for Security Fabric

Fortinet Security Fabric setup procedures and interface options

NEW QUESTION 22

Refer to the exhibit, which shows the partial output of a diagnose command.

```
# diagnose sys session list expectation
session info: proto=6 proto_state=00 duration=6 expire=23 timeout=3600 refresh_dir=both flags=00000000 sockflag=00000000
sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
ha_id=0 policy_dir=1 tunnel=/
state=new npu acct-ext complex
statistic(bytes/packets/allow_err): org=0/0/0 reply=0/0/0 tuples=2
origin->sink: org pre->post, reply pre->post dev=5->7/7->5 gwy=10.1.1.2/172.17.97.3

hook=pre dir=org act=dnat 93.157.14.94:0->10.200.1.1:60428(10.0.1.10:55402)
hook=pre dir=org act=noop 0.0.0.0:0->0.0.0.0:0(0.0.0.0:0)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=25 id_policy_id=0 auth_info=0 chk_client_info=0 vd=0
serial=008423f4 tos=ff/ff ips_view=0 app_list=0 app=0
```

Which two conclusions can you draw from the output shown in the exhibit? (Choose two.)

- A. FortiGate will drop the expected traffic if it does not arrive within 23 seconds.
- B. Clearing the master session has no impact on the expectation session.
- C. This is a pinhole session to allow traffic for a TCP protocol that dynamically assigns TCP ports.
- D. The session is checked against firewall policy ID 25.

A.

Answer: AC

NEW QUESTION 24

Refer to the exhibit, which shows the port1 interface configuration on FortiGate and partial session information for ICMP traffic.

```
config system interface
  edit "port1"
    set preserve-session-route enable
  next
end

# diagnose sys session list
session info: proto=1 proto_state=00 duration=4 expire=55 timeout=0 refresh_dir=both flags=00000000 socktype=0 sockport=0 av_idx=0 use=3
state-log may_dirty npu f00 route_preserve
origin->sink: org pre->post, reply pre->post dev=7->19/19->7 gwy=100.64.1.1/10.0.1.101

# diagnose netlink interface list | grep index=19
if=port1 family=00 type=768 index=19 mtu=1420 link=0 master=0
```

What happens to the session information if a routing change occurs that affects this session?

- A. Only the interface and gateway information for dev=7 will be removed.
- B. The session information will not change unless the current route has been removed from the routing table.
- C. The session will be flagged as dirty but no route lookups will be performed.
- D. Sessions involving port7 or port19 will not have their routing information flushed.

A.

Answer: B

NEW QUESTION 25

Refer to the exhibit, which shows the output of get router info bgp summary.

```
get router info bgp summary

VRF 0 BGP router identifier 172.16.1.254, local AS number 65100
BGP table version is 3
2 BGP AS-PATH entries
0 BGP community entries

Neighbor      V      AS MsgRcvd MsgSent  TblVer  InQ  OutQ Up/Down  State/PfxRcd
100.64.1.254   4      100     18     20       3    0    0 00:02:55        1
100.64.2.254   4      100      0      0       0    0    0 never        Active

Total number of neighbors 2
```

Which two statements are true? (Choose two.)

- A. The local FortiGate has received one prefix from BGP neighbor 100.64.1.254.
- B. The TCP connection with BGP neighbor 100.64.2.254 was successful.
- C. The local FortiGate has received 18 packets from a BGP neighbor.
- D. The local FortiGate is still calculating the prefixes received from BGP neighbor 100.64.2.264

Answer: AC

Explanation:

The get router info bgp summary output lists BGP neighbor status:
Prefix Reception: The "State/PfxRcd" column shows the number of prefixes received from the neighbor—neighbor 100.64.1.254 has "1", confirming option A.
Received Message Count: Under "MsgRcvd", 18 packets have been received from neighbor 100.64.1.254. This matches option C.
The second neighbor 100.64.2.254 is in "Active" state and has received/sent 0 packets, indicating that its TCP connection is NOT established, disproving option B.
There is no indication anywhere that the router is "still calculating" prefixes; "Active" just means no session is established, so option D is incorrect.
[References:, , FortiOS BGP Command Reference: BGP Neighbor States, PfxRcd, and Counters]

NEW QUESTION 27

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 30

Refer to the exhibit, which contains partial output from an IKE real-time debug.

Debug output

```
ike 0:624000:98: responder: main mode get 1st message...
ike 0:624000:98: VID DPD AFCAD71368A1F1C96B8696FC77570100
ike 0:624000:98: VID FRAGMENTATION 4048B7D56EBCE88525E7DE7F00D6C2D3
ike 0:624000:98: VID FRAGMENTATION 4048B7D56EBCE88525E7DE7F00D6C2D3C0000000
ike 0:624000:98: VID FORTIGATE 8299031757A36082C6A621DE00000000
ike 0:624000:98: incoming proposal:
ike 0:624000:98: proposal id = 0:
ike 0:624000:98:   protocol id = ISAKMP:
ike 0:624000:98:   trans_id = KEY_IKE.
ike 0:624000:98:   encapsulation = IKE/none
ike 0:624000:98:   type=OAKLEY_ENCRYPT_ALG, val=AES_CBC, key-len=256
ike 0:624000:98:   type OAKLEY_HASH_ALG, val=SHA2_256.
ike 0:624000:98:   type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:624000:98:   type=OAKLEY_GROUP, val=MODP2048.
ike 0:624000:98: ISAKMP SA lifetime=86400
ike 0:624000:98: proposal id = 0:
ike 0:624000:98:   protocol id = ISAKMP:
ike 0:624000:98:   trans_id = KEY_IKE.
ike 0:624000:98:   encapsulation = IKE/none
ike 0:624000:98:   type OAKLEY_ENCRYPT_ALG, val=AES_CBC, key-len=256
ike 0:624000:98:   type=OAKLEY_HASH_ALG, val=SHA2_256.
ike 0:624000:98:   type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:624000:98:   type=OAKLEY_GROUP, val=MODP1536.
ike 0:624000:98: ISAKMP SA lifetime=86400
ike 0:624000:98: my proposal, gw Remotesite:
ike 0:624000:98: proposal id = 1:
ike 0:624000:98:   protocol id = ISAKMP:
ike 0:624000:98:   trans_id = KEY_IKE.
ike 0:624000:98:   encapsulation = IKE/none
ike 0:620000:98:   type=OAKLEY_ENCRYPT_ALG, val=AES_CBC, key-len=128
ike 0:624000:98:   type=OAKLEY_HASH_ALG, val=SHA.
ike 0:624000:98:   type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:624000:98:   type=OAKLEY_GROUP, val=MODP2048.
ike 0:624000:98: ISAKMP SA lifetime=86400
ike 0:624000:98: proposal id = 1:
ike 0:624000:98:   protocol id = ISAKMP:
ike 0:624000:98:   trans_id = KEY_IKE.
ike 0:624000:98:   encapsulation = IKE/none
ike 0:624000:98:   type=OAKLEY_ENCRYPT_ALG, val=AES_CBC, key-len=128
ike 0:624000:98:   type=OAKLEY_HASH_ALG, val=SHA.
ike 0:624000:98:   type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:624000:98:   type=OAKLEY_GROUP, val=MODP1536.
ike 0:624000:98: ISAKMP SA lifetime=86400
ike 0:624000:98: negotiation failure
ike Negot:: 624ea7bibba276fb/0000000000000000:98: no SA proposal chosen
```

The administrator does not have access to the remote gateway.

Based on the debug output, which configuration change the administrator make to the local gateway to resolve the phase 1 negotiation error?

- A. In the phase 1 proposal configuration, add AES256-SHA256 to the list of encryption algorithms.
- B. In the phase 1 proposal configuration, add AESCBC-SHA2 to the list of encryption algorithms.
- C. In the phase 1 network configuration, set the IKE version to 2.
- D. In the phase 1 proposal configuration, add AES128-SHA128 to the list of encryption algorithms.

Answer: A

NEW QUESTION 32

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

```
# diagnose debug application fssod -l
# 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 36

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 39

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 41

Which two statements about an auxiliary session are true? (Choose two.)

- A. With the auxiliary session setting disabled, only auxiliary sessions are offloaded.
- B. With the auxiliary session setting enable
- C. ECMP traffic is accelerated to the NP6 processor.
- D. With the auxiliary session setting enable
- E. Two sessions are created in case of routing change.
- F. With the auxiliary session setting disabled, for each traffic path
- G. FortiGate uses the same auxiliary session.

Answer: BC

NEW QUESTION 46

Exhibit.

```
NGFW-1 # get sys ha status
HA Health Status: OK
Model: FortiGate-VM64
Mode: HA A-P
Group: 0
Debug: 0
Cluster Uptime: 0 days 0:1:25
Cluster state change time: 2023-04-18 12:07:47
Primary selected using:
<2023/04/18 12:07:47> FGVM010000077649 is selected as the primary because its override priority is larger than peer member
FGVM010000077650.
ses_pickup: disable
override: disable
Configuration Status:
FGVM010000077649(updated 4 seconds ago): in-sync
FGVM010000077650(updated 1 seconds ago): out-of-sync
System Usage stats:
FGVM010000077649(updated 4 seconds ago):
sessions=166, average-cpu-user/nice/system/idle=1%/0%/0%/99%, memory=45%
FGVM010000077650(updated 1 seconds ago):
sessions=3, average-cpu-user/nice/system/idle=0%/0%/0%/100%, memory=44%
HBDEV stats:
FGVM010000077649(updated 4 seconds ago):
port7: physical/1000auto, up, rx-bytes/packets/dropped/errors=167663/567/0/0, tx=262623/656/0/0
FGVM010000077650(updated 1 seconds ago):
port7: physical/1000auto, up, rx-bytes/packets/dropped/errors=271373/680/0/0, tx=176013/592/0/0
Primary      : NGFW-1          , FGVM010000077649, HA cluster index = 1
Secondary    : NGFW-2          , FGVM010000077650, HA cluster index = 0
number of vcluster: 1
vcluster 1: work 169.254.0.2
Primary: FGVM010000077649, HA operating index = 0
Secondary: FGVM010000077650, HA operating index = 1
```

Refer to the exhibit, which shows the output of get system ha status. NGFW-1 and NGFW-2 have been up for a week. Which two statements about the output are true? (Choose two.)

- A. If a configuration change is made to the primary FortiGate at this time, the secondary will initiate a synchronization reset.
- B. If port 7 becomes disconnected on the secondary, both FortiGate devices will elect itself as primary.
- C. If FGVM...649 is rebooted
- D. FGVM...650 will become the primary and retain that role, even after FGVM...649 rejoins the cluster.
- E. If no action is taken, the primary FortiGate will leave the cluster because of the current sync status.

Answer: BC

NEW QUESTION 51

Refer to the exhibit.

Debug output

```
FGT # diagnose debug application ike -l
FGT # diagnose debug enable

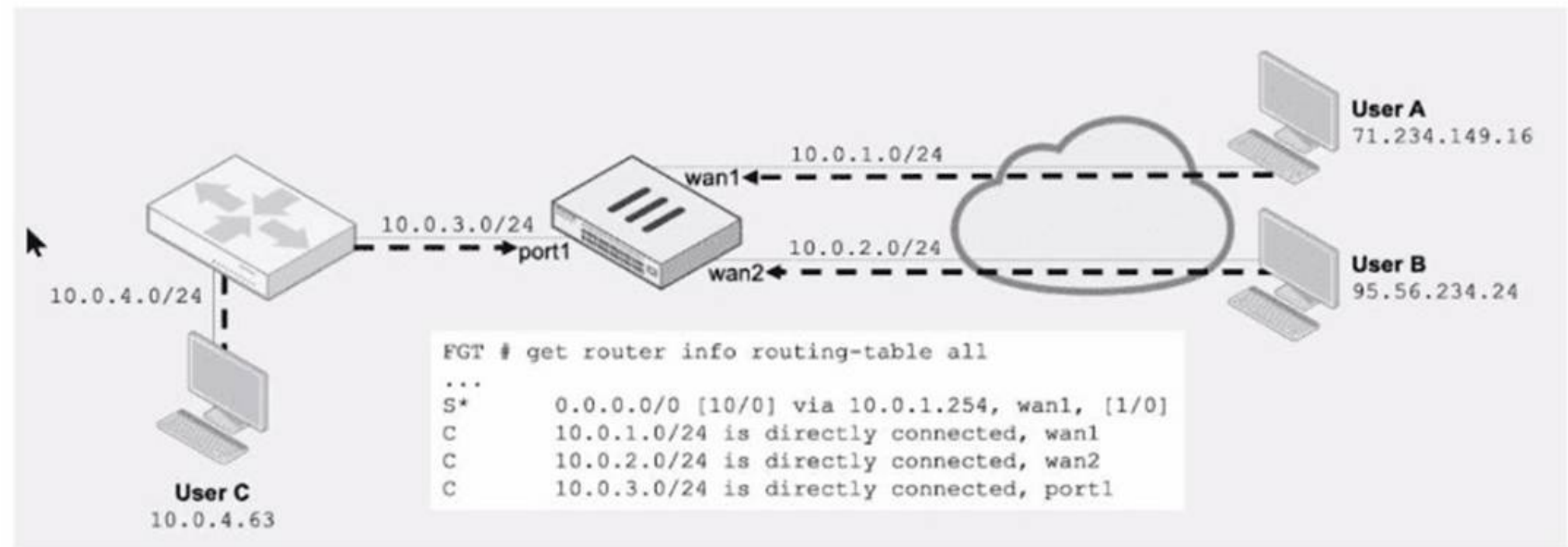
FGT # ike 0: comes 73.25.189.174:4500->96.71.182.225:4500,ifindex=18,vrf=0....
ike 0: IKEv1 exchange-Informational id=61bba3725bd738d3/265a0b7a271799b7:9e253b0b len=108 vrf=0
ike 0: in
61BBA3725BD738D3265A0B7A271799B7081005019E253B8B00000006CE306FFBD5AD97F5AD027B12CAE19C5EFA091209F6D184E10DF2548B9B1FF68F6A13167A172
26398E 051BE86CDACD29234B58E5F48024711F4EA1F216E791CB1B13650F1E4698CFASA653CE9E627C92E9
ike 0:VPN_0:24266: dec 977A47FB000000200000000101108D2861BBA3725BD738D3265A0B7A271799B70000014D85DB9684B6CFE9C681AE840B
ike 0:VPN_0:24319: notify msg received: R-U-THERE
ike 0:VPN_0:24319: enc 0F45C660000000200000000101108D2930DB9994E7E8547D50F9D18113B6CA9900000000
ike 0:VPN_0:24319: out AD893C189C22FA2E8D3B17E7FB9574BA4BF1D49AD47DE62294ECA9B8204D890A367DBDDDB20E5812CB470F87CB15504E
ike 0: comes 73.25.189.174:4500->96.71.182.225:4500,ifindex=18,vrf=0....
ike 0: IKEv1 exchange-Informational id=30db9994e7e8547d/50f9d18113b6ca99:bldd9b5f len=108 vrf=0
ike 0: in 82A79C36BC7F9ECDE1062B00FEBCE8E239F55E1F3E38196550041FDAAF20304B253855D2A3E253A6480D90
ike 0:VPN_0:24319: dec 8CC06CBD000000200000000101108D2830DB9994E7E8547D50F9D18113B6CA9900000001E186A982E6B2A3E9FBF8F30B
ike 0:VPN_0:24319: notify msg received: R-U-THERE
ike 0:VPN_0:24319: enc 11AEC31B000000200000000101108D2930DB9994E7E8547D50F9D18113B6CA99000000001
ike 0:VPN_0:24319: out E83C93D51EF44D937E260373CC9A86A09398EA3EDDD78FAEC8DE4E1F650DDC2E9E5626F34EF2346DF1807983C12E80D2
ike shrink heap by 335872 bytes
ike 0: comes 73.25.189.174:4500->96.71.182.225:4500,ifindex=18,vrf=0....
ike 0: IKEv1 exchange-Informational id=30db9994e7e8547d/50f9d18113b6ca99:a9040efb len=108 vrf=0
ike 0: in 0710D9A5184A392DC8DB96B354FF46B84E6A79622FC1D44BC7F964986AD95D49AC93BEDE376CB31EA2BD57
ike 0:VPN_0:24319: dec 03A44559000000200000000101108D2830DB9994E7E8547D50F9D18113B6CA99000000002C0D9F8CEB8B2B7CDD5CACA0B
ike 0:VPN_0:24319: notify msg received: R-U-THERE
ike 0:VPN_0:24319: enc E18A8338000000200000000101108D2930DB9994E7E8547D50F9D18113B6CA99000000002
ike 0:VPN_0:24319: out C4906BDD8812D02AE16728D0E893431344D78C31E9323A2C56E27DB43B747870885D7954558993B25BC431186958EA47
ike 0:VPN_0:24266: rcv IPsec SA delete, spi count 1
ike 0:VPN_0: deleting IPsec SA with SPI 6161297a
ike 0:VPN_0:vpn2-1: deleted IPsec SA with SPI 6161297a, SA count: 0
ike 0:VPN_0:7220167: del route 172.21.27.56/255.255.255 tunnel 73.25.189.174 of VPN_0(12922) metric 15 priority 1
ike 0:VPN_0: sending SNMP tunnel DOWN trap for vpn2-1
ike 0:VPN_0:vpn2-1: delete
```

An IPsec VPN tunnel is dropping, as shown by the debug output. Analyzing the debug output, what could be causing the tunnel to go down?

- A. Phase 2 drops but Phase 1 is up.
- B. Dead Peer Detection is not receiving its acknowledge packet.
- C. The tunnel drops during rekey negotiation.
- D. The tunnel drops after the timer expires.

Answer: B

NEW QUESTION 53
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 routing table.

Answer: BDE

NEW QUESTION 58

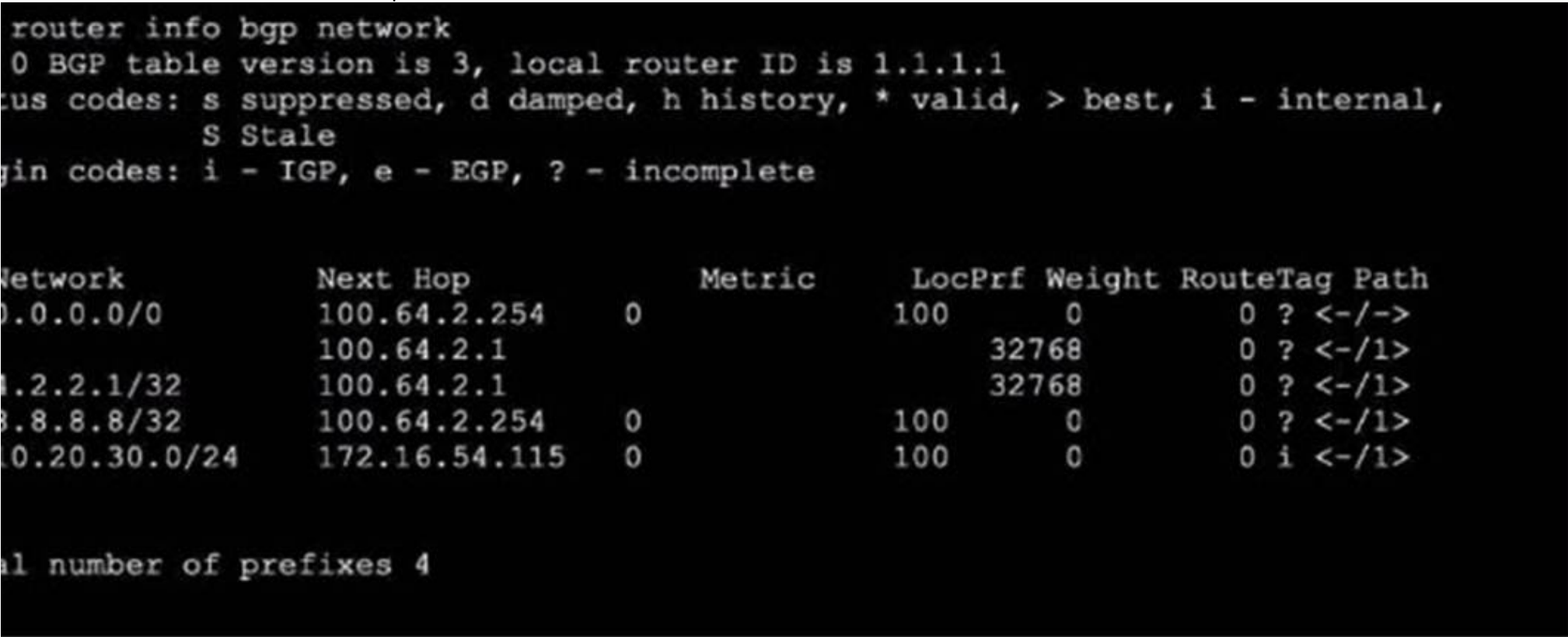
In the SAML negotiation process, which section does the Identity Provider (IdP) provide the SAML attributes utilized in the authentication process to the Service Provider (SP)?

- A. SP Login dump
- B. Authentication Response
- C. Authentication Request
- D. Assertion dump

Answer: D

NEW QUESTION 63

Refer to the exhibit, which shows the output of the BGP database.



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 68

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 gwy=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 69

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
```

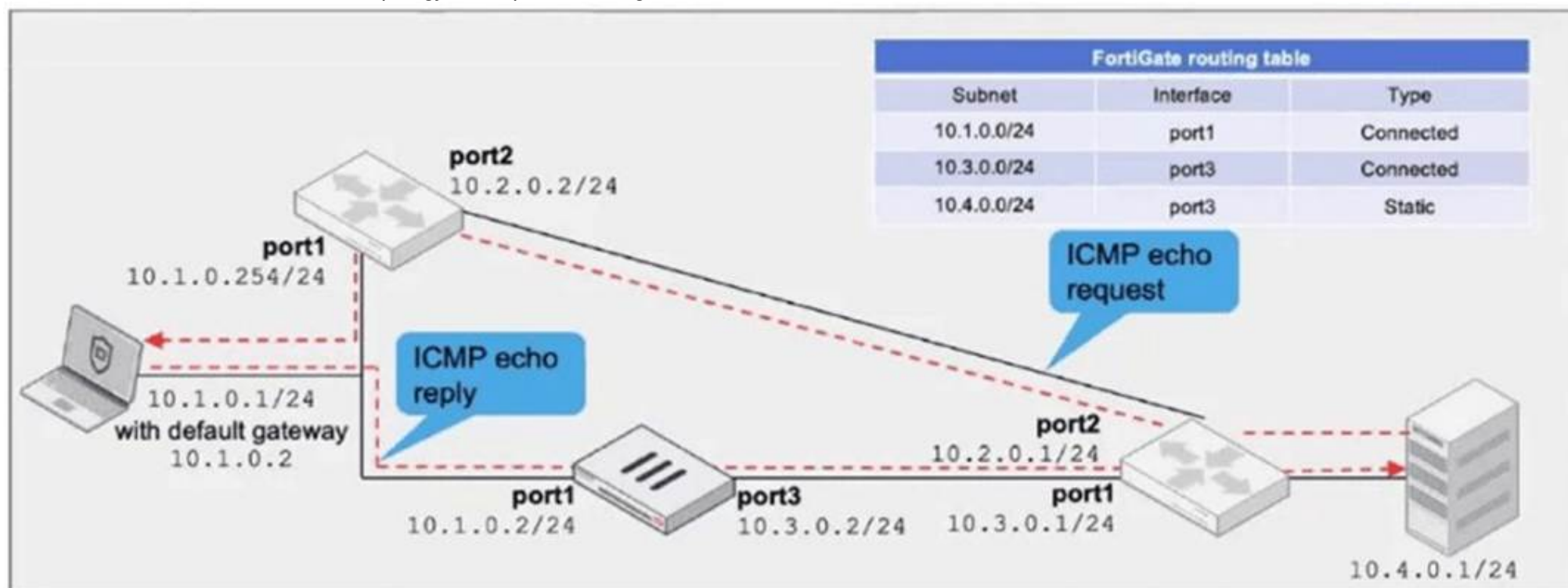
What two conclusions can you draw from the output? (Choose two.)

- 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 71

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 76

.....

Relate Links

100% Pass Your FCSS_NST_SE-7.6 Exam with Examible Prep Materials

https://www.exambible.com/FCSS_NST_SE-7.6-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>